Informační podpora bezpečnostního manažera

Information support of security manager

Bc. Jan Brhel

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan BRHEL**
Osobní číslo:	**A09347**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Informační podpora bezpečnostního manažera**

Zásady pro vypracování:

1. **Analyzujte obsah pracovní pozice bezpečnostního manažera organizace.**
2. **Specifikujte současný stav v oblasti informačních systémů a informační podpory.**
3. **Analyzujte informační potřeby bezpečnostního manažera.**
4. **Zhodnoťte dostupné softwarové nástroje a technické prostředky pro zajištění informační podpory bezpečnostního manažera.**
5. **Navrhněte možnosti zlepšení informační podpory bezpečnostního manažera.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **FRYŠAR, Miroslav, et al. Bezpečnost pro manažery, podnikatele a politiky. Praha : Public History Praha, 2006. 176 s. ISBN 80-86445-22-4.**
2. **LUKÁŠ, Luděk; HRŮZA, Petr; KNÝ, Milan. Informační management v bezpečnostních složkách. Praha: Ministerstvo obrany - Agentura vojenských informací a služeb, 2008. 214 s. ISBN 978-80-7278-460-8.**
3. **POŽÁR, Josef. Manažerská informatika. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2010. 357 s. ISBN 978-80-7380-276-9.**
4. **ŠULER, Oldřich. 5 rolí manažera a jak je profesně zvládnout?. Praha: Vydavatelství a nakladatelství Computer Press, a.s., 2008. 240 s. ISBN 978-80-251-2316-4.**
5. **VEBER, Jaromír, et al. Management: Základy - prosperita - globalizace. Praha: Management Press, 2000. 700 s. ISBN 80-7261-029-5.**
6. **ČECH, Pavel; BUREŠ, Vladimír. Podniková informatika. Hradec Králové: GAUDEAMUS, 2009. 232 s. ISBN 978-80-7041-479-8.**
7. **POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005. 311 s. ISBN 80-86898-38-5.**

Vedoucí diplomové práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem diplomové práce je analýza informačních potřeb bezpečnostního manažera organizace a možnosti jejich uspokojení využitím informačních systémů. V návaznosti na to je zhodnoceno, jaké informační a telekomunikační prostředky napomáhají bezpečnostnímu manažeru k jejich naplnění. V závěru jsou specifikovány trendy a výzvy v dané oblasti.

Klíčová slova:

Bezpečnostní manažer, informační podpora, informační potřeba, technické a softwarové nástroje

ABSTRACT

The aim of this thesis is an analysis of information security manager needs of the organization and the possibility of satisfying use of information systems. Following that is evaluated, what information and telecommunication equipment help security managers to meet them. At the end of specified trends and challenges in the area.

Keywords:

Security manager, information support, information needs, technical and software tools

Tímto bych chtěl poděkovat vedoucímu mé diplomové práce doc. Ing. Luďku Lukášovi, CSc., za jeho pomoc při vedení diplomové práce, za jeho připomínky i čas, který se mnou strávil při konzultacích. Dále bych chtěl poděkovat mojí rodině za její podporu a rady. V neposlední řadě bych chtěl poděkovat všem, kteří přispěli k tvorbě této diplomové práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně 17. 5. 2011 …….

podpis diplomanta

OBSAH

ÚVOD

Na úvod diplomové práce bych chtěl říci, že jejím úkolem je analyzovat informační potřeby bezpečnostního manažera. V návaznosti na to zhodnotit, jaké informační a telekomunikační prostředky napomáhají bezpečnostnímu manažerovi k jejich naplnění.

Téma jsem si vybral mimo jiné i proto, abych získal určitou představu o tom, co obsahuje práce bezpečnostního manažera, jelikož je možné, že to bude mé budoucí povolání.

Při psaní diplomové práce byla využívána literatura a metoda průzkumu. S využitím analýzy jsem z využité literatury získával klíčové informace. Metodou syntézy a dedukce jsem spolu s výsledky průzkumu dospěl k jednotlivým dílčím závěrům.

Samotná práce obsahuje pět kapitol. V prvních dvou kapitolách je pojednáváno o působnosti bezpečnostního manažera, informacích a informačních systémech. Je zde specifikována charakteristika a role nejen bezpečnostního manažera. Dále jsou zde zmíněny především manažerské funkce, dovednosti a je zde pojednáno o činnosti bezpečnostního manažera v podniku.

Následující dvě kapitoly jsou zaměřeny na analýzu informačních potřeb, technických prostředků a softwarových nástrojů pro zajištění informační podpory bezpečnostního manažera. Jsou zde specifikovány informační potřeby bezpečnostních manažerů a pojednáno o technických prostředcích a softwaru, se kterým pracují nebo mohou přijít do styku.

V poslední kapitole jsou uvedeny výsledky dotazníkového šetření, jehož cílem bylo zjistit, jak bezpečnostní manažer pracuje s informacemi, jak je získává či využívá a jaké technické prostředky k tomu používá. V závěru práce je nastíněna možnost zlepšení informační podpory bezpečnostních manažerů.

1 PŮSOBNOST BEZPEČNOSTNÍHO MANAŽERA

Úvodní kapitola je zaměřena na charakteristiku manažerů, jejich funkcí a rolí, dále pak na vymezení činnosti bezpečnostního manažera v rámci podniku. Dříve, než se dostaneme k jednotlivým bodům této kapitoly, objasníme si nejprve základní pojem management.

V lidské činnosti dochází z mnoha důvodů k dělbě práce a v rámci specializace činností se někteří lidé zabývají organizací jednotlivých lidských aktivit, jinak řečeno, zabývají se řízením činností lidí. Čím větší je organizační uskupení lidí spojených nějakými společnými cíli, tím větší je i skupina řídících pracovníků, kteří se hierarchicky organizují mezi sebou a vzniká tak celá struktura pracující s informacemi podobně jako lidský mozek. [3]

Řízení se tak stává profesí a na kvalitě řídících pracovníků závisí prosperita řízených celků a celé lidské společnosti. [3]

Pro řízení na vyšších úrovních hierarchicky uspořádaných řídicích struktur se používá výraz management a pro vyšší řídicí prvky je používán výraz manažer. [3]

V dnešní době existuje řada definic a výkladů slova management. Výklad tohoto slova nalezneme v encyklopediích různých světových literatur.

Výklad slov z anglického slovníku:

- manage – ovládat, řídit, vést, zvládnout, spravovat, postarat se;
- management – správa, řízení, vedení;
- manager – správce, ředitel, vedoucí.

Výklad slova management ze slovníku cizích slov:

- management – systém teoretických a praktických řídících znalostí a činností.

Definice managementu podle některých autorů:

Management – nejobecněji lze charakterizovat jako souhrn všech činností, které je třeba udělat, aby byla zabezpečena funkce organizace. [12]

Management – je oblast studia, která se věnuje stanovení postupů, jak nejlépe dosáhnout cíle organizace. *(Robbins, H.)*

Management – je vykonávání věcí prostřednictvím ostatních lidí (je umění dosahovat cíle organizace rukama a hlavami jiných). *(Pale, E.)*

Závěrem lze říci, že neexistuje jednoznačná definice pojmu management. Ba naopak na tento pojem existuje řada definic z různých úhlů pohledu. Management můžeme tedy charakterizovat jako souhrn všech metod, postupů, funkcí a technik používaných při řízení (lidí, organizací) a dosahování stanovených cílů organizace a její vlastní funkčnosti.

1.1 Charakteristika a role bezpečnostního manažera

Stejně jako management má i pojem manažer několik různých definic. Již z výkladu anglického slovníku lze chápat slovo **manažer** jako ředitele, správce nebo vedoucího. Jde tedy o člověka, který něco řídí (např. ředitel banky, vedoucí oddělení, šéf ostrahy objektu, vedoucí úseku pro dodávku a montáž bezpečnostních systémů atd.).

Postavení manažera v procesu řízení je možno ilustrovat následujícím schématem:

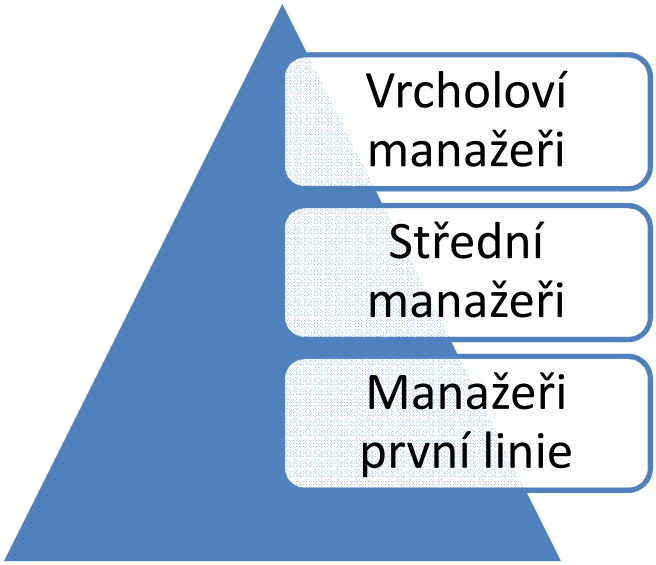
Obr. 1 Schéma postavení manažera v podniku

Ve schématu můžeme spatřit tři role – vlastník, manažer a zaměstnanec. Dříve existovaly podniky, kde tyto role splývaly v jednu roli. Dnes již existuje řada podniků, u kterých jsou tyto role osamostatněné. Je to dáno tím, že podniky se rozrůstají do všech stran a už by nebylo možné zajistit dosahování jejich stanovených cílů. Jeden člověk už by nebyl schopen řídit tak velký podnik. Ovšem i nyní se ještě můžeme setkat s tím, že ne všechny podniky mají tyto role odděleny. Jedná se především o soukromé menší rodinné podniky, kde samotný vlastník vykonává funkci manažera a někdy i zaměstnance.

Manažera tedy můžeme označit jako specifického zaměstnance podniku, který zodpovídá za jeho provoz. Jeho úkolem je řídit, organizovat, plánovat určité činnosti v podniku. Pracovní náplň manažera může být rozdílná a na různých řídících úrovních. Ne každý člověk má předpoklady stát se dobrým manažerem. Pro tento druh práce je zapotřebí mít příslušné znalosti a dovednosti. Manažer pracuje prostřednictvím svých podřízených, zodpovídá za jejich práci, stimuluje je a snaží se o soulad potřeb jejich i potřeb organizace.

Dále informuje jak své podřízené tak i nadřízené. Reaguje na chyby v systému, dělá důležitá rozhodnutí a vyjednává.

V současné době se manažeři rozdělují obvykle do tří základních kategorií – manažeři první linie, střední manažeři a vrcholoví manažeři.



Obr. 2 Úrovně manažerů v podniku

V pomyslné pyramidě můžeme vidět dělení manažerů podle úrovně řízení v podniku. Na prvním stupni řízení jsou manažeři označováni jako manažeři první linie. Tito lidé dohlížejí především na plnění jednotlivé práce, kterou vykonávají zaměstnanci. Řadíme zde lidi, kteří působí jako mistři na svých pracovištích, předáky, vedoucí pracovišť apod. (např. v bezpečnostní agentuře to může být člověk, který dohlíží nad montáží bezpečnostních systémů). Tito lidé by měli mít co nejvíce odborných znalostí týkajících se produkce výrobků nebo poskytovaných služeb. Na druhém stupni řízení jsou střední manažeři. Zde je zařazena početná a rozmanitá skupina vedoucích pracovníků z mnoha různorodých útvarů (např. z personalistiky, zásobování, prodejního úseku apod.). Jako příklad bych opět uvedl pracovníka bezpečnostní agentury, který působí jako vedoucí úseku montáže bezpečnostních systémů. Vrcholoví manažeři (nazývaní taky jako top manažeři) tvoří nejvyšší stupeň řízení managementu podniku. Mají za úkol usměrňovat a koordinovat chod celého systému organizace. Tvoří politiku organizace a částečně přebírají odpovědnost za vlastníky podniku a mají na ně velmi úzké vazby (např. v bezpečnostní agentuře člověk, který koordinuje celý systém poskytovaných služeb).

1.1.1 **Manažerské dovednosti**

Stejně jako všichni zaměstnanci, tak i manažeři musí plnit stanovené úkoly tzv. řídit práci, pracovníky apod. Být dobrým manažerem znamená mít mnoho dovedností, znalostí a zkušeností. Manažerské dovednosti můžeme vymezit na tři okruhy:

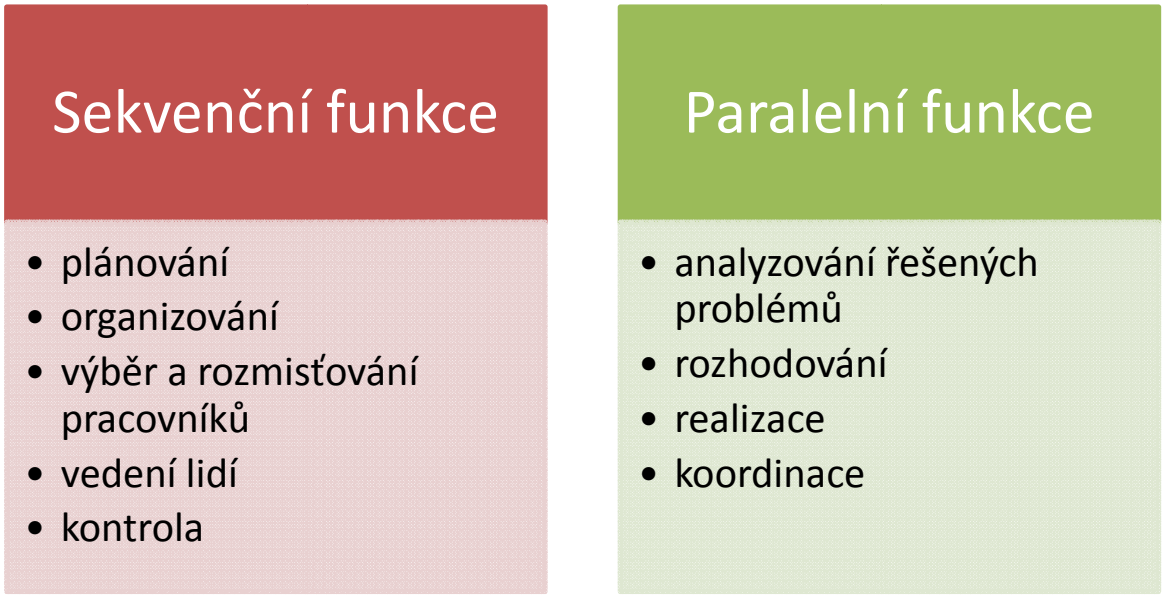
- **lidské dovednosti** - jsou obecné dovednosti důležité zejména pro provozního manažera, personalistu. Tyto dovednosti jsou důležité pro vedení lidí, motivaci, komunikaci, spolupráci a vzájemné pochopení;
- **technické dovednosti** - schopnosti využívat specifické vlastnosti, postupy, znalosti techniky, využívat specializované pracovníky. Manažer by měl mít stejné dovednosti technického rázu, jako mají lidé, které řídí. A to proto, aby zajistil 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. [37]

Další vlastnosti, kterými by měl disponovat dobrý manažer:

- vždy jasně vymezit cíle, aby lidé věděli, na čem mají vlastně pracovat;
- zřetelně vyjadřovat pokyny;
- umět 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. [37]

1.1.2 **Manažerské funkce**

Jedná se o činnosti, které manažer ve své práci vykonává. Jsou to činnosti podstatné, které musí zvládnout. Manažerské funkce můžeme rozdělit na sekvenční a paralelní.



Obr. 3 Rozdělení manažerských funkcí

Sekvenční manažerské funkce se realizují postupně. Pro každou z těchto sekvenčních manažerských funkcí je společné to, že jimi prostupují funkce paralelní (označovány taky jako průběžné).

Nyní se v krátkosti seznámíme s některými funkcemi.

Plánování

„Plánování staví mosty mezi tím, kde jsme, a tím, kam chceme jít.“ [12]

Plánování je jedna z hlavních činností manažera, protože obsahuje vymezení cílů a naznačení cest, jimiž má být těchto cílů dosaženo. Plánování je dále často označováno za východisko dalších sekvenčních manažerských funkcí – organizování, výběr a rozmisťování pracovníků, vedení lidí a kontrolování. Výchozím dokumentem plánování bývá plán. Každý podnik obvykle mívá několik druhů plánů (např. plán výrobního procesu, plán únikových cest, havarijní plán, finanční plán apod.).

Organizování

Po plánování řadíme organizování mezi druhou hlavní činnost manažera. V organizování se jedná především o činnost manažera, jehož konečným cílem je uspořádání prvků v systému tak, aby přispěly k dosažení stanovených cílů systému. Tak jako výsledkem

plánování byl plán, tak za výsledek organizování můžeme považovat organizační strukturu podniku. Jejím posláním je optimální rozdělení úkolů, kompetencí a pravomocí mezi pracovníky podniku. Například manažer podniku má za cíl udělat havarijní plán. Sestaví si tým, který s ním na tom bude spolupracovat. Rozdělí si spolupracovníky na dvě skupiny. V každé skupině určí šéfa. Zároveň stanoví jejich práva, povinnosti a vzájemný způsob komunikace. Tím si manažer pomocí organizování vytvořil organizační strukturu, která mu umožní dosáhnout vytyčeného cíle.

Výběr a rozmisťování pracovníků

Tato manažerská činnost je definována jako obsazování pozic v organizační struktuře a udržování jejich obsazení.

Tato funkce je realizována pomocí identifikace požadavků na pracovní sílu, najímáním, vybíráním, umísťováním, povyšováním, přemísťováním, zastupováním, školením a také propouštěním pracovníků. [3]

Za výběr a rozmisťování pracovníků na určitém úseku odpovídá příslušný manažer. [3]

Vedení lidí

Vedení lidí patří mezi další sekvenční funkci. Jedná se o způsob, jakým manažeři vedou své lidi, jak umějí ze skupiny lidí vytvořit tým a využívat jeho potenciál efektivními technikami týmové práce, udržovat na pracovištích dobré mezilidské vztahy, řešit konflikty, volit vhodné komunikační styly a úroveň komunikace, má zásadní vliv na efektivnost práce týmu, organizačních jednotek i celých firem. [11]

Kontrola

Pro úspěšný chod podniku a dosahování stanovených cílů je kontrola činnosti podniku nezbytnou součástí. Je prováděna na všech úrovních řízení. Pomocí kontroly můžeme identifikovat odchylky od stanoveného plánu a učinit nápravná opatření vedoucí k dosažení cílů.

Účelem kontroly je:

- ověřit si jaký je skutečný stav;
- dosáhnout jistoty, že plán je úspěšně realizován;
- zjistit včas odchylky mezi záměry (úkoly) a jejich realizací;
- zjistit příčiny odchylek;
- vyvození závěrů (odstranění odchylek, změna plánu).

Analyzování řešených problémů

Tuto funkci již řadíme mezi funkce paralelní. Hlavním úkolem manažera při řešení problému je jeho správné definování, ze kterého je pak provedena analýza. Následně jsou pak stanoveny příčiny, které vedly ke vzniku problému. Na závěr jsou pak stanoveny možnosti k odstranění problému.

Rozhodování

Řadíme podobně jako analyzování řešených problémů mezi paralelní manažerské funkce. Rozhodování je proces, při kterém vybíráme alespoň mezi dvěma možnými variantami. Pak už je na schopnostech manažera, aby vybral tu variantu, která bude ta nejlepší.

Manažer provádí obvykle rozhodnutí týkající se buď běžných problémů, nebo problémů složitých. Existují dva základní typy rozhodovacích problémů:

- Dobře strukturované problémy
  - jednoduché
  - opakované
  - programované
- Špatně strukturované problémy
  - vždy do určité míry nové a neopakovatelné
  - existence většího množství faktorů ovlivňujících řešení
  - nejistota budoucího vývoje faktorů

Jako příklad dobře strukturovaného problému můžeme uvést rozhodnutí týkající se rozdělení odměn nebo výběr pracovníka na uvolněné místo vedoucího. Příkladem špatně strukturovaného problému může být uvedení nového výrobku na trh, změna organizační struktury nebo inovace.

Koordinace

Koordinování nám slouží k zabezpečení souladu mezi jednotlivými cíly podniku, útvary, činnostmi a funkcemi. Bývá realizováno ve všech funkcích řízení. Je prováděno zejména prostřednictvím porad a osobního styku.

V této podkapitole jsme se seznámili s pojmem manažer, jeho dovednostmi a funkcemi, které využívá ke své práci. Za manažera je považován člověk, který něco řídí (ředitel divize pro bezpečnost, vedoucí prodejního úseku apod.). Může se jednat o zaměstnance podniku ale taky i o vlastníka podniku. Zde záleží na tom o jak velký a o jaký druh

podniku se jedná. Dále jsme si objasnili základní manažerské funkce. Tyto funkce můžeme dále rozdělit na sekvenční a paralelní. Mezi sekvenční funkce řadíme plánování, organizování, výběr a rozmisťování pracovníků, vedení lidí a kontrolu. Do paralelních funkcí označovaných taky jako průběžné řadíme analyzování řešených problémů, rozhodovaní, realizaci a koordinaci. Plánování řeší, co nebo čeho chce podnik dosáhnout a určí, jakým způsobem toho bude chtít dosáhnout. Organizování je zaměřeno na uspořádání prostředků a sil tak, aby bylo s jejich pomocí dosaženo stanovených cílů. Kontrola nám pak poskytuje zpětnou vazbu v celém cyklu řízení a umožňuje nám reagovat na chyby. S funkcí rozhodování se většina z nás setkává denně. Jedná se o činnost, kdy máme na výběr alespoň ze dvou možností. Tato funkce klade vyšší nároky na naše psychické schopnosti.

1.2 Činnost bezpečnostního manažera v rámci podniku

Dříve, než se dostaneme k vlastní činnosti, kterou by měl bezpečnostní manažer či vedoucí v podniku vykonávat, přiblížíme si, s jakou oblastí bezpečnosti se můžeme v podniku setkat.

