Jihočeská univerzita v Českých Budějovicích
Zdravotně sociální fakulta

BEZPEČNOST JAKO SOUČÁST MODERNÍHO MANAGEMENTU VE ZDRAVOTNICKÉM ZAŘÍZENÍ - APLIKACE NA KLINIKU ANESTEZIOLOGIE A RESUSCITACE INSTITUTU KLINICKÉ A EXPERIMENTÁLNÍ MEDICÍNY V PRAZE

Bakalářská práce

Autor práce: Monika Körnerová
Studijní program: Ochrana obyvatelstva
Studijní obor: Ochrana obyvatelstva se zaměřením na CBRNE

Vedoucí práce: Mgr. Jiří Folvarský

Datum odevzdání práce: 4.5. 2012

ABSTRAKT

Tato bakalářská práce má téma „Bezpečnost jako součást moderního managementu – aplikace na Kliniku anesteziologie a resuscitace Institutu Klinické a Experimentální Medicíny v Praze“. Popisuje bezpečnostní systém, bezpečnostní prostředí, jeho trendy, strategii, zájmy a hrozby s následným řešením komplexní bezpečnosti zdravotnického zařízení v rámci uceleného bezpečnostního systému ve třech základních rovinách: personální bezpečnost, safety (provozní a technologická bezpečnost), security (klasická bezpečnost osob, majetku, informací a režimová opatření).

Cílem mé bakalářské práce je nastínění a následné stanovení požadované úrovně minimální bezpečnosti v souvislosti s reflexí bezpečnostních potřeb ve vědomí a praxi zaměstnanců a managementu s pochopením vztahu mezi vnitřním a vnějším prostředím zdravotnického zařízení a logikou vývoje intenzity vlastních bezpečnostních potřeb pro naplňování stanovených cílů.

KLÍČOVÁ SLOVA

Bezpečnostní systém, bezpečnostní prostředí, základní prvky bezpečnostního systému, zákonná norma v bezpečnostním systému s aplikací do vnitřního normativu organizace.

ABSTRACT

The topic of this bachelor thesis is “Security as a part of modern management – application to the Anaesthesiology and resuscitation clinic of the Institute for Clinical and Experimental Medicine in Prague”. It describes the security system, security environment, its trends, strategy, interests and threats with subsequent solution of complex security of health care facilities within comprehensive security system at three basic levels: personnel safety, safety (operational and technological safety), security (general security of people, possession, information and regime measures).
The aim of my thesis was to outline and subsequently determine the required levels of the minimum security with reflection of security needs in the awareness and practice of employees and the management with understanding the relation between internal and external environments of a health care facility and the logic of intensity development of the security needs themselves for fulfilment of the set goals.

KEY WORDS

Security system, security environment, basic elements of a security system, legal standard in a security system with application to organization’s internal standard system.

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval(a) samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47 b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to – v nezkrácené podobě – v úpravě vzniklé vypuštěním vyznačených částí archivovaných fakultou – elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejich internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 4.5.2012 .....

Monika Körnerová

Poděkování

Děkuji svému vedoucímu mé bakalářské práce Mgr. Jiřímu Folvarskému za odborné připomínky, velmi cenné rady, doporučení, vstřícné konzultace a především za poskytnutí materiálů k vypracování této bakalářské práce. Děkuji také zaměstnavateli, svým rodičům a příteli, kteří mi umožnili studium a byli mi při tomto studiu oporou.

Obsah

SEZNAM POUŽITÝCH ZKRATEK

ACS	- přístupový a docházkový systém
AČR	- Armáda České republiky
ARO	- anesteziologické a resuscitační oddělení
BOZP	- bezpečnost a ochrana zdraví při práci
BRS	- Bezpečnostní rada státu
BSL 3,4	- (Biological Safety Level) – stupeň biologického rizika
CBRN	- chemické, biologické, radiologické, nukleární
CCTV	- kamerový systém
ČR	- Česká republika
DIČ	- daňové identifikační číslo
EKV	- elektronická kontrola vstupu
EPS	- elektronický požární systém
EU	- Evropská unie
EZS	- elektronický zabezpečovací systém
FN	- fakultní nemocnice
GSM	- globální systém pro mobilní komunikaci
HD	- hard disk, záznamová jednotka
HW+SW	- technické vybavení počítače, programové vybavení počítače
HZS	- hasičský záchranný sbor
ICT	- informační a komunikační technologie
ID	- identifikace
IR LED	- infračervený přísvit
IT	- síťová technologie
IZS ČR	- Integrovaný záchranný systém České republiky
JBS	- Jednotný bezpečnostní systém
JIP	- jednotka intenzivní péče
KS	- krizový stav

LAN	- lokální síť
MU	- mimořádná událost
MV	- Ministerstvo vnitra
MZDR ČR	- Ministerstvo zdravotnictví České republiky
NATO	- Severoatlantická aliance
OOÚ	- ochrana osobních údajů
OUI	- ochrana utajovaných informací
PC	- počítač
PCO PČR	- pult centrální ochrany
PDA	- osobní digitální pomocník
PO	- požární ochrana
PTZ kamera	- panel s možností ostření, přiblížení, clona, otáčení, naklápění
THP	- technicko – hospodářský pracovník
WAN	- počítačová síť - internet
ZHN	- zbraně hromadného ničení
Z+L	- záchranné + likvidační práce
ZZ	- zdravotnické zařízení
ZZKS	- Zdravotnické zabezpečení krizových stavů

ÚVOD

Jak je již obsaženo v názvu, moje bakalářská práce se bude zabývat bezpečností jako součástí moderního managementu a jeho hlavními komponenty v rámci uceleného bezpečnostního systému s aplikací na zdravotnické zařízení - Kliniku anesteziologie a resuscitace Institutu Klinické a Experimentální Medicíny v Praze.

Ve zdravotnických zařízeních není v současné době řešena bezpečnost komplexně jako celek (vyjma klasické BOZP a požární prevence), bezpečnost je rozložena do jednotlivých dílčích úseků, každý zodpovídá za svůj úsek podle pracovního zařazení. Ve větších zdravotnických zařízeních typu fakultních nemocnic mnohdy bezpečnost jako komplexní celek „zastřešuje“ vedoucí odboru, útvaru či oddělení krizového managementu nebo požární preventista.

Pročítám-li studijní literaturu a jednotlivé statě v rámci zpracování mé bakalářské práce, které byly již v minulosti zpracovány na téma bezpečnosti s aplikací na zdravotnická zařízení, nemůžu nevidět, že každý z autorů sleduje bezpečnost ze svého úhlu pohledu (podle svoji dřívější profese, podle svého zaměření apod.). Úhel pohledu na bezpečnost platí i v rámci naší kliniky, něco jiného hodnotí pacient, něco jiného trápí lékaře, jiný problém řeší zdravotnický personál, jiný aspekt hodnotí zaměstnanec THP a celkem odlišný pohled má ten, který přijde do naší kliniky jako návštěva (pacienta, či zaměstnance).

Význam bezpečnosti jako součástí moderního managementu, především v současné době dále roste, aniž si to někteří uvědomujeme. Růst významu je způsoben nejen terorismem, na který se často odvoláváme, ale zejména změnami, kterými svět prochází. Svoji roli zde sehrávají globální rizika, vědecko-technický pokrok, ale i samotná podstata naší často konzumní společnosti.

Toto velice široké téma, které je dle dynamiky společnosti hodně proměnné, obsahuje mnoho částí, které zde ani nebude moci být plně rozebráno a objasněno. Tato bakalářská práce podává ucelený pohled na základní prvky či aspekty bezpečnosti moderního managementu ve zdravotnickém zařízení v rámci celkového bezpečnostního systému ČR.

1. SOUČASTNÝ STAV BEZPEČNOSTNÍ PROBLEMATIKY

1.1. Bezpečnostní systém ČR, základní prvky[2], [21], [23], [26]

Bezpečnostním systémem je realizována bezpečnostní politika. Základní funkcí bezpečnostního systému ČR je řízení a koordinace činnosti jednotlivých složek odpovědných za zajišťování bezpečnostních zájmů ČR. Bezpečnostní systém ČR je vytvořen jako systém komplexní hierarchicky uspořádaný, zajišťující bezpečnost ČR ve vzájemné propojenosti roviny politické (vnitřní a zahraniční), vojenské, vnitřní bezpečnosti a ochrany obyvatel, hospodářské, finanční, legislativní, právní a sociální, při respektování mezinárodních smluvních a politických principů a závazků ČR, Ústavy ČR základních práv a svobod a právního řádu ČR. Cíl a jeho funkce jsou přesně definovány v Bezpečnostní strategii ČR.

Bezpečnostní systém je v naší zemi vytvářen v souladu s ústavním pořádkem ČR a jeho základními prvky jsou především ústavní instituce a činitelé, to znamená Prezident republiky, Parlament České republiky a vláda České republiky, ale dále i Bezpečnostní rada státu a její stálé pracovní orgány. Výkonnými prvky v rámci bezpečnostního systému ČR jsou např. krajské a obecní úřady, záchranné sbory, záchranné a havarijní služby.

1.2. Bezpečnostní prostředí ČR[1] ,[2]

Bezpečnostní prostředí velice úzce souvisí s bezpečnostním systémem, který je na tomto prostředí závislý a bezpečnostní prostředí velmi ovlivňuje fungování tohoto systému.

Prostředí, které ovlivňuje bezpečnost ČR, prochází dynamickými změnami. Jeho předvídatelnost se vzhledem k rostoucí provázanosti bezpečnostních trendů a faktorů snižuje. Postavení ČR se během několika pár let rapidně změnilo. Zatímco dříve jsme byli stát, který byl odříznutý od okolního světa, v současné době jsme státem, který je součástí globalizace a moderní doby. ČR je uvnitř Evropy obklopena zeměmi, které

jsou všechny součástí EU a všechny kromě Rakouska také členy NATO, což jednoznačně posiluje její bezpečnost. V tomto geografickém postavení roste význam komplexního přístupu, který kombinuje vojenské a civilní nástroje, včetně diplomatických a ekonomických prostředků k předcházení hrozeb a zmírnění jejich negativních vlivů. Charakteristickým rysem současného prostředí je skutečnost, že i nestabilita a konflikty za hranicemi Evropy mohou mít přímý dopad na naši bezpečnost.

1.3. Největší hrozby a rizika pro ČR, aplikace na zdravotnická zařízení [2], [3]

V rámci největších hrozeb a rizik vyplývajících pro ČR je velmi významná spolupráce s mezinárodními organizacemi pro bezpečnost a dodržování jejich platné legislativy a úmluv. Bezpečnostní hrozby se do značné míry odvíjejí od slabých či zhroucených států, jejichž vlády nejsou schopny zajistit vlastní obranu, bezpečnost svých občanů a vládu práva. Mezi hlavní zdroje hrozeb a rizik patří vyhrocené postoje vůči hodnotovým základům naší společnosti, zpochybňující koncept demokratického právního státu a popírající základní lidská práva a svobody. Nositelem těchto postojů mohou být jak státy, tak stále častěji různá uskupení a jejich stoupenci.

Na základě analýzy bezpečnostního prostředí, ve kterém se ČR nachází, lze identifikovat specifické hrozby a rizika pro její bezpečnost. Tyto hrozby a rizika mohou být záměrné (úmyslného charakteru) tak i nezáměrné (neúmyslného charakteru).

Úmyslné hrozby jsou hrozby, které vznikají v přímé souvislosti s působením sil a jevů vyvolaných činností člověka s cílem poškodit určitou skupinu lidí, či celého státu. V současné době se jedná zejména o terorismus, šíření zbraní ZHN (látek CBRN) a jejich nosičů, organizovaný zločin a korupce s možným prorůstáním do veřejné správy, ohrožení funkčnosti kritické infrastruktury, přerušení dodávek strategických surovin nebo energií, kybernetické útoky.

Neúmyslné hrozby jsou hrozby, které vznikají v rámci působení sil a jevů vyvolanými přírodou bez přičinění lidského faktoru, je to například šíření různých infekčních virů a nákaz, známých jako epidemie, či pandemie a dále pak přírodní katastrofy.

Terorismus je charakterizován jako souhrn nehumánních metod hrubého zastrašování odpůrců hrozbou síly a užitím násilí. Cílem teroristů je upozornit na sebe tak, aby bylo otřeseno veřejné mínění. Hovoří se o něm také jako o cílevědomém použití organizovaného násilí proti nezúčastněným osobám za účelem dosažení politických, kriminálních nebo jiných cílů. Tyto cíle představují ve svých důsledcích ohrožení velkých skupin nebo i celé společnosti a negativně se promítají do politických vztahů státu. K základním druhům terorismu můžeme řadit ideologický, etnický, náboženský, chemický, biologický, radionukleární. Jsou schopny přímo ohrozit lidské životy a zdraví, ale také kritickou infrastrukturu.

ZHN (látky CBRN) slouží k usmrcení nebo paralyzování velkého množství lidí. Proto jejich užití především v oblastech s nedemokratickým systémem vládnutí a mezi teroristickými skupinami představuje obrovské riziko pro celý svět a je nutné toto nebezpečí eliminovat a zajistit preventivní opatření proti jejich šíření. Proto je důležité kontrolovat pohyb nejen legálních zbraní, ale především zjišťovat chod a transfer zbraní nelegálních. Vzhledem k možným účinkům představují největší nebezpečí zbraně biologické a jaderné. Při hodnocení pravděpodobnosti útoku jsou největším nebezpečím zbraně chemické a radiologické.

Organizovaný zločin a korupce získává v současném bezpečnostním prostředí širší rozměr, který prostřednictvím obchodních i osobních vztahů překračuje hranice států, tedy nevyjímaje i našeho. Narůstá schopnost kriminálních sítí narušovat normální chod institucí a hodnoty právního státu, infiltrovat především orgány státní správy a ohrožovat bezpečnost občanů.

Ohrožení funkčnosti kritické infrastruktury by mělo bezpochyby závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví nebo ekonomiku státu. Kritická infrastruktura představuje klíčový systém prvků s vysokým stupněm vzájemného propojení jednotlivých odvětví, je tedy ohrožena komplexně a to přírodními, technologickými a asymetrickými hrozbami.

Přerušení dodávek strategických surovin nebo energií – ropa, plyn, voda, elektrická energie jsou nepostradatelnou součástí každého z nás. Bez těchto strategických surovin

by dnešní svět jen stěží fungoval. Proto je významné a důležité se o zásoby těchto strategických surovin starat a zajistit jejich bezporuchový chod.

Kybernetické útoky mohou představovat nový způsob vedení války nebo mohou mít kriminální či teroristickou motivaci a mohou být použity k destabilizaci společnosti. Čím více roste závislost na informačních a komunikačních technologiích, využívání propojenosti sítí, tím více se zvyšuje zranitelnost státu a jeho občanů vůči kybernetickým útokům.

Přírodním katastrofám bohužel nemůžeme zabránit, lze pouze snížit následky jejich působení a to preventivními opatřeními jako jsou např. včasné předpovědi a následné reakce. Extrémní projevy počasí a pohromy přírodního původu mohou mít kromě ohrožení bezpečnosti, životů, zdraví obyvatel a jejich majetku a životního prostředí dopad také na ekonomiku země, zásobování surovinami např. pitnou vodou či poškození kritické infrastruktury. Šíření infekčních nemocí s pandemickým potenciálem zvyšuje zranitelnost populace a klade větší nároky na ochranu veřejného zdraví s následným zajištěním poskytování zdravotní péče.

V rámci největších hrozeb a rizik pro ČR má při zajištění bezpečnosti v oblasti životních a dalších významných zájmů nenahraditelnou roli oblast zdravotnictví, zabezpečující připravenost na zvládání situací spojených s hromadným postižením osob na zdraví takového rozsahu, který si vyžádá přijetí mimořádných opatření, od úrovně vyhlášení Traumatologických plánů až po krizová opatření. Pro vytipované hrozby a rizika jsou v rámci zdravotnických zařízení zpracovány Typové plány (epidemie – hromadné nákazy osob, narušení dodávek léčiv a zdravotnických prostředků velkého rozsahu apod.). Limitujícím faktorem připravenosti systému zdravotnictví je okamžitá příjmová kapacita zdravotnických zařízení k zajištění hromadného příjmu postižených osob na zdraví. Kapacitu nejvíce omezuje konečný počet odborného zdravotnického personálu a počet operačních sálů s lůžky následné intenzivní péče vybavených potřebnou zdravotnickou technikou. Lůžková kapacita zdravotnických zařízení související s vyhlášením Traumatologických plánů je garantována v rámci tzv. uvolnění celkového lůžkového fondu (lůžka následné péče, lůžka ARO a lůžka JIP) a to do 60

minut, 180 minut a 360 minut s centralizací jejich počtů v rámci Traumatologických plánů jednotlivých krajů.

Za jednu z aktuálně nejzávažnějších hrozeb je považováno teroristické zneužití vysoce nebezpečných biologických agens, proti kterým není dostatečně účinná prevence ani léčba. Vážným problémem ve zdravotnických zařízeních je ten, že zde nejsou k dispozici zařízení stacionárního či mobilního typu, která by pracovala v podmínkách standardů bezpečnosti BSL 3 nebo BSL 4 (Biosafety level), tj. taková, která by bez rizika úniku zmíněných vysoce nebezpečných agens do okolí zajistila bezpečnou mikrobiologickou diagnostiku a izolaci nemocných. V současné době splňuje stupeň bezpečnosti BSL 3 specializované pracoviště biologické ochrany Nemocnice Na Bulovce s omezenou lůžkovou kapacitou, BSL 3 a 4 specializované zdravotnické zařízení Armády ČR, tzv. Centrum biologické ochrany Těchonín. Zařízení slouží ke komplexnímu zabezpečení biologické ochrany AČR ve specializované infekční nemocnici pro izolaci a léčení osob se zvláště nebezpečnými a exotickými infekcemi, poskytuje izolačně – karanténní kapacity pro vyšetření vojáků po jejich návratu z misí. Slouží jako výukové, výcvikové a školicí středisko pro vojenské, ale i civilní specialisty. Centrum biologické ochrany Těchonín je součástí IZS ČR.

