Univerzita Karlova v Praze

FILOZOFICKÁ FAKULTA

ÚSTAV INFORMAČNÍCH STUDIÍ A KNIHOVNICTVÍ

Rigorózní práce

Mgr. Tomáš Bien

Competitive Intelligence: aspekt ochrany informací a informačního systému

Competitive Intelligence: aspect of protection information and information system

Konzultant: PhDr. Beáta Sedláčková, Ph.D.

2012

Prohlašuji, že jsem rigorózní práci vypracoval samostatně a že jsem uvedl všechny použité prameny a literaturu.

V Praze dne …… Tomáš Bien ……

Anotace

Rigorózní práce se zabývá konkurenčním zpravodajstvím v současném podnikatelském prostředí a oblasti státní správy. Zaměřuje se na význam ochrany informací v organizacích a informačních systémech před úniky a ztrátami důležitých informací. Analyzuje příčiny a důvody zneužívání informací. Navrhuje metodiku zabezpečení ochrany utajovaných informací v konkurenčním prostředí organizace. Práce se opírá o ochranu informací v právních normách. Cílem práce je stanovit preventivní opatření proti únikům a ztrátám důležitých informací a stanovení příčin a podmínek zločinnosti v oblasti práce s informacemi.

Klíčová slova: konkurenční zpravodajství, informace, informační systémy, ochrana informací

Annotation

The rigorous thesis deals with competitive reporting in the current business enviroment and the area of public administration. It focuses on the importance of protecting information and information systems in organizations from fraud and loss of important information. Analyzes the causes and the reasons for the abuse of information. Proposes a methodology for ensuring protection of classified information in a competitive atmosphere organization. The work is based on the protection of information in legal standards. The aim of the work is to establish preventive measures against fraud and loss of important information and determine the causes and circumstances of crime in the are of work with the information.

Keywords: competitive intelligence, infromation, information systems, protection of information

Obsah

Úvod

Rigorózní práce se zabývá konkurenčním zpravodajstvím a působením informací v podnikatelském prostředí, ale též státní sféře, jelikož informace bere na sebe roli významné strategické zbraně. Působení v dnešním globalizovaném světě vyžaduje neustále nové metody a přístupy. Bez těchto moderních metod a trendů se dnes neobejde žádná organizace. Informace mají, a budou mít, v dnešním světě klíčovou roli. Obzvláště v tržním mechanismu představují významnou výhodu pro soutěžící subjekty. Roste množství příležitostí a hrozeb, složitost vztahů mezi konkurenty a rychlost, s jakou se dění na trhu odehrává. Bez systematického vyhodnocování informací dnes již nikdo není schopen využitelné příležitosti, reálné hrozby a důležité změny ani identifikovat a ani na ně adekvátně a včas zareagovat. V této souvislosti dochází také k únikům, ztrátám a zneužívání informací. Na významu a nepostradatelnosti pro organizace nabývají také informační technologie, jenž jsou a vždy budou nástrojem, který lidé mohou používat k tomu, aby lépe a efektivněji vykonávali to, co považují za potřebné či vhodné vykonávat. Kvalitativní změna je v tom, že možnosti tohoto nástroje radikálně mění naše dosavadní představy o tom, co je dosažitelné, schůdné a realizovatelné. Jelikož počátky konkurenčního zpravodajství mají kořeny v činnosti státní bezpečnosti a vojenských služeb, budou proto v práci aplikovány metody a poznatky z mého působení v Celní správě České republiky, jakožto organizace, denně přicházející do styku s širokou sférou podnikatelské veřejnosti a dalšími orgány státní správy.

První kapitola pojednává o konkurenčním zpravodajství, označovaném jako Competitive Inteligence (CI). V zásadě se jedná o legální shromažďování a analýzu informací, týkajících se strategie konkurence, schopností a zranitelnosti s využitím veřejně přístupných a dostupných zdrojů informací. Jedním z problémů českého podnikatelského prostředí je přetrvávající informační izolace firem. Tento stav je přirozeným důsledkem toho, že firemní informační systémy jsou vytvářeny především pro podporu standardních procesů a není v nich příliš velký prostor pro individuální a kreativní formy zpracování informací. CI je stručně řečeno řízené monitorování všech našich konkurentů a analýza zjištěných informací. Jedná se o systém jak se zajímat o své obchodní protivníky a jak nakládat s informacemi, které zjistíme. Možnost získávat důležité informace je také zakotvena v právních předpisech. Základním právním předpisem obsahujícím komplexní úpravu práva na informace je zákon číslo 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Jedná se o

obecný právní předpis, který zajišťuje právo veřejnosti na informace, které mají k dispozici státní orgány, orgány územní samosprávy a další subjekty, jenž rozhodují na základě zákona o právech a povinnostech občanů a právnických osob.

Druhá kapitola se zabývá současným podnikatelským prostředím a podnikatelskou strategií. Orientace v tomto prostředí, se všemi jeho problémy, není jednoduchá. Ještě náročnější je najít si v tomto složitém prostředí vlastní cestu, tedy strategii. Strategie stojí na počátku procesu, kterým se lidské myšlenky mění ve skutečnost a kterým člověk tuto skutečnost aktivně ovlivňuje a přetváří. Moderní společnost stojí právě na základě takovéhoto vědomého přetváření skutečnosti. Jakákoliv firma, která se chce dnes prosadit na trhu, má své určité tržní zájmy. Z těchto zájmů se odvíjejí určité cíle, kterých chce firma dosáhnout na určitém trhu v určitém časovém období. Na základě takto jasně stanovených cílů se vytváří firemní strategie. Řešení konkurenčního boje je pro vrcholový management firmy velice složitou, náročnou a značně rizikovou záležitostí, vyžadující značné zkušenosti a vysokou úroveň znalostí. Informace důležité pro rozhodování jsou dostupné na úrovni, na které je třeba rozhodnutí provést. Za každým úspěchem stojí schopnost včasné mobilizace a zužitkování dostupných informací. Získávání informací pro vlastní potřebu podnikání se vztahuje ke zdroji informace a místu sledované činnosti. Z důvodu neustále rostoucích požadavků na IT systémy a zvyšující se závislosti na nich, je i tlak na rozsáhlá bezpečnostní opatření stále větší. Aby se potřebné celkové náklady na bezpečnost IT minimalizovali, využívají se v praxi většinou standardní soubory kritérií, které osoby odpovědné za bezpečnost podporují po metodické nebo obsahové stránce. V této části formou srovnání budou posouzeny tyto soubory kritérií, jenž zahrnují standardy s největší relevancí ve sledované tématické oblasti: ISO/IEC 17799:2005 a ISO 27001:2006, ISO TR 13335, ITSEC/Common Criteria a CobiT.

Vzhledem k tomu, že každá organizace by měla mít vyvinutý systém strategií, které díky vzájemné provázanosti a synergickému efektu pomohou organizaci v dosahování stanovených cílů, bude se třetí kapitola zabývat informační strategií na příkladu Celní správy ČR. Česká celní správa, stejně jako celní správy ostatních států, má dva základní úkoly, kterými jsou ochrana a regulace domácího trhu formou výběru cla z dováženého zboží a dohled nad tímto zbožím. Bude zde také pojednáváno o pravidlech bezpečné výměny dat informačního systému Celní správy ČR (ISCS), a to tak, aby byla zajištěna bezpečnost přenášených dat i souvisejících komunikačních prostředků a aby datové přenosy nebyly zdrojem bezpečnostních incidentů. Komunikační prostředky ISCS musí být odolné proti vlastním chybám tak, aby nebylo možným zdrojem

ztráty důvěrnosti, integrity a dostupnosti přenášených dat anebo možným zdrojem nedostupnosti komunikačních služeb ISCS.

V současné době je vysoce aktivní ztráta informací, zejména jestliže je zpracováváme či uchováváme prostřednictvím výpočetní techniky. Problematikou ochrany informací se zabývá čtvrtá kapitola. Neúprosný konkurenční boj snižuje úroveň společenské hierarchie, na níž je třeba informace chránit. Tedy nejen na úrovni vrcholové, ale i na stupních nižších. Ochrana informací se stává významným faktorem soudobého úspěchu či naopak neúspěchu podniku. Skutečností je, že v oblasti automatizovaných informačních systémů, tedy při využívání výpočetní techniky, se problém nedovoleného získávání informací dostal až k páchání trestné činnosti. Nezřídka se v této oblasti setkáváme také s praktikami týkající se průmyslové špionáže.

Kapitola pátá pojednává již o samotných příčinách, důvodech úniku, ztrátách a zneužívání informací. Je zde v hojné míře aplikován zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. Protože je třeba poukázat na fakt, že informace může být získávána a využívána racionálním, zákonným či nekonfliktním způsobem, ale také na druhé straně, že se může stát objektem, předmětem a nástrojem zločinu. Každý občan, a to jak fyzické osoby, tak i právnické, je také spotřebitelem informací. Proto i v této oblasti může docházet k trestným činům různé povahy a nebezpečnosti. Vznik a přežívání zločinnosti v oblasti práce s informacemi, jsou zvláště v této oblasti charakterizovány složitými vazbami.

Poslední, šestá kapitola, je zaměřena v největší míře na praktické využití v nejrůznějších typech organizací, a to všude tam, kde je potřeba vytvořit konkrétní metodiku pro plnění úkolů vyplývajících ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a prováděcích právních předpisů Národního bezpečnostního úřadu v konkurenčním prostředí, a to zejména v oblasti personální, administrativní a fyzické bezpečnosti, registru utajovaných informací a certifikaci informačních systémů. Dále je zde nastíněna bezpečnostní politika. Bezpečnostní politika přijatá vedením organizace, slouží jako návod a podpora k zavedení a zachování bezpečnosti informací. Ze strany vedení organizace je proto nutné zveřejnit jasné prohlášení k zavedení bezpečnosti informací v organizaci. Tento vrcholný dokument tvoří špičku pyramidy dokumentů, která pokrývá všechny aspekty IS od těchto zásad až po technické popisy.

1 Competitive intelligence

Není pochyb o tom, že základem konkurenceschopnosti je správné rozhodování, správná a rychlá reakce na změny v konkurenčním prostředí. Faktem je, že podkladem pro správné rozhodnutí jsou správné informace. Prudký rozvoj informačních a komunikačních technologií dramatickým způsobem ovlivnil všechny oblasti našeho života a podnikání, díky tomu, že je možné informace snadno vytvářet, sdílet a přenášet. Schopnosti lidského mozku se ale přitom výrazně nemění. Na jedné straně je tedy rostoucí přetlak informací, které reflektují stále rychlejší, složitější a globálnější procesy, a na straně druhé jsou omezené kapacity člověka tyto informace přijímat. Z těchto důvodů dochází k tomu, že člověk informace záměrně filtruje a k rozhodování využívá více své intuice a zkušenosti než objektivní fakta. V případě jednotlivce to může způsobit nemilá překvapení nebo zmařené příležitosti. Daleko vážnější důsledky to ale může mít v případě manažera firmy odpovědného za majetek akcionářů a pracovní místa lidí nebo v případě veřejného činitele, který odpovídá za veřejné prostředky či bezpečnost.

Competitive Intelligence (dále jen „CI“) je obor, který vznikl z naléhavé potřeby organizací lépe vyhodnocovat a využívat informace o svém okolí pro své rozhodování. Úkolem CI je realizovat proces organizovaného informování těch, kdo rozhodují o dění vně organizace, o dopadu na organizaci a jak na to co nejlépe zareagovat.

1.1 Vymezení pojmu CI

V češtině nemá pojem CI zcela přesný ekvivalent. Nejbližší užívaný překlad je „konkurenční zpravodajství“, který vystihuje CI z hlediska procesu (Vejlupek, 2006):

- jako činnost založenou na organizovaném informování – zpravodajství, a toto informování je prováděno za účelem získání konkurenčních výhod.

Druhý možný, ale příliš nepoužívaný, překlad je „konkurenční inteligence“, který by zase CI vystihoval z hlediska cíle:

- výsledkem CI je schopnost organizace dosahovat svých cílů v měnících se podmínkách - přizpůsobovat se svému okolí - chovat se inteligentně, resp. jsou to informace zpracované do formy potřebné pro rozhodování manažerů organizace - zpravodajské produkty („intelligence“).

Různé definice pojmu CI:

- CI je etická podnikatelská (firemní) praktika nutná pro kvalifikované rozhodování v konkurenčním prostředí.
- CI je systematický a etický proces shromažďování, analýzy a využívání informací o konkurenčním prostředí organizace, které mohou ovlivnit její plány, rozhodnutí či aktivity.
- CI je multidisciplinární obor, vycházející ze specifického, ale výhradně legálního a etického způsobu shromažďování, analyzování a využívání informací pro zvyšování konkurenceschopnosti. Umožňuje správné a rychlé manažerské rozhodování v dynamicky se měnícím tržním prostředí (Vejlupek, 2006, s. 2).

Za jednu z nejvýznamnějších osobností CI lze považovat Leonarda M. Fulda, který se zabývá oblastí konzultací konkurenčního zpravodajství. Podle Fulda (c1996-2010) je možno definovat CI v těchto bodech:

- informace analyzované na takové úrovni, aby bylo možné udělat na jejich základě rozhodnutí,
- nástroj varování, který upozorní management na ohrožení i příležitosti,
- prostředek pro racionální odhady a hodnocení,
- různá podoba pro různé pracovníky v rámci organizace
- způsob života podniku jako neustálý proces,
- součást všech top společností,
- činnost, která je řízena shora (hierarchie organizace),
- způsob, jak vidět sám sebe (z pohledu organizace),
- krátkodobý i dlouhodobý proces

Fuld byl také jeden z prvních členů Society of Competitive Intelligence Professionals (SCIP). SCIP (2004) definuje CI jako *„systematický a etický proces shromažďování, analýzy a řízení externích informací, které mohou ovlivňovat řízení záměrů organizace, jejich rozhodnutí a fungování“*. Tato definice je všeobecně uznávaná. Lze tedy říci, že CI je tedy proces, při kterém dochází k zvyšování konkurenceschopnosti důkladným a etickým poznáváním konkurence a konkurenčního prostředí. V zásadě se jedná o legální shromažďování a analýzu informací, týkajících se strategie konkurence, schopností a zranitelnosti s využitím veřejně přístupných a dostupných zdrojů informací, kterými jsou například databáze.

Americké centrum kvality a produktivity definuje CI podobně jako:

„Systematický proces získávání a analyzování veřejně dostupných informací o konkurentech k zajištění firemního učení, zlepšení, odlišení a konkurenčního zaměření na podniky, trhy a zákazníky“.

Podle Hoffmana (1999) lze nahlížet na CI jako na proces a produkt zároveň. Procesem je metodické shromažďování, analýzou a zhodnocením informací o konkurenci a produktem je užitečná informace, která managementu umožňuje dělat informační rozhodnutí o marketingu, výzkumu a vývoji v dlouhodobých strategiích. Dobré konkurenční zpravodajství nejen poskytuje informace a data, ale také naznačuje směr akce nebo varuje před potenciálními problémy.

V anglicky mluvících zemích se o CI často hovoří jako o *„intelligence“* (Vejlupek, 2002) nebo se také často v americké odborné literatuře užívá pojem *„business intelligence“*. Bock (2000) ale považuje business intelligence (dále jen „BI“) za širší disciplínu, která také zahrnuje CI a považuje ho za jeden z aspektů BI. Podle něho je konkurenční zpravodajství zúžené na informace o konkurentech a na to, jak tyto informace ovlivňují strategii, taktiku a podnikové procesy. Business intelligence tak představuje nadřazenou sféru problematiky a lze ji chápat jako prostředek a nástroj pro podporu rozhodování managementu na všech stupních řízení s důrazem na zlepšení informovanosti manažerů.

Ve Francii se nejčastěji užívá pojem *intelligence economique* (Vejlupek, 2001). Také v České republice není definice konkurenčního zpravodajství jednoznačná a v různých zdrojích se může lišit. V současné době došlo sice k přijetí pojmu konkurenční zpravodajství, nicméně lze se také často setkat s termíny *„podnikatelské“* či *„komerční zpravodajství“* eventuelně také *„soutěživé zpravodajství“* (Brabec, 2000). Všechny tyto termíny však mají stejný význam.

Papík (2001) definuje konkurenční zpravodajství jako *„zjišťování, sledování a vyhodnocování konkurenčního prostředí (firmy, organizace) s cílem odhalit slabé a silné stránky konkurence, rozpoznat její strategické záměry. Zahrnuje analýzu a syntézu dat, resp. Informací, které se transformují do strategických znalostí, shromažďování informací o konkurenci a sledování subjektů firemního okolí (trh, stát, právo a legislativa, politické a demografické souvisloti)“*.

Dále upřesňuje (Papík, 2003) pojem s ohledem na shromažďování informace. Pokud se konkurenční zpravodajství primárně zabývá akvizicí informací o podnicích, pak ho nazýváme výrazem *„company intelligence“*. Pokud se blíže zaměříme na firmy jako na konkurenty, používáme potom termín *„competitive intelligence“*. V rámci

akvizice informací o určitých státech (konkurence z ostatních zemí) hovoříme o tzv. *„country intelligence“*. Obecně ale používáme termín competitive intelligence.

Na Slovensku se setkáváme s výrazem *„konkurenčné zpravodajstvo“* popřípadě i s výrazem *„komerčné zpravodajstvo“*. Některé slovenské zdroje uvádějí i překlad *„podnikatelská inteligencia“* (EURO-INFO, 2003).

Pro porozumění pojmu competitive intelligence je důležité pochopit rozdíl mezi informací a zpravodajstvím. Informace je konkrétní, věcná a založená na faktech. Mohou to být čísla, statistiky, data o firmách apod. Naproti tomu zpravodajství představuje určitý soubor informací, které byly vytříděny a podrobeny analýze. To co manažeři potřebují pro svá rozhodování je zpravodajství a nikoliv jen informace. V některých zdrojích se můžeme setkat s přirovnáním zpravodajství ke znalosti. (Kahaner, 1996).

Ani v dnešní době se firmy nevyhýbají praktikám, jako je průmyslová špionáž. Nemůžeme ani zabránit, aby se sama firma nestala obětí některé z nekalých praktik. Proto je důležité, aby firmy stále častěji využívaly nejen ofenzivní funkci konkurenčního zpravodajství, ale také defenzivní funkci konkurenčního zpravodajství a minimalizovaly možné ztráty. V této souvislosti potom hovoříme o tzv. *„obranném zpravodajství“* (competitive counter intelligence – CCI), v jiných zdrojích uváděno také jako *„defensive intelligence“* - DI (Helms, 2000). V našem prostředí o tomto termínu hovoříme jako o *„kontrašpionáži“*.

Brabec (2000) na tuto problematiku pohlíží z pozice znalce sektoru bezpečnostních služeb a definuje CI jako *„produkt, jehož cílem je zabránit konkurenci získat informace umožňující konkurenci získat kvalifikované rozhodnutí“* nebo *„dodat dezinformace, které neumožní konkurenci kvalifikované a správné rozhodnutí“*.

CI se podle Molnára (2009) dělí na čtyři oblasti, a to strategické zpravodajství, zpravodajství o konkurentech, tržní zpravodajství a nakonec technologické zpravodajství. *Strategické zpravodajství* se uplatňuje především při strategickém plánování, plánování rizikového kapitálu, hodnocení rizik, fúzích a akvizicích, dlouhodobého výzkumu a vývoje. *Zpravodajství o konkurentech* se zaměřuje na zodpovězení klíčových otázek:

- kdo jsou naši současní a potencionální konkurenti,
- jak vnímají konkurenti sebe a jak vnímají nás,
- jaké jsou krátkodobé a dlouhodobé trendy v oboru působnosti podniku,
- jak na tyto trendy reagovali naši konkurenti v minulosti,
- jak na ně pravděpodobně zareagují v budoucnu,

- jaké patenty nebo technologie získali nedávno naši současní/potencionální konkurenti,
- co pro nás tyto inovace znamenají,
- jak a kde naši konkurenti propagují své výrobky a služby,
- jaká je jejich hladina úspěšnosti,
- které trhy a geografické oblasti nebudou zabrány našimi konkurenty v budoucnu,
- jsou schopny naše tržní a geografické sektory zareagovat na změny v cenách, dodacích lhůtách a trvanlivosti,
- a budou toho schopny i do budoucna,
- jaké jsou plány našich konkurentů, se kterými v současnosti soupeříme, pro následujících 2 – 5 let.

Tržní zpravodajství je zaměřeno na informace o cenových hladinách výrobků, promočních akcích a jejich efektivnosti. Proto slouží pro podporu marketingového plánování, poskytuje retrospektivní data o úspěších a chybách při zavádění výrobků na trh. Technologické zpravodajství odpovídá na následující otázky:

- jaké nejnovější technologie v současnosti využívá konkurence,
- existuje ze strany konkurenta požadavek po nových technologiích, eventuelně zda konkurenti využívají outsourcing,
- jaký je počet a způsobilost výzkumných pracovníků konkurence,
- jaká je úroveň výzkumu a vývoje, stanovení cen budoucích výdajů pro výzkum.

Autor dále rozděluje CI na aktivní a pasivní. *Aktivní CI* je konvenční, obecně známé. Obsahuje zpravodajství ve všech podobách podnikání a konkurenčního prostředí. Pro účely zpravodajství se procesy aktivního CI zaměřují na sběr a analýzu dat. Toto zpravodajství je prováděno za účelem zlepšení rozhodování. V případě *pasivní CI* jde o proces obrany proti CI konkurence. Závisí na technikách, které konkurence využívá. Nejčastěji je vedeno v podobě poradenství a vzdělávání pracovníků za účelem monitorování citlivých dat a způsobu jejich ochrany.

1.2 Informační a znalostní izolace organizace

Jedním z problémů českého podnikatelského prostředí je přetrvávající informační izolace firem. Tento stav je přirozeným důsledkem toho, že firemní informační systémy jsou vytvářeny především pro podporu standardních procesů a není v nich příliš velký prostor pro individuální a kreativní formy zpracování informací, zejména informací z externích zdrojů, ani pro systematické vyváření přidané hodnoty v důsledku efektivní analýzy těchto informací.

Získat informace je pouze část cesty k tomu, abychom se dozvěděli to, co nám nakonec skutečně pomůže. Informace je nutné pochopit a především také využít. Jak je známo z literatury zvládnutí celého procesu není pro velké nadnárodní korporace takový problém, jako je mnohdy nepřekonatelnou překážkou pro malé a střední podniky. Nejde jen o finanční nebo personální možnosti, ale mnohdy malé a střední podniky nevědí, jaké jsou možnosti, co vlastně chtějí nalézt či jim zkrátka nezbývá dostatek času. Logicky v takovéto situaci napadá řešení sdružit se podobně, jako když podniky spolupracují při nákupu surovin a získávají tím mnohé výhody. Znamenalo by to spolupracovat na získávání a sdílení znalostí. Tuto problematiku by mohl zároveň podpořit systém, který by plně nebo alespoň částečně zautomatizoval vyhledávání, monitorování, třídění a analyzování informací pro určitou konkrétní oblast zájmu manažera.

Zavedení CI v organizacích zlepší především znalosti jejich manažerů předvídat změny na trhu, tahy konkurence a zmapování nových a potenciálních konkurentů. Využití veškerých metod Competitive Intelligence umožní učit se z chyb druhých a zvyšovat tak svou doménu a kvalitu u vyřčených cílů. Pomocí odnože Competitive inteligence *Technical Inteligence* je možno lépe poznat nové technologie, produkty, procesy, chystané politické a legislativní změny, které se týkají daného odvětví. Competitive Inteligence je vlastně uceleným systémem získávání informací a jejich zpracování. V současné době je nutné se na vlastní obchod dívat prakticky a s otevřenou myslí a současně implementovat poslední nástroje managementu (Has, Molnár, 2006, s 16-17).

1.2.1 Monitoring konkurence

CI je stručně řečeno řízené monitorování všech našich konkurentů a analýza zjištěných informací. Jedná se o systém jak se zajímat o své obchodní protivníky a jak nakládat s informacemi, které zjistíme, pro náš prospěch. *„CI může být srovnána s šachy: umožňuje myslet na mnoho tahů dopředu, které může udělat protivník. CI umožňuje identifikovat slabosti konkurence a vytvořit z ní budoucí příležitosti, které nám přinesou užitek“* (Molnár, 2009, s. 33). Konkurentem se zde rozumí libovolný subjekt, který považujeme za hrozbu pro naše podnikání a se kterým se dělíme o podíl na trhu. Úkolem CI je monitorovat co konkurence dělá a za pomoci takových informací sestavit předpověď co hodlá konkurence udělat, ještě před tím než to udělá. Řečeno ve strategických pojmech se jedná o předpovídání trendů a plánů konkurentů a o plánování naší vlastní strategie podnikání tak, abychom z budoucích událostí co nejvíce těžili ve

svůj prospěch. Aby bylo CI úspěšné, je nutná integrace do stávající struktury podniku, aby rozhodovací procesy využívaly ve správný čas ty správné informace.

Prosté sledování co dělá konkurenční firma nestačí. Pro efektivní fungování a rozvoj je třeba se zajímat i o obecné trendy na trhu, se kterým má naše podnikání spojení. Pokud např. naše společnost vyrábí určité díly a obecný trend ukazuje, že v příštích letech se uskuteční prudký nárůst určitého výrobku vhodného pro naše díly, mělo by nám toto napovědět, které díly vyrábět v hlavní produktové řadě, neboť ty budou s vysokou pravděpodobností v blízké době velmi žádaným obchodním artiklem – a my budeme připraveni uspokojit poptávku.

Jak je vidět CI nevyužívají pouze podniky produkující produkty nebo služby pro koncové zákazníky, ale všechny společnosti na trhu. Každé podnikání, které má konkurenty (dnes 99% všech oborů), chytrým využíváním CI získáváme konkurenční výhody.