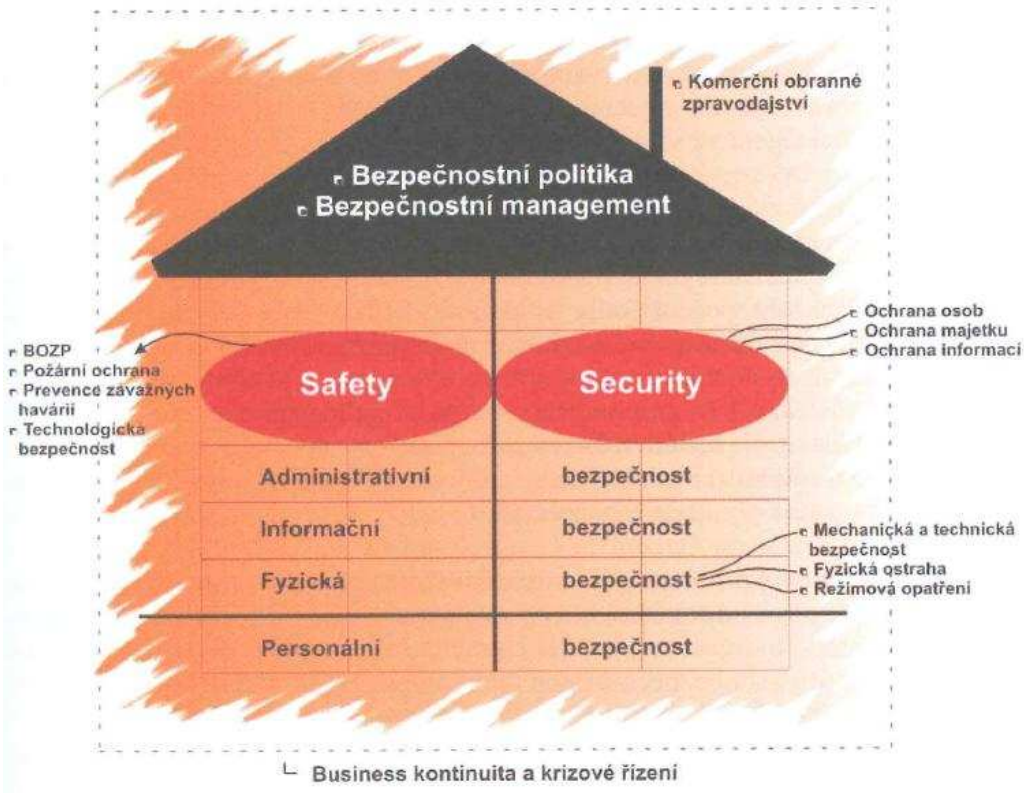
Jak je definována a co to vlastně bezpečnost je? S pojmem bezpečnost se denně setkáváme v různých mediích. Hovoří se o bezpečnosti výrobků, bezpečnosti na letištích, bezpečnosti potravin apod. S pojmem bezpečnost se čím dál více setkáváme i v podnicích (informační, fyzická, personální bezpečnost apod.).

***Bezpečnost je stav**, kdy jsou na akceptovatelnou míru eliminovány hrozby pro objekt a jeho zájmy. Tím objektem může být stát, organizace, systém, sociální skupina (národ, národnostní menšina, ženy, jednotlivec).*

***Bezpečnost**, tj. systém ochrany sloužící k poznání a eliminaci vnějších a vnitřních bezpečnostních rizik, vystupuje ve vztahu k roli manažera, vlastníka, vedoucího apod. v několika rovinách.* [2]

První a základní z nich chápe bezpečnost jako nezbytnou podmínku zajištění prosperity společnosti, kontinuity činnosti úřadu, instituce nebo naplnění cílů projektu, produktu, služby. Odpovědnost za bezpečnost má vždy manažer – vedoucí organizace. Tato odpovědnost je v obecné rovině stanovena právními předpisy a vyplývá z komplexní odpovědnosti vedoucího. Zároveň však logicky pramení z odpovědnosti a ze zájmu manažera o funkčnost organizace jako celku. V současných podmínkách si

funkčnost bez bezpečnosti nelze představit. Nejde však pouze o bezpečnost práce, ale o bezpečnost v nejširším významu slova, tj. bezpečnost komplexní. [2]



Obr. 4 Komplexní bezpečnost podniku

Náš virtuální dům na obrázku č. 4 tvoří ucelený bezpečnostní systém. Jeho základem je **personální bezpečnost.** Pod tímto pojmem se skrývají veškeré otázky spojené s bezpečnostními podmínkami pro výběr top managementu, zaměstnanců nebo poměru u organizace. Pod personální bezpečnost dále zahrnujeme proces bezpečnostního vědomí (spoluzodpovědnosti za bezpečnost) a bezpečnostní vzdělání. [2]

Dům je dále rozdělen do dvou hlavních částí bezpečnosti. Části **safety** (provozní a technologická bezpečnost) a **security** (klasická bezpečnost). Oběma částmi bezpečnosti se pak prolínají jednotlivá bezpečnostní opatření (oblasti, prostředky, druhy zajištění apod.), kterými jsou zejména:

- fyzická bezpečnost;
- informační bezpečnost;
- administrativní bezpečnost. [2]

Nástavbou a střechou virtuálního domu je pak bezpečnostní politika a bezpečnostní management. **Bezpečnostní politikou** v tomto případě nechápeme pouze vlastní základní

dokument řídící dokumentace v oblasti bezpečnosti, tj. **komplexní bezpečnostní politiku**, ale veškerou navazující bezpečnostní dokumentaci. Rovněž bezpečnostní management není chápán pouze jako bezpečnostní manažer nebo tým, ale také vedoucí zaměstnanci jednotlivých úrovní, kteří jsou za bezpečnost ve svých funkcích odpovědni. [2]

Jako bleskosvod je znázorněno komerční obranné zpravodajství, jehož účelem je chránit organizaci proti útokům zevnitř i zvenku. Pro orgány státu zajišťují roli obranného zpravodajství zpravodajské služby. V privátním sektoru se toto zajišťuje vlastními specialisty nebo specializovanými společnostmi. [2]

Druhá rovina je rovinou osobní a je bezprostředně spojena s výkonem činností manažera, jeho dalšími aktivitami i soukromým životem. Patří sem především události a jednání, které mohou být zneužity k diskreditaci manažera a v konečném důsledku ohrozí kontinuitu jeho působení ve funkci či podnikání. Zajímavé přitom je, že velká část obvinění klíčových státních úředníků a top manažerů nemá příčinu v úmyslném jednání, ale v nedbalosti. Ta vyplývá z nedostatečné znalosti legislativy nebo podceňování rizik souvisejících s řešením dané situace. V některých případech se pak trestná činnost manažera či úředníka neprokáže, ale vlivem medializace dojde k poškození jeho dobrého jména a dobrého jména úřadu či společnosti. S odstupem času se někdy navíc ukazuje, že problém vznikl uměle na základě úniku informací, které neměly být veřejnosti přístupné. Nejsou výjimkou ani případy, kdy se celý problém odehraje na základě komerční objednávky. Zdrojů incidentů může být celá řada, od konkurenčních vlivů přes záležitosti vyplývající z minulosti manažera až po osobní ambice podřízených nebo aktivity propuštěných zaměstnanců. Ideální možností je zavedení specializovaného bezpečnostního vzdělávání pro top management. Základním krokem může být vystoupení bezpečnostního experta nebo znalce na poradě vedení či představenstva společnosti. [2]

Komplexní řešení problematiky ochrany managementu je poměrně rozsáhlou oblastí bezpečnosti a zahrnuje plánování preventivních opatření, vzdělávání manažerů, vytvoření materiálně-technické základny ochrany, komerční obranné zpravodajství, fyzický výkon ochrany a řešení bezpečnostních incidentů a ohrožení. Je to v zájmu manažerů se o tuto problematiku začít vážně zajímat. [2]

Třetí rovinou je rovina business kontinuity. Obvykle chápeme, že společnost by měla mít krizové scénáře pro řešení nejrůznějších problémů a incidentů. Ne vždy se však dokážeme odpoutat od mýtu, že se toto týká pouze ekonomické úrovně řešení. Bezpečnostní opatření

spojená s kontinuitou podnikání jsou stále nadále podceňována, řešení ohrožení bezpečnostního charakteru schází nebo jsou nedostatečně rozpracována. Přitom nemusí jít o nákladná opatření technického charakteru, ale o opatření organizační. Příkladem jsou zpracované a zvládnuté postupy při vzniku incidentů bezpečnostního charakteru s minimalizací jejich dopadu. Pro subjekty kritické infrastruktury je povinnost zpracování krizové dokumentace stanovena legislativou. Ta je však vázána na vyhlášení tzv. krizového stavu. Ne vždy si uvědomujeme, že neřeší, a ani řešit nemůže, situace, které ještě nedosáhly uvedeného rozměru, nebo vnitřní incidenty. [2]

Čtvrtá rovina, ve které se promítají roviny předchozí, je rovinou bezpečnostní praxe. Její výslednicí je reálná úroveň bezpečnosti podniku, úřadu, instituce. [2]

Podniky se více či méně od prvopočátku zabývají problematikou bezpečnosti. Jednak to mají dané legislativou, kde se jedná především o:

- bezpečnost a ochranu zdraví při práci;
- krizové řízení;
- prevenci závažných průmyslových havárií;
- bezpečnost na úseku požární ochrany;
- nakládaní s utajovanými informacemi;
- ochranu osobních údajů a prevenci kriminality.

Aby ale mohly podniky dále růst a stávat se úspěšnými, je zapotřebí dbát nejenom na dodržování již zmiňované legislativní bezpečnosti, ale i na bezpečnost chápanou v širším slova smyslu (informační bezpečnost, bezpečnost výrobního know-how, fyzická bezpečnost aj.). Proto, aby bylo možno dosáhnout plnění celé bezpečnosti a tím zároveň zajištění správného chodu podniku (organizace, společnosti, instituce), je zapotřebí mít personál, který bude řídit jednotlivé úseky bezpečnosti. Nejedná se o nikoho jiného než právě o bezpečnostní manažery (vedoucí) podniku. Jejich přesnější název se pak uvádí podle toho, na jakou oblast jsou zaměřeni. Poté můžeme mluvit např. o bezpečnostním manažerovi pro: fyzickou bezpečnost, informační bezpečnost, personální bezpečnost, člověka, který má na starost bezpečnost a ochranu zdraví při práci aj.

1.2.1 **Manažer pro informační bezpečnost**

Manažer, který se stará o informační bezpečnost v podniku, prosazuje politiku a standardy informační bezpečnosti v souladu s interními i externími normami podniku. Podílí se zejména na návrhu a implementaci efektivního systému řízení informační bezpečnosti. Jeho hlavní odpovědnost a povinnost pak může být následující:

- Příprava metodiky systému řízení informační bezpečnosti s ohledem na efektivní ošetření informačních rizik a odpovědnost za její aktuálnost.
- Provádění analýzy rizik informačních systémů a jejich změn.
- Poskytování odborné pomoci, navrhování a schvalování bezpečnostních opatření při výběru, vývoji, provozu a změnách informačních systémů.
- Řízení implementace projektů informační bezpečnosti a koordinování aktivit informační bezpečnosti spojené především se sdílenými informačními systémy a IT infrastrukturou.
- Kontrolování dodržování norem a standardů informační bezpečnosti, kontrolování konfigurace a bezpečnostních záznamů informačních systémů.
- Průběžné monitorování novinek v oblasti informační bezpečnosti, zejména s ohledem na nové standardy a rizika provozovaných systémů a navrhuje adekvátní opatření pro zvýšení úrovně informační bezpečnosti.
- Zajišťování činnosti spojené se zvyšováním povědomí o informační bezpečnosti, vzděláváním a školením zaměstnanců.
- Řešení bezpečnostních incidentů v oblasti informační bezpečnosti.

1.2.2 **Manažer pro fyzickou bezpečnost**

Fyzikou bezpečností podniku nerozumíme jenom fyzickou ostrahu, ale spadá sem i technické a organizační opatření a technické zabezpečení. Právě dobré zvládnutí technických a organizačních opatření mají vliv na funkčnost technického zabezpečení a fyzické ostrahy. Manažer starající se o fyzickou bezpečnost podniku má tedy na starosti:

1. *Organizační a technická opatření:*

- zpracování provozních řádů a jejich aktualizace;
- koordinaci a provádění kontroly realizace navrhovaných opatření;
- zpracování zprávy o mimořádných událostech, koordinaci, řešení, případně i řízení opatření k mimořádným událostem a krizovým situacím;

- zajišťování a provádění školení v oblasti organizačních a režimových opatření a zpracování jednotlivých forem školení a metodických materiálů.

2. *Technické zabezpečení:*
   - zpracování nebo zajišťování zpracování analýzy bezpečnostních rizik, bezpečnostního posouzení objektu;
   - vyjadřování se k projektové dokumentaci systémů zabezpečovací techniky;
   - podílení se na zajišťování bezporuchového provozu systémů zabezpečovací techniky;
   - koordinování a kontrolování realizace systémů technického zabezpečení se smluvními dodavateli a ostatními zainteresovanými organizačními útvary.
3. *Fyzická ostraha:*
   - navrhování systému a způsobu provádění fyzické ostrahy pro objekt/ty podniku;
   - vyjadřování se ke směrnici pro výkon ostrahy v daném objektu;
   - kontrolování a koordinování výkonu ostrahy se smluvním dodavatelem a s ostatními zainteresovanými organizačními útvary.

1.2.3 Manažer pro bezpečnost ochrany zdraví při práci a požární ochranu

Dalším důležitým úsekem bezpečnosti ve firmě je bezpečnost ochrany zdraví při práci (BOZP) a požární ochrana (PO). Obě tyto činnosti bývají většinou spojeny do jednoho celku. BOZP je souhrn opatření stanovených legislativou nebo zaměstnavatelem, která mají předcházet ohrožení nebo poškození lidského zdraví v pracovním procesu. Požární ochrana je souhrn nařízení, která mají předcházet vzniku požáru a která nám říkají, jak se chovat v případě vzniku požáru.

BOZP:

- kontroluje dodržování předpisů BOZP, podílí se na navrhování způsobu zajištění BOZP na pracovištích a podílí se na realizaci navrhovaných řešení;
- spolu s příslušnými vedoucími zaměstnanci organizuje komplexní roční prověrky BOZP na všech pracovištích;
- připravuje podklady a podmínky pro činnost externích dodavatelů v oblasti BOZP, zadává, koordinuje, kontroluje a přebírá práci – dodávku.

Požární ochrana:

- podílí se na navrhování způsobu zajištění PO na pracovištích a podílí se na realizaci navrhovaných řešení;
- kontroluje dodržování předpisů PO;
- zajišťuje a provádí školení ohledně PO;
- připravuje podklady a podmínky pro činnost určených externích dodavatelů v oblasti PO, zadává, koordinuje, kontroluje a přebírá práci;
- v případě vzniku požáru informuje osobu odborně způsobilou a příslušný HZS a účastní se vyšetřování.

Pokud bychom měli říci, kolik bezpečnostních manažerů se bude nacházet v podniku (organizaci, firmě), tak na to můžeme odpovědět následujícím způsobem. Bezpečnostní manažeři a jejich počet v podniku vždy bude záležet na konkrétním podniku. Stejně tak i popis práce BM se bude odvíjet a bude přizpůsobený konkrétním podmínkám podniku.

1.3 Shrnutí

V první částí diplomové práce jsem se zaměřil na definování managementu a pak zejména na charakteristiku manažera, jeho funkce a dovednosti. Dále zde byla nastíněna komplexní bezpečnost podniku a činnost bezpečnostních manažerů.

Jak již bylo zmíněno, na management existuje různá řada pohledů a názorů. Management můžeme tedy charakterizovat jako souhrn všech metod, postupů, funkcí a technik používaných při řízení (lidí, organizací, podniků). S jeho pomocí taky dosahujeme cíle podniku, které byly stanoveny. Každý podnik (firma, organizace, instituce) má nebo by měl mít stanoveny cíle (tj. čeho a jak by toho chtěl dosáhnout). A právě ke správnému plnění těchto cílů využívá lidi, kteří jsou označováni jako manažeři. Pokud se budeme bavit o bezpečnostních manažerech podniku, tak se bude jednat především o ty manažery, kteří budou mít na starost fyzickou, informační, personální a administrativní bezpečnost. Jaký bude přesný popis jejich činností, záleží na daném podniku. Budou ale především řídit, organizovat, kontrolovat a dohlížet na správný chod přiděleného úseku.

2 DATA, INFORMACE A INFORMAČNÍ SYSTÉMY

V této kapitole se seznámíme s pojmy, jako jsou data, informace a informační systémy. Dalo by se říct, že každý z nás by tyhle předešlé pojmy zvládl více či méně objasnit. My všichni totiž potřebujeme informace k různým našim aktivitám během každého dne. Ať už se jedná o informace důležité při naší práci nebo jen informace, které uspokojí naše mimo pracovní záležitosti. Dennodenně stojí před každým z nás spousta rozhodnutí. A pokud chceme dosáhnout té nejlepší volby, tak každý ví, že je potřeba důkladné analýzy všech podmínek, dat a informací, jejichž kvantita a kvalita hraje významnou roli při našem rozhodování. Proto kvalitní informovanost je velmi důležitá nejen pro každého z nás, ale především pro manažery, kteří, dalo by se říct, zodpovídají za úspěch či neúspěch svých organizací, ve kterých pracují.

2.1 Definice dat a informací

Pojem informace a data jsou většině z nás jasné. Ovšem někdy přesto dochází k záměně těchto dvou slov. Pro běžné lidi nemá záměna těchto dvou slov zas až tak výrazný vliv pro další práci. Pro práci odborníků je třeba tyto různé pojmy odlišit a vymezit jejich vztah mezi sebou.

Informace

Původ slova informace vychází z latinského slova *informatio*, což znamená vtištění formy či tvaru, utváření. Slovo se však používalo pro „utváření mysli“ – učení a vzdělávání a odtud dalším významovým posunem mohlo znamenat i sdělení, zprávu. Odtud pochází slovo *informátor*, doložené od 16. století. Zkrácený tvar *info* vznikl až ve 20. století v angličtině. Vědecký zájem o *informaci* začíná také až ve 20. století v souvislosti s elektronickou komunikací a počítači a na druhé straně se studiem obecného uspořádání struktur a kódů.

Pojem informace patří k nejobecnějším kategoriím současné vědy i filozofie, řadí se mezi takové pojmy jako hmota, vědomí, myšlení, poznání, pohyb, čas. Podle toho, ve kterém vědním oboru nebo ve které oblasti lidské činnosti se používá, jsou aplikovány specifické přístupy ke zkoumání informace a jsou k dispozici různé způsoby jejího definování. [9]

Informace je:

- sdělení, zpráva;

- znalost sdílená tím, že se komunikuje – to co MY víme. Je to sdělitelná znalost;
- sdělení, komunikovatelný poznatek, který má význam pro příjemce nebo údaj usnadňující volbu mezi alternativními rozhodovacími možnostmi;
- soubor údajů, které mají pro příjemce význam a slouží ke snížení neurčitosti. [9]

Data

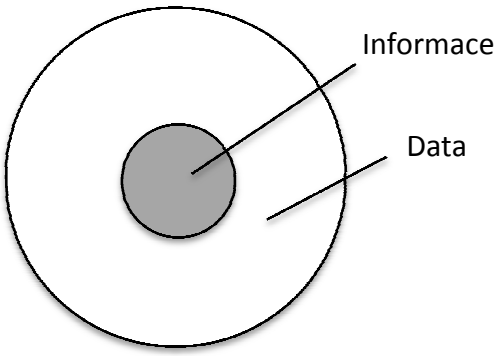
Již na začátku bylo zmíněno, že pojmy data a informace jsou často zaměňovány. Pro specialisty z oboru informatiky a pro manažery však mají tyto dva pojmy rozdílný význam.

*Údaje, **data**, jsou fakta, čísla, události, grafy, mapy, transakce atd., které byly zaznamenány. Jsou základním materiálem, surovinou pro informace.* [9]

Informace jsou údaje, které byly zpracovány do podoby užitečné pro příjemce. [9]

Údaje nebo také **data** jsou fakta získaná čtením, pozorováním, výpočtem, měřením, vážením, kreslením atd. Data, údaje chápeme jako:

- vyjádření faktů a poznatků ve formě, která je vhodná pro další zpracování;
- vyjádření skutečností a myšlenek v předepsané podobě tak, aby je bylo možné přenášet a zpracovávat;
- objektivní, sledovatelné vyjádření skutečností nebo znalostí na nějakém médiu tak, že je lze předávat. [9]



Obr. 5 Vztah mezi daty a informacemi

Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí stát nutně informací. Informací se totiž stanou teprve v okamžiku, kdy příjemci přinesou něco nového. Pojem data chápeme jako zkratkové profesionální označení pro čísla, text, zvuk,

obraz, popř. další smyslové vjemy atd. Tuto skutečnost lze schematicky vyjádřit vztahem množiny a podmnožiny.

2.1.1 **Druhy informací**

Tak jako rozlišujeme různé druhy čaje, zeleniny, koření, smluv, silnic tak i informace můžeme rozdělit na několik druhů. Dělení pak může vypadat následovně:

Z hlediska stability informačního obsahu:

- informace stálé (fixní) – trvale platné a využitelné pro rozhodování;
- informace proměnné;

Z historického hlediska se informace dělí:

- informace o minulosti (ex post);
- informace o budoucnosti (ex ante);

Dělení podle formy podání:

- ústní;
- písemné;

Dělení podle skladování:

- uchovávané;
- neuchovávané;

Dělení podle opakovatelnosti:

- jednorázové;
- nepravidelné;

Dělení podle oboru:

- ekonomické;
- technické;
- kriminalistické aj. [9]

2.1.2 **Vlastnosti informací**

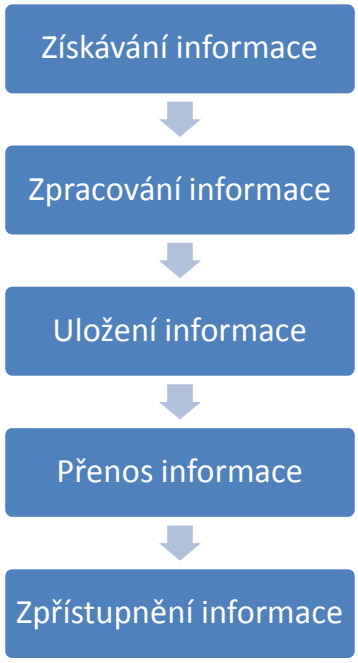
Každá informace by měla disponovat určitými vlastnostmi, které mají vliv na její vlastní kvalitu. Mezi nejdůležitější z nich pak patří následující:

1. *Relevance* – charakter informace by měl odpovídat charakteru jejího užití.

2. *Správnost* – informace by měla být pravdivá a spolehlivá. Měla by mít přijatelnou přesnost.
3. *Včasnost* – informace je třeba předávat v pravý čas, tj. v době jejich potřeby a užití. Důležitá rozhodnutí nelze dělat bez potřebných informací, nejsou-li k dispozici. Nemá však ani smysl naléhat na přehnaně rychlé poskytování informací, které nelze bezprostředně využít.
4. *Aktuálnost* – informace by měly co nejlépe odrážet aktuální skutečnost.
5. *Úplnost* – je třeba, aby byly k dispozici veškeré požadované informace, ne pouze některé z nich. Nedostatečná znalost v důsledku nekompletních informací je pro rozhodování velmi nebezpečná.
6. *Přiměřenost* – informace by měly být přiměřeně podrobné.
7. *Nákladová přiměřenost* – vyžaduje-li získání potřebné informace nepřiměřeně dlouhou dobu nebo nadměrné úsilí vzhledem k užitku, který poskytuje, nelze ji považovat za nákladově přiměřenou. [6]

2.1.3 Životní cyklus informace

Na následujícím obrázku je znázorněn životní cyklus informace. Jedná se o procesy od jejího získání až po její zpřístupnění.



Obr. 6 Životní cyklus informace

Prvním procesem je získávání informací. Zde je snaha o získání co nejvíce údajů a informací o daném tématu, problematice. Poté jsou naše informace zpracovávány (jedná

se o různé evidence, kategorizace, třídění, agregace a odvozování nových informací). Po zpracování přichází na řadu jejich uložení (zaznamenávání, shromažďování na nosiči apod.). To nám umožňuje v případě potřeby její další použití. Dalším procesem je realizace přenosu informace. Nakonec je informace zpřístupněna. To může být za použití jednoduchého zobrazení jejím tiskem apod.