V rámci optimalizace současného stavu spojené se zneužitím vysoce nebezpečných biologických agens a následnou možnou izolací provádí MZDR ČR aktivní činnost za účasti příspěvkových organizací, jejímž zřizovatelem je MZDR ČR a to především Zdravotnického zabezpečení krizových stavů a jednotlivých Fakultních nemocnic, o racionálním využívání pohotovostních zásob dekontaminačních a izolačních bioboxů pořízených pro resort zdravotnictví, které jsou uloženy v centrálním skladě ZZKS tak, aby tyto materiálové prostředky byly začleněny do materiálových prostředků jednotlivých FN např. formou zápůjčky a v případě MU spojené se zneužitím vysoce nebezpečných biologických agens a tyto mohly být plně využity. S touto aktivitou souvisí v rámci FN vyřešení organizačních a technických opatření s pravděpodobností vydáním vyhlášky v rámci resortu zdravotnictví s následným řešením těchto základních otázek:

- stanovit způsob součinnosti mezi ZZKS Příbram (určená pobočka) a FN pro „případ potřeby umístění dekontaminační sprchy a ochranného izolačního prostředku“,
- stanovit v součinnosti se ZZKS Příbram systém provozní údržby o prostředky biologické ochrany (kdo , v jakých periodách , v jakém rozsahu),
- zpracovat v součinnosti se ZZKS Příbram a IZS (HZS) metodiky činnosti pro použití a využití prostředků biologické ochrany ve FN ke vztahu k činnostem IZS,
- (typové plány) - návaznost postupů,
- vyčlenit prostředky (finance, osoby) na pravidelnou údržbu a revizi prostředků biologické ochrany,
- stanovit osoby v příslušném pracovním zařízení s odpovědností tzv. „dekontaminačního družstva“,
- definovat rizika práce ve vztahu k prováděné činnosti,
- stanovit rozsah a obsah potřebných znalostí těchto osob a jejich technického a materiálního zabezpečení,
- stanovit způsob vzdělávání a potřebný stupeň způsobilosti,
- stanovit způsob dosažitelnosti členů „dekontaminačního družstva“ (režim pohotovosti, svolání, hrazení nákladů),
- stanovit systém nácviků („dekontaminačního družstva“, potřebný zdravotnický personál).

Tabulka č.1 Hrozby a rizika narušení bezpečného prostředí zdravotnického zařízení v rámci vnějších vazeb – výčet

P.č.	Typ (druh) ohrožení	Způsob projevu – určující znaky	Výpis z krizového plánu			
			Ohrožující faktor		Zařazení ZZ do Z+L prací *)	
			ano	ne	ano	ne
1.	živelní a ekologická katastrofa	a) protržení přehrady a hrází menších vodních ploch	xx			xx
		b) sesuv půdy a skal		xx		xx
		c) větrná bouře, vichřice, smršť	xx			xx
		d) rozsáhlé požáry porostů				xx
		e) povodeň	xx			xx
		f) epidemie	xx		xx	
		g) epizootie		xx		xx
2.		a) výbuch a následný rozsáhlý požár objektů	xx		xx	
	technické a technolog. havárie	b) toxická havárie	xx		xx	
		c) únik látek z dálkovodů a zásobníků (plyn, ropa, voda)	xx			xx
			xx		xx	
		d) havárie na dopravní cestě nebo koridoru (silniční, železniční, letecká , vodní)	xx		xx	
3.		e) únik radioaktivních látek	xx			xx
		a) dočasná omezení a limity,celní omez.,certifikáty	xx			xx
	narušení ekonomických	b) platební neschopnost a směnitelnost národní měny	xx			xx
4.	vztahů	c) ekonomický konflikt		xx		xx
		a) sociální a etnické nepokoje		xx		xx
5.		b) rozsáhlá migrace uvnitř státu, c) vně státu	xx		xx	
	narušení sociálních vztahů	a) vnitř. ohrožení stability státu (terorismus, diversní akce)	xx			xx
			xx		xx	
		b) vnější ohrožení celistvosti státu				
	ozbrojené nebo vojenské ohrožení	c) vyhlášení nouzového stavu, stavu ohrožení a vál. stavu				
Poznámka - zařazení ZZ jako ostatní složky IZS při řešení MU v rámci teritoria						

Zdroj: Výpis „Vnitřní havarijní plán zdravotnického zařízení“

Tabulka č.2 Hrozby a rizika narušení bezpečného prostředí zdravotnického zařízení v rámci vnitřních vazeb – výčet

P. č.	Typ (druh) ohrožení	Způsob projevu – určující znaky	Výpis z krizového plánu			
			Ohrožující faktor		Zapojení ZZ do Z+L prací *)	
			ano	ne	ano	ne
1.	živelní a ekologická katastrofa	a) protržení přehrady a hrází menších vodních ploch	xx		xx	
		b) sesuv půdy	xx		xx	
		c) větrná bouře, vichřice, smršť	xx		xx	
		d) požáry (atmosférický vznik)	xx		xx	
		e) povodeň	xx		xx	
2.	technické a technolog. havárie	a) výbuch	xx		xx	
		b) požáry	xx		xx	
		c) toxické havárie v provozech	xx		xx	
		d) únik látek z dálkovodu a zásobníků (voda,plyn)	xx		xx	
		e) únik radioaktivních látek				
3.	porušení dodavatelsko-odběratelských vztahů	a) dovozní omezení a limity,celní omezení a certifikáty				
		b) platební neschopnost				
	Poznámka	- vlastní postižení ZZ mimořádnou událostí, řešení v rámci zásahu složek IZS v nemocnici				

Zdroj: Výpis „Vnitřní havarijní plán zdravotnického zařízení“

Tabulka č.3 Analýza hrozeb a rizik narušení bezpečného prostředí – dopad na činnost zdravotnického zařízení

Pořadové číslo	Druh ohrožení	Působení v rámci ZZ – vnitřní struktury	Působení v rámci teritoriální působnosti - vnější vazby
1.	Protržení přehrady, hrází, menších vodních ploch	- s vysoce rizikovým vlivem narušení bezpečného prostředí – viz. „Povodňový plán FN HK“	- hromadné postižení osob s předpokladem vzniku zranění, infekčních chorob a nemocí spojených se sníženým hygienickým standardem
2.	Sesuv půdy, skal	- bez vlivu narušení bezpečného prostředí	- hromadné postižení osob – převážně se vznikem specifických zranění, sekundárně – infekční choroby
3.	Větrné bouře, vichřice, smršť	- poškození budov (druhotně přerušení inženýrských sítí), zranění osob - ošetření, evakuace, povolání záložních sil	- individuální i možné hromadné postižení osob - zranění, infekční choroby
4.	Rozsáhlé požáry porostů	- bez vlivu narušení bezpečného prostředí	- hromadné postižení osob – zranění (včetně specifických – popáleniny, dušnost), infekční choroby
5.	Povodeň	- se středním vlivem narušení bezpečného prostředí – viz „Povodňový plán FN HK“	- hromadné postižení osob s předpokladem vzniku zranění, infekčních chorob a nemocí spojených se sníženým hygienickým standardem; duševní pomoc
6.	Epidemie	- onemocnění personálu – narušení standardních léčebných týmů – povolání záložních sil (ČSČK, medici z LF dle „Pandemického plánu FN HK“)	- hromadné postižení osob – podíl na prevenci a eliminaci působících vlivů v rámci epidemiologických standardů
7.	Epizootie, antropozooneza	- onemocnění personálu – narušení standardních léčebných týmů – povolání záložních sil	- hromadné infekční postižení osob – podíl na eliminaci působících vlivů ; individuální onemocnění – izolace, transport
8.	Výbuch a následný požár objektů	- rozsáhlé destrukční poškození budov, zranění osob – ošetření, obnovení provozu povoláním záložních sil	- hromadná postižení osob s předpokladem vzniku specifických zranění vyžadujících cílenou specializační péči, příp. transport po základním ošetření
9.	Toxická havárie	- postižení osob v rámci provozních úkonů FN při nakládání a využívání látek toxické povahy (pevné, tekuté, plynné) - postižení personálu – ošetření - evakuace	- hromadné postižení osob v příslušném rozsahu, havárie zařízení (výrobní, skladovací, přepravní) s rozsahem poškození zdraví odpovídající uniklé látce
10.	Únik látek z dálkovodů a zásobníků	- poškození budov a možné stižení př přítomných ob – ošetření, evakuace	- lokální postižení osob s rozsahem zranění odpovídající prvotním a sekundárním projevům uniklé látky
11.	Havárie na dopravní cestě, koridoru	- ohraničená jednotlivá - ošetření	- hromadné postižení osob s předpokladem vzniku zranění (polytraumata) a zasažení v důsledku kontaminace prostředí
12.	Únik radioaktivních látek	- postižení osob (rámcově) v rámci speciál. provozních	- hromadné postižení osob ve specifickém rozsahu postižení - kontaminace

		úkonů ve FN při manipulaci a použití specifických typů látek v rámci diagnostických a léčebných postupů	
13.	Dočasná omezení a limity, celní omezení	- narušení dodavatelsko-odběratelských vztahů s dopadem na provozní a léčebné standardní postupy – přechod na krizové plánování	- nedostatek surovin pro výboru lékových forem a jiného zdrav.materiálu. Nedostatek hotových léků z dovozu a jiného zdrav. materiálu, vyčerpání zásob lékových forem
14.	Platební neschopnost a směnitelnost národní měny	- narušení dodavatelsko-odběratelských vztahů s dopadem na provozní a léčebné standardní postupy - přechod na krizové plánování	- nedostatek finančních prostředků na úhradu závazků. Zastavení dodávek zdravot.materiálu , služeb a léčiv pro provoz léčebných zařízení
15.	Ekonomický konflikt	- zastavení všech dodávek léčebných preparátů, zdravotnického materiálu a léčiv	- zastavení všech dodávek zdravotnického materiálu a léčiv ze zahraničí. Kritický nedostatek zahraničních léčebných preparátů dovezených z dané oblasti
16.	Sociální a etnické nepokoje obyvatelstva	- bez vlivu na narušení bezpečného prostředí při projevech mimo lokalitu FN	- soustředění velkého množství obyvatelstva s předpokladem snížení hygienických podmínek, zranění v důsledku dočasných nepokojů (vlastní účastníci, ostatní obyvatelstvo)
17.	Rozsáhlá migrace obyvatel uvnitř státu	- bez vlivu na narušení bezpečného prostředí při projevech mimo lokalitu FN	- soustředění velkého množství obyvatelstva s předpokladem vzniku epidemických nákaz v důsledku výrazného zhoršení hygienických podmínek
18.	Rozsáhlé migrace obyvatel ze zahraničí	- bez vlivu na narušení bezpečného prostředí při projevech mimo lokalitu FN	- soustředění velkého množství obyvatelstva s předpokladem vzniku epidemických nákaz v důsledku výrazného zhoršení hygienických podmínek
19.	Vnitřní ohrožení stability státu (terorismus, diversní akce)	- postižení osob při namíření teroristického útoku ve FN – provozní části, zdravotnická odd. a kliniky	- hromadná postižení osob v důsledku poranění při výbuchu, zamoření chemickými, biologickými a radioaktivními prostředky
20.	Vnější ohrožení celistvosti státu (ozbrojený konflikt)	- realizace opatření při přípravě přechodu FN z mírového na válečný stav (nouzový stav, stav ohrožení státu a válečný stav). Úkoly směrem k personálu, pacientům, směrem k řídícím funkcionářům FN – ukrytí živé síly	- kritický nedostatek zdravotnického materiálu a léčiv - možné povolání vojáků v záloze – nedostatek odborného personálu v rámci nemocnic
21.	Vyhlášení nouzového stavu,stavu ohrožení státu, válečného stavu	- přechod FN z mírového na válečný stav. Plnění úkolů personálu dle statutu FN, regulovaný přechod na změnu zajišťování léčebně-preventivní péče	- kritický nedostatek zdravot. materiálu a léčiv - podpora vojsk na režim PřO,… - zdravotnická oblast

Zdroj: Výpis „Vnitřní havarijní plán zdravotnického zařízení“

1.4. Trendy bezpečnostního prostředí[2]

Předpověď budoucích trendů bezpečnostního prostředí vychází z předpokládaných vývojů na mezinárodní úrovni, v institucích a společenstvích, jejichž členem ČR je. Protože v současné době nelze brát jakýkoliv stát jako jednotlivce, ale jako součást velkého celku, bude i v nadcházejících letech velice důležité prohlubovat vzájemnou spolupráci. Trendy bezpečnostního prostředí ústí v jen obtížně předvídatelné hrozby. Jejich vznik a rychlé šíření usnadňuje globalizace. Původci jsou stále častěji nestátní aktéři (tradiční a nové teroristické organizace, radikální náboženská, sektářská a extremistická hnutí a skupiny), kteří vytvářejí účelová spojenectví mezi sebou či s totalitními, diktátorskými a ideologicky nesnášenlivými režimy. Cíleně ohrožují náš způsob života a demokratický systém chránící základní lidská práva a svobody.

Obtížné předvídání hrozeb a možnost jejich rychlého šíření vyžadují kvalitnější a účinnější analýzy, prostředky a systémy včasného varování.

Vývoj ve světě bude určován několika klíčovými faktory:

- ❖degradace životního prostředí s následnými klimatickými změnami,
- ❖soupeřením o energetické zdroje,
- ❖růstem nových mocností a novou konfigurací globálního vládnutí.

Dopady klimatických změn a jejich vliv na životní prostředí i zdraví obyvatelstva lze obtížně předpovídat. Samotné obavy z těchto změn však mohou vést k růstu napětí mezi státy, ústit v humanitární krize s přímými dopady na místní, státní i mezinárodní struktury, včetně možné eskalace lokálních konfliktů doprovázené zvýšenými migračními tlaky.

Rostoucí závislost na dostupnosti přírodních zdrojů vede k intenzivnější globální soutěži v zajištění přístupu ke strategickým surovinám a energiím. Zvyšuje se význam ochrany kritické infrastruktury a prostředků přepravy strategických surovin, které se vyznačují vysokou mírou zranitelnosti. Trend zneužívání pozice výhradního dodavatele těchto surovin či tranzitní země k prosazení vlastních zájmů má dopad i na zajištění základních potřeb ČR a lze jej označit za asymetrickou hrozbu strategické povahy.

Na rovnováhu bezpečnostního prostředí mají vliv rostoucí ambice nových globálních a regionálních aktérů. Aspirace některých z těchto států jsou spojeny s významným růstem jejich vojenských kapacit včetně zbraní hromadného ničení a jejich nosičů, rostoucí aktivitou na finančních trzích, soutěžení o vliv ve strategických oblastech a agresivnějším prosazováním jejich politických ambic na mezinárodních fórech.

1.5. Bezpečnostní strategie a zájmy ČR

Bezpečnostní strategie ČR je základním dokumentem bezpečnostní politiky ČR, na který navazují dílčí strategie a koncepce, byla poprvé přijata v roce 1999 a v roce 2003 byla po roce 2001 podruhé novelizována. Je definována v pěti hlavních bodech, které mají za úkol přiblížit otázku bezpečnosti, provádět nezbytné kontroly a přijímat různá bezpečnostní opatření. Do těchto pěti hlavních bodů patří: Východiska bezpečnostní politiky ČR, Bezpečnostní zájmy ČR, Bezpečnostní prostředí ČR a Strategie prosazování bezpečnostních zájmů ČR včetně popisu bezpečnostního systému ČR. Základní hodnotový právní rámec pro tvorbu a uplatňování Bezpečnostní strategie ČR představuje ústavní pořádek ČR, zejména Ústava ČR, Listina základních práv a svobod a ústavní zákon č.110/1998 Sb., o bezpečnosti České republiky, v platném znění.

Bezpečnostní strategie ČR (Bezpečnostní strategie) je vládní dokument zpracovaný ve spolupráci s Kanceláří prezidenta republiky a Parlamentem ČR na principu nadstranickosti. Na tvorbě dokumentu se rovněž podílela bezpečnostní komunita ČR zahrnující zástupce státní i nestátní sféry.

Bezpečnostní strategie ČR definuje v pěti kapitolách základní hodnoty, zájmy, postoje a ambice ČR při zajišťování své bezpečnosti:

V kapitole „Východiska bezpečnostní politiky ČR“ jsou zformulovány principy, na nichž je bezpečnostní politika ČR založena.

V kapitole „Bezpečnostní zájmy ČR“ jsou definovány životní, strategické a další významné zájmy ČR.

V kapitole „Bezpečnostní prostředí“ jsou identifikovány trendy, hrozby a z nich plynoucí rizika, jež formují prostředí, v němž ČR ochraňuje a prosazuje své zájmy.

Ve stěžejní kapitole „Strategie prosazování bezpečnostních zájmů ČR“ jsou vymezeny přístupy k ochraně zájmů ČR v oblastech zahraniční, obranné a hospodářské politiky a v oblasti politiky vnitřní bezpečnosti a veřejné informovanosti.

V kapitole „Bezpečnostní systém ČR“ jsou definovány prvky bezpečnostního systému ČR, jejich struktura, a vymezeny povinnosti, kompetence a odpovědnosti jednotlivých součástí systému.

Bezpečnostní strategie ČR chápe pojem bezpečnost jako žádoucí stav, kdy jsou na nejnižší míru snížena rizika pro ČR plynoucí z hrozeb vůči: obyvatelstvu, svrchovanosti a územní celistvosti, demokratickému zřízení a principům právního státu, vnitřnímu pořádku, majetku, životnímu prostředí, plnění mezinárodních bezpečnostních závazků a dalším definovaným zájmům.

1.6. Manažer, zaměstnavatel, bezpečnostní manažer a bezpečnost[6],[27]

Manažer, zaměstnavatel je ve své roli vedoucím pracovníkem, který vždy zodpovídá za chod dané organizace. Ke své práci potřebuje určité předpoklady a to získané i vrozené.