Může se zdát, že velká společnost, která má dnes na trhu jméno a roční obrat se pohybuje v desítkách milionů dolarů, nemůže zkrachovat. Toto je však mylná představa. Na světě je nespočet takových společností, které před dvaceti lety byly považovány za leadery svého odvětví a dnes mají velké dluhy, případně již byly pohlceny konkurentem. Jaké mohly být příčiny tohoto stavu? Vedení ustrnulo a stylem řízení zaostalo. Doba pokročila a trh se změnil. Přišla řada nových firem, které jsou dravé a aktivně využívají prostředky moderní doby. Díky tomu měly ve správný čas ten správný nápad, co trh potřebuje a za co je ochoten zaplatit. Z hlediska konkurenční výhody byly napřed. Tato výhoda mohla pramenit z několika zdrojů (Slabý, 2006).

Vývojové oddělení mohlo mít dobrý nápad, který se ujal, nebo vedení na základě zjištěných informacích o trhu a o předpokládaných plánech konkurentů nařídilo vývoj něčeho, s čím hodlá přijít konkurence. Případně šikovný nápad komplementárního produktu k něčemu, co se na trh chystá vstoupit ve velkém. Aby toto mohlo vedení nařídit, muselo by mít dobré podklady a vědět co konkurence chystá, jak v nejbližších dnech tak i vzdálenější budoucnosti. Tyto informace jim poskytuje jistá forma CI.

1.3 Získávání informací pro podnikání

Získávání informací pro vlastní potřebu podnikání se vztahuje ke zdroji informace a místu sledované činnosti. Informace získáváme měřením, pozorováním, čtením, odposlechem, studiem apod. Ve vlastní podnikatelské činnosti je velmi mnoho různorodých zdrojů, v závislosti na konkrétním zaměření. Zaměříme se proto pouze na některé obecné, dle našeho názoru nejdůležitější.

Lze předpokládat, že podnikatel má potřebné vzdělání k provozování příslušné činnosti, ale to neznamená, že by tím měl skončit jeho zájem o odborné nové informace nebo všeobecné předpisy apod. Můžeme mít ovšem k dispozici odborníka-manažera, který podnik povede, ale to nesnižuje význam tvrzení, která dále předkládáme. Naopak spíše může dojít k problému v nutnosti vyznat se, zvláště v oblasti ekonomické či právní. I když máme možnost nechat si radit či dokonce zpracovávat různé úkony odborníky ze specializovaných firem, mnohé informace musíme ovládat sami. Vymětal (2005) uvádí přehled informací obvyklých v podnikání. Jedná se o informace:

a) z oboru podnikání, u kterých lze tvrdit, že je nejmenším problémem je získat. V této oblasti si je třeba nenechat si ujít žádnou příležitost k poučení, protože je důležité, aby bylo poznáváno vše nejnovější, co pomůže přispět k rozvoji výroby, služeb či jiné poskytované činnosti. Jedná se o informace výrobní a technologické, technické, politice podniku, o výrobních postupech, patentové informace, ovládnutí nové technologie atd.,
b) informace právní jsou pro podnikatele jistě nezbytné, z důvodu ovládání alespoň základních ustanovení z právních předpisů, týkajících se podnikání. K tomuto účelu je vydáváno mnoho různých příruček pro podnikatele, a je třeba vybrat si takové, které poučení skutečně přinášejí. Tedy jejichž obsahem nejsou jen ustanovení ze zákonů, vyhlášek či předpisů, ale i jejich výklad s doporučením přístupným právě mladým či začínajícím podnikatelům. Bývá též výhodné radit se s odborníky (poradenské firmy),
c) informace ekonomické a obdobně je tomu s problematikou ekonomiky, zejména účetnictví. Nejrozumnějším způsobem je nechat si tyto úkony zpracovat specializovanou firmou nebo profesionální účetní. V tomto případě bude alespoň větší záruka, že vlastní vztahy k finančním úřadům, jiným firmám či zákazníkům budou v pořádku,
d) informace o trhu jsou důležitými informacemi pro podnikání a jsou to ty, které se týkají trhu, samozřejmě oblasti, která bude sledována, informace

marketingové, marketingová politika, prodej, odbyt, marketingová a odbytová strategie, informace o partnerech, informace o konkurenci, hodnocení potenciálu apod. Vlastní rozbor informací z této oblasti je předpokladem úspěšnosti. Mohou být získávány různými způsoby – studiem odborných časopiseckých článků, účasti na odborných setkáních (výstavách, veletrzích, shromážděních podnikatelů), rozhovory se zákazníky, sledováním inzerce a reklam, osobním průzkumem co se prodává, jaké služby se nabízejí, včetně zhodnocení jejich kvality. Výborné výsledky také přináší sledování patentové literatury,

e) informace všeobecné jsou také důležité, aby podnikatelé měli rovněž vědomosti o všeobecném dění ve světě a samozřejmě v jejich vlastním podnikání. Toho všeho mohou dosáhnout vlastním úsilím, studiem, pozorováním, čtením, poslechem rozhlasu či televize. Nabízí se spousta příležitostí absolvovat krátkodobé kurzy nebo rekvalifikační studium. I z této oblasti je třeba získávat informace o všech různorodých nabídkách a podle konkrétní potřeby si vybrat. Je třeba mít na paměti, že svět nestojí na jednotlivci, i když i jednotlivec je jedním z maličkých prvků jeho pokroku, ale spíše je třeba se od světa hodně poučit,
f) informace obchodní jsou informace o obchodní politice, obchodních smlouvách, cenách nákupních, dodavatelských, maržích, cenové politice, obchodních záměrech a plánech, odběrových harmonogramech, obsah dokumentace obchodních předpisů a další,
g) informace organizační jsou interní informace o organizaci, týkající se záměrů a koncepcí organizačního rozvoje, vztahů mezi organizacemi, jednotkami, silných a slabých stránek organizace, koordinace mezi pracovišti apod.,
h) u informací personálních se jedná o informace z oblasti personální politiky, charakteristik a vlastností vedoucích pracovníků, klasifikace potenciálu lidských zdrojů aj.,
i) informace o informačním systému organizace jsou většinou informace dosti citlivé, např. o závislosti organizace na jejím informačním systému, jeho silných a slabých stránkách apod.

Dále sem patří také informace, které zdánlivě nezapadají do tohoto přehledu, ale mají svůj význam. Jsou to informace, které je nutno chránit podle zákona, tj. informace tvořící státní tajemství, osobní a zdravotní informace apod.

1.4 Zdroje informací při CI

Mohlo by se zdát, že pozorovatel zvenčí má malou možnost zjistit správné informace, ale opak je pravdou. Každá společnost o sobě do světa vysílá značné množství informací. Zcela jistě více, než by si přála. Slabý uvádí příkladů a ukázek, z čeho všeho se dají těžit užitečné informace (2006, s. 55-56).

- Diskusní skupiny jsou nástrojem na internetu dnes hojně používaným. Jak by nám mohl být nápomocen? Do fór, diskusních skupin a mailinglistů píší lidé své dotazy, na které hledají odpovědi. Naopak lidé věci znalí jim odpovídají. Pokud budeme pozorně sledovat jednotlivé diskuze, dříve nebo později zjistíme, kde dotyčné osoby pracují, s čím se zabývají, v čem jsou dobří a co naopak hledají. Pokud takto identifikujeme několik zaměstnanců jedné společnosti, je možné si udělat velmi dobrý obrázek o jejich odbornosti a o tom na čem zrovna pracují. To nám dává dobrý přehled, na čem daná společnost pracuje a s jakými cíly hodlá přijít.
- Nabídky zaměstnání, též *personální portály*, které nabízejí zaměstnání, se zdají být z pohledu strategie firem zcela „mimo obor“, ale není tomu tak. Je vhodné projít si nabídky zaměstnání, které daná společnost nabízí, a z nabízených pozic lze spatřit jaké odborníky společnost shání a z jejich specializace lze uhádnout jakým oborem a jakým odvětvím se hodlá ve startujících projektech zabývat.
- Profily a rozhovory s vysoce postavenými manažery, které v odborných časopisech čas od času vycházejí. Krom vlastních užitečných informací, které může manažer v odpovědích na redaktorovi otázky prozradit, se mezi řádky lze dozvědět o tom, jakou má povahu. To by nám mohlo napovědět, jestli se bude společnost snažit útočit na ceny agresivní cenovou válkou nebo naopak jestli se jedná o rozvážného vizionáře, což může napovědět to, že firma se bude snažit prosadit nové technologie, ale pravděpodobně nebude útočit na nejnižší ceny.
- Webové stránky společnosti jsou vždy dobrým zdrojem pro rešerše. Množství firem zde udává svou řídící strukturu, dělení na divize či závody, oficiální firemní kulturu, své sídlo, probíhající výzkum, vizi a misi společnosti, své produkty, ceníky a mimořádné nabídky, dodací podmínky a mnoho dalších informací, které nám mohou pomoci rychle si vytvořit o firmě obrázek.
- Dalším zdrojem je lokální tisk. Novináři jsou od toho, aby zveřejňovali informace. Je to jejich práce. Lokální tisk, vycházející v místě sídla zkoumané firmy, je jistě velmi dobrým zdrojem informací. To co může uniknout globálním

informačním zdrojům a agenturám jen stěží unikne menším novinám, působícím na konkrétním území. V dnešní době existují databáze a archivy starých článků všech významnějších deníků. Nabízí se zde možnost zapátrat po internetu a po knihovnách a nalézt zde řadu užitečných informací o subjektu naší pozornosti.

- Vertikální vyhledávače a portály. Internet, tak jako má svou obrovskou výhodu v množství informací, které lze na něm nalézt, má i stinnou stránku v tom samém. V takto obrovském a zvětšujícím se množství je velmi těžké nalézt relevantní informace, k určitému tématu. Dnes se proti tomuto lidé brání dvěma způsoby. Prvním je tvorba vertikálních vyhledavačů. To jsou odborně zaměřené portály a vyhledávače, které mají ve svých databázích tříděné informace jen na daná témata. Případně informace jim příbuzné. Tyto portály mají tu výhodu, že jsou ve většině případů pojaté jako komunitní a tedy zdarma. Navíc sdružují v sobě i diskusní skupiny a fóra o daných tématech, kde odpovídají odborníci na tato témata. Právě z odpovědí těchto lidí se dá ledacos odhadovat a předpovídat.
- Jako v předchozím případě vznikaly neplacené portály a vyhledávače, existují i jejich placené varianty. Prestižní databázová centra budují obrovské databáze z rejstříků knih, příspěvků z konferencí a článků z odborných časopisů. Jejich obrovskou výhodou je jejich relevance a aktuálnost. Databáze jsou udržované a tříděné. Obsahují skutečně kvalitní příspěvky o dané problematice, a proto jistě stojí za pozornost, pokud hledáme informace o nějakém trendu.
- Blogy jsou v poslední době velmi oblíbený a rozšířený způsob sebeprezentace na internetu. Některé společnosti dokonce nařizují části svých zaměstnanců, aby psali a udržovali pravidelně svůj internetový deníček. V takovém podnikově zaměřeném blogu zjistíme nejen značné množství informací o člověku samotném, ale i o projektech, na kterých pracuje, o potížích se kterými se setkal a o výhledech budoucích projektů. Jedná se o ideální zdroj vnitřních informací.

1.4.1 Zákon o svobodném přístupu k informacím

Možnost získávat důležité informace je zakotvena také v právních předpisech. Základním právním předpisem obsahujícím komplexní úpravu práva na informace je zákon číslo 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Jedná se o obecný právní předpis, který zajišťuje právo veřejnosti na informace, které mají k dispozici státní orgány, orgány územní samosprávy a další subjekty, jenž rozhodují na základě zákona o právech a povinnostech občanů a právnických osob. Mates (2002) ho charakterizuje tak, že na jeho základě může

kdokoliv získat od státních a jiných orgánů informace, týkající se jejich činnosti, rozhodování, struktur a jiných záležitostí. Je třeba uvést, že právo na informace jako právo politické je chápáno tak, že se jedná o informaci, kterou člověk žijící ve státě (nemusí být ovšem občanem státu) potřebuje k tomu, aby v prakticky dosažitelné míře znal, co se děje na veřejnosti v jeho blízkém okolí i dalekém okolí (Pavlíček, 1999).

Základní zásady, na nichž je zákon o svobodném přístupu k informacím postaven (Kolman, 2010):

- posílení zásady publicity veřejné správy, oslabení historicky překonaného principu diskrétnosti (důvěrnosti, uzavřenosti),
- na informace má právo každá osoba (fyzická, právnická či osoba bez státního občanství), mohou žádat také cizinci i cizozemské právnické osoby,
- není nutné uvádět důvod žádosti o informaci,
- zásada generální použitelnosti – týká se všech veřejnoprávních subjektů i subjektů soukromých, které plní funkci správního úřadu či pracují s veřejnými prostředky,
- zásada přiměřenosti – poplatek za poskytnutí informací nesmí být nepřiměřený práci a času, který povinný subjekt na získání informace vynaložil,
- zásada primární publicity (veřejnosti) informací a z toho vyplívající povinnost považovat prvotně informaci za poskytnutelnou,
- zásada konkrétního zákonného důvodu – odepírání přístupu pouze ex lege předvídatelného důvodu, což přirozeně posiluje právní jistotu žadatelů o informace,
- zásada řádného odůvodňování – konkrétní a jasné zdůvodnění odepření poskytnutí informace,
- parciální odepření – odepření části informace nesmí být důvodem pro odepření zůstatkové (nezávadné) části informace,
- přezkoumatelnost – po odepření přístupu k informaci je možné podat opravný prostředek, popřípadě následně je rozhodnutí povinného subjektu přezkoumatelné soudem.

1.4.2 Účel zákona

Stěžejním účelem zákona č. 106/1999 Sb. je zajištění ústavního práva na informace fyzických osob, a to práva na takové informace, které mají k dispozici státní orgány, orgány územní samosprávy, jakož i další veřejné instituce (dříve označované jako tzv. veřejné instituce hospodařící s veřejnými prostředky) a další subjekty, které rozhodují na základě zákona (tedy nikoliv podzákonného právního předpisu) o právech

a povinnostech fyzických a právnických osob v oblasti veřejné správy. Připomeňme si, že zákon č. 106/1999 Sb. je obecným a komplexním předpisem, tedy že reglementuje (upravuje zvláštním předpisem) každou hlavní právní stránku dotýkající se svobodného přístupu k veřejnoprávním informacím. Nedopadá jen na tu skupinu informací, která je komplexně upravena jiným předpisem, stanovuje obecný rámec přístupu k informacím veřejného sektoru s možností jejich dalšího využití. Vládní novela klade důraz na rychlé a pro povinné subjekty méně zatěžující poskytování informací díky upřednostnění elektronické komunikace. Obecnou zásadou k uskutečnění účelu zákona č. 106/1999 Sb. je dle hlavní předkladatelky novely tehdejší ministryně informatiky Dany Bérové zejména důraz na použití elektronických prostředků pro získávání informací a poskytování informací v jazycích a formách, ve kterých byly vytvořeny, nebo do kterých mohou být snadno konvertovány, pokud je to možné a vhodné (Kolman, 2010).

1.4.3 Povinné subjekty

Jedním ze zásadních prvků zákona č. 106/1999 Sb. je otázka, na koho se vztahuje informační povinnost. Tedy jaké subjekty mají ze zákona povinnost poskytovat informace vztahující se k jejich působnosti. Zákon je vymezuje v ustanovení § 2 a jsou jimi jednak státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce.

Tyto povinné subjekty mají povinnosti poskytovat všechny údaje, kterými disponují anebo se kterými by disponovat měly, mají tedy tzv. úplnou informační povinnost. Dále pak ty subjekty, kterým zákon svěřil rozhodování o právech, právem chráněných zájmech nebo povinnostech fyzických nebo právnických osob v oblasti veřejné správy, a to pouze v rozsahu této jejich rozhodovací činnosti – tzv. částečná (parciální) informační povinnost (Kolman, 2010).

1.4.4 Veřejné instituce

Za veřejnou instituci se pokládá takový subjekt, jehož založení a režim řízení se odvodí z veřejného práva, zvláště z norem práva správního a finančního. Tedy právních pravidel, jimiž je popsán výkon veřejné správy. Veřejná správa přitom neznamená jenom autoritativní rozhodování o právech či povinnostech, ale zahrnuje i obhospodařování (správu) veřejných statků. Jestliže instituce hospodaří s veřejnými prostředky, potom to znamená její napojení na veřejné rozpočty nebo na rozpočty jinak na veřejné prostředky navázané. Pojem veřejné prostředky nelze vykládat pouze ve smyslu peněžních prostředků, ale patří sem i věci movité, nemovité, práva a jiné majetkové hodnoty, které mají veřejný charakter (tzn., buď jsou ve vlastnictví státu,

obcí či krajů, anebo stát převedl vlastnické či jiné majetkové právo, aby účelněji dosáhl veřejného zájmu).

Povinnými subjekty podle zákona č. 106/1999 Sb. se tak staly např. Česká televize a Český rozhlas, Česká tisková kancelář, Pozemkový fond ČR a veřejné nemocnice. Všechny veřejné školy (tedy i vysoké školy – kromě soukromých) se přesunuly z kategorie povinných subjektů, které mají částečnou informační povinnost (ustanovení § 2 odst. 2 zákona č. 106/1999 Sb.) do kategorie úplné informační povinnosti. Stejně tak Všeobecná zdravotní pojišťovna, která má po novele z roku 2006 rovněž informační povinnost úplnou. Jak v této souvislosti judikoval NSS (Nejvyšší správní soud): Všeobecná zdravotní pojišťovna je podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, subjektem s informační povinností, neboť prostředky, které jsou získávány v systému zdravotního pojištění, mají charakter veřejných prostředků a slouží k úhradě zdravotní péče, která má charakter veřejné služby.

Zajímavá je otázka státních podniků, zda jsou či nejsou povinnými subjekty. Např. polostátní ČEZ a.s. (stát vlastní v této společnosti většinový podíl) se dlouho tomuto zařazení bránil, světlo do celé věci vnesl až rozsudek NSS ze dne 06. 10. 2009, čj. 2 Ans 4/2009-93, v němž elektrárenskou společnost označil za „veřejnou instituci“, jenž musí poskytovat informace dle zákona č. 106/1999 Sb.

Dalším zajímavý příklad rozsudku NSS v oblasti vymezení povinných subjektů – Fotbalový klub Hradec Králové, který jako akciovou společnost ovládá město, musí na základě zákona o svobodném přístupu k informacím poskytovat informace žadatelům. Obecně lze říci, že akciová společnost ovládaná městem (nebo krajem) je povinným subjektem. Obec (kraj) nemůže vlastnit (ovládat) právnickou osobu k soukromému účelu.

Aplikační praxe se zatím staví dosti zdrženlivě k faktu, že by do této skupiny povinných subjektů byly zařazeny i politické strany. Fyzické ani právnické osoby prozatím příliš nevyužívají svého práva žádat je o informace. Z právního hlediska musíme zmíněné strany vnímat jako veřejnoprávní korporace, byť do značné míry jako korporace svého druhu, nicméně hospodaří rovněž s veřejnými prostředky, jelikož majoritní část jejich příjmu tvoří na základě zákona č. 424/1991 Sb., o sdružování v politických stranách tzv. příspěvek ze státního rozpočtu ČR na úhradu volebních nákladů a na činnost těchto stran. Informační povinnost ovšem nedopadne na politické strany, které tento státní příspěvek nedostávají – zpravidla tedy menší politické, možno říci méně společensky významné subjekty, které v rámci volebních „soubojů“ nedosáhly

relevantní hranice zisku hlasů, od které se vyplácí příslušný volební příspěvek, a rovněž nejsou držiteli zastupitelských mandátů, za něž je taktéž politickým stranám vyplácen státní příspěvek.

Skutečnost, že státní příspěvek není jediným příjmem politických stran – dále jsou financovány např. z členských příspěvků a ze sponzorských darů soukromých fyzických a právnických osob – neznamená, že by se na ně nevztahovalo ustanovení § 2 odst. 2, kde se hovoří o hospodaření s veřejnými prostředky. Jazykovou interpretací tohoto ustanovení dojdeme k tomu, že se nemusí jednat o absolutní hospodaření s veřejnými prostředky, takže skutečnost, že politický subjekt je zčásti financován ze soukromých zdrojů, jej nemusí vylučovat ze skupiny povinných subjektů dle zákona č. 106/1999 Sb. Pokud bychom došli k opačnému závěru, tedy, že bychom politické strany nechápali jako výše zmíněné povinné informační subjekty, tak by mohlo dojít k paradoxní situaci odporující principu transparentnosti veřejného demokratického politického života a taktéž vyjmutí politických stran by bylo nutno pokládat za protiústavní – omezení ústavního práva na informace.

Taktéž judikatura Ústavního soudu ČR v posledních letech chápe pojem veřejná instituce (dříve označovaná jako hospodařící s veřejnými prostředky) demokraticky extenzivně, s čímž lze souhlasit, tudíž v potenciálním případě ústavní stížnosti určité politické strany proti tomu, že byla zařazena pod § 2 odst. 1, lze předpovídat její neúspěch ve věci. Taktéž i z pohledu občana – voliče by se jevil problematický fakt, že strana, která tají relevantní informace o sobě samé, by následně realizovala transparentní činnost při správě věcí veřejných.

Další spornou skupinou, jsou tzv. neziskové organizace (obecně prospěšné společnosti, občanská sdružení, nadace). Kužílek (2002) v této otázce zastává názor, že tyto nejsou povinnými subjekty. Podle platného zákona o povinný subjekt opravdu nejde. Například Kolman (2010) se přiklání k tomu, že pokud by rozpočet takového neziskového subjektu byl tvořen z více než padesáti procent z příjmů z veřejných prostředků, tak by i příjemci různých veřejných dotací spadali do této skupiny „povinně informujících subjektů“.

Do čtvrté skupiny povinných subjektů, kterým zákon svěřil rozhodování o právech, právem chráněných zájmech nebo povinnostech fyzických nebo právnických osob v oblasti veřejné správy řadíme například orgány profesní samosprávy (např. Česká advokátní komora, Komora auditorů České republiky). Dále jsou to některé fyzické osoby nadané výkonem veřejné moci např. soudní exekutor, notář, ředitel školy, rektor univerzity, soudní lékař.

Zásadním rozdílem mezi subjekty spadající do této množiny a subjekty zmíněnými výše je rozsah povinnosti poskytovat informace žadatelům. Zatímco povinné subjekty zmíněné v první až třetí skupině, mají úplnou informační povinnost, tedy musí poskytnout všechny údaje, se kterými disponují nebo se kterými by disponovat měly, pro subjekty spadající pod tento bod je povinnost informace poskytnout dána pouze v rozsahu jejich rozhodovací činnosti. Jinak napsáno mají jen částečnou (parciální) informační povinnost. Základním rozdílem je, že tyto orgány podléhají kontrole pouze ve své rozhodovací činnosti, tedy pouze a jen v tom sektoru jejich působnosti, který jim byl propůjčen k realizaci ze strany veřejné moci (Kolman, 2010).

Následující informace povinný subjekt ex lege neposkytuje:

- utajované informace (dříve označované jako utajované skutečnosti)
- informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje
- příjemci veřejných prostředků
- ochrana obchodního tajemství
- informace narušující ochranu důvěrnosti majetkových poměrů
- vnitřní pokyny a personální předpisy
- nehotové (připravované) informace
- informace poskytované NATO a EU
- „podmíněné“ informace
- pravidelně publikované informace
- ochrana duševního vlastnictví
- parciální omezení dle § 11 odst. 3 InfZ – informace, které získal povinný subjekt od třetí osoby při plnění úkolů v rámci kontrolní, dozorové, dohledové nebo obdobné činnosti
- informace spadající pod jiná omezení – např. o probíhajícím trestním řízení

1.4.5 Právo na informace, ochrana obchodního tajemství a veřejné rozpočty

Obce jsou podle zákona č.106/1999 Sb., o svobodném přístupu k informacím nejpočetnějšími povinnými subjekty. Z toho vyplývá, že aplikace tohoto zákona se v praktickém každodenním životě setkává s řadou úskalí, o čemž svědčí i problematika práva na informace a ochrany obchodního tajemství. Z důvodu, že se jedná o praktický problém, si lze problematiku názorně ukázat na jednom z judikátů. Konkrétně se jedná o

rozsudek Krajského soudu v Hradci Králové ze dne 25. 5. 2001, č. j. Ca 189/2000-27. Ve stručnosti si řekněme, o co se v celé právní věci jednalo. Žalobce žádal Městský úřad o poskytnutí informace o financování výstavby základní školy. Předmětný Městský úřad žádosti nevyhověl, proti čemuž se žalobce v souladu s platným právním řádem odvolal k Městské radě. Zmíněná rada odvolání zamítla s odůvodněním, že se jedná o obchodní tajemství a tudíž daná informace nemůže být poskytnuta.

Poté se žalobce obrátil na příslušný soud s žalobou na přezkoumání zákonnosti rozhodnutí orgánů veřejné správy, jimiž nebylo vyhověno žalobcově žádosti o poskytnutí informací týkající se financování výstavby základní školy. Předmětná žaloba byla odůvodněna následujícím způsobem: žalobce požádal žalovaného o poskytnutí informace, týkající se financování výstavby základní školy, a to v rozsahu předložení smlouvy o dílo, včetně jejich dodatků, položkového rozpočtu jako součásti smlouvy, položkového rozpočtu změn ve smyslu odpočtů a připočtu k původnímu dohodnutému rozpočtu. Své právo na informace přitom zdůvodnil výkonem funkce člena městské rady a jako nárok podle zákona č.106/ 1999 Sb., o svobodném přístupu k informacím.