2.2 Základní pojmy v informačních systémech

Informační systémy tvoří součást každé organizace. Informačně podporují realizaci řady procesů a celkově zajišťují uspokojování informačních potřeb příslušníků organizace. Výkonnostní vlastnosti informačních systémů byly a jsou podmíněny především úrovní použitých informačních technologií. Vývoj informačních systémů ovlivnilo několik historických mezníků, zvláště vznik písma, vynález papíru a knihtisku a vynález elektronických počítačů. V současné době jsou určujícím faktorem právě elektronické počítače, které významně zlepšují rychlostní, objemové, dostupnostní a prezentační vlastnosti informačních systémů. Digitalizace významně usnadnila pořizování a zpracování dat. [6]

Definice informačního systému (IS):

- IS je soubor lidí, metod a technických prostředků zajišťujících sběr, přenos, uchování a prezentaci dat s cílem tvorby a poskytování informací podle potřeb příjemců informací činných v systémech řízení. [6]
- Podle normy ČSN/ISO IEC 23821 je IS definován jako systém zpracování informací spolu s návaznými organizačními prostředky, např. personálem, technickými a funkčními prostředky; takový systém získává a distribuuje informace. [9]
- Účelové uspořádání vztahů a informačních toků mezi informačními zdroji, lidmi a technologickými prostředky spolu s procesy zpracování a komunikace informací. [18]

2.2.1 **Počítačově orientované informační systémy**

Jak již bylo v úvodu zmíněno, fenoménem dnešní doby jsou počítačově orientované informační systémy. Základem jsou počítače pracující samostatně nebo propojeny do počítačové sítě. Základními prvky počítačově orientovaných informačních systémů jsou:

- technické prostředky (hardware) - počítačové prostředky a systémy;

- programové prostředky (software) - systémové programy řídící činnost počítače, práci s daty, komunikaci počítačového systému s okolím a reálným světem a aplikační programy řešící požadované třídy uživatelských úloh;
- organizační prostředky (orgware) - soubor zásad, nařízení a pravidel definujících provozování a využívání informačního systému a informačních technologií;
- lidská složka (peopleware) - řešení problémů přizpůsobení a účinného fungování člověka v počítačovém prostředí. [6]

Výhody počítačově orientovaných informačních systémů:

- přenos dat elektronicky na libovolnou vzdálenost se zanedbatelným zpožděním, snadnost kopírování a archivace dat;
- schopnost zpracovávat velké objemy dat a získat informace ze širokého spektra zájmových oblastí;
- odezvy na informační požadavky v psychologicky přijatelných lhůtách;
- schopnost vytvářet nové způsoby procesních a pracovních postupů, založené na možnostech ICT;
- možnost prezentovat informace v obrazové, akustické a znakové formě, statickou nebo dynamickou scénou;
- snadná distribuce softwaru libovolnému počtu uživatelů;
- relativně nízké náklady na pořízení hardware. [6]

Nevýhody:

- obtížně specifikovatelné detailní požadavky na informační potřeby;
- složitý, časově dlouhý a nákladný proces návrhu, výstavby, inovace a provozu informačního systému;
- závislost fungování informačního systému na zdroji a dodávce elektrické energie;
- relativně krátký životní cyklus hardwaru a softwaru, způsobený agresivní marketingovou politikou výrobců ICT a krátkým inovačním cyklem ICT, morálním opotřebením;
- složitá informační podpora špatně strukturovaných problémů;
- závislost činnosti organizace na fungování informačního systému, na technologiích a počítačové gramotnosti personálu, riziko nadbytečnosti dat;
- nutnost ochrany v počítačových sítích. [6]

2.2.2 Klasické manuální informační systémy

I přes dnešní nadvládu počítačově orientovaných informačních systémů hrají nezastupitelnou roli v organizacích i klasické manuální informační systémy. Jsou vhodné zejména pro informační podporu jednotlivých pracovníků, kde se nevyžaduje práce v reálném čase.

Mezi jejich výhody pak můžeme zařadit:

- schopnost pracovat bez technických prostředků a zařízení;
- snadnost čtení, aktualizace i archivace;
- jednoduchost při přidělování oprávnění pracovat s tímto informačním systémem;
- snadná přeměna v postupu zpracování a vyřizování dokumentu. [6]

Nevýhody:

- v případě velkého množství dat obtížnější vyhledávání a zpracování údajů;
- pomalý přenos informací. [6]

2.2.3 Funkce informačního systému

Mezi základní funkce IS řadíme funkci pořizování, sběru, přenosu, zpracování, distribuce, prezentace a ochrany informací. Funkce jsou vymezeny následovně:

- **Pořizování** je účelově uskutečňované snímání údajů dané skutečnosti. Jedná se např. o určení polohy nepřátelského letadla pomocí radiolokátoru, automaticky sledované množství spotřebované munice zbraňového systému, nebo snímání a digitalizaci otisku prstů.
- **Sběr** představuje časově a systémově uspořádané shromažďování údajů umožňující jejich zpracování. Systém sběru dat určuje např. do jakých databází, případně aplikací zpracování dat mají být údaje o otisku prstu.
- **Přenos** se chápe jako přemisťování informací mezi fyzicky oddělenými místy, zpravidla se realizuje šířením signálů nesoucích dané údaje. Funkce vyjadřuje, jaký komunikační systém zajišťuje přenos pořízených dat, jde-li o přenos off-line převozem datového média, nebo on-line pomocí sítě přenosu dat.
- **Zpracování informací** představuje proces třídění, filtrování a slučování údajů, vymezení informačních významů, uskutečňovaný účelově s cílem vytvořit obraz vyžadované skutečnosti. Funkce je zpravidla realizována aplikacemi IS, např.

srovnáním identifikačních dat nově pořízeného otisku s daty otisků prstů uložených v databázi.

- **Distribuce** je funkce zajišťující výdej zpracovaných informací oprávněným příjemcům. Distribuce zajišťuje předání výsledků zpracování dat uživatelům, kteří informaci využívají ke své činnosti. Např. komu bude výsledek otisků předán.
- **Prezentace** zajišťuje příjemcům zobrazení informací ve srozumitelné formě. Funkce prezentace určuje formu zobrazení, např. textovou zprávu, grafické zobrazení s využitím symbolů, případně multimediální prezentaci integrující vizuální a zvukovou prezentaci.
- **Ochrana** představuje zajištění přístupu k informacím pouze oprávněným subjektům. Bezpečnost informací se stává novým důležitým oborem. [6]

2.2.4 Členění informačních systémů

Stejně jako systém, tak i IS má svou strukturu a chování. V rámci struktury IS členíme IS podle různých hledisek.

1. ***Podle zdrojů informací***
   - informace vnější – přicházejí do systému z okolí;
   - informace vnitřní – tok informací je omezen hranicemi systému a lze je dělit dle směru pohybu na vertikální a horizontální.
2. ***Podle vztahu k procesu řízení***
   - direktivní – jedná se o pokyny ke konkrétní činnosti nebo o pokyny obecného charakteru;
   - metodické – jde o zobecněné zkušenosti a sjednocování výkladu přepisů, zákonu, směrnic;
   - sdělovací, konkrétní informace k předmětům zájmu.
3. ***Ve vztahu k místu uložení***
   - banky dat systému – evidence, archivy apod.;
   - vlastní vnitřní paměť pracovníků – vlastní zkušenosti, vzpomínky apod.
4. ***Podle nositele dat***
   - klasické noviny, časopisy, patenty, výzkumné zprávy, normy, knihy apod.;
   - elektronické banky dat počítačů, sítí, zejména internet.
5. ***Podle věcného obsahu***
   - bibliografické;

- referenční, odkazují na určitá fakta, instituce, osoby, události, vztahují se k určité problematice;
- faktografické.

6. ***Podle příjemce informací***
   - zpracovatelé přepracovávají informace do podoby využitelné zejména řídícími subjekty, ale i objekty ke správnému výkonu v podobě direktivní či metodické informace sdělené manažerem;
   - uživatelé, vykonavatelé využívající informaci ke konkrétnímu účelu podle charakteru činnosti. [9]

2.3 Shrnutí

Základním kamenem pro správnou činnost manažera organizace jsou bezesporu informace. Aby bylo rozhodování manažerů co nejlepší a co nejprospěšnější celé organizaci, je dobré, aby informace, se kterými pracuje manažer, bylyrelevantní, správné, včasné a aktuální.

Elektronické informační systémy jsou důležitým zdrojem informací, jejich absence v organizacích by v dnešní „elektronické době“ hodně ztěžovala chod dané organizace. Důležité jsou především pro manažery. Je to jejich informační podpora (vyhledávání, zpracování a prezentace informací). Manažer totiž účelově shromažďuje, či vybírá vhodné informace (data), které svými myšlenkovými procesy transformuje tak, aby uspokojil svoji informační potřebu, spojenou s řešením určitého problému. Říká se, že manažer až 80 % svého času spotřebuje získáváním, předáváním informací. Proto je důležité mít informační systémy, které by mu tuto práci usnadnily (úspora jeho času).

3 ANALÝZA INFORMAČNÍCH POTŘEB BEZPEČNOSTNÍCH MANAŽERŮ

3.1 Vymezení informační potřeby

I když jsme kvalifikovanou osobou na konkrétní pracovní pozici, neobejdeme se při výkonu pracovní činnosti bez dalších informací. Tyto informace pak můžeme nazvat našimi informačními potřebami. Informační potřebou pak rozumíme stav, ve kterém chceme získat informace, které nám přispějí k řešení našich problémů nebo úkolů (dosažení stanoveného cíle).

Terminologický informatický slovník definuje informační potřebu jako stav nebo vlastnost určité osoby, kolektivu nebo systému vyjadřující nevyhnutelnost získání informace související s charakterem vykonávané činnosti nebo práce.

Informační potřeby můžeme rozdělit:

- **osobní informační potřeby;**
- **profesní informační potřeby.**

Osobní informační potřeby jsou praktické informace k řešení každodenních problémů. Týkají se např. rodiny a domácnosti, volného času, práce (ale pouze co se týká např. nabídky míst, právního poradenství apod.), krizových situací (vážná nemoc, rozvod atd.). Některé z těchto informačních potřeb mohou zajistit veřejné knihovny, ale většinou jsou uspokojovány konzultacemi s odborníky (lékaři, učiteli, sociálními pracovníky atd.). Druhou skupinou informačních potřeb jsou již zmiňované profesní informační potřeby. To jsou potřeby odborných informací, které se vztahují přímo k práci, k profesi člověka. Mezi lidi, kteří velice často chtějí uspokojit své informační potřeby, patří bezesporu manažeři organizací, podniků, firem. Manažeři totiž dennodenně řeší spoustu problémů a ke správnému rozhodnutí shromažďují či vybírají vhodná data a informace.

3.2 Informační potřeby bezpečnostních manažerů

S pojmem bezpečnostní manažer jsme se již seznámili v první kapitole. Byla tam zmíněna i jeho pracovní náplň. Z pracovní činnosti manažerů pak můžeme analyzovat a určit jeho informační potřeby. Jak již bylo zmíněno, bezpečnostní management můžeme rozdělit po tradičních bezpečnostních odbornostech – úsek požární ochrany, bezpečnost a ochrana zdraví při práci, ostraha a bezpečnostní technologie, bezpečnost informačních systémů,

ochrana utajovaných informací, ochrana osobních údajů atd. V čele takto vymezených rámců pak působí osoby plnící roli bezpečnostního manažera. Každý z nich se tedy zabývá jinou oblastí bezpečnosti. V další části kapitoly budou analyzovány vybrané informační potřeby, které jednotliví bezpečnostní manažeři potřebují a přicházejí s nimi do styku.

3.2.1 **Bezpečnost a ochrana zdraví při práci**

V každé organizaci by nejen mělo, ale musí být dbáno na bezpečnost a ochranu zdraví při práci (dále jen BOZP). Vyplývá to ze zásadního právního předpisu, kterým je zákon *č. 262/2006 Sb.* (zákoník práce). Tento zákon, konkrétně jeho ČÁST PÁTÁ zavazuje zaměstnavatele k povinnosti zajistit BOZP zaměstnanců při práci s ohledem na rizika možného ohrožení jejich života a zdraví, která se výkonu práce týkají. Zmíněná část zákoníku práce upravuje:

- předcházení ohrožení života a zdraví při práci;
- povinnosti zaměstnavatele, práva a povinnosti zaměstnance;
- účast zaměstnanců na řešení otázek BOZP.

Jsou zde podrobněji rozepsány nejen povinnosti zaměstnavatele vůči svým zaměstnancům, ale i práva a povinnosti samotných zaměstnanců. Mezi povinnosti zaměstnavatelů řadíme zejména:

- vytváření bezpečného a zdraví neohrožujícího pracovního prostředí;
- vyhledávání nebezpečných činitelů a procesů pracovního prostředí a pracovních podmínek, zjišťování jejich příčin a zdrojů;
- zajištění zaměstnancům poskytnutí první pomoci;
- zajištění školení o právních a ostatních předpisech k BOZP;
- poskytnutí ochranných pomůcek, mycích a dezinfekčních prostředků.

Z důvodu rozdílnosti organizací se bude BOZP lišit. Jiná situace bude ve slévárenské organizaci, jiná bude v organizaci zabývající se informačními technologiemi. Pracovníci, kteří budou mít tuto problematiku na starost, ale budou postupovat ve všech organizacích podobně. Vždy si nejprve budou muset zjistit a uvědomit, jaké pracovní pozice jejich organizace nabízí a podle toho budou identifikovat a hodnotit jejich pracovní rizika. Dále pak budou zpracovávat dokumentaci BOZP pro dané prostředí. Vycházet přitom budou i z organizačních směrnic a provozních řádů organizace. Důležitým bodem poté bude

vstupní, posléze i periodické školení zaměstnanců a jejich seznámení nejen s riziky, která se mohou v jejich pracovním procesu vyskytnout, ale i s postupem v případě vzniku úrazu.

Manažer tedy musí znát samotnou činnost organizace. Bez toho by nemohl kvalifikovaně provádět školení nových, ale i stávajících zaměstnanců. Důležitou znalostí bude znalost nabízených pracovních pozic, ze kterých budou vyplývat jeho další informační potřeby (např. bude-li představovat novému zaměstnanci pracovní pozici, musí ho seznámit s pracovním postupem, předepsanými ochrannými prostředky, zákazy některých činností při práci apod.).

Obr. 7 Ochranné pomůcky

Mezi další dokumenty, související s BOZP, můžeme zařadit např. nařízení vlády *č. 201/2010Sb.* o způsobu evidence úrazů, hlášení a zasílání záznamu o úrazu. V tomto nařízení vlády je stanoveno, že každý zaměstnavatel musí vést evidenci úrazů a další požadavky spojené s pracovními úrazy (hlášení, zasílání záznamu o úrazu). Evidence může být v elektronické nebo listinné podobě a je nazývána knihou úrazů.

Většina organizací využívá ke své pracovní činnosti auta. K této problematice se vztahuje nařízení vlády *č. 168/2002 Sb.* kterým se stanoví způsob organizace práce a pracovních postupů, které je zaměstnavatel povinen zajistit při provozování dopravy dopravními prostředky.

Manažeři zabývající se BOZP jsou povinni sledovat ostatní nově vydané zákony, technické normy a jiné dokumenty související s BOZP a související s činnostmi organizace, které jsou důležité pro zajištění správného chodu organizace (např. různá nařízení vlády – o bližších požadavcích na BOZP při práci na pracovištích s nebezpečím pádu z výšky, do hloubky, při práci v prostředí s nebezpečím výbuchu; o podrobnějších požadavcích

na pracoviště a pracovní prostředí; o stanovení vzhledu a umístění bezpečnostních značek a zavedení signálů, o stanovení bližších požadavků na bezpečný provoz a používání strojů, technických zařízení, přístrojů a nářadí; apod.). V dnešní době je taky zvykem najímat si na BOZP a všechno co se této problematiky týká, externí organizaci.

Základní informace bezpečnostních manažerů na úseku BOZP:

- informace o nabízených pracovních pozicích organizace;
- informace o pracovním prostředí;
- informace o rizicích na pracovišti;
- informace o pracovních postupech;
- informace o odvozu do nemocnice;
- traumatologické informace;
- informace o strojích, zařízeních, nástrojích;
- informace o ochranných pomůckách, mycích a dezinfekčních prostředcích;
- informace o poskytování první pomoci;
- informace o školení – kdy a jak často školit;
- informace o způsobu evidence úrazů – hlášení, zápis, zasílání záznamů úrazu;
- informace o organizaci práce a pracovních postupů souvisejících s provozováním dopravních prostředků a dopravy v organizaci;
- informace o bezpečnostních značkách – druhy, umístění;
- kontakty např. na dodavatele ochranných pomůcek, mycích a dezinfekčních prostředků, na jiné firmy poskytující služby v oblasti BOZP.

3.2.2 Bezpečnost na úseku požární ochrany

Dalším důležitým článkem dobře fungující organizace je zajištění ochrany života a zdraví osob a majetku před požáry. Manažer pracující v této oblasti se podílí na navrhování způsobu zajištění požární ochrany (PO) na pracovištích a podílí se na realizaci vnitropodnikových předpisů. Dále se podílí na prevenci a školení související s PO a v neposlední řadě taky kontroluje dodržování předpisů. Jeho nosným informačním zdrojem je v tomto případě zákon *č. 133/1985 Sb.* zákon o požární ochraně.

Další informační potřebou bude beze sporu vyhláška *č. 246/2001 Sb.* o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci). V této vyhlášce se mimo jiné hovoří o:

- vybavení prostor právnických osob a podnikajících fyzických osob věcnými prostředky požární ochrany a požárně bezpečnostními zařízeními;
- způsobu vytváření podmínek pro hašení požárů a pro záchranné práce;
- lhůtě a způsobu provádění pravidelných kontrol dodržování předpisů o PO;
- druhu, obsahu a vedení dokumentace PO.

Další znalosti, kterými bude muset disponovat manažer zabývající se problematikou PO:

- znalost nebezpečných látek, hořlavých látek, přípravků a plynů, s nimiž je možné se setkat v organizaci;
- znalost hasících prostředků a jejich způsobu použití;
- znalost značek, příkazů, zákazů a pokynů ve vztahu k požární ochraně (např. ČSN ISO 3864 Bezpečnostní barvy a bezpečnostní značky, ČSN 01 8013 Požární tabulky);
- znalost požárně bezpečnostního zařízení instalovaného v organizaci a příslušných norem (např. ČSN 73 0802 Požární bezpečnost staveb – nevýrobní objekty, ČSN 73 0804 Požární bezpečnost staveb – výrobní objekty, ČSN 73 0875 Požární bezpečnost staveb – navrhování elektrické požární signalizace aj.).

Obr. 8 Hasicí přístroje

Základní informace bezpečnostních manažerů na úseku PO:

- informace o nebezpečných, hořlavých látkách, přípravcích a plynech, s nimiž je možné se setkat v organizaci;
- informace o skladování těchto látek;
- informace o hasících prostředcích;

- informace o podnikovém HZS;
- informace o plánování PO;
- informace o únikové cestě;
- informace používání značek, příkazů a zákazů ve vztahu k požární ochraně;
- informace o rozmístění hasicích přístrojů a hydrantů;
- informace o požárním bezpečnostním zařízení instalovaným v organizaci;
- informace o způsobu vytváření podmínek pro hašení požárů a pro záchranné práce.

3.2.3 **Prevence závažných průmyslových havárií**

Pokud se jedná o organizaci, která se zabývá výrobou, skladováním a užíváním nebezpečných látek, bude jedním ze zdrojů informací pro bezpečnostního manažera této organizace zákon *č. 59/2006 Sb.* zákon o prevenci závažných průmyslových havárií způsobených vybranými chemickými látkami nebo chemickými přípravky. Tento zákon ukládá povinnosti organizaci (provozovateli) začlenit svůj objekt nebo zařízení, ve kterém se pracuje s nebezpečnými látkami, do skupiny A nebo skupiny B a to podle množství nebezpečných látek a zpracovat bezpečnostní program nebo bezpečnostní zprávu. Důležitým zdrojem informací v souvislosti s prevencí závažných havárií jsou bezpečnostní listy vytvářené podle nařízení Evropského parlamentu a Rady (ES) č. 1907/2006. Bezpečnostní listy se skládají zpravidla z následujících údajů:

- identifikace látky nebo přípravku;
- identifikace organizace, podniku;
- identifikace nebezpečnosti;
- složení a informace o jednotlivých složkách;
- pokynů pro první pomoc;
- opatření pro hašení požáru;
- opatření při náhodném úniku;
- fyzikálních a chemických vlastností látek;
- informace pro přepravu.

Tyto body jsou v bezpečnostním listě podrobněji rozepsány, takže při práci s tímto listem je danému člověku hned patrné, co všechno smí a nesmí s danou látkou, přípravkem dělat a jak se chovat v případě jeho úniku.

Základní informace bezpečnostních manažerů na úseku prevence závažných průmyslových havárií:

- informace o množství nebezpečných látek v organizaci;
- informace o složení nebezpečných látek;
- informace o skladování nebezpečných látek;
- informace o poskytování první pomoci při styku s nebezpečnou látkou;
- informace o přepravě;
- informace o způsobu hašení těchto látek;
- kontakty např. na dodavatele, odběratele, hasiče, zdravotní záchrannou službu.

3.2.4 **Krizové řízení**

Každá organizace a především její vedení by nemělo zapomínat na další oblast bezpečnosti, do které nepochybně patří krizové řízení a všechno, co je s ním spojeno.

Tato oblast je upravena především zákonem *č. 240/2000 Sb.* o krizovém řízení a o změně některých zákonů (krizový zákon). Zákon stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávných celků a **práva a povinnosti právnických a fyzických osob** při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením a při jejich řešení.

Dalším důležitým zákonem v této oblasti je zákon *č. 239/2000 Sb.* o integrovaném záchranném systému a o změně některých předpisů. Tento zákon vymezuje integrovaný záchranný systém, stanoví složky integrovaného záchranného systému a jejich působnost, pokud tak nestanoví zvláštní právní předpis, působnost a pravomoc státních orgánů a orgánů územních samosprávných celků, **práva a povinnosti právnických a fyzických osob** při přípravě na mimořádné události a při záchranných a likvidačních pracích a při ochraně obyvatelstva před a po dobu vyhlášení stavu nebezpečí, nouzového stavu, stavu ohrožení státu a válečného stavu (dále jen "krizové stavy").

V neposlední řadě krizové řízení upravuje i zákon *č. 241/2000 Sb.* zákon o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů. Tento zákon upravuje přípravu hospodářských opatření pro stav nebezpečí, nouzový stav, stav ohrožení státu a válečný stav (dále jen "krizové stavy") a přijetí hospodářských opatření po vyhlášení krizových stavů. Zákon rovněž stanoví pravomoc vlády a správních úřadů při přípravě a přijetí hospodářských opatření pro krizové stavy. Stanoví též **práva**

a povinnosti fyzických a právnických osob při přípravě a přijetí hospodářských opatření pro krizové stavy.

Výše uvedené zákony obsahují práva a povinnosti právnických a fyzických osob ať už při přípravě na mimořádné události, na krizové situace tak i při přípravě a přijetí hospodářských opatření pro krizové stavy. Proto by se měly tyto zákony objevit mezi informačními potřebami bezpečnostních manažerů organizací.

