

Logistické zabezpečení dohledových a poplachových přijímacích center

Logistic security surveillance and alarm receiving centers

Radek Holík

Bakalářská práce
2012



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Radek HOLÍK**
Osobní číslo: **A09222**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Logistické zabezpečení dohledových a poplachových přijímacích center.**

Zásady pro vypracování:

- 1. Zpracujte manuál k obsluze dohledových a poplachových center v průmyslu komerční bezpečnosti z pohledu norem EU.**
- 2. Popište funkci těchto center.**
- 3. Charakterizujte personální zabezpečení center.**
- 4. Popište technické zabezpečení center.**
- 5. Analyzujte současné problémy.**
- 6. Navrhněte řešení.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. Laucký, V. Technologie komerční bezpečnosti II. UTB Zlín. 2007 FAI ISBN 978-80-7318-631-9.
2. Laucký, V. Technologie komerční bezpečnosti I. UTB Zlín. 2010 FAI ISBN 978-80-7318-889-4.
3. Laucký, V. Řízení technol. procesů v komerční bezpečnosti. UTB Zlín. 2006 FAI ISBN 80-7318-432-X.
4. ČSN EN 50518-1. Dohledová a poplachová přijímací centra. Brusel: Cenelec, 2010
5. ČSN EN 50518-2. Dohledová a poplachová přijímací centra. Brusel: Cenelec, 2011
6. ČSN EN 50518-3. Dohledová a poplachová přijímací centra. Brusel: Cenelec, 2011
7. KAMENÍK, J a BRABEC, F. Komerční bezpečnost. Praha: ASPI, a. s., 2007. ISBN 978-80-7357-309-6.

Vedoucí bakalářské práce:

JUDr. Vladimír Laucký

Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce:

24. února 2012

Termín odevzdání bakalářské práce:

25. května 2012

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan



L.S.

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Cílem této práce je zavedení do problematiky dohledových a poplachových přijímacích center (DPPC) a popsat složení i komunikace mezi centrem a objektem. Dalším úkolem je charakterizovat technické a personální zabezpečení center. Na závěr zanalyzovat současné problémy a podívat se do budoucna v čem tyto centra můžeme využívat. Jako praktickou část popíši manuál k obsluze pro dispečery (obsluhu) dohledového a poplachového přijímacího centra z pohledu norem Evropské Unie (EU).

Klíčová slova: Dohledová a poplachová přijímací centra, technické zabezpečení, personální zabezpečení.

ABSTRACT

Aim of this thesis is to introduce the problems of surveillance and alarm receiving centres and to describe their composition and communication between centre and object. Next task is to define technical support and personnel security of these centres. In the end I analyse current problems and possibilities how to use the centres in future. In the practical part of this thesis is described handbook for operators of surveillance and alarm receiving centres in the view of European Union's norms.

Keywords: Surveillance and alarm receiving centres, technical support, personnel security.

Rád bych poděkoval vedoucímu mé bakalářské práce panu JUDr. Vladimíru Lauckému za odborné vedení, konzultace a za poskytnuté odborné informace k práci. Dále bych chtěl poděkovat panu Ivu Kolářovi za poskytnuté důležité informace a potřebné materiály a kontakty k tvorbě bakalářské práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	11
I TEORETICKÁ ČÁST	12
1 SLOŽENÍ DOHLEDOVÉHO A POPLACHOVÉHO PŘIJÍMACÍHO CENTRA	13
1.1 SAMOSTATNÝ SYSTÉM NEBOLI AUTONOMNÍ SYSTÉM.....	13
1.2 INTEGROVANÉ SYSTÉMY DO POČÍTAČE.....	13
2 KOMUNIKACE DPPC	15
2.1 JTS - ANALOG	15
2.2 ISDN – DIGITAL (DIGITÁLNÍ SÍŤ INTEGROVANÝCH SLUŽEB)	15
2.3 RÁDIOVÝ PŘENOS NA VYHRAZENÝCH FREKVENCÍCH.....	16
2.4 PŘENOS PO SÍTI GSM	17
2.4.1 Hovorové pásma.....	17
2.4.2 Prostřednictvím GPRS	17
2.4.3 Prostřednictvím SMS	17
3 TECHNICKÉ ZABEZPEČENÍ CENTRA	18
3.1 POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY.....	18
3.2 KAMEROVÝ MONITOROVACÍ SYSTÉM CCTV.....	19
3.3 POŽÁRNÍ OCHRANA	19
3.4 SÍŤOVÉ NAPÁJENÍ	19
3.5 ZÁLOŽNÍ NAPÁJENÍ.....	20
3.6 ZÁLOŽNÍ AKUMULÁTORY	20
3.7 ZÁLOŽNÍ GENERÁTORY	20
3.8 OCHRANA PŘED BLESKEM A PŘEPĚTÍ.....	21
4 PERSONÁLNÍ ZABEZPEČENÍ CENTRA	22
4.1 BEZPEČNOSTNÍ PROVĚŘENÍ PERSONÁLNÍHO OBSAZENÍ.....	22
4.2 VÝCVIK.....	22
5 UMÍSTĚNÍ A KONSTRUKČNÍ POŽADAVKY	23
5.1 VOLBA MÍSTA.....	23
5.1.1 Posouzení rizik	23
5.1.2 Přístupnost místa.....	23
5.1.3 Umístění	23
5.2 STAVEBNÍ ŘEŠENÍ.....	24
5.2.1 Konstrukce DPPC	24
5.2.1.1 Konstrukční požadavky ohledně fyzického útoku.....	24
5.2.1.2 Odolnost proti útoku střelnou zbraní	24
5.2.1.3 Ochrana proti požáru	24
5.2.1.4 Ochrana proti blesku	25
5.2.2 Příslušenství	25
5.2.3 Otvory.....	25
5.2.4 Vstupní předsíň.....	25
5.2.5 Zamykací mechanismus.....	26
5.2.5.1 Elektromechanický zámek.....	26

5.2.5.2	Mechanické zámky	27
5.2.6	Nouzový východ	27
5.2.7	Zasklené plochy	27
5.2.8	Ventilace	27
5.2.9	Technologické otvory	28
5.2.10	Manipulační okénko / propust'	28
5.3	POPLACHOVÉ SYSTÉMY	28
5.3.1	Útok zvenčí	29
5.3.2	Požár	29
5.3.3	Vchod/východ	29
5.3.4	Plyn	29
5.3.5	Komunikace	30
5.3.6	Tíseň (přepadení)	30
5.3.7	Monitorování bezpečí personálu	30
5.3.8	Signály bezpečnostních systémů	30
5.3.9	Dohled kamerovým systémem	31
5.4	NAPÁJENÍ ELEKTRICKÝM PROUDEM	31
5.4.1	Síťové napájení	31
5.4.2	Záložní zdroj napájení	31
5.4.3	Záložní akumulátor (UPS)	32
5.4.4	Pohotovostní generátor	32
6	TECHNICKÉ POŽADAVKY	33
6.1	POŽADAVKY NA VÝKONNOST	33
6.2	POŽADAVKY NA KOMUNIKACI	33
6.3	PŘÍJEM SIGNÁLU	33
6.3.1	Všeobecné požadavky	33
6.3.2	Zásah dispečera	34
7	TESTOVÁNÍ	34
7.1	VŠEOBECNĚ	34
7.2	KAŽDODENNÍ TESTY	34
7.3	TÝDENNÍ TESTY	34
7.4	POSTUPY PŘI ZÁVADÁCH A PODÁVÁNÍ ZPRÁV	34
8	ÚDAJE	35
8.1	VŠEOBECNĚ	35
8.2	ÚDAJE O ZÁKAZNÍKOVÍ	35
8.3	ÚDAJE O VNĚJŠÍ KOMUNIKACI DPPC	35
8.4	ZÁZNAM ZÁSAHU DISPEČERA	35
9	UCHOVÁVÁNÍ ÚDAJŮ	36
10	VYUŽITÍ A OVĚŘEVÁNÍ VÝKONNOSTI DPPC	36
11	NOUZOVÁ PLÁN	36
11.1	VŠEOBECNĚ	36
11.2	PŘÍKLADY ABNORMÁLNÍCH UDÁLOSTÍ	36
12	PRACOVNÍ POSTUPY A POŽADAVKY NA PROVOZ	37
13	PERSONÁLNÍ OBSAZENÍ	37

13.1	VŠEOBECNĚ.....	37
13.2	BEZPEČNOSTNÍ PROVĚŘENÍ A LUSTRACE	37
13.3	VÝCVIK	37
14	PROVOZNÍ POSTUPY.....	38
14.1	VŠEOBECNĚ.....	38
14.2	TESTOVÁNÍ.....	38
14.3	VSTUP A ODCHOD Z DPPC.....	38
14.4	SPRÁVA DATABÁZÍ.....	38
14.5	PROVOZNÍ KONTINUITA A NOUZOVÉ STAVY.....	39
14.6	EVAKUAČNÍ POSTUPY.....	40
14.6.1	Všeobecně.....	40
14.6.2	Nouzový vstup.....	40
14.7	ZPRACOVÁNÍ SIGNÁLU.....	40
15	AUDIT.....	41
16	REKLAMAČNÍ POSTUP	41
17	ÚDAJE.....	41
17.1	VŠEOBECNĚ.....	41
17.2	ÚDAJE O ZÁKAZNÍKOVÍ	42
17.3	UCHOVÁVÁNÍ ÚDAJŮ	42
17.4	LIKVIDACE ÚDAJŮ	42
17.5	ZÁZNAMY.....	42
18	BUDOUCNOST DPPC	42
II	PRAKTICKÁ ČÁST	43
19	MANUÁL K OBSLUZE DOHLEDOVÝCH A POPLACHOVÝCH PŘIJÍMACÍCH CENTER.....	44
19.1	DEFINICE A ZKRATKY	44
19.2	CO MUSÍ DISPEČER (OBSLUHA) SPLŇOVAT.....	46
19.2.1	Obsazení DPPC	46
19.2.2	Patřičná kvalifikace	46
19.3	PROVOZNÍ POSTUPY.....	48
19.3.1	Testování	48
19.3.2	Výstup a vstup z DPPC	49
19.3.3	Správa databází	49
19.4	NOUZOVÝ PLÁN A NOUZOVÝ STAV	50
19.5	EVAKUAČNÍ POSTUPY.....	51
19.5.1	Nouzový vstup/výstup.....	51
19.6	ZPRACOVÁNÍ SIGNÁLŮ	52
19.6.1	Optické ověřování	52
19.6.2	Akustické ověření.....	52
19.6.3	Zákaznické nebo uživatelské ověřování.....	52
19.6.4	Sekvenční ověřování	53
19.7	ÚDAJE	53
19.7.1	Údaje o zákazníkovi.....	54

19.7.2 Uchovávání údajů.....	54
ZÁVĚR	55
ZÁVĚR V ANGLIČTINĚ.....	56
SEZNAM POUŽITÉ LITERATURY.....	57
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	59
SEZNAM OBRÁZKŮ	61
SEZNAM TABULEK.....	62

ÚVOD

Historie monitorovacích pultů začala v České republice kolem roku 1990. Pulty měly za úkol přenášet zprávy z ústředí PZTS (dříve EZS). Mezi průkopníky monitorovacích pultů (dnešních dohledových a poplachových přijímacích center DPPC) patří firmy TELEPATROL s.r.o, SV AGEBCY, BARA, AVES Group Brno a mnoho dalších firem po celé České republice. Tyto firmy také spolupracovaly s dalšími firmami, jako jsou např. Kelcom Hradec Králové, Euroalarm Praha, Olympo Controls z Brna, které patřily mezi první distributory systémů PZTS, přijímacích a monitorovacích zařízení. Signál byl přenášen jen po telefonní lince a vyhodnocovací zprávy byly tisknuty na kotoučové papíry.

V dnešní době jsou centra vybaveny nejmodernější technikou. Vyhodnocovací zprávy jsou převáděny rychlými telefonními linkami, rádiovým přenosem, GPRS nebo po internetu. Všechny tyto komunikační systémy jsou přiváděny přes dané moduly, které jsou umístěny na základní desce počítače. Počítač pomocí speciálních softwarů zpracovává zprávy a poté je vyhodnocuje na monitoru. Na všechnu tuto práci počítače dohlíží proškolený dispečer, který kontroluje a vyhodnocuje tísňové zprávy. V případě, že je objekt narušen, má za úkol, vyslat hlídku, zároveň kontaktovat příslušnou osobu a sdělit jí, že objekt byl napaden.