Získané předpoklady jsou takové, které získáme výchovou a vzděláním, částečně sem patří i intelektuální vlastnosti, které jsou sice vrozené, ale dají se částečně ovlivnit i výchovou. Příkladem pro získané předpoklady jsou: zkušenosti, znalosti, asertivita a komunikace.

Vrozené předpoklady se nedají výchovou moc ovlivňovat. Patří sem: temperament, empatie a zejména intelekt.

Manažer pracuje prostřednictvím svých podřízených. Zodpovídá za jejich práci, pozitivně je motivuje a snaží se o dodržení souladu potřeb jejich i potřeb firmy. Má povinnost informovat jak své podřízené tak i nadřízené. Reaguje na chyby v systému, provádí důležitá rozhodnutí. Každý manažer by měl dodržovat určité zásady, aby jeho práce byla efektivní, to znamená, že by měl stanovit jasné cíle a cestu jak jich dosáhnout. Dobrý manažer by měl dbát na prevenci – spíše předcházet nedostatkům, než pak řešit problémy, kterým se dalo vyhnout. Manažer by měl mít schopnost

komunikovat, měl by splňovat princip přirozené autority. Být dobrým manažerem znamená mít mnoho dovedností, příslušné znalosti a to především v psychologii.

Existují tři okruhy manažerských dovedností:

- **lidské dovednosti** - obecné dovednosti důležité zejména pro provozního manažera, personalistu. Tyto dovednosti jsou důležité pro vedení lidí, motivaci, komunikaci, spolupráci a vzájemné pochopení.
- **technické dovednosti** - schopnosti využívat specifické vlastnosti, postupy, znalosti techniky, využívat specializované pracovníky. Manažer by měl mít stejné dovednosti technického rázu jako mají lidé, které řídí, aby dokázal zajistit provedení příslušné práce.
- **koncepční dovednosti** - schopnost vidět věci jako celek např.: strategické vedení – vidět dopředu. Patří sem také schopnost řídit, integrovat a slaďovat zájmy a aktivity podniku.

Dobrý manažer by měl především umět:

- vždy jasně vymezit cíle, aby lidé věděli, na čem mají vlastně pracovat,
- zřetelně vyjadřovat pokyny,
- jednat s různými typy lidí,
- rozumět pracovníkům a tolerovat je,
- rozhodovat se ve složitých situacích,
- přijímat i poskytovat zpětnou vazbu,
- dobře organizovat a kontrolovat práci,
- být schopný přizpůsobovat se změnám.

V rámci zařazení na manažerskou funkci musí manažer vykonávat především tyto činnosti:

- plánování - stanovení cílů, určit varianty, určit termín,
- organizování – stanovení úkolů jednotlivým lidem a určování pravomocí, odpovědnost, organizační struktura,
- vedení - ovlivňování a motivování lidí, usměrňování a odměňování,
- rozhodování - důležité je znát rizika a používat modely rozhodování,
- kontrola - zjišťování odchylek, hledání příčin a způsoby nápravy.

Položme si na základě výše uvedených faktů, jaké je postavení bezpečnostního managementu a místo bezpečnostního manažera v organizační struktuře zdravotnického zařízení, co by měl znát a prosazovat v oblasti bezpečnosti?

Ve společnosti, úřadě, zdravotnickém zařízení s funkčním bezpečnostním systémem je bezpečnostní management uznávanou součástí managementu společnosti a bezpečnostní manažer partnerem vedení. Nejvhodnějším řešením ve zdravotnickém zařízení je přímá podřízenost bezpečnostního manažera, obvykle řediteli. U subjektů, které podléhají režimu zákona o ochraně utajovaných informací (mohou to být např. FN), je jednoznačně stanovena podřízenost bezpečnostního manažera odpovědné osobě.

Co by měl minimálně znát a prosazovat v oblasti bezpečnosti každý manažer nebo vedoucí?

- ❖Uvědomit si, že vrcholovou odpovědnost za bezpečnost nese právě on. Pochopit, že podcenění bezpečnostních rizik může vést k ohrožení ekonomické stability organizace nebo narušení kontinuity, činnosti. Respektovat, že celá řada povinností v bezpečnosti je dána legislativou včetně odpovědnosti vedoucího. Bezpečnostní legislativu znát alespoň rámcově, včetně rizika uložení sankcí.
- ❖Ztotožnit se s tím, že bezpečné chování organizace je velmi úzce spojeno s jeho vlastní bezpečností a naopak. Osobně znát a dodržovat požadavky bezpečnostní legislativy, zejména ve vztahu k ochraně osob a informací. Využít nabídky pro vzdělání se v této oblasti. Naučit se nakládat s bezpečnostními informacemi jako s financemi. Dodržovat zásadu „need to know“ pro veškerou práci s klasifikovanými a dalšími citlivými informacemi. Nezveřejňovat zdroje získaných bezpečnostních informací.
- ❖Za klíčovou osobu pro řešení komplexní bezpečnosti považovat bezpečnostního manažera. Zajistit mu odpovídající postavení v organizační struktuře a vybavit ho nezbytnými pravomocemi. Obracet se na něho s důvěrou při řešení všech bezpečnostních problémů. Kontakt s bezpečnostním manažerem má být přímý. Čím dále je vrcholový manažer od bezpečnosti, tím více je vystaven bezpečnostním rizikům.

- ❖Řízení bezpečnosti se musí odehrávat systémově a komplexně. Základem řízení bezpečnosti je bezpečnostní politika, která byla vytvořena na základě analýzy rizik. Zpracování bezpečnostní politiky a další řídicí dokumentace v oblasti bezpečnosti je možné zajistit dodavatelsky. Dodavatel těchto služeb by neměl být současně jejich realizátorem.
- ❖Vyžadovat u všech podřízených prosazování a hodnocení bezpečnosti jako součást procesu řízení.
- ❖Bezpečnost není jen o nejnižší ceně dodávek outsourcovaných služeb, důležitými kritérii jsou kvalita a bezpečnostní spolehlivost. Cena by proto neměla být u bezpečnostních služeb jediným měřítkem. Pro výběr dodavatele bezpečnostních služeb a následný smluvní vztah je důležitá odborná specifikace předmětu služeb a stanovení míry a úrovně bezpečnosti.
- ❖Bezpečnost vyžaduje jako ostatní oblasti periodickou údržbu a kontrolu. Manažera by proto neměly výstupy auditů a kontrol bezpečnosti zajímat nejen tehdy, když se stane mimořádná událost. Pro ověření efektivnost bezpečnostních opatření, kvality outsourcovaných služeb a optimalizace bezpečnostních nákladů využívat externí bezpečnostní audit. Dodavatelem auditu nemají být z důvodu objektivnosti posouzení dodavatelé bezpečnostních technologií ani bezpečnostní služby.

Znát alespoň rámcově oblasti činnosti, které zajišťuje bezpečnostní manažer (útvar):
ochrana osob včetně VIP a bezpečnostní vzdělávání,

- ❖ochrana hmotného majetku,
- ❖ochrana klasifikovaných a důležitých informací (OOÚ, OUI…),
- ❖bezpečnost informačních a komunikačních technologií (ICT),
- ❖BOZP a požární ochrana,
- ❖řešení mimořádných událostí a bezpečnostních incidentů,
- ❖krizové řízení,
- ❖business kontinuita,
- ❖zajišťování spolupráce s bezpečnostními orgány a orgány činnými v trestním řízení,
- ❖technologická bezpečnost a havarijní plány,
- ❖správa bezpečnostních technologií,

❖řízení výkonu a kvality outsourcovaných služeb,

❖vydávání interních předpisů v oblasti bezpečnosti,

❖kontrola bezpečnosti.

Zamyslíme-li se nad bezpečností komplexně, hodnotíme tím objektivní stav celého subjektu, tedy můžeme definovat bezpečnost jako permanentní proces identifikace hrozeb, analýzy rizik, přijímání preventivních opatření k zabránění vzniku nestandardních bezpečnostních situací, případně opatření k odstranění následků, obnovení standardního stavu a minimalizaci ztrát na oprávněně chráněných zájmech, mezi které patří :

❖život a zdraví člověka,

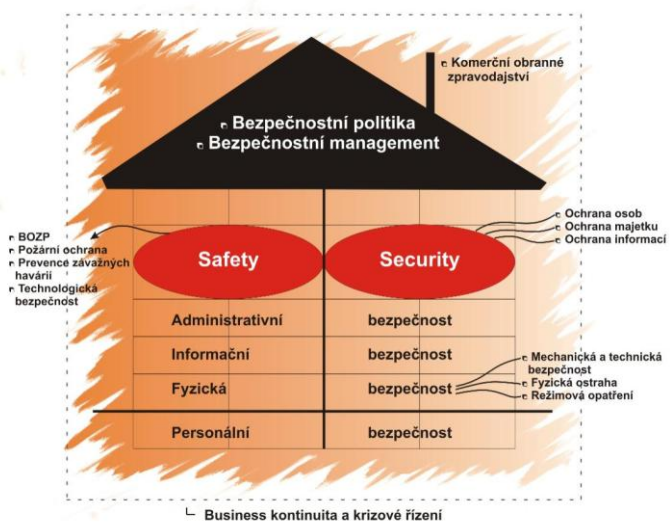
❖hmotný majetek,

❖nehmotný majetek (informace),

❖životní prostředí,

❖dobré jméno firmy (organizace; instituce).

Názorně můžeme vidět celkový rozsah bezpečnosti na schématu domu, viz.obrázek č.1.



Obrázek č. 1

Zdroj: Miroslav Fryšar a kolektiv, Bezpečnost pro manažery, podnikatele a politiky, Praha 2006 ISBN 80-86445-22-4 str.1

Virtuální dům tvoří ucelený bezpečnostní systém. Jeho základovým pilířem je personální bezpečnost. Jak je z obrázku zřejmé, dům je rozdělen na dvě poloviny, tedy do dvou hlavních částí bezpečnosti, části safety (provozní a technologická bezpečnost), a části security (klasická bezpečnost osob, majetku, informací a režimová opatření).

Oběma polovinami bezpečnosti se pak prolínají jednotlivá bezpečnostní opatření, kterými jsou zejména:

- ❖fyzická bezpečnost,
- ❖informační bezpečnost,
- ❖administrativní bezpečnost.

1.7. Personální bezpečnost[6]

Pod tímto pojmem se skrývají veškeré otázky spojené s bezpečnostními podmínkami pro výběr top managementu, managementu, zaměstnanců a ověřování splňování těchto podmínek po celou dobu trvání zaměstnaneckého nebo jiného poměru u organizace až po ukončení pracovního vztahu. Personální bezpečnost rozdělujeme do tří základních fází: před vznikem pracovního poměru, během pracovního poměru a ukončení nebo změna pracovního poměru.

Před vznikem pracovního poměru je cílem organizace zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace. Role a odpovědnosti zaměstnanců, smluvních a třetích stran v oblasti bezpečnosti musí být definovány a dokumentovány v souladu s bezpečnostní politikou organizace. Závazky a odpovědnosti zaměstnanců, případně smluvních a třetích stran v oblasti bezpečnosti jsou stanoveny a zdokumentovány v personální dokumentaci v souladu s touto bezpečnostní politikou. V dokumentech musí být jednoznačně určena odpovědnost zaměstnance za provedené činnosti.

Závazky a odpovědnosti v oblasti bezpečnosti zahrnují:

- ❖ závazek na realizaci a dodržování zásad v souladu s bezpečnostními normativy a směrnicemi organizace,
- ❖ závazek ochrany aktiv před neautorizovaným přístupem, prozrazením, modifikací, zničením nebo znepřístupněním,
- ❖ závazek vykonávání bezpečnostních postupů nebo činností v souladu s bezpečnostními normativy,
- ❖ závazek hlásit bezpečnostní události nebo jiná bezpečnostní rizika bezpečnostnímu managementu.

V rámci přijímacího řízení musí být zájemcům o práci jasně sděleny role a odpovědnosti spojené s místem, o které se ucházejí.

Všichni uchazeči o zaměstnání, smluvní a třetí strany musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků stanovených organizací, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, ale také z hlediska jejich spolehlivosti a potenciálních rizik.

Pro potřeby této politiky je bezpečnostní prověrka chápána jako dodatečný personální proces, používaný pro hodnocení uchazečů na citlivá pracovní místa, mající za cíl získat co nejvíce informací o uchazeči, aby se zvýšily záruky výběru kvalitního a spolehlivého pracovníka. Prověrka se provádí pouze u kandidátů na přijetí na citlivá pracovní místa a to ještě před vznikem pracovněprávního vztahu. Seznam citlivých pracovních míst u zdravotnického zařízení stanoví bezpečnostní rada, vedoucí krizového managementu.

Prověrky jsou prováděny na základě požadavků stanovených touto politikou, dále s ohledem na klasifikaci informací, ke kterým by měl uchazeč získat přístup, ale také z hlediska spolehlivosti uchazeče a případných potenciálních rizik. Při prověřování je brán zřetel na ochranu soukromí, ochranu osobních dat uchazeče a na související legislativu.

Prověrka se provádí vyhodnocením podkladových materiálů dobrovolně předložených uchazečem. Uchazeč může kdykoli ukončit prověrku – v takovém

případě se mu vrátí jeho podkladové materiály a přijetí na místo, o které se ucházel, se nerealizuje.

Tam, kde jsou smluvní strany zajišťovány agenturou, smlouva s agenturou jasně specifikuje odpovědnost agentury za prověrky a v případě, že agentura za provedení prověrky odpovídá, také způsob, jakým agentura upozorní na skutečnost, že prověrka agenturou nebyla provedena, nebo že její výsledky vzbuzují podezření či pochybnosti.

S informacemi o všech uchazečích - potenciální zaměstnanci, smluvní a třetí strany, které jsou získány v rámci prověrek je nakládáno v souladu s existujícími právními normami, zejména ustanoveními zákona č. 101/2000 Sb., v platném znění. Uchazeči musí být informováni o faktu, že budou prověřováni a musí s provedením prověrky vyjádřit svůj souhlas.

Podmínky výkonu pracovní činnosti.

Pracovní smlouvy uzavřené se zaměstnanci, smluvními a třetími stranami musí obsahovat ustanovení o jejich odpovědnostech za bezpečnost informací.

Pracovní smlouvy, v souladu s bezpečnostní politikou, mimo to také upřesňují následující:

- práva a právní odpovědnost zaměstnanců, smluvních stran a ostatních uživatelů (například ve vztahu k autorskému zákonu nebo zákonu na ochranu osobních údajů),
- odpovědnost za klasifikaci a správu aktiv spojených s informačním systémem a službami zaměstnavatele,
- odpovědnosti zaměstnanců, smluvních a třetích stran pro nakládání s informacemi obdrženými od jiných společností a zúčastněných stran,
- odpovědnosti při nakládání s osobními údaji, včetně těch údajů, které byly vytvořeny v průběhu pracovního poměru,
- rozšíření odpovědností i mimo objekty zdravotnického zařízení a mimo normální pracovní dobu,
- popis kroků, které budou následovat při nedodržení bezpečnostních požadavků ze strany zaměstnanců, smluvních a třetích stran.

Zdravotnické zařízení musí mít smluvně zajištěn souhlas zaměstnanců, smluvních a třetích stran s tím, že budou dodržovat bezpečnost přiměřenou rozsahu jejich přístupu k aktivům.

Během pracovního vztahu je cílem organizace zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spojených, svých odpovědností a povinností a aby byli připraveni podílet se na dodržování politiky bezpečnosti během své běžné práce a na snižování rizika lidské chyby.

Vedoucí zaměstnanci musí po zaměstnancích, smluvních a třetích stranách požadovat dodržování bezpečnosti v souladu se zavedenými politikami a postupy. Mezi odpovědnosti vedoucích zaměstnanců patří zajištění toho, že zaměstnanci smluvní a třetí strany:

- ❖jsou dostatečně informováni o svých rolích a odpovědnostech za bezpečnost předtím, než je jim udělen přístup k citlivým informacím, informačním systémům,
- ❖obdrží metodické pokyny stanovující bezpečnostní očekávání spojené s rolí, kterou vykonávají,
- ❖jsou dostatečně motivováni dodržovat bezpečnostní politiku,
- ❖získají dostatečné povědomí o bezpečnosti, která se týká jejich rolí a odpovědností v rámci zdravotnického zařízení,
- ❖řídí se smluvními podmínkami, jednají v mezích bezpečnostní politiky a příslušných pracovní postupů,
- ❖udržují a zlepšují svoje dovednosti a kvalifikaci.

Pokud nejsou zaměstnanci, smluvní a třetí strany dostatečně seznámeni se svými odpovědnostmi za bezpečnost, mohou způsobit závažné škody. Naopak dostatečná motivace personálu vede k vyšší spolehlivosti a nižší pravděpodobnosti vzniku bezpečnostních incidentů.

Neschopnost nadřízených dostatečně motivovat a řídit své podřízené může vést u zaměstnanců k pocitu, že jejich práce není dostatečně oceněná a důležitá, což může vyústit až v negativní dopad na zdravotnické zařízení. Špatné vedení může například vést k zanedbání bezpečnosti nebo ke zneužití aktiv. V tomto případě musí být zahájeno disciplinární řízení. Disciplinární řízení se zahajuje vždy, když je uplatněno personální

opatření v souvislosti s bezpečnostním rizikem. Při tomto řízení se stanoví disciplinární komise, sestávající z předsedy (zpravidla vedoucího zaměstnance) a dvou dalších zaměstnanců. Všichni členové komise musí splňovat podmínku nepodjatosti vůči předmětu řízení.

Při disciplinárním řízení musí být obviněný zaměstnanec seznámen s obviněním a musí mu být poskytnut adekvátní prostor k vlastní obhajobě.

Po formulaci závěrů disciplinární komise musí být viník (viníci) seznámen s těmito závěry a v případě, že se chce k těmto závěrům vyjádřit, musí být jeho vyjádření postoupeno společně se závěry komise vedení zdravotnického zařízení.