Základní informace pro výkon práce v oblasti krizového řízení

- informace o možných rizicích spojených s činností organizace;
- informace o zpracování havarijního plánu a plánu krizové připravenosti;
- informace o tom, jak čelit haváriím, které mohou vzniknout v organizaci;
- informace o haváriích vzniklých v dřívější době v objektu organizace;
- informace o možnosti vzniku havárií zapříčiněné přírodními živly;
- geografické informace;
- kontakty na správní úřady a subjekty zúčastňující se zneškodňování havárií např. na hasičský záchranný sbor, na krajský úřad, apod.

3.2.5 Fyzická bezpečnost

Pojem ***fyzická bezpečnost*** v sobě zahrnuje nejenom fyzickou ostrahu majetku a osob, ale i technické zabezpečení a organizační a režimová opatření. Největší nároky z hlediska informací budou kladeny především na technické zabezpečení. Je to dáno tím, že v dnešní době již existuje celá řada nových technologií, systémů a zařízení. Jejich výběr a práce s nimi klade větší nároky na odbornou znalost, ale i na sledování nových výrobků a standardů.

Obr. 9 Dělení fyzické bezpečnosti

Fyzická ostraha

Fyzická ostraha, pokud ji daná organizace má, je většinou ve všech organizacích vykonávána externí organizací (soukromou bezpečnostní službou). To, zda bude chtít daná organizace zabezpečit ochranu osob a majetku pomocí fyzické ostrahy, záleží na vyhodnocení bezpečnostního manažera, který má na starost fyzickou bezpečnost. Všeobecně platí, že fyzická ostraha patří k nejstarším službám poskytující činnosti k zajištění ochrany osob a majetku. Fyzická ostraha může probíhat:

- nepřetržitě – tato ostraha probíhá 24 hodin denně;
- nárazově – probíhá jen podle domluvy se zákazníkem;
- v závislosti na pracovní době hlídané organizace – je vykonávána pouze v pracovní době organizace.

Tato ochrana pak může být nabízena ve formě následujících služeb soukromou bezpečnostní službou (dále jen SBS):

1. Strážní služba

Pracovník SBS má na starost střežení objektů zákazníků před vniknutím cizích osob s úmyslem krádeže, poškození nebo jinými nezákonnými úmysly. Mezi hlavní úkoly strážní služby patří ochrana zařízení a osob pracujících v objektu. Dále se pracovník SBS zabývá pozorováním přilehlého okolí objektu, kde sleduje, zda nedochází k nedovoleným činnostem. Dále se může zabývat ochranou cenností, informací a peněžní hotovostí.

2. Bezpečnostní dohled

Bezpečnostní dohled můžeme rozdělit na přímý, který je konaný pracovníkem SBS a dálkový, který je konaný pracovníkem SBS za využití monitorovacích systémů s fyzickým výjezdem k místu události.

Bezpečnostním dohledem zajišťuje pracovník SBS vnitřní ochranu objektu či prostoru, kde především kontroluje oprávněnost pohybu a činnosti osob v objektech, dodržování stanoveného vnitřního režimu, doprovází cizí osoby po objektu, uzavírá a uzamyká svěřené objekty.

3. Bezpečnostní ochranný doprovod

Zde se jedná o činnost SBS zajišťující ochranný doprovod majetku a osob při přesunech. Cílem je zajistit bezpečný doprovod zásilky včetně osob zákazníků, kteří ji doprovází, za využití obranných opatření, které umožňuje zákon a nepřipustit odcizení či poškození

zásilky a zajistit ochranu života a zdraví doprovázejících osob zákazníka. Bezpečnostní ochranný doprovod můžeme rozdělit:

- bezpečnostní ochranný doprovod osob;
- bezpečnostní ochranný doprovod peněžních hotovostí a cenností;
- bezpečnostní ochranný doprovod kamionové přepravy. [5]

4. Kontrolní propustková činnost

Kontrolní propustková služba slouží ke kontrole osob a vozidel při vstupu a výstupu do ochranných prostorů či objektů. Cílem je chránit majetek, osoby a informace. Kontrola probíhá pomocí fyzické i technické ostrahy. Pracovník kontrolní propustkové služby zpravidla vykonává následující úkoly:

- kontroluje vstup a výstup osob a vjezd a výjezd vozidel;
- kontroluje přicházející a odcházející osoby;
- zamezuje vstupu a vjezdu neoprávněných osob a vozidel;
- poskytuje informace návštěvníkům objektu v potřebném rozsahu;
- vede potřebnou a stanovenou režimovou dokumentaci;
- plní vrátnou službu včetně odemykání a zamykání objektu;
- plní další úkoly dle pokynů a požadavků zákazníka.

Obr. 10 Kontrolní propustková služba

Každý manažer vytvoří vlastní směrnice, kde bude stanoveno, jakou formou bude poskytována fyzická ostraha organizace. Pro správné nastavení a vytvoření směrnic o fyzické ostraze se bude muset orientovat v předchozích službách SBS. Další informační podklady potřebné pro vytvoření a nastavení směrnic pro fyzickou ostrahu představují informace o střeženém objektu (poloha, velikost, počet budov, vchodů, možná místa

vniknutí do objektu), informace o zaměstnancích a jiných osobách, u nichž je pravděpodobnost pohybu uvnitř objektu (uklízečky, dodavatelé, aj.), informace o pracovní době, informace o vozidlech (která vozidla mají povolen vjezd do objektu – ředitelé, dodavatelé apod.).

Technické zabezpečení

Technické zabezpečení tvoří další část fyzické bezpečnosti organizace. Technické zabezpečení zajišťuje ochranu organizace za využití mechanických, elektronických a speciálních technických prvků. V dnešní době již existuje nepřeberné množství technických prvků od různých výrobců.

Mechanické prvky, neboli mechanické zábranné systémy (MZS, nám pomáhají zamezit nebo znesnadnit přístup do chráněného objektu, nebo ke chráněné osobě. Tyto systémy rozdělujeme na MZS:

- obvodové ochrany;
- plášťové ochrany;
- předmětové ochrany.

Mezi MZS obvodové ochrany patří všechny klasické a bezpečnostní oplocení, vrcholové zábrany, podhrabové překážky, brány, závory, hřebenové bariéry, zastavovací pásy, průjezdové retardéry, turnikety a jiné bezpečnostní propusti.

Obr. 11 Bezpečnostní mříž

Mezi MZS plášťové ochrany pak řadíme otvorové výplně, okna a balkónové dveře, mříže, rolety, žaluzie, bezpečnostní a ochranné fólie, bezpečnostní skla, bezpečnostní dveře,

bezpečnostní kování, cylindrické vložky, přídavné zámky, dveřní pojistné řetízky, dveřní zastavovače a jiné bezpečnostní systémy k zamykání.

Mezi MZS předmětové ochrany patří komorové trezory, komerčně úschovné objekty, skříňové trezory, trezorové skříně, ohnivzdorné skříně, účelové trezory, vestavěné trezory, trezory na zbraně, příruční pokladničky a manipulační schránky.

Po mechanických prvcích může být technická ochrana dále zajišťována pomocí prvků elektronických:

- poplachové zabezpečovací a tísňové systémy;
- sledovací systémy pro použití v bezpečnostních aplikacích;
- systémy kontroly vstupů pro použití v bezpečnostních aplikacích;
- elektrická požární signalizace;
- biometrické identifikační systémy;
- elektronická ochrana zboží;
- průmyslová havarijní signalizace;
- satelitní vyhledávání vozidel.

Jak již bylo zmíněno, bezpečnostní manažer zabývající se problematikou technického zabezpečení, bude potřebovat ke své práci množství znalostí a informací. Tento manažer má především na starost zpracování nebo zajištění analýzy bezpečnostních rizik, bezpečnostního posouzení objektu, vyjadřuje se k projektové dokumentaci zabezpečovací techniky a kontroluje realizaci systémů technického zabezpečení a dbá na její provozuschopnost.

Informace a znalosti potřebné pro výkon práce bude bezpečnostní manažer čerpat jednak z technických norem v oblasti ochrany majetku, osob a informací (např. normy týkající se poplachových systémů - ČSN EN 50 130, 50 131…, komentáře k technické normě ČSN CLC/TS 50 131-7 týkající se návrhu, montáže, prohlídky a zkoušky poplachových zabezpečovacích a tísňových systémů, aj.), dále to jsou informace o provádění kontrol a servisu bezpečnostních systémů, informace o kontaktech na dodavatele a zhotovovatele bezpečnostních systémů, informace a znalosti o používaných bezpečnostních technologiích.

Organizační a režimová opatření

Poslední část fyzické bezpečnosti tvoří organizační a režimová opatření. Je to důležitý článek celé fyzické bezpečnosti. Bez těchto opatření nemůže být funkční fyzická ostraha ani technické zabezpečení. V řadě organizací je tato problematika podceňována. Cílem je zpracování provozních řádů, zásady chování při mimořádných událostech, provádění kontrol zda jsou dodržovány stanovená opatření a v neposlední řadě provádění školení zaměřené na organizační a režimová opatření.

Základní informace bezpečnostních manažerů na úseku fyzické bezpečnosti organizace:

- informace o objektech organizace;
- informace o zaměstnancích a jiných osobách, u nichž je pravděpodobnost pohybu uvnitř objektu;
- informace o režimových opatřeních organizace;
- informace o pracovní době;
- informace o vozidlech oprávněných ke vjezdu do organizace;
- informace týkající se návrhu a montáže poplachových zabezpečovacích a tísňových systémů;
- informace o používaných bezpečnostních systémech;
- informace o provádění kontrol bezpečnostních systémů;
- kontakty např. na dodavatele a zhotovitele bezpečnostních systémů, na poskytovatele fyzické ostrahy apod.

3.2.6 Informační bezpečnost

Dříve byl důraz na ochranu informací (ztráta, zneužití, záměna) kladen především v armádě, policii a ve významných organizacích. V současné době se dbá na ochranu informací již ve všech organizacích.

Informační bezpečnost představuje zajištění důvěrnosti, integrity a dostupnosti informací. Důvěrnost znamená zajištění přístupu k informacím pouze uživateli s potřebným oprávněním. Integrita pak obnáší zajištění správnosti a úplnosti informací. A dostupnost znamená, že oprávnění uživatelé mají přístup k informacím tehdy, kdy potřebují.

Dohled a správu informací a informačních systémů a jejich bezpečnost bude mít na starost bezpečnostní manažer organizace, který za pomocí svých podřízených pracujících v oblasti

informatiky bude dbát na zajištění bezpečného a oprávněného přístupu k informacím, provádění analýzy rizik informačních systémů, poskytování odborné pomocí týkající se informačních systémů organizace, dodržování norem a legislativy týkající se informací a informačních systémů, sledování novinek v oblasti informační bezpečnosti, zajišťování vzdělávání a školení o informační bezpečnosti, řešení bezpečnostních incidentů spojených s informační bezpečností.

Tento bezpečnostní manažer bude muset být vybaven znalostmi týkajícími se práce s počítačem a jeho příslušenstvím. Musí mít znalost informačních systémů organizace, mít informace o přihlašování do systémů a používání hesel, informace o programech a licencích, musí mít také kontakty na dodavatele a servisní služby starající se o software či hardware organizace, informace o novinkách na trhu v oblasti informačních a komunikačních zařízení a v neposlední řadě taky znalost a orientace v normách (např. ČSN ISO/IEC TR 13335-1 Informační technologie – směrnice pro řízení bezpečnosti IT) a v legislativě viz následující zákony:

- zákon č. 412/2005 Sb. zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti;
- zákon č. 101/2000 Sb. o ochraně osobních údajů.

Ochrana utajovaných informací

V organizaci je možné se setkat s informacemi, se kterými by neměl nakládat každý. Kdo a jak může zacházet s informacemi, které by mohly způsobit újmu zájmu České republiky, nebo mohou být pro tento zájem nevýhodné, je stanoveno v zákoně *č. 412/2005 Sb*. zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. Je zde specifikována ochrana informací podle konkrétně vymezeného stupně utajení (vyhrazené, důvěrně, tajné, přísně tajné) a druhy zajištění ochrany utajovaných informací (personální, průmyslová, administrativní a fyzická bezpečnost, bezpečnosti informačních nebo komunikačních systémů a kryptografická ochrana).

Stupně utajení

Utajovaná informace se stupněm utajení *vyhrazené* znamená, že její vyzrazení nebo zneužití může být nevýhodné pro zájmy České republiky. Se stupněm utajení *důvěrné* může způsobit její vyzrazení nebo zneužití prostou újmu zájmům České republiky. Stupeň *tajné* a *přísně tajné* pak způsobuje vážnou, respektive mimořádně vážnou újmu zájmům České republiky v případě jejího vyzrazení či zneužití.

Druhy zajištění ochrany utajovaných informací

Jak již bylo nastíněno, ochrana utajovaných informací je zajišťována:

a) **personální bezpečností,** kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana;
b) **průmyslovou bezpečností**, kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem;
c) **administrativní bezpečností**, kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi;
d) **fyzickou bezpečností**, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat;
e) **bezpečností informačních nebo komunikačních systémů**, kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému;
f) **kryptografickou ochranou**, kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací. [13]

Ochrana osobních údajů

V dnešní době se často setkáváme s problémem ochrany osobních údajů. Již několikrát jsme se mohli z televizních nebo rozhlasových prostředků doslechnout o tom, že ta či ona organizace neoprávněně zveřejňovala a nakládala se soukromými daty. To, jaká má práva a povinnosti při zpracování a zacházení s osobními údaji, je stanoveno v zákoně *č. 101/2000 Sb.* o ochraně osobních údajů.

Základní informace bezpečnostních manažerů na úseku informační bezpečnosti:

- informace o informačních systémech organizace;
- informace o přihlašování do systému a používání hesel;
- informace o přístupových oprávněních zaměstnanců;
- informace o programech a licencích;

- informace o tom, zda se nachází v organizaci utajované informace;
- informace o zpracování a zacházení s osobními údaji;
- informace o vzniklých bezpečnostních incidentech týkajících se informační bezpečnosti;
- informace o provádění školení;
- kontakty např. na dodavatele starající se o software či hardware organizace.

3.3 Shrnutí

Každý z nás se dennodenně dozvídá spoustu informací. Některým nevěnujeme takovou pozornost a na jiné přímo čekáme. Tyto informace jsou pro nás nějakým způsobem důležité a potřebné pro naši další práci nebo jen proto, abychom uspokojili svou osobní informační potřebu. V této kapitole jsem se zaměřil na vybrané informační potřeby bezpečnostních manažerů organizací. Jednotlivé organizace jsou různorodé a jinak zaměřené, ale kostra informačních potřeb bezpečnostních manažerů bude velice podobná. Základními informačními potřebami bezpečnostních manažerů budou platné právní předpisy, kde můžeme zařadit především legislativu spojenou s BOZP, PO, ochranou utajovaných informací, ochranou osobních údajů a krizového řízení. Další informační potřeby vychází z problematiky, kterou se bezpečnostní manažer zabývá. Jedná se o různé kontakty, informace a znalosti různých programů a zařízení, informace o prováděných kontrolách v organizaci, informace o organizaci a zaměstnancích, technické normy, přehled v bezpečnostních technologiích, metodách a nástrojích, aj.

4 ANALÝZA TECHNICKÝCH PROSTŘEDKŮ A SOFTWAROVÝCH NÁSTROJŮ PRO ZAJIŠTĚNÍ INFORMAČNÍ PODPORY BEZPEČNOSTNÍHO MANAŽERA

V dnešní době informačních a telekomunikačních prostředků je téměř nemožné, aby bezpečnostní manažer nevyužíval alespoň některé z technických zařízení dnešní doby. V této kapitole se v první části zmíním o technických prostředcích, systémech a softwaru využívaného bezpečnostním manažerem za účelem zajištění informační podpory. V druhé časti kapitoly bude představen specializovaný software.

4.1 Technické prostředky a systémy

Technické prostředky a systémy umožní bezpečnostnímu manažerovi snadnější a efektivnější práci. Existuje celá řada těchto technických prostředků a systémů. Mezi nejčastěji využívané pak můžeme zařadit následující:

- počítač;
- mobilní telefon;
- datový projektor;
- kancelářský softwarový balík;
- intranet;
- internet.

4.1.1 **Počítač**

Osobní počítač

Mezi základní technický prostředek využívaný bezpečnostním manažerem bude bezesporu osobní počítač (PC) a jeho součásti (hardware a software). Vývoj PC a celé výpočetní techniky doznal za několik posledních let velkého růstu a rozmachu. V dnešní době jsou již k dispozici vysoce kvalitní PC. Kostru každého PC tvoří (jeho hardware):

- počítačová skříň (základní deska, procesor, operační paměť, pevný disk, napájecí zdroj, grafická, síťová a zvuková karta, mechanika DVD nebo CD-ROM…);
- monitor;
- počítačová klávesnice;
- počítačová myš;
- další vstupní-výstupní zařízení (tiskárna, scanner, reproduktory…).

Obr. 12 Osobní počítač

Samotný hardware k provozu počítače nestačí. Je potřeba ještě software, který řeší konkrétní úlohy ve spolupráci s uživatelem. Základním softwarem PC bývá operační systém, který zpřístupňuje hardware PC aplikačním programům. Dále existuje řada různých softwarů (viz. níže), pomocí nichž jsme schopni lépe či hůře zrealizovat naše úkoly a plány.

Notebook

Obdobou PC je notebook (přenosný počítač). Slouží ke stejným účelům jako PC. Taky jeho hardware je stejný jako u PC s tím rozdílem, že je minimalizovaný a přizpůsobený jeho fyzickým rozměrům. Jeho nesmírnou výhodou je mobilnost. Bezpečnostní manažer je tedy schopen pracovat nejen ve své kanceláři, ale i mimo ni.

4.1.2 **Mobilní telefon**

Stejně tak jako PC, tak i mobilní telefony poslední dobou zaznamenaly obrovský rozvoj. První mobilní telefony byly využívány především k volání a psaní krátkých textových zpráv. Dnes již pomocí mobilních telefonů jsme schopni běžně poslouchat rádio, fotografovat, nahrávat video, posílat e-maily, být připojeni k internetu a využívat jiné aplikace. Dnes jsou mobilní telefony také opatřeny operačním systémem podobně jako PC. Díky operačním systémům v mobilních telefonech je umožněna uživateli instalace dalších různých druhů aplikací, které může využít ke své práci.

Obr. 13 Mobilní telefon

Bezpečnostní manažer bude mobilní telefon využívat nejen k volání či k využívání textových zpráv, ale zajisté kladně ohodnotí přístup pomocí tohoto zařízení i k internetu. To mu umožní rychlý přístup k získání informací, které požaduje, téměř odkudkoliv. Další uplatnění nalezne ve využití kancelářských aplikací přímo v mobilním telefonu. Jedná se o aplikace, pomocí nichž je schopen vytvářet, upravovat a prohlížet dokumenty formátů jako jsou Word, Excel, PDF, ale taky přijímat zprávy o narušení organizace apod.

4.1.3 **Datový projektor**

Datový projektor slouží pro promítání a prezentaci informací většímu počtu posluchačů. V dřívější době se pro prezentaci informací využívaly zpětné projektory s předem připravenými nebo i na místě zhotovovanými fóliemi. Dnes je již pro prezentaci informací hojně využíván datový projektor. Datové projektory mají oproti svým předchůdcům nesporné výhody: lze jimi promítat nejen to, co máme ve svém PC (notebooku), ale například i soubory, které otevřeme prostřednictvím napojení na síť ze serveru nebo z internetu. Můžeme proto kdykoliv během jeho využívání ukázat soubory, se kterými jsme během naší prezentace původně ani nepočítali.

Datové projektory můžeme rozdělit do několika skupin:

- ultralehké – určeny především pro individuálního uživatele, který provádí prezentaci pro několik posluchačů;
- osobní – vhodné pro školení na cestách, menší počet posluchačů;
- mobilní – sdílení mezi více uživateli, pro školení a vzdělávání většího počtu posluchačů;
- konferenční – konferenční sály, školicí střediska, veletrhy a výstavy.

Obr. 14 Datový projektor

Datový projektor je v dnešní době hojně využíván (školy, firmy, restaurace…). Také patří mezi technické prostředky bezpečnostní manažera, který jej využívá ke své práci. Využití nachází především při školení nových zaměstnanců a proškolování stávajících zaměstnanců. Dále jej využívá na poradách s vedením firmy, kde jim předává informace seznamuje je s bezpečností organizace. Pro tuto práci jsou pro něj vhodné zejména mobilní datové projektory.

4.1.4 **Kancelářský softwarový balík**

Společnost Microsoft vydala několik počítačových programů. Pomocí těchto programů je uživateli umožněna lepší práce s daty, ať už jde o jejich zpracování, uchování nebo prezentaci a to zejména v oblasti kancelářských a administrativních činností. Mezi nejvyužívanější programy Microsoft Office řadíme: Microsoft Word, Excel, PowerPoint.

Bezesporu budou tyto programy využívat i bezpečnostní manažeři. A to hlavně při:

- sestavování různých řádů organizace (např. požární, organizační);
- tvorbě bezpečnostních směrnic organizace;
- zpracování zpráv o mimořádných událostech;
- sestavování rozpočtu na technické zabezpečení organizace;
- provádění školení aj.

Bezpečnostní manažer nejen sestavuje a tvoří, ale také pracuje s řadou dokumentů, které jsou zpracovány pomocí těchto programů (např. zákony/vyhlášky, technické listy, manuály zařízení a přístrojů). Takže při jejich použití je zapotřebí mít nainstalovaný v PC (notebooku) příslušný software.

4.1.5 **Intranet**

Dalším systémem, který podporuje získávání informací, může být firemní intranet. Jedná se o obdobu internetu. Pracuje na stejné bázi. Liší se ovšem tím, že slouží k informační podpoře činnosti organizace a zpravidla k němu mají přístup pouze zaměstnanci organizace, která si ho nechala zřídit. Tento systém je nezávislý na internetu, což znamená, že není nutné, aby organizace byla připojena k internetu. Na intranetu je možno nalézt velké množství vnitropodnikových informací. Zpravidla zde bývají různé řády, pravidla, dokumenty a formuláře. Je zde možné nainstalovat i další služby (např. emailový server pro zasílání e-mailů v organizaci).

4.1.6 **Internet**

Můžeme říct, že internet je fenomén dnešní doby. Téměř každá domácnost i organizace je připojena k internetu. Internet je globální systém navzájem propojených počítačových sítí, ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP. Pomocí internetu můžeme načítat webové stránky, a to ať už jsou osobní, veřejné, akademické, obchodní či vládní, ze serveru, kam jsou tyto stránky uloženy. Internet obsahuje miliony informací a služeb. Po internetu se mohou posílat taky e-maily a uskutečňovat hovory.

Internet může sloužit jako rychlý zdroj informací bezpečnostním manažerům. Lze zde najít kontakty a informace o organizacích, se kterými manažeři spolupracují, popř. hodlají spolupracovat. Dále zde mohou nalézt spoustu dalších informací potřebných ke své práci (např. zákony a vyhlášky).