Hlavními funkcemi dohledového a poplachového přijímacího centra je minimalizovat následky škody z rizikových situací, rizika vloupání či prevence kriminality.

I. TEORETICKÁ ČÁST

1 SLOŽENÍ DOHLEDOVÉHO A POPLACHOVÉHO PŘIJÍMACÍHO CENTRA

Dohledová a poplachová přijímací centra (dále jen „DPPC“) se běžně rozdělují dvěma způsoby. Prvním způsobem se DPPC určí jako samostatný systém s vlastním síťovým napájením a zálohováním. U druhého způsobu se využívají integrované systémy do počítače (dále jen „PC“).

1.1 Samostatný systém neboli autonomní systém

Tento systém je stavěn tak, aby mohl pracovat samostatně bez dalších přístrojů. Běžně se skládá z tří řádkového displeje, ke kterému je připojena tiskárna a napájecí zdroj se záložním akumulátorem. Pro vylepšení systému se může použít PC s různými softwarovými kombinacemi. Tyto softwary umožňují obsluze centra sledovat další doplňkové funkce. Obsluha může sledovat stavy např. ústředny, detektorů, akumulátorů nebo napájení. Tyto technické informace (stavy) využívá především obsluha pro rychlé a přesné zmapování hlídaného objektu.

1.2 Integrované systémy do počítače

U těchto systémů se využívají především osobní počítače, ve kterých je nainstalovaný převážně operační systém Windows. Dále je systém vybaven LCD monitorem, klávesnicí a komunikačním zařízením (zvaným myš). Na základní desce počítače jsou běžně umístěny komunikační karty. Mohou být také umístěny externě v boxu vedle počítače a připojeny USB kabelem k počítači v případě, že nedostačují porty na základní desce PC. Aby byla vyřešena porucha systému (např. výpadek proudu), musí být automaticky zaručeno připojení na záložní zdroj energie v případě výpadku síťového napájení. V první řadě se aktivuje záložní akumulátor (UPS), který zaručí bezvýpadkový provoz systému, než naskočí náhradní zdroj. Musí se zapojit přenosný naftový nebo benzinový generátor. V případě použití naftového, nebo benzinového generátoru musíme zároveň dodržovat pravidla pro uchovávání hořlavých látek na pracovišti, kanystry musí být umístěny v samostatné místnosti. Přepětí je vyřešeno přepětíovou ochranou, která bývá většinou umístěna v rozvaděči a následně může být i u samotných počítačů v objektu. Případná porucha počítače je řešena prostřednictvím zálohového počítače, na který se souběžně nahrávají veškeré události. Zálohový počítač tedy v případě poruchy hlavního počítače převezme bez výpadku jeho činnost. Data jsou nepřetržitě zálohovaná zrcadlově

na externí harddisky a v určitých časových úsecích vypalována a archivována na pevná media DVD nebo Blue-Ray. Co se týká náhradních dílů na provoz DPPC, je třeba mít k dispozici záložní kompletní anténní systém, pokud je použit radiový přenos, aby v případě poškození anténního systému byl k dispozici systém záložní, který bude zapojen v co nejkratší době.



Obr. 1 Dohledové a poplachové přijímací centrum[1]

2 KOMUNIKACE DPPC

2.1 JTS - analog

JTS – jednotná telefonní síť. Po této lince je dnes přenášeno nejvíce zpráv na DPPC. Připojení JTS - Pokud je v objektu ústředna PZTS, musí se nejprve připojit přívod telefonní linky do ústředny a teprve poté se připojí koncové zařízení (telefonní aparáty uživatele). Tato podmínka musí být vždy dodržena, aby komunikace proběhla v pořádku. Ústředna PZTS má v sobě zabudovaný telefonní komunikátor, který přenáší zprávy v nastaveném formátu na DPPC. Proto je výhodou mít ústřednu PZTS s komunikátorem, protože odpadá dodatečné náklady na pořízení zařízení, jako jsou např. externí komunikátory, radiovysílače nebo GSM brány, které jsou nutné pro přenos jak poplachových, tak technických zpráv z objektu na DPPC. Nevýhodou přenosu po JTS je, že nejde kontrolovat trvale spojení přenosové trasy, a to vzhledem k nákladům za telefonické spojení. Proto se běžně používá spojení s DPPC centrem 1x za 24 hod.[2]

2.2 ISDN – digital (Digitální síť integrovaných služeb)

Pro přenos se používá datový hlasový přenos jako u linky JTS. Výhodou oproti klasické analogové JTS je vyšší rychlost přenosu dat. Na jednom spojení může bez omezení probíhat hlasový hovor a datový přenos. V tomto případě, pokud se kanály nespojí, je rychlost přenosu poloviční. Nevýhodou je, že musí mít DPPC ISDN kartu pro tento typ přenosu. ISDN přenos se v ČR neujal, protože byl na svou dobu příliš drahý a ústředny v sobě neměly integrovaný komunikační modul, který komunikoval ve formátu ISDN. Rozvoj ISDN linky byl v České republice rovnou nahrazen mobilní sítí GSM.[2]

2.3 Rádiový přenos na vyhrazených frekvencích

Jedná se o jednu z nejbezpečnějších a nejrychlejších přenosových cest. Před vytvořením rádiového přenosu na DPPC musí majitel centra zvážit, kde se vybudují retranslační stanice. Poté si musí u Českého telekomunikačního úřadu (dále jen „ČTÚ“) požádat o přidělení dané frekvence, na které bude DPPC komunikovat s objekty. Daná frekvence je zapsána v databázi ČTÚ a nikdo už tuto frekvenci nesmí používat.

System pro přenos musí obsahovat vysílač, který je zabudován ve střeženém objektu a přijímač který přijímá signál z vysílačů umístěných v objektech. Tento přijímač je součástí přijímacího centra DPPC. Pokud je to nutné z hlediska členitosti terénu a vzdálenosti, musí se použít retranslační stanice, které zaručí kvalitní přenos signálu. Rádiový přenos monitoruje nejen poplachové a technické stavy, ale také kontroluje v náhodných periodách kontrolu spojení.

Časové prodlevy:

- 1- Poplach na smyčce, (kontrola, zda-li nejde jen o rušení) 300 ms
- 2- integrovaný obvod převede zprávu do podoby telegramu 1 ms
- 3- Zapnutí a ustálení vysílače na frekvenci 3 ms
- 4- Přenos zprávy (podle druhu) 25 ms
- 5- Odkličování 1 ms
- 6- Přijmutí sběrnou stanicí a převedení z telegramu na číslo 1ms 1 ms
- 7- Odeslání do PC a uložení v databázi NET-G 10 ms
- 8- Okno důležitých zpráv čerpá z databáze nové informace každých 10 s
(záleží tak ve kterém okamžiku nová zpráva přišla) 10 000 ms

Takže maximální doba přenosu je okolo 10 330ms

Nejdůležitější body jsou 1 – 5 kde se informace vysílají a to je 330ms[3]

2.4 Přenos po síti GSM

2.4.1 Hovorové pásma

Stejně jako u předchozích typů přenosu, je i u hovorového pásma využíván hlasový přenos. Majitel objektu si musí obstarat GSM bránu pro přenášení informací. Tento typ přenosu se nejvíce používá v oblastech, kde není zavedena telefonní linka nebo kde nelze použít radiový přenos. Jedná se např. o chatové oblasti nebo mobilní domy. Dříve tyto přenosy byly finančně náročné, ale v současné době si může majitel dohodnout lepší podmínky. [4]

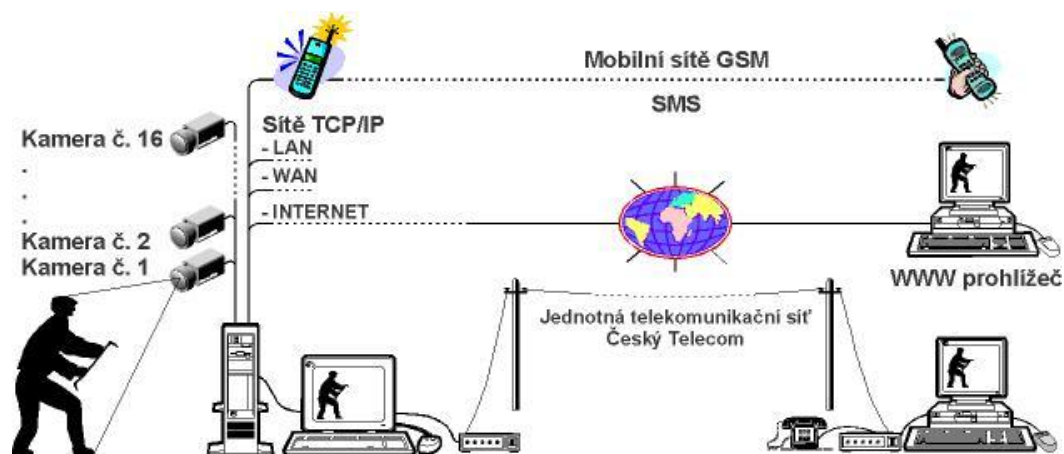
2.4.2 Prostřednictvím GPRS

Tento typ přenosu informací má v budoucnu velkou perspektivu, a to zejména z důvodu kvality pokrytí a provozních nákladů vynaložené za přenosy zpráv na DPPC. Výhodou je obousměrná komunikace mezi centrem a systémem instalovaným v objektu. Je možno provádět neustále test přenosové trasy, a to v intervalu od 1 minuty a výše. Toto řešení nahrazuje radiový přenos. Radiovou sítí je možné pokrýt jen určitou oblast, ale GPRS signál pokrývá 99% území ČR. [4]

2.4.3 Prostřednictvím SMS

Přenos prostřednictvím SMS se používá v případě, kdy je DPPC založeno na přijímání SMS zpráv. SMS zprávy se odesílají z objektu pomocí GSM brány nebo v horším případě upraveným mobilním telefonem. Když je použita GSM brána, lze nastavit hovor jako alarmovou zprávu.

S přijatými SMS zprávami lze provádět filtrace, uložit je na disk nebo je vytisknout. Zprávy posílané na DPPC mohou být paralelně zasílány i majiteli objektu. Nevýhodou jsou finanční náklady spojené se zakoupením a instalací SMS brány v objektu. V případě využívání přenosu poplachových zpráv si musíme uvědomit, že mobilní operátoři mají ze zákona 72 hodinovou lhůtu na doručení SMS zprávy. V případě přetížení sítě v dané lokalitě (např. v průběhu fotbalového utkání), nebo přetížení sítě ve významných dnech (např. vánoční svátky), se může doručení poplachové SMS zprávy výrazně zpozdít. [4]



Obr. 2 Komunikace s DPPC[5]

3 TECHNICKÉ ZABEZPEČENÍ CENTRA

DPPC musí být chráněno zabezpečovacím systémem, který vyžaduje instalaci v souladu s nejnovějšími a příslušnými normami pro zabezpečovací systémy. Tyto zabezpečovací systémy musí obsahovat poplachové zabezpečovací a tísňové systémy (PZTS).

3.1 Poplachové zabezpečovací a tísňové systémy

V případě aktivace PZTS, musí být dispečink upozorněn na narušení objektu. Poplachové zabezpečovací a tísňové systémy musí být instalovány na vnější stěny, dveře, střechy nebo stropy. Detektory musí být instalovány v souladu s novými normami pro PZTS. Tyto detektory jsou umístěny v objektu tak, aby snímaly vstupní prostory do budovy, schodiště, zádveří, předsíň a samotné přijímací poplachové centrum. Další zabezpečovací prostředky musí být instalovány na rozvaděč, kde je přivedena elektřina z veřejné elektrické sítě a také je tam umístěn rozvod pro komunikaci. Na tento rozvaděč je umístěn magnetický kontakt, který se aktivuje při otevření dvířek a spustí poplach. Tyto magnetické kontakty jsou také umístěny na všechny dveře, které vedou do dohledového a poplachového přijímacího centra (DPPC).