Ukončení nebo změna pracovního vztahu je cílem organizace zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem.

Za proces a náležitosti spojené s ukončením, nebo změnou pracovního vztahu je odpovědný vedoucí personálního oddělení, který spolupracuje s nadřízeným zaměstnance opouštějícího organizaci tak, aby byly dodrženy veškeré aspekty bezpečnosti a odpovídající postupy. V případě změny pracovního vztahu spojené se změnou pracovního zařazení musí být realizovány činnosti navrácení zapůjčených předmětů, které zaměstnanec v novém pracovním zařazení nebude potřebovat. Vždy ale musí být provedeno odebrání všech přístupových práv zaměstnance k informačním systémům před tím, než jsou zaměstnanci v nové pozici vydefinována nová oprávnění odpovídající jeho novému zařazení.

Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí být uživatelům, smluvním a třetím stranám odejmuta nebo pozměněna přístupová práva k informacím a prostředkům pro zpracování informací.

Po zabezpečení těchto opatření následují standardní procedury ukončení pracovního vztahu.

1.8. Provozní a technologická bezpečnost

Pod tímto pojmem se skrývají veškeré otázky spojené s bezpečnostními podmínkami pro zabezpečení provozních a technologických zařízení chodu zdravotnického zařízení. Do zabezpečení bezpečnosti provozních a technologických zařízení zahrnujeme i zabezpečení hlavních zdrojů energií. Zajištění těchto prvků organizace vychází z potřeby zajistit je různými technickými prostředky (technickým zabezpečením), režimovým a organizačním opatřením, ostrahou a zabránění následného přístupu nepovolaných osob do provozních prostor a technologických částí. Existují zdroje, bez kterých si chod zdravotnického zařízení vůbec nedokážeme představit. Tyto zdroje je nutné nejen udržovat v činnosti, ale i snižovat rizika jejich napadení a je třeba vytvořit postupy jejich nahrazení.

Jedná se zejména o:

- elektrickou energii,
- telekomunikační a IT kabely,
- plyn,
- pitnou vodu,
- teplo,
- technické – medicinální plyny (kyslík, vzduch).

V rámci bezpečnostních opatření k zabezpečení provozní a technologické části zdravotnického zařízení platí tyto hlavní zásady:

- z hlediska umístění zařízení a jeho ochrana - zařízení by měla být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup,
- z hlediska podpůrných zařízení - zařízení by mělo být chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb,
- z hlediska bezpečnosti kabelových rozvodů – silové, telekomunikační kabelové rozvody a IT sítě, které jsou určeny pro přenos dat a podporu informačních služeb, by měly být chráněny před poškozením či odposlechem,

- ❖kabely a zařízení jsou zřetelně označeny, aby se zabránilo možnosti záměny v případech provádění oprav poškozených kabelů,
- ❖napájecí a telekomunikační linky připojené k prostředkům IT jsou, kde je to možné, vedeny pod zemí, napájecí kabely jsou odděleny od komunikačních rozvodů, aby se zabránilo interferenci,
- ❖z hlediska údržby zařízení - zařízení by mělo být správně udržováno pro zajištění jeho stálé dostupnosti a integrity,
- ❖z hlediska bezpečné likvidace nebo opakovaného používání - všechna zařízení obsahující paměťová média by měla být kontrolována tak, aby bylo možné zajistit, že před jejich likvidací nebo opakovaným použitím budou citlivá data a licencované programové vybavení odstraněna nebo přepsána,
- ❖z hlediska bezporuchového chodu těchto důležitých zdrojů pro chod zdravotnického zařízení jsou vytvořeny „Vnitřní havarijní plány“, kde jsou stanoveny postupy, které vycházejí ze zabezpečení běžného provozu, hodnotí možná rizika a determinují postupy a opatření jejich snižování. Po aktivování nouzového provozu (na nezbytně nutnou dobu) a odstranění škod a příčin havarijní situace dokážou obnovit původní běžný provoz.

1.9. Bezpečnost osob a majetku, informací a režimová opatření[6]

V poslední době se stává stále více případů útoků na personál zdravotnických zařízení ze strany cizích osob, tedy pacientů, návštěv pacientů a ostatních nebo krádeží majetku a informací ve zdravotnických zařízeních. Bohužel lze v budoucnosti předpokládat další stupňování této problematiky. Zdravotnická zařízení budou stát před problémem eliminace těchto činů. Základním předpokladem, jak tyto situace účinně řešit, je vymezení pohybu cizích osob pouze v prostorách určených pro veřejnost a důkladnější evidence osob vstupujících do jednotlivých částí budov. Bezpečnost osob, majetku a informací koncipujeme v rámci tzv. objektové bezpečnosti.

Objektová bezpečnost je složitým procesem, kterým se zajišťuje technické a personální zajištění ostrahy objektu tak, aby narušení, napadení nebo zcizení, resp.

zničení jakékoliv citlivé a utajované skutečnosti bylo eliminováno na minimum. Žijeme v době, kdy je jakékoliv napadení, ať již teroristické nebo kriminální, velice reálné. Důvodů je mnoho : od náboženských, přes ideologické, militantní až po ryze zištné důvody.

Ochrana objektu se zabezpečuje kombinací bezpečnostních opatření, kterými jsou:

- ❖fyzická ostraha objektu,
- ❖mechanické a technické prostředky,
- ❖režimová opatření.

Fyzická ostraha objektu se zabezpečuje vyškolenými zaměstnanci provozovatele objektu nebo zaměstnanci pověřené bezpečnostní ochranné služby (bezpečnostní agentury). Profese fyzické ostrahy je na samém spodním žebříčku, v nejnižších třídách, s nejnižšími nároky na vzdělání, praxi, psychologický profil, jazykové znalosti. Z tohoto důvodu je ostraha jedním z nejslabších článků bezpečnostního systému. Samostatnou otázkou zůstává personální výběr tzv. bezpečnostních agentur a to především outsourcingem.

U důležitých objektů se fyzická ostraha objektu zabezpečuje nepřetržitě. Fyzickou ostrahu objektu zajišťují na stanovišti určeném pro stálý výkon fyzické ostrahy objektu nejméně 2 pracovníci fyzické ostrahy objektu. Na stanoviště určené pro stálý výkon fyzické ostrahy objektu jsou vyvedena výstupní hlášení technických prostředků. Provádění fyzické ostrahy objektu je upraveno bezpečnostními standardy – směrnicí.

Mechanické a technické prostředky, jsou bezpečnostním prvkem, jehož použitím se zabraňuje, ztěžuje nebo oznamuje narušení ochrany objektu nebo zabezpečené oblasti.

Technickými prostředky jsou zejména:

- ❖mechanické zábranné prostředky, kterými jsou úschovné objekty, zámky, dveře, mříže, fólie, bezpečnostní skla,
- ❖elektrická zámková zařízení a systémy pro zabezpečení vstupů do objektů a zabezpečených oblastí, zařízení a systémy sloužící k elektronickému prokazování oprávněnosti a totožnosti osob, tzv. ACS systémy,

- ❖zařízení elektrické zabezpečovací signalizace sloužící ke zjišťování a vyhodnocení neoprávněného vstupu, tzv. EZS systémy,
- ❖speciální televizní systémy pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků v objektech, tzv. CCTV systémy,
- ❖tísňové systémy, zejména tísňové hlásiče, které fungují jako součást elektrické zabezpečovací signalizace, tzv. Alarm systémy,
- ❖zařízení elektrické požární signalizace, tzv. EPS systémy,
- ❖detektory látek nebo zařízení sloužící zejména k vyhledávání kovů,
- ❖zařízení fyzického ničení nosičů informací, tzv. Skart systémy,
- ❖zařízení proti pasivnímu a aktivnímu odposlechu utajované skutečnosti z míst vně objektu.

Režimová opatření, bez tohoto opatření nemůže být plně funkční technické zabezpečení ani ostraha. Mezi nejčastější závady v rámci režimového opatření patří chyby v klíčovém režimu a vstupu osob do objektu v mimopracovní době. Školení zaměřené na dodržování režimových a organizačních opatřeních jsou výjimečnou záležitostí. Režimovými opatřeními jsou zejména:

- ❖režim vstupu a výstupu osob, vjezdu a výjezdu dopravních prostředků, který stanoví

1. oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu, výstup a výjezd z objektu a způsob kontroly,
2. podmínky a způsob kontroly vynášení a vyvážení věcí nebo utajovaných skutečností z objektu,

- ❖režim pohybu osob, věcí, dopravních prostředků a utajovaných skutečností v objektu a jeho jednotlivých částech v pracovní a mimopracovní době,
- ❖režim manipulace s klíči, identifikačními prostředky a médii, které se používají pro systémy zabezpečení vstupů, kterým se zejména určuje systém a způsob označování, přidělování a odevzdávání klíčů, jejich úschovy a evidence, uložení duplikátů a způsob jejich použití,
- ❖režim manipulace s technickými prostředky a jejich používání.

Vnější ochrana objektu, je zajišťována souborem bezpečnostních opatření k zajištění ochrany hranice objektu, vstupů do objektu a ochrany nouzových cest a jiných průstupových a průlezných otvorů do objektu. V případě, že hranice objektu je zároveň i hranicí zabezpečené oblasti, se používají certifikované technické prostředky podle požadavků a kategorizace zabezpečených oblastí. V pracovní době mohou být, podle provozních podmínek vyřazena některá bezpečnostní opatření použitá pro ochranu hranice objektu. V těchto případech se však vždy učiní opatření, která zabrání tomu, aby se nepovolaná osoba dostala do objektu a seznámila se s citlivou či utajovanou skutečností. V mimopracovní době se celá hranice objektu nepřetržitě zabezpečuje stanoveným bezpečnostním opatřením.

Vnitřní ochrana objektu, je zajišťována souborem bezpečnostních opatření k zajištění zabezpečených oblastí. Rozsah a podmínky zabezpečení vnitřní ochrany objektu stanoví statutární orgán provozovatele objektu v souladu s dokumentací objektové bezpečnosti. K zajištění ochrany zabezpečených oblastí se použijí certifikované technické prostředky příslušných kategorií.

Dokumentace a režimová opatření objektové bezpečnosti

- vyhodnocení všech rizik,
- bezpečnostní projekt ochrany objektu, obsahující zejména umístění zabezpečených oblastí v objektu, včetně jejich třídy a kategorie a způsob použití bezpečnostních opatření při vnější a vnitřní ochraně objektu,
- technická dokumentace objektové bezpečnosti obsahující technické údaje, pokyny a pravidla pro používání technických prostředků, schéma rozmístění technických prostředků v objektu a u technických prostředků certifikovaných Úřadem doložení certifikátů nebo jejich kopií,
- provozní řád, stanovující zejména režim pohybu osob a dopravních prostředků v objektu, režim pohybu utajovaných skutečností v objektu, režim manipulace s klíči a pravidla pro výkon fyzické ostrahy objektu, obsahující režim vstupu a výstupu osob, vjezdu a výjezdu dopravních prostředků z objektu a další pokyny pro činnost fyzické ostrahy objektu,

- plán ochrany objektu, který obsahuje pokyny pro ochranu životů, zdraví, majetku a utajovaných skutečností v případě vzniku mimořádné události objektu i jeho bezprostředního okolí.

Z hlediska bezpečnosti informací se ve zdravotnických zařízeních používají následující klasifikační úrovně :

- **právně chráněná informace**

  Právně chráněná informace je taková informace, jejíž šíření je omezeno závazkem organizace (např. obchodní tajemství) nebo zvláštním právním předpisem (např. osobní údaj, informace ze zdravotnické dokumentace, zvláštní skutečnost, apod.). Nakládání s právně chráněnými informacemi a jejich označování se řídí příslušným předpisem (zákonným nebo interním) nebo v souladu se závazkem organizace.

- **citlivá informace**

  Citlivá informace je taková informace, která nespadá do výše uvedené kategorie a jejíž šíření je omezeno výhradně na okruh osob, které ji potřebují znát pro plnění svých pracovních povinností. Okruh osob, které se s informací mohou seznamovat, se vhodným způsobem vyznačí na nosič informace nebo na informaci samotnou.

- **běžná informace**

  Běžnou informací je taková informace, jejíž zveřejnění nemá negativní vliv na zdravotnické zařízení. Jsou to všechny schválené dokumenty, které nespadají do žádné výše uvedené kategorie. Tyto informace se v rámci zdravotnického zařízení mohou šířit bez omezení, ale zveřejňovány mohou být pouze stanovenými postupy.

- **informace určená ke zveřejnění**

  Jedná se o informace, o kterých bylo rozhodnuto, že budou zveřejněny. U těchto informací musí proběhnout před zveřejněním proces autorizace, v jehož průběhu dojde ke schválení správnosti obsahu a k jazykové (gramatické) kontrole. U elektronických dokumentů musí být navíc schválen jejich popis a umístění v rámci webových stránek zdravotnického zařízení.

1.10. Cyklus managementu bezpečnosti[6]

Cyklus managementu bezpečnosti představuje sled periodicky se opakujících kroků: ujasnění úkolu,

- ❖zhodnocení situace,
- ❖přijetí rozhodnutí,
- ❖realizace rozhodnutí,
- ❖kontrola a zhodnocení účinnosti realizovaných opatření.

Ujasnění úkolu v oblasti bezpečnosti zahrnuje především pochopení zadání (společenské objednávky) v rozsahu:

- ❖jaké jsou bezpečnostní potřeby firmy (organizace, instituce),
- ❖jakou váhu uděluje vedení problematice bezpečnosti,
- ❖jak je vedením definován cíl v oblasti bezpečnosti.

Zhodnocení situace je zaměřeno na:

- ❖zhodnocení vnitřní bezpečnostní situace (struktura chráněných aktiv-zájmů, dislokace chráněných aktiv, systém správy chráněných aktiv, hrozby a rizika, priority z hlediska kritičnosti rizik z pohledu potenciálních ztrát a podmínek pro zachování kontinuity podnikání, stav v aktuálním času a vývojové trendy),
- ❖zhodnocení vnější bezpečnostní situace (průmět úrovně obecné bezpečnosti a bezpečnosti v okruhu bezprostředního ovlivnění chráněných zájmů, legislativní a normativní závazky firmy, organizace, instituce, aktuální stav a vývojové trendy),
- ❖zhodnocení podmínek pro management bezpečnosti (disponibilní zdroje, čas, organizační a věcná podpora, nejvlivnější nositelé odporu a nejvlivnější zastánci).

Rozhodnutí vychází z pochopení situace a zakládá se na výsledcích hodnotících analýz.

Jeho hlavními obsahovými body jsou především:

- ❖stanovení cílů,

- ❖cíle by měly mít formální podobu (dokument; zápis z porady vedení; usnesení a pod.),
- ❖cíle by měly být zveřejněny (měli by s nimi být seznámeni všichni zaměstnanci, kterým z jejich naplnění vyplyne konkrétní úkol, kteří se budou muset podrobit změnám v oblasti režimových a organizačních opatření, aktivní spolupráce kterými usnadní dosahování cílů, u kterých zřetelné zacílení bezpečnosti způsobí jejich ukáznění na principu odstrašení).

1.11. Struktura bezpečnostního systému organizace[6]

Pod tímto pojmem rozumíme optimalizovaný soubor sil, prostředků, režimových a organizačních opatření, zacílený na minimalizaci panujících rizik a spolehlivé zajištění požadované úrovně bezpečnosti organizace, viz. obrázek č.2.

Bezpečnostní systém organizace		
Lidské síly	**Materiální prostředky**	**Organizační normy**
Vlastní zaměstnanci zapojeni trvale zapojeni dočasně **Zaměstnanci poskytovatele** zapojeni trvale zapojeni dočasně **Zaměst. subdodavatelů poskytovatele** zapojeni trvale zapojeni dočasně **Zaměstnanci dalších stran** zapojeni trvale zapojeni dočasně	EZS EPS EKV CCTV Mechanické zábrany Ochrana IS Prostředky PO Spojovací prostředky Dopravní prostředky Prostředky vyčleněné pro případ MU nebo KS atd.	Bezpečnostní politika Vnitřní bezpeč. směrnice, normy, postupy a standardy Průmět bezpečnostních směrnic do systému postupů řízení kvality Průmět bezpečnost. směrnic do systému technicko-organizačních postupů Závazná bezpečnostní dokumentace ze zákona Bezpečnostní dokumentace a postupy subdodavatelů

Obrázek č. 2

Zdroj: Miroslav Fryšar a kolektiv, Bezpečnost pro manažery, podnikatele a politiky, Praha 2006 ISBN 80-86445-22-4 str.33, vlastní úprava

1.12. Bezpečnostní politika organizace[6]

Bezpečnostní politika firmy, organizace, instituce je dokumentem koncepčního charakteru, kterým se vedení organizace či instituce hlásí ke kultuře bezpečnosti a k budování bezpečnostního systému. Patří mezi dokumenty vrcholového strategického řízení a v tomto smyslu je v plné míře závazná pro všechny zaměstnance.

Bezpečnostní politika má zpravidla tuto strukturu obsahu:

- **deklarace závaznosti,**
- **vymezení odpovědnosti,** (odpovědnost za efektivnost a účinnost koncepce, odpovědnost za praktickou realizaci, odpovědnost za odborné řízení, odpovědnost za komplexní hodnocení účinnosti, odpovědnost za efektivnost a účinnost koncepce bezpečnostní politiky nese vrcholové vedení, odpovědnost za její praktickou realizaci nesou všichni zaměstnanci v souladu se svojí služební pozicí v organizační struktuře a v souladu se svou náplní práce, odpovědnost za její odborné řízení a komplexní hodnocení účinnosti nesou vedoucí zaměstnanci, bezpečnostní management),
- **hlavní cíle,** (minimalizovat přímé hmotné a finanční ztráty, vyloučit možnost vzniku druhotných ztrát v důsledku úniku a zneužití informací nebo poškozením dobrého jména společnosti, vytvořit organizační podmínky pro to, aby byly minimalizovány možné ztráty, plynoucí z akcí nepřátelských osob a skupin, případně působení živlů či jiných destruktivních sil, minimalizovat újmy plynoucí z nedodržení ustanovení BOZP, nebo z absence takových ustanovení),
- **zaměřenost bezpečnostní práce na konkrétní rizika,** (analýza rizik; hlavní vnější a vnitřní rizika),
- **úkoly v oblasti budování, rozvoje a fungování bezpečnostního systému,** (cílový stav, úkoly v oblasti cílevědomého rozvoje všech prvků struktury bezpečnostního systému, etapy a úkoly v jednotlivých etapách, základní pravidla pro plánování sil a prostředků).