4.2 Specializovaný software

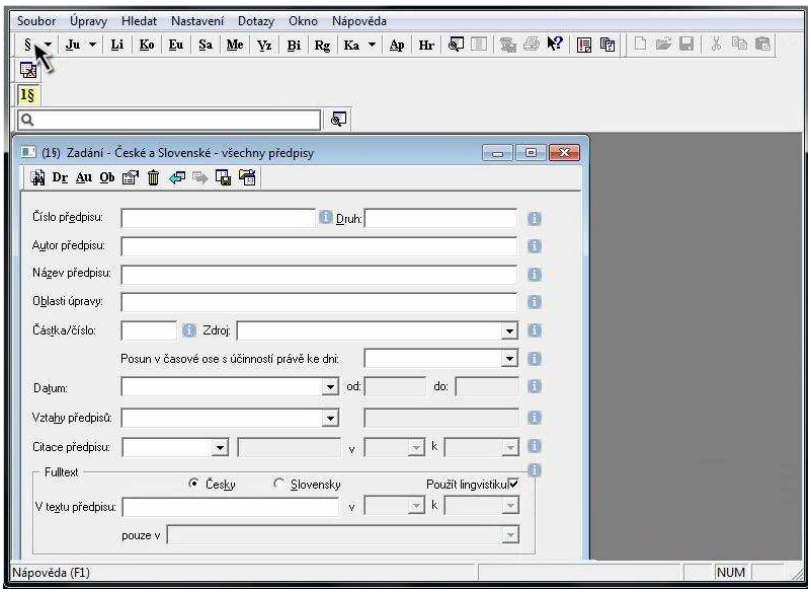
Nejen technické prostředky a systémy slouží k zajištění informační podpory bezpečnostního manažera. Existuje řada specializovaných softwarových aplikací, které umožňují snadnější a efektivnější práci bezpečnostního manažera. Tyto softwary obsahují celou řadu informací, které mají charakter právní, informativní a bezpečnostní. Mezi takovéto specializované softwarové aplikace pak můžeme zařadit:

- systém ASPI;
- RISKAN;
- CRAMM;
- SFERA;
- TEREX;

- ALOHA;
- EMOFF.

4.2.1 **Systém ASPI**

ASPI představuje automatizovaný systém právních informací. Bezpečnostní manažer využívá ke své činnosti mnoho právních předpisů. Systém ASPI mu umožní rychlé vyhledání legislativy, kterou právě potřebuje. Tento systém pokrývá všechny předpisy publikované na území ČR včetně předpisů měst a obcí a předpisů Evropského parlamentu/ Evropské unie.



Obr. 15 Pracovní prostředí ASPI

Přednosti ASPI jsou:

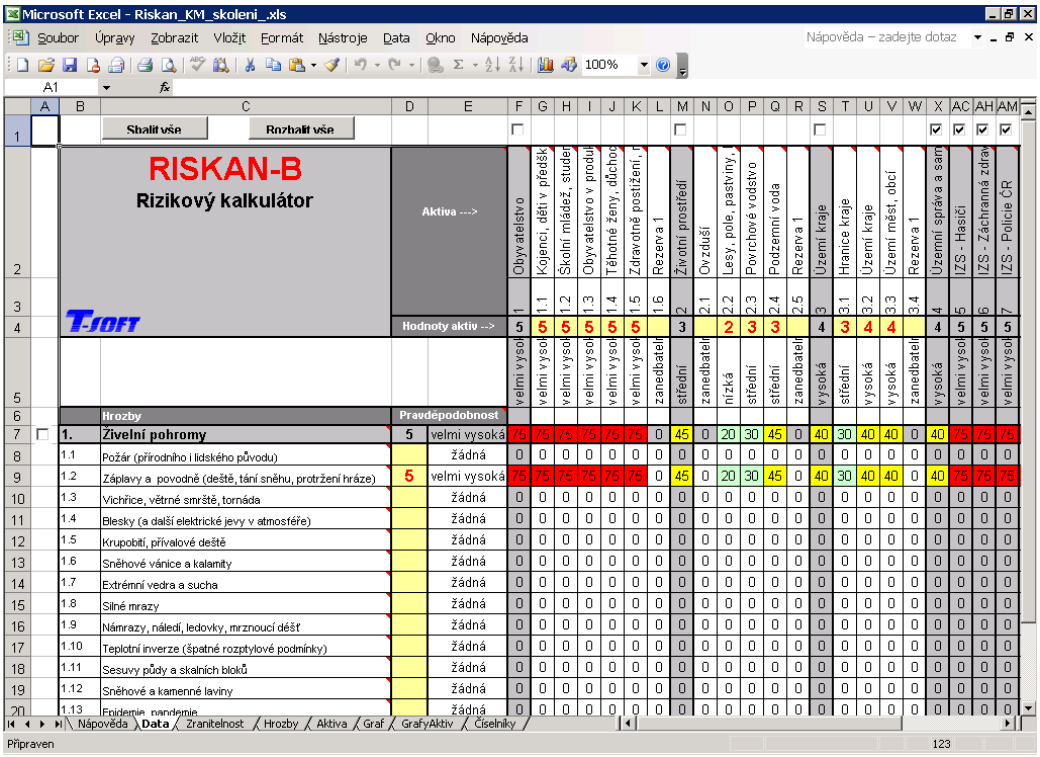
- přesné a rychlé vyhledávání informací pomocí libovolných pojmů ve všech textech předpisů;
- komplexní řešení a nejrozsáhlejší databáze právních předpisů;
- snadné ovládání programu;
- vzájemná provázanost všech informací;
- kvalitní uživatelská podpora (uživatelský web, hot-line, školení, Email INFO);
- systém ASPI lze provozovat v různých počítačových prostředích od serverů na bázi UNIX nebo WINDOWS NT až po běžné osobní počítače s operačním systémem WINDOWS. [19]

4.2.2 **RISKAN**

Program slouží pro rychlou analýzu rizik, čímž pomáhá odhalit bezpečnostní rizika působící na organizaci. Tento produkt mohou využívat nejen bezpečnostní a krizoví manažeři, ale i všichni, kteří rozhodují na základě analýzy možných následků. Rychlé zhodnocení rizik v kalkulátoru RISKAN zahrnuje:

- identifikace aktiv a jejich ohodnocení;
- identifikace hrozeb a ohodnocení jejich pravděpodobnosti;
- ohodnocení zranitelností aktiv jednotlivými hrozbami;
- výpočet výsledného rizika pro každou relevantní dvojici aktivum-hrozba;
- roztřídění výsledných rizik na nízká, střední a vysoká dle stanovených kritérií.

Provedení analýzy rizik s využitím softwarového produktu RISKAN umožňuje zrychlit celý proces, připravit přehledné výstupy a závěry pro rozhodování o dalším postupu ze strany vedení organizace i specialistů bezpečnosti. Kromě toho tento postup usnadňuje opakování analýzy při změně podmínek analyzovaného systému (prostředí) nebo jeho bezpečnosti a celý proces urychluje. [20]



Obr. 16 Prostředí softwaru RISKAN

Uvedený systém umožní bezpečnostním manažerům analyzovat rizika, což pomůže odhalit bezpečnostní rizika ohrožující jejich organizaci. Výstupy z tohoto programu jim poté

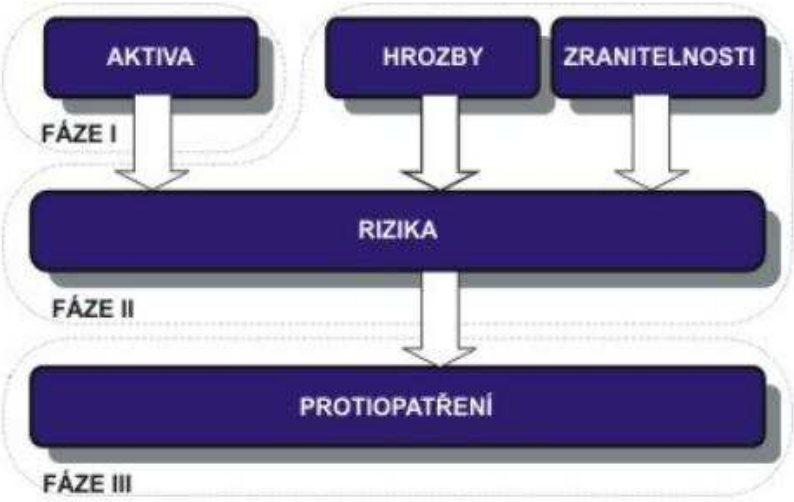
umožní připravit se na hrozby (např. živelní pohromy, technická selhání, průmyslové havárie aj.) a minimalizovat nebo úplně zabránit jejich dopadům na organizaci.

4.2.3 **CRAMM**

Mezi další specializovaný software můžeme zařadit nástroj CRAMM. Jedná se o metodiku a soubor nástrojů pro řízení a analýzu rizik informačních systémů. CRAMM obsahuje komplexní nástroje pro analýzu rizik, které jsou plně v souladu se s ISO/IEC 27002:2005 a ISO/IEC 27001:2005 a zahrnují:

- tvorbu modelu aktiv;
- hodnocení dopadů na činnost organizace;
- identifikaci a hodnocení hrozeb a zranitelností;
- hodnocení míry rizika;
- doporučení protiopatření pokrývající zjištěná rizika. [22]

Analýza a řízení rizik za pomoci CRAMM probíhá ve třech fázích.



Obr. 17 Fáze - analýza a řízení rizik pomocí CRAMM

1. Identifikace a hodnocení aktiv

V první fázi se definují hranice analyzovaného systému a provádí se analýza aktiv systému. V této fázi metodika a nástroj pokrývají činnosti inventarizace aktiv systému, určování jejich hodnoty, hodnocení závažnosti dopadů bezpečnostních incidentů na podnikové činnosti (Business Impact Analysis) podle tzv. vodítek hodnocení a určování požadavků na obnovu aktiv v případě havárie.

2. Analýza hrozeb a zranitelností

Ve druhé fázi se provádí analýza hrozeb a zranitelností pro informační systém. V této fázi pokrývá CRAMM určování závažnosti hrozeb a zranitelností s pomocí detailních dotazníků a stanovení míry rizika u jednotlivých aktiv informačního systému.

3. Řízení rizik

Ve třetí fázi se na základě provedených analýz navrhují protiopatření, která odpovídajícím způsobem pokrývají určená rizika. Nástroj v této fázi dále poskytuje prostředky pro podporu rozhodování o realizaci protiopatření, návrhu systémové bezpečnostní politiky a bezpečnostních směrnic a podporu při návrhu bezpečnostních požadavků na poskytovatele služeb.

Příklady využití souboru nástrojů pro analýzu rizik CRAMM:

- určení, existují-li požadavky na specifická protiopatření, např. silnou autentizaci, šifrování, ochranu napájení či redundanci hardware;
- identifikace požadavků na bezpečnost pro novou aplikaci;
- pomoc při formulaci požadavků na bezpečnost pro outsourcing / managed service;
- revize požadavků na fyzickou bezpečnost a bezpečnost prostředí v novém sídle;
- prověření důsledků povolení přístupu na Internet pro uživatele;
- prokázání souladu s legislativou (např. zákon 101/2000 Sb., O ochraně osobních údajů, který vyžaduje zajištění „dostatečné“ bezpečnosti);
- vytvoření bezpečnostní politiky pro nový informační systém;
- audit vhodnosti a stavu bezpečnostních protiopatření ve stávajícím systému. [22]

Nástroj CRAMM umožní bezpečnostním manažerům komplexní řešení informační bezpečnosti organizace. Manažer dokáže nalézt rychlou odpověď na to, jaké hrozby a jaké slabiny má informační systém organizace, na to, jestli je fyzická bezpečnost informačního systému dostatečná, jakou úroveň bezpečnosti zvolit, aby byla efektivní aj.

4.2.4 **SFERA**

Program SFERA je nový softwarový nástroj vyvinutý speciálně pro analýzu rizika územních a objektových havarijních plánů. Program byl od roku 1996 postupně vyvíjen a testován krizovými manažery na modelových příkladech. S podporou Sdružení požárního a bezpečnostního inženýrství se podařilo realizovat první uživatelský pohodlný produkt. Program SFERA myšlenkově navazuje na známé analytické metody ve snaze se co nejvíce přiblížit filozofii myšlení krizových manažerů při zvažování možných hrozeb

v analyzovaném systému. Důraz je položen na rychlost a jednoduchost práce na jedné straně a přehlednost a stručnost interpretace výstupů na straně druhé. Za samozřejmost je považována týmová práce a možnost verifikace výstupů s ostatními analytickými metodami. Program SFERA je explicitně určen pro analytické účely, avšak lze jej s výhodou využít pro rychlé kriteriální rozhodování, kdy manažer nepracuje s pravděpodobností a velkým množstvím rizik. Program lze obecně využít i k prostému uspořádání prvků technických systémů, u kterých potřebujeme sestavit strom souvislostí definovaných prvků. Od podobných systémů se program SFERA liší svou schopností řešit problematiku neviditelných cyklických vztahů uvnitř analyzované struktury. Program SFERA v principu umožňuje tvorbu kontingenční tabulky, matematické operace třídící data v definovaných souvislostech pod diagonálu, formální editaci dat a jejich zápis do databáze analytických závěrů, návrh a zapracování hodnotových kritérií do výpočtů, výpočet zranitelností jednotlivých rizik s ohledem na časové parametry, export vypočítaných dat od Excelu, HTML stránek nebo do Wordu a zobrazení výsledků do vývojového stromu nebo orientačního grafu. [23]

Tento nástroj lze využít bezpečnostními a krizovými manažery pro analýzu rizika územních a objektových havarijních plánů, což přispěje ke zkvalitnění jejich práce.

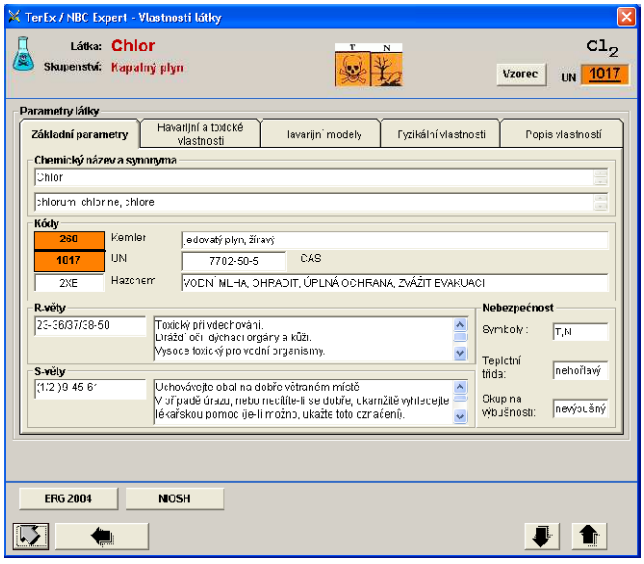
4.2.5 **TEREX**

Jedná se o program vytvořen firmou T-SOFT určený pro okamžité vyhodnocení ohrožení způsobeného únikem nebezpečné chemické látky, otravné látky či použitím nástražného výbušného systému. Program je určen podnikům, institucím, samosprávám a složkám IZS. Je vhodný pro plánování, výpočet prvních odhadů a také pro potřeby různých cvičení. Program obsahuje obsáhlou databázi látek včetně příslušných parametrů (např. vlastnosti látky, zásady první pomoci, způsob dekontaminace).

Dále program nabízí uživateli pracovat s havarijními modely:

- modely typu TOXI – vyhodnocují dosah a tvar oblaku, které jsou dány zvolenou koncentrací toxické látky;
- modely typu UVCE – vyhodnocují dosah působení vzdušné rázové vlny, vyvolané detonací směsi látky se vzduchem pro modely s jednotlivými druhy havárií;
- model PLUME – vyhodnocuje déletrvající únik plynu do oblaku, déletrvající únik vroucí kapaliny s rychlým odparem do oblaku, pomalý odpar kapaliny z louže do oblaku;

- model PUFF – vyhodnocuje jednorázový únik plynu do oblaku, jednorázový únik vroucí kapaliny s rychlým odparem do oblaku;
- modely typu FLASH FIRE – vyhodnocují velikost prostoru ohrožení osob plamennou zónou – efekt Flash Fire:
    - BLEVE – ohrožení nádrže plošným požárem;
    - JET FIRE – déletrvající masivní únik plynu se zahořením;
    - POOL FIRE – hoření louže kapaliny nebo vroucí kapaliny;
- model typu TEROR – vyhodnocuje možné dopady detonace výbušných systémů založených na kondenzované fázi, použité s cílem ohrožení okolí detonace;
- model POISON – pro předpověď šíření oblaku vzniklého rozptýlením otravné látky na určité území. Vstupním parametrem je rozloha území v hektarech. Program umožňuje zvolit podle typu látky jak následky primárního rozptylu volbou Rozptýlení (výbuch, rozstřik apod.), tak sekundárního odparu volbou Odpar z louže. Při bodovém užití otravné látky se zadává hodnota 0,01 ha, což je minimální programem akceptovaná hodnota.
- model ATP-45B – opět pro předpověď šíření oblaku otravné látky. Výsledky jsou závislé na způsobu použití látky a na síle větru. Zasažená oblast je představována kružnicí o poloměru 1 resp. 2 km bez ohledu na typ použité látky. Podle síly větru menší nebo větší než 10 m/s je ohrožená oblast představována kružnicí o poloměru 10 km resp. výsečí ve směru větru dlouhou 10 km.
- model podle předpisu ATP-45B – se ukazuje pro vyhodnocení teroristického použití otravné látky jako velmi hrubý a je určen spíše pro vojenské nasazení. [21]



Obr. 18 Prostředí programu TEREX – vlastnosti látky

Celkové výsledky výpočtů modelu TEREX jsou uspořádány jednoduše a jednoznačně, takže usnadňují rychlé rozhodování. Výsledky je možno uložit do databáze havarijních událostí. Součástí programu je také modul mapa, který umožní zobrazení výsledků přímo na konkrétní místo do mapy.

Tento produkt poslouží bezpečnostním manažerům jako zdroj informací o vlastnostech látek a umožní jim rychlé rozhodování při vyhodnocování úniku nebezpečných chemických látek, otravných látek nebo zneužití výbušných systémů.

4.2.6 **ALOHA**

ALOHA je jednoduchý 2D simulační software, určený k přibližnému modelování tvaru a rozsahu úniku nebezpečné látky do atmosféry. Výpočty provádí pomocí statistického gaussovského rozdělení nebo modelu „heavy gas“ pro simulace pohybu mraků plynů těžších než vzduch. Dále dokáže určit velikost ohrožené oblasti výbuchem či hořením hořlavé látky. [24]

Program je v angličtině, ale uživatelsky příjemný a jednoduchý. Obsahuje databázi několika set nejběžnějších chemických látek používaných v průmyslu. V případě potřeby větší databáze je možné stáhnout jako doplněk databázi CAMEO, která obsahuje mnohem větší databázi chemikálií než samotná ALOHA, hlavně méně obvyklé. Grafické výstupy jsou tvořeny jednou až třemi zónami, uživatel může zadat vlastní hodnoty koncentrací nebo použít hodnoty stanovené výrobcem pro ještě neškodné hodnoty koncentrace. Zóny jsou informativního rázu, v silně členitém terénu (město, hustý les) se reálná mapa šíření škodliviny může velmi odlišovat. Také nejsou brány v úvahu nerovnosti reliéfu (údolí, srázy), které také mohou změnit směr mraku škodlivin, typicky plynů těžších než vzduch (např. chlór). Pro základní orientaci však dobře stačí, protože model předem počítá s určitou nepřesností. [24]

Tento software poslouží bezpečnostním manažerům jako zdroj informací, které budou potřeba při zpracování havarijních plánů a řešení vzniklých havárií spojených s únikem nebezpečných látek.

4.2.7 **EMOFF**

Jedná se o další software vyrobený firmou T-SOFT. Obsahuje sadu nástrojů, které slouží pro podporu informačních procesů při prevenci a řízení mimořádných událostí/krizových situací. Tento software může pomoci v následujících oblastech:

- analýze nebezpečí a rizik;
- vyhodnocení bezpečnostních rizik;
- plánování, organizování, realizování a kontrola činností;
- shromažďování a vyhodnocování informací o organizacích, osobách, silách, prostředcích a zařízeních pro zvládání mimořádných událostí/krizových situací;
- podpora řešení mimořádných událostí/krizových situací. [25]

Samotný program obsahuje několik modulů. Jedná se o následující moduly:

- ohrožení – modul evidence rizik, jejich příčin a možných dopadů, určení ohrožujících a ohrožených objektů;
- plány – modul tvorby havarijních a krizových plánovacích dokumentů, které shrnují nezbytné činnosti, procedury a vazby uskutečňované krizovým managementem;
- opatření – modul přípravy a provádění opatření pro prevenci vzniku, podporu řešení a zmírnění dopadů mimořádných událostí/krizových situací;
- postupy (SOP) – modul přípravy standardních operačních postupů;
- orgány a organizace – modul pro evidenci a přehledy orgánů a organizací zapojených do krizového řízení a řešení mimořádných událostí/krizových situací;
- osoby – modul pro evidenci osob zapojených do plánu řešení a kontaktních osob orgánů a organizací;
- zdroje (síly, prostředky, zařízení) – modul pro evidenci a přehledy sil, prostředků a zařízení pro podporu řešení;
- vyrozumění – modul pro přípravu vyrozumění osob a orgánů;
- události – modul pro podporu řešení mimořádných událostí/krizových situací;
- obnova – modul pro vedení záznamů vzniklých škod a ztrát. [25]

4.3 Shrnutí

Bezpečnostní manažer při své činnosti využívá řadu technických prostředků a softwarových aplikací. Mezi jeho základní technický prostředek řadíme PC s příslušným softwarem, který využívá k řadě činností (např. k tvorbě dokumentů, směrnic a řádů, ke zpracování a vyhledávání informací). Dále využívá řadu specializovaných softwarů, které mu poslouží ke zjištění informací, které potřebuje, aby splnil a dosáhl stanovených cílů.

5 HODNOCENÍ A MOŽNOST ZLEPŠENÍ INFORMAČNÍ PODPORY BEZPEČNOSTNÍCH MANAŽERŮ

5.1 Dotazníkové šetření

Je možno říci, že dotazníkové šetření je snad nejrozšířenější technikou, která slouží k získání informací. Je to proto, že jeho použití je zdánlivě velmi nenáročné, je ze všech technik nejlevnější a snadno také zasáhne velký počet zkoumaných osob. Dotazníkové šetření je nenahraditelnou pomůckou v případě, kdy je třeba získaný materiál podrobit kvantitativní analýze, jak je tomu při reprezentativních výzkumech.

Dotazník je konkrétním výzkumným nástrojem, jehož pomocí máme získat konkrétní materiály o konkrétních věcech. Dotazník nám dopomůže k získání údajů o společenských znacích zkoumané společenské skutečnosti. Je třeba však problém, který chceme dotazníkem zkoumat, rozložit na jednotlivé otázky.

Otázky v dotazníku lze rozdělit na tři základní typy: otevřené (volná formulace odpovědi respondenta), uzavřené (výběr z několika předdefinovaných variant), polozavřené (kombinace obou předchozích typů).