Městský úřad uvedené žádosti nevyhověl s tím, že jí nelze poskytnout pro rozpor s ustanovením § 9 odst. 1 zákona č. 106/1999 o svobodném přístupu k informacím, neboť tomu brání ujednání mezi dodavatelem a zhotovitelem předmětné stavby ve smlouvě o dílo, že veškeré obchodní a technické informace, týkající se tohoto smluvního vztahu, jsou označeny za důvěrné a žádná ze smluvních stran je nezpřístupní třetím subjektům pro další účely, než pro plnění dané smlouvy. Z tohoto ujednání městský úřad dovodil, že se jedná o obchodní tajemství dle ustanovení § 17 zákona č. 513/1991, ve znění pozdějších předpisů (obchodní zákoník). Tuto skutečnost v odvolacím řízení potvrdila i Rada města. Žalobce se ve své soudní žalobě domáhal toho, že se o žádné obchodní tajemství nejedná, jelikož nebyly naplněny všechny znaky obchodního tajemství - dle ustanovení § 17 zákona č. 513/1991 ve znění pozdějších předpisů (obchodní zákoník) - tj., že se musí jednat o skutečnosti obchodní, výrobní nebo technické povahy související s podnikem, které mají alespoň potenciální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle podnikatele utajeny a podnikatel musí utajení odpovídajícím způsobem zajišťovat. A má-li se jednat o obchodní tajemství ve smyslu obchodního zákoníku, musí obligatorně nést všechny tyto pojmové znaky. Žalovaná strana se bránila následujícím způsobem: žalobní námitky neshledala důvodnými (tj. Městská rada nadále trvala na skutečnosti, že se o obchodní tajemství jedná) a navrhovala zamítnutí žaloby.

Předmětný krajský soud poté rozhodl následovně. Aby se jednalo o obchodní tajemství, je nutné, aby byly naplněny všechny pojmové znaky obchodním zákoníkem stanovené, tzn., že se musí jednat o skutečnosti obchodní, výrobní nebo technické povahy související s podnikem, které mají alespoň potenciální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle podnikatele utajeny a podnikatel musí utajení odpovídajícím způsobem zajišťovat. Ochrana obchodního tajemství přitom nevzniká evidencí nebo zápisem, ani uvedením této skutečnosti do smlouvy o dílo, ale vzniká okamžikem naplnění všech pojmových znaků obchodního tajemství. Navíc je potřeba připomenout, že pokud již jsou naplněny všechny zákonem stanovené znaky obchodního tajemství, přísluší právo k tomuto tajemství pouze tomu kterému určitému podnikateli a také pouze jemu přísluší ochrana obchodního tajemství proti jeho porušení nebo ohrožení. Obchodním tajemstvím ovšem nemůže být informace o rozsahu finančních prostředků poskytnutých podnikateli z rozpočtu obce, tedy ani údaj o ceně za provedené dílo, jež je hrazena z příjmů od daňových poplatníků.

Výdaje obcí jsou věcí navýsost veřejnou, že s jejich zdroji nespojuje toho kterého podnikatele žádná tvůrčí souvislost, jež by jen v náznaku mohla vést k domnění, že by se mohlo jednat o obchodní tajemství. Pod toto spadá samozřejmě i konkrétní užití rozpočtových prostředků obce. Předmětný soud rozhodl tím, že žalovaná strana neposkytla požadovanou informaci žalobci, nejednala v souladu se zákonem. Závěrem lze říci, že obchodní tajemství není (a nikdy nebylo) jen subjektivní kategorií, nýbrž musí zcela splňovat objektivně dané znaky vymezené v ustanovení § 17 obchodního zákoníku. Tudíž nestačí se na něm pouze dohodnout ve smlouvě o dílo (či v jiné obdobné smlouvě). Tento rozsudek je dalším výrazným varovným signálem pro všechny starosty a radní, kteří za pomoci právní kličky zneužívající institutu ochrany obchodního tajemství a brání občanům v přístupu k informacím. A to k údajům, jak se vynakládají prostředky pocházející z jejich daní, tedy informacím důležitých pro správu veřejných věcí (Kolman, 2003).

1.4.6 Svobodný přístup k informacím

Článek 17 Listiny základních práv a svobod (dále jen „LZPS“) mimo jiné říká, že právo na informace je zaručeno (odst. 1). A dále: státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti (odst. 5). Podmínky a provedení měl stanovit zákon, na který si občané České republiky museli počkat. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, byl přijat v roce 1999 a většina jeho ustanovení vstoupila v účinnost 1. 1. 2000 (u některých ustanovení, respektive u několika povinností zakotvených v § 5 a § 14 byla jejich

účinnost odložena, a to od 1. 1. 2001 či 1. 1. 2002). Přestože zmíněný zákon působí již déle než jedenáct let, lze se oprávněně domnívat, že jedno z politických práv člověka, právo na informace (viz uvedený článek 17 LZPS), touto zákonnou úpravou bezproblémově, ústavně konformním způsobem zaručeno není (Červenka, 2001).

Zmíněný zákon upravuje podmínky práva svobodného přístupu k informacím a stanoví základní podmínky, za nichž jsou informace poskytovány (§ 1). Avšak text zákona obsahuje dle Červenky jeden závažný, byť na první pohled nenápadný nedostatek, který realizaci ústavně zaručeného práva velmi ztěžuje, ba dokonce i ohrožuje. Většina práv a povinností žadatele i povinného subjektu je zde sice upravena poměrně podrobně (podáním žádosti počínaje, jejím kladným či záporným vyřízením konče), avšak otázka hrazení nákladů je vměstnána do jediného paragrafu (§ 17). Uvedený fakt by sám o sobě nebyl tak zajímavý, kdyby se nejednalo o zásadní problém, jehož vyřešení může mít v konkrétním případě za následek to, že informace nemusí být poskytnuta.

Povinné subjekty (státní orgány a orgány územní samosprávy, které mají povinnost poskytovat informace vztahující se k jejich působnosti) jsou v souvislosti s poskytováním informací oprávněny žádat úhradu ve výši, která nesmí přesáhnout náklady spojené s vyhledáváním informací, pořízením kopií, opatřením technických nosičů dat a s odesláním informací žadateli. Vzhledem k tomu, že celá oblast veřejné správy je ovládána zásadou hospodárnosti a peněžní prostředky určené pro činnost správních úřadů se pohybují v přísných limitech, nelze spravedlivě a rozumně požadovat, aby informace byly poskytovány bezplatně. Kromě ekonomického zhroucení celé soustavy správních úřadů by navíc hrozilo nebezpečí, že např. orgány obcí (obecní úřady) s minimálním počtem pracovníků by bezplatným vyřizováním velkého počtu žádostí mohly být v ostatní činnosti zcela ochromeny, respektive by kromě vyhledávání informací nedělaly nic jiného. I vzhledem k tomu, že poskytnuté informace mohou mít nemalou majetkovou hodnotu, bylo nutné stanovit, že žadatel musí nést náklady jejich vyhledání. Zejména pokud povinnému subjektu vzniknou zvýšené náklady dané tím, že úřad informace složitě získává od dalších orgánů, právních poradců, atd.

Sporné je však ustanovení § 17 odst. 3, podle kterého *„povinný subjekt může podmínit vydání informací zaplacením úhrady nebo zálohy.“* Pokud správní úřad podle svého uvážení určí jako předpokládanou výši úhrady nebo zálohy jakoukoli částku (na základě nejednotných, úřad od úřadu se lišících sazebníků úhrad za provedené úkony) a jejím zaplacením podmíní vydání informace, musí žadatel tuto částku uhradit na každý pád. Nezaplatí-li, povinný subjekt se žádostí zabývat vůbec nebude a informace

jednoduše neposkytne. K postupu předpokládanému v ust. § 13 až § 16 (žádost, postup úřadu při vyřizování žádosti, rozhodnutí, odvolání) tak vůbec nedojde.

Lze namítnout, že zaplacení úhrady nebo zálohy může být v konkrétním případě nezbytné jako „zajišťovací prostředek“ před neseriózními žadateli, kteří by nákladně zjištěnou informaci odmítli převzít a zaplatit, či jako nutnost posílit zainteresovanost žadatele na celém, mnohdy složitém a finančně náročném procesu vyhledávání informací. Požadavek do jisté míry oprávněný, ale z hlediska ústavnosti silně nedokonalý a podezřelý. Zájem správního úřadu (ochrana před nezaplacením, snaha vyhnout se následnému vymáhání plateb) je zde stavěn nad ústavně zaručené právo jednotlivce. Ustanovení § 17 odst. 3 ještě zvyšuje „sílu úřadu“, jako by nestačilo, že ve státní správě je správní úřad v nadřízeném, jednotlivec v podřízeném postavení, a úřad má na každý pád k dispozici dostatek mocenských prostředků, jak občana donutit k poslušnosti, k zaplacení. Ustanovení § 17 odst. 3 může být úřadem zneužito (a v praxi se tak skutečně děje) k tomu, aby účinky zákona o svobodném přístupu k informacím vůbec nenastaly.

Zákon č. 106/1999 Sb., ve znění pozdějších předpisů, neumožňuje proti rozhodnutí o stanovení výše úhrady nákladů (a o podmínění vydání informací jejím zaplacením) podat opravný prostředek. Pokud tedy povinný subjekt sám, bez jakékoliv zákonem předpokládané kontroly záměrně částku nadsadí, může tím omezit právo na informace „cestou faktickou“, pod jakousi pseudoekonomickou záminkou. Pro rozhodnutí o výši náhrady nepředepisuje zákon žádnou formu, a protože se na ustanovení § 17 nevztahuje správní řád, nelze uvažovat o řádných, ani o mimořádných opravných prostředcích, které správní řád obecně upravuje. Nepoužijí se ani příslušná ustanovení občanského soudního řádu o soudním přezkumu rozhodnutí orgánů veřejné správy, neboť z hlediska práva zde vlastně o žádné rozhodnutí nejde (byť má určení výše úhrady v praxi zásadní vliv), a proto by byla žaloba bezpředmětná.

Nezbývá než konstatovat, že naznačený stav odporuje zásadám právního státu zejména tím, že na neformálním rozhodnutí orgánu veřejné správy fakticky závisí, zda jednotlivec se svého ústavně zaručeného práva domůže či nikoliv. Zdá se, že je tím porušena zásada přezkoumatelnosti rozhodnutí ve veřejné správě, avšak vzhledem k výše uvedenému (přezkoumat lze pouze takové rozhodnutí, které má určitou právem předpokládanou formu) máme před očima učebnicový příklad zastřeného a pro demokratický právní stát, založený na úctě k právům a svobodám člověka a občana, nebezpečného útoku „obyčejného“ zákonodárce na ústavní pořádek České republiky.

Do budoucna je tedy naprosto nezbytné, aby se ustanovení § 17 zák. č. 106/1999 Sb., ve znění pozdějších předpisů, zásadním způsobem změnilo, zejména aby byl vypuštěn odst. 2 tohoto paragrafu. Zákon by měl též stanovit formu, ve které bude napříště vydáváno rozhodnutí o výši úhrady nákladů, a umožnit žadateli podat proti rozhodnutí opravný prostředek. O podmíněnosti vydání informací zaplacením úhrady nebo zálohy nemůže být řeč – v opačném případě by musel jako negativní zákonodárce zasáhnout Ústavní soud (Červenka, 2001).

1.4.7 Opakovaná žádost o informaci

V praxi se někdy stává, že žadatel žádá opakovaně (tedy stále dokola) o tu samou informaci (popř. změní slovosled), čímž de facto šikanuje správní úřady. Této otázce se věnoval i NSS, který k takovému postupu mj. judikoval: Pokud má povinný subjekt za to, že požadovaná informace již byla poskytnuta, má novu žádost z tohoto důvodu zamítnout. Je pravdou, že takový důvod odepření poskytnutí informace zákon o svobodném přístupu k informacím výsledně nezmiňuje, vyplývá však z jeho smyslu a účelu, neboť účelem zákona skutečně není opakované poskytování informací, které má žadatel již k dispozici. To platí samozřejmě za předpokladu, že žadateli již byly požadované informace poskytnuty v písemné formě, nebo v jiné formě, která umožňuje jejich trvalé zaznamenání, takovým případem tedy není ústní sdělení těchto informací. Samozřejmě nový problém nastává, pokud žadatel ve své „nové – opakované“ žádosti smísí požadavek na informace, které již má e svém držení s požadavky na informace nové. Zde by bylo nesprávné zamítnutí celé žádosti a informaci. Dle Kolmana (2003) by bylo právně korektní zamítnout jen tu část žádosti, ve které žadatel chce ty informace, které již má k dispozici.

1.4.8 Poskytování informací a ochrana osobních údajů

K poskytování informací v souvislosti s ochranou osobních údajů se vztahuje rozsudek Nejvyššího správního soudu v Brně zn. 7 As 47/2010 ze dne 6. 8. 2010 ke sdělování výsledku ověřování osobnostní způsobilosti příslušníků bezpečnostních sborů. Pokud žadatel obdrží informaci o tom, zda u příslušníka bezpečnostního sboru byla za doby trvání jeho pracovního, resp. služebního poměru ověřována jeho osobnostní způsobilost pro výkon služby v bezpečnostním sboru, nemá taková informace žádnou vypovídací hodnotu o zdravotním stavu dotčeného příslušníka. Pokud bude znít odpověď na tuto otázku „Ano“, bude to svědčit pouze o tom, že u konkrétního příslušníka bezpečnostního sboru nastal některý z důvodů zjišťování jeho osobnostní způsobilosti vymezených v § 2 vyhlášky č. 487/2004 Sb. Pokud bude znít odpověď na

tuto otázku „Ne“, pak to bude svědčit pouze o tom, že žádný z těchto důvodů za dobu trvání jeho pracovního, resp. služebního poměru nenastal. Nic víc. Z této informace nelze zjistit ani to, z jakého konkrétního důvodu se případně příslušník zjišťování osobnostní způsobilosti podrobil a s jakým výsledkem.

Příjemce požadované informace tak nebude moci usuzovat, zda dotčený příslušník splnil předpoklady osobnostní charakteristiky vymezené v § 1 této vyhlášky či nikoliv. Zjistí pouze to, zda se dotčený příslušník bezpečnostního sboru podrobil zjišťování své osobnostní způsobilosti jako jednoho z předpokladů pro výkon služby v bezpečnostním sboru, anebo že k takovému postupu nebyl důvod. Zdravotní stav dotčené osoby však tato informace nikterak neodhaluje.

Požadovaná informace tedy nepředstavuje ani osobní údaj dle § 4 písm. a) zákona o ochraně osobních údajů, ani citlivý údaj o zdravotním stavu subjektu údajů ve smyslu § 4 písm. b) téhož zákona, a žalovanému tak nevzniká povinnost zacházet s touto informací dle § 13 zákona o ochraně osobních údajů.

Pokud povinný subjekt a žalovaný na podporu svých tvrzení odkazovali také na ustanovení § 202 zákona o služebním poměru příslušníků bezpečnostních sborů, nejde o přiléhavou argumentaci. Není sporu o tom, že doklady o způsobilosti příslušníka vykonávat službu představují nedílnou součást dokumentace o průběhu služebního poměru příslušníka bezpečnostního sboru, která je vedena v jeho osobním spise (§ 202 odst. 2). Žadatel také nepochybně není osobou, která by do osobního spisu jiného příslušníka bezpečnostního sboru mohla nahlížet. V osobním spise jsou totiž uloženy kompletní doklady o způsobilosti příslušníka vykonávat službu včetně dokladů o případném zjišťování jeho osobnostní způsobilosti, tedy včetně výsledků případného psychologického vyšetření. Takový údaj by již kritéria citlivého údaje splňoval a na poskytnutí takové informace by žadatel s ohledem na znění § 8a informačního zákona nárok neměl. O poskytnutí takové informace však stěžovatel nežádal.

Jistě se najde ještě mnoho dalších možností, které slouží jako zdroje pro CI proces zjišťování informací. Výše jsme uvedli pouze některé významné zdroje informací, abychom ukázali na první pohled neviděné souvislosti. Dobrý CI analytik je považován právě díky tomu, že umí získat a spojovat zdánlivě nesouvisející informace v jeden přehledný a ucelený obraz.

Zdánlivě bychom mohli nabýt dojmu, že CI je pouze synonymum pro vojenskou špionáž v komerčním světě. Avšak není tomu tak. Podkladem jsou pouze běžně dostupné informace, jako bylo představeno v předchozích kapitolách. Dříve by byl problém tyto informace v rozumném čase vyhledat a setřídit dohromady a poté udržovat

aktuální. V dnešní době globálního internetu je toto velmi zjednodušeno. Nicméně se zde ukazuje nový problém, a tím je jak z obrovského množství informací na internetu prezentovaných, získat v akceptovatelném čase pouze ty relevantní. Vyhledávacími technikami se zabývá na světě mnoho výzkumných týmů, jak univerzitních, tak komerčních. Výzkum není pouze o vlastních metodách a vyhledávání, ale už o způsobu vytváření a značkování dokumentů a tvorbě metadat. Vznikají koncepty v čele se Sémantickým webem a Topic Maps, které se snaží značně ulehčit relevantní vyhledávání (Garshol, 2004). Pokrok je každý rok obrovský a nezbývá než doufat, že již brzy výzkum dospěje do takového stádia, kdy bude možné ony koncepty začít používat v praxi.

Pokud se vůbec někdy v minulosti dalo říci, že nebylo třeba sledovat konkurenci a firma měla zajištěn odbyt svých výrobků nebo služeb, pak toto již dnes zcela jistě neplatí. Informační a telekomunikační technologie svět velmi zmenšili a informační doba nutí společnosti, aby využívali moderních technologií a postupů napříč celou firmou. Jen tak mohou obstát v sílícím tlaku konkurentů celého světa (Vejlupek, 2002 s. 47-62).

2 Současné podnikatelské prostředí a informační strategie

Podnikání v současné době vyžaduje neustále nové tvořivé přístupy, které by naplnily stále rostoucí očekávání potenciálních zákazníků. Tyto moderní metody a trendy se nemohou vyhnout žádnému odvětví nebo segmentu trhu. Současná dynamizace těchto trendů je produktem vytváření kvalitativně nové propojené světové ekonomiky – procesu nazývaného jako globalizace. Proces globalizace nemá vliv pouze na samotné podnikání. Ovlivňuje naše životy a jejich kvalitu po všech jejich stránkách. Dotýká se celkových společenských poměrů, ekonomiky, politiky apod. Orientace v tomto prostředí, se všemi jeho problémy, není jednoduchá. Ještě náročnější je najít si v tomto složitém prostředí vlastní cestu, tedy strategii.

Strategie stojí na počátku procesu, kterým se lidské myšlenky mění ve skutečnost a kterým člověk tuto skutečnost aktivně ovlivňuje a přetváří. Moderní společnost stojí právě na základě takovéhoto vědomého přetváření skutečnosti. Panuje obecná shoda o tom, že další vývoj je v globálním měřítku závislý právě na rozvoji vzdělanosti a s ní spojené tvořivosti, která je zřejmě jediným nevyčerpatelným zdrojem, kterým lidstvo vládne (Preuss, 2008).

Neexistuje jednotná, všeobecně přijímaná definice strategie. Různí autoři se rozcházejí v názorech, pokoušejí se strategii vymezit jak z obsahového hlediska, tak z hlediska užití v praxi. Johnson a Scholes (1998, s. 7) definují strategii následujícím způsobem: *„Strategie dlouhodobě určuje směr a rozsah aktivit organizace. V ideálním případě přizpůsobuje zdroje organizace měnícímu se prostředí, v němž organizace působí, trhům, zákazníkům a očekáváním zainteresovaných stran (stakeholders)“.* Jiný přístup chápe strategii jako „herní plán“, který si management vytvořil proto, aby dokázal firmu dobře umístit v tržním prostředí, aby posílil její konkurenceschopnost, její schopnost uspokojovat zákazníky a dosahovat dobrých podnikatelských výsledků. Mintzberg (2002, s. 16) považuje strategii za *„model či plán, který integruje hlavní organizační cíle, politiky a posloupnost činností do soudržného celku“.* Z našeho pohledu je základním charakteristickým rysem strategie specifická nosná myšlenka, která jí dává jedinečnost a určuje charakter činnosti pro určité období. Strategie není detailní plán nebo program konkrétních instrukcí. Nemůže nahradit konkrétní plány. Je to spíše jednotící téma, které dává aktivitám a rozhodnutím manažerů a dalších pracovníků, a tím i celé organizaci, soudržnost a směr.

Podle Preusse (1998) úspěšná strategie vyžaduje:

- jednoduché, konzistentní, dlouhodobé cíle jednoznačně formulované,
- porozumění konkurenčnímu prostředí, znalost charakteru odvětví,
- schopnost zhodnocení zdrojů, jejich potřeby a charakteru.

Strategie představuje určení dlouhodobých základních cílů podnikatelského subjektu a určení nezbytných činností a zdrojů potřebných pro jejich dosahování. Účelem strategie je formulovat a prostřednictvím strategických cílů a s nimi spojených hrozeb popsat cílový obrat podnikání. Nejde tedy o to, jak určit, jak podnik dosáhne svých cílů. To je úkolem především taktiky, složené z množství hlavních a vedlejších programů. Strategie vytváří rámec pro organizování a činnost.

Zejména v kombinaci se stavem konkurence může vznikat řada situací, které charakterizují podnikatelské prostředí v daném odvětví (Porter, 1994). Při tvorbě strategie, nebo již ve fázi hledání klíčové myšlenky, se k němu můžeme postavit v zásadě dvojím způsobem. Buďto ho vezmeme na vědomí jako skutečnost, které hledanou strategii přizpůsobíme, nebo naopak budeme hledat metody, kterými by bylo možno stávající stav překonat, změnit a využít v náš prospěch.

Při zkoumání konkurence z hlediska možné strategie se soustřeďujeme zejména na tyto tři otázky:

- jaký je stav daného odvětví,
- jaký je stupeň konkurence v daném odvětví,
- jaký je práh pro vstup do podnikání v daném odvětví.

Obecně platí, že čím více je na trhu soutěžitelů s přibližně stejnou tržní silou, tím vyšší je stupeň konkurence v daném odvětví. Se stupněm konkurence pak přímo souvisí stabilita daného odvětví. Nestabilní prostředí je vždy náchylné k prudkým reakcím na změny konkurenčního prostředí a v důsledku toho i k vypuknutí konkurenční války. Vedle stability odvětví je jeho důležitým znakem intenzita konkurence, která v něm panuje. Konkurence v odvětví není jen otázkou samotných přímých konkurentů. Podílejí se na ni i činitelé vstupující do odvětví zvenčí. Mohou to být jednak firmy usilující o vstup do odvětví, jednak firmy, jejichž produkty jsou schopny produkty odvětví nahradit. Na konkurenčních podmínkách v odvětví se také významně podílejí i dodavatelé a odběratelé díky síle své vyjednávací pozice. Výsledný efekt působení těchto typů podnikatelských subjektů ve vzájemných vztazích pak určuje celkový obraz konkurence v odvětví (Porter, 1994, s. 5).

Soupeření přímých konkurentů je především věcí hledání nejvyššího dosažitelného efektu. Možnosti zvyšování příjmů jsou přitom omezeny jednak činností konkurentů (cena), jednak limitními možnostmi trhu (kapacita).

2.1 Význam informace v konkurenceschopnosti organizace

Jakákoliv firma, která se chce dnes prosadit na trhu, má své určité tržní zájmy. Z těchto zájmů se odvíjejí určité cíle, kterých chce firma dosáhnout na určitém trhu v určitém časovém období. Na základě takto jasně stanovených cílů se vytváří firemní strategie, kterou rozumíme nějaký postup, prostředky a metody, kterými chce firma splnit své stanovené cíle v určitém časovém horizontu. Přitom vstupují do popředí nové faktory, vznikající buď uvnitř firmy zejména v jejím okolí. Okolní faktory působící na firmu jsou hlavní příčinou jejího vzestupu, úpadku nebo jiných významných změn. Obecně je platné, že úspěch firmy závisí právě na schopnosti a způsobu řešení problémů odvislých od okolních faktorů působících na firmu (Bartes, Dostál, 1999). Vlivem těchto faktorů je nutné stanovenou strategii změnit, případně ji zcela přetvořit.

Mezi problémy týkající se vnějšího prostředí firmy patří například:

- působení konkurence na určitém trhu,
- včasné nalezení potřeb zákazníků a jejich správné uspokojení,
- co nejpřesnější odhad marketingové strategie firmy možnost jejího ovlivnění,
- odhad vývoje makroekonomických faktorů, apod.

Na základě těchto informací vyplývá, že řešení konkurenčního boje je pro vrcholový management firmy velice složitou, náročnou a značně rizikovou záležitostí, vyžadující značné zkušenosti a vysokou úroveň znalostí.

Je nezvratným faktem, že žijeme v době neustále se rozvíjející globalizace tržní ekonomiky, charakterizované neustále se vyvíjejícími změnami a ostrými konkurenčními střety. Díky fenomény globalizace se konkurenční boje neustále vyostřují. Objevují se stále nové hrozby, kterým firmy musí čelit. Informace jsou dnes velmi ceněným a drahým zbožím. Informace jsou stavebním materiálem managementu znalostí a jeho rozhodovacích procesů. Úspěšnou firmu odlišuje od šedi průměru, jak dobře využívá informace. Prostředkem k dosažení managementu znalostí je konkurenční zpravodajství. Konkurenční zpravodajství není pouze záležitostí bezpečnosti, ale představuje celý komplex. Pokud budeme hovořit o konkurenčním zpravodajství, v podstatě tím myslíme komplexní konkurenční boj, který je vlastně

ekonomickou válkou vedenou podnikateli, ale i národními ekonomikami, o nové zákazníky, o nové trhy a o vyšší zisky.

Nezbytnou podmínkou úspěchu v konkurenčním boji vždy byla znalost konkurence a trhu. Nicméně v době, kdy konkurenční boj probíhal na více méně vymezených teritoriích, kde se konkurenti vzájemně znali a kde platila neměnná pravidla, nebylo tak obtížné tyto informace získávat a využívat. Důsledkem globalizace je dnes ale pro kohokoliv dosažitelný jakýkoliv trh, segment zákazníků či obor podnikání. Roste množství příležitostí a hrozeb, složitost vztahů mezi konkurenty a rychlost, s jakou se dění na trhu odehrává. Bez systematického vyhodnocování informací dnes již nikdo není schopen využitelné příležitosti, reálné hrozby a důležité změny ani identifikovat a ani na ně adekvátně a včas zareagovat. Do arzenálu zbraní pro konkurenční boj tak firmy dnes nezbytně musí zařadit *„konkurenční zpravodajství“* (Ivanka, 2009).