Mezi základní principy koncipování bezpečnostní politiky firmy, organizace, instituce řadíme:

- **princip všeobecné povinnosti,** tento princip vyjadřuje skutečnost, že povinností každého zaměstnance společnosti je přispívat k ochraně majetku a dalších oprávněných zájmů svého zaměstnavatele. Z této všeobecné povinnosti není principiálně nikdo vyňat. Jakým způsobem je zaměstnanec povinen přispívat k ochraně oprávněných zájmů organizace, je stanoveno organizačním řádem, statutem úseků (odborů) a popisem práce na jednotlivých služebních pozicích.
- **princip systémového přístupu,** tento princip vyjadřuje požadavek chápání a praktického výkonu všech opatření k ochraně majetku a dalších oprávněných zájmů společnosti, ne jako výčet vzájemně izolovaných úkonů, ale jako vzájemně se doplňující a podporující soustavu jednotného úsilí. Vyjadřuje požadavek na funkční součinnost osob a úseků, stanovení a respektování hierarchie důležitosti jednotlivých opatření a hierarchii pravomocí rozhodovat o činnostech majících různý bezpečnostní význam. O činnostech, majících zvláštní bezpečnostní význam může rozhodovat jen striktně určený, omezený okruh osob.
- **princip konkrétní osobní odpovědnosti**, tento princip vyjadřuje skutečnost, že každý zaměstnanec má v JBS svoje místo. V rámci toho jsou mu stanoveny konkrétní povinnosti, za jejichž plnění osobně odpovídá, včetně oznamovací povinnosti.
- **princip permanentní kontroly**, tento princip vyjadřuje skutečnost, že JBS v sobě zahrnuje systém permanentní kontroly a prověřování celého systému i jednotlivých osob a jejich činností.
- **princip systematického hodnocení,** účinnosti JBS i osobního podílu každého zaměstnance na jeho fungování je předmětem pravidelného hodnocení. Závěry hodnocení slouží k bezpečnostní a personální práci a jsou jedním z nástrojů zdokonalování JBS.
- **princip přiměřené profesionality**, tento princip vyjadřuje skutečnost, že některé činnosti v rámci JBS jsou svěřovány na smluvním základu profesionálním

dodavatelům specializovaných bezpečnostních služeb a na některé bezpečnostní činnosti jsou systematicky cvičeni a zaškolováni zaměstnanci organizace.

- **princip flexibility**, tento princip vyjadřuje skutečnost, že JBS předpokládá pružnou reakci na změnu bezpečnostní situace, ať celkovou nebo na jednotlivých úsecích (pracovištích).
- **princip práva**, tento princip vyjadřuje skutečnost, že JBS je založen na takových normách a postupech, které respektují a využívají legislativního rámce v ČR.

2. CÍLE PRÁCE A HYPOTÉZY

2.1. Cíle práce

a) Definování bezpečnostních hrozeb s posouzením existujících bezpečnostních opatřeních ve zdravotnických zařízeních.

b) Nastínění a následné stanovení požadované úrovně minimální bezpečnosti v souvislosti s reflexí bezpečnostních potřeb ve vědomí a praxi managementu a zaměstnanců zdravotnických zařízení.

2.2. Hypotéza

Stanovila jsem si hypotézu ve znění „Spolupráce a postupy vrcholového managementu a všech pověřených zaměstnanců v rámci jednotné metodiky řízení komplexního bezpečnostního prvku je dostatečně přehledná“.

3. METODIKA

Tato bakalářská práce je rozdělena do třech částí. V teoretické části je nejdříve rozebrán bezpečnostní systém ČR s jeho základními prvky, povinnostmi, funkcemi, které svojí propojeností vytvářejí funkční vztahy pro rychlou reakci při nestandardních až kritických situacích.

Dále je objasněn trend bezpečnostního prostředí ČR v rámci pozice evropských států a mezinárodních organizací s největšími hrozbami a riziky vyplývající pro ČR s následnou aplikací na zdravotnická zařízení s rozebráním základních prvků bezpečnostního systému jako celku.

V rámci části základních zákonných norem bude provedena analýza související se základními prvky bezpečnostního systému vyplývající pro zdravotnická zařízení.

V praktické části je věnována pozornost analýze jednotlivým elektronickým systémům, jejich použití ve specifických podmínkách zdravotnických zařízeních, přednosti jejich použití, související organizační opatření, naplnění zákonných podmínek používání systémů souvisejících se zpracováním osobních údajů s koncovým návrhem bezpečného pracoviště ve zdravotnickém zařízení a to v grafické podobě půdorysu Kliniky anesteziologie a resuscitace Institutu Klinické a Experimentální Medicíny v Praze.

4. VÝSLEDKY

V této kapitole se budu zabývat dokumenty, které jsou nezbytné při zpracování komplexní metodiky. Při shromažďování dat jsem zjistila že nejen v mém ale i v jiných zdravotnických zařízeních není jednotná metodika v rámci bezpečnosti. Kapitolu jsem rozdělila na dvě části. V první části se budu zabývat zákonnými normami v bezpečnostním systému zdravotnického zařízení s aplikací do vnitřního normativu organizace. Druhá část obsahuje bezpečnostní systémy, které je možno použít ve zdravotnických zařízeních. Doplňkem této kapitoly je aplikace bezpečnostních systémů s jednotlivými prvky na Kliniku anestezie a resuscitace IKEM.

4.1. ZÁKONNÁ NORMA V BEZPEČNOSTNÍM SYSTÉMU ZDRAVOTNICKÉHO ZAŘÍZENÍ – APLIKACE DO VNITŘNÍHO NORMATIVU ORGANIZACE

4.1.1 Ústava České republiky – ústavní zákon č.1/1993 Sb., v platném znění[7]

Ústava ČR je základní právní normou právního systému ČR. Byla přijata jako ústavní zákon Českou národní radou 16.12.1992 a publikována v české Sbírce zákonů pod č.1/1993 Sb. Ústava ČR je psanou ústavou, je také ústavou původní a dohodnutou. Přestože v roce 1992 existovala snaha přijmout ústavní listinu z roku 1920, čímž bychom hovořili o přenesené ústavě, nakonec tento pokus nebyl úspěšný a Ústava ČR, ač je tou prvorepublikovou silně inspirována, je ústavou původní. Ústava ČR byla výsledkem politického kompromisu završeného na půdě České národní rady 16. prosince 1992.

Ústava ČR je tvořena preambulí a 8 hlavami tvořenými 113 paragrafy, zahrnujícími základní ustanovení, moc zákonodárnou, moc výkonnou, moc soudní, Nejvyšší kontrolní úřad, Českou národní banku, územní samosprávu a přechodná a závěrečná ustanovení. Do konce roku 2011 byla Ústava ČR šestkrát novelizována.

4.1.2 Ústavní zákon č.23/1991 Sb., Listina základních práv a svobod, v platném znění[8]

Listina základních práv a svobod je součástí ústavního pořádku ČR. Listina je prvním uceleným ústavním dokumentem, který zakotvil tradiční demokratická práva a svobody. Listina je pramenem ústavního práva a je srovnatelná z hlediska právní síly s ústavními zákony, ačkoliv není jako ústavní zákon v současnosti formálně označena.

Základní práva a svobody obsažené v listině v zásadě vyjadřují vztah mezi státem a občanem.

Listina má 44 článků členěných do šesti hlav. Hlava první garantuje některá práva, hlava druhá obsahuje katalog základních lidských práv a svobod, hlava třetí upravuje práva národnostních menšin, hlava čtvrtá hospodářská, sociální a kulturní práva, hlava pátá se zabývá právem na soudní a jinou právní ochranu, hlava šestá pak upravuje společná ustanovení.

4.1.3 Zákon č.110/1998 Sb., o bezpečnosti České republiky, v platném znění[9]

Zákon je součástí ústavního pořádku ČR. Definuje základní povinnost státu , zajištění svrchovanosti a územní celistvosti České republiky, ochranu jejích demokratických základů a ochranu životů, zdraví a majetkových hodnot. Zákon má třináct článků členěných do základního ustanovení, nouzového stavu, stavu ohrožení státu, zkráceném jednání o návrzích zákonů, bezpečnostní rady státu, prodloužené volební období, společné a závěrečné ustanovení.

4.1.4 Zákon č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, v platném znění[10]

Tento zákon upravuje způsoby a podmínky hospodaření s majetkem České republiky (dále jen "stát"), vystupování státu v právních vztazích, jakož i postavení, zřizování a zánik organizačních složek státu. V § 14 jsou stanoveny základní práva a povinnosti při hospodaření s majetkem, v odstavci 3 je definována přímá povinnost

organizační složky státu k ochraně majetku – „chrání jej před poškozením, zničením, ztrátou, odcizením nebo zneužitím“. V rámci vnitřního normativu organizace v návaznosti na zákon o majetku ČR jsou zpracovávány směrem k majetku vnitřní předpisy (základní dokumenty, dočasné příkazy, směrnice, metodické pokyny). Jedná se především o tyto vnitřní předpisy:

- ❖pravidla hospodaření s majetkem,
- ❖provádění inventarizace majetku,
- ❖oceňování hmotného majetku pro účely vyčíslení škody,
- ❖nakládání s nepotřebným a neupotřebitelným majetkem,
- ❖stanovení norem ztrát k ochraně majetku,
- ❖k ochraně majetku, klíčový režim apod.

4.1.5 Zákon č.20/1966 Sb., o péči o zdraví lidu, v platném znění[11]

V průběhu zpracovávání bakalářské práce byl tento zákon zrušen a nahrazen zákonem č.372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) s účinností od 1.4.2012.

Tento zákon upravuje zdravotní služby a podmínky jejich poskytování a s tím spojený výkon státní správy, druhy a formy zdravotní péče, práva a povinnosti pacientů a osob pacientům blízkých, poskytovatelů zdravotních služeb, zdravotnických pracovníků, jiných odborných pracovníků a dalších osob v souvislosti s poskytováním zdravotních služeb, podmínky hodnocení kvality a bezpečí zdravotních služeb, další činnosti související s poskytováním zdravotních služeb a zapracovává příslušné předpisy Evropské unie.

Základní změny ve zdravotnickém systému podle nového zákona o zdravotních službách směřují k posílení práv pacienta z hlediska rovnocennosti v postavení s lékařem, posílení práv dětí, posílení práv lékaře, zdravotnického zařízení apod.

4.1.6 Zákon č.106/1999 Sb., o svobodném přístupu k informacím, v platném znění[12]

Tento zákon upravuje pravidla pro poskytování informací a dále upravuje podmínky práva svobodného přístupu k těmto informacím. Naplnění zákona z hlediska organizace vidím ve dvou rovinách:

- ❖podávání informací na základě žádosti,
- ❖povinně zveřejňované informace.

Podávání informací na základě žádostí - žádost o poskytnutí informace lze podat u příslušné organizace ústně nebo písemně, a to i prostřednictvím telekomunikačních zařízení.

Ústně, tj. i telefonicky podané žádosti o poskytnutí informace, se vyřizují neformálním způsobem a nejsou evidovány. Nevyhoví-li příslušná organizace ústní žádosti o poskytnutí informace, nevydává o tom rozhodnutí. Není-li žadateli na ústně podanou žádost o informace poskytnuta odpověď, anebo nepovažuje-li žadatel poskytnutou informaci za dostačující, je třeba podat žádost písemně.

U písemné žádosti datem podání se rozumí den doručení žádosti povinnému subjektu (§ 14 odst. 1 zákona č. 106/1999 Sb.). Na žádost učiněnou písemně poskytne příslušná organizace informaci do 15 dnů od přijetí podání. Lhůta může být ze závažných důvodů prodloužena, nejvíce však o 10 dní.

Ve lhůtě do sedmi dnů od přijetí žádosti může příslušná organizace vyzvat tazatele k upřesnění žádosti. Učiní tak v případě, že je žádost nesrozumitelná, není z ní jasné, jaká informace je požadována, či je formulována příliš obecně. Není-li taková žádost ve lhůtě 30 dnů tazatelem upřesněna, příslušná organizace rozhodnutím žádost odmítne.

Nevztahují-li se informace, které tazatel požaduje, k působnosti příslušné organizace, ta žádost odloží. O této skutečnosti informuje tazatele do sedmi dnů.

V případě, že příslušná organizace žádosti o informaci nevyhoví, vydá správní rozhodnutí o odmítnutí žádosti. Lhůta pro rozhodnutí o odmítnutí žádosti je shodná se lhůtou k jejímu vyřízení.

Povinně zveřejňované informace - dle § 5 odst. 1 a 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve struktuře předepsané prováděcí vyhláškou č. 442/2006 Sb., kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup, v platném znění:

- ❖název organizace,
- ❖důvod a způsob založení organizace,
- ❖organizační struktura,
- ❖kontaktní spojení,
- ❖identifikační číslo, DIČ,
- ❖seznam hlavních dokumentů,
- ❖žádosti o informace,
- ❖formuláře,
- ❖nejdůležitější používané předpisy,
- ❖licenční smlouvy,
- ❖výroční zprávy.

4.1.7 Zákon č.101/2000 Sb., ochrana osobních údajů, v platném znění[13]

Tento zákon v souladu s právem Evropských společenství, mezinárodními smlouvami, kterými je ČR vázána, a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.

Jedná se o osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby. Tento zákon se vztahuje na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky. Z hlediska dodržení právní normy definujeme dva pojmy (osobní údaj a zpracování osobních údajů).

Osobním údajem je jakákoliv informace, týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt

údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

V rámci příslušné organizace, která používá bezpečnostní prvky v rámci ochrany osob, majetku, informací (CCTV, EKV apod.), tato jednoznačně postupuje v souladu s výše citovaným zákonem.

4.1.8 Zákon č.133/2000 Sb., o evidenci obyvatel a rodných číslech, v platném znění[14]

Tento zákon stanovuje pravidla pro výkon státní správy v oblasti evidence obyvatel. V evidenci obyvatel se vedou údaje o:

- ❖státních občanech ČR,
- ❖osobách, které pozbyly státní občanství ČR,
- ❖cizincích, kteří jsou matkou, otcem, popřípadě jiným zákonným zástupcem, manželem, registrovaným partnerem nebo dítětem občana.
- ❖Rodné číslo je oprávněna užívat nebo rozhodovat o jeho využívání v mezích stanovených zákonem výlučně fyzická osoba, které bylo rodné číslo přiděleno, nebo její zákonný zástupce, jinak lze rodné číslo využívat jen v případech stanovených v § 13c tohoto zákona.

Rodná čísla lze využívat jen:

- ❖jde-li o činnost ministerstev, jiných správních úřadů, orgánů pověřených výkonem státní správy, soudů, vyplývající z jejich zákonem stanovené působnosti nebo notářů pro potřebu vedení Centrální evidence závětí,

❖stanoví-li tak zvláštní zákon nebo

❖se souhlasem nositele rodného čísla nebo jeho zákonného zástupce.

Pro využívání rodných čísel se rodným číslem rozumí i jakákoliv kombinace čísel vyjadřující den, měsíc, rok narození a třímístnou nebo čtyřmístnou koncovku rodného čísla, z níž je možné dovodit identifikaci fyzické osoby.

4.1.9 Zákon č. 412/2005 Sb., ochrana utajovaných informací, v platném znění[15]

Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy. V rámci příslušné organizace jde ve smyslu zákona, trvale přehodnocovat seznamy míst a především funkcí, u kterých je nezbytné mít přístup k utajovaným informacím (všech stupňů utajení včetně základního stupně „Vyhrazené“).

4.1.10 Zákon č.262/2006 Sb., zákoník práce, v platném znění[16]

Tento zákon upravuje především právní vztahy vznikající při výkonu závislé práce mezi zaměstnanci a zaměstnavateli, tyto vztahy jsou vztahy pracovněprávními, upravuje rovněž právní vztahy kolektivní povahy. Z hlediska bezpečnosti osob a majetku ze strany zaměstnavatele a zaměstnance je striktní dodržování části jedenácté, hlavy 1 zákoníku práce, a to předcházení škodám (§ 248 a § 249).

V rámci příslušné organizace, která používá bezpečnostní prvky v rámci ochrany osob, majetku, informací (CCTV, EKV apod.), je striktní dodržování části třinácté, hlavy 8 zákoníku práce, a to ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance (§ 316) - zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu

jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.

Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, § 316, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.

4.1.10 Zákon č.499/2004 Sb., o archivnictví a spisové službě, v platném znění[17]

Tento zákon především upravuje výběr, evidenci a kategorizaci archiválií, jejich ochranu, práva a povinnosti vlastníků archiválií, práva a povinnosti držitelů a správců archiválií, využívání archiválií, zpracování osobních údajů pro účely archivnictví, soustavu archivů, práva a povinnosti zřizovatelů archivů a spisovou službu. V rámci příslušné organizace jde ve smyslu zákona o zpracování vnitřních dokumentů, jedná se především o provozní řád centrální spisovny, spisový řád a skartační řád s jasnými pravidly nakládání se spisovým materiálem.

4.1.11 Prováděcí vyhláška č.645/2004 Sb., o archivní službě[18]

Touto vyhláškou se provádějí některá ustanovení zákona o archivnictví a spisové službě, především definuje podrobnosti skartačního řízení, opatření dokumentů digitální podoby určené ke skartaci, způsoby vedení základní, druhotné a ústřední evidence, specifikuje kategorizaci archiválií a pořizování výpisů, opisů nebo kopií archiválií.