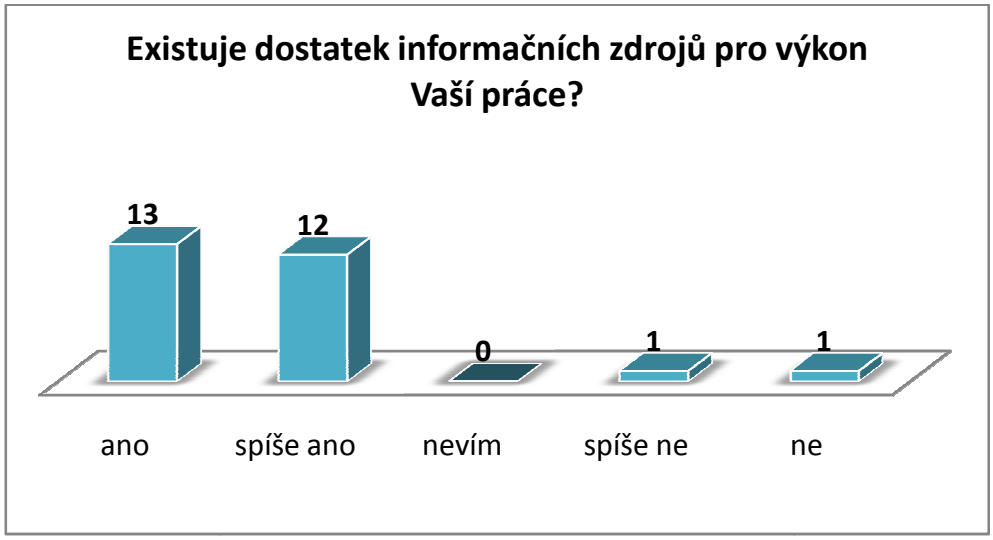
Požadavky kladené na dotazník:

- dotazník má obsahovat všechny podstatné problémy, na které výzkum hledá odpověď a na které nemůže odpověď získat jiným způsobem;
- otázky mají být formulovány tak, aby bylo možno na ně získat vyčerpávající odpověď;
- dotazník má být konstruován tak a otázky v něm postaveny takovým způsobem, aby neodradil a neznechutil respondenta, ale naopak ho nabádal k odpovědím;
- otázky v dotazníku mají být zformulovány zcela srozumitelným způsobem;
- otázky mají být zformulovány tak, aby odpovědi na ně byly zcela jednoznačné;
- v dotazníku mají být otázky, na které je možno upřímně odpovídat;
- formulace otázek má být taková, aby respondent na ně mohl odpovídat bez nadměrné myšlenkové námahy;
- dotazník nemá respondenta příliš namáhat. [10]

5.2 Dotazník – práce bezpečnostního manažera s informacemi, jejich získávání či využívání a použití technických prostředků

Následující dotazníkové šetření má za cíl zjistit, jak bezpečnostní manažer pracuje s informacemi, jak je získává či využívá a jaké technické prostředky k tomu používá. Dotazník se skládá ze 20 otázek. Je využito všech tří základních typů otázek (uzavřené, otevřené, polozavřené). Průzkum byl zaměřen na bezpečnostní manažery organizací. Dotazník byl rozeslán buď přímo konkrétnímu bezpečnostnímu manažerovi organizace, nebo byl zaslán do organizace, kde byl následně předán příslušnému bezpečnostnímu manažerovi. Rozesílání probíhalo výhradně pomocí e-mailu. Celkem je zde vyhodnoceno 27 dotazníků, které byly vyplněny bezpečnostními manažery.

Otázka č. 1 Existuje dostatek informačních zdrojů pro výkon Vaší práce?

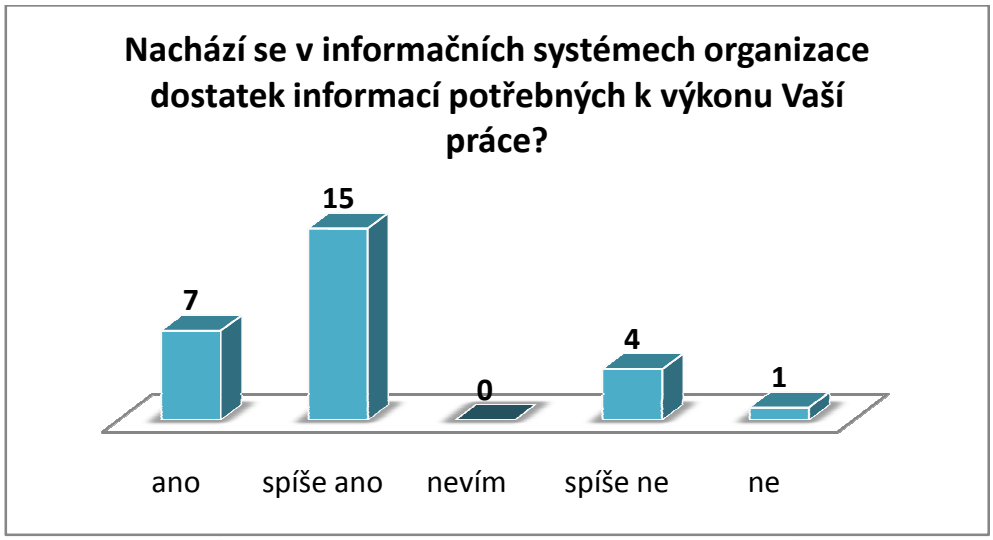


Graf 1 Výsledky otázky č. 1

V první otázce byl položen dotaz respondentům na to, zda mají dostatek informačních zdrojů pro výkon své práce. Z odpovědí dotázaných vyplývá: 48 % respondentů říká, že je dostatek informačních zdrojů pro práci bezpečnostního manažera, 44 % říká, že spíše je dostatek informačních zdrojů a shodně 4 % respondentů se vyjádřilo pro to, že spíše neexistuje dostatek informačních zdrojů pro výkon jejich práce. Odpověď nevím nezatrhl ani jeden z dotazovaných.

Na základě vyhodnocení této otázky můžeme říci, že existuje dostatek informačních zdrojů pro výkon práce bezpečnostních manažerů.

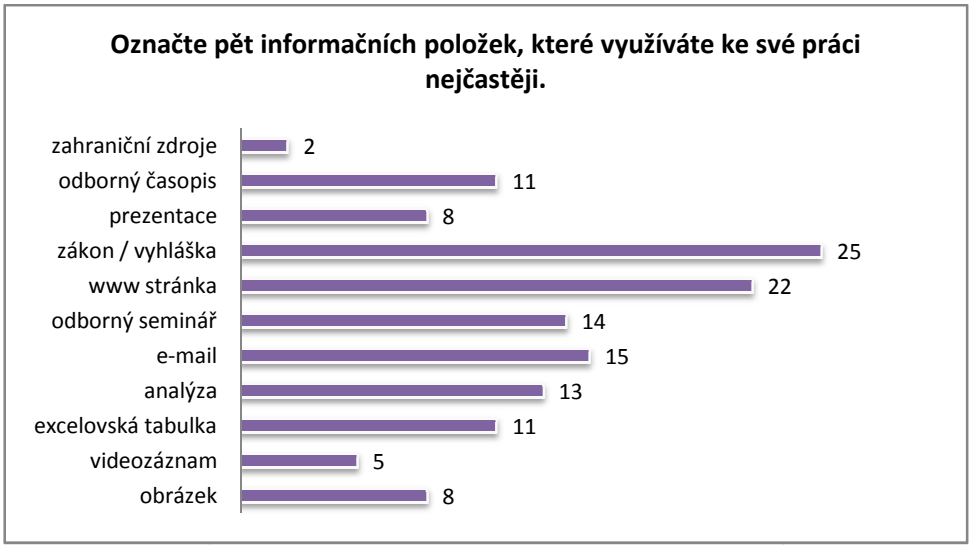
Otázka č. 2 ***Nachází se v informačních systémech organizace dostatek informací potřebných k výkonu Vaší práce?***



Graf 2 Výsledky otázky č. 2

Otázka na dostatek informací v informačních systémech organizace potřebných pro výkon práce bezpečnostních manažerů byla položena z důvodu zjištění, zda informace, se kterými bezpečnostní manažeři pracují, se nacházejí v informačních systémech organizací, nebo naopak si je musí pracovníci hledat jinde. S odpovědí dotázaných vyplývá, že bezpečnostní manažeři mají většinou spíše dostatek informací přímo v podnikových informačních systémech. Což zároveň znamená, že ne všechny informační systémy organizací pokrývají zcela informační potřeby bezpečnostních manažerů.

Otázka č. 3 ***Označte pět informačních položek, které využíváte ke své práci nejčastěji.***



Graf 3 Výsledky otázky č. 3

Po zodpovězení této otázky je patrné, že bezpečnostní manažeři využívají nejčastěji informační položku ve formě zákona/vyhlášky. Dále následuje internetová www stránka. Poté jsou využívány téměř rovnoměrně odborné časopisy a semináře, e-maily, analýzy a tabulky z programu MS Excel. Mezi posledními se umístnily videozáznamy, prezentace a obrázky. Za nejméně využívanou informační položku patří zahraniční zdroje. Viz. Graf 3.

Z uvedeného vyplývá, že zákon/vyhláška je jednoznačně nedílným informačním zdrojem potřebným pro práci bezpečnostních manažerů.

Otázka č. 4 ***Každý manažer se setkává se základními informačními činnostmi, kterými jsou: vyhledávání informací, rutinní zpracování dat, tvůrčí vytváření informačního obsahu, prezentace a komunikace. Stanovte pořadí výše uvedených činností z hlediska četnosti provádění (1 – nejčastěji, 5 – nejméně často).***

nejčastěji – nejméně často	**1**	**2**	**3**	**4**	**5**
vyhledávání informací	**11**	**6**	**5**	**3**	**2**
rutinní zpracování dat	**3**	**3**	**8**	**8**	**5**
tvůrčí vytváření informačního obsahu	**1**	**3**	**11**	**5**	**7**
prezentace	**1**	**2**	**4**	**10**	**10**
komunikace	**12**	**11**	**1**	**2**	**1**

Tab. 1 Výsledky otázky č. 4

V tabulce 1 můžeme vidět, jak respondenti odpovídali na otázku č. 4, kde se vyjadřovali k tomu, jakou informační činnost nejčastěji provádí. Každou možnost měli oznámkovat číslem 1 – 5, kde 1 = nejčastěji provádím, 5 = nejméně často provádím. V tabulce je u každé činnosti uvedeno číslo, které znamená, kolikrát byla dané činnosti přisouzena známka 1 – 5. Čím vyšší je číslo, tím vícekrát byla přisouzena dané činnosti známka uvedena v záhlaví tabulky.

Z tab. 1 vyplývá, že bezpečnostní manažeři nejčastěji komunikují, dále pak vyhledávají informace, vytvářejí si svůj informační obsah, prezentují a jako nejméně často z uvedených informačních činností zpracovávají data.

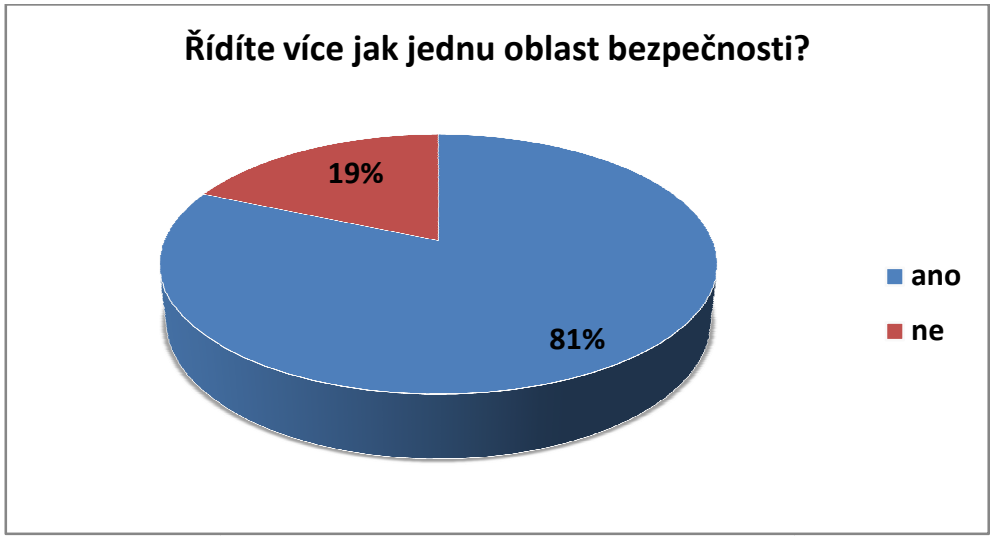
Dále jsem provedl srovnání, jak odpovídali respondenti, kterým nebylo více jak 40 let s respondenty nad 41 let. Z výsledků vyplynulo, že respondenti pod 40 let nejčastěji vyhledávají informace, dále pak komunikují, vytváří si informační obsah, provádí rutinní

zpracování dat a nejméně často prezentují. Naproti tomu dotazování nad 40 let nejčastěji komunikují, dále pak vyhledávají informace, vytvářejí si svůj informační obsah, prezentují a jako nejméně často z uvedených informačních činností zpracovávají data (viz. Tab. 2).

méně než 20 -- 40 let	41 -- 51 a více let
vyhledávání informací	komunikace
komunikace	vyhledávání informací
tvůrčí vytváření informačního obsahu	tvůrčí vytváření informačního obsahu
rutinní zpracování dat	prezentace
prezentace	rutinní zpracování dat

Tab. 2 Porovnání otázky č. 4 podle věku respondentů

Otázka č. 5 Řídíte více jak jednu oblast bezpečnosti?



Graf 4 Výsledky otázky č. 5

Více jak jednu bezpečnost ve své organizací řídí 81 % respondentů. Zbylých 19 % uvedlo, že se zabývá pouze jednou oblastí bezpečnosti.

Otázka č. 6 Uveďte, jakou oblast/ti bezpečnosti v organizaci řídíte (např. bezpečnost a ochrana zdraví při práci (BOZP); požární ochrana; fyzická bezpečnost; informační bezpečnost; krizové řízení).

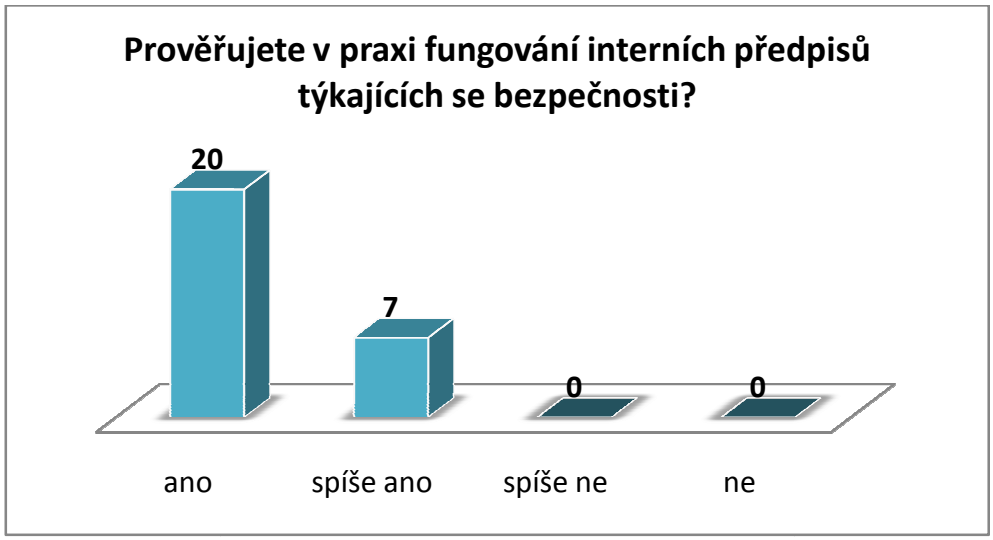
Dotazovaní respondenti uváděli, že nejčastěji mají na starost: bezpečnost a ochranu zdraví při práci, požární ochranu, fyzickou bezpečnost, oblast krizového řízení a bezpečnost spojenou s chemickými látkami.

Otázka č. 7 Myslíte si, že by bylo lepší, aby každý úsek bezpečnosti měl jednoho bezpečnostního manažera?

Graf 5 Výsledky otázky č. 7

Na otázku, zda je lepší, aby každý úsek bezpečnosti měl jednoho bezpečnostního manažera, odpovědělo 59 % dotázaných, že NE. Zbylých 41 % se vyjádřilo v tom smyslu, že by bylo lépe, aby měl každý úsek bezpečnosti na starost jeden manažer. V podotázce se dále měli možnost vyjádřit, proč jsou pro variantu ANO respektive variantu NE. V odpovědích na tuto otázku se často vyskytovaly názory, že záleží na velikosti a zaměření organizace. Pokud je organizace menšího typu, vystačí si s jedním bezpečnostním manažerem a naopak. Dále ti, kteří byli pro více bezpečnostních manažerů, viděli problém ve složité a neustále se měnící legislativě a ve velkých nárocích kladených na znalosti bezpečnostního manažera, který musí řídit více úseků bezpečnosti (trpí kvalita řízení). Důvod pro jednoho bezpečnostního manažera byl především v nedostatku financí a taky v tom, že některé oblasti jsou spolu úzce spojeny např. BOZP a PO tudíž není potřeba více pracovníků. To neplatí ovšem o informační bezpečnosti, kde se vyjadřovali pro samostatného bezpečnostního manažera. A to především z toho důvodu, že tento úsek považují za specifický.

Otázka č. 8 Prověřujete v praxi fungování interních předpisů týkajících se bezpečnosti?

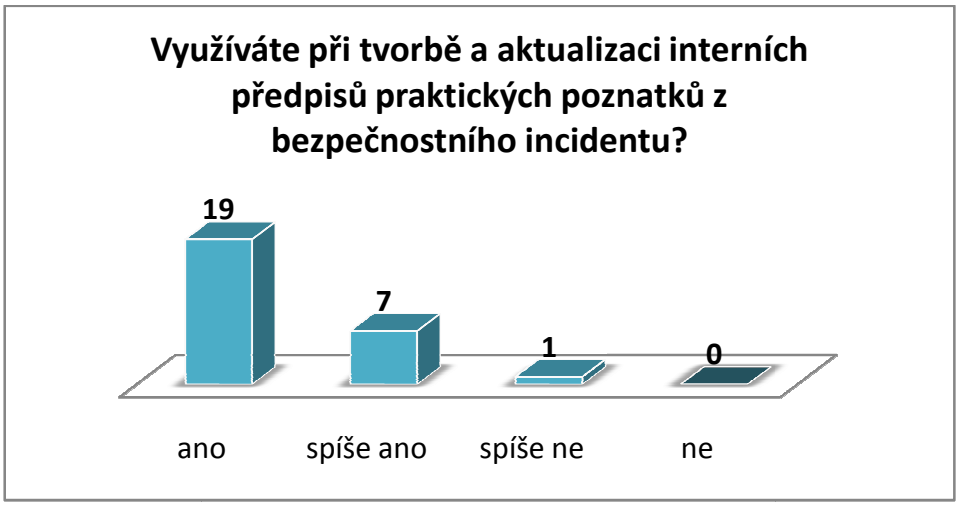


Graf 6 Výsledky otázky č. 8

Otázka týkající se prověřování fungování interních bezpečnostních předpisů v praxi dopadla jednoznačně.

74 % respondentů prověřuje fungování interních bezpečnostních předpisů v praxi a zbylých 26 % dotázaných se přiklonilo k odpovědi, že spíše prověřuje bezpečnostní předpisy v praxi. Odpověď spíše ne a ne se nevyskytla ani jednou.

Otázka č. 9 Využíváte při tvorbě a aktualizaci interních předpisů praktických poznatků z bezpečnostního incidentu?



Graf 7 Výsledky otázky č. 9

Podobně jako předchozí otázka dopadla i otázka č. 9. Při tvorbě a aktualizaci interních předpisů používá 70 % respondentů praktických poznatků z bezpečnostního incidentu. 26 % respondentů spíše využívá těchto poznatků. Na odpověď spíše ne připadají 4 % respondentů a odpověď ne se zde nevyskytla ani jednou.

Otázka č. 10 Očíslujte vlastnosti informací, které jsou pro Vás nejvíce důležité při vzniku bezpečnostního incidentu. (1 – nejvíce důležité, 5 – nejméně důležité).

	1	**2**	**3**	**4**	**5**
přesnost	**8**	**8**	**2**	**7**	**2**
rychlost	**6**	**2**	**3**	**4**	**12**
aktuálnost	**5**	**8**	**4**	**4**	**6**
úplnost	**3**	**4**	**11**	**6**	**3**
srozumitelnost	**4**	**5**	**6**	**7**	**5**

Tab. 3 Výsledky otázky č. 10

V tabulce 3 můžeme vidět, jak respondenti odpovídali na otázku č. 10, kde se vyjadřovali k tomu, jaká vlastnost informace je pro ně nejvíce důležitá při vzniku bezpečnostního incidentu. Každou vlastnost informace měli možnost oznámkovat číslem 1 – 5, kde 1 = nejvíce důležité, 5 = nejméně důležité. V tabulce je u každé vlastnosti informace uvedeno číslo, které znamená, kolikrát byla dané vlastnosti přisouzena známka 1 – 5. Čím vyšší je číslo, tím vícekrát byla přisouzena dané činnosti známka uvedena v záhlaví tabulky. Z průzkumu vyplývá, že pro respondenty je „nejvíce důležitá“ přesnost, dále je to pak aktuálnost, úplnost, srozumitelnost, a za „nejméně důležitou“ považují rychlost.

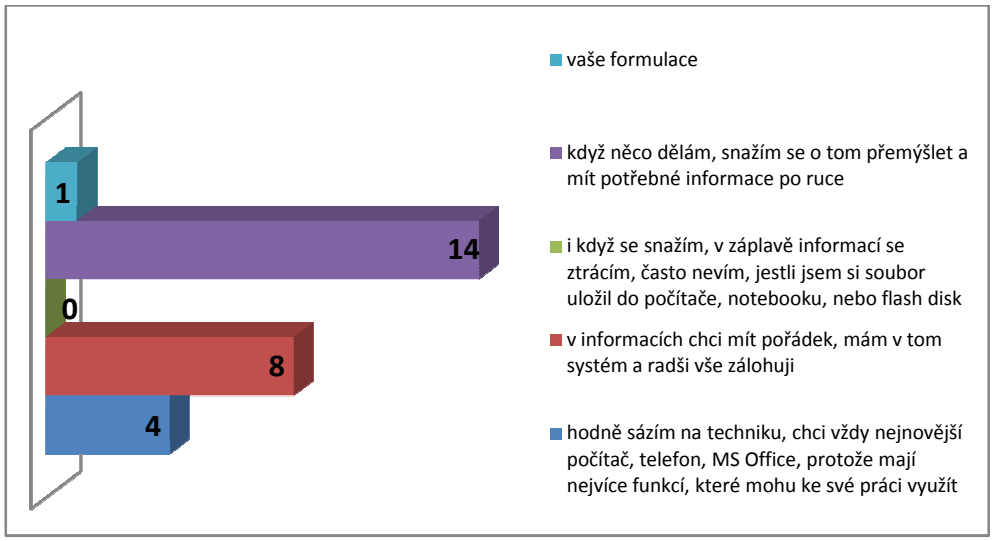
Opět jsem provedl srovnání, mezi věkovými skupinami respondentů do 40 let a nad 41 let. Výsledky je možno vidět v Tab. 4.

méně než 20 -- 40 let	41 -- 51 a více let
přesnost	přesnost
úplnost	aktuálnost
srozumitelnost	úplnost
aktuálnost	srozumitelnost
rychlost	rychlost

Tab. 4 Srovnání věkových skupin

Otázka č. 11 Každý člověk přistupuje k vytváření svého informačního prostředí jinak. Využívá k zajištění informací nezbytné nástroje, technologie, kancelářské

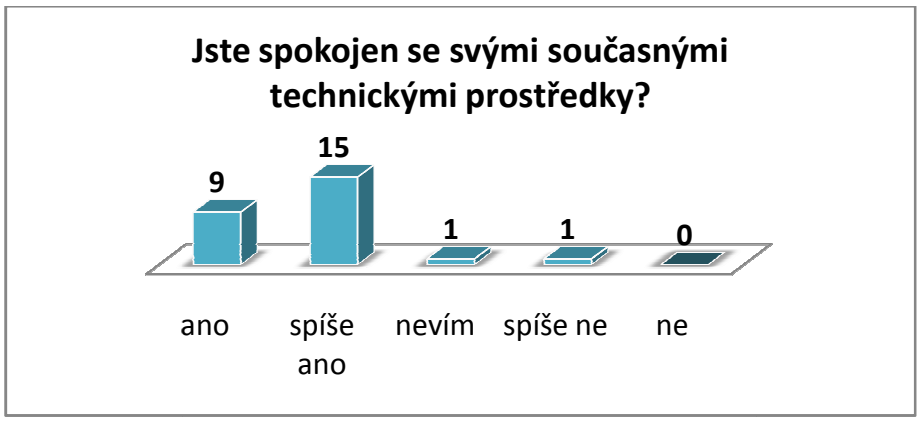
pomůcky. Z uvedeného přehledu vyberte položku, která nejlépe vystihuje Vaše informační prostředí.