Podle Vejlupka (2002), hlavním rozdílem mezi zpravodajstvím ve válce a konkurenčním bojem (ve standardní tržní ekonomice) je to, že ve válce jde o zničení protivníka bez pravidel, zatímco v konkurenčním boji jde o udržení co nejlepší pozice mezi mnoha hráči na trhu, kteří přitom musí dodržovat zákony a obchodní etiku.

Právě proto je přívlastek „konkurenční“ tak důležitý, protože vymezuje hranice zpravodajství, jako nástroje legitimního konkurenčního boje. Legitimní znamená, že vylučuje takové metody, jako je špionáž, vydírání a korupce. Fenomén informační společnosti míru využívání těchto nelegálních, riskantních a zbytečně drahých metod výrazně snižuje i v rámci tajných zpravodajských služeb, které stále více využívají tzv. otevřené informační zdroje. Obrovské množství žurnalistů, široká nabídka poskytovatelů informačních služeb a nejrůzněji motivované skupiny na internetu tvoří totiž tu největší zpravodajskou síť na světě, kterou může využívat úplně každý, kdo k tomu má potřebné znalosti a nástroje.

V důsledku prudkého vývoje a neustálých změn v ekonomice se konkurenční zpravodajství dnes týká všech firem, různých typů a velikostí, protože:

- velké firmy musí díky své velké setrvačnosti včas odhalovat rizika a slepé cesty rozvoje,
- střední firmy musí usilovat o svoji pozici na trhu a vyhledávat příležitosti svého růstu,
- malé firmy musí odhalovat skulinky, kde se díky své pružnosti mohou uplatnit,

- očekávanou rolí konkurenčního zpravodajství bezpochyby je vyplňovat nedostatek informací pro rozhodování, tj. nacházení odpovědí na otázky. V podnikání se však vyskytují dva zásadně odlišné typy otázek, resp. problémů:
- hádanky – otázky, které mohou být zodpovězeny na základě informací, které někde existují, a které tedy s vynaložením patřičného úsilí lze získat („Proč zakázku dostal konkurent a ne my?“);
- záhady – otázky, pro jejichž zodpovězení informace prostě ještě neexistují, a proto je také žádným způsobem nelze získat („Jaký vliv bude mít nová technologie na loajalitu našich zákazníků?“).

Nejkritičtější rozhodnutí týkající se konkurenceschopnosti firmy se týkají právě problémů spadajících do kategorie záhad. Konkurenceschopnost, tedy schopnost existovat a úspěšně se rozvíjet jako samostatný ekonomický subjekt na trhu, závisí na dvou základních parametrech:

- operační efektivnost – schopnost dělat věci správně. Ke zvyšování efektivnosti v podstatě stačí schopnost nacházet odpovědi na otázky spadající do oblasti hádanek, tj. co konkurenti dělají a jak to dělat lépe než oni. Dlouhodobě to však může vést pouze ke sbližování konkurentů, protože všichni pak jedou stejný závod po stejné trati,
- strategický záměr – schopnost dělat správné věci. Volba odlišné strategie naproti tomu znamená zvolit si jiný závod, resp. jinou trať. Tato volba však vyžaduje zodpovídání otázek spadajících právě do oblasti záhad. Protože odpovědi na ně neexistují, vyžaduje to schopnost kvalifikovaného odhadu vývoje na základě slabých signálů, které zpravodajství může identifikovat, a dostatek odvahy a fantazie tento vývoj aktivně ovlivňovat (Brabec, 2001).

Nejdůležitější role konkurenčního zpravodajství tedy spočívá v podpoře tvorby a prosazování konkurenceschopné strategie. Jedním z nejdůležitějších úkolů potom je pomáhat manažerům, aby si uvědomili, že jejich myšlenkový model nemusí odpovídat realitě. Většina lidí si totiž myslí, že to, jak vidí svět, je reálné. To, co si ale člověk myslí, je ale pouze to, co bylo selektivně profiltrováno přes jeho myšlenkový model. Tento myšlenkový model lze aktualizovat jedině kladením nových otázek, které vytvářejí místo pro nové informace (Ivanka, 2009).

Dlouhodobá prosperita podniku a její udržitelnost je určena jednáním okolí a nikoliv jen analýzou výsledků a jejich historického vývoje. V případě vytváření informačního systému pro podporu strategického rozhodování je důležité brát v úvahu, že organizace působí v určitém oboru nebo odvětví podnikání. Z tohoto důvodu je pro ni nezbytné sledovat, analyzovat a včas reagovat na vývoj v okolí jejího působení a na změny v něm probíhající. Organizace by také měla zjišťovat a zaznamenávat jednotlivé měnící se faktory v jejím okolí a měla by se snažit nalézt pro organizaci významné faktory a vazby, důležité pro strategické rozhodování. Bill Gates (1999, s. 184) v knize Business rychlostí myšlenky píše, že *„organizací se musí nejrychleji šířit špatné zprávy a organizace musí mít vybudovaný takový informační systém, proto si vybudujte takový informační systém, který:*

- *umožní rozpoznat špatné zprávy kdekoliv v organizaci a rychle je předat tam, kde je třeba,*
- *rychle shromáždí potřebné informace vztahující se k vzniklému problému,*
- *umožní rychle identifikovat pracovníky či celé organizace mající potřebné kompetence (znalosti) k řešení vzniklého problému.“*

Současná globální ekonomika vyžaduje od organizací, které chtějí být konkurenceschopné, zaměření se na rozhodování v oblasti produktových strategií z externích informačních zdrojů a využívání intelektuálního kapitálu vlastních zaměstnanců. S rozšířením internetu došlo k prudkému distribuování informací, které ztrácejí své hmotné umístění a často i svého majitele. Jedním z podstatných problémů informační společnosti je vyhledávání v neustále rostoucím množství různorodých a rozptýlených informací. Toto omezení je velice problematické v podnikatelské oblasti, kde jsou dnes informace regulérním hospodářským zdrojem. Výkonnost technologií poskytujících informace v elektronické podobě neustále roste a ostře kontrastuje s obecně nedostatečnou schopností tyto informace účinně využívat. Jedná se zejména o oblast řešení jednorázových a málo strukturovaných úloh, které jsou typické pro rozhodování na strategické úrovni, například v oblasti vyhledávání nových příležitostí vyplývajících z možnosti kooperační spolupráce s dalšími organizacemi ve stejném anebo příbuzném oboru.

V praxi a teorii moderního managementu se setkáme s řadou přístupů k zvyšování konkurenceschopnosti. Příkladem může být proces analýzy, návrhu a implementace strategie vedoucí k získání a udržení konkurenční výhody, který zahrnuje širokou škálu nástrojů a metod strategického řízení (Johnson, Scholes, 1997).

Nejčastějším přístupem v oblasti konkurenceschopnosti a nalezení vlastních konkurenčních výhod je Porterova analýza pěti konkurenčních sil (1980). Dle Hamela (1987) a Prahalada (1990) lze zvyšovat konkurenceschopnost také na základě klíčových kompetencí a klíčových produktů nebo pomocí hierarchie strategií rozvíjejících poslání podniku a využívajících koncept strategických podnikatelských jednotek (Keřkovský, Vykypěl, 2003).

Aplikace jakéhokoliv z uvedených přístupů k zvyšování konkurenceschopnosti je vždy závislá na dostupnosti potřebných informací a schopnosti účinně tyto informace využít při podpoře rozhodování. Systematické vyhledávání informací, analýza souvislosti a návrh nejlepších možných řešení rozhodovacích úloh jsou v praxi velice obtížné. Příčinou je složitost, množství, různorodost a rozptýlenost informací o podniku a jeho okolí. Pro časovou tíseň, kdy není možno z nedostatku času proniknout hlouběji do problému, omezenost relevantních informačních vstupů, omezenost přístupů k jejich zpracování a omezená rozhodovací způsobilost rozhodovatele (omezené analytické schopnosti, omezená schopnost systémového myšlení), zabraňují hledání všech relevantních informací, analýze klíčových souvislostí a vyhodnocení všech uskutečnitelných rozhodovacích variant. Rozhodovatel se raději spokojí s omezeným množstvím kritérií a volí první nalezenou variantu, která na základě dostupných informací a intuice splňuje alespoň rámcové požadavky (Vágner, 2003). Takovýmto způsobem se ale spíše zvyšuje riziko špatného rozhodnutí, namísto zvyšování konkurenceschopnosti.

Zvyšování konkurenceschopnosti je tedy omezováno nedostatečnou dostupností kvalitních manažerských informací a nedostatečnou schopností je účinně využít. Mezi nejvýznamnější faktory, které mohou zlepšit práci s externími informacemi, patří integrace informací a znalostí z různých informačních zdrojů. Mezi hlavní problémy spojené s vyhledáváním externích informací patří nedostupnost informací, časová náročnost jejich vyhledávání a neefektivnost jejich zpracování. Problémem je tzv. *informační fragmentace*, tj. situace, kdy jsou informace uložené v různých formátech, rozptýlené na různých místech, přístupné prostřednictvím různých aplikací a vzájemně nepropojené. Příkladem informační fragmentace je řešení úlohy, při které řešitel pracuje s dokumenty ve Wordu, s emaily v Outlooku a využívá také oblíbené položky v Exploreru. Uložení informací, které se týkají jednoho problému, na třech různých místech podle jejich formátu ukazuje potenciální nesoulad mezi informačním systémem a potřebami řešitele (Bergman, 2006).

Klíčem k řešení problému informační fragmentace, která omezuje dostupnost a využitelnost manažerských informací, je využití vhodných nástrojů a metod znalostního managementu, zvláště potom konkurenčního zpravodajství. Princip efektivní integrace znalostí pomocí konkurenčního zpravodajství vychází z faktu, že společným jmenovatelem znalostí ve všech sledovaných doménách je možnost jejich částečného nebo úplného vyjádření pomocí jazykových, tedy slovních prostředků (Tondl, 1998). Slovním vyjádřením rozumíme nestrukturovanou informaci a schopnost vyhledávání nestrukturovaných informací v různorodých zdrojích a je jednou z klíčových předností nástrojů a metod konkurenčního zpravodajství. Jeho další předností je podpora grafické analýzy mnohočetných souvislostí. S pomocí těchto nástrojů je možno vytvořit systematicky uspořádaný soubor znalostí, který slouží k rychlému a snadnému vyhledávání potřebných informací, jejich analýze a poskytování těm uživatelům, kteří je potřebují a dokáží je plně využít.

Současnost lze označit jako informační věk, kdy se ekonomické činnosti spoléhají na informace a komunikační sítě, energie se transformuje na data a dochází k externalizaci lidského myšlení. Informace důležité pro rozhodování jsou dostupné na úrovni, na které je třeba rozhodnutí provést. Za každým úspěchem stojí schopnost včasné mobilizace a zužitkování dostupných informací. Informace je dále chápána jako údaj, který snižuje neurčitost chování jejího příjemce. Příjemcem může být člověk, stroj či jiný systém. Pokud jsme tedy příjemci my lidé, lze říci, že informace je údaj, který snižuje neurčitost našeho chování. Každou informaci je možné ohodnotit důležitostí a včasností (Berger, Luckman, 1999).

Pro dobrou funkci jakékoliv podnikatelské aktivity je třeba, aby existovala včasná oprava odchylek a chyb mezi stanovenými cíly a jejich realizacemi. K tomu je ovšem třeba:

- rychle a operativně se rozhodovat,
- pružně a efektivně získávat, přenášet a zpracovávat informace,
- neustále zdokonalovat celý informační systém.

Narušení informačního procesu, nevydávání nebo nezískávání správných a potřebných informací, opožďování jejich přenosů – to vše vede ke špatné funkci podnikatelské aktivity. Schopnost podnikatele přijímat užitečné informace a oddělovat pro svoji činnost zbytečné či škodlivé, závisí i na jeho zkušenostech:

- ze vzájemného vlivu způsobu podnikání a prostředí, v němž se podnikatelská aktivita uskutečňuje,

- z řešení problémových situací spojených s rušivými vlivy, které se v podnikatelské činnosti vyskytují.

Čím různorodější a mnohostrannější zkušenosti podnikatel má, tím je jeho podnikání stabilnější a tím větší okruh rušivých vlivů je schopen profiltrovat. Podnikatelská činnost totiž funguje v podmínkách neustále se měnícího prostředí a zvyšování množství a různorodostí informací, které na podnikání působí. V případě konkurence metody konkurenčního působení nemusí být vždy zcela korektní. Proto v takových podmínkách nemůže existovat dlouhodobý absolutní soulad mezi informacemi, které podnikatel zná a informacemi vznikajícími ve vnějším prostředí ekonomickém (tržním, obchodním) i všeobecně politickém, společenském atd. Podnikatel je totiž nemůže všechny okamžitě znát a tím na ně reagovat. Tedy prakticky nemůžeme dosáhnout absolutní dokonalosti systému podnikání (Vymětal, 2005).

Na podnikání lze nahlížet také z informačního hlediska. Než dojde k rozhodnutí se pro nějaký cíl, než dojde k investici finančních prostředků nebo přijetí nového pracovníka, vždy je cílem získat informace, jejichž obsahem se dále řídíme. Je třeba ale, v souladu s podnikavostí, nepřetržitě, cílevědomě pracovat a proto podnikavost musíme zajišťovat nepřetržitým tokem informací.

Bez informací nelze:

- efektivně podnikat,
- zajistit racionální fungování a úspěšný rozvoj vlastního podniku,
- dosáhnout cílů, které jsme si jako podnikatelé vytýčili.

Nebudeme-li mít dostatek informací, budeme podléhat:

- subjektivizmu, tj. čistě intuitivním a nepodloženým rozhodnutím,
- způsobům chování neslučitelným s racionální podnikavostí

Informace jsou jakýmsi kompasem, který nám umožňuje orientaci v nesmírně složitém labyrintu podnikatelských jevů, působení na ně, využívání sociálních i přírodních sil a dosahování stanovených cílů.

Obsah objemu informací potřebných pro podnikání závisí na:

- úkolech, které podnikatel řeší, rozsahu významu přijímáních rozhodnutí (čím, významnější rozhodnutí, tím rozsáhlejší informace jsou potřeba),

- počtu a charakteru podmínek, které ho ovlivňují (čím je větší jejich počet, tím různorodější musí být informace),
- době trvání podnikatelské akce,
- množství variant množného stavu a chování podnikatelského systému,
- velikosti a mnohotvárnosti působících vnitřních i vnějších podnětů,
- počtu a kvalitě ukazatelů charakterizujících výsledky podnikání.

Látal (1996, s. 14) definuje podnikatelskou informaci následovně:

„Podnikatelské informace jsou informace obíhající v podnikatelské sféře a využívané v ovlivňování výrobních, obchodních a jiných procesů. Týkají se především vztahů lidí k podnikatelské aktivitě, vztahů mezi sebou, jejich vzájemného působení, potřeb, zájmů i cílů apod. Jestliže považujeme podnikatelskou činnost za důležitou, pak musíme mít také určité požadavky na vlastnosti informací z procesů v podnikání. Požadujeme, aby byly komplexní, úplné, přesné, spolehlivé, včas a hospodárně získané, někdy stručné ale přitom logicky uspořádané a zejména užitečné pro vlastní podnikatelskou činnost. To zajišťujeme vytvářením informačního systému.“

2.2 Bezpečnost informací

Bezpečnost IT je zpravidla iniciována jednostranně, buď managementem, projektovými pracovníky například v elektronickém obchodování nebo pracovníky IT jako jsou správci sítě nebo správci serverů. Hledání řešení se většinou stává technickým úkolem, ale zadání úkolu není často pochopeno správně nebo komplexně. Hledá se nebo doporučí se řešení, aniž by se problém dostatečně definoval. Organizační cíle v řízení bezpečnosti, např. zavedení nebo proveditelnost zůstávají často nezohledněny a ekonomické cíle projektu, které by mohly ospravedlnit návratnost investic v podobě výdajů na bezpečnost, zůstávají obvykle neznámé. Řízení bezpečnosti a kvality představuje v organizaci dva důležité pilíře. Řízení bezpečnosti chrání před nebezpečími, které podniku hrozí a management kvality zabezpečuje definovaný, pokud možno konstantní výstup produktů nebo služeb. V době změn z průmyslové společnosti na společnost vědomostí představují informace nejdůležitější složku. Je nutné je chránit a zabezpečit. To pro většinu podniku ovšem také znamená duševní převrat v nakládání s těmito oběma tématy. Mezitím si ve většině podniků i v oblasti státní správy uvědomili, jak silně jsou závislí na elektronické komunikaci, jaké výhody a nevýhody přinesla nová „elektronická“ vlna. Také vznikly s pokrokem informační společnosti nové výzvy. Ty teď začínají být pomalu vnímány, blíží se ovšem mnohem rychleji, než

to bylo v minulosti obvyklé. Jestli budeme celou situaci sledovat a zredukujeme ji na jádro, musíme konstatovat, že většina obratů a zisků firem je vytvářena na základě stávajících IT struktur. Důležité obchodní procesy nejsou v současnosti v mnoha středních a velkých podnicích myslitelné bez IT podpory. Tak se informační technologie staly páteří úspěšnosti podniku, vznikl vztah závislosti, který řada odpovědných pracovníků na různých úrovních managementu ještě nerozpoznala nebo nechce akceptovat (Sedláček, 2010).

Samotná investice do technických systémů je u spousty podniků realizovatelná pouze na několika málo pracovištích. Malé pobočky, dislokovaná pracoviště nebo domácí kanceláře lze sice za určitých okolností napojit pomocí bezpečného síťového spojení (VPN), ale většinou nejsou na místě technickými prostředky dostatečně chráněny před nebezpečími zevnitř a zvenčí. Jak pořízení a instalace, tak i provoz jsou nákladné. Kromě toho často nejsou k dispozici dostatečné znalosti, jak zacházet s technickým vybavením. V neposlední řadě jako nejdůležitější aspekt je nejméně předvídatelný faktor člověk. Neexistuje stoprocentní bezpečnost, jde jednak o vyváženost úrovně bezpečnosti a jednak o zvýšení stávající bezpečnostní úrovně, například prostřednictvím směrnic o bezpečnostním chování, zacházení s hesly nebo administrativních postupech. Zvládnout tento problém znamená dostat se od neznámé bezpečnostní úrovně k definované bezpečnostní úrovni. Základem toho je na jedné straně úměrné zprostředkování znalostí v podniku a důsledná informační politika. Na druhé straně ale také nutná a přiměřená organizační opatření. K nim patří vytvoření a zavedení individuálních bezpečnostních směrnic na různých úrovních organizace, které vytvoří solidní, celopodnikový soubor pravidel. Pravidelně a profesionálně používané kontrolní mechanismy nakonec přinesou požadovanou bezpečnost. Komplexní bezpečnostní systém se skládá z organizačních a technických složek a liší se firma od firmy. Závisí na obchodním modelu, stupni elektronického modelování obchodů, dostupných IT struktur, komunikačních a bezpečnostních struktur a homogenity a disciplíny v organizaci.

Podrobíme- li organizaci, která důležité procesy realizuje na bázi IT, bližšímu pozorování, nalezneme většinou velmi heterogenní realitu IS. Podle toho, který výchozí bod si snahy o informační bezpečnost zvolily, jsou buď etablována dobrá technická detailní řešení většinou v oblasti firewallu nebo antivirové ochrany, nebo jsou k dispozici dobře vypracované dokumenty IS. Téměř všude ale chybí obsáhle strukturovaný pohled na situaci IS jako základu pro soustředěný proces IS, který stejnoměrně sleduje všechny požadavky, rámcové podmínky a ostatní ovlivňující

veličiny. Aby se bezpečnost IT etablovala jako komplexní proces, nabízí se soubory standardních kritérií, které osoby pověřené bezpečností podporují po metodické a obsahové stránce. Jak pro produkty, tak i pro celková řešení se vedle sebe etablovaly různé soubory kritérií pro tematickou oblast bezpečnost IT. Tato bezpečnostní kritéria IT se částečně obsahově překrývají, vytyčují ovšem rozdílné stěžejní úkoly a zaměřují se na různé cílové skupiny. Cílem ISO 17799/ISO 27001 je vytvořit systém řízení bezpečnosti informací – Information Security Management Systém (ISMS), který svou komplexností smysluplně zahrnuje jak nejvyšší pozice v organizaci, tak i administrativní pracovníky. Pouze v této komplexnosti prokazuje bezpečnost informací v konečném efektu svůj prospěch a splňuje očekávání, která do ní byly předem vloženy (Sedláček, 2010).

Z důvodu neustále rostoucích požadavků na IT systémy a zvyšující se závislosti na nich, je i tlak na rozsáhlá bezpečnostní opatření stále větší. Aby se potřebné celkové náklady na bezpečnost IT minimalizovali, využívají se v praxi většinou standardní soubory kritérií, které osoby odpovědné za bezpečnost podporují po metodické nebo obsahové stránce. Jak pro produkty, tak i pro celková řešení se vedle sebe etablovaly různé soubory kritérií pro tématickou oblast bezpečnosti IT. Tato bezpečnostní kritéria IT se částečně obsahově překrývají, mají ale různá těžiště a zaměřují se na různé cílové skupiny.

Standardy lze podle Doucka (2008) srovnat a vyhodnotit podle určitých kritérií, kterými jsou cíle standardů, cílové skupiny, aplikovatelnost atd.

2.2.1 ISO/IEC 17799:2005 a ISO 27001:2006

Cílem ISO/IEC 17799:2005 je v první řadě poskytnout rozsáhlou sbírku opatření, která vyhoví koncepci „best practice“ (nejlepších postupů/praktik) v oblasti bezpečnosti informací. Norma má být společný vztažný bod k identifikování různých opatření. ISO 17799 má za úkol tato vhodná opatření prezentovat (informativní norma) a ISO 27001 (kriteriální norma – rozhodná pro certifikaci ISMS) tvoří základ pro systematiku jak tato opatření specificky pro danou organizaci posoudit a použít podle ekonomických kritérií a kritérií prostředí. V normě ISO 17799 se sledují aspekty bezpečnostní politiky, organizace bezpečnosti, klasifikace a kontroly hodnot, personální bezpečnost, fyzická bezpečnost a bezpečnost prostředí, řízení komunikace provozu, vstupní kontroly, vývoj systému a údržba, řízení kontinuity činnosti organizace a dodržování závazků.

Norma ISO/IEC 17799 (ISO 27001) se v zásadě zaměřuje na úřady a podniky všech velikostí, ne však na soukromé uživatele. Cílová skupina normy není definována, ale na základě struktury a obsahu lze za logickou cílovou skupinu považovat jak

všechna místa, která jsou odpovědná za výběr a realizaci bezpečnostních opatření IT, jako např. administrátor IT, bezpečnostní ředitel IT, apod., tak i osoby odpovědné za řízení (dodržování opatření), jako např. interní audit nebo certifikační audit. Protože se norma zabývá řízením bezpečnosti informací, je způsobilost k hodnocení jednotlivých produktů dána pouze velmi omezeně, proto má smysl sledovat pouze sociotechnický systém. Vsazení produktu do systémového prostředí lze zase podrobit normativně zaměřenému posouzení.

Aplikační postup zahrnuje tyto kroky: definování politiky informační bezpečnosti, stanovení oblasti použití systému řízení bezpečnosti informací, provedení přiměřené analýzy rizik, identifikování rizikových oblastí, výběr bezpečnostních cílů a opatření, „Prohlášení o aplikovatelnosti“ (PoA) opatření. Normu lze aplikovat různými způsoby. Na jedné straně umožňuje použití jako příručka k vyhledávání specifických otázek o použití jednotlivých opatření, dále při systematickém zpracování doporučeného opatření umožňuje vybudování systému řízení bezpečnosti informací (ISMS) odpovídající současnému stavu vědy a techniky a za třetí připouští zřízení certifikovaného systému řízení založeného na této normě.

Norma je explicitně určena pro instituce všech velikostí a také pro jejich dílčí části. Na základě orientace na řízení systémů tento princip v principu splňuje, přičemž opatření jsou zaměřena spíše na větší instituce. Mnoho ustanovení normy je relativně nezávislé na velikosti sledované instituce, takže náročnost vzrůstá velmi proporcionálně k velikosti. Pouze v rámci analýzy rizik platí klasické poměry velikosti-náklady, přičemž tvoření skupin umožňuje redukci nákladů. Jestliže se systém rozloží na dílčí systémy, hrozí problém spojení dílčích systémů, protože seskupení již není jednoduše možné.

Norma ISO 27001 byla přijata jako ČSN, podobně jako ISO/IEC 17799. Pravidelná aktualizace je plánována podle obecného postupu k přizpůsobení norem ISO/IEC, neexistují ovšem pevně organizované závazné cykly.

Norma ISO/IEC 17799 se silně orientuje na přístup „top-down“ a obsahuje v první řadě generická standardní bezpečnostní opatření. Tato opatření pokrývají všechny v současnosti relevantní oblasti. Neobsahuje produktově orientovaná opatření a pouze silně kumulovaná technologická opatření, protože u opatření obecně existuje spíše maximálně střední detailizace. Norma se všeobecně neomezuje na specifickou úroveň bezpečnosti, ale doporučená opatření se zaměřují především na koncepci základní ochrany a jsou pro vysoké až vyšší bezpečnostní úrovně vhodná až po úpravách. Koncept zaměřený na řízení ale nabízí podporu i pro tyto bezpečnostní

úrovně. Při nižších úrovních bezpečnostních požadavků norma umožňuje doporučení odůvodněně odmítnout, přičemž je umožněno i přizpůsobení na menší podniky.