4.1.12 Prováděcí vyhláška č.646/2004 Sb., o spisové službě[19]

V průběhu zpracovávání bakalářské práce byla tato vyhláška zrušena a nahrazena vyhláškou č.191/2009 Sb., o podrobnostech výkonu spisové služby. Tato vyhláška stanoví podrobnosti výkonu spisové služby, které se vztahují k původcům dokumentů,

jimiž se pro účely vyhlášky rozumí určení původci zřízeni nebo založeni územními samosprávnými celky v rozsahu, v jakém vykonávají spisovou službu podle zákona.

4.1.13 Prováděcí vyhláška č. 496/2004 Sb., o elektronických podatelnách[20]

Tato vyhláška stanoví postupy orgánů veřejné moci uplatňované při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny a strukturu údajů kvalifikovaného certifikátu, na základě kterých je možné podepisující osobu při přijímání datových zpráv prostřednictvím elektronické podatelny jednoznačně identifikovat.

4.1.14 Vyhláška č.385/2006 Sb., o zdravotnické dokumentaci, v platném znění[11]

V průběhu zpracovávání bakalářské práce byla tato vyhláška zrušena a nahrazena částí šestou „zdravotnická dokumentace a národní zdravotnický informační systém“ (§ 52 - § 78) zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) s účinností od 1.4.2012. Tato část ukládá poskytovateli povinnost vést a uchovávat zdravotnickou dokumentaci a nakládat s ní podle tohoto zákona a jiných právních předpisů. Zdravotnická dokumentace je souborem informací vztahující se k pacientovi, o němž je vedena.

4.1.15 Směrnice zdravotnického zařízení

V rámci zpracování směrnic a vnitřních předpisů ve zdravotnických zařízení musíme především stanovit závazná pravidla pro jejich vypracování, schvalování a implementaci. Tento proces se řídí navrhovaným algoritmem:

- ❖určení správce systému vnitřních předpisů,
- ❖iniciace tématu formou záměru – schválení tématu poradou vedení zdravotnického zařízení,

- ❖určení kategorie předpisu (směrnice, základní dokument, dočasný příkaz, metodický pokyn), určení garanta a způsob oponentury,
- ❖vlastní vypracování předpisu,
- ❖odborná a právní oponentura,
- ❖schválení ředitelem zdravotnického zařízení,
- ❖anotace,
- ❖zveřejnění v rámci vnitřní sítě elektronické databáze (intranet).

Vlastní struktura směrnic a vnitřních předpisů – přední strana:

- ❖kategorie předpisu, značení předpisu, název a jeho číslo,
- ❖verze,
- ❖platnost a účinnost,
- ❖údaj o tom, jaký stávající předpis se ruší nově vydávaným předpisem,
- ❖v určené části titulní strany uvést jména, příjmení a funkce odborného garanta, nadřízeného odborného garanta, správce systému, právníka a přezkoumávajícího předpis a schvalovatele předpisu, jejich podpisy a datum podpisu,
- ❖obsah vnitřního předpisu.

Směrnice musí mít stanoveny následující kapitoly:

- ❖účel – uvede se stručně účel, kterému směrnice slouží,
- ❖popis činností – rozhodující část směrnice, popisující pravidla, postupy a povinnosti pro zabezpečení dané problematiky,
- ❖rozsah platnosti – uvede se rozsah činností, které jsou směrnicí řízeny, případně funkce, které je zabezpečují a okruh zaměstnanců, kteří musí být se směrnicí seznámeni, důkazem o seznámení zaměstnance se směrnicí je podpis v „Záznamu o proškolení“,
- ❖odpovědnosti – uvedou se odpovědnosti za nejdůležitější činnosti nebo jejich soubory, které jsou pro postupy uvedené v předpise rozhodující,
- ❖pojmy, zkratky – uvedou se vysvětlivky pro jednotlivé vrstvy, případně seznam použitých zkratek,

- ❖právní předpisy a související dokumentace – uvede se přehled právních norem a vnitřních předpisů, které souvisí s danou směrnicí,
- ❖změnové řízení – uvádí se funkce zaměstnance, který zajišťuje změny dané směrnice, v popisu změn se uvede číslo a název kapitoly nebo kapitol, u nichž došlo ke změně, číslo revize a datum počátku účinnosti dané revize,
- ❖rozdělovník – pracoviště, pro která je směrnice určena a je pro ně závazná,
- ❖přílohy – zde jsou uvedeny jednotlivé související přílohy k vnitřnímu předpisu, případně vzory příslušných tiskopisů, na nějž je odkaz v textu nebo jiné zpřesňující informace, povinná příloha každého předpisu je „Záznam o proškolení“.

V rámci uplatňování principů bezpečnostního systému zdravotnického zařízení je zřejmé zpracování těchto základních směrnic a vnitřních předpisů:

- ❖Organizační řád,
- ❖Provozní řád,
- ❖Pracovní řád,
- ❖Pravidla pro komunikaci se zástupci médií,
- ❖K ochraně majetku zdravotnického zařízení s pravidly klíčového režimu,
- ❖Hlášení o mimořádných událostech (nežádoucích účincích),
- ❖Vjezdový systém,
- ❖Pravidla telefonního provozu,
- ❖Pravidla potrubní pošty,
- ❖Dopravně provozní řád,
- ❖Inventarizace majetku,
- ❖Používání osobních identifikačních karet,
- ❖Přístupová práva ke zdravotnické dokumentaci v elektronické databázi,
- ❖Používání elektronické pošty pro služební účely,
- ❖Vedení zdravotnické dokumentace,
- ❖Příjem, překlad, propuštění pacientů,
- ❖Zacházení s léčivy,
- ❖Provozní řád centrální spisovny,

❖Spisový řád,

❖Skartační řád,

❖Požární ochrana pracovišť a organizační zabezpečení požární ochrany,

❖Aplikace náhradních zdrojů elektrické energie,

❖Traumatologický plán,

❖Pandemický plán,

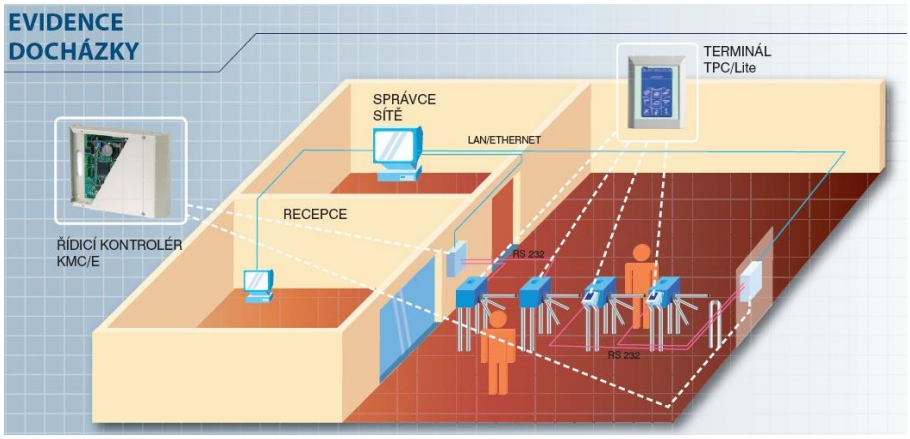
❖Evakuační plán,

❖Povodňový plán.

4.2. PRAKTICKÁ ČÁST

4.2.1 Docházkové systémy[28]

Docházkové systémy jsou v podstatě velice jednoduché. Zavedení docházkového systému umožní nahradit tzv. bývalé „píchací hodiny“, docházkové sešity a knihy docházky. Slouží k automatickému snímání a evidenci příchodů, odchodů zaměstnanců, přerušení pracovní doby s následným informačním výstupem pro další využití, viz. obrázek č.3.



Obrázek č. 3

Zdroj: http://www.aktion.cz/cs/sluzby-a-reseni/dochazkovy-system.html příklad aplikace JPEG (11.4.2012)

Umožní vedoucím pracovníkům okamžitý přehled o svých podřízených zaměstnancích. Docházkový systém jednoznačně identifikuje zaměstnance pomocí karty, čipu, popřípadě biometrických údajů (otisk prstů, oční duhovka apod.) a jejich vzájemné kombinaci. Základní viditelnou součástí docházkového systému jsou docházkové terminály, viz obrázek č. 4.

Obrázek č. 4

Zdroj: http://www.alveno.cz/cz/146/dsi-200-otisk-cip/ kolonka fotogalerie (11.4.2012)

Docházkový systém se obvykle skládá z jednoho terminálu , který je obvykle umístěn u vchodu do objektu zdravotnického zařízení. Záměrně říkám obvykle, protože terminálů i vchodů může být více. Docházkový terminál zaznamenává jednotlivé průchody a vlastní uživatelský software je zpracuje a upraví. Data z terminálu jsou přenášena prostřednictvím speciálních metalických vedení nebo počítačovými sítěmi (LAN i WAN) do tzv. centrálního úložiště, které řídí síť terminálů, data lze mimo jiné importovat do mzdového programu.

K systému je dodáván záložní zdroj, který umožňuje zachovat plnou funkci docházkového systému po dobu minimálně 24 hodin. Po vybití záložního zdroje se data obsažená v terminálu neztratí, pouze není možné s terminálem komunikovat a používat ho do té doby, než je dodávka elektrické energie obnovena.

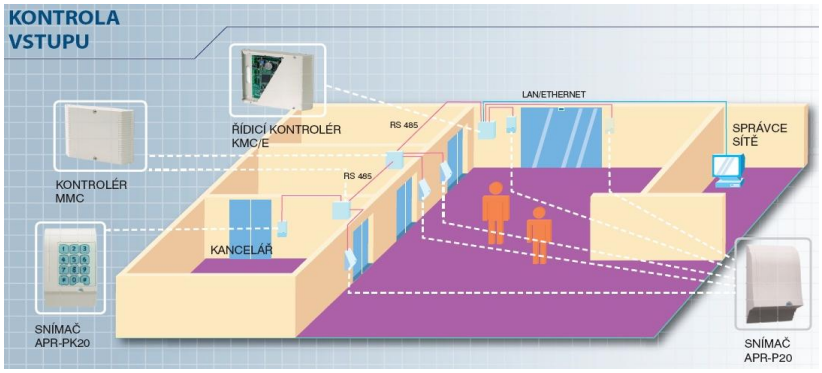
Z definice docházkového systému je zřejmé, že v rámci použití ve zdravotnickém zařízení potřebujeme jednoduché, levné a především efektivní zařízení. K identifikaci

zaměstnance navrhuji použití stávající osobní identifikační karty jako samostatného prvku (je zde ale vyšší riziko zneužití osobní identifikační karty) a možné kombinace s biometrickým údajem, především s oční duhovkou (v tomto případě se z hlediska uložených dat snižuje kapacita počtu zaměstnanců). Záměrně zde neuvádím biometrický údaj otisk prstů z důvodu hygienických podmínek a specifikace jednotlivých pracovišť. Použití docházkového systému v rámci zdravotnických zařízení spíše doporučuji v rámci objektů s provozní či technologickou částí zabezpečení chodu zdravotnických zařízení (prádelna, centrální sterilizace, stravovna, dopravní odbor apod.), v případě klinických pracovišť, která jsou detašována ve více objektech je použití všech terminálů s pokrytím těchto pracovišť neefektivní, neekonomické a musí se ošetřit tzv. organizačním opatřením.

Centrální úložiště zřídit v rámci odboru bezpečnosti a krizového řízení nebo odboru výpočetních systémů s pověřeným počtem zaměstnanců s definicí oprávnění vstupu a provádění jednotlivých operací.

4.2.2 Přístupové systémy[29]

Přístupový systém, viz. obrázek č.5 na rozdíl od docházkového systému, nemá za úkol pouze monitorovat pracovní dobu zaměstnance, je určen pro tzv. elektronickou kontrolu vstupu do objektu, či definovaného prostoru. Jeho hlavní funkcí je zabezpečit přístup správných osob na správná, předem definovaná místa. U přístupových systémů je třeba jasně definovat, k čemu je zdravotnické zařízení potřebuje a co od nich vyžaduje.



Obrázek č. 5

Zdroj: http://www.aktion.cz/cs/kontrola-pristupu.html příklad aplikace JPEG (11.4.2012)

Přístupový systém je sestaven z řídící jednotky, terminálu (čtečky), viz. obrázek č.6 a č.7, propouštěcího elektromechanického zámku a identifikačního čipu nebo karty. Přiložením čipu nebo karty k terminálu jsou informace o médiu přeneseny do řídící jednotky. V řídící jednotce dojde k porovnání - verifikaci - informací o čipu nebo karty , a jsou-li informace shodné s programovým nastavením, dojde k otevření elektronického zámku.

Obrázek č. 6 **Obrázek č.7**

Zdroj: http://www.technopark.cz/pristupove-systemy detaily produktu (11.4.2012)

Data z terminálu jsou přenášena prostřednictvím speciálních metalických vedení nebo počítačovými sítěmi (LAN i WAN) do tzv. centrálního úložiště, které řídí síť terminálů. K identifikaci zaměstnance navrhuji použití stávající osobní identifikační karty jako samostatného prvku (je zde ale vyšší riziko zneužití osobní identifikační karty) a možné kombinace s biometrickým údajem, především s oční duhovkou (v

tomto případě se z hlediska uložených dat snižuje kapacita počtu zaměstnanců). Záměrně zde neuvádím biometrický údaj otisk prstů z důvodu hygienických podmínek a specifikace jednotlivých pracovišť.

K systému je dodáván záložní zdroj, který umožňuje zachovat plnou funkci přístupového systému po dobu minimálně 24 hodin. Po vybití záložního zdroje se data obsažená v terminálu neztratí, pouze není možné s terminálem komunikovat a používat ho do té doby, než je dodávka elektrické energie obnovena.

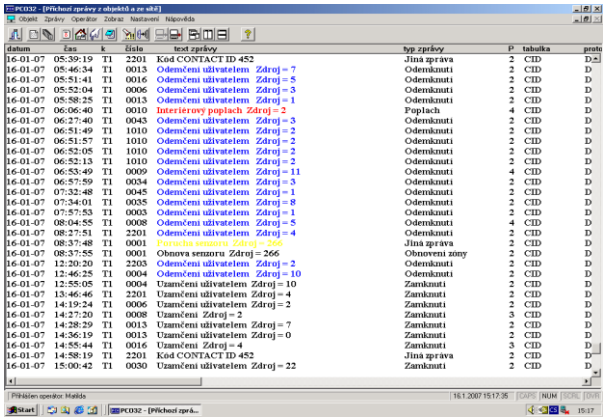
Použití přístupového systému v rámci zdravotnických zařízení spíše doporučuji v rámci tzv. režimových pracovišť jako např. operačních sálů, pracovišť JIP a ARO, lůžkových částí jednotlivých klinik s řízeným pohybem osob, technologických místností s uzávěry slaboproudů, telefonních linek, serverů apod., prostorů s omezeným počtem osob – kolárna. Centrální úložiště zřídit v rámci odboru bezpečnosti a krizového řízení nebo odboru výpočetních systémů s pověřeným počtem zaměstnanců s definicí oprávnění vstupu a provádění jednotlivých operací.

4.2.3 Elektronické zabezpečovací systémy

Elektronický zabezpečovací systém slouží především k ochraně objektu a následné včasné signalizaci nežádoucího vniknutí nebo pokusu o vniknutí do předem určeného střeženého prostoru (objektu), k ochraně pracovníků proti verbálnímu či fyzickému napadení nebo nežádoucí činnosti narušitele. Samočinně nebo prostřednictvím lidského činitele urychluje předání této informace určené osobě nebo osobám. Tento systém chrání objekt podle požadavků proti:

- ❖neoprávněnému vniknutí cizí osoby,
- ❖vloupání,
- ❖ohrožení osob,
- ❖úniku plynu,
- ❖vzniku požáru,
- ❖zatopení vodou,
- ❖a mnoho dalších dle rozsahu systému EZS.