Graf 8 Výsledky otázky č. 11

V této otázce byl položen dotaz na to, jak každý z bezpečnostních manažerů, přistupuje k vytváření svého informačního prostředí. Více jak polovina dotázaných označila odpověď: když něco dělám, snažím se o tom přemýšlet a mít potřebné informace po ruce. Dále dotazovaní označovali odpověď: v informacích chci mít pořádek, mám v tom systém a radši vše zálohuji a odpověď: hodně sázím na techniku, chci vždy nejnovější počítač, telefon, MS Office, protože mají nejvíce funkcí, které mohu ke své práci využít. Jeden respondent svou odpověď zformuloval sám. V ní se vyjádřil, že k vytváření svého informačního prostředí upřednostňuje zajištění bezpečnosti na dostatečné úrovni s co nejmenšími náklady.

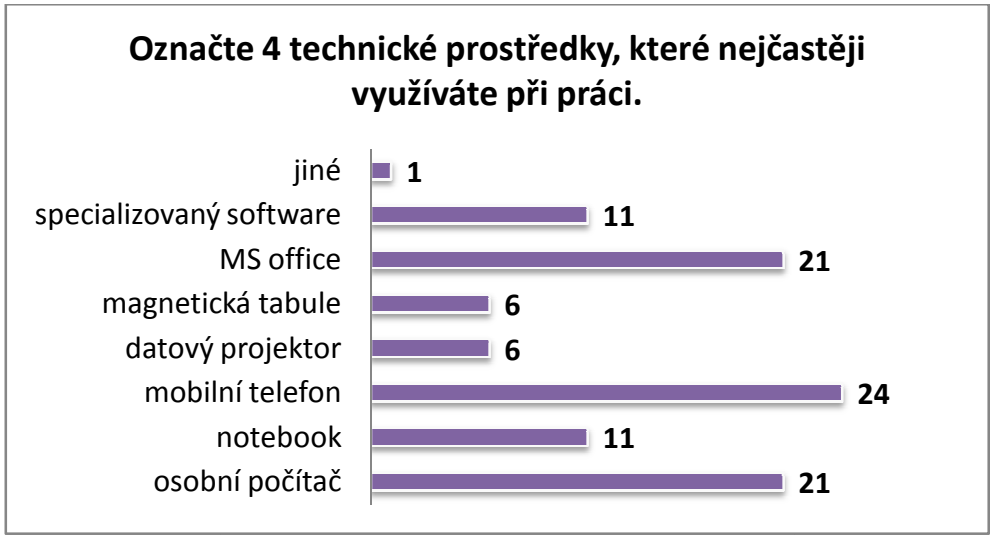
Otázka č. 12 Jste spokojen se svými současnými technickými prostředky?



Graf 9 Výsledky otázky č. 12

V otázce, zda jsou respondenti (bezpečnostní manažeři) spokojeni se svými současnými technickými prostředky, je spíše spokojeno 58 % dotázaných, 34 % je spokojených, 4 % respondentů je spíše nespokojených a zároveň neví, zda je spokojeno se svými současnými technickými prostředky. Nikdo z respondentů není nespokojen se stavem technických prostředků, které má k dispozici.

Otázka č. 13 Označte technické prostředky, které nejčastěji využíváte při práci.



Graf 10 Výsledky otázky č. 13

Cílem otázky bylo zjistit, jaké technické prostředky bezpečnostní manažeři využívají při své práci nejčastěji. Z odpovědí dotázaných je patrné, že nejvíce využívají mobilní telefon, MS Office a osobní počítač. Dále je to pak specializovaný software, notebook, magnetická tabule, datový projektor a jiné zařízení (bylo uvedeno klasické PDA).

Otázka č. 14 V případě, že využíváte specializovaný software, uveďte jaký.

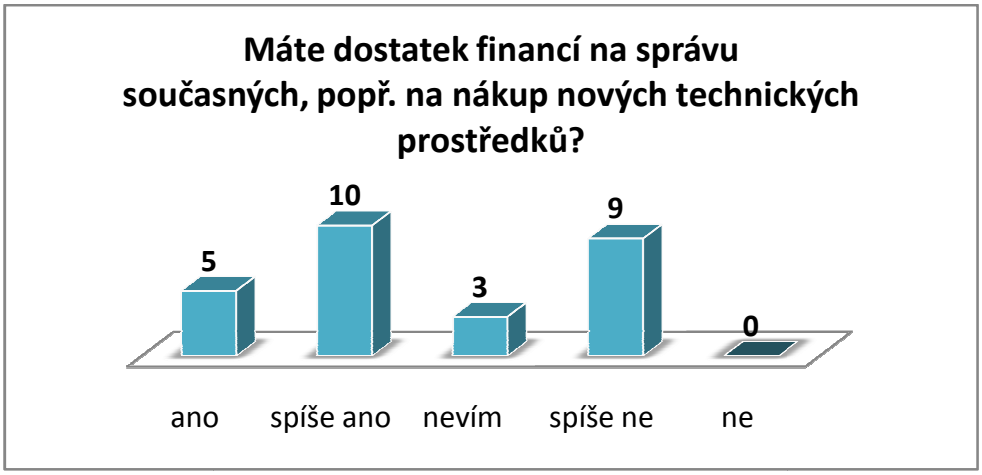
Tato otázka se týkala jenom těch respondentů, kteří odpověděli, že využívají i specializovaný software.

V jedenácti případech bylo respondenty uvedeno, že využívají specializovaný software. Jednalo se o softwary RISCON, ARGIS, KRIZKOM, Lotus NOTES, SIB_LEX, databáze předpisů a rizik.

Tyto softwary slouží především pro řízení BOZP (RISCON, SIB_LEX), dále software ARGIS (nástroj informační podpory hospodářských opatření pro krizové stavy v oblasti zajišťování věcných zdrojů), KRIZKOM (nástroj informační podpory pro řízené a evidované předávání požadavku na věcné zdroje, které orgány krizového řízení potřebují

k překonání krizové situace nebo k odstranění jejich následků), software Lotus NOTES (navzájem provázané aplikace pro oblast týmové spolupráce, plánování, vykazování času a další specifická zákaznická řešení).

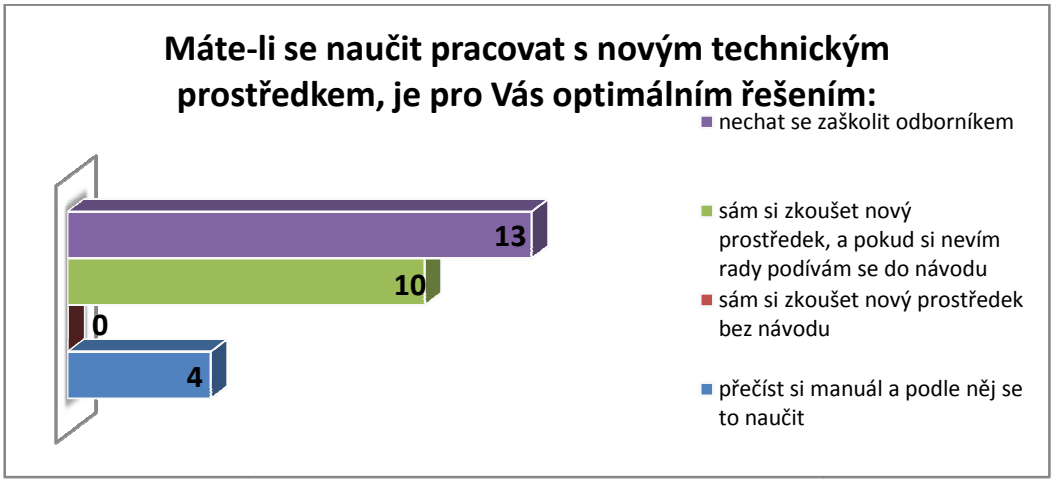
Otázka č. 15 Máte dostatek financí na správu současných, popř. na nákup nových technických prostředků?



Graf 11 Výsledky otázky č. 15

V této otázce bylo zjišťováno, zda mají dostatek financí na správu současných, popř. na nákup nových technických prostředků. 37 % respondentů uvedlo, že spíše mají dostatek financí. Dále z průzkumu vyplývá, že 33 % respondentů spíše nemá dostatek financí na správu technických prostředků. Dostatek financí má 19 % dotázaných. Zbylých 11 % neví, zda má dostatek financí na správu popř. nákup nových technických prostředků.

Otázka č. 16 Máte-li se naučit pracovat s novým technickým prostředkem je pro Vás optimálním řešením.

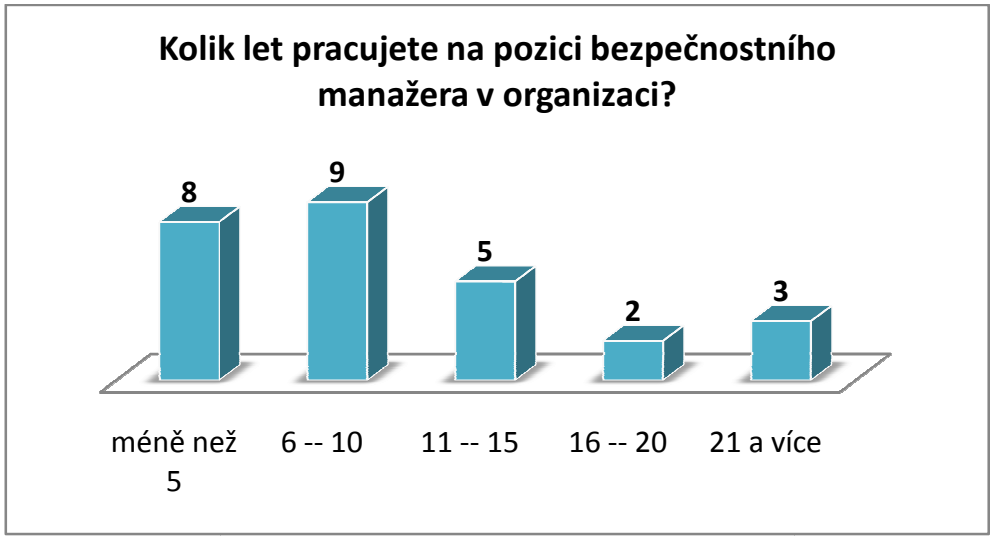


Graf 12 Výsledky otázky č. 16

V této otázce bylo zjištěno, jaké je optimální řešení pro respondenty, když se musí naučit pracovat s novým technickým prostředkem. 48 % považuje za optimální při práci s novým technickým prostředkem se nechat zaškolit odborníkem, 37 % si raději samo zkouší nový prostředek a v případě nějaké nesrozumitelnosti se podívá do návodu. Zbylých 15 % si přečte manuál a pomocí něj se naučí pracovat s novým technickým prostředkem.

Při srovnání věkových skupin vyplývá, že optimální řešení pro věkovou skupinu do 40 let je se naučit pracovat s novým technickým prostředkem sám nebo pomocí manuálu. K tomuto kroku se přihlásilo 78 % respondentů, zbylých 22 % preferuje zaškolení odborníkem. Věková skupinu nad 41 let naopak považuje za optimální řešení, konkrétně 61 % respondentů, nechat se zaškolit odborníkem, pokud jde o to naučit se pracovat s novým technickým prostředkem. Zbylých 39 % si zkouší technický prostředek sám nebo pomocí manuálu.

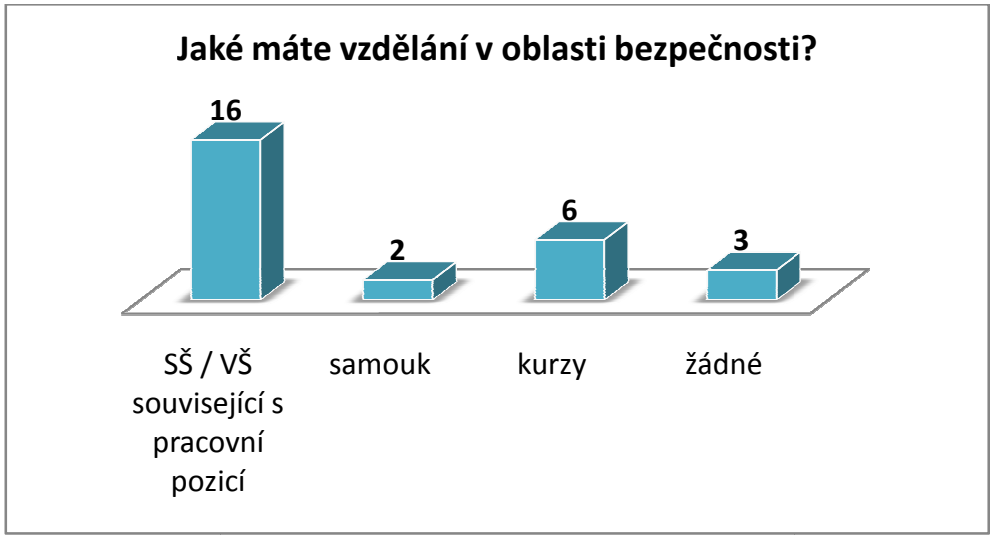
Otázka č. 17 Kolik let pracujete na pozici bezpečnostního manažera v organizaci?



Graf 13 Výsledky otázky č. 17

V otázce kolik let pracujete na pozici bezpečnostního manažera v organizaci, vyplynuly následující údaje. V rozmezí 6 – 10 let se této práci věnuje 33 % respondentů, 30 % se jí věnuje méně než 5 let, 19 % se ji věnuje 11 – 15 let, 11 % respondentů se věnuje práci 21 a více let a zbylých 7 % respondentů se věnuje své práci 16 – 20 let.

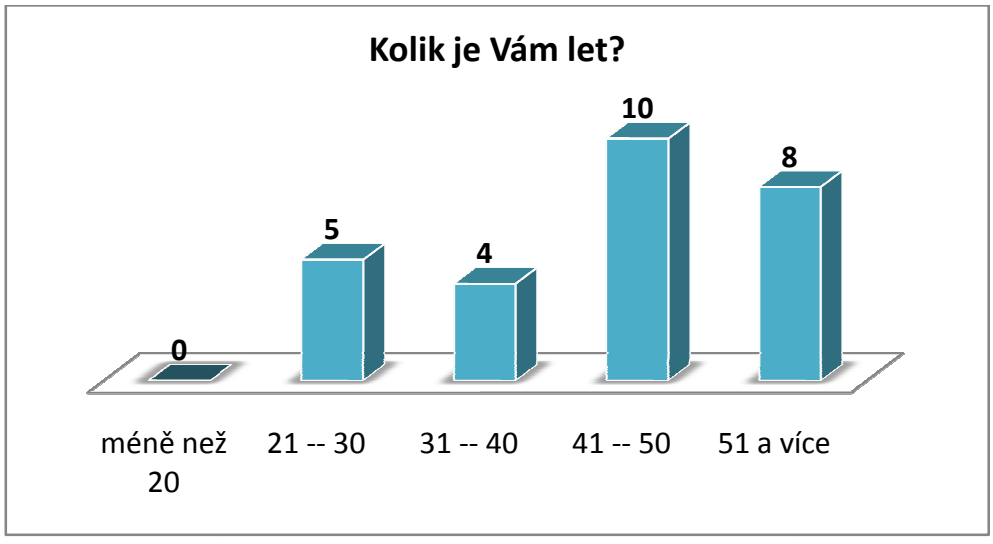
Otázka č. 18 Jaké máte vzdělání v oblasti bezpečnosti?



Graf 14 Výsledky otázky č. 18

V této otázce bylo cílem zjistit, jakým vzděláním disponují pracovníci organizací na pozici bezpečnostní manažer. Z dotazovaných bezpečnostních manažerů 59 % má vzdělání SŠ/VŠ související s pracovní pozicí, 22 % dotázaných má udělány různé kurzy týkající se bezpečnosti, 11 % z dotazovaných nedisponuje žádným vzděláním v oblasti bezpečnosti a 8 % respondentů připadá na samouky v této oblasti.

Otázka č. 19 Kolik je Vám let?



Graf 15 Výsledky otázky č. 19

Byla zde položena také otázka na věk respondentů z důvodu získání přehledu o zastoupení věkových skupin v rámci bezpečnostních manažerů v organizaci. Nejvíce respondentů, 37 % je zastoupeno ve věkové skupině 41 – 50 let, 30 % ve skupině 51 a více let, 18 % ve

skupině 21 – 30 let a 15 % respondentů je zastoupeno ve skupině 31 – 40 let. Věková skupina méně než 20 let nebyla zastoupena žádným respondentem.

Otázka č. 20 Jaké je Vaše pohlaví?

Graf 16 Výsledky otázky č. 20

V poslední otázce byl položen dotaz na pohlaví respondentů. Cílem bylo zjistit, kolik procent žen a kolik procent mužů pracuje na pozici bezpečnostního manažera organizace. Z odpovědí dotazovaných vyplývá, že 89 % je zastoupeno mužským pohlavím. Ženy jsou zastoupeny zbylými 11 %.

5.3 Trendy a potenciální možnosti zlepšení informační podpory

Na základě analýz a hodnocení vyplývajících z dotazníkového šetření vyplývá, že bezpečnostní manažeři jsou převážně spokojeni jak s dostatkem informačních zdrojů potřebných pro výkon jejich práce, tak i s technickými prostředky, které jim usnadňují a zefektivňují jejich práci. Potenciální možnost zlepšení informační podpory bych proto viděl především v integraci aplikací, systému a databází, které bezpečnostní manažer využívá při své práci. Tato integrace umožní jednak zefektivnění práce bezpečnostního manažera a jednak nebudou problémy s kompatibilitou. Takovouto integraci lze zajistit pomocí ***Cloud computingu***.

5.3.1 Cloud computing

Výraz Could computing se dá volně přeložit jako počítačový mrak, počítačové nebe. Co všechno dokážeme pomocí cloud computingu a co nám umožní?

Základní myšlenkou Cloud computingu je poskytovat hardware, software anebo vývojovou a aplikační platformu ve formě služby. Samotný zákazník musí vlastnit pouze nějaký terminál umožňující mu přístup ke službám cloudu (např. počítač, notebook, mobil, tablet apod.) a konektivitu k internetu. Jedná se o léta ověřený koncept, který využívají stovky milionů uživatelů po celém světě. V cloudu můžete mít poštovní server, CRM systém, intranetový portál anebo třeba jen serverovou infrastrukturu pro naše vlastní aplikace.[26]

Technologie Cloud computingu se vyznačuje následujícími atributy:

- multitenancy - tento pojem lze volně přeložit jako "více nájmů". Jedná se o to, že počítačové zdroje jsou sdílené mezi všemi uživateli;
- obrovská škálovatelnost a elasticita - umožní uživatelům rychle změnit výpočetní zdroje dle potřeby;
- pay as you go - tento přístup je založen na principu kolik toho uživatel spotřebuje, tolik zaplatí;
- aktualizovanost (Up-to-date) - všechen software jsou automaticky aktualizovaný, uživatel nemusí do tohoto procesu nijak zasahovat, vše zařídí poskytovatel;
- přístup přes internet - uživatelé se mohou ke svému softwaru připojit kdekoliv po celém světě. [27]

Rozdělení Cloud computingu:

Cloud computing dělíme podle služby, kterou poskytují a podle toho, jak je poskytován.

Model nasazení

Tento model nám říká jak je cloud poskytován.

- Veřejný (Public cloud computing) - někdy je označován jako klasický model cloud computingu. Jedná se o model, kdy je poskytnuta a nabídnuta široké veřejnosti výpočetní služba.
- Soukromý (Private cloud computing) - oblak je v tomto případě provozován pouze pro organizaci a to buď organizací samotnou, nebo třetí stranou.
- Hybridní (Hybrid cloud computing) - hybridní cloudy kombinují jak veřejné, tak soukromé cloudy. Navenek vystupují jako jeden cloud, ale jsou propojeny pomocí standardizačních technologií.

- Komunitní (Comunity cloud computing) - jedná se o model, kdy je cloud infrastruktura sdílena mezi několika organizacemi skupinou lidí, kteří ji využívají. Tyto organizace může spojovat bezpečnostní politika, stejný obor zájmu. [27]

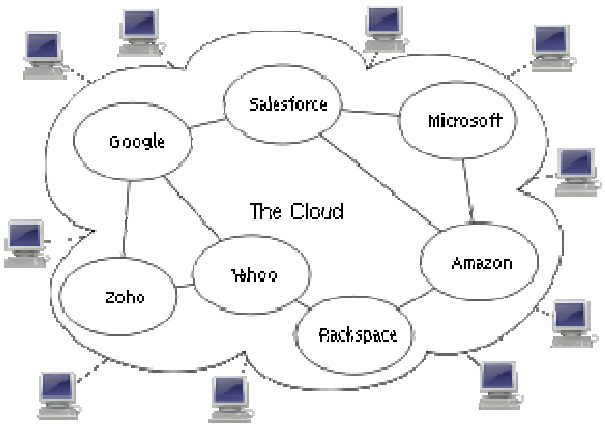
Distribuční model

Model se zabývá tím, co je v rámci služby nabízeno, obvykle software nebo hardware, či jejich kombinace.