3.2 Kamerový monitorovací systém CCTV

Dále je v budově umístěn kamerový monitorovací systém (CCTV), který musí snímat hlavní vstup do budovy, prostor pře vchodem do DPPC a prostor před nouzovým východem. Kamerový systém je přiveden přímo do DPPC, kde ho má pod neustálým dohledem dispečer. Všechny prostory, které jsou monitorovány, musí být neustále dostatečně osvětleny. Pořízené záznamy jsou ukládány do záznamového zařízení DVR, který obsahuje HDD s vysokým úložištěm.

3.3 Požární ochrana

Centrum musí být chráněno elektrickou požární signalizací (EPS), která musí být instalována v souladu s aktuálními normami a předpisy. Dále musí být vybaveno detekcí škodlivých plynů, alespoň proti oxidu uhelnatého a kouře. Tyto detektory varují dispečery předtím, než koncentrace dosáhne stupně, kdy je zapotřebí nutná evakuace.

3.4 Síťové napájení

Síťové napájení by se mělo použít jako hlavní zdroj. Mohou být použity jiné spolehlivé alternativy, které mohou zabezpečit stálý přívod elektřiny. Jsou to například fotovoltaické panely, které přeměňují sluneční záření na elektřinu. Na pracovišti dispečerů by mělo být tablo pro znázornění, jakou má kapacitu aktuální zdroj napájení. Napájení ze sítě by mělo být dimenzováno na příslušné zařízení, které se v centru nachází a také musí mít dostatečný příkon pro aktuální přístroje. Dále musí být přivedeno napájení na záložní akumulátory, které musí dosáhnout požadované kapacity, aby vydržely 24 hodin v provozu.

3.5 Záložní napájení

V DPPC musí být umístěno zařízení, které při případném výpadku síťového napájení nebo při výpadku jiného alternativního napájení přejde automaticky bez jakékoli výkyvy na záložní zdroj. Zdroj musí mít dostatečnou kapacitu, aby nedošlo ke ztrátě funkčnosti všech důležitých zařízení jakými jsou např. zařízení pro přenos signálů, signalizaci, základního větrání, základního osvětlení, monitoringu, záznamu a včetně osvětlení kamerového dohledu. Záložním zdrojem musí být buď akumulátor, anebo záložní generátor či kombinace generátoru s akumulátorem. Akumulátor musí vydržet v provozu 24 hodin nebo 4 hodiny, pokud je rovnou instalován s generátorem, nebo 30 minut pokud jsou instalovány naráz dva generátory. Kapacita záložních zdrojů se musí vypočítat na základě průměrného odběru násoskového faktorem 1,5. Všechny záložní zdroje musí být umístěny v DPPC. [4]

3.6 Záložní akumulátory

Záložní akumulátor (UPS) musí být automaticky spuštěn, jakmile dojde k poklesu napětí primárního zdroje pod stanovenou úroveň, která je potřebná pro provoz DPPC. Pokud dojde k obnově primárního zdroje, musí se automaticky přepnout přívod elektřiny ze záložního zdroje zpět na primární zdroj.

3.7 Záložní generátory

Pokud se v centru používá generátor jako záložní zdroj energie, musí být umístěn v oddělené místnosti mimo ostatní pracovní prostory. Generátor musí být v dostatečném množství zásoben palivem, aby vydržel v činnosti nejméně 24 hodin. Kromě toho musí být vybaven nezávislým prostředkem pro automatické startování, v případě, že dojde k výpadku primárního zdroje. Jestliže dojde k výpadku energie, musí být informován dispečink o tom, že byl převeden primární zdroj na záložní generátor. Součástí generátoru je akumulátor, který je potřebný k nastartování generátoru a ten musí být nabíjen z primárního zdroje.

3.8 Ochrana před bleskem a přepětí

Ochrana před bleskem se dělí na vnější a vnitřní ochranu. Při vnější ochraně proti blesku se na budovách používají zařízení, která svedou blesk do země, tzv. bleskosvody. Tím pádem jsou všechna zařízení, včetně budovy samotné, chráněna proti zásahu bleskem. Vnitřní ochrana je tvořena s vyrovnáním kapacity mezi kovovou instalací a vedením uvnitř zařízení. Veškerá vedení, která jsou pod napětím (např. síťová přípojka, telefonní linka nebo GSM anténa) jsou nepřímo napojena na zemnicí zařízení, které poskytuje přístroji ochranu proti přepětí.

Ochrana proti přepětí slouží k eliminování škod na elektrických a elektronických zařízení z důvodu zvýšení napětí z primární sítě. K ochraně proti přepětí se používají přístroje SPD (Surge Protection Device), které v případě zatížení vyrovnávají kapacitu mezi připojenými vodiči. Tím pádem je zamezeno projití špičky napětí do zařízení. [6]

4 PERSONÁLNÍ ZABEZPEČENÍ CENTRA

V DPPC by měly být podle směrnic a norem minimálně dva dispečeri, kteří mají za úkol dohlížet na chod centra. Dále je jejich úkolem dohlížet na příchozí poplarchy, CCTV kamery, PZTS. Mohou také dělat administrátorskou činnost, a to např. dopisovat smlouvy, revize, atd. Dispečeri mají stanovenou pracovní dobu vždy na celý měsíc. Směna je stanovena na 8 hod., o víkendu se střídají po 12 hodinách. Střídající skupina musí být před výměnou na pracovišti o 15 minut dříve, aby bylo možné si vyměnit informace o tom, co se stalo během provozu. Další člen personálu je technik, který také dohlíží na chod centra, ale z pohledu technického. V případě poruchy jakékoliv části centra, musí být stále k dispozici nový kus, který se rovnou vymění. Všechny části centra by měly být umístěny ve skladu. Technik má dále za úkol dávat do systému nové objekty a vysílat výjezdovou hlídku. Výjezdová hlídka může patřit mezi personál DPPC, ale také nemusí. Vše záleží na majiteli centra, jestli výjezdovou hlídku bude poskytovat nebo ne. Výjezdová hlídka čeká na pokyn technického dispečera. Když dispečer zaznamená poplach v objektu nebo narušení objektu, má za úkol po zjištění dalších informací vyslat hlídku k prozkoumání objektu.

4.1 Bezpečnostní prověření personálního obsazení

Veškerý personál DPPC musí být prověřen alespoň za období pěti let před zahájením pracovního poměru v DPPC nebo od data ukončení řádného studia. Musí být prověřeny a zkontrolovány veškeré osobní údaje, tzn. je provedena tzv. lustrace (kontrola trestního rejstříku, občanského průkazu atd.) Aby prověření proběhlo bezpečně, musí být kontrola pod dohledem a vše musí být řádně zdokumentováno. U všech pořízených informací musí být proveden záznam.

4.2 Výcvik

Než bude moci dispečer vykonávat příslušnou práci, měl by projít kompletním výcvikem, který je potřebný k provádění konkrétních úkolů, které bude při práci vykonávat. Výcvik obsahuje proškolení v oblasti používaných operačních systémů a příslušných softwarů. Dále se musí naučit dokonale ovládat metodiku řízení zásahu.

Výpis norem ČSN EN 50518-1 až 3:2010, které byly schváleny evropským výborem pro normalizaci v elektrotechnice CENELEC.

5 UMÍSTĚNÍ A KONSTRUKČNÍ POŽADAVKY

5.1 Volba místa

Dohledové a poplachové přijímací centrum (dále DPPC) musí být situováno v místě s nízkým rizikem požáru, výbuchu, zaplavení, vandalismu a nebezpečí hrozícímu z jiných míst. V případě, že DPPC není jediným uživatelem objektu, v němž je umístěno, musí být od zbytku budovy odděleno fyzickou bariérou, sestávající ze stěn, podlah, stropů a nezbytných otvorů.

5.1.1 Posouzení rizik

Posouzení rizik představuje řadu logických kroků, umožňujících prověřit veškerá rizika spojená s DPPC. Posouzení rizik obsahuje analýzu rizik a vyhodnocení rizik, a musí být kontinuálním procesem. Záznam a posouzení rizik musí být archivován a být k dispozici pro audit třetí straně.

5.1.2 Přístupnost místa

Přístup do budovy nebo části budovy, v níž je DPPC umístěno, musí být výhradně v užívání organizace provozující DPPC.

5.1.3 Umístění

Posouzení rizik musí být provedeno jako první krok při volbě umístění DPPC. DPPC musí být umístěno uvnitř objektu, který odpovídá následující kapitole Stavební řešení.

5.2 Stavební řešení

5.2.1 Konstrukce DPPC

Obvodový plášť sestává z vnějších stěn, podlah, stropů, vstupních a výstupních dveří, ventilačních kanálů, vstupních otvorů pro kabeláž a potrubí, zasklených ploch a manipulačních okének.

5.2.1.1 Konstrukční požadavky ohledně fyzického útoku

Obvodový plášť DPPC musí poskytovat odolnost proti fyzickému útoku v souladu s tabulkou 1.

<i>Stavební prvky</i>	<i>Materiál</i>	<i>Tloušťka</i>
<i>Vnější stěny včetně stěn mezi dispečinkem a vstupní halou.</i>	<i>Plné zdivo</i>	<i>>200 mm</i>
	<i>Litý beton</i>	<i>>150 mm</i>
	<i>Železobeton</i>	<i>>100 mm</i>
	<i>Plná ocel</i>	<i>>8 mm</i>
<i>Vnitřní stěny</i>	<i>Žádné požadavky</i>	<i>Žádné požadavky</i>
<i>Podlahy a stropy</i>	<i>Litý beton</i>	<i>>150 mm</i>
	<i>Železobeton</i>	<i>>100 mm</i>

Tab. 1 Minimální odolnost DPPC proti fyzickému útoku[7]

Stavební prvky uvedené v tabulce 1 představují minimum pro odolání fyzickému útoku. Jsou-li použity jiné stavební materiály, musí zaručit stejnou úroveň odolnosti proti fyzickému útoku.

Odolnost dveří a zasklených ploch DPPC a satelitních DPPC proti ručně vedenému útoku musí odpovídat EN 1627, bezpečnostní třídě 4.

5.2.1.2 Odolnost proti útoku střelnou zbraní

Odolnost dveří a zasklených ploch v DPPC a satelitních DPPC proti střelám musí odpovídat EN 1522.

5.2.1.3 Ochrana proti požáru

Vnější plášť DPPC musí mít požární odolnost podle EN 13501-2, ale ne méně než 30 minut.

5.2.1.4 Ochrana proti blesku

Pro každé DPPC musí být provedena analýza rizik v souladu s EN 62305-2, a musí být učiněna vhodná opatření k ochraně DPPC proti úderu blesku v souladu s EN 62305.

5.2.2 Příslušenství

Uvnitř prostoru DPPC musí být toalety a umývárny. Jsou-li uvnitř DPPC k dispozici prostory pro přípravu jídla a pití, musí tyto prostory být odděleny od operační místnosti konstrukcí s požární s požární odolností.

5.2.3 Otvory

V konstrukci DPPC jsou povoleny pouze následující otvory:

- *Vstup z haly*
- *Nouzový východ*
- *Zasklené plochy*
- *Vstupní otvory pro kabeláže a potrubí*
- *Manipulační okénko*
- *Ventilace*

5.2.4 Vstupní předsíň

Vstupní předsíň musí mít dvoje dveře, jejichž rozměry nesmí přesáhnout 2,5 m výška a 1,1 m šířky, oddělené vstupní předsíní, jejíž podlahová plocha nesmí být větší než 6 m². Dveře musí být navzájem provázány tak, aby je bylo možné otevřít současně, s výjimkou řízených okolností. Dveře z přijímacího centra se musí otevírat do vstupní předsíně. Dveře z předsíně do vnějšího prostoru se musí rovněž otevírat ven. Jedny z dveří musí mít požární odolnost v souladu s požadavky bodu 1.2.1.3. Druhé dveře musí mít bezpečnostní třídu 4 podle normy EN 1627.

Zámky a závory odpovídající EN 12209, zámkové vložky odpovídající EN 1303, madla a dveřní kování odpovídající EN 1906 musí být v souladu s požadavky uvedenými v tabulce 2, aby splňovaly třídu bezpečnosti 4.