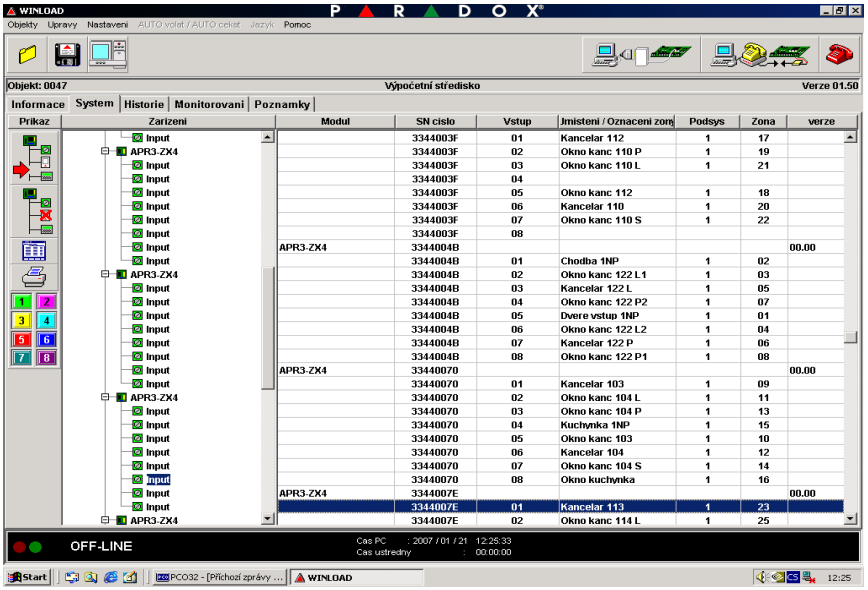
Jádrem EZS je zabezpečovací ústředna, která vyhodnocuje stav detektorů a je uživatelem ovládána nejčastěji pomocí klávesnice. Uživatel pomocí kódu přes klávesnici ústřednu zapíná nebo ji ze střežení vypne a může se po objektu volně pohybovat. Pomocí detektorů jsou hlídány všechny prostory, u kterých je nežádoucí, aby do nich pachatel vniknul nebo se v nich pohyboval. Detektorem je myšleno zařízení, které předá zabezpečovací ústředně signál v případě, že vyhodnotí stav, který je považován za narušení. Je potřeba si uvědomit, že EZS nezabrání narušení objektu, ale pouze upozorní na skutečnost, že k narušení došlo. Na tento stav může systém upozornit (lokálně) akustickou a optickou signalizací nebo (dálkově) předat zprávu definovaným osobám či ostraze. Akustická a optická signalizace je aktivována ihned po narušení, na pachatele působí psychologicky a nezaručuje ochranu objektu. Zprávu o narušení fyzické ostraze lze předat pomocí telefonních linek přes modem nebo bezdrátovým přenosem na tzv. pult centrální ochrany, viz. obrázek č.8 a č.9, obsluha vidí jednotlivé průběhy narušených zón u monitorovaného objektu.



datum	čas	k	číslo	text zprávy	typ zprávy	P	tabulka	prefix
16-01-07	05:39:19	T1	2201	Kod CONTACT ID 452	Jina zprava	2	CID	D
16-01-07	05:46:34	T1	0013	Odemčení uživatelem Zdroj = 7	Odemknuti	2	CID	D
16-01-07	05:51:41	T1	0016	Odemčení uživatelem Zdroj = 5	Odemknuti	2	CID	D
16-01-07	05:52:04	T1	0006	Odemčení uživatelem Zdroj = 3	Odemknuti	2	CID	D
16-01-07	05:58:25	T1	0013	Odemčení uživatelem Zdroj = 1	Odemknuti	2	CID	D
16-01-07	06:06:40	T1	0010	Interierovy poplach Zdroj = 2	Poplach	4	CID	D
16-01-07	06:27:40	T1	0043	Odemčení uživatelem Zdroj = 3	Odemknuti	2	CID	D
16-01-07	06:51:49	T1	1010	Odemčení uživatelem Zdroj = 2	Odemknuti	2	CID	D
16-01-07	06:51:57	T1	1010	Odemčení uživatelem Zdroj = 2	Odemknuti	2	CID	D
16-01-07	06:52:05	T1	1010	Odemčení uživatelem Zdroj = 2	Odemknuti	2	CID	D
16-01-07	06:52:13	T1	1010	Odemčení uživatelem Zdroj = 2	Odemknuti	2	CID	D
16-01-07	06:53:49	T1	0009	Odemčení uživatelem Zdroj = 11	Odemknuti	4	CID	D
16-01-07	06:57:59	T1	0034	Odemčení uživatelem Zdroj = 3	Odemknuti	2	CID	D
16-01-07	07:32:48	T1	0045	Odemčení uživatelem Zdroj = 1	Odemknuti	2	CID	D
16-01-07	07:34:01	T1	0035	Odemčení uživatelem Zdroj = 8	Odemknuti	2	CID	D
16-01-07	07:57:53	T1	0003	Odemčení uživatelem Zdroj = 1	Odemknuti	2	CID	D
16-01-07	08:04:55	T1	0008	Odemčení uživatelem Zdroj = 5	Odemknuti	4	CID	D
16-01-07	08:27:51	T1	2201	Odemčení uživatelem Zdroj = 4	Odemknuti	2	CID	D
16-01-07	08:37:48	T1	0001	Testovaci zprava Zdroj = 266	Jina zprava	2	CID	D
16-01-07	08:37:55	T1	0001	Obnova senzoru Zdroj = 266	Obnoveni zony	2	CID	D
16-01-07	12:20:20	T1	2203	Odemčení uživatelem Zdroj = 2	Odemknuti	2	CID	D
16-01-07	12:46:25	T1	0004	Odemčení uživatelem Zdroj = 10	Odemknuti	2	CID	D
16-01-07	12:55:05	T1	0004	Uzamčení uživatelem Zdroj = 10	Zamknuti	2	CID	D
16-01-07	13:46:46	T1	2201	Uzamčení uživatelem Zdroj = 4	Zamknuti	2	CID	D
16-01-07	14:19:24	T1	0006	Uzamčení uživatelem Zdroj = 2	Zamknuti	2	CID	D
16-01-07	14:27:20	T1	0008	Uzamčení Zdroj = 2	Zamknuti	3	CID	D
16-01-07	14:28:29	T1	0013	Uzamčení uživatelem Zdroj = 7	Zamknuti	2	CID	D
16-01-07	14:36:19	T1	0013	Uzamčení uživatelem Zdroj = 0	Zamknuti	2	CID	D
16-01-07	14:55:44	T1	0016	Uzamčení Zdroj = 4	Zamknuti	3	CID	D
16-01-07	14:58:19	T1	2201	Kod CONTACT ID 452	Jina zprava	2	CID	D
16-01-07	15:00:42	T1	0030	Uzamčení uživatelem Zdroj = 22	Zamknuti	2	CID	D

Obrázek č. 8

Zdroj: Pult centrální ochrany EZS zdravotnického zařízení PCO 32 Matilda, průběhy zón objektů



Obrázek č. 9

Zdroj: Pult centrální ochrany zdravotnického zařízení PCO 32 Matilda, objekt č.0047, jednotlivé prvky.

Celý systém má být navržen tak, aby zároveň hlídal sám sebe. V případě, že je systém v režimu ostrahy, nesmí se osoba dostat ke klávesnici, aniž by nenarušila detektor, obsluha musí do určitého časového sledu zadat platný kód a systém vypnout, jinak je vyvolán poplach.

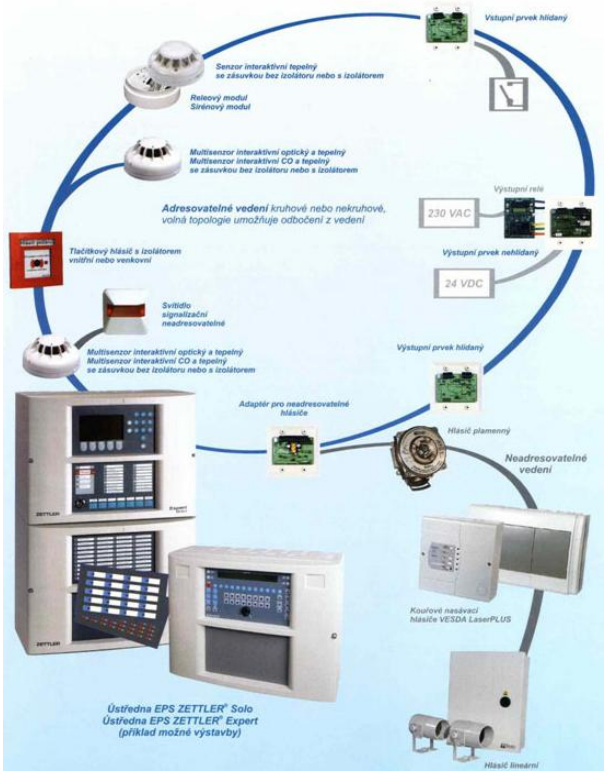
K systému je dodáván záložní zdroj, který umožňuje zachovat plnou funkci přístupového systému po dobu minimálně 24 hodin. Po vybití záložního zdroje se data obsažená v ústředně neztratí, pouze není možné s ústřednou komunikovat a používat ho do té doby, než je dodávka elektrické energie obnovena.

Použití EZS v rámci zdravotnických zařízení spíše doporučuji v objektech, kde není stálá přítomnost zaměstnanců mimo pracovní dobu, o sobotách, nedělích a svátcích (skladové haly, technické provozy apod.) a u tzv. režimových pracovišť s trvalou vysokou hodnotou materiálních či finančních hodnot (pokladny, lékárny, vyšetřovny apod.) s možností napojení na PCO PČR.

Centrální úložiště a správu nad systémem zřídit v rámci odboru bezpečnosti a krizového řízení s pověřeným počtem zaměstnanců s definicí oprávnění vstupu a provádění jednotlivých operací a zadávání osob s oprávněným vstupem do jednotlivých střežených prostorů.

4.2.4 Elektronické požární systémy [30], [31]

Elektrická požární signalizace EPS je slaboproudé zařízení, které je schopno včas detekovat vznik požáru a tím zajistit včasnou a úspěšnou evakuaci osob, zvířat a majetku, a také zajistit účinný a rychlý protipožární zásah. Nutnost instalace systému požární signalizace EPS je dána zejména legislativními předpisy z oblasti požární ochrany. EPS se skládá z automatických nebo lineárních hlásičů požáru sloužící k detekci požáru, tlačítkových hlásičů u únikových východů, ústředny EPS pro zpracování a vyhodnocení signálů z hlásičů, poplachovými sirénami, popřípadě vysílače pro přenos poplachové informace na hasičský záchranný sbor a zařízení pro návazná zařízení, která ústředna EPS ovládá, viz. obrázek č.10.



Obrázek č. 10

Zdroj: http://www.mselektro.cz/elektronicke-pozarni-systemy/ (11.4.2012)

Úkolem moderních systémů elektrické požární signalizace EPS není pouze včasná signalizace požáru. Podstatnou funkcí elektrické požární signalizace je také ovládání dalších návazných požárně - bezpečnostních zařízení (např. odvod tepla a kouře,

evakuační rozhlas, evakuační výtahy, požární klapky, nouzové osvětlení) a dalších určených zařízení (např. provozní vzduchotechnika, otvírání a zavírání dveří, výtahy, eskalátory, atd.) a také monitoring jejich stavu. Výše zmíněnými funkcemi se systém elektrické požární signalizace EPS stává jedním z nejdůležitějších prvků požárního zabezpečení moderních objektů. Na rozdíl od ostatních slaboproudých technických zařízení budov je však zákonnou povinností provozovatele mít na systém elektrické požární signalizace EPS zajištěný provozní servis a provádění pravidelných kontrol, funkčních zkoušek a revizí systému EPS. Jejich četnost a způsob provádění je dán požadavky legislativy (vyhlášky, normy, zákony), doporučeními v projektu a výrobcem konkrétního systému elektrické požární signalizace EPS.

Základní termíny pro provádění pravidelných kontrol provozuschopnosti elektrické požární signalizace dle vyhlášky č. 246/2001 Sb., jsou:

- 1x za rok - pravidelné jednoroční kontroly provozuschopnosti – revize EPS,
- 1x za měsíc funkční zkouška u ústředen a doplňujících zařízení,
- 1x za 6 měsíců funkční zkouška u samočinných hlásičů požáru a zařízení, které elektrická požární signalizace ovládá.

Požární ústředny zabezpečují kompletní funkce celého systému EPS. Jedná se zejména o napájení a vyhodnocování stavu požárních hlásičů, ovládání požární signalizace a aktivace ovládacích prvků návazných zařízení a v neposlední řadě též o kontrolu stavu a provozuschopnosti celého zařízení EPS nebo i ostatních připojených zařízení. Napájení každé požární ústředny musí být zálohováno proti výpadku napájecí sítě akumulátory. Každé zařízení elektrické požární signalizace musí být schopno provozu na náhradní zdroj po dobu minimálně 24 hod, z toho 15 minut ve stavu signalizace požáru.

Použití EPS v rámci zdravotnických zařízení vychází ze zákonných norem, nové ale i stavebně upravované objekty, které podléhají stavebnímu nebo kolaudačnímu řízení musí mít instalován systém EPS povinně. V ostatních objektech doporučuji umístění EPS tam, kde jsou lůžková zařízení, ambulance, vyšetřovny s velkým pohybem osob (ochrana života a zdraví), v technologických a provozních objektech, kde není stálá přítomnost zaměstnanců mimo pracovní dobu, o sobotách, nedělích a svátcích (skladové

haly, technické provozy apod.) a u tzv. režimových pracovišť s trvalou vysokou hodnotou materiálních hodnot a přítomností nebezpečných látek, které by mohly ohrozit běžný chod zdravotnického zařízení.

Centrální správu nad systémem zřídit v rámci stálého pohotovostního pracoviště provozního odboru, např. centrální velín s definicí oprávnění vstupu do systému a provádění jednotlivých operací .

4.2.5 Kamerové systémy CCTV

Kamerové systémy patří k nejvyššímu standardu zabezpečení objektu. Kamerové systémy - CCTV (Closed Circuit Television) - jsou velmi významným prostředkem pro monitorování a to nejen pro bezpečnostní účely, např. pro ověření poplachového stavu, ale také pro sledování různých výrobních či nevýrobních procesů. Tyto systémy jsou vhodné především jako podpora klasické EZS. Náklady na pořízení kvalitního kamerového systému jsou v porovnání s hodnotou zabezpečeného majetku a osob zanedbatelné.

Samotné bezpečnostní kamery dělíme podle snímání obrazu na barevné a černobílé, z pohledu zpracování obrazu na bezpečnostní kamery analogové a digitální (IP kamery), z pohledu monitorovaného prostoru na vnitřní a venkovní a z hlediska konstrukčního na bezpečnostní kamery standardní, kompaktní, dome kamery, otočné kamery, bezdrátové kamery, deskové a speciální skryté kamery.

Návrh bezpečnostního kamerového systému by měl vycházet ze zadání konkrétní aplikace CCTV a analýzy potřeb zdravotnického zařízení. V úvodní fázi realizace kamerového systému by mělo být jasné, jaký účel bude kamerový systém plnit, resp. jaký přínos bude mít kamerový systém pro uživatele a jakým způsobem bude obsluhován. Jednotlivá kamerová stanoviště jsou určována s ohledem na velikost a druh sledovaných prostor. Z hlediska umístění a instalace konkrétního typu bezpečnostní CCTV kamery je důležité, zda se jedná o sledování interiéru nebo o venkovní prostory, jak velké prostory bude CCTV kamera sledovat, jaké detaily mají být zobrazeny a jaké jsou ve snímaném prostoru světelné podmínky.

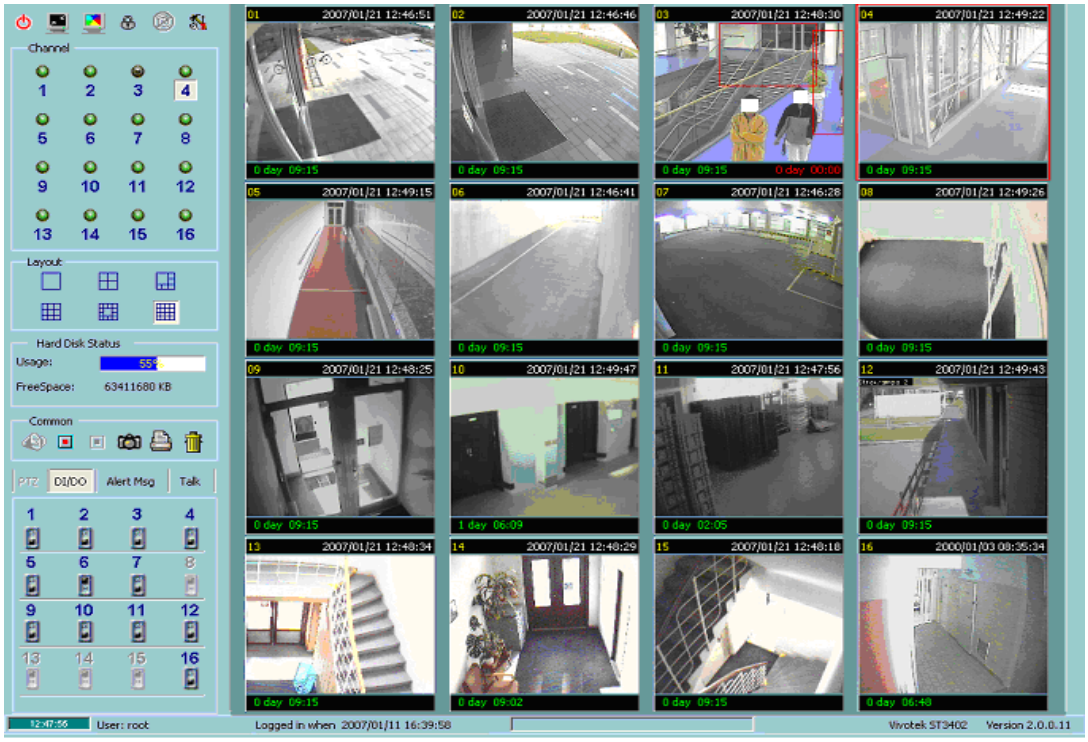
V běžném interiéru můžeme použít standardní kameru s držákem a objektivem bez potřeby povětrnostního krytí, protože předpokládáme stálé tepelné podmínky a minimální vzdušnou vlhkost, která neohrozí orosení objektivu. V tomto případě nemusí být kamera chráněna ani proti korozi a zvýšené prašnosti.

Ve venkovním prostředí musíme počítat se změnou okolní teploty, vysokou vlhkostí, prašností, průnikem dešťové vody, námrazami apod. Vzhledem k povaze venkovních prostor chráníme CCTV kamery instalací do venkovních krytů s odpovídajícím povětrnostním krytím, vybavené vytápěním nebo případně chlazením. Kompaktní venkovní CCTV kamery jsou zpravidla opatřeny nočním infra přisvětlením, vari-objektivem, držákem a rovněž jsou nabízeny v anti-vandal provedení. Proti vandalismu a případnému odcizení kamery se lze poměrně účinně chránit umístěním kamery tak, aby nebyla vandalům snadno dostupná nebo umístěním druhé kamery se vzájemným krytím.

Zorné pole kamery a zobrazování detailů v obraze - ve spolupráci s provozovatelem bezpečnostního kamerového systému je nutné stanovit, jaké konkrétní detaily mají být zobrazeny, tj. určit zorné pole kamery (resp. objektivu) s ohledem na vzdálenost kamery od snímané scény. Zorné pole reprezentuje snímaný úhel záběru kamery.