- IAAS — infrastruktura jako služba (z "Infrastructure as a Service") — v tomto případě poskytovatel služeb se zavazuje poskytnout infrastrukturu. Typicky se jedná o virtualizaci. Hlavní výhodou tohoto přístupu je to, že se o veškeré problémy s hardwarem stará poskytovatel. Na druhou stranu je někdy velice těžké toto akceptovat vzhledem k tomu, že hardware se bere jako něco, co vlastníme, na co můžeme sáhnout a jsme za to zodpovědní. IAAS je vhodné pro ty, kteří vlastní software (či jejich licence) a nechtějí se starat o hardware. Příkladem IAAS jsou Amazon WS, Rackspace nebo Windows Azure. Zkratka IAAS může také znamenat integrace jako služba (z "Integration as a Service").
- PAAS — platforma jako služba (z "Platform as a Service") — poskytovatel v PAAS modelu poskytuje kompletní prostředky pro podporu celého životního cyklu tvorby a poskytování webových aplikací a služeb plně k dispozici na Internetu, bez možnosti stažení softwaru. To zahrnuje různé prostředky pro vývoj aplikace, jako je IDE, nebo API, ale také např. pro údržbu. Nevýhodou tohoto přístupu je proprietární uzamčení, kdy může každý poskytovatel používat např. jiný programovací jazyk. Příkladem PAAS poskytovatelů jsou Google App Engine nebo Force.com (Salesforce.com).
- SAAS — software jako služba (ze "Software as a Service") — aplikace je licencována jako služba pronajímaná uživateli. Uživatelé si tedy kupují přístup k aplikaci, ne aplikaci samotnou. SaaS je ideální pro ty, kteří potřebují jen běžné aplikační software a požadují přístup odkudkoliv a kdykoliv. Příkladem může být známá sada aplikací Google Apps, nebo v logistice známý systém Cargopass. [27]

Vzhledem k tomu, že internet je doménou současnosti a je k němu připojeno 99 % organizací, vidím cloud computing jako trend budoucnosti nejen v organizacích, ale i v domácnostech. Jak již bylo na začátku zmíněno, cloud computing je počítačový mrak. Jedná se o ukládání věcí (dokumenty, fotky, filmy, e-maily, tabulky i celé programy),

někde do prostoru internetu, mraku. To přináší velkou výhodu v tom, že pokud se chceme dostat k našim datům, tak není potřeba být doma (v organizaci), popř. nosit sebou flash disk či jiné paměťové medium. Stačí mít připojení k internetu a nějaké zařízení umožňující přístup ke cloudu (tj. počítač, mobil, notebook, tablet apod.). Další výhodu cloud computingu vidím v tom, že pokud by náhodou vyhořel náš počítač, server, tak nepřijdeme o žádná data, protože je máme uloženy někde v mracích na jiných serverech.



Obr. 19 Znázornění Cloud computingu

Pokud se na Cloud computing podíváme z hlediska ekonomického, tak jeho základní myšlenkou je eliminace investičních výdajů na straně zákazníka. Vše je poskytováno formou služby, a tudíž za pravidelný měsíční, případně roční, poplatek, jehož výše závisí na počtu uživatelů a/nebo parametrech služby (např. kapacitě diskového prostoru). Sekundárně však dochází i ke snižování podnikatelského rizika a celkových provozních nákladů. Firma využívající cloud si nemusí platit žádné vlastní IT odborníky, nemusí kupovat žádný vlastní serverový software ani hardware a v případě, že už nechce nebo nepotřebuje danou službu využívat, tak její využívání ukončí, a to bez nákladů na odprodej hardware a hlavně bez nákladného propouštění zaměstnanců. Firma také platí skutečně jen to, co potřebuje. Nemusí si kupovat nadbytečné kapacity do zálohy, protože je má v případě potřeby během pár minut k dispozici. [26]

Možný problémem vidí spousta lidí v oblasti bezpečnosti a to především v úniku citlivých informací. Cokoli ovšem nahrajeme do cloudu, tak je šifrované a nikdo by se k tomu neměl dostat. Pro větší bezpečnost lze využít privátní cloud, který může sloužit pro provoz kritických aplikací. Také statistiky ukazují, že nejvíce úniků informací je zapříčiněno tím, že dojde ke krádeži počítače či harddisku.

5.3.2 **Návrh Cloud computingu**

Pro práci bezpečnostních manažerů bych navrhl hybridní cloud computing. To znamená, že budeme mít k dispozici cloud veřejný i soukromý. Veřejný cloud je model, ve kterém je poskytnuta výpočetní služba široké veřejnosti. K soukromému cloudu bude mít přístup pouze jedna daná organizace či člověk, který bude znát přístupový kód. V takto navrženém cloudu by se potom objevovaly různé druhy aplikací např. kancelářský balík, speciální softwary a jiné dokumenty se kterými bezpečnostní manažeři pracují. Cloud computing by pak byl výhodný nejen v tom, že by se ušetřily peníze za zaměstnance, který se stará o informační technologie v organizaci, ale nevznikaly by i problémy s kompatibilitou. Další výhodu proč použít tento systém vidím ve vzájemné spolupráci jednotlivých bezpečnostních manažerů z různých organizací.

5.4 Shrnutí

Dotazníkového šetření se zúčastnili bezpečnostní manažeři ve věku od 21 let z různých typů organizací. Co se týká jejich vzdělání, tak 59 % z nich disponuje SŠ/VŠ vzděláním souvisejícím s jejich pracovní pozicí. Zbylých 41 % respondentů buď: nemá žádné vzdělání, nebo absolvovali kurzy, anebo jsou to samouci v tomto oboru. Co se týká zastoupení mužů a žen, tak 89 % respondentů jsou muži. Většina z dotázaných uvedla, že pro výkon jejich práce existuje dostatek informačních zdrojů, ze kterých můžou čerpat. Většina těchto zdrojů se pak přímo nachází v informačních systémech organizace, ve které pracují. Nejčastěji ke své činnosti využívají zákon/vyhlášku, www stránky, e-mail a odborného semináře.

Více jak jednu oblast bezpečnosti řídí 81 % dotázaných. Mezi nejčastější oblasti bezpečnosti, které respondenti řídí, pak patří BOZP, PO, fyzická bezpečnost a krizové řízení. Větší polovina (59 %) respondentů se vyjádřila k tomu, že není potřeba, aby každý úsek bezpečnosti měl jednoho bezpečnostního manažera. Více bezpečnostních manažerů v organizaci by zvolili pouze u velkých organizací. Vlastního bezpečnostního manažera by měla mít pouze oblast informační bezpečnost, kterou považují za specifičtější obor. Respondenti se dále vyjádřili k tvorbě interních předpisů, při kterých využívají poznatků z dříve vzniklých bezpečnostních incidentů v organizaci. Pokud vznikne bezpečnostní incident, požadují respondenti informace přesné, aktuální, úplné, srozumitelné a rychlé.

Při práci dotázaní bezpečnostní manažeři nejčastěji používají mobilní telefon, osobní počítač, MS Office a notebook. Využívají ovšem i specializovaný software, který je určen především pro řízení BOZP (např. RISCON, SIB_LEX), dále software ARGIS (nástroj informační podpory hospodářských opatření pro krizové stavy v oblasti zajišťování věcných zdrojů), KRIZKOM (nástroj informační podpory pro řízené a evidované předávání požadavku na věcné zdroje, které orgány krizového řízení potřebují k překonání krizové situace nebo k odstranění jejich následků) a další různé databáze obsahující předpisy a rizika. Se svými technickými prostředky je většina respondentů spokojena. Na nákup nových popř. správu stávajících technických prostředků spíše nemá dostatek financí 33 % respondentů. Zbylých 67 % má, spíše má, nebo neví, zda má dostatek finančních zdrojů na nákup nových technických prostředků. Mají-li respondenti pracovat s novým technickým prostředkem, považuje většina z nich za optimální řešení nechat se zaškolit odborníkem. Pokud zde provedeme srovnání věkových skupin tak zjistíme, že respondenti do 40 let (78 % z nich) považuje za optimální řešení zkoušet si nový technický prostředek sám popř. se podívat do jeho manuálu. Naproti tomu respondenti nad 41 let dávají přednost nechat se zaškolit odborníkem.

Pokud jde o nové trendy v oblasti informační podpory bezpečnostních manažerů tak se to bude týkat především nových technických prostředků, ať už se bude jednat o hardware, či software. Záležet bude na každém bezpečnostním manažerovi, co bude považovat za nejoptimálnější řešení pro výkon své práce. Další možnost zlepšení informační podpory bych pak viděl v integraci aplikací, systémů a databází, které bezpečnostní manažer využívá při své práci. Tato integrace umožní jednak zefektivnění práce bezpečnostního manažera, dále nebudou vznikat problémy s kompatibilitou, sníží se náklady organizace vynaložené na placení IT odborníků a softwaru. Takovou integraci lze zajistit pomocí již zmíněného Cloud computingu.

ZÁVĚR

V diplomové práci je řešena problematika informační podpory bezpečnostního manažera. V první polovině práce je objasněna působnost bezpečnostního manažera, vztahy mezi informacemi a daty a základní pojmy v informačních systémech. Druhá část práce je pak již přímo zaměřena na informační potřeby bezpečnostních manažerů, jejich technické prostředky a softwarové nástroje. V posledním bodu je provedeno zhodnocení práce bezpečnostních manažerů pomocí dotazníkového šetření a možnosti zlepšení jejich informační podpory.

Hlavní náplní a cílem této práce byla analýza informačních potřeb bezpečnostního manažera a jeho technických prostředků a softwarových nástrojů, které využívá k usnadnění své práce a následné zhodnocení a možnosti zlepšení informační podpory bezpečnostních manažerů.

Při zpracování informačních potřeb bylo vycházeno z působnosti bezpečnostních manažerů a z jejich pracovních náplní. Bezpečnostní management je možno rozdělit do několika oblastí např. požární ochrana, bezpečnost a ochrana zdraví při práci, ochrana utajovaných informací, ostraha a bezpečnostní technologie apod. V každé oblasti bezpečnosti jsou pak v této práci specifikovány základní informace, které jsou nezbytné pro výkon práce bezpečnostního manažera a zároveň mu pomáhají dosáhnout stanovených cílů. Dále bezpečnostní manažer využívá ke své práci a k efektivnějšímu dosahování stanovených cílů technické prostředky a různé druhy softwaru. Mezi nejčastěji využívané technické prostředky pak patří osobní počítač s kancelářským softwarem MS Office a mobilní telefon. To vyplývá z dotazníkového šetření, které bylo provedeno a jeho výsledky jsou součástí této diplomové práce. Z průzkumu dále vyplývá, že bezpečnostní manažeři jsou převážně spokojeni jak s dostatkem informačních zdrojů, tak i s technickými prostředky, které používají. Na základě vyhodnocení dotazníkového šetření vyplývá, že zlepšení informační podpory bezpečnostních manažerů je především v integraci aplikací, systémů a databází, které jsou využívány při jejich práci. Docílí se tím zefektivnění jejich práce a odstraní se problémy s kompatibilitou.

Diplomová práce může posloužit jako podkladový materiál nejen pro začínající a stávající bezpečnostní manažery, ale i pro vlastníky a manažery organizací, firem, institucí.

ZÁVĚR V ANGLIČTINĚ

The thesis approaches the problem of information support of the security manager. In the first half of the work is to clarify the scope of the security manager, the relationship between information and data and basic concepts in information systems. The second part is then directly targeted at the needs of information security managers and their technical resources and software tools. The last point is an assessment work of the security managers through the survey and ways to improve their information support.

The main scope and purpose of this study was to analyze the information needs of the security manager and technical resources and software tools used to facilitate their work and subsequent evaluation and ways to improve information support for security managers.

The processing of information needs to begin by the scope of security managers and their job descriptions. Safety management can be divided into several areas such as fire protection, health and safety at work, protection of classified information, surveillance and security technologies, etc. Each security is then in this work vyspecifikovány basic information necessary for work safety manager and give him help to achieve their goals. Furthermore, the security manager used to work more efficiently and achieve the objectives of technical equipment and various types of software. The most commonly used technical means is a personal computer with MS Office software, office and mobile phone. It is clear from the survey that was conducted and its results are included in this thesis. The survey also shows that security managers are largely satisfied with plenty of information sources, and with the technical means they use. Based on the evaluation survey suggests that improving information support for security managers is mainly the integration of applications, systems and databases that are used in their work. We can gain by streamlining their work and eliminate problems with compatibility.

This thesis can serve as background material for beginners and existing security managers but also for owners and managers of organizations, companies, institutions.

SEZNAM POUŽITÉ LITERATURY

[1] ČECH, Pavel; BUREŠ, Vladimír. *Podniková informatika.* Hradec Králové: GAUDEAMUS, 2009. 232 s. ISBN 978-80-7041-479-8.

[2] FRYŠAR, Miroslav, et al. Bezpečnost pro manažery, podnikatele a politiky. Praha: Public History Praha, 2006. 176 s. ISBN 80-86445-22-4.

[3] HANDLÍŘ, Jiří. *Management pro střední a vyšší odborné školy.* Praha: Vydavatelství a nakladatelství Computer Press, 1998. 268 s. ISBN 80-7226-095.

[4] HARTL, Pavel, HARTLOVÁ, Helena. *Psychologický slovník.* Praha: Portál, 2000. 776 s. ISBN 80-7178-303-X.

[5] JUDr. LAUCKÝ, V.: Technologie komerční bezpečnosti., 2. vyd. Univerzita Tomáše Bati ve Zlíně, červen 2004. ISBN 80-7318-194-0.

[6] LUKÁŠ, Luděk; HRŮZA, Petr; KNÝ, Milan. *Informační management v bezpečnostních složkách.* Praha: Ministerstvo obrany - Agentura vojenských informací a služeb, 2008. 214 s. ISBN 978-80-7278-460-8.

[7] PETRUSEK, Miloslav. *Teorie a metoda v moderní sociologii.* Praha: Karolinum, 1993. 204 s. ISBN 80-7066-799-0.

[8] POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005. 311 s. ISBN 80-86898-38-5.

[9] POŽÁR, Josef. *Manažerská informatika.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2010. 357 s. ISBN 978-80-7380-276-9.

[10] SCHNEIDER, Milan, KOUDELKA, Ferdinand. *Úvod do základů sociologických výzkumů.* Olomouc: Vydavatelství Univerzity Palackého v Olomouci, 1993. 118 s. ISBN 80-7067-302-8.

[11] ŠULER, Oldřich. *5 rolí manažera a jak je profesně zvládnout?.* Praha: Vydavatelství a nakladatelství Computer Press, a.s., 2008. 240 s. ISBN 978-80-251-2316-4.

[12] VEBER, Jaromír, et al. *Management: Základy - prosperita - globalizace.* Praha: Management Press, 2000. 700 s. ISBN 80-7261-029-5.

[13] Zákon č. 412/2005 Sb., Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.

[14] Zákon č. 240/2000 Sb., Zákon o krizovém řízení a o změně některých zákonů (krizový zákon).

[15] Zákon č. 133/1985 Sb., Zákon o požární ochraně.

[16] Zákon č. 101/2000 Sb., Zákon o ochraně osobních údajů a o změně některých zákonů.

[17] Zákon *č. 59/2006 Sb.* zákon o prevenci závažných průmyslových havárií způsobených vybranými chemickými látkami nebo chemickými přípravky.

[18] KUČEROVÁ, Helena. SKS [online]. 2009 [cit. 2011-03-04]. Informační systém. Dostupné z WWW: <http://web.sks.cz/users/ku/ZIZ/isystem.htm#cile>.

[19] Wolters Kluwer ČR [online]. 2009 [cit. 2011-03-05]. Co je systém ASPI. Dostupné z WWW: <http://www.systemaspi.cz/Co_je_system_ASPI/Co_je_system_ASPI.html>.

[20] T-SOFT a.s. [online]. 2009 [cit. 2011-03-09]. RISKAN. Dostupné z WWW: <http://www.tsoft.cz/riskan>.

[21] T-SOFT a.s. [online]. 2009 [cit. 2011-03-09]. TEREX. Dostupné z WWW: <http://t-soft.cz/terex>.

[22] Risk Analysis Konzultans [online]. 2010 [cit. 2011-03-10]. CRAMM. Dostupné z WWW: <http://www.rac.cz/rac/homepage.nsf/CZ/CRAMM-AR>.

[23] SPBI [online]. 2007 [cit. 2011-03-12]. SFERA. Dostupné z WWW: <http://www.spbi.cz/eshop/shop.php?param1=REVUQUlMLDgwLTg2NjM0LTg3LTY>.

[24] Wapedia [online]. 2010 [cit. 2011-03-15]. ALOHA. Dostupné z WWW: <http://www.spbi.cz/eshop/shop.php?param1=http://wapedia.mobi/cs/ALOHA>.

[25] T-SOFT [online]. 2009 [cit. 2011-03-15]. EMOFF. Dostupné z WWW: <http://www.tsoft.cz/emoff-emergency-office>.

[26] HRUŠKA, David. ITBIZ [online]. 2011 [cit. 2011-04-10]. Cloud computing v praxi. Dostupné z WWW: <http://www.itbiz.cz/cloud-computing-v-praxi-maly-pohled-do-historie-aneb-vse-co-jste-o-nem-chteli-vedet-ale-bali-jste-se-zeptat>.

[27] Wikipedia [online]. 2011 [cit. 2011-04-10]. Cloud computing. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Cloud_computing>.

[28] Wikipedia [online]. 2011 [cit. 2011-03-21]. Dataprojektor. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Dataprojektor>.

[29] Úspěšná prezentace [online]. 2007 [cit. 2011-03-21]. Dataprojektor. Dostupné z WWW: <http://www.uspesnaprezentace.cz/pomucky-a-technika/dataprojektor/>.

[30] Netservis [online]. 2011 [cit. 2011-03-25]. Intranet. Dostupné z WWW: <http://www.netservis.cz/intranet.php>.

[31] Wikipedia [online]. 2011 [cit. 2011-03-25]. Intranet. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Intranet>.

[32] Inetmag [online]. 2007 [cit. 2011-03-27]. Internet. Dostupné z WWW: <http://www.inetmag.cz/>.

[33] Wikipedia [online]. 2011 [cit. 2011-03-27]. Internet. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Internet>.

[34] Wikipedia [online]. 2011 [cit. 2011-03-28]. Osobní počítač. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Osobní_počítač>.

[35] Wikipedia [online]. 2011 [cit. 2011-03-28]. Počítač. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Počítač>.

[36] Online-slovník [online]. 2011 [cit. 2011-03-28]. Slovník. Dostupné z WWW: <http://www.online-slovnik.cz/>.

[37] Wikipedia [online]. 2011 [cit. 2011-03-28]. Počítač. Dostupné z WWW: < http://cs.wikipedia.org/wiki/Manažer>.

SEZNAM OBRÁZKŮ

Obr. 19 Wikipedia [online]. 2011 [cit. 2011-04-10]. Znázornění Cloud computingu. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Cloud_computing>.

SEZNAM GRAFŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK K DIPLOMOVÉ PRÁCI

Vážený respondente, dovoluji si Vás požádat o vyplnění tohoto dotazníku. Cílem je zjistit, jak bezpečnostní manažer pracuje s informacemi, jak je získává či využívá a jaké technické prostředky k tomu používá. Výsledky dotazníku budou využity při zpracování mé diplomové práce na téma Informační podpora bezpečnostního manažera.

Vyplnění dotazníku Vám zabere přibližně 10 min.

Děkuji Vám za čas a ochotu, kterou budete věnovat vyplňování tohoto dotazníku. Vyplněný dotazník, prosím, zašlete na následující e-mail: brh.honzik@post.cz

S pozdravem

Jan Brhel

Otázka č. 1

Existuje dostatek informačních zdrojů pro výkon Vaší práce?

☐ ano ☐ spíše ano ☐ nevím ☐ spíše ne ☐ ne

Otázka č. 2

Nachází se v informačních systémech organizace dostatek informací potřebných k výkonu Vaší práce?

☐ ano ☐ spíše ano ☐ nevím ☐ spíše ne ☐ ne

Otázka č. 3

Označte pět informačních položek, které využíváte ke své činnosti nejčastěji.

☐ obrázek
☐ videozáznam
☐ excelovská tabulka
☐ analýza
☐ e-mail
☐ odborný seminář
☐ www stránka
☐ zákon / vyhláška
☐ prezentace

☐ odborný časopis

☐ zahraniční zdroje

Otázka č. 4

Každý manažer se setkává se základními informačními činnostmi, kterými jsou: vyhledávání informací, rutinní zpracování dat, tvůrčí vytváření informačního obsahu, prezentace a komunikace. Stanovte pořadí výše uvedených činností z hlediska četnosti provádění (1 – nejčastěji, 5 – nejméně často).

☐ vyhledávání informací

☐ rutinní zpracování dat

☐ tvůrčí vytváření informačního obsahu

☐ prezentace

☐ komunikace

Otázka č. 5

Řídíte více jak jednu oblast bezpečnosti?

☐ ano ☐ ne

Otázka č. 6

Uveďte, jakou oblast/ti bezpečnosti v organizaci řídíte (např. bezpečnost a ochrana zdraví při práci (BOZP); požární ochrana; fyzická bezpečnost; informační bezpečnost; krizové řízení)

Otázka č. 7

Myslíte si, že by bylo lepší, aby každý úsek bezpečnosti měl jednoho bezpečnostního manažera?

☐ ano ☐ ne

A mohl/a byste uvést proč?

Otázka č. 8

Prověřujete v praxi fungování interních předpisů týkajících se bezpečnosti?

☐ ano ☐ spíše ano ☐ spíše ne ☐ ne

Otázka č. 9

Využíváte při tvorbě a aktualizaci interních předpisů praktických poznatků z bezpečnostního incidentu?

☐ ano ☐ spíše ano ☐ spíše ne ☐ ne

Otázka č. 10

Očíslujte vlastnosti informací, které jsou pro Vás nejvíce důležité při vzniku bezpečnostního incidentu (1 – nejvíce důležité, 5 – nejméně důležité).

☐ přesnost ☐ rychlost ☐ aktuálnost ☐ úplnost ☐ srozumitelnost

Otázka č. 11

Každý člověk přistupuje k vytváření svého informačního prostředí jinak. Využívá k zajištění informací nezbytné nástroje, technologie, kancelářské pomůcky. Z uvedeného přehledu vyberte položku, která nejlépe vystihuje Vaše informační prostředí:

☐ hodně sázím na techniku, chci vždy nejnovější počítač, telefon, MS Office, protože mají nejvíce funkcí, které mohu ke své práci využít

☐ v informacích chci mít pořádek, mám v tom systém a radši vše zálohuji

☐ i když se snažím, v záplavě informací se ztrácím, často nevím, jestli jsem si soubor uložil do počítače, notebooku, nebo flash disk

☐ když něco dělám, snažím se o tom přemýšlet a mít potřebné informace po ruce

☐ vaše formulace:

Otázka č. 12

Jste spokojen se svými současnými technickými prostředky?

☐ ano ☐ spíše ano ☐ nevím ☐ spíše ne ☐ ne

Otázka č. 13

Označte 4 technické prostředky, které nejčastěji využíváte při práci?

- ☐ osobní počítač
- ☐ notebook
- ☐ mobilní telefon
- ☐ datový projektor
- ☐ magnetická tabule
- ☐ MS Office
- ☐ specializovaný software
- ☐ jiné:

Otázka č. 14

V případě, že využíváte specializovaný software, uveďte jaký.

Otázka č. 15

Máte dostatek financí na správu současných, popř. na nákup nových technických prostředků?

☐ ano ☐ spíše ano ☐ nevím ☐ spíše ne ☐ ne

Otázka č. 16

Máte-li se naučit pracovat s novým technickým prostředkem, je pro Vás optimálním řešením:

- ☐ přečíst si manuál a podle něj se to naučit
- ☐ sám si zkoušet nový prostředek bez návodu
- ☐ sám si zkoušet nový prostředek, a pokud si nevím rady podívám se do návodu
- ☐ nechat se zaškolit odborníkem

Otázka č. 17

Kolik let pracujete na pozici bezpečnostního manažera v organizaci?

☐ méně než 5 ☐ 6 - 10 ☐ 11 - 15 ☐ 16 - 20 ☐ 21 a více

Otázka č. 18

Jaké máte vzdělání v oblasti bezpečnosti?

☐ SŠ/VŠ související s pracovní pozicí ☐ samouk ☐ kurzy ☐ žádné

Otázka č. 19

Kolik je Vám let?

☐ méně než 20 ☐ 21 - 30 ☐ 31 - 40 ☐ 41 - 50 ☐ 51 a více

Otázka č. 20

Jaké je Vaše pohlaví?

☐ žena ☐ muž