Bezpečnostní třída	4
EN 1303	
Vložka (číslice 7)	6
Vložka (číslice 8)	2
EN 1906	
Kování (číslice 7)	4
EN 12209	
Zámky (číslice 7)	7

Tab. 2 Bezpečnostní třída[7]

Oboje dveře musí být opatřeny zamykatelným systémem ovládaným pouze z prostoru DPPP a musí být opatřeny samouzavíracím a samozamykatelným systémem. Dveře musí být elektricky vzájemně vázány tak, aby nemohly být otevřeny oboje současně. V DPPP musí být zajištěna možnost překonání této vzájemné vazby pro případ nouzového úniku.

5.2.5 Zamykací mechanismus

5.2.5.1 Elektromechanický zámek

K zajištění dveří vstupní haly musí být použity elektromechanické zámky splňující požadavky EN 14846 klasifikace 2-R-2-B-0-C-7-H-B-3-E-4-3. Upevňovací šrouby musí být chráněny proti manipulaci, když jsou dveře v zavřené poloze. Musí být zajištěna možnost mechanického překonání v nouzových případech, s ochranou proti náhodnému použití. Jestliže je zamykací mechanismus umístěn ve dveřním křídle, musí být připojovací kabel veden v pancéřové průchodce, nebo musí být jeho přístupná část chráněna jiným způsobem.

5.2.5.2 Mechanické zámky

Pro zajištění ostatních dveří musí být použity mechanické zámky splňující požadavky EN 12209 klasifikace 2-R-2-1-0-C-7-H-B-3-E. Jsou-li použity alternativní zamykací prostředky, musí splňovat výše uvedené kritéria.

5.2.6 Nouzový východ

Dveře dalších nouzových východů, včetně jejich zárubní, závěsů, upevňovacích prvků, vícenásobných zamykacích bodů a zámků musí splňovat kritéria týkající se fyzické pevnosti a odolnosti. Dveře nouzových východů se musí otevírat směrem ven a musí být opatřeny zámky splňujícími požadavky EN 179, aby bylo možné je uvolnit pouze v případě nouze. Odemykání zařízení musí být možné pouze zevnitř prostoru DPPC.

5.2.7 Zasklené plochy

Zasklené plochy musí být odolné proti fyzickému útoku a proti průstřelu podle specifikace v tabulce 3.

	Fyzický útok	Průstřel
Zasklené plochy	EN 356 třída P6B	EN 1063 třída BR 4 - S

Tab. 3 Fyzický útok a průstřel[7]

Zasklení by mělo mít požární odolnost. Vnitřní prostor DPPC nesmí být viditelný z žádného místa vně budovy.

5.2.8 Ventilace

Ventilační systémy v DPPC musí splňovat požadavky EN 13779. Kvalita vzduchu uvnitř DPPC je stanovená v závislosti na velikosti podlahové plochy na osobu musí odpovídat požadavku pro „malou kancelář“. Použití filtrů musí být v souladu s tabulkou A.5 normy EN 13779:2007, kvalita venkovního vzduchu, kvalita vnitřního vzduchu, vedoucí použití filtrů třídy F5. Hladina hluku v DPPC nesmí překročit hodnotu (30–40) dB. S ohledem na interní zatížení musí být produkce tepla osob (jednotlivců) v souladu s kategorií aktivity „sedící odpočinek“.

Otvory ventilačních systémů v objektu DPPC musí splňovat požadavky 1.2.1.1 pro odolnost proti fyzickému útoku. V případě, že průřez vstupních a výstupních otvorů

ventilační ch systémů překročí $0,02 \text{ m}^2$, musí být použit vhodný poplachový systém, detekující jakýkoli pokus vniknutí do ventilačního otvoru. Ventilační otvory v plášti vlastního DPPC musí být chráněny fyzicky. Ventilační otvory musí být chráněny vzduchotěsnými klapkami, které lze z prostoru DPPC uzamknout v uzavřeném stavu.

5.2.9 Technologické otvory

Otvory v obvodovém plášti DPPC slouží pro veškeré kabely nebo potrubí nesmí mít průřez větší než $0,02 \text{ m}^2$. Mezery mezi kabely nebo trubkami nesmí být větší než 1,5 mm. Tam, kde by mezera byla větší než 1,5 mm, musí být vyplněna materiálem ekvivalentním materiálu pláště.

5.2.10 Manipulační okénko / propust'

Manipulační okénko nebo propust' může být umístěno v obvodovém plášti DPPC. Manipulační okénko / propust' se musí otevírat do zabezpečeného prostoru. Manipulační okénko / propust' musí být konstruováno podle obdobného standardu jako plášť DPPC. Vstupní otvory musí být vzájemně propojeny, aby bylo vždy zabráněno přímému přístupu do prostoru DPPC, a otevírání a zavírání musí být ovládáno z prostoru DPPC. Vnější otvory se musí otevírat směrem ven od DPPC.

Musí být zajištěna hlasová komunikace mezi dispečinkem DPPC a vnějším přístupem před manipulačním okénkem / propustí.

5.3 Poplachové systémy

Elektrická detekce pro všechny základní části DPPC musí postihovat následující události:

- Útok zvenčí (narušitel)
- Požár
- Vchod a východ
- Plyn
- Komunikace
- Tíseň (přepadení)
- Monitorování bezpečnosti personálu
- Signalizace elektronických ochranných systémů
- CCTV

Veškeré systémy uvedené v této kapitole musí být udržovány podle požadavků příslušných norem. V případech kdy normy neexistují, se musí údržba podle směrnic výrobce tak, aby byla zajištěna trvalá spolehlivost.

5.3.1 Útok zvenčí

Budova DPPC musí být vybavena poplachovým zabezpečovacím systémem stupně zabezpečení 3 podle požadavků EN 50131-1. V případě, že se DPPC nenachází v přízemí nebo je-li možné získat přístup zespoda (například ze suterénu), musí být poplachovým systémem zabezpečena i podlaha.

Části budovy, které jsou využívány provozovatelem DPPC a v níž je DPPC umístěno, musí být chráněny poplachovým zabezpečovacím systémem instalovaným podle požadavků normy EN 50131-1. Tento poplachový systém musí obsahovat výstražné zařízení podle EN 50131-4, které okamžitě upozorní personál DPPC na nastalý poplach.

Doporučení pro návrh, projekt, montáž a údržbu jsou obsaženy ve směrnici pro aplikaci CLC/TS 50131-7.

Pro stanovení stupně zabezpečení poplachového systému musí být provedeno posouzení rizik.

5.3.2 Požár

Části budovy, které jsou využívány provozovatelem DPPC a, v níž je DPPC umístěno, musí být chráněno poplachovým požárním systémem (elektrickou požární signalizací), který musí být sestaven z komponentů certifikovaných podle EN souboru 54 a musí být instalován v souladu s EN 54-14.

5.3.3 Vchod/východ

Akustická nebo optická signalizace musí být v činnosti, aby upozornila dispečery na kterékoli nezajištěné dveře do prostoru DPPC a vstupní předsíň. Musí být signalizován poplachový stav, je-li otevřen nouzový východ, nebo jsou-li současně otevřeny oboje dveře.

5.3.4 Plyn

DPPC musí být vybaveno detekčním systémem detekujícím minimálně oxid uhelnatý varující personál DPPC dříve, než nastane nutnost evakuace.

5.3.5 Komunikace

Veškerá kabelová nebo bezdrátová komunikační zařízení slouží k přenosu poplachových informací do/z DPPC a vzdálených poplachových systémů připojených do DPPC musí být chráněna uvnitř objektu, v němž se DPPC nachází, tak, aby bylo jakékoli rušení detekováno v souladu s EN 50136-1.

5.3.6 Tíseň (přepadení)

Tísňové hlásiče instalované v souladu s EN 50131-1 musí být umístěny uvnitř DPPC v blízkosti dveří do vstupní předsíně, nouzového východu (východu), manipulačních okének / propustí, a na všechny obvyklých pracovištích personálu.

5.3.7 Monitorování bezpečí personálu

Bezpečí a zabezpečení personálu DPPC musí být automaticky monitorováno v intervalu nepřesahujícím 60 minut. Jestliže obsluha nereaguje na kontrolní bezpečnostní signál do 60 s, musí být automaticky vyslán poplach do jiného DPPC

5.3.8 Signály bezpečnostních systémů

Signál bezpečnostních systémů musí být přenášeny do jiného DPPC prostřednictvím systému zdvojené přenosové trasy splňující požadavky EN 50136-1 a musí odpovídat kvalitativním parametrům uvedených v tabulce 4.

Jiné DPPC přijímací signály s bezpečnostních systémů nesmí být umístěno v téže budově nebo v bezprostředním sousedství.

<i>ATP</i>	<i>Doba přenosu</i>	<i>Maximální hodnota přenosového času</i>	<i>Doba do oznámení opatření</i>	<i>Náhradní bezpečnostní opatření</i>	<i>Bezpečnost přenášené informace</i>	<i>Dostupnost</i>
<i>Primární ATP</i>	<i>D3</i>	<i>M3</i>	<i>T5</i>	<i>S2</i>	<i>I3</i>	<i>A4</i>
<i>Sekundární ATP</i>	<i>D2</i>	<i>M2</i>	<i>T4</i>	<i>S2</i>	<i>I3</i>	<i>A3</i>

Tab. 4 Kvalitativní parametry systému zdvojené přenosové trasy[7]

5.3.9 Dohled kamerovým systémem

Musí být instalován kamerový systém umožňující zevnitř DPPC sledování všech přístupových cest k budově, v níž je umístěno DPPC v souladu směrnici pro aplikaci EN 50132-7. Musí být instalován kamerový systém umožňující personálu DPPC identifikovat oprávněné osoby před vstupem do vstupní předsíně, sledovat veškerou aktivitu v ní a její bezpečné opuštění. Rovněž musí být instalován kamerový systém umožňující personálu DPPC identifikovat kohokoli, kdo užívá manipulační okénko.

5.4 Napájení elektrickým proudem

5.4.1 Síťové napájení

Napájení ze sítě musí být použito jako hlavní zdroj, avšak mohou být použity spolehlivé alternativy. Na pracovišti operátorů musí být identifikováno, jaký je aktuální zdroj napájení. Síťové napájení musí být dimenzováno tak, aby byl zajištěn dostatečný příkon pro napájení veškerého zařízení a pro současné nabíjení záložních akumulátorů k dosažení požadované kapacity během 24 hodin. Napájecí kabely vedené vně obvodového pláště DPPC musí být chráněny proti mechanickému poškození a proti požáru.

5.4.2 Záložní zdroj napájení

Záložní zdroj napájení musí mít kapacitu dostatečnou pro nepřerušovanou funkčnost veškerých přenosů, signalizace, monitoringu, záznamu, základního větrání a základního osvětlení včetně osvětlení pro kamerový dohled po dobu 24 hodin při zatížení 1,5 násobkem průměrného odběru. Přepínání na/ze záložního zdroje napájení nesmí ovlivnit normální provoz zařízení. Záložním zdrojem napájení musí být buď záložní akumulátor nebo záložní generátor nebo generátory podporované záložním akumulátorem dle EN 62040-1.

Záložní akumulátor a veškeré zařízení pro automatické přepínání z hlavního na záložní zdroj napájení musí být umístěn v DPPC. Záložní akumulátor, který není umístěn v DPPC, musí být v kontrolovaném bezpečnostním prostoru chráněném proti napadení a požáru systémem stejného stupně jako je chráněno DPPC.

5.4.3 Záložní akumulátor (UPS)

Záložní akumulátor musí být automaticky uveden do činnosti, jakmile napětí primárního zdroje napájení poklesne pod úroveň nutnou pro provoz DPPC. DPPC musí přejít zpět na primární zdroj napájení, jakmile dojde k obnově dodávky proudu z primárního zdroje. Umístění akumulátoru musí odpovídat požadavkům EN 50272-2.