Důležitým parametrem pro návrh kamerového systému jsou i světelné podmínky. Zvláště u venkovních CCTV aplikací se světelné podmínky výrazně mění, v průběhu dne a noci, právě tak v různých ročních obdobích a za konkrétních povětrnostních podmínek (např. za slunného dne při zasněženém pozadí sledovaného prostoru, kdy sníh odráží převážnou část světla a mnohonásobně zvyšuje intenzitu světla snímané scény). Intenzita přirozeného denního světla se pohybuje řádově v hodnotách 10.000 až 70.000 luxů. Současné kamery disponují zcela běžně minimální citlivostí v úrovních desetin až setin luxů. Moderní kompaktní CCTV kamery nabízejí ve venkovním prostředí automatické spínání infračervených IR LED diod, které snímanou scénu nasvětlí. Maximální dosvit IR LED diod je vždy uváděn v technické specifikaci kamer.

Po stanovení počtu a typu konkrétních CCTV kamer je nutné specifikovat použití SW s počtem monitorovaných prostor, viz. obrázek č.11 a monitorovací pracoviště s ohledem na provoz bezpečnostního kamerového systému.



Obrázek č. 11

Zdroj: Pult centrální ochrany zdravotnického zařízení CCTV ST 3402 Vivotek, průběhy monitorovaných zón

Provoz kamerového systému může být tzv. bezobslužný (tj. pouze s požadavkem na záznam, bez ohledu na vyhodnocování aktuální situace), s částečnou obsluhou (např. pouze v pracovní době) nebo s nepřetržitou obsluhou vyhodnocující aktuální vzniklou situaci a přijímající odpovídající opatření. Umístění a vybavení monitorovacího pracoviště by také mělo odpovídat provozu kamerového systému, zvláště pokud je požadován režim s nepřetržitou obsluhou (směnný režim) a jedná se o velký počet kamer. Rozmístění, počet a velikost videomonitorů a ovládacích prvků kamerového systému by měl odpovídat počtu připojených kamer také s ohledem na počet bezpečnostních pracovníků vyčleněných ke sledování videosystému.

Kapacita a parametry záznamového zařízení (bezpečnostního digitálního videorekordéru, HD u PC apod.) by měla korespondovat s počtem připojených kamer, délkou požadovaného záznamu, způsobem vyhodnocování záznamu a režimem

pořizování záznamu (kdy, jak a z které kamery bude záznam aktivován). Bezpečnostní kamerový systém může být připojen a spolupracovat i s jinými bezpečnostními systémy (např. EZS, EPS, ACS), také s použitím grafické uživatelské nadstavby, vč. informování obsluhy o vzniku alarmové události.

S ohledem na dispozici monitorovaného objektu a umístění monitorovacího pracoviště volíme způsob přenosu videosignálu včetně uložení přenosové trasy a také s ohledem na případné elektromagnetické rušení signálu.

Provozování kamerového systému z hlediska zákona o ochraně osobních údajů je považováno za zpracování osobních údajů, pokud je vedle kamerového monitorování prováděn i záznam pořizovaných záběrů a zároveň účelem pořizovaných záznamů, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním. Samotné kamerové sledování fyzických osob není zpracováním osobních údajů podle zákona č. 101/2000 Sb., protože postrádá úroveň podmínek pro zpracování údajů ve smyslu § 4 písm. e) zákona č.101/2000 Sb. To však nevylučuje aplikaci jiných právních předpisů, zejména ustanovení občanského zákoníku, upravujícího podmínky ochrany osobnosti. Údaje uchovávané v záznamovém zařízení, ať obrazové či zvukové, jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu - tedy, že informace z obrazových či zvukových nahrávek umožňují, byť i nepřímo, identifikaci konkrétní osoby. Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji, je možná plná identifikace osoby. Osobní údaj pak ve svém souhrnu tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým, na snímku zachyceným, jednáním.

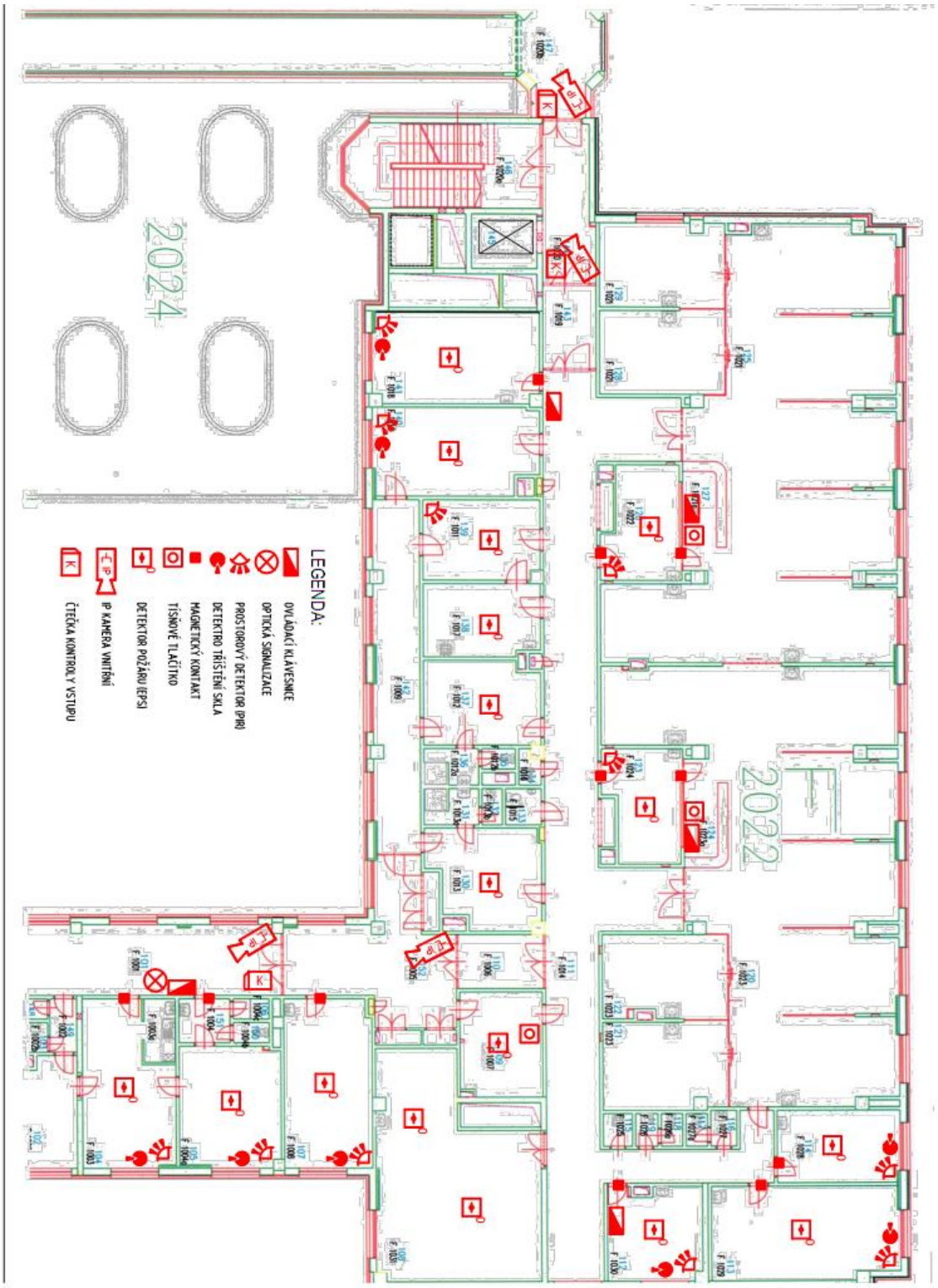
Centrální úložiště a správu nad systémem zřídit v rámci odboru bezpečnosti a krizového řízení s pověřeným minimálním počtem prověřených zaměstnanců s definicí oprávnění vstupu a provádění jednotlivých operací.

4.2.6 Ostatní biometrické aplikace

V rámci naplňování principů bezpečnostního systému ve zdravotnickém zařízení a po předchozí citaci jednotlivých systémů uvedených v praktické části doporučuji použít tyto ostatní biometrické aplikace:

- ❖biometrický zámek s klikou se snímačem otisku prstů, který lze namontovat na běžné dveře. Z vnější strany obsahuje snímač otisku prstů a elektromagneticky ovládanou kliku, která je v klidové, základní poloze volně otočná o 90^0 , aniž se zámek otevře. Po přiložení prstu a sejmutí známého otisku prstu (proces identifikace netrvá déle než vteřinu) se klika aktivuje a na krátkou dobu (cca do 10 vteřin) umožní otevření zámku a tedy i dveří, na kterých je zámek namontován. Kromě otisku prstů lze kliku aktivovat použitím osobní identifikační karty,
- ❖ochrana přístupu do PC, PDA, mobilního telefonu biometrickými senzory z důvodu uložených důvěrných osobních nebo pracovních dat. Jedná se především o biometrický snímač otisku prstů, uživatel místo hesla přiloží prst a heslo se do formuláře doplní,
- ❖další systémy by jistě šlo vyhledat a popisovat, ale byl by to zřejmě dlouhý seznam, neboť biometrie začíná silně pronikat do všech oborů bezpečnosti.

4.2.7 Bezpečné pracoviště ve zdravotnickém zařízení – návrh s půdorysem pracoviště



Jedná se o pouze o návrh bez vlastní realizace.

5. DISKUZE

Dle studijního materiálu, který jsem měla k dispozici při zpracování mé bakalářské práce jsem zjistila, že každý máme úplně jiný pohled na problematiku bezpečnosti v rámci zdravotnického zařízení. Záleží na tom, zda tuto problematiku hodnotí lékař, požární preventista či krizový manažer. V současné době není řešena bezpečnost jako celek., dokonce ani neexistuje žádná ucelená metodika a také není přímo pověřená osoba , která by se měla zabývat bezpečností komplexně.

Existuje spoustu zdravotnických zařízení, které mají bezpečnostní problematiku rozdělenou do dílčích úseků, za každý úsek zodpovídá pověřená osoba dle svého pracovního zařazení. Dále jsou zdravotnická zařízení které nemají žádného „specialistu“, který by se zabýval bezpečností komplexně jako celku. Profesionální osoba zabývající se dílčí problematikou bezpečnosti je např. požární preventista. V některých případech zdravotnická zařízení s tímto specialistou sepíšou dohodu s částečným pracovním poměrem. Tento krok je z mého pohledu velmi nešťastný zejména v případě vzniklých mimořádných událostí a v jejich následných řešeních.

Ve větších zdravotnických zařízeních fakultního typu mnohdy bezpečnost jako celek zabezpečuje vedoucí odboru , útvaru čí oddělení krizového managementu či požární preventista.

Myslím si , že tato problematika by měla být řešena komplexně a to proto abychom předešli vzniku komplikací při řešení mimořádných událostí a to z důvodu nespolupráce čí nesehranosti daných dílčích úseků.

6. ZÁVĚR

V úvodní teoretické části je pozornost věnována bezpečnostnímu systému ČR s jeho základními a výkonnými prvky, vzájemná jejich provázanost a spolupráce, bezpečnostnímu prostředí ČR, jeho trendům, nebezpečím, která nás ohrožují s následnou tabulkovou aplikací nebezpečí vztažená na zdravotnická zařízení, Bezpečnostní strategii s bezpečnostními zájmy. Chtěla jsem v bakalářské práci upozornit na skutečnost, že pokud chceme v bezpečnosti jakékoliv organizaci pokročit dále, tak se neobejdeme bez aktivní účasti top managementu zaměstnavatelů, současně jsem chtěla více přiblížit problematiku práce bezpečnostního managementu v jeho nejrůznějších podobách.

V rámci uplatňování základních zákonných norem v bezpečnostním systému ve zdravotnických zařízeních jsem se snažila o analýzu jejich jednotlivých částí (statí v § znění).

V praktické části byla věnována pozornost analýze jednotlivým elektronickým systémům, jejich použití ve specifických podmínkách zdravotnických zařízeních, přednosti jejich použití, související organizační opatření, naplnění zákonných podmínek používání systémů souvisejících se zpracováním osobních údajů s koncovým návrhem bezpečného pracoviště ve zdravotnickém zařízení a to v grafické podobě půdorysu Kliniky anesteziologie a resuscitace Institutu Klinické a Experimentální Medicíny v Praze.

Udržení vysoké úrovně bezpečnosti zdravotnických zařízeních je velmi složité a to především ke specifickým rysům prostředí. Musíme si uvědomit, že úroveň bezpečnosti zdravotnických zařízeních nikdy nebude na úrovni zabezpečení např. vládních objektů, objektů Ministerstva obrany, atomových elektráren, subjektů kritické infrastruktury apod. Je však třeba udělat vše, co je možné zabezpečit s využitím stávajících zdrojů, které jsou v rámci zdravotnických zařízeních k dispozici, pro zabezpečení standardů, které jsou zdravotnickým zařízením předepsány. Zajištění opravdu bezpečného prostředí pro zaměstnance, současné i budoucí potencionální pacienty je pro vedoucí

pracovníky, bezpečnostní a krizový management zdravotnických zařízeních úkol prvořadý, někdy připomínající boj s větrnými mlýny s prvky nekonečného příběhu.

7. KLIČOVÁ SLOVA [2][21][32]

Bezpečnostní systém státu - komplexní systém státu, který zajišťuje bezpečnost republiky, udržení a prosazení jejích životních a strategických zájmů proti všem formám destabilizace bezpečnostní situace uvnitř i vně státu.

Bezpečnostní prostředí - Bezpečnostní prostředí je vnějším prostředím ovlivňujícím bezpečnostní politiku státu. Lze jím rozumět prostor, v němž se realizují a střetávají zájmy státu se zájmy jiných aktérů systému mezinárodních vztahů a odehrávají se zde procesy, které mají významný vliv na úroveň bezpečnosti státu.

Základní prvky bezpečnostního systému jsou především ústavní instituce a činitelé, to znamená Prezident republiky, Parlament České republiky a vláda České republiky, ale dále i Bezpečnostní rada státu a její stálé pracovní orgány.

Zákonná norma v bezpečnostním systému s aplikací do vnitřního normativu organizace – jedná se o základní zákony aplikovatelné do bezpečnostního systému organizace.

8. SEZNAM POUŽITÉ LITERATURY

1) BALABÁN, Miloš, STEJSKAL, Libor. Bezpečné Česko v bezpečné Evropě. Praha: Úřad vlády ČR, 2007. ISBN 978-80-87041-17-8.
2) Bezpečnostní strategie České republiky 2011. Praha, září 2011: Vláda České republiky 2011. ISBN 978-80-7441-005-5.
3) ČESKO, BEZPEČNOSTNÍ RADA STÁTU. Zpráva o zajištění bezpečnosti České republiky. Praha: Úřad vlády České republiky, 2006. ISBN 80-86734-91-9.
4) JANOŠEC J. a kol. Bezpečnost a obrana České republiky 2015 – 2025. Praha: Ministerstvo obrany – Agentura vojenských informací a služeb, 2005. ISBN 80-7278-303-3.
5) LINHART p., ŠILHÁNEK B. Ochrana obyvatelstva v Evropě. Praha: MV – generální ředitelství HZS ČR, 2005. ISBN 80-86640-55-8.
6) Miroslav Fryšar a kolektiv, BEZPEČNOST PRO MANAŽERY, PODNIKATELE A POLITIKY, Public History Praha 2006, ISBN 80-86445-22-4.
7) Ústava České republiky – ústavní zákon č.1/1993 Sb., v platném znění.
8) Ústavní zákon č.23/1991 Sb., Listina základních práv a svobod, v platném znění.
9) Zákon č.110/1998 Sb., o bezpečnosti České republiky, v platném znění.
10) Zákon č.219/2000 Sb., o majetku České republiky a jejím vystupováním v právních vztazích, v platném znění.
11) Zákon č.372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), v platném znění.
12) Zákon č.106/1999 Sb., o svobodném přístupu k informacím, v platném znění.
13) Zákon č.101/2000 Sb., ochrana osobních údajů, v platném znění.
14) Zákon č.133/2000 Sb., o evidenci obyvatel a rodných číslech, v platném znění.
15) Zákon č.412/2005 Sb., ochrana utajovaných informací, v platném znění.
16) Zákon č.262/2006 Sb., zákoník práce, v platném znění.
17) Zákon č.499/2004 Sb., o archivnictví a spisové službě, v platném znění.
18) Prováděcí vyhláška č.645/2004 Sb., o archivní službě.
19) Prováděcí vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby.

20) Prováděcí vyhláška č.496/2004 Sb., o elektronických podatelnách.
21) http://www.vlada.cz/cz/pracovni-a-poradni-organy-vlady/brs/brs-uvod-3851/ (4.4.2012)
22) http://www.vlada.cz/cz/ppov/brs/clenove/default.htm (4.4.2012)
23) http://www.vlada.cz/cz/pracovni-a-poradni-organy-vlady/brs/cinnost/terminy-
24) jednani-bezpecnostni-rady-statu-3538/ (4.4.2012)
25) http://www.army.cz/avis/vojenske_rozhledy/2001_2/21.htm (4.4.2012)
26) http://www.psp.cz/docs/laws/constitution.html (4.4.2012)
27) http://articles.gourt.com/cs/prezident%20%C4%8Cesk%C3%A9%20republiky (4.4.2012)
28) http://www.dovednostimanazera.cz/ (4.4.2012)
29) http://www.alveno.cz/cz/32/dochazkovesystemy?utm_source=sklik&utm_medium=ppc&utm_campaign=dochazkovy_system_top (4.4.2012)
30) http://www.timelink.cz/pristupove-systemy/ (4.4.2012)
31) http://www.mselektro.cz/elektronicke-pozarni-systemy/ (4.4.2012)
32) http://www.delnet.cz/slaboproude-systemy/elektricka-pozarni-signalizace-eps.html (4.4.2012)
33) Frank, Libor (2003): Bezpečnostní prostředí České republiky. Obrana strategie, roč. 3., č. 1,s.1

9. SEZNAM TABULEK A OBRÁZKŮ

10.SEZNAM PŘÍLOH