Aplikovatelnost normy dalekosáhle závisí na struktuře instituce, přičemž vhodnost pro velké instituce je větší než pro menší instituce a také zohlednění institucí a organizačních úseků s velmi vysokými bezpečnostními požadavky je možné pouze po doplnění. Na základě koncepce zaměřené na řízení není dáno omezení její použitelnosti na určité technické systémy a typy systémů.

Z důvodu silného zdůrazňování organizačních opatření jsou náklady na realizaci silně odvislé od obecné organizační kvality organizace. Instituce, které mají spíše nedostatečnou organizaci, budou muset vynaložit mnohem větší náklady, než instituce, které jsou organizovány normálně až nadprůměrně. Díky konceptu základní bezpečnosti je zpravidla možné (bez dodatečných nákladů) existující opatření v podniku s výhodou použít ke zvýšení bezpečnostní úrovně. Náklady na provedení analýzy výrazně závisejí na rozsahu analýzy rizik. Zde je možné výběrem různých typů analýz rizik generovat velmi rozdílné náklady (Doucek, 2008).

2.2.2 ISO TR 13335

Co se týká cíle standardu, tak ISO TR 13335 se v současnosti přepracovává, moduly označené níže jako Část 1 a 2 byly mezitím shrnuty do části 1, části 3 a 4 se stanou částí 2. V budoucnosti se bude ISO 13335 skládat už jenom ze dvou částí. Soubor současných čtyř „technických zpráv“ (technical reports), pátý k bezpečnosti sítí je také k dispozici, nabízí v podstatě technické informace a nebyl jako ČSN vydán) nabízí podporu pro řízení bezpečnosti IT, aniž by vnucoval určitá řešení. Část 1 „Koncepty a modely bezpečnosti IT“ definuje základní pojmy bezpečnosti IT a základní aspekty (hrozby, rizika, slabá místa atd.), jakož i procesy (např. prevence havárií, analýza rizik, senzibilizování). Obrací se na odpovědné manažery a bezpečnostní referenty v organizacích. Část 2 „Řízení a plánování bezpečnosti IT“ podává informace k utváření procesu bezpečnosti IT, jeho integraci do stávajících podnikových procesů a navrhuje organizace bezpečnosti IT. Část 3 „Techniky pro řízení bezpečnosti IT“ vylepšuje kroky procesu bezpečnosti IT a upozorňuje na metody a techniky, které lze k tomu využít. Část 4 „Výběr bezpečnostních opatření“ na závěr přináší informace, jaká opatření přicházejí v úvahu pro jaké hrozby a jak lze např. určit přiměřenou úroveň základní ochrany organizace.

Ústřední cílovou skupinou v tomto případě jsou vedoucí pracovníci organizace, kteří přicházejí do styku s plánováním nebo realizováním procesu bezpečnosti IT,

přičemž jednotlivé díly mají různou relevanci: Část 1 se obrací na vedoucí pracovníky na úrovni představenstva, zejména na osoby odpovědné za celopodnikový systém bezpečnosti IT. Část 2 se zaměřuje na vedoucí pracovníky, kteří jsou odpovědni za IT systémy organizace nebo jejichž sféra kompetencí silně závisí na využívání IT. Části 3 a 4 se obrací na všechny, kteří se během různých fází v životním cyklu projektů musejí potýkat s bezpečností IT.

Jednotlivé části výslovně nepředepisují žádné postupy a řešení, nýbrž obsahují informace, jak je možné je pro organizaci vyvinout a přizpůsobit a jaké metody a modely jsou k tomu účelu k dispozici. Není plánováno použít dokumenty k měření úrovně bezpečnosti IT nebo jiným způsobem využít pro doložení shody s normou.

Co se týká rozšiřitelnosti, tak zprávy je v jejich obecnosti zásadně nutné přizpůsobit specifickým zvláštnostem libovolných institucí a jejich IT infrastruktuře resp. projektů, a jsou také přizpůsobitelné. Ve svých různých částech podávají pomocnou ruku od úrovně představenstva až po projektovou úroveň. Procesy a postupy lze v reálu plně realizovat pouze ve středních a velkých institucích. Jako návod jsou však zprávy univerzálně použitelné.

Část 1 je datována do roku 1996, část 2 1997, část 3 1998 a část 4 2000. Část 5 ještě nebyla vydána. Technické zprávy ISO je možné v případě potřeby aktualizovat v nepravidelných intervalech. Díky obecnosti výroků to ale v dohledné době nebude nutné.

Zprávy jsou co do popisu organizace a komponent procesu bezpečnosti IT úplné. Protože pouze dávají návod pro definování těchto procesů a struktur v rámci organizace, není ani stanovena úroveň bezpečnosti IT, protože k určení takové úrovně dochází až v rámci takto vytvořené organizace a procesů.

Zprávy jsou použitelné pro všechny instituce v závislosti na jejich výchozí struktuře. Směřují ovšem k prověřování a eventuálně přizpůsobení struktury ohledně potřebných bezpečnostních procesů IT. K tomu uvedené pokyny nezávisí na komplexnosti existujících struktur a požadované bezpečnostní úrovně.

Náročnost a náklady na zavedení – náklady na zavedení a udržování procesu bezpečnosti IT v podniku závisí na již existující organizační struktuře a není možné je uvést paušálně. Platí stejné úvahy jako pro ISO/IEC 17799 (Doucek, 2008).

2.2.3 ITSEC/Common Criteria (ISO 15408)

Cílem evaluačních kritérií ITSEC a Common Criteria je definovat kontrolní postup, jehož pomocí lze strukturovaně zkoumat bezpečností aspekty produktů a systémů IT ohledně jejich bezpečnostních vlastností, a sice takovým způsobem, aby

výsledky těchto šetření byly doložitelné a srovnatelné. K tomu účelu definují soubory kritérií funkční a kvalitativní požadavky na zkoumané předměty šetření, které se vztahují jak na jejich vlastnosti, tak i na postupy jejich vytváření.

Soubory kritérií se obracejí na výrobce IT systémů, IT produktů a IT komponent, kteří plánují jejich použití v prostředí s požadavky na bezpečnost. Těmto výrobcům je do ruky dána hodnotící mřížka, jejíž pomocí mohou vývoj a ošetřování svých produktů utvářet tak, aby tyto produkty měly definované bezpečnostní vlastnosti a aby existence těchto vlastností byla doložitelná pro třetí subjekty. Zaměřením vývoje na bezpečnostní profily definované pro Common Criteria mohou výrobci zlepšit a standardizovat bezpečnostní vlastnosti svých produktů. Tak jako druhá cílová skupina pro soubory kritérií uživatele IT v bezpečnostních oblastech, který potřebuje informace o bezpečnostně-technické kvalitě používaných IT systémů. Prověření takových systémů nezávislou, kompetentní organizací může uživateli pomoci získat potřebnou důvěru v bezpečnostní vlastnosti celých systémů nebo jejich součástí. Objektivní, na systému nezávislý charakter kritérií, přitom napomáhá vzájemně porovnávat různé systémy anebo produkty a nalézt optimální řešení pro příslušné bezpečnostní požadavky, pokud takové existuje.

Soubory kritérií se jako specifikace používají při vývoji popř. dalším rozvoji IT systémů, IT produktů a IT komponentů. Tato specifikace zahrnuje funkční a kvalitativní aspekty předmětů prověřování. Funkční vlastnosti se přitom vztahují na existenci a charakter určitých technických funkcí, jejichž pomocí lze budovat bezpečné systémy. Kvalitativní aspekty se naproti tomu vztahují na samotný postup vývoje, jehož pomocí se má na jedné straně zaručit správnost realizovaných funkcí a na druhé straně účinnost stanovených bezpečnostních opatření. Podrobné zkušební návody přitom mají zajistit, že funkční a kvalitativní aspekty předmětů prověřování budou doložitelně dokumentovány. Samotné zkoušky provádějí v rámci takzvané evaluace nezávislé zkušební organizace podle zadání zkušebních instrukcí a jsou dokumentovány v protokolu o zkoušce.

Náklady na zkoušku podle jednoho ze souboru kritérií závisí jak na komplexnosti předmětu prověřování, tak i na hloubě zkušební metody. Komplexnosti lze vyhovět tím, že se zkouška může omezit na bezpečnostní aspekty, jestliže lze rozpoznat jasné oddělení od nebezpečnostních aspektů. Hloubku zkušební metody lze zvolit v definovaných stupních, v závislosti na bezpečnostních požadavcích, které mají být předmětem prověřování splněny. Výsledkem je široké spektrum ohledně nákladů na

zkoušku, ale je nutné mít na paměti, že tyto náklady s rostoucí komplexností a hloubkou prověřování velmi výrazně narůstají.

Soubory kritérií jsou relativně stabilní a zřídka se mění. ITSEC pocházejí z roku 1991 a aktualizace se již neplánuje, protože tento soubor kritérií nahradí Common Criteria. Aktuální verze 2.1 standardu Common Criteria nese datum srpen 1999 a následnická verze se v dohledné době neplánuje.

Soubory kritérií si činí nárok moci libovolné IT systémy, IT produkty a IT komponenty prověřit z hlediska jejich bezpečnostních vlastností. Common Criteria přitom umožňují přesnější stanovení bezpečnostních vlastností předmětu prověřování, než je to možné pomocí ITSEC, protože obsahují rozsáhlejší specifikaci bezpečnostních funkcí, se kterými lze předmět prověřování modelovat. Definováním bezpečnostních profilů lze definovat standardizované aplikační případy pro Common Criteria. Definováním bezpečnostních úrovní lze předepsat různé hloubky prověřování, které mohou sahat od globálního back box testu až po podrobné analýzy podle matematických modelů. Reálně lze ale komplexní předměty prověřování zkoumat pouze do určité omezené hloubky, protože náklady na prověřování jsou jinak neúnosné.

Přímá aplikovatelnost souboru kritérií na běžné podnikové struktury by měla být spíše výjimkou, protože v jednoduchých případech jsou náklady na evaluaci podle takovéhoto standardu tak vysoké, že samostatné prověření není opodstatněné. Význam spočívá spíše v tom, že je možné zde pomocí definovaných zkoušek poskytnout standardizované komponenty, které disponují definovanou, doloženou bezpečnostní úrovní. Použití takových komponentů v IT podniku pak může tyto informační technologie vybavit definovanými bezpečnostními funkcemi s předepsanou kvalitou. Přitom je ale nutné dbát na to, že se evaluace bezpečnosti vždy vztahuje pouze na definované hardwarové a softwarové konfigurace, které se ne bezpodmínečně shodují ve všech detailech s konfiguracemi praktického použití.

Náročnost a náklady na evaluaci podle jednoho ze souborů kritérií jsou spíše vysoké, jestliže usilujeme o poněkud průkaznou hloubku prověření. Zde je nutné obzvláště zohlednit aspekty délky takového prověření, protože se stává, že zkoumaný produkt při ukončení prověření již není aktuální a je nahrazen následnou verzí. Problém aktualizace výsledků prověřování je v současnosti nutné považovat v podstatě za nevyřešený.

2.2.4 CobiT

„Jedná se o sadu všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, která má za cíl pomoci organizaci maximalizovat užitek plynoucí z informačních technologií“ (Doucek, 2008, str. 48).

Intenzivní používání IT na podporu a realizaci obchodních postupů vyžaduje zavedení vhodného kontrolního prostředí. CobiT (Control Objectives for Information and Related Technology) vyvinula organizace ISACA (Information Systems Audit and Control Associacion) jako jednu metodu, která má umožňovat prověřovat úplnost a efektivitu takového kontrolního prostředí k omezení vznikajících rizik.

Cílové skupiny – CobiT rozlišuje cílové skupiny:

- management – na podporu při zvažování mezi riziky a investicemi do kontrolních opatření,
- uživatelé – k lepšímu odhadu spolehlivosti a kontroly IT služeb, které jsou poskytovány interně nebo třetími subjekty,
- kontroloři – k věcnému zdůvodnění výsledků kontrol nebo při poradenství v rámci vybudování a provozu interních kontrol a
- osoby odpovědné za procesy nebo IT – na podporu při své práci.

Při aplikování standardu CobiT uživatel nejprve určuje, které IT procesy jsou pro konkrétní situaci relevantní. Pro každý kontrolní cíl vybraných IT procesů je pak nutné zvážit, do jaké míry splňují stávající opatření požadavky. CobiT rozlišuje sedm různých obchodních požadavků a seskupuje je do tří kategorií kvalita, bezpečnost a řádnost:

- Kvalita IT určená účinností a hospodárností provozních procesů se odráží v kritériích efektivita a účinnost.
- Bezpečnostní požadavky důvěrnost, integrita a dostupnost jsou v CobiTu také vyjádřeny.
- Pro zajištění spolehlivosti finančních hlášení (účetní předpisy) zná CobiT kritérium spolehlivost a pro dodržování interních a externích norem kritérium dodržování právních požadavků.

Podle standardu CobiT jsou obchodní procesy podporované IT založeny na těchto IT zdrojích:

- Data: externí a interní datové prvky v nejširším smyslu.
- Jako aplikace se označuje suma manuálních a programovaných postupů.
- Technologie zahrnují HW, operační systémy, systémy správy databází, sítě, komunikační aplikace, atd.
- Zařízení: všechny zdroje k umístění a podpoře informačních systémů.
- Personál: znalosti, vědomí a produktivita k plánování, organizování, pořizování, plnění, podpoře a monitorování informačních systémů a služeb.

IT zdroje se mají kontrolovaně plánovat, vyvíjet a implementovat, stejně jako provozovat a monitorovat. Prostřednictvím CobiT jsou definovány 34 kritické procesy, které jsou rozhodující pro úspěch řízení IT. Tyto IT procesy, které jsou základem IT zdrojů, lze seskupit do čtyř nadřazených domén, které tvoří uzavřený životní cyklus:

- plánování a organizace,
- pořízení a implementace,
- provoz a podpora,
- monitorování.

Pro 34 kritických IT procesů je uvedeno celkem asi 300 klíčových úkolů. Ke každému klíčovému úkolu se přiřazují potřebné IT zdroje a na základě požadavků z kategorií kvalita, bezpečnost a řádnost jsou definovány kontrolní cíle.

Z důvodu maticové struktury standardu CobiT uživatel může sledovat pouze jednotlivé domény nebo procesy nebo vybrat podmnožinu ze sedmi obchodních požadavků (např. pouze bezpečnostní požadavky důvěrnost, integrita a dostupnost).

Standard CobiT vytvořila v roce 1996 asociace Information Systems Audi and Control Foundation a v roce 1998 ho rozšířila a kompletně přepracovala. Druhé vydání nabízí zejména materiály a software pro práci c CobiT. Třetí vydání z roku 2000 bylo publikováno jako „otevřený standard“. Od roku 2006 je k dispozici 4. Vydání.

CobiT nabízí metodu k evidování procesů orientovaných na IT a doprovodných procesů. Příslušné kontrolní cíle jsou definovány nezávisle na technice a lze je použít pro různá systémová prostředí. Pro vytvoření bezpečnostních konceptů je ovšem nutné doplnění o specifická systémová opatření. CobiT je zaměřen na bezpečnostní zájmy typického podniku. Jsou zohledněna témata jako hájení původních firemních zájmů (integrita a důvěrnost interních informací a procesů), stejně jako dodržování zákonných předpisů (ochrana dat, účtování). Pevná bezpečnostní úroveň není předepsána, existuje zaměření na podnikové cíle.

CobiT lze jako procesně orientovanou metodu použít nezávisle na interní struktuře nebo právní formě podniku. Úplná analýza všech kontrolních cílů v rámci středně velkého podniku pomocí CobiT by měla být ukončena asi do jednoho pracovního měsíce (Doucek, 2008).

2.3 Podnikatelské klastry

Jedním z osvědčených způsobů rozvoje konkurenceschopnosti a hospodářského růstu je také sdružování malých a středních firem do podnikatelských klastrů (Sölvell, 2003). Podpora rozvoje klastrů se stala nástrojem mikroekonomické podpory rozvoje konkurenceschopnosti ve vyspělých, přechodových i rozvojových ekonomikách na celém světě včetně České republiky. Porterova definice klastrů, kterou uvedl v časopise Harvard Business Review „Klastry a nová ekonomika soutěže“ je následující (Porter, 1990): *„Klastry jsou místní koncentrace vzájemně propojených firem a institucí v konkrétním oboru. Klastry zahrnují skupinu provázaných průmyslových odvětví a dalších subjektů důležitých pro hospodářskou soutěž. Obsahují např. dodavatele specializovaných vstupů, jako jsou součásti, stroje a služby, a poskytovatele specializované infrastruktury. Klastry se často rozšiřují směrem dolů k odbytovým kanálům a zákazníkům, a do stran k výrobcům komplementárních produktů a společnostem v průmyslových odvětvích příbuzných z hlediska dovedností, technologií nebo společných vstupů. Mnoho klastrů také zahrnuje vládní či jiné instituce – jako např. univerzity, normotvorné agentury, výzkumné týmy či obchodní asociace – které poskytují specializovaná školení, vzdělávání, informace, výzkum a technickou podporu.“*

OECD specifikuje klastry s důrazem na specifické rozlišení „sektorů“ a „klastrů“.

„Klastry jsou skupiny nezávislých firem a přidružených institucí, které:

- *spolupracují a soutěží,*
- *jsou mírně koncentrované v jednom či několika regionech, i když tyto klastry mít globální rozsah*
- *jsou specializované v konkrétním průmyslovém odvětví provázaném společnými technologiemi a dovednostmi*
- *jsou buď znalostní či tradiční.“*

Dnešní globalizovaný svět neustále přináší novou konkurenci, inovace a technologie. Podniky jsou vystavovány tlaku z celého světa a získané konkurenční

výhody jsou často rychle pohlcovány. Dochází k neustálým změnám podnikatelského prostředí a pro podnik je nesmírně těžké tuto konkurenční výhodu dlouhodobě udržet. Jednou z možností pro vytváření konkurenčních výhod a růstu konkurenceschopnosti je zapojení podniku do průmyslového klastru. Konkrétní podoba takto získaných konkurenčních výhod se odvíjí od strategie klastru, jeho cílů a přínosů, které poskytuje svým členům.

Dle definice M. E. Portera (1990) klastr představuje *„geograficky blízké seskupení vzájemně provázaných firem, specializovaných dodavatelů, poskytovatelů služeb a souvisejících institucí v konkrétním oboru i firem v příbuzných oborech, které spolu soutěží, ale také spolupracují, mají společné znaky a také se doplňují“*. Klastr tedy představuje efektivní prostředek pro rozvoj spolupráce všech zapojených subjektů, kterým je schopen přinášet různé přínosy a efekty.

Klastry si mohou stanovit nejrůznější cíle svých aktivit, mezi nejčastější patří: společný výzkum a networking, ovlivňování politik, obchodní spolupráce, vzdělávání a školení, inovace a technologie , expanze klastru. Klastr má většinou více než jeden cíl a některé cíle se navzájem prolínají. Rozeznáváme dva základní typy klastrů (Sölvell, 2003):

- klastry založené na hodnotovém řetězci,
- klastry založené na kompetencích.

Někteří autoři také uvádějí členění na klastry horizontální, vertikální a laterální.

Mezi vyspělými zeměmi, jež pozvolna ztrácejí konkurenční výhody, hraje důležitou roli sofistikovanost (vyspělost) podnikatelských aktivit, které jsou utvářeny jednak celkovým národním podnikatelským prostředím, a také kvalitou jednotlivých podnikových operací a strategií. Jako pozitivní se proto hodnotí množství kvality regionálně blízkých dodavatelů a rozsah jejich vzájemných vazeb. Pokud dochází v daném regionu k většímu propojení mezi subjekty z různých sektorů ekonomiky i společnosti, hovoří se o vzniku tzv. „klastrů“.

Samotná existence klastrů příznivě ovlivňuje konkurenceschopnost podniků a ekonomickou úroveň regionu, případně země, a to díky růstu produktivity, k němuž dochází prostřednictvím jednoduššího přístupu ke specializovaným dodavatelům, znalostem a informacím. Prostřednictvím klastrů může být rozšířena také inovační základna. Vzhledem k tomu, že jsou v rámci klastru lokálně dostupnější zkušenější pracovníci, celkové potřebné zdroje a specializované služby, existují předpoklady pro vznik dalších podnikatelských formací, jejichž cílem je hlubší spolupráce při informacích a dalším rozvoji klastru (Lopez-Claros, 2005, s. 27).

Součástí klastru jsou často také univerzity, které mají v takovém zapojení lepší přehled o potřebách průmyslu či daného odvětví, což poté promítají do zaměření své vzdělávací a výzkumné činnosti. Efektivita vynaložených finančních prostředků z veřejných i soukromých zdrojů je tak vyšší, než když je činnost vzdělávacích a výzkumných institucí realizována izolovaně. Slabou stránkou řady evropských ekonomik je nedostatečné financování odborného vzdělávání a výzkumu ze soukromých zdrojů a také nedostatečně rozvinutá schopnost uvádět nové poznatky do praxe, tj. inovace. Obojí může být zlepšeno existenci klastru, v jehož rámci dochází k lokálnímu zapojení a spolupráci s univerzitami.

Vědecký výzkum tak může být v rámci klastru o mnoho efektivnější, než když je realizován bez potřebných vstupních motivů a zpětné vazby a také zainteresovanosti soukromých subjektů na jeho výsledcích. Navíc pro národní vlády může být klastr využit při finanční podpoře výzkumu a vývoje jak na straně soukromých společností, tak i v rámci univerzit. V zemích střední a východní Evropy však nejsou v praxi vztahy mezi soukromým sektorem a univerzitami adekvátně rozvinuty. Nové členské země EU například zaostávaly v roce 2007 v počtu zaregistrovaných patentů na obyvatele (Rada pro výzkum a vývoj ČR, 2008, s. 92 – 102).

Význam Klastrů stále jasně roste v období prohlubujícího se procesu Globalizace světové ekonomiky, která vyvolává na jednotlivé ekonomiky unifikační tlak. Země se totiž odlišují rozdílnou úrovní specializace, konkurenceschopnosti a dynamiky průmyslového rozvoje. V podmínkách, kdy dochází k napodobování úspěšných podnikatelských aktivit ze strany konkurence, mohou klastry uchovat regionální (a tím i národní) specifika, a to prostřednictvím vyšší konkurenceschopnosti klastrově organizovaných odvětví a funkčních průmyslových klastrů.

Předpoklady pro úspěšné rozvinutí klastrů jsou především čtyři důležité předpoklady pro úspěšné rozvinutí efektů z činnosti klastrových iniciativ. Tyto faktory jednak souvisejí s dispozičními možnostmi pro vznik potenciální spolupráce mezi subjekty, které by se klastrové iniciativy mohly účastnit, ale také je důležitá kvalita potenciálních vazeb (např. co do charakteru spolupráce a zapojení jednotlivých subjektů). Hodnotí se tak již zmíněné množství a kvalita lokálních dodavatelů, dále dostupnost lokálních zdrojů (výrobních faktorů) a dostupnost místních služeb v oblasti výzkumu a vývoje, které by mohly být v rámci klastru využity (Abrhám, 2006, s. 237).

2.3.1 Výhody členství v klastru

V České republice jsou klastry novou záležitostí, firmy v zahraničí už s nimi ale mají bohaté zkušenosti. V našich podmínkách chybí dostatečně silné a výkonné informační zázemí, a zejména pak metodika (znalosti) jeho efektivního využívání jak pro identifikace subjektů vhodných pro vytváření klastrů, tak pro jejich další rozvoj, resp. pro udržení a rozvíjení jejich specifické konkurenční výhody.

Úspěšné klastry nabízejí zúčastněným společnostem mnoho konkrétních přínosů. Tyto přínosy se odráží především v růstu efektivity, produktivity, inovačních aktivit a tím do zvyšování konkurenceschopnosti. Klastr ovlivňuje konkurenceschopnost tím, že vytváří podmínky pro lepší využití vstupů, mobilizuje firmy k náročnější strategii, spoluvytváří podnikatelské prostředí a ovlivňuje hospodářskou politiku. Členové klastru sdílejí chápání konkurenceschopnosti jako výsledku produktivity a inovací. Klastry ovlivňují konkurenceschopnost třemi významnými způsoby:

- zvyšováním produktivity vlastních firem nebo celého odvětví,
- zvyšováním kapacity vlastních firem pro inovace a tudíž pro růst produktivity,
- stimulací vzniku nových podnikatelských subjektů podporujících inovace rozšiřujících klastr.

Člen klastru má usnadněnou cestu k zvyšování produktivity tím, že uvnitř klastru získává:

- přístup ke specializovaným vstupům a pracovním silám, což pomáhá snižovat transakční náklady,
- přístup k optimalizaci dodavatelského řetězce,
- přístup k informacím,
- přehled o možnostech doplňkových aktivit chybějících v klastru s cílem zvýšení přidané hodnoty produktu,
- možnost sdílení nákladů a investic,
- přístup k institucím a veřejným zdrojům,
- možnost porovnání vlastní výkonnosti s jinými v klastru – benchmarking.

Na základě dostupných zdrojů (CzechInvest, 2007) lze mezi přínosy klastru zařadit:

- Úspory z rozsahu a snížení nákladů – klastr poskytuje podnikům příležitost dosáhnout kritického množství v klíčových oblastech, což jim přináší úspěch, který nebyl možný, kdyby pracovaly izolovaně. Klastr může vytvářet zájmové skupiny a iniciovat kooperační projekty s cílem dosažení synergických a nákladově úsporných efektů. Přítomnost firmy v klastru ve svém důsledku snižuje podnikatelské náklady, ať už jde o zorganizování společných nákupů, společného marketingu, společného výzkumcově-vývojového projektu, společné logistiky nebo společné výchovy nových pracovních sil, což vytváří prostor pro zvyšování produktivity.

- Zisk nových zákazníků a otevření trhů – noví zákazníci pohlížejí na klastr jako na místo, kde mohou nalézt o vyšší kvalitě a konkurenčních cenách, a to všechno pohodlně na jednom místě. Členství v klastru umožňuje získávání větších zakázek, na které by samostatné podniky nedosáhly. To vše přináší vyšší tržby, zisk nebo marži.