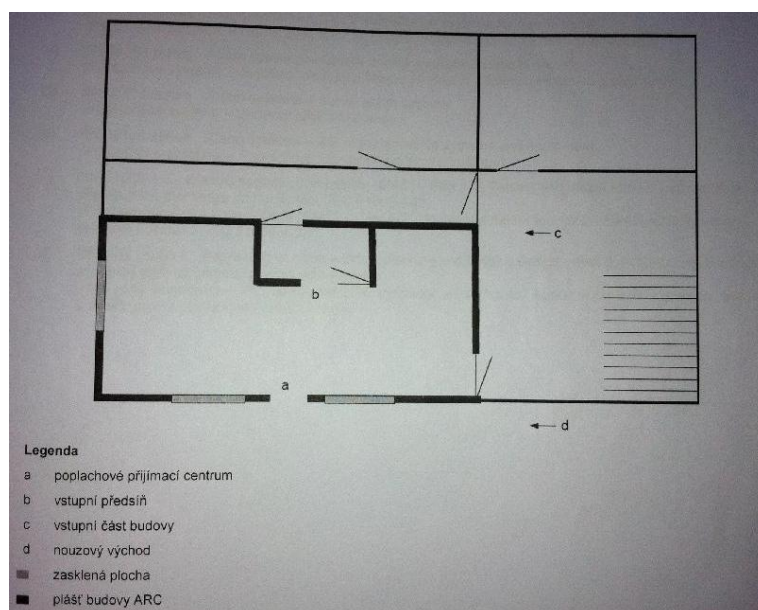
Je-li pro nouzové napájení použit záložní generátor, musí být kapacita záložního akumulátoru dostatečná pro napájení DPPC po dobu nejméně 10 minut.

5.4.4 Pohotovostní generátor

Generátor umístěný uvnitř prostoru DPPC musí být od zbytku pracovního prostoru oddělen stavební konstrukcí poskytující příslušnou požární odolnost. Veškeré záložní generátory musí být zásobeny palivem pro činnost generátoru po dobu nejméně 24 hodin.

Veškeré záložní generátory musí mít nezávislé prostředky pro automatické startování, jakmile dojde k výpadku normálního zdroje napájení. Činnost záložních generátorů musí být ohlášena v DPPC. Akumulátor nezbytný pro startování záložního generátoru musí být nabíjen z primárního zdroje napájení. Záložní generátor instalovaný vně prostoru DPPC musí být umístěn v kontrolovaném bezpečnostním prostoru a musí být chráněn proti napadení a požáru systémem stejného stupně jako je chráněno DPPC.

[7]



Obr. 3 Typické rozložení DPPC[7]

6 TECHNICKÉ POŽADAVKY

6.1 Požadavky na výkonost

Obrázek ukazuje sled operací v rámci odpovědnosti DPPC, který platí pro jakýkoli signál generovaný poplachovým a zabezpečovacím, tísňovým systémem (PZTS) po zpracování komunikátorem přijímacího centra. Musí být vykládáno společně s EN 50136-1:201X. Poplachové přijímací zařízení a zdroje musí zajišťovat následující výkonost. Čas mezi T_{RX} a T_{reakce} musí splňovat následující výkonostní kritéria:

- V případě tísňových poplachů: 30 s u 80% přijatých signálů a 60 s u 95,5% přijatých signálů
- V případě všech ostatních signálů: 90 s u 80% přijatých signálů a 180 s u 98,5% přijatých signálů

Souladu z výše uvedenými kritérii musí být dosaženo v průběhu dvanácti po sobě jdoucích měsíců.

6.2 Požadavky na komunikaci

Musí být splněny následující požadavky:

- V DPPC musí být taková zařízení, aby vnější komunikace byla automaticky zaznamenávána s časem a datem, a aby ji bylo možno obnovit, zobrazit/znovu přehrát a uchovat po dobu nejméně tři měsíců
- Zařízení bude používáno jako prostředek komunikace po celé vstupní předsíni

6.3 Příjem signálu

6.3.1 Všeobecné požadavky

Každý přijatý signál musí být v DPPC samostatně identifikovatelný a musí být zaznamenán automaticky a poskytovat následující informace:

- Identifikace střežených prostorů
- Typ signálu
- Datum a čas přijetí signálu

6.3.2 Zásah dispečera

V případě, že je potřeba zásahu dispečera, podrobnosti zásahu musí být zaznamenány, včetně data a času jeho dokončení a totožnosti dispečera/dispečerů, který/kteří zásah provedl/i. Pokud zásah automatický, musí být zaznamenáván.

7 TESTOVÁNÍ

7.1 Všeobecně

Pro pravidelné testování všech zařízení potřebných pro provoz DPPC musí existovat dokumentované postupy. Zařízení, které mají vnitřní hodiny, musí být synchronizována se světovým časem nejméně každých 24 hodin.

7.2 Každodenní testy

U následujících zařízení musí být denně kontrolována jejich správná funkčnost a výsledky musí být zaznamenávány:

- Komunikátor přijímacího centra*
- Indikační zařízení*
- Komunikační systémy*
- Všechny příchozí a odchozí komunikační linky*

7.3 Týdenní testy

Následující zařízení musí být kontrolována každý týden jejich správná funkčnost a výsledky musí být zaznamenávány:

- Poplachová systémy DPPC*
- Elektrické napájecí zdroje*
- Zařízení pro nouzové osvětlení*

7.4 Postupy při závadách a podávání zpráv

Jakákoli součást zařízení zapojená do příjmu, zobrazení nebo dalšího přenosu poplachového signálu, včetně napájení, musí mít záložní zařízení a postup, kterým může být uvedeno do provozu buď automaticky, nebo dispečerem DPPC do 1 h od okamžiku, kdy se dispečer o existenci závady dozví.

Musí také existovat zdokumentovaný postup pro opravu poškozeného zařízení uvedeného v bodech 3.2 a 3.3. Tento postup musí obsahovat časový rámec pro zahájení podání zprávy o poruše, který nesmí přesáhnout 15 min od jejího zjištění.

8 ÚDAJE

8.1 Všeobecně

Je nutné věnovat pozornost evropské směrnici o ochraně osobních údajů. U následujících kategorií je to nezbytné:

- Údaje o zákazníkovi*
- Údaje o vnější komunikaci DPPC*
- Záznamy o zákrocích dispečera*

8.2 Údaje o zákazníkovi

Údaje o každém poplachovém systému připojeném k DPPC musí být k dispozici dispečerům a musí obsahovat:

- Jméno, adresu a kontaktní telefonní číslo zabezpečených prostor*
- Referenční číslo prostorů a všech zvláštních opatření*
- Jméno, adresu a telefonní číslo uživatelů*
- Opatření, která musí být učiněna v případě poplachu*
- Dohodnutou dobu uvádění do stavu střežení a stavu klidu v případě potřeby*

8.3 Údaje o vnější komunikaci DPPC

Všechny údaje o vnější komunikaci musí být zaznamenávány v dohádatelném formátu.

8.4 Záznam zásahu dispečera

Záznamy musí vést evidenci zákroků dispečera. Tyto záznamy musí obsahovat podrobnosti o veškerém obvyklém testování, údržbě a pohotovostní obsluze zařízení DPPC.

9 UCHOVÁVÁNÍ ÚDAJŮ

Veškeré údaje o klientovi musí být uchovávány po dobu nejméně dvou let. Veškeré údaje o vnější komunikaci DPPC musí být uchovávány po dobu nejméně tří měsíců. Záznamy zákroků dispečera DPPC musí být uchovávány po dobu nejméně dvou let.

10 VYUŽITÍ A OVĚŘEVÁNÍ VÝKONNOSTI DPPC

Při určování, zda je celková výkonnost poplachového systému v souladu s EN 50131-1 a EN 50136-1, musí být stanoveno měsíční využití DPPC jako procento času, kdy DPPC, včetně všech jeho funkčních částí, funguje v souladu s touto normou. DPPC musí dodržovat procento využití tak, jak je uvedeno v EN 50136-1 pro poplachové přenosné systémy, pokud jde o zpracování signálů. Využití DPPY v procentech, jak je formulováno výše, musí být podrobena ověření plnění postupů.

11 NOUZOVÁ PLÁN

11.1 Všeobecně

V případě vyřazení DPPC z činnosti musí být připravený vypracovaný nouzový plán pro vypořádání se s následky. Nouzový plán se musí ošetřovat přiměřeně na základě předvídatelné mimořádné události s potenciálem zhoršení kvality služeb DPPC. Opatření, která budou provedena, musí být jasně vymezena a musí se vztahovat na technické nebo jiné havárie. Nouzový plán musí obsahovat:

- Kontaktní údaje dodavatelů a poskytovatelů služeb schopných provést obnovení při zachování dané služby*
- Prostředky, kterými budou pokračovat nebo budou obnoveny dodávky služeb*
- Přezkoumání nouzového plánu ne dále než do šesti měsíců vedením, které musí zdokumentovat a navrhnout všechna nápravná opatření*

11.2 Příklady abnormálních událostí

Příklady abnormálních událostí, které musí být brány v úvahu při sepisování nouzového plánu, jsou:

- Úplné selhání schopnosti provádění úkonů*
- Poruchy, nebo poškození technické infrastruktury stanoviště, komunikačního zařízení nebo komunikačních okruhů*

- *Požár, včetně vystavení ohni v sousedních a přilehlých objektech*
- *Povodně nebo jiné průnik vody*
- *Poškození při bouřce, včetně přepětí v důsledku blesku při dodávce elektřiny a telefonního vedení*
- *Náraz vozidla, včetně kolejových vozidel a letadel*
- *Úmyslné poškození*
- *Zločinný útok, vyhrožování bombou, nebo jiné situace protiprávního nátlaku*

[8]

12 PRACOVNÍ POSTUPY A POŽADAVKY NA PROVOZ

13 PERSONÁLNÍ OBSAZENÍ

13.1 Všeobecně

DPPC musí být trvale obsazeno nejméně dvěma dispečery. Pokud je DPPC provozováno současně s druhým DPPC a provozní provozy zajišťují stejný efekt jako u DPPC obsazeného dvěma dispečery, je tento požadavek splněn.

13.2 Bezpečnostní prověření a lustrace

Veškerý personál DPPC musí být prověřen za období minimálně pěti let před zahájením řádného pracovního poměru v DPPC nebo od data ukončení řádného denního studia. Veškerý personál musí absolvovat bezpečnostní lustraci. Pro dohled a dokumentaci přijatých opatření musí být veden záznam o informacích získaných během prověřovacího a lustračního procesu. Pokud je jednotlivec zaměstnán před dokončením prověřování nebo bezpečnostní lustrace, potom musí být upozorněn, že jeho zaměstnání je podmíněno vyhovujícím výsledkem prověřování a lustrace.

13.3 Výcvik

Společnost musí pro všechny příslušné zaměstnance dodržovat výcvikové postupy, pokrývající teoretické a praktické znalosti splňující výcvikové požadavky stanovené pro DPPC. Všichni dispečeri musí být před tím, než dostanou povolení zpracovávat poplachy bez dozoru, absolvovat výcvik zajišťující minimální způsobilost k provádění konkrétních úkolů. V případě nového technického vybavení nebo změny provozních postupů musí být

dispečeri znovu proškoleni na danou oblast činnosti. Výcvik musí být dokumentován a vyhodnocován v pravidelných intervalech.

14 PROVOZNÍ POSTUPY

14.1 Všeobecně

Předpisy pro provozní postupy musí být dostupné všem dispečerům a obsahovat postupy pro:

- *Testování*
- *Vstup do DPPC a odchod z DPPC*
- *Správu databází*
- *Provozní kontinuita a nouzové stavy*
- *Evakuační postupy*
- *Zpracování signálu*

14.2 Testování

Technické vybavení DPPC musí být pro normální provoz prověřováno v souladu s EN 50518-2:2010 kapitola 3 a výsledky musí být zaznamenávány.

14.3 Vstup a odchod z DPPC

Předpis pro vstup do DPPC a odchod z DPPC musí být součástí dokumentovaných postupů dostupných všem dispečerům. Tento předpis musí definovat metody používané pro identifikaci osob požadujících vstup do DPPC, a musí vyžadovat pozitivní identifikaci těchto osob dříve, než je jim vstup povolen. Přístup do DPPC musí být v každém případě po celou dobu řízen dispečerem zevnitř DPPC. Musí být prováděn záznam o všech osobách, které navštívili DPPC.

14.4 Správa databází

Systémy správy databází musí být udržovány v prostorách DPPC, jenž ukládá, organizuje, řídí, spravuje a umožňuje přesuny všech klientských údajů a musí být propojeny s vybavením pro příjem poplachových signálů pro automatické ohlášení vše signálů z každého poplachového systému. DPPC musí zavést a dodržovat ochranná opatření zajišťující nedotknutelnost zákaznických údajů před nepřátelskými činy nebo

vlivy. Musí být stanoveny a zaznamenány jasné a jednoznačné postupy pro všechny zaměstnance, jak zacházet bezpečně se všemi důvěrnými informacemi člověka ke kterým mají přístup. Každý zákazník, jehož poplachový systém je připojen na DPPC, musí mít přidělen individuální, jednoznačně označený záznam, v němž jsou o něm uvedeny podrobnosti spolu s jinými odpovídajícími instrukcemi. Je v něm rovněž veden individuální záznam historie, který může být součástí záznamu, v němž jsou zaznamenávány veškeré relativní signály a zásahy dispečerů.

14.5 Provozní kontinuita a nouzové stavy

- 1) *Postupy pro nouzový zásah musí být uspořádány s dodavateli a pohotovostními službami tak, aby umožňovali DPPC udržovat monitorovací službu, zatímco je incident prošetřován, škody zjištěny nebo opravovány.*
- 2) *Pro případy, kdy je DPPC vyřazeno z provozu, musí být vypracován nouzový plán pro řešení takové situace.*
- 3) *Postupy, nezbytné pro zjištění provozu DPPC, řešící selhání nebo rizika, musí být zpracovány pro následující situace:*
 - *Útok zvenčí (narušitel)*
 - *Požár*
 - *Povodeň (vodovodní havárie)*
 - *Vchod/východ*
 - *Plyn*
 - *Komunikace*
 - *Přepadení*
 - *Monitorování bezpečnosti personálu*
 - *Signály elektronických ochranných systémů*
 - *CCTV*

14.6 Evakuační postupy

14.6.1 Všeobecně

Musí být zpracován detailní plán pokrývající částečnou evakuaci a úplnou evakuaci. Plán musí rovněž obsahovat postupy pro návrat nebo obnovu následující po evakuaci. Veškerý personál musí mít instrukce a výcvik v nouzových postupech v intervalech nepřekračujících šest měsíců, tento výcvik musí být zaznamenáván.

14.6.2 Nouzový vstup

Prostředky nouzového vstupu do DPPC hlavním vchodem musí být zahrnuty v konstrukci a v pracovních postupech DPPC. Způsob nouzového vstupu musí být zpracován v dokumentu a veškeré klíče/kódy nebo přístupové karty používané ke vstupu do DPPC musí být bezpečně uloženy a přístupné jen oprávněným osobám.

14.7 Zpracování signálu

Pro zacházení se signály přijatými DPPC musí být zpracovány zdokumentované postupy, zahrnující příjem, zpracování a úkony dispečera od přijetí signálu (T_{reakce}) do ukončení akcí (T_{konec}).

V případě verifikace (ověřování) poplachového signálu, musí být tyto postupy zdokumentovány. Verifikace poplachového signálu může být například:

- Akustická*
- Vizuální*
- Zákaznická/uživatelská*
- Sekvenční*

Akusticky ověřený je zaznamenaný poplachový signál ověřený akustickou informací z hlídaného prostoru, takže je požadovaný za ostrý poplach.

Vizuálně otevřený je zaznamenaný poplachový signál otevřený obrazem (obrazy) z hlídaného prostoru tak, že je považovaný za ostrý poplach.

Uživatelsky ověřený je zaznamenaný poplachový signál pokládáný za ověřený zákazníkem/uživatелеm a DPPC bude vyžadovat ověření použitím odsouhlasené identifikace.

Sekvenčně ověřený je zaznamenaný poplachový signál vyslaný ze dvou nebo více nezávislých zdrojů konfigurovaných tak, že poplach je považován za ostrý. Zpracování sekvenčního ověřování může být provedeno v hlídaném prostoru systémem PZTS nebo v DPPC v následujícím způsobem:

- a) PZTS schopné zpracování sekvenčně ověřovaného poplachového signálu. Poplachový signál označený zabezpečovací firmou jako sekvenčně ověřený je přenesen do DPPC.*
- b) DPPC zpracovává sekvenčně ověřovaný poplachový signál.*

Kombinovaný účinek dvou samostatných poplachových signálů přijatých DPPC, z nichž každý pochází z nezávislého zdroje a oba vznikly ve stanoveném časovém intervalu v hlídaných prostorech.

Sekvenční ověřování poruchy přenosu:

- 1) DPPC přijme signál poruchy přenosu následovaný poplachovým signálem, nebo obráceně, z téhož hlídaného prostoru během jediné stanovené periody.*
- 2) Z téhož hlídaného prostoru existují dva signály poruchy přenosu, každý po jiné přenosové cestě řešené jinou technologií (např. kabel a rádio) během jedné stanovené periody.*

15 AUDIT

Audit shody musí být proveden každoročně orgánem akreditovaným podle EN 45011 nebo EN-ISO/IEC 17020 kterýmkoli signatářem EA MLA pro soubor EN 50518. Vedení DPPC musí zajistit, že všechny neshody budou odstraněny a opraveny ve lhůtě stanovené podle EN 45011 nebo EN-ISO/IEC 17020.

16 REKLAMAČNÍ POSTUP

DPPC musí mít zdokumentovaný postup pro přijímání a zpracovávání stížností zákazníků.

17 ÚDAJE

17.1 Všeobecně

Musí být ustanoveny zdokumentované postupy definující ukládání, ochranu, oprávněné přemístování, dobu platnosti a nakládání s údaji. Musí být vypracován postup

pro zacházení, údržbu, ukládání, likvidaci a vedení zákaznickým údajů. Pro elektronicky ukládané údaje musí být všechny údaje bezpečně ukládány a musí být zavedeny zálohovací postupy.

17.2 Údaje o zákazníkovi

Údaje o zákaznících musí být udržovány v souladu s EN 50518-2:2010. Dokumentované postupy musí být k dispozici pro záznam a aktualizaci údajů o zákaznících. Změny v zákaznických údajích musí být označeny datem a časem v rámci systému správy databází.

17.3 Uchovávání údajů

Údaje musí utuchovány v souladu s EN 50518-2:2010 a musí být k dispozici dokumentované postupy.

17.4 Likvidace údajů

Pokud je třeba smazat údaje důvěrné povahy, jejich odstranění musí být provedeno v souladu s EN 15713. EN 15713 uvádí doporučení pro správu a kontrolu likvidace důvěrných informací, pro zajištění, že tento materiál je likvidován bezpečně a řádně.

17.5 Záznamy

DPPC musí vést záznamy o všech pravidelných zkouškách a údržbě zařízení DPPC.

[9]

18 BUDOUCNOST DPPC

V dnešní době jsou funkce DPPC rozšířeny o další služby. Jsou to služby pro lidi se zdravotními problémy a pro lidi, kteří jsou v penzi. Tito lidé mají k dispozici pro aktivaci poplachového signálu bezdrátová tlačítka, která mohou mít neustále u sebe. Dále mohou použít tlačítko na ovládací klávesnici, která je umístěna v místnostech, kde se nejvíce pohybují.

Zabezpečení DPPC se vylepšuje. Kontroly vstupu jsou vybaveny biometrickými systémy, které využívají otisky prstů, snímání sítnice, snímání duhovky atd.

Komunikace DPPC se střeženými prostory/objekty se začíná častěji provádět pomocí Internetu.

II. PRAKTICKÁ ČÁST

19 MANUÁL K OBSLUZE DOHLEDOVÝCH A POPLACHOVÝCH PŘIJÍMACÍCH CENTER

Tento manuál k obsluze DPPC je zpracován z pohledu evropských norem ČSN EN 50518-1 až 3: 2010 zejména pro dispečery nebo obsluhu příslušných center.

Objasním:

- co musí dispečer (obsluha) splňovat,
- jaké mají dodržet provozní postupy,
- jak se mají zachovat v nouzových stavech
- jak se mají zachovat při evakuačních postupech,
- jak mají zacházet s příslušnými signály,
- jak mají zacházet s údaji.

19.1 Definice a zkratky

Poplachový zabezpečovací a tísňový systém (PZTS)

Je to systém, který slouží pro vyhodnocení a vyvolání poplachového stavu ve střeženém prostoru/objektu.

Poplach

Je stav při výskytu nebezpečí, které hrozí člověku, majetku nebo okolnímu prostředí a většinou je vyvolaný tísňovým systéme.

Dohledové a poplachové přijímací centrum (DPPC)

Je to zařízení, které má trvalý dohledový provoz. Přijímá poplachové signály ze střežených prostorů/objektů. DPPC přijímá signály pomocí komunikačních karet, které jsou připojené k osobnímu počítači. Software, který je nainstalovaný v PC vyhodnocuje, potvrzuje a zálohují zobrazené poplachové informace.

Dispečink dohledového a poplachového přijímacího centra (Dispečink DPPC)

Nepřetržitě obsazené pracoviště, kde jsou posílány testovací nebo poplachové zprávy o stavech střeženého prostoru/objektu PZTS. Dispečer pracoviště, vyhodnocuje testované nebo poplachové zprávy a po jejich vyhodnocení v případě nebezpečí vysílá zásahovou hlídku.

Zásahová hlídka

Je to zásahová skupina bezpečnostní agentury, která provádí zásah. Tato zásahová skupina je informována z dispečinku a poté je vyslána ke střeženému prostoru/objektu odkud přišla poplachová zpráva.

Přenosová cesta

Je to spojení mezi PZTS střeženého prostoru/objektu a DPPC.

Radiové spojení

Je to bezdrátový způsob přenosu poplachových zpráv na vyhrazených rádiových frekvencích.

Záložní zdroj energie

Jsou to akumulátory, které jsou schopné samoregenerace a mají příčinnou kapacitu pro udržení chodu systému.

Náhradní zdroj energie

Je to generátor elektrické energie, který musí být spojený s DPPC a musí být naprogramovaný tak, aby byl automaticky spuštěn při výpadku elektrické energie.

Nouzové volání dispečinku DPPC

Je to signál, který je vyslán dispečerem z DPPC v případě napadení nebo jiného nouzového stavu na dispečink jiné bezpečnostní agentury, která má neustálou obsluhu.

Dispečer (operátor) DPPC

Je to obsluha dispečinku DPPC.

Objektová karta

V objektové kartě jsou informace, telefonní čísla, přesná adresa o střeženém prostoru/objektu, které je napojené na DPPC. Všechny tyto informace jsou umístěny v databázi počítače DPPC.

Poplachový plán objektu

Je to seznam činností, které musí dispečer DPPC a poté i zásahová skupina provést při příjmu poplachové zprávy z PZTS střeženého prostoru/objektu.

19.2 Co musí dispečer (obsluha) splňovat

19.2.1 Obsazení DPPC

DPPC musí mít 24 hodinovou obsluhu, která musí být patřičně kvalifikovaná. Poskytovatel DPPC musí hlídat dispečink, aby byl pořád doplňován dalšími dispečery, pokud je nějaký nemocný nebo je mimo pracovní stav. V dispečinku musí být neustále daný počet dispečerů.

19.2.2 Patřičná kvalifikace

Veškerý personál DPPC musí mít patřičnou kvalifikaci. V kvalifikaci je obsažena příprava pro úkon fyzické ochrany v rozsahu minimálního standardu Evropského výcvikového modulu. Pro obecnou ostrahu je zapotřebí, aby dispečer byl proškolen 16 hodinovou teorií a 8 hodinovou praxí v přiděleném DPPC. Celá tahle kvalifikace je pod neustálým dohledem odborných instruktorů.