- Lepší dostupnost kvalifikované pracovní síly – klastry často rostou díky dostupnosti kvalifikované a specializované pracovní síle v dané lokalitě. Existence větší zásoby pracovní síly snižuje náklady firem na hledání nových zaměstnanců. Konkurence pracovní síly udržuje nízké mzdy a přitom se dělníci neustále jeden od druhého učí a zvyšují tím své dovednosti.

- Zvýšení specializace – klastr může sdružovat firmy z různých článků hodnotového řetězce. Umožňuje jim spolupracovat při konkurenci proti větším, vertikálně propojeným firmám. Současně s tím, jak jsou firmy přitahovány do klastru, snaží se navzájem odlišovat pomocí specializace, vyráběním různých součástek či přebíráním role poskytovatelů služeb.

- Lepší dostupnost vstupů a subdodavatelů – velký počet specializovaných dodavatelů a poskytovatelů služeb přináší místním firmám významné přínosy jako konkurenční vstupní ceny, rychlé dodávky, snížení zásob a s tím související snížení nákladů. Zapojení do klastru současně zlepšuje vyjednávací sílu při nákupu (odběr ve velkém, slevy, apod.) i vyjednávací sílu při prodeji.

- Lepší přístup k informacím a vyšší rychlost jejich přenosu – tento přínos nastává v důsledku blízkosti firem, silných vazeb mezi nimi a vysokou konkurenční podstatou klastru. Přínos informací umožňuje snazší a rychlejší přístup ke znalostem a novým nápadům, což podporuje inovační aktivity. Firmy se od sebe navzájem či od podpůrných institucí učí, a to jim umožňuje jejich zdokonalování a větší konkurenceschopnost vůči okolnímu světu. Rychlý tok informací také snižuje transakční náklady.

- Zvýšení inovačního potenciálu – vzájemná rivalita firem uvnitř klastru podporuje ve firmách inovace, pomocí kterých se snaží zlepšit efektivitu a konkurenceschopnost. Cílem podpory inovací v klastru je rozvoj výrobků s vyšší přidanou hodnotou. Stálým kontaktem mezi sebou navzájem se firmy rychle dozvídají o vyvíjející se technologii, dostupných součástkách a strojích, nových službách a marketingových koncepcích. Do inovací se může zapojovat společně více firem a sdílet tak náklady na vývoj nových výrobků a technologií. Vytváří se silné vazby firem s vědci, výzkumníky a vývojovými pracovníky, dochází k vzájemné inspiraci a k efektu „přelévání“ (spillover).

- Zvýšení image firmy a lepší možnosti propagace – konkrétní přidanou hodnotu členům klastru přináší jak budování společné identity firem v klastru, tak i různé formy propagace: akce v rámci Public Relations, médií, internetu, zpracování prezentačních materiálů a publikací. Marketing klastru je tudíž pevně spojen s užitkem každého člena, přičemž o náklady na tuto činnost se dělí s ostatními. Zvláště u menších firem takto člen dosáhne na mezinárodní veletrhy, zahraniční prezentace, odvětvové akce, apod. v míře, kterou by sám nemohl finančně, organizačně ani materiálně zvládnout.

- Získání nových investorů – významným cílem marketingu klastru a potažmo daného regionu je i přilákání zahraničního investora, který by byl právě tím náročným odběratelem vyžadujícím kvalitu, inovace a vzdělávání a umožňujícím tak další rozvoj místních dodavatelů.

- Větší moc a hlas menších firem – pomocí networkingu jsou menší firmy schopny ovlivňovat události a lobovat u vlády za zlepšení služeb a infrastruktury. Znalost problémů a potřeb firem v klastru umožní prosazování společných

zájmů členů klastru u místních, regionálních a státních orgánů. Klastr umožňuje také posilovat hospodářskou spolupráci mezi veřejnými institucemi, státní správou a samosprávou, politickou a hospodářskou sférou. V neposlední řadě může klastr ovlivňovat vznik nebo zdokonalení státního nebo regionálního modelu podpory průmyslových klastrů.

- Vliv na vládu v oblasti investic do specializované infrastruktury – díky viditelnosti klastru, jakož i díky nákladové efektivitě a vyšší návratnosti investic, které představuje klastr, jsou tyto investice snadněji zdůvodnitelné. Specializovaná infrastruktura by mohla zahrnovat zřízení školicích středisek, technologických institutů, vládou podporovaného výzkumu a vývoje či zajištění nákladného výrobního zařízení potřebného pro místní průmysl. Vedení klastru úzce spolupracuje s regionálními vedoucími institucemi a společně vytvářejí prostor pro celou škálu podpůrných aktivit ve prospěch rozvoje klastru.

- Spolupráci se vzdělávacími institucemi – viditelnost a důležitost klastru může také podnítit reakci akademických institucí. Agregované potřeby klastru v profesní oblasti mohou ovlivňovat vzdělávací instituce od učňovského přes střední a vysoké školství včetně rekvalifikačních kurzů k přesměrování vyučovacích oborů na chybějící nebo zcela nové profese.

2.3.2 Prvky klastru

Struktura klastru je většinou tvořena těmito subjekty:

- jádro klastru – v jádru klastru jsou podniky, které jsou jeho vedoucími účastníky. Většina jejich příjmů pochází od zákazníků mimo klastr,
- podpůrné podniky – existují podniky, které přímo či nepřímo podporují podniky v jádru klastru. Nejčastěji se jedná o dodavatele specializovaných strojů, součástek, surovin a subdodavatele, kterým mohou výrobci přidělit jednotlivé úkoly,
- měkká podpůrná infrastruktura – ve vysoce výkonných klastrech nejsou podniky v jádru a podpůrné podniky izolovány. Především jde o angažovanost celé komunity. Místní školy, univerzity, polytechniky, místní obchodní a profesní asociace, agentury pro ekonomický rozvoj a další instituce podporují jejich aktivity a jsou zásadními složkami vysoce výkonného klastru. Kvalita měkké

infrastruktury a rozsah týmové práce v ní jsou velmi důležité faktory pro rozvoj jakéhokoliv klastru,

- tvrdá podpůrná infrastruktura – je posledním prvkem klastru. Jedná se především o silniční komunikace, přístavy, nakládání s odpady, komunikační spojení atd. Kvalita této infrastruktury musí minimálně dosahovat stejné kvality jako u konkurenčních klastrů, ať místních či vzdálených.

2.4 Konkurenceschopnost a globalizace

Konkurenceschopnost je v současném globalizovaném světě jednou z nejsledovanějších charakteristik národních ekonomik. Zájem o tuto ekonomickou veličinu ze strany akademických pracovníků, politiků a zástupců podnikového sektoru se začal rozvíjet především od 80. let 20. století, což bylo vyvoláno důsledky vývoje 70. let spjatých se strukturálními krizemi a růstem nové konkurence ve světové ekonomice. Otázka teoretického zachycení konkurenceschopnosti na makroekonomické úrovni se tak do centra pozornosti dostává až v souvislosti s rozvojem globalizačních procesů ve světové ekonomice, a to vzhledem k silnému nárůstu konkurence mezi jednotlivými zeměmi, resp. světovými ekonomickými centry. Tento proces je zvláště spojen s úspěšným nástupem asijských zemí. V oblasti výzkumu se pozornost rovněž zaměřila především na vazbu mezi mezinárodní konkurenceschopností a ekonomickým růstem či životní úrovní obyvatel.

Základní otázkou, která v souvislosti s měřením konkurenceschopnosti na úrovni států vyvstává, je, zda má vůbec smysl posuzovat soutěž a konkurenci mezi národy. Odpověď lze odvodit na základě logiky otevřených konkurenčních světových trhů, které byly zformovány na základě zkušeností z období velké hospodářské recese a multilaterálního či regionálního institucionálního rámce vzniklého po 2. světové válce. Mohutný rozvoj globalizace v podobě rozvinuté od 80. let 20. století přiměl k posuzování a ve většině případů k rozvíjení atraktivnosti daného prostředí pro domácí i zahraniční subjekty, které prostřednictvím svých aktivit generují ekonomický blahobyt.

Definice konkurenceschopnosti se v ekonomické literatuře liší. Přestože neexistuje jednotný výklad tohoto pojmu, lze vysledovat několik úhlů pohledu na tento termín. V nejužším pojetí je možné konkurenceschopnost chápat jako komparativní pohled na zkoumaný subjekt a jeho schopnost (statický přístup) či výkonnost (dynamický přístup) prodávat a nabízet zboží či službu na daném trhu (takovém, kde dochází ke konkurenčnímu střetu, tj. může jít jak o domácí, tak i zahraniční trh).

V této koncepci je pozornost věnována zvláště vnějším aspektům výkonnosti země či regionu. Základem jsou především cenově-nákladové a kvalitativní faktory, které ovlivňují exportní výkonnost ekonomiky. Cílem těchto přístupů pak je rozšířit nebo zachovat tržní podíl dané země na mezinárodních trzích. Takovou mezinárodní konkurenceschopnost je možné vnímat jako schopnost proniknout se svým zbožím (případně službami) na zahraniční trhy a z takové mezinárodní směny získávat komparativní výhody (Kubišta, 1999, s. 316). Problematické jsou však v tomto pojetí praktické příklady např. americké ekonomiky, která v některých ukazatelích své vnější ekonomické pozice nedosahuje relativně dobrých výsledků a zároveň je tato země celkově hodnocena jako vysoce konkurenceschopná.

Další přístup, z něhož například vychází Organizace pro hospodářskou spolupráci a rozvoj (OECD), se týká produktivity pracovníků dané země. Její výše může být ovlivněna jednak kapitálovou vybaveností a mírou vzdělání pracovníků, ale také nedostatečnou efektivitou výroby (Causa, 2004, s. 8). Úroveň celkové produktivity hraje poté důležitou roli pro životní úroveň obyvatel, neboť je jednou z determinant příjmů ve společnosti. Definice konkurenceschopnosti OECD je vymezena jako schopnost korporací, odvětví, regionů, národů a nadnárodních celků generovat vysokou úroveň příjmů z výrobních faktorů i relativně vysokou úroveň jejich využití, a to za podmínek, kdy jejich prostřednictvím vyprodukované zboží a služby obstály v testu mezinárodní konkurence na trzích, kde panují podmínky volného obchodu a rovných tržních podmínek (Garelli, 2008). V tomto vymezení již lze vysledovat přesah na širší pojetí konkurenceschopnosti, které je rozebráno níže.

Nutno poznamenat, že pohled na konkurenceschopnost založený na schopnosti zkoumaného subjektu uspět na trhu, kde se v soutěži střetává s jinými konkurenty (i ze zahraničí), souvisí se zmíněným hodnocením dle produktivity práce. Jde o teorie komparativních výhod analyzující úspěch zemí, které se rozhodnou obchodovat v mezinárodním prostředí. Model komparativních výhod se rozvíjí mezi subjekty, které jsou strukturálně odlišné a které se liší mírou vybavenosti výrobními faktory. Pokud jsou splněny předpoklady klasického modelu komparativních výhod, je rozdílná úroveň produktivity práce determinantou úspěchu jednotlivých zemí.

Existují také širší pojetí konkurenceschopnosti, jež jsou pojmenovávána jako agregátní či víceúrovňová – zohledňují i další faktory, které mají vliv na klíčové ekonomické veličiny. Provedená analýza se tak zaměřuje na ty činitele (zdroje konkurenceschopnosti), které předurčují úspěšné postavení národních ekonomik. Cílem pak je dosahovat příznivých hodnot celkového produktu (či spíše jeho růstu),

zaměstnanosti, životní úrovně. Ve svém základě tento přístup zdůrazňuje roli produktivity, jejíž vývoj ovlivňuje již zmíněné makroekonomické indikátory. Vzhledem k míře otevřenosti ekonomik se v soudobé literatuře obě pojetí víceméně spojují, a to vzhledem k vlivu vnějších konkurenceschopností (v pozitivním i negativním smyslu) na makroekonomické agregáty (Beneš, 2006, s. 15).

Významným teoretickým základem výzkumu konkurenceschopnosti je přístup, který rozvinuli Michael Porter. V jeho pojetí je pro pochopení konkurenceschopnosti důležité poznat její zdroje. Skutečná konkurenceschopnost je opět měřena prostřednictvím produktivity, protože ta umožňuje růst životní úrovně, mezd, nebo má vliv na měnový kurz, výnosnost kapitálu apod. Nejčastějším cílem politik založených na tomto pojetí je pak vysoké tempo ekonomického růstu (růstové teorie), růst příjmů obyvatelstva, vysoká míra využití výrobních faktorů, především lidského kapitálu v podobě míry zaměstnanosti. Pozornost je rovněž věnována rozvoji v rámci regionu, např. pomocí klastrových iniciativ. Těmito cíli je spjat také evropský integrační proces v rámci politiky konkurenceschopnosti.

Posledním teoretickým východiskem, které vychází z Porterovy teorie, je koncept, jenž dává do souvislosti fáze ekonomického rozvoje a zdroje konkurenční výhody. První stadium je tzv. faktorové tažené. Další dvě jsou spjaty s kvalitativními aspekty konkurenceschopnosti – založené na efektivnosti a inovacích. V některých pojetích bývá z poslední fáze vydělován nový specifický typ konkurenční výhody, který je založen na kreativitě. Tento koncept tak vnímá konkurenceschopnost nikoliv pouze odvozenou od vývoje měnového kurzu jakožto zdroje možné cenové konkurenční výhody, ale jde i o další faktory, politiky a instituce, jenž příznivě ovlivňuje prosperitu dané země.

Významnou institucí, která se problémem konkurenceschopnosti v jejím širším chápání zabývá, je Světové ekonomické fórum (World Economic Forum, WEF). Její definice vychází z vícekriteriálního přístupu, v jehož rámci jsou hodnoceny vedle měřitelných také kvalitativní data získaná z dotazníkových šetření. Tato metoda je společná pro frekventovaná a populární hodnocení nejen Světového ekonomického fóra, ale také Mezinárodního institutu pro manažerskou průpravu (International Institute for Management Development, IMD). Podobná metodika je dána tím, že obě instituce původně vydávaly od roku 1979 společný hodnotící žebříček. Od konce 80. let 20. století však jde každá z institucí vlastní cestou.

Hodnocení obou institucí se i přes podobný základ výpočtu konkurenční pozice dané země liší v těžišti chápání termínu konkurenceschopnost. Zatímco IMD ji hodnotí

více jako sílu obstát při tržním střetu (s odpovídající mírou jak zisku pro podnikatelský sektor, tak i prosperity pro obyvatele) WEF ji posuzuje více jako schopnost dosahovat hospodářského růstu (Jirásek, 2001, s. 43). V roce 2005 změnilo Světové ekonomické fórum metodologii a konkurenceschopnost země nově hodnotí nakolik soubor rozličných faktorů, politik a institucí příznivě ovlivňuje produktivitu dané země a tím i zprostředkovaně prosperitu (Lopez-Claros, 2005, s. 23).

Výhodou obou konceptů je především komplexnost, jejímž prostřednictvím jsou hodnocení a na jejich základě výsledky získávány. Rovněž teoretické zázemí umožňuje vnášení nových názorů a poznání z akademické sféry. Zaznívají však také kritické hlasy, jež se dotýkají především metodologické části – jednak ke způsobu získávání části dat (zejména těch tzv. měkkých zjišťovaných ze šetření mezi zástupci businessu), ale také charakteru posuzovaných dat a k tomu, jaký význam je jim přidělován. Někteří autoři rovněž přirovnávají tento koncept konkurenceschopnosti spíše k posuzování atraktivity dané země pro zahraniční investory. Svůj kritický postoj opírají o tezi oportunistického chování zainteresovaných subjektů, jejichž názor se promítá do měkkých dat, a nemusí tak být prospěšný pro obyvatele a daný stát, který je centrem těchto hodnocení.

Role státu v ekonomice je při posuzování konkurenceschopnosti na úrovni zemí či národů hodně často analyzována. Tlak na vládní politiky je vytvářen zvláště v souvislosti s procesem globalizace a technologického pokroku, jež ztěžují realizaci vládních politik v jejich tradiční podobě (regulace, rozvoj infrastruktury – sociální, zdanění atd.) Větší nároky na chování a politiku vlád vyplývají především z větší mobility kapitálu a dematerializace ekonomických hodnot a transakcí vycházejících z technologického pokroku. Proto se uvádí v případě konkurenčních výhod přechod od hmatatelných faktorů k nehmotným, jako jsou znalosti, vzdělání, nové technologie, nehmotné statky. Technologický rozvoj ovšem vytváří pro společnost (a tím i pro státní úřad) nová rizika spjatá s větší zranitelností (např. ze strany hackerů).

Stát tak není posuzován, zda je jeho role v ekonomice větší či menší (pokud jde o míru zdanění, vlivu na vzdělání a zdravotní systém), ale spíše jak se vyrovnává s novými výzvami v oblasti bezpečnosti (národní, technologické, energetické), imigrace, ochrany životního prostředí či obecně charakteru regulace a součinnosti s různými úrovněmi vládnutí. V současné době se tak začínají opět zdůrazňovat takové funkce státu, které mají vliv na zajištění efektivního a transparentního fungování ekonomiky a všech jejích subjektů, zejména v oblasti finančního trhu. Ve svých tradičních rolích dokonce některé vlády mění svou roli, což se promítá do privatizace vybraných sítí

(telekomunikačních, energetických, dopravních), jež přecházejí do soukromých rukou a stát nově plní roli garanta integrity (Garelli, 2008).

Dalším pojetím posuzování vládní politiky ve vazbě na míru konkurenceschopnosti soukromé sféry jsou přístupy zdůrazňující ekonomickou svobodu a minimální roli státu. Vycházejí z liberálních ekonomických konceptů, které akceptují nezastupitelnou roli jedince či soukromého sektoru při rozhodování o ekonomické aktivitě a využití výrobních faktorů. Vládní politika je v tomto rámci posuzována, nakolik podporuje tuto ekonomickou svobodu, což se promítá do preference minimální míry regulace (např. v oblasti podnikání, obchodu, fungování trhu výrobních faktorů), zajištění bezpečnosti vlastnických práv atd.

2.4.1 Multikriteriální přístupy

Příkladem širších pojetí konkurenceschopnosti jsou tzv. multikriteriální metody (Steinmetzová, 2008, str. 36-37) měřící konkurenceschopnost z různých úhlů pohledu. Jejich základní charakteristikou je způsob, jakým hodnotí vybraný subjekt. Zdroje konkurenceschopnosti jsou měřeny dvěma základními soubory informací. První skupinu tvoří tzv. tvrdá, měřitelná data, která jsou získávána z mezinárodních činorodých statistik. Naopak druhá skupina tzv. měkkých dat představuje komplex evaluací, které se sice nedají přesně změřit, ale dají se ocenit s pomocí dotazníkových šetření, jejichž respondenty jsou zástupci vrcholového managementu společností, které působí v hodnocené zemi. Na jedné straně s pomocí tohoto typu informací je možné zhodnotit i charakteristiky ekonomik, jež nelze postihnout statistickými „tvrdými“ veličinami, ale zároveň tyto údaje vypovídají o subjektivním pohledu vybraných odborníků.

Nevýhodou multikriteriálních hodnocení s vysokým podílem měkkých dat je značná míra subjektivity. Respondenti často vyjadřují osobní přání, dojmy, optimistická, nebo naopak pesimistická očekávání dalšího vývoje dané ekonomiky. Výsledný obrázek hodnocené země může být odlišný od reality. Pokud navíc respondenti hodnotí pouze danou zemi, chybí při jejich posuzování možnost mezinárodního srovnání. Na druhou stranu ale tyto žebříčky vypovídají o tom, jak vrcholoví manažeři sami vnímají národní prostředí, v němž působí. Tato hodnocení tak mohou odrážet např. pohled globálních investorů, kteří se rozhodují, kde mají nakupovat své zdroje, kde mají rozvíjet činnost. Tyto faktory se následně promítají i do ekonomického růstu a růstu zaměstnanosti dané země. O subjektivním hodnocení vypovídají odlišné výsledky jednotlivých zemí mezi vybranými institucemi, které šetření provádějí (Steinmetzová, 2008).

Již zmíněnou společností, která multikriteriální hodnocení analyzuje a zveřejňuje je Světové ekonomické fórum. Faktory, které mají dle jejího konceptu významný vliv na

úspěšné konkurenční postavení, je možné rozčlenit do několika skupin. V jejich rámci bylo detailně rozpracováno 12 pilířů, jež se příznivě promítají do konkurenceschopnosti dané země (Lopez-Claros, 2007) a které obsahují desítky měřených či statistických (dotazníkově) zjišťovaných indikátorů:

1. institucionální rámec,
2. infrastruktura,
3. makroekonomická stabilita,
4. kvalita zdraví a základní vzdělání obyvatelstva,
5. vyšší stupeň vzdělání a systém dalšího vzdělání,
6. efektivita trhu zboží,
7. efektivita trhu práce,
8. efektivita (vyspělosti) finančního trhu,
9. technologická připravenost (přijímat a využívat nové technologie),
10. velikost trhu (domácího i zahraničního),
11. vyspělost podnikatelského sektoru,
12. inovace.

Jak již bylo uvedeno výše, jde tedy o soubor základních faktorů, politik a institucí, které mají vliv na úroveň produktivity dané země, a každý z nich je poté dále rozčleněn a zpracováván (Porter, 2008). Proč jsou důležité právě tyto zdroje pro dosažení stanoveného cíle či prostředí, které má příznivý vliv na faktorovou produktivitu dané země?

První pilíř je chápán jako rámec, který formuje prostředí, v němž působí jednotlivci, firmy a vládní sektor. Institucionální rámec hraje důležitou roli díky svému vlivu na efekty rozvojových strategií a politik (rozdělení jejich přínosů a nákladů). Ovlivňuje rovněž samotné investiční rozhodování a organizaci výroby. Příkladem může být ochrana vlastnických práv. V případě, že není zabezpečena, klesá ochota vlastníků kapitálu či jiných výrobních zdrojů je v dané zemi použít či rozvíjet. Dalším příkladem slabého institucionálního rámce, který má nedbalý vliv na fungování firem (např. tím, že zvyšuje jejich náklady) je nepřiměřená byrokracie, nadměrná regulace podnikatelské činnosti, korupce, nečestné praktiky v zadávání a výběru veřejných zakázek, nedostatečná transparentnost a důvěryhodnost činnosti veřejných institucí, závislost soudní moci na politicích. Na druhé straně ovlivňují obyvatelé a podniková sféra kvalitu institucí prostřednictvím svých volebních zástupců a odvodem daní.

Zároveň se v posledních letech ukazuje rovněž vedle kvality veřejných institucí také význam odpovědného chování soukromých subjektů. Příkazem slabin institucionálního rámce ve vazbě na činnost soukromého sektoru mohou být skandály ve falšování účetních záznamů, nedostatky v kontrole účetnictví externími firmami, podvody či jiná selhání manažerů, která podlomila důvěru ze strany investorů a spotřebitelů. Z tohoto důvodu se klade rovněž velký důraz na transparentnost ve fungování soukromého sektoru v podobě jasných standardů v oblasti auditu, vedení účetnictví či včasnému přístupu k relevantním informacím.

Dále se hodnotí kvalita infrastruktury, která je vnímána jako část národohospodářského odvětví, které umožňuje rozvoj ekonomiky. Většinou jde o poměrně široký soubor zahrnující infrastrukturu jak fyzickou (např. doprava, energetika), tak i sociální (školství, zdravotnictví). Ovšem v rámci WEF je ve 2. pilíři posuzována pouze její fyzická část, neboť je chápána jako faktor, jež umožňuje propojení jednotlivých částí hospodářství, ať již uvnitř země (tj. mezi jednotlivými regiony), tak i navenek – vůči jiným zemím či regionům. Pozornost je proto směřována na hodnocení dopravní, komunikační a energetické infrastruktury, jejíž kvalita má vliv na výši produktivity a flexibility firemního sektoru.

Třetím základním faktorem konkurenceschopnosti je *makroekonomická stabilita*. Přestože mezi ní a úrovní produktivity neexistuje přímá vazba, nezdravé makroekonomické prostředí poškozuje hospodářství jako celek a ztěžuje firmám jejich rozhodování (např. kvůli vysoké míře inflace). Zároveň míra zadlužení spjatá s vyššími platbami za úroky pozvolna čím dál více svazuje vládě ruce při realizaci efektivní a účinné rozpočtové politiky.

Posledním základním pilířem je dostupná zdravá a minimálně vzdělaná pracovní síla, která je jedním ze základních výrobních faktorů a nositelů produktivity. V tomto rámci se posuzují dva základní aspekty: dostupnost a kvalita zdravotní péče a podíl populace s ukončeným základním vzděláním na odpovídající kvalitativní úrovni. Oba uvedené faktory jsou základní determinantou úrovně produktivity jednotlivých pracovníků. Na druhé straně nejnižší úroveň vzdělání sice umožňuje zapojení do základních manuálních prací, je ale nedostatečná pro firmy, které hodlají produkovat výrobky s vyšším stupněm přidané hodnoty nebo v pokročilejších fázích výrobního řetězce.

Prvním, kvalitativně vyšším kompetitivním faktorem, je kvalita vyššího (sekundárního a terciárního) vzdělávání a systému (celoživotního) školení, či vzdělávání, jde o požadavky vyplývající z měnícího se vnějšího okolí, které prostřednictvím efektu

globalizace vytvářejí vyšší nároky na flexibilitu firem i jejich zaměstnanců. Záleží ovšem také na reálné kvalitě znalostí získaných na této úrovni vzdělání. Proto se hodnotí, nakolik jsou získané dovednosti ceněné soukromým sektorem. Vyšší podíl lidí se středním a vysokoškolským vzděláním spolu s rozvinutým systémem průběžného školení v rámci zaměstnání je předpokladem pro lepší schopnost pracovníků a firem se snadněji přizpůsobovat měnícím se globálním ekonomickým podmínkám.

I vysoce produktivní pracovní síly ovšem nemusejí automaticky znamenat, že jejich zaměstnavatelé (potažmo celá společnost) budou prosperovat. Proto je důležité hodnotit, jak fungují trhy, na nichž se s hotovou produkcí obchoduje. Efektivně fungující komoditní trhy zaručují, že je vyráběn správný mix hodnotných výrobků a služeb jednak na základě interakce nabídky a poptávky, ale také ve vazbě na vysokou výrobní produktivitu. V praxi to znamená, že nepokřivené tržní vztahy vedou k tomu, že uspějí pouze ty společnosti, které jsou nejvíce efektivní. Reálně tak mohou konkurenceschopnost snižovat daně, které zkreslují efektivnostní vlastnosti firem nebo je neúměrně nákladově zatěžují, nebo také restriktivní či diskriminační omezení vlastnictví výrobních faktorů pro zahraniční subjekty. Sociokulturní odlišnosti mezi jednotlivými zeměmi mohou rovněž ovlivnit fungování komoditivních trhů na straně poptávky. Na některých trzích se například spotřebitelé tolik nepoptávají na nových high-tech výrobcích, což snižuje tlak na inovativní přístup firem.

V obdobném duchu je hodnocena funkčnost trhů výrobních faktorů – pracovního finančního trhu. Jejich základní příspěvek ke konkurenceschopnosti jednotlivých zemí spočívá v pokud možno co nejvíce efektivní alokaci práce či kapitálu do jejich konkrétního využití. Trhy práce by proto měly vykazovat vysokou flexibilitu při usměrňování pracovníků mezi jednotlivými firmami, sektory, regiony, případně zeměmi, resp. jejich zapojení do ekonomické aktivity v regionálním či sektorovém měřítku. Pro řadu zemí spjatých s realizací solidaristických ekonomicko-sociálních modelů je velmi citlivá další charakteristika efektivních pracovních trhů, a to pružnost mezd, jež mnohdy vykazuje značnou rigiditu. Efektivní trhy práce by měly svým účastníkům zprostředkovávat dostatečné stimuly, které mají vliv na jejich ekonomickou aktivitu. Rovněž by neměly obsahovat bariéry pro firmy při získávání talentované pracovní síly. Pozitivní vliv efektivně fungujícího pracovního trhu (s konkurenčními vztahy na straně poptávky i nabídky) na konkurenceschopnost je tak patrný – pracovní síla je alokována tam, kde nachází svého nejlepšího uplatnění a je odměněna na rovnovážné úrovni dle svých kvalit, znalostí a dovedností.

Kvalita finančního trhu se hodnotí kvůli svému rozhodujícímu vlivu na produktivitu. Finanční trh je často označován za životně důležitý krevní oběh každého hospodářství. Měl by umožňovat efektivní transformaci domácích i zahraničních úspor do investičních akcí. Efektivita v tomto případě podobně jako na trhu práce znamená alokaci disponibilních finančních prostředků do těch projektů, které se jeví pro investory jako potenciálně nejvíce výnosné (atraktivní). Pro fungující finanční trh je nesmírně důležité, aby na něm byly k dispozici pravdivé relevantní informace nutné pro zhodnocení jednotlivých investičních alternativ dle míry jejich rizika (potažmo likvidity). V opačném případě může dojít k vážným strukturálním problémům finančního sektoru, které se ve velkém množství mohou přelít do závažných hospodářských problémů celé ekonomiky.

Nedostatečně rozvinutý finanční sektor je ovšem také brzdou ekonomického rozvoje, protože neumožňuje dostatečné financování podnikatelské činnosti. Nejde pouze přitom o zprostředkování vazby mezi střadateli a investory (příp. dlužníky), ale také mezi jednotlivými zprostředkujícími subjekty. Pokud dojde k přerušení toků mezi nimi (např. z důvodu poklesu důvěryhodnosti jednotlivých účastníků), nebo pokud jsou vazby mezi nimi neefektivní, má to neblahý vliv pro fungování celé ekonomiky. Rozvinuté a efektivní finanční trhy dále umožňují zprostředkovat vazby mezi subjekty v různých rizikových profilech. Díky tomu mohou získat finanční prostředky například začínající podnikatelé, kteří mají sice rizikovější, ovšem také potenciálně vysoce perspektivní a inovativní nápady.

Jednotlivé země (a zprostředkovaně i firmy v nich působící) se liší schopností pracovat s vyspělými technologiemi, čili dalšími aspekty, které mají vliv na úroveň produktivity vybraných sektorů. Tato tzv. technologická připravenost v sobě jednak obsahuje hodnocení, zda mají firmy z dané země přístup k vyspělým technologiím, a také nakolik s nimi dokážou pracovat. Jde především o oblast informačních a komunikačních technologií, které mají rozhodující vliv na produktivitu většiny národohospodářských sektorů a efektivitu obchodních transakcí. Zvláštní pozornost je v této oblasti věnována posouzení vyspělosti vlastní inovační základny dané země, což je rozebráno dále v textu.

Jedním z klasických teoretických přístupů, jenž posuzuje možnosti zvýšení celkové produktivity firem, je koncept úspor realizovaných z rozsahu. Čím vyšší velikost trhu, na němž firmy mohou působit, tím mají větší možnost odbytu pro svou produkci a využívat tak úspory z rozsahu. Tato koncepce je vzhledem ke globalizaci rozšířena o působnost v mezinárodním měřítku. Tradiční státní hranice vymezující

národní trhy byly prakticky eliminovány obchodní liberalizací vedoucí ke vzniku mezinárodních globálních trhů, které mohou nahradit ty původní, domácí. Současné teoretické práce zabývající se efekty liberalizace obchodu zdůrazňují příznivý vliv otevřených trhů na ekonomický růst a ekonomický rozvoj především malých států s omezeným domácím trhem.

Podnikatelská strategie je součástí informační strategie, skládající se z informačního sytému, informačních technologií a informačního managementu. Cílem každého podnikatelského subjektu je konkurenceschopnost. V následující kapitole se zaměříme na informační strategii ve veřejné správě, resp. na informační strategii Celní správy ČR. I když se nejedná o subjekt podnikatelský, má svou informační strategii, avšak s rozdílnými cíly. Informační systém Celní správy ČR slouží k podpoře výkonu kompetencí orgánů celní správy. Některé části tohoto IS proto spadají do kategorie informačních systémů veřejné správy. Obecným cílem CS v oblasti kvality ICT je splnit oprávněné požadavky zákazníků, tedy celních úředníků a deklarantské veřejnosti. K tomu se CS snaží dospět vyvíjením trvalého úsilí pro zajištění kvality:

- dat zpracovávaných v IS CS,
- služeb poskytovaných prostřednictvím IS CS,
- technických a programových prostředků používaných pro zpracování dat a poskytování služeb.

Zajištění kvality ve všech uvedených oblastech vyžaduje integrovaný procesní přístup, který umožňuje identifikaci a efektivní řízení vzájemně propojených entit a činností souvisejících s informačním uspokojováním požadavků zákazníka (a to od vzniku požadavku až po provoz systému).

Dlouhodobým cílem v oblasti bezpečnosti IS CS je zajištění bezpečnosti jeho aktiv podle ČSN ISO/IEC 27001, přičemž těmito aktivy jsou:

- data zpracovávaná v IS CS,
- služby poskytované prostřednictvím IS CS,
- technické a programové prostředky používané pro zpracování dat a poskytování služeb.

Koncepce bezpečnosti IS CS vychází ze znalosti kritických procesů, kritických aktiv a rizik IS CS. Z tohoto důvodu byly kritické procesy, kritická aktiva i rizika IS CS identifikována a musí podléhat pravidelné revizi a aktualizaci.

3 Informační strategie na příkladu Celní správy ČR

Každá organizace by měla mít vyvinutý systém strategií, které díky vzájemné provázanosti a synergickému efektu pomohou organizaci v dosahování stanovených cílů. V současné době je aktuálním problémem propojení konkurenční strategie postavené na klasickém managementu a znalostní strategii, která je výstupem moderních přístupů k vedení organizace ve znalostní ekonomice a znalostní společnosti. Tato provázanost má totiž vliv na globální podnikovou strategii. Ačkoliv je význam podnikové informační strategie zřejmý, není dosud bohužel zvykem, aby měla každá organizace explicitně definovanou informační strategii. Informační strategie organizace totiž dává smysl a cíl všem podnikovým aktivitám. Neexistence informační strategie vede k situaci, kdy se podnik vyvíjí nekoordinovaně a živelně. Čím déle tato situace trvá, tím silněji se zabudovávají její hodnoty, vzory a modely do organizační kultury, což následně způsobuje zdroj silné rezistence při snaze o prosazení jakékoliv změny. Není možné ovšem vycházet z předpokladu, že existence informační strategie a její prosazování automaticky zajistí úspěšnost podniku. Je zřejmé, že v situaci chybně definované podnikové strategie bude mít její prosazování spíše negativní dopad.

Česká celní správa, stejně jako celní správy ostatních států, má dva základní úkoly, kterými jsou ochrana a regulace domácího trhu formou výběru cla z dováženého zboží a dohled nad tím, aby toto zboží neohrožovalo životy nebo zdraví lidí, zvířat či rostlin. Vývoj ekonomické situace, včetně zahájení příprav na členství v EU, naléhavě vyžadoval, aby celní správa při plnění svých úkolů co nejvíce usnadňovala legální mezinárodní obchod. Tohoto cíle mohlo být dosaženo jen za pomoci modernizace celní správy, a to jak v oblasti celního řízení, tak i v oblasti technického vybavení, zejména celního informačního systému. Další významnou okolností, která výrazně předurčila současnou podobu české celní správy, byl vstup České republiky do Evropské unie. Z pohledu celní správy nešlo jen o samotný akt vstupu, ale o dlouholeté období sbližování celní legislativy a celních postupů s evropskými standardy. Navíc došlo v důsledku rozšíření EU ke zrušení pravidelných celních kontrol na pozemních hranicích České republiky a naopak celní správě přibyly nové úkoly, např. v oblasti společné zemědělské politiky nebo statistiky vnitrounijního obchodu. Významnou oblastí, jež celní správě pomáhá plnit úkoly v celé šíři její působnosti, je informatika (Celní správa ČR, 2009).

Dlouholetá vůle vedení zajistit pro výkon celní služby i ostatní související činnosti kvalitní a moderní vybavení informačními technologiemi sleduje především snahu zjednodušit celní řízení a poskytovat celní službu obchodní veřejnosti v nejvyšší možné rychlosti, kvalitě a dostupnosti. Základním předpokladem rozvoje informatiky

byla příprava a vlastní plnění úkolů v souvislosti se vstupem ČR do EU. Velké úsilí patřilo zejména řešením souvisejícím se sjednocením postupů v oblasti celního řízení a s komunikací se systémy spravovanými Evropskou komisí. Neméně podstatné bylo i rozvíjení systémů rizikových analýz, datové skladby i nových portálových řešení.

Základní úkoly v oblasti zajištění ochrany trhu a bezpečnosti mezinárodního obchodu jsou v zásadě všem celním správám společné. Mezinárodní obchod se vždy dotýká minimálně dvou a zpravidla více celních správ a každá z nich má kontrolu jen nad částí celé obchodní operace. Z toho důvodu je nezbytné, aby celní správy vzájemně úzce spolupracovaly, a to na základě mezinárodních smluv, které poskytují právní rámec pro výměnu informací, předávání dokumentů, vzájemnou pomoc při šetřeních týkajících se porušování celních předpisů, apod. Česká republika podepsala smlouvy o vzájemné pomoci v celních otázkách s více než dvaceti státy. V tomto ohledu nelze opominout ani další podstatnou skutečnost, že Celní správa České republiky patří k dlouholetým členům Světové celní organizace, což významnou měrou přispívá ke snazší komunikaci s ostatními celními správami po celém světě. Je samozřejmé, že nejužší spolupráce probíhá mezi celními správami Evropské unie, které společně zajišťují provádění dohledu nad jednotným celním územím Společenství na základě společné celní legislativy. Tato spolupráce je upravena právními předpisy EU a je rozšířena Úmluvou Neapol II a Úmluvou o celním informačním systému. Důležitým úkolem Evropské komise je zajistit, aby společné celní předpisy byly prováděny na celém území EU jednotně a pro všechny obchodní subjekty ve Společenství, které dovážejí nebo vyvážejí zboží, tak existovaly stejné podmínky.

3.1 Informační koncepce a systémy Celní správy ČR

Informační koncepce celní správy (dále IK) je pro správce Informačních systémů veřejné správy (ISVS) povinným dokumentem (vyhláška č. 529/2006 Sb.). Používá se pro dlouhodobé řízení ISVS. Služby informačních a komunikačních technologií (ICT) jsou poskytovány jak vlastním pracovníkům k podpoře jejich činností a rozhodování, tak veřejnosti k podpoře plnění zákonných povinností při registraci zboží v mezinárodním obchodě (celní řízení). Informační systémy Celní správy ČR, jsou nejčastěji využívány pro podporu celního a daňového řízení, tj. pro veškeré úkony spojené s registrací, kontrolou zboží v mezinárodním obchodě ČR a vybíráním povinných poplatků. Zabývají se tedy informační podporou rozhodování o zařazení zboží do navrhovaných celních režimů (a ukončováním takového zařazení) a podporou

registrace osob nakládajících se zbožím a účastnících se celního řízení (deklaranti, dovozci, vývozci, speditéři, přepravci = ekonomičtí operátoři).

Dále se zabývají podporou výběru cel a daní a konečně vyvozováním důsledků vůči osobám, které porušily příslušné zákonné normy. Tyto systémy musí přitom poskytovat služby ekonomickým operátorům, aby mohli své povinnosti plnit s co nejmenším vynaložením administrativních nákladů a času, pracovníkům celní správy – jak pracovníkům ve výkonu služby, tak vedoucím funkcionářům. Vybrané informace jsou, na základě příslušných norem, poskytovány dalším oprávněným orgánům státní správy a oprávněným orgánům Společenství. Řešení celní problematiky v informačním systému by mělo pokrývat potřeby společností obchodujících v rámci EU, které mají povinnost vykazovat data pro Intrastat, tak těch, jejichž oborem je obchod v zemích mimo EU, u kterých je nutné absolvovat celní řízení (Informační koncepce Celní správy ČR, 2009).

3.1.1 Pravidla bezpečné výměny dat informačního systému Celní správy ČR

Účelem této podkapitoly je stanovit síly, prostředky a způsob, resp. postupy bezpečné výměny dat informačního systému Celní správy ČR (ISCS) při respektování současného stavu ochrany datových přenosů uvnitř i vně ISCS, a to tak, aby byla zajištěna bezpečnost přenášených dat i souvisejících komunikačních prostředků a aby datové přenosy nebyly zdrojem bezpečnostních incidentů. Systém bezpečné výměny dat ISCS je jedním ze systémů ochrany ISCS a vychází z platných právních předpisů, usnesení vlády a norem ČSN.

Důležité je vymezit si následující základní pojmy:

- bezpečná výměna dat – takový přenos dat, při kterém je chráněna důvěrnost, integrita a dostupnost přenášených dat a s nimi spojené priority, např. nepopíratelnost,
- komunikační infrastruktura ISCS – komunikační prostředky ISCS,
- komunikační služba ISCS – jakákoliv služba poskytovaná uživateli ISCS prostřednictvím komunikačních prostředků, např. e-mail nebo vzdálený přístup,
- komunikační (přenosový) protokol – soubor zásad pro přenos dat,
- komunikační rozhraní ISCS – prvek komunikačního zařízení určený k logickému oddělení ISCS od přenosové cesty,
- komunikační zařízení ISCS – zařízení pro přenos dat v uzlech, mezi uzly i vně ISCS, zejména směrovače (routery) a datové přepínače,

- komunikační prostředky ISCS – komunikační zařízení, rozhraní, přenosové cesty, protokoly a služby využívané pro přenos dat v uzlech, mezi uzly i vně ISCS; tyto prostředky, které splňují stanovené bezpečnostní požadavky, jsou současně prostředky bezpečné výměny dat ISCS,
- přenosová cesta – komunikační linka nebo kanál mezi komunikačními rozhraními na straně odesilatele i příjemce zprávy.

Základním principem bezpečné výměny dat ISCS je omezení přístupu uživatelů ISCS ke komunikačním prostředkům, tj. ke komunikačním zařízením, rozhraním, přenosovým cestám, protokolům a službám, na nezbytnou míru odpovídající vykonávané činnosti, a dále zaznamenávání detailů chyb a činnosti uživatelů v auditním záznamu a analyzování zaznamenaných detailů, aby byla příslušným způsobem detekována a řešena narušení bezpečnosti ISCS. Výběr, instalace a konfigurace nově zaváděných komunikačních prostředků ISCS musí být předem prokazatelně autorizovány organizačním útvarem CS odpovědným za bezpečnou výměnu dat ISCS. Neautorizované komunikační prostředky nesmí být v ISCS instalovány ani používány. Musí být vedena provozní evidence autorizovaných komunikačních prostředků ISCS. K využívání komunikačních prostředků ISCS, zejména komunikačních služeb, musí být uživatelé ISCS autorizováni, a to v rámci systému řízení přístupu v ISCS. Stav a funkčnost komunikačních prostředků ISCS musejí být pravidelně anebo podle potřeby stanoveným způsobem dohlíženy a testovány. Zjištěné nedostatky musí být neprodleně napraveny. Zatížení a propustnost komunikačních prostředků ISCS musejí být pravidelně anebo podle potřeby stanoveným způsobem monitorovány a zjištěné nedostatky neprodleně napraveny.

3.1.2 Fyzická ochrana

Organizačním útvarem CS, odpovědným za bezpečnou výměnu dat ISCS, musí být zajištěno, že vymezené komunikační prostředky ISCS, zejména komunikační zařízení, rozhraní a související technologie (servery antivirové ochrany, autentizací servery pro vzdálený přístup, proxy servery apod.), budou umístěny v zabezpečených prostorách objektů CS. Fyzický přístup do zabezpečených prostor musí být, v působnosti provozovatelů subsystémů ISCS (subISCS), omezen na minimální nezbytný počet osob. O přístupu jiných osob, např. pracovníků údržby objektů, pracovníků systémové podpory apod. musí být veden záznam. Fyzické prostředí instalovaných komunikačních prostředků ISCS, zejména komunikačních zařízení,

rozhraní a související technologie, musí být zajištěno v rozmezí parametrů předepsaných nebo doporučených jejich výrobci či dodavateli. Je-li to v působnosti a možnostech CS, musí být přenosové cesty ISCS, včetně LAN kabeláže v objektech CS, chráněny před neoprávněným fyzickým přístupem jak zaměstnanců CS, tak zejména cizích osob.

3.1.3 Organizace bezpečné výměny dat ISCS

Organizace bezpečné výměny dat ISCS stanoví organizaci akvizice, vývoje, provozu a údržby komunikačních prostředků ISCS s ohledem na bezpečnost přenášených dat, včetně účasti a odpovědnosti organizačních útvarů CS, služebních funkcionářů CS, rolí a poskytovatele systémové podpory přenosu dat ISCS. Organizace bezpečné výměny dat ISCS vychází z organizační struktury CS, organizačního řádu CS, technických projektů souvisejících s přenosem dat ISCS a nejlepších praktik této problematiky. Pro výkon všech rolí bezpečné výměny dat ISCS musí být stanoveni zástupci a vhodné osoby výkonem rolí „zástupce“ pověřeny. Kombinace nebo kumulace rolí bezpečné výměny dat ISCS v rámci tohoto systému nebo s rolemi jiných systémů ochrany ISCS je přípustná. V případě specifických požadavků na organizaci bezpečné výměny dat ISCS, vyplývajících z mezinárodních i vnitrostátních smluv nebo dohod, musí být tyto požadavky respektovány a naplněny.

3.1.4 Role bezpečné výměny dat ISCS

Rolemi bezpečné výměny dat ISCS jsou správce bezpečné výměny dat ISCS a doménový administrátor bezpečné výměny dat v BD ISCS. Správce bezpečné výměny dat ISCS zejména metodicky řídí doménové administrátory bezpečné výměny dat v BD ISCS, provádí nebo zajišťuje kontrolu bezpečné výměny dat ISCS, stanoví metodiku kontrol a metodiku auditu bezpečné výměny dat ISCS, stanoví pravidla správy a bezpečného užívání komunikačních služeb ISCS, vede aktuální evidenci doménových administrátorů bezpečné výměny dat v BD ISCS, včetně jejich případných zástupců. Rolemi bezpečné výměny dat nejsou provozní role personálu ISCS, přestože příslušné subjekty těchto rolí vykonávají činnosti představující provádění ochrany komunikačních prostředků ISCS.

Správce bezpečnosti ISCS koordinuje výstavbu a provoz systému bezpečné výměny dat ISCS s ostatními systémy ochrany ISCS. Navrhuje vnitřní pokyny k bezpečné výměně dat ISCS. Má právo kontrolovat činnost správce bezpečné výměny dat ISCS. Správci BD ISCS koordinují provoz systému bezpečné výměny dat ISCS s ostatními systémy ochrany ISCS v jim příslušných BD ISCS. Mají právo kontrolovat

činnost doménových administrátorů bezpečné výměny dat v BD ISCS. Poskytovateli systémové podpory bezpečné výměny dat ISCS (poskytovatel SP) jsou vybrané externí subjekty, obvykle dodavatelé komunikačních zařízení ISCS.

Poskytovatel SP provádí systémovou podporu bezpečné výměny dat ISCS ve struktuře a rozsahu stanoveném smlouvou uzavřenou mezi CS a poskytovatelem SP. Relevantní smlouvy musí obsahovat, kromě provozně technických, i smluvní bezpečnostní podmínky. Jejich plnění je správcem i doménovými administrátory systému bezpečné výměny dat ISCS kontrolováno a v případě negativních zjištění jsou přijímána odpovídající opatření. Aktuální přehled takových smluv vede správce bezpečné výměny dat ISCS. Poskytovateli komunikačních služeb ISCS (dále jen „poskytovatel KS“) jsou zejména telekomunikační operátoři poskytující přenosové cesty a dále VAN operátoři poskytující internetové služby.

3.1.5 Zásady bezpečné výměny dat ISCS

Pro řešení implementace nebo změn (údržby) komunikačních prostředků ISCS musí být založeny projekty. V rámci projektu musí být zpracován projektový záměr a podle něho provedena specifikace zahrnující systémové a bezpečnostní požadavky nebo podmínky. Jedná-li se o rozsáhlejší projekt, musí být též zpracován globální a detailní návrh řešení. Pro zajišťování provozu implementovaných nebo změněných komunikačních prostředků ISCS musí být založen projekt provozu. Záměr, specifikace i návrhy řešení musí být zpracovány s ohledem na nové komunikační prostředky ISCS; musí však brát do úvahy i jejich vliv na komunikační prostředky stávající, jakož i na bezpečnost výměny dat ISCS. Zásady implementace, vývoje, provozu i údržby (změn) komunikačních prostředků ISCS budou stanoveny provozovatelem ISCS.

Komunikační zařízení ISCS musí být řešeno tak, aby plně pokrývalo stávající kapacitní provozní potřebu s rezervou pro případné navýšení požadavků na kapacitu provozu, musí být vybaveno tak, aby pokrývalo stávající typy připojených přenosových cest, a musí být vybaveno pro vzdálenou správu, dohled a monitoring. Komunikační rozhraní ISCS musí být řešeno tak, aby plně pokrývalo nejen stávající počet připojených přenosových cest, ale i předpokládané navýšení tohoto počtu alespoň v nejbližších dvou letech a musí být kompatibilní nejen se stávajícími typy připojených přenosových cest, ale i typů předpokládaných využívat alespoň v nejbližších dvou letech. Přenosové cesty ISCS musí být řešeny tak, aby plně pokrývaly stávající kapacitní provozní potřebu s rezervou pro případné navýšení požadavků na kapacitu provozu, musí být kompatibilní s komunikačními rozhraními ISCS.

Komunikační protokoly ISCS musí být voleny tak, aby plně pokrývaly stávající provozní potřebu, aby bylo umožněno poskytnutí komunikačních služeb oprávněným uživatelům ISCS a aby byly umožněny přenosy dat mezi ISCS a třetími stranami. Systémové požadavky, týkající se komunikačních služeb ISCS jsou již stanoveny ve vztahu ke komunikačnímu zařízení, rozhraní, přenosovým cestám a komunikačním protokolům ISCS. Systémové požadavky, týkající se lokální (LAN) i vzdálené (WAN) komunikace ISCS jsou již stanoveny ve vztahu ke komunikačnímu zařízení, rozhraní, přenosovým cestám a protokolům ISCS. Specifickým systémovým požadavkem, týkajícím se WAN komunikace, je uplatnění VPN a MPLS. Vnější komunikace ISCS se uskutečňuje prostřednictvím komunikačního centra ISCS. Komunikační a bezpečnostní prostředky vnější komunikace ISCS musí být instalovány a provozovány v demilitarizované zóně (DMZ) komunikačního centra ISCS. Vnější komunikace ISCS může být prováděna mimo komunikační centrum ISCS pouze v případě, že je schválena určeným pracovníkem, a za podmínky, že se uskutečňuje ze samostatného počítače nezapojeného do některé z LAN ISCS (Strategie ISCS, 2009).

3.1.6 Systémové požadavky na výměnu dat

Systémové požadavky, týkající se komunikace s orgány a organizacemi EU, jsou obvykle stanoveny spolupracujícím orgánem nebo organizací EU. V některých případech mohou být spolupracujícím orgánem nebo organizací EU stanoveny nebo i dodány příslušné komunikační prostředky spolu s pokyny k jejich instalaci, provozu a údržbě. Systémové požadavky, týkající se komunikace s orgány a organizacemi členských států EU, jsou obvykle navrženy jednou ze stran a oboustranně dohodnuty. V některých případech mohou být jednou ze stran navrženy a dohodnuty nebo i jednou ze stran druhé straně dodány příslušné komunikační prostředky spolu s pokyny k jejich instalaci, provozu a údržbě. Systémové požadavky, týkající se komunikace s orgány a organizacemi ČR, jsou obvykle navrženy tou ze stran, u níž existuje zákonná či jiná potřeba takové komunikace. Tyto požadavky jsou oboustranně dohodnuty. V některých případech mohou být jednou ze stran navrženy a dohodnuty nebo i jednou ze stran druhé straně dodány příslušné komunikační prostředky spolu s pokyny k jejich instalaci, provozu a údržbě.