Dispečeri, kteří chtějí pracovat v DPPC musí splňovat následující podmínky:

- Musí mít potvrzení, že byli podrobeni psychodiagnostickému vyšetření. Toto vyšetření nesmí být starší jak tři roky.
- Musí být proškoleni na určité typy operačních systémů a příslušných softwarů.
- Musí ovládat určité kvalifikace, kterými jsou např. nutná obrana, krajní nouze.
- Musí všeobecně zvládat obsluhu bezpečnostních technologií.
- Musí být proškolen, jak pracovat pod tlakem, aby neudělal nějakou zásadní chybu.
- Musí umět komunikovat s člověkem, který je pod tlakem.
- Musí rychle a efektivně ovládat metodiku řízení zásahu.
- Musí za každých okolností umět poradit zásahové hlídce.
- Musí bezchybně umět poradit zásahové hlídce, jak má provést základní první pomoc. První pomoc se skládá z těchto kroků:
 1. Navázat kontakt: hlasitě oslovit zraněného
 2. Zjistit bolestivé podněty
 3. Uvolnit dýchací cesty: záklon hlavy + tah za bradu
 4. Musí se kontrolovat dech: kontrola pohledem zvedání hrudníku. Přiložíme ucho k nosu. Je zapotřebí kontrolovat minimálně 10s
 5. Musí být přivolána odborná pomoc: 155
 6. Pokud zraněný nedýchá, musí se začít s masáží srdce:
 - 30 kompresí hrudníku
 - hloubka 4-5 cm (střed hrudní kosti)
 - frekvence: 100/min
 - dýchání z úst do úst není nutné v případě, že sanitka přijede do deseti minut
 8. Pokud je zapotřebí umělé dýchání: 2 vdechy - zaklonění hlavy, zvednutí brady, stisknutí nosu

9. Pozor na výjimku při resuscitaci dětí a stavu po tonutí – první pomoc zahájíme vždy pěti úvodními vdechy
10. Resuscitace s použitím AED (automatický externí defibrilátor) - můžeme ho používat, vždy nám říká, co máme dělat.
 - Musí umět poradit zásahové hlídce při případném požáru.
 - Musí ovládat místopis.
 - Musí být bezúhonný.
 - Musí mít bezpečnostní prověrku (screening, petting).

19.3 Provozní postupy

19.3.1 Testování

Testování DPPC musí provádět dispečer pravidelně u všech zařízení, které se nachází v centru. Testování by mělo být prováděno alespoň dvakrát za 24 hodin a dále při každé změně pracovní směny. Střídající dispečer by měl být v centru minimálně patnáct minut před zahájením své pracovní doby, aby si mohl vyměnit informace o tom, co se odehrálo za uplynulou pracovní dobu.

Zařízení, u kterých se hlavně musí provádět testy jsou: indikační zařízení, komunikátor přijímacího centra, komunikační systémy, příchozí a odchozí komunikační linky. U telefonní linky (JTS) se testování musí provádět minimálně 1x za 24 hodin. U rádiové komunikace se musí testování provádět každou půl hodinu. U komunikace GPRS musí mít dodavatel u mobilního operátora vyhrazené šifrované pásmo. Počet testování se určuje podle toho, jaký střežený objekt se jedná a jaký má stupeň zabezpečení. Také záleží na majiteli střeženého objektu, kolikrát si určí testování na základě financí. Testování může probíhat 1x, 3x nebo 6x za 15 minut. Pokud vypadne GPRS, je okamžitě poslána na DPPC SMS zpráva. Dalšími zařízeními, u kterých musí být prováděno testování, zda mají správnou funkčnost jsou: poplachové systémy, zařízení pro nouzové systémy a zařízení pro elektrické napájecí zdroje. Testování těchto zařízení se musí provádět každý týden. Všechny výsledky těchto testů musí být pravidelně zálohovány na přiděleném zálohovacím PC.

19.3.2 Výstup a vstup z DPPC

Přístup do centra musí být pod neustálým dohledem kamerových systémů a systému pro kontrolu vstupu. Kontrola vstupu může být konstruována dvěma způsoby.

První způsob spočívá v tom, že dispečer bude mít k dispozici seznam všech pracovníků, kteří pracují v centru, a bude mít u každé osoby jejich identifikační znak, podle kterého je bude identifikovat a následně jim povolí vstup do předsíně centra. Neznámé osoby budou vpuštěny do centra po příslušné legitimaci.

Druhý způsob, na základě kterého by mohl dispečer pouštět osoby do centra, využívá kontroly vstupu pomocí biometrické identifikace a to především identifikaci například otisku prstu. Všichni pracovníci centra si budou muset uložit své otisky prstů do databáze systému, který bude příslušné otisky prověřovat a po vyhodnocení bude příslušná osoba vpuštěna do předsíně centra. U tohoto způsobu bude mít dispečer usnadněnou práci. Bude jenom kontrolovat, zda systém pracuje správně.

Dále musí dispečer kontrolovat, jestli osoby, které vstupují do předsíně, vstupují jednotlivě a zda se podrobily vstupní kontrole. V předsíni nesmí být více jak tři osoby, a to z bezpečnostních důvodů-

Při výstupu z centra se osoby nemusí ničím prokazovat. Dispečer pomocí kamerového systému vidí, kdo se chystá vyjít z centra. Poté co se osoba přiblíží ke dveřím a je vpuštěna dispečerem ven.

19.3.3 Správa databází

Veškerá správa databází se musí provádět uvnitř DPPC. O všechno, co se týče spravování, organizování, odstraňování a nahrávání nových klientských údajů, se stará dispečer. V DPPC musí být umístěno automatizované zařízení na příjem poplachových signálů. Při příjmu poplachového signálu se musí automaticky objevit na PC zpráva o narušení objektu. DPPC musí dodržovat veškerá ochranná opatření proti zneužití klientských údajů, které centrum má v databázi. Databázi může spravovat jen určitý počet lidí, kteří jsou informovaní o tom, že nesmějí z centra vynášet či publikovat žádné informace, které by mohly poškodit klienta nebo dobré jméno firmy.

Jestliže bezpečnostní agentura s DPPC má smlouvou o vzájemné spolupráci při případném narušení nebo při výpadku centra s jinou agenturou, která provozuje DPPC, musí mít vzájemný přístup k údajům o klientech obě centra.

Každý klient, který je připojen na DPPC má svou složku s veškerými údaji, které centrum vyžaduje. Jsou to údaje o střeženém objektu (prostoru), informace o klientovi, veškeré telefonní čísla, na které je případně klient informován o narušení objektu. Do této složky jsou poté vkládány zprávy o narušení. Dále je zde zaznamenávána historie poplachů a všechny zásahy dispečera.

19.4 Nouzový plán a nouzový stav

Jestliže je DPPC vyřazeno z provozu, musí být vypracován nouzový plán, který slouží pro vyřešení nouzové situace a pro případné vypořádání vzniklých škod. Nouzový plán se musí zhotovovat tak, aby byl použitelný při mimořádné události, která může zhoršovat kvalitu služeb DPPC. Při opatření se musí dodržet určitá pravidla, která jsou striktně určena a musí se aplikovat na technické nebo jiné havárie.

Nouzový plán se skládá z:

- Kontaktních údajů dodavatelů a poskytovatelů služeb schopných provést obnovení při zachování dané služby,
- Prostředků, které budou pokračovat nebo budou obnoveny dodávky služeb,
- Přezkoumání nouzového plánu, který nebude trvat déle než do šesti měsíců vedení. Poté musí být zdokumentován a na základě výsledků navrhnout veškerá nápravná opatření, [8]

Vybrané abnormální události, které musí být brány v úvahu při plánování nouzového plánu:

- Kompletní selhání schopností provádět veškeré úkony,
- Poruchy nebo poškození technické infrastruktury stanoviště, komunikačního zařízení,
- Požár včetně vystavení ohně v sousedních a přilehlých objektech,
- Povodně nebo jiné průniky vody,

- Poškození při bouřce, včetně přepětí v důsledku blesku,
- Náraz vozidla nebo kolejového vozidla či letadla,
- Úmyslné poškození,
- Zločin pomocí útoku nebo vyhrožování bombou. [8]

19.5 Evakuační postupy

Každé DPPC musí mít svůj vypracovaný plán částečné evakuace a plán úplné evakuace. Evakuační plán musí být sepsán tak, aby obsahoval všechny možnosti, kvůli kterým je evakuace spuštěna. Dále musí obsahovat zásady, při kterých může být evakuace ukončena. Na úkor ukončení evakuace musí být sepsán postup pro obnovení provozu centra a jeho bezchybného provozu. Než vejdou do centra příslušné osoby, musí být budova kompletně zkontrolována hasičskou záchranou jednotkou. Ta stanoví, jestli v budově nehrozí žádné nebezpečí jakými jsou např. rozpad budovy, únik nebezpečných látek atd. Po vypracování protokolu, mohou do budovy vstoupit příslušné osoby a zahájit provoz centra.

Všechny osoby, které pracují v DPPC musí projít výcvikem, v jehož průběhu dostanou instrukce, jak se zachovat při evakuaci centra. Musí znát veškeré nouzové postupy. Musí vědět, kde jsou umístěna signalizační tlačítka pro vyvolání poplachu a musí vědět, kde se nachází všechny nouzové východy.

19.5.1 Nouzový vstup/výstup

Veškeré nouzové vstupy/výstupy v DPPC musí být zaznamenány v konstrukčním plánu a v pracovním postupu DPPC. Nouzové vstupy/výstupy musí být viditelně označeny v celé budově, kde se nachází přijímací centrum. Každé DPPC musí mít zpracovaný dokument, kde jsou vypsány všechny nouzové postupy.

Dále musí existovat dokumentace o tom, kde jsou umístěny veškeré přístupové prostředky jakými jsou např. klíče, kódy nebo přístupové karty, které slouží pro vstup/výstup z DPPC. Tyto přístupové prostředky musí být bezpečně uloženy na přístupném místě, o kterém vědí jen vybrané oprávněné osoby.

19.6 Zpracování signálů

Dispečer DPPC musí pečlivě zacházet se signály, které jsou přijaty do DPPC. Musí umět zpracovávat dokumentaci, která zahrnuje příjem, zpracování a ovládání úkonů přijatých signálů.

Postup při ověřování poplachových signálů, musí být zdokumentovaný v určitém pořadí. Ověřování poplachových signálů se dělí na čtyři typy:

- Optický
- Akustický
- Sekvenční
- Zákaznické nebo uživatelské

19.6.1 Optické ověřování

Optické ověřování se provádí tak, že poplachový signál je ověřován kamerovým systémem. Dispečer má k dispozici digitální nebo analogový obraz ze střeženého prostoru/objektu. Při vniknutí nepovolené osoby do střeženého prostoru/objektu, musí dispečer vyhlásit tzv. ostrý poplach

19.6.2 Akustické ověření

Akustické ověření se provádí tak, že poplachový signál je ověřován kamerovým systémem. U tohoto ověřování nemusí být dispečer, protože poplach vyvolává sám kamerový systém pomocí autodetekce. Pokud se neoprávněná osoba pohybuje ve střeženém prostoru/objektu, kamerový systém to vyhodnotí a sám spustí akustickou informaci, tzv. ostrý poplach.

19.6.3 Zákaznické nebo uživatelské ověřování

Zákaznické/uživatelské ověření probíhá tak, že poplachový signál spustí sám zákazník/uživatel, který tvrdí, že se ve střeženém prostoru/objektu se pohybuje neoprávněná osoba. Povinností dispečera v DPPC je ověřit střežený prostor kamerovým systémem, zda se opravdu pohybuje ve střeženém prostoru neoprávněná osoba.

19.6.4 Sekvenční ověřování

Sekvenční ověřování probíhá tak, že poplachový signál je vyslán ze dvou nebo více nezávislých zdrojů, kterými může být např. kamerový systém nebo sám uživatel. Sekvenční ověření může být provedeno ve střeženém prostoru/objektu za pomoci systému PZTS nebo v DPPC.

Zpracování sekvenčního poplachového signálu umí provést i systém PZTS. Aby mohl být sekvenčně ověřený signál poslán z PZTS do DPPC, musí být označen jako poplachový signál od jiné zabezpečovací agentury. Dispečer DPPC má za úkol znovu provést sekvenční ověření přijatého poplachového signálu.

Kombinace dvou nebo více samostatných poplachových signálů, které jsou přijaté do DPPC, které musí být z nezávislého zdroje a musí být poslané v určitém časovém intervalu z daného střeženého prostoru/objektu.