Systémové požadavky, týkající se komunikace s poskytovateli systémové podpory ISCS, jsou obvykle navrženy poskytovatelem systémové podpory ISCS a oboustranně dohodnuty. V některých případech mohou být jednou ze stran navrženy a dohodnuty nebo i poskytovatelem systémové podpory ISCS dodány příslušné komunikační prostředky spolu s pokyny k jejich instalaci, provozu a údržbě.

Komunikace mezi ISCS a informačními systémy podnikatelských subjektů ČR obvykle vychází z legislativy ČR nebo ze zákonných či jiných potřeb jedné ze stran. Může být založen na dvoustranné smlouvě nebo dohodě. Systémové požadavky, týkající se této komunikace, jsou obvykle oboustranně dohodnuty na základě zákonného předpisu nebo smlouvy. V některých případech mohou být jednou ze stran stanoveny a jednou ze stran druhé straně dodány příslušné komunikační prostředky spolu s pokyny k jejich instalaci, provozu a údržbě. Systémové požadavky, týkající se komunikace s ostatní veřejností, jsou již stanoveny ve vztahu ke komunikačnímu zařízení, rozhraní, přenosovým cestám a protokolům ISCS.

3.1.7 Bezpečnostní požadavky na výměnu dat ISCS

Komunikační prostředky ISCS musí být odolné proti vlastním chybám tak, aby nebylo možným zdrojem ztráty důvěrnosti, integrity a dostupnosti přenášených dat anebo možným zdrojem nedostupnosti komunikačních služeb ISCS. Je-li odolnost komunikačního zařízení ISCS nižší než je požadováno nebo je-li riziko vlastní chyby vyšší, než je přípustné, musí být takové zařízení zdvojeno. Současně musí být zajištěno automatické přesměrování přenášených dat ze zařízení nefunkčního na zařízení funkční. Porty komunikačního zařízení, určené pro vzdálenou správu, dohled a monitoring, musí být chráněny před neautorizovaným přístupem. Nevyužívané porty musí být deaktivovány. Komunikační zařízení ISCS musí být jednoznačně určeno identifikačním číslem nebo jiným údajem pro potřebu vzájemné autentizace.

Komunikační zařízení ISCS musí obsahovat mechanismus pro záznam autorizovaných lokálních i vzdálených přístupů v souvislosti se správou, dohledem a monitoringem. Tento mechanismus musí zaznamenat i pokusy o neautorizovaný přístup. Komunikační zařízení ISCS musí být umístěno v prostorách, do kterých má fyzický přístup pouze vymezený počet autorizovaných osob a kde jsou zajištěny výrobcem nebo dodavatelem předepsané parametry fyzického prostředí. Je-li odolnost přenosové cesty ISCS nižší než je požadováno nebo je-li riziko vlastní chyby vyšší než je přípustné, musí být taková přenosová cesta zdvojena. Současně musí být zajištěno automatické přesměrování přenášených dat z přenosové cesty nefunkční na cestu funkční. Přenosové cesty ISCS musí být vybaveny tak, aby byl možný jejich dohled a monitoring jak ze strany příslušného operátora, tak i ze strany CS. Kabeláž LAN ISCS musí být provedena tak, aby k ní neměly nekontrolovatelný fyzický přístup neautorizované osoby.

Komunikační protokoly ISCS musí obsahovat mechanismy pro ochranu důvěrnosti, integrity a dostupnosti přenášených dat, případně i údajů o odesilateli a adresátovi zprávy. Pro užívání komunikační služby nebo služeb ISCS musí být uživatel

ISCS bezpodmínečně prokazatelně autorizován. Užívání komunikačních služeb ISCS může být autorizovaným uživatelům ISCS časově nebo adresně omezeno, např. omezením přístupu na některé adresy (servery) Internetu, k některým složkám nebo souborům Intranetu. Na užívání komunikačních služeb ISCS se vztahují další omezení stanovená zvláštními právními předpisy. Bezpečnostní požadavky, týkající se komunikačních služeb ISCS služby, jsou již stanoveny ve vztahu ke komunikačnímu zařízení, rozhraní, přenosovým cestám a protokolům ISCS. Specifickým bezpečnostním požadavkem, týkajícím se služby elektronické pošty ISCS je, že poštovní systém CS musí být chráněn prostředky antivirové a antispamové ochrany. Specifickým bezpečnostním požadavkem, týkajícím se internetových služeb, je to, že rozhraní mezi ISCS a Internetem musí být vybaveno technologií FW, antivirové a antispamové ochrany. Specifickým bezpečnostním požadavkem, týkajícím se služby vzdáleného přístupu do ISCS, je to, že při vzdáleném přístupu musí být prováděna dodatečná autentizace uživatele, nejlépe pomocí autentizačního serveru.

Bezpečnostní požadavky, týkající se interní LAN i WAN komunikace ISCS, jsou již stanoveny ve vztahu ke komunikačnímu zařízení, rozhraní, přenosovým cestám a protokolům ISCS. Specifickými bezpečnostními požadavky, týkajícími se WAN komunikace, je to, že hlavní (páteřní) přenosové cesty musí být provedeny formou horké zálohy, tzn., že musí být zdvojeny a že každá z těchto hlavních a záložních přenosových cest musí být vedena do jiné lokality CS. Bezpečnost komunikace mezi ISCS a informačními systémy orgánů a organizací EU je založena na legislativě EU. Bezpečnostní požadavky, týkající se komunikace mezi ISCS a informačními systémy orgánů a organizací EU, jsou obvykle rovněž stanoveny spolupracujícím orgánem nebo organizací EU. V některých případech mohou být spolupracujícím orgánem nebo organizací EU stanoveny nebo i dodány příslušné bezpečnostní prostředky spolu s pokyny k jejich instalaci, provozu a údržbě (např. šifrovací zařízení NCTS).

Bezpečnostní požadavky, týkající se komunikace s orgány a organizacemi členských států EU, jsou obvykle navrženy jednou ze stran a oboustranně dohodnuty. V některých případech mohou být jednou ze stran navrženy a dohodnuty nebo i jednou ze stran druhé straně dodány příslušné bezpečnostní prostředky spolu s pokyny k jejich instalaci, provozu a údržbě. Bezpečnostní požadavky, týkající se komunikace s orgány a organizacemi ČR, jsou obvykle navrženy tou ze stran, u níž existuje zákonná či jiná potřeba takové komunikace. Tyto požadavky jsou oboustranně dohodnuty. V některých případech mohou být jednou ze stran navrženy a dohodnuty nebo i jednou ze stran druhé straně dodány příslušné bezpečnostní prostředky spolu s pokyny k jejich instalaci,

provozu a údržbě. Bezpečnostní požadavky, týkající se komunikace s poskytovateli systémové podpory ISCS, jsou obvykle stanoveny ze strany CS a poskytovatelé systémové podpory ISCS jsou smluvně povinni tyto požadavky respektovat.

Bezpečnostní požadavky, týkající se komunikace s podnikatelskými subjekty ČR, jsou obvykle oboustranně dohodnuty na základě zákonného předpisu nebo smlouvy. V některých případech mohou být jednou ze stran stanoveny a jednou ze stran druhé straně dodány příslušné bezpečnostní prostředky spolu s pokyny k jejich instalaci, provozu a údržbě. Specifickým bezpečnostním požadavkem, týkajícími se komunikace s ostatní veřejností, je to, že portálový server CS musí být chráněn proti narušení integrity prezentovaných informací, podsunutí neautorizovaných informací, úmyslnému zahlcení přístupových portů a neoprávněnému přístupu ze strany ISCS.

3.1.8 Řízení bezpečné výměny dat ISCS

Pro řízení bezpečné výměny dat ISCS musí být stanoveny a prováděny bezpečné postupy a procedury správy provozně technické dokumentace, akvizice, vývoje, provozu a údržby komunikačních prostředků ISCS. Personálně musí být řízení bezpečné výměny dat ISCS založeno na subjektech organizace bezpečné výměny dat ISCS, přičemž činnosti související s prováděním ochrany komunikačních prostředků ISCS realizuje personál ISCS v souladu s pravidly uvedenými v tomto VP. Zúčastněné osoby, především pak personál ISCS, provádějící činnosti související s bezpečnou výměnou dat, musí mít k dispozici vhodné technologické prostředky.

V rámci pravidel, která představují stanovení bezpečných postupů a procedur bezpečné výměny dat ISCS, musí být začleněno, jaká provozní dokumentace musí být k jednotlivým komunikačním prostředkům ISCS vedena a kým. Jedná se např. o provozní deníky, testovací protokoly, auditní protokoly apod. Projekty akvizice, vývoje, provozu a údržby související s jedním nebo více komunikačních prostředků ISCS vedou správce a administrátoři bezpečné výměny dat ISCS. Technickou dokumentaci, tj. funkční a technické popisy, administrátorské příručky, konfigurační údaje apod. vedou provozní správci jednotlivých komunikačních prostředků ISCS z řad personálu ISCS.

Akvizicí komunikačních prostředků ISCS se rozumí proces jejich získání na základě projektu akvizice, a to nákupem od externího dodavatele. Zadavatelem akvizice je provozovatel ISCS, který též určuje vedoucího projektu akvizice. Ve složitějších nebo rozsáhlejších případech může být pro řešení akvizice vytvořen projektový tým. V rámci akvizice musí být provedena analýza důvodu a potřeb, a to formou projektového záměru. Poté se provádí věcná, finanční a časová specifikace. Věcnou specifikaci představují systémové a bezpečnostní požadavky. Dodávky, montáž a instalace komunikačních

prostředků ISCS podléhají dohledu, který provádí nebo zajišťuje vedoucí projektového týmu. Závěrem akvizice je akceptace, tj. přejímka. Vývojem komunikačních prostředků ISCS se rozumí proces jejich získání na základě projektu vývoje, a to zakázkou, obvykle na externí vývoj uceleného subsystému přenosu dat ISCS, např. WAN ISCS. Zadavatelem vývoje je provozovatel ISCS, který též určuje vedoucího projektu vývoje. Pro řešení vývoje bývá obvykle vytvořen projektový tým. V rámci vývoje musí být provedena analýza důvodu a potřeb, a to formou projektového záměru. Poté se provádí věcná, finanční a časová specifikace. Věcnou specifikaci představují systémové a bezpečnostní požadavky. Vybraný dodavatel zpracuje, podle složitosti anebo rozsahu zakázky, úvodní studii, globální a detailní návrh (projekt) řešení. Dodává rovněž provozně technickou a bezpečnostní dokumentaci. Dodávky, montáž a instalace komunikačních prostředků ISCS podléhají dohledu, který provádí nebo zajišťuje vedoucí projektového týmu. Závěrem vývoje je akceptace, tj. přejímka.

Provozem komunikačních prostředků ISCS se rozumí proces zajišťování jejich provozuschopnosti a provozní podpory uživatelů komunikačních služeb na základě projektu provozu, a to s využitím sil a prostředků provozovatelů subISCS a externích poskytovatelů systémové podpory. Provozovatel ISCS určuje vedoucího projektu provozu komunikačních prostředků ISCS, kterým by měl být vedoucí komunikačního centra ISCS. Projekt provozu zahrnuje, ve vztahu ke komunikačním prostředkům ISCS, provozní: obsluhu a řízení přístupu, servis, dohled a monitoring, evidenci a statistiku, testování a podporu uživatelů. Tyto činnosti jsou dále členěny vůči jednotlivým komunikačním prostředkům ISCS. Údržbou komunikačních prostředků ISCS se rozumí proces jejich modifikace (změn) na základě zjištěných problémů, potřeby zdokonalení, adaptace na nové podmínky nebo migrace do nového prostředí, a to obvykle nákupem řešení od externího dodavatele, např. od smluvního poskytovatele příslušné systémové podpory. Provozovatel ISCS určuje vedoucího projektu údržby komunikačních prostředků ISCS. V rámci údržby musí být provedena analýza důvodu a potřeb, a to formou projektového záměru. Poté se provádí věcná, finanční a časová specifikace. Věcnou specifikaci představují systémové a bezpečnostní požadavky. Údržba komunikačních prostředků ISCS je prováděna podle detailního návrhu (projektu) zpracovaného vybraným dodavatelem; podléhá dohledu, který provádí nebo zajišťuje vedoucí projektového týmu. Závěrem údržby je akceptace, tj. přejímka (Strategie ISCS, 2009).

3.2 Bezpečnostní opatření

Komunikační prostředky interní i vnější komunikace ISCS představují z objektivního hlediska prvky ISCS se střední rizikovostí, ve výjimečných případech i prvky s vysokou rizikovostí. Interní i vnější komunikace ISCS musí být chráněny užitím vhodné kombinace bezpečnostních opatření organizačně personálního, administrativně procedurálního, technologického i fyzického charakteru.

Stav, funkčnost, zatížení a propustnost komunikačních prostředků ISCS musí být dohlíženy, testovány a monitorovány. Dohled, testování a monitoring provádí personál ISCS anebo poskytovatel systémové podpory, a to s využitím vhodných technických a programových nástrojů. Provádí-li dohled, testování anebo monitoring poskytovatel systémové podpory, může při tom využívat službu vzdáleného přístupu ISCS. Při zjištění problémů nebo nedostatků je subjekt dohledu, testování a monitoringu povinen postupovat podle stanovených pravidel nebo, je-li zaměstnancem CS, podle pokynů svého nadřízeného.

Ochrana důvěrnosti dat přenášených v rámci interní komunikace ISCS je prováděna s využitím komerčních kryptografických technik. Ochrana důvěrnosti dat přenášených v rámci vnější komunikace ISCS je prováděna, a to s využitím kryptografických technik, tehdy, jedná-li se o ochranu smluvní nebo dohodnutou s druhou stranou, např. ochrana dat přenášených v rámci NCTS. Správu příslušných kryptografických prostředků, zejména pak správu klíčů, provádí, zajišťuje nebo dohlíží správce těchto prostředků z řad personálu ISCS.

Ochrana integrity dat přenášených rámci interní komunikace ISCS je prováděna s využitím komerčních kryptografických technik. Ochrana integrity dat přenášených v rámci vnější komunikace ISCS je prováděna s využitím vlastností uplatněných přenosových protokolů, např. kontrolních součtů, nebo s využitím jiných, vzájemně dohodnutých technik. Pro ochranu integrity dat přenášených v rámci interní i vnější komunikace ISCS může být využita technologie digitálního podpisu.

Ochrana před vnějším zneužitím komunikačních prostředků ISCS je prováděna řadou bezpečnostních opatření naplňujících bezpečnostní požadavky na komunikační prostředky ISCS uvedené v tomto VP. Některá bezpečnostní opatření k ochraně před vnějším zneužitím komunikačních prostředků ISCS jsou součástí systémů ochrany ISCS. Jedná se zejména o opatření fyzické ochrany, antivirové ochrany, řízení přístupu stanovená, řízení rizik.

Ochrana fyzického přenosu dat na datových nosičích musí být prováděna kombinací bezpečnostních opatření různého charakteru, přičemž za datový nosič nutno

považovat i notebook s daty uloženými na pevném disku. Relevantními bezpečnostními opatřeními, odvislými zejména od kategorie citlivosti dat, jsou např. autorizace a poučení osoby data přenášející, zašifrování dat, užití bezpečnostních schránek (Bezpečnostní politika CS ČR, 2007).

3.2.1 Zvládání bezpečnostních incidentů

Zvládání bezpečnostních incidentů je specifický proces zajištění nebo obnovy provozu komunikačních prostředků ISCS při pokusu o narušení anebo při narušení bezpečnosti interní anebo vnější komunikace ISCS, zejména pak bezpečnosti pro CS důležitých, tzv. kritických přenosů dat. Bezpečnostní incidenty související s interní nebo vnější komunikací ISCS jsou podle Bezpečnostní politiky Celní správy ČR (2007) členěny na bezpečnostní události a na havárie. Zdrojem bezpečnostních událostí jsou lidé, zdrojem havárií vlastnosti komunikačních prostředků ISCS a prostředí, ve kterém jsou provozovány. Bezpečnost interní a vnější komunikace ISCS je založena na řízení rizik těchto komunikací, tj. na jejich znalosti, eliminací nebo alespoň minimalizaci.

Kritické přenosy dat jsou závislé na bezpečnosti kritických prvků komunikačních prostředků ISCS. Kritické prvky určuje správce bezpečné výměny dat ISCS. Rizika, ve formě hrozeb a zranitelnosti komunikačních prostředků ISCS, musí být správcem bezpečné výměny dat ISCS pravidelně, nejméně 1x za 3 roky, analyzována a hodnocena z hlediska jejich pravděpodobnosti a dopadů. Bezpečnostní opatření, uplatněná vůči komunikačním prostředkům ISCS, musí být správcem bezpečné výměny dat ISCS pravidelně, nejméně 1x za 3 roky, auditovaná a hodnocena z hlediska jejich úplnosti, správnosti a účinnosti.

Pro zvládání bezpečnostních incidentů, tj. bezpečnostních událostí a havárií, musí být správcem bezpečné výměny dat ISCS stanoveny typické bezpečnostní incidenty a s nimi prokazatelně seznámeni jak personál, tak i uživatelé ISCS. Osoba, která zjistí pokus o narušení nebo narušení bezpečnosti interní nebo vnější komunikace ISCS, je povinna tuto skutečnost neprodleně nahlásit správci bezpečné výměny dat ISCS nebo svému nadřízenému služebnímu funkcionáři. Správce bezpečné výměny dat ISCS ověří nebo zajistí ověření hlášení, zajistí ochranu dotčených kritických prvků komunikačních prostředků ISCS a zjištění zdroje pokusu o narušení nebo narušení bezpečnosti interní nebo vnější komunikace ISCS. V nezbytném případě je možno pozastavení provozu všech nebo části komunikačních prostředků ISCS, zejména přenosových cest. Byl-li provoz všech nebo části komunikačních prostředků ISCS pozastaven, lze jej obnovit po zajištění provozuschopnosti a ochrany dotčených kritických prvků komunikačních prostředků ISCS, a dále po zjištění a odstranění zdroje

pokusu o narušení nebo narušení bezpečnosti interní nebo vnější komunikace ISCS. Obnovu provozu je možno znovu schválit pouze na návrh správce bezpečné výměny dat ISCS. Personál a uživatelé ISCS musí být k typickým bezpečnostním incidentům a ke zvládání bezpečnostních incidentů souvisejících s komunikačními prostředky ISCS pravidelně, nejméně 1x ročně prokazatelně školeni. Správce a doménoví administrátoři bezpečné výměny dat ISCS musí, s jimi vybraným personálem anebo uživateli ISCS nejméně 1x za 3 roky organizovat a provádět nácviky řešení simulovaných bezpečnostních incidentů souvisejících s komunikačními prostředky ISCS.

3.2.2 Směrnice o uchovávání údajů z elektronických komunikací

V současné době se aktuálně vyskytují problémy při implementaci směrnice o uchovávání údajů vzniklých při poskytování elektronických služeb v rámci EU s jejich negativním dopadem na telekomunikační operátory a poskytovatele služeb elektronických komunikací. Evropská komise (dále jen „Komise“) dne 18. dubna 2011 zveřejnila zprávu o implementaci a aplikaci směrnice 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí pro účely boje s trestnou činností (dále jen „směrnice“). Zprávu o implementaci a aplikaci tohoto poměrně kontroverzního právního předpisu připravila Komise s velkým zpožděním oproti termínu stanovenému v čl. 14 směrnice, kterým bylo 15. září 2010.

V této souvislosti je třeba zmínit, že směrnice na evropské úrovni částečně harmonizuje povinnosti poskytovatelů služeb elektronických komunikací a telekomunikačních operátorů při uchovávání provozních a lokalizačních údajů o proběhlé elektronické komunikaci za účelem odhalování, vyšetřování a stíhání závažné trestné činnosti. Definuje kategorie provozních a lokalizačních údajů, které mají být uchovávány, stanoví základní pravidla o jejich ochraně a možnostech přístupu orgánů činných v trestním řízení a stanoví limitní lhůty pro jejich uchovávání. V České republice se implementace této směrnice stala předmětem přezkumu Ústavního soudu ČR, který dne 22. března 2011 svým nálezem pod sp. zn. Pl. ÚS 24/10 zrušil § 97 odst. 3 a odst. 4 zákona č. 127/2005 Sb., o elektronických komunikacích, a doprovodnou vyhlášku č. 485/2005 Sb. Ve svém nálezu Ústavní soud konstatoval kolizi předmětných ustanovení zákona s principy právního státu a jejich nesoulad s požadavky na omezení základního práva na soukromí v podobě práva na informační sebeurčení ve smyslu čl. 10 odst. 3 a čl. 13 Listiny, které plynou také z principu proporcionality zásahu státu do soukromí občanů. Obdobně v Německu a Rumunsku došlo ke zrušení implementační legislativy této směrnice ze strany ústavních soudů.

Komise ve zprávě konstatuje, že směrnice se stala účinným a užitečným nástrojem orgánů vymáhajících právo v členských státech EU. Na druhou stranu je její dopad limitní z důvodů pouze částečné harmonizace v určitých klíčových bodech. Jsou jimi chybějící unijní úprava náhrady nákladů poskytovatelů elektronických služeb vynaložených v souvislosti s aplikací směrnice, kdy pouze ve dvou členských státech (Finsko a Česká republika) stát plně hradí náklady vynaložené poskytovateli elektronických služeb z důvodů plnění povinností stanovených směrnicí. Rovněž chybí společná definice závažné trestné činnosti, což způsobuje zásadní rozdíly v rozsahu implementace směrnice vzhledem k rozdílným existujícím definicím v jednotlivých členských státech.

Velké rozdíly mezi členskými státy existují také v seznamu orgánů oprávněných k přístupu k uchovávaným informacím. Kromě orgánů činných v trestním řízení umožňuje 6 členských států přístup daňových a celních orgánů a 3 členské státy umožňují také přístup pohraniční policie. Značné rozdíly při implementaci směrnice panují v délce lhůty, po kterou jsou poskytovatelé služeb povinni uchovávat provozní a lokalizační údaje. Maximální lhůtu 2 let dle směrnice využilo Polsko, 1,5 roku Litva a 10 členských států stanovilo lhůtu na 1 rok. Řada členských států využívá rozdílné lhůty pro jednotlivé kategorie uchovávaných lokalizačních a provozních údajů. Z pohledu stáří požadovaných údajů ze strany orgánů činných v trestním řízení je v průměru 70% požadovaných údajů mladší 3 měsíců a dalších 20% údajů „ve stáří“ mezi 3 a 6 měsíci. Pouze okolo 10% požadovaných údajů ze strany orgánů činných v trestním řízení je tedy starší 6 měsíců. Zajímavou skutečností je, že pouze 1% vyžadovaných údajů ze strany orgánů činných v trestním řízení mělo přeshraniční charakter. Zde tedy nadále silně působí jako bariéra nutnost využití vzájemné právní pomoci ve věcech trestních mezi členskými státy při vyžadování údajů uchovávaných na základě směrnice.

Na základě výše uvedeného Komise konstatuje, že směrnice má v současné podobě velmi limitovaný dopad na předvídatelnost a právní jistotu poskytovatelů elektronických a telekomunikačních služeb, kteří působí ve více členských státech. Jedná se zejména o případy, kdy poskytovatelé služeb mají svoji datovou a IT základnu v jednom členském státě a současně poskytují datové a telekomunikační služby do jiného členského státu. Nedostatečná harmonizace ve směrnici nadnárodním operátorům telekomunikačních a elektronických služeb působí vysoké dodatečné náklady na vybavení hardwarem a softwarem, kdy při současném stavu je nutné pro každý národní trh členského státu připravit individuální technické řešení pro uchovávání provozních a lokalizačních údajů (Solský, 2011).

4 Význam ochrany informací

Informace mají, a v budoucnu budou mít, v dnešním světě klíčovou roli. Obzvláště v tržním mechanismu představují významnou výhodu pro soutěžící subjekty. Cenu informací ještě umocňuje počítačová technologie, která prorůstá současným životním stylem.

Známe všichni lidskou zkušenost – hodnotu něčeho zpravidla oceníme, až to ztratíme. V současné době je vysoce aktivní ztráta informací, zejména jestliže je zpracováváme či uchováváme v prostředcích výpočetní techniky. Zatímco přijímání, evidování, zpracování či archivování informací se věnuje poměrně značná pozornost, jejich ochrana před zneužitím byla dosud většinou jen výsadou specializovaných odvětví (armáda, policie, vrcholové státní instituce, výzkumné ústavy apod.).

Nové vlastnické normy v naší zemi však přinášejí i potřebu ochrany informací obchodního či osobního charakteru. O tom, že je informační bezpečnosti věnována v České republice (ČR) pozornost svědčí i to, že vláda ČR schválila „Národní strategii informační bezpečnosti“ usnesením č. 1340 ze dne 19. 10. 2005.

Neúprosný konkurenční boj snižuje úroveň společenské hierarchie, na níž je třeba informace chránit. Tedy nejen na úrovni vrcholové, ale i na stupních nižších. Ochrana informací se stává významným faktorem soudobého úspěchu či naopak neúspěchu podniku. Nepochybně je však ztráta či získání informace i významným motivačním faktorem pro páchání kriminální trestné činnosti. Složité společenské a ekonomické podmínky vedou nejen k ochraně jednotlivých informací, ale spíše k ochraně celých informačních systémů. V nich se totiž v současné době soustřeďují informace tak, aby je bylo možné efektivně využívat. Ztráty, které vznikají poškozením, zneužitím, nebo zničením informačního systému