DPPC musí ověřovat poruchy přenosu u sekvenčního ověřování. Porucha se většinou pozná tak, že do DPPC přijdou ze střeženého prostoru/objektu minimálně dva poplachové signály během jediného určeného intervalu.

19.7 Údaje

Dispečer DPPC musí být obeznámen, jak jsou v centru stanoveny dokumentované postupy. Tyto postupy určují, jak má dispečer zacházet s ukládáním, ochranou, oprávněným přemísťováním, dobou platnosti a nakládání s příslušnými údaji. Dále musí být zpracován postup, kde je sepsáno, jak zacházet, udržovat, ukládat, likvidovat a vést zákazníkovi údaje.

Při ukládání údajů v elektronické podobě se musí všechny údaje bezpečně uložit na zálohovací disky. Při zálohování na zálohovací disky se musí dodržet veškeré zálohovací postupy.

19.7.1 Údaje o zákazníkovi

Když se zákazník domluví na spolupráci s DPPC, je podepsána smlouva o případném střeženém prostoru/objektu, které bude centrum hlídat, musí zákazník poskytnout určité informace:

- Jméno, adresu, kontaktní telefonní čísla střeženého prostoru/objektu,
- Referenční číslo prostoru/objektu a všechna zvláštní opatření,
- Jméno, adresu, telefonní čísla uživatelů,
- Postupy, které musí být provedeny v případě poplachu,
- O dohodnuté době, jakou potřebuje uživatel, aby zvládl dát hlídaný prostor/objekt do stavu zastřeženo a do stavu klidu v případě potřeby,

Při příchodu poplachového signálu do DPPC musí dispečer vyhodnotit, o jaký poplachový signál se jedná a zda to není jen planý poplach.

Po vyhodnocení poplachu má za úkol dispečer podle zadaných údajů uskutečnit protiopatření. Při vyhlášení poplachu si dispečer otevře databázi a v ní složku klienta, u kterého byl zaznamenán poplach. Zde je sepsáno, za jakých okolností má dispečer vyslat hlídku, jestli ji má vůbec vyslat nebo zda stačí jen kontaktovat prioritní osobu, které dispečer oznámí, že střežený prostor/objekt byl napaden nežádoucí osobou. Dále jsou ve složce vypsány zmiňované telefonní čísla, které jsou seřazeny podle priorit.

Dále má dispečer k dispozici informaci o tom, v jakém pořadí má volat uživateli nebo v jakém pořadí vyslat hlídku:

- Jen kontaktovat prioritní osobu,
- Kontaktovat + vyslat hlídku
- Vyslat hlídku + kontaktovat (hovorem nebo jen SMS)
- Bez vyslání hlídky, jen kontaktovat

19.7.2 Uchovávání údajů

Údaje o klientovi by měly být uchovávány po stanovenou dobu, minimálně však po dobu dvou let. Ostatní údaje by měly být uchovávány nejméně tři roky.

ZÁVĚR

Cílem této práce bylo popsat logistické zabezpečení dohledových a poplachových přijímacích center (dále DPPC). V první řadě jsem popsal z čeho se DPPC skládá. Zjistil jsem, že centrum je rozděleno do dvou systémů. První systém je samostatný s vlastním síťovým napájením a zálohováním. Tento systém se využíval v dřívější době, protože byl velmi jednoduchý a za přijatelnou cenu. Byl stavěn tak, aby pracoval samostatně bez dalších přídavných zařízení. Druhý systém je integrovaný s osobním počítačem (dále PC). V počítači musí být vložený operační systém Windows, v kterém je nainstalovaný příslušný software k DPPC. V České republice se nachází dvě firmy, které programují tyto softwary. Jsou to firmy RADOM z Pardubic a NAM GLOBAL z Karviné. K PC jsou přiřazeny komunikační karty, které komunikují ze střeženým prostorem/objektem vysíláním testovaných nebo poplachových signálů. V dnešní době se nejvíce používá komunikace přes GSM systém, pomocí hovoru nebo SMS zprávou. Další komunikace může být přes JTS systém, který využívá veřejnou telefonní linku k přenášení signálů. V poslední řadě se může komunikace provádět přes rádiový systém. U této komunikace musí mít zprostředkovatel vyhrazené rádiové pásmo, v kterém může vysílat signály. Dále jsem popsal technické zabezpečení DPPC, kde jsem rozebral zabezpečení centra. V DPPC musí být zabudovaný poplachový zabezpečovací a tísňový systém (PZTS), kamerový monitorovací systém (CCTV), elektronický požární systém (EPS). DPPC musí mít zajištěn stálý přísun elektrického napájení. Proto jsem se v práci zmínil a vypsals potřebné záložní napájení. Jsou to záložní napájecí akumulátory a záložní generátory, které se starají o nepřetržitou dodávku elektrické energie. Další zabezpečení je personální, v kterém jsem popsal, co musí dispečer podstoupit a zvládnout, aby mohl pracovat v DPPC. Na personální zabezpečení navazuje praktická část, v které jsem navrhl manuál k obsluze pro dispečery a personál který pracuje v DPPC. Celá práce byla psána z pohledu evropských norem ČSN EN 50518 – 1 až 3 : 2010, které jsou vypsány v technické části této bakalářské práce. Podle mých zkušeností a příslušných informací jsem zjistil, že kolem 80% DPPC v ČR nesplňuje příslušné normy, protože nemá dostatečné finance na obnovení a patřičnou rekonstrukci centra.

ZÁVĚR V ANGLIČTINĚ

Aim of this thesis is to describe logistic security of surveillance and alarm receiving centre (hereinafter as "SARC"). In the first part of the thesis I described which parts constitute the SARC. I have found out that centre is divided into the two systems. The first system is independent with own power supply and backup. This system was used earlier because it was very simple and has reasonable price. It was built to operate independently without any additional devices. The second system is integrated into personal computer (hereinafter as "PC"). PC must be equipped with operating system Windows and must have installed appropriate software to SARC. In the Czech Republic reside two companies programming this software – the RADOM from Pardubice and the NAM GLOBAL from Karviná. To the PCs are attached communication cards which communicates with guarded area/object via transmitting of tested and alarm signals. Nowadays is the most used communication via GSM system that uses phone calls or SMS. Another communication is via JTS system which uses public phone line for transmitting the signals. It can not be forget to mention that communication can be done via radio system too. But in the case of this type of communication, the provider must have reserved a radio brand in which he can transmit the signals. In the next part of the thesis I described technical support of SARC and security of centre. In SARC must be installed security and emergency alarm system, CCTV monitoring system and electronic fire system. There must be also ensured a constant supply of electrical power for SARC. This is the reason why I also mentioned and made a list of necessary backup powers. These are battery backup power and backup generators that ensure continuous supply of electrical energy. In the part of thesis devoted to personnel security is described what must persons undergo and be able to manage to become the controllers in SARC. Next part of the thesis is focused on practical issues. I designed a handbook for operators and controllers employed in SARC. Entire thesis was written from the perspective of European norms ČSN EN 50518 – 1 to 3:2010 which are listed in technical part of the thesis. According to my experience and relevant information I have found out that 80 % of SARC in the Czech Republic do not fulfil relevant norms because they do not have sufficient financial resources for renovating and reconstruction.

SEZNAM POUŽITÉ LITERATURY

- [1] *Bezpečnostní a úklidové služby po celé ČR: Napojení na PCO - pult centrální ochrany*. In: Služba pultu centralizované ochrany [online]. 2006 [cit. 2012-05-16]. Dostupné z: http://www.google.cz/imgres?hl=cs&safe=off&sa=X&biw=1440&bih=794&tbm=isch&prmd=imvns&tbnid=VUDa9M9-4AyhxM:&imgrefurl=http://www.diseven.cz/sluzby/pco/&docid=yGf40Qzk58balM&imgurl=http://www.diseven.cz/files/pco5.jpg&w=306&h=229&ei=lc2zT_qAGqjC0QXmmqikCQ&zoom=1&iact=hc&vpx=195&vpy=155&dur=1148&hovh=183&hovw=244&tx=112&ty=95&sig=115010045299186827289&page=1&tbnh=135&tbnw=194&start=0&ndsp=27&ved=1t:429,r:0,s:0,i:71
- [2] *Pulty centralizované ochrany*. Zlín, 2005. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně
- [3] *Tvorba edukačního materiálu s prvky e-learningu systému PCO GLOBAL*. Zlín, 2007. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.
- [4] KAMENÍK, J a BRABEC, F. *Komerční bezpečnost*. Praha: ASPI, a. s., 2007. ISBN 978-80-7357-309-6.
- [5] *Střežení objektů přes kamerový pult centrální ochrany* [online]. 2011 [cit. 2012-05-16]. Dostupné z: http://www.google.cz/imgres?hl=cs&safe=off&sa=X&biw=1440&bih=794&tbm=isch&prmd=imvns&tbnid=yS_bSWMvP9VPnM:&imgrefurl=http://www.torex-security.cz/strezeni-objektu-pres-kamerovy-pult-centralni-ochrany&docid=SXSa5Js4lYvcIM&imgurl=http://www.torex-security.cz/wp-content/uploads/pco-kam.jpg&w=630&h=285&ei=lc2zT_qAGqjC0QXmmqikCQ&zoom=1&iact=hc&vpx=933&vpy=179&dur=350&hovh=123&hovw=272&tx=187&ty=89&sig=115010045299186827289&page=1&tbnh=88&tbnw=194&start=0&ndsp=27&ved=1t:429,r:4,s:0,i:79
- [6] *Ochrana proti přepětí: Ochrana před bleskem a ochrana proti přepětí*. [online]. 2010 [cit. 2012-05-16]. Dostupné z: http://files.sma.de/dl/7418/U_Schutz-UCZ101610.pdf

- [7] ČSN EN 50518-1. *Dohledová a poplachová přijímací centra*. Brusel: Cenelec, 2010.
- [8] ČSN EN 50518-2. *Dohledová a poplachová přijímací centra*. Brusel: Cenelec, 2011.
- [9] ČSN EN 50518-3. *Dohledová a poplachová přijímací centra*. Brusel: Cenelec, 2011.
- [10] Laucký, V. *Technologie komerční bezpečnosti II*. UTB Zlín. 2007 FAI ISBN 978-80-7318-631-9.
- [11] Laucký, V. *Technologie komerční bezpečnosti I*. UTB Zlín. 2010 FAI ISBN 978-80-7318-889-4.
- [12] Laucký, V. *Řízení technol. procesů v komerční bezpečnosti*. UTB Zlín. 2006 FAI ISBN 80-7318-432-X.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DPPC	Dohledové poplachové přijímací centrum.
EU	Evropská Unie.
PZTS	Poplachové zabezpečovací a tísňové systémy.
EZS	Elektrické zabezpečovací systémy.
GPRS	General Packet Radio Service.
PC	Personal computer.
LCD	Liquid crystal display.
UPS	Uninterruptible Power Supply.
DVD	Digital Video Disc.
JTS	Jednotná telefonní síť.
GSM	Groupe Spécial Mobile.
ISDN	Integrated Services Digital Network.
ČR	Česká republika.
ČTÚ	Český telekomunikační úřad.
SMS	Short message service.
CCTV	Closed-circuit television.
DVR	Digital video recorder.
HDD	Hard disk drive.
EPS	Elektrická požární signalizace.
SPD	Surge Protection Device.
ČSN	Česká státní norma.
EN	Evropská norma.
ATP	Alarm transmission path.
AED	Automatický externí defibrilátor.

SARC Surveillance and alarm receiving centre

SEZNAM OBRÁZKŮ

Obr. 1 Dohledové a poplachové přijímací centrum[1]	14
Obr. 2 Komunikace s DPPC[5].....	18
Obr. 3 Typické rozložení DPPC[7].....	32

SEZNAM TABULEK

Tab. 1 Minimální odolnost DPPC proti fyzickému útoku[7]	24
Tab. 2 Bezpečnostní třída[7].....	26
Tab. 3 Fyzický útok a průstřel[7].....	27
Tab. 4 Kvalitativní parametry systému zdvojené přenosové trasy[7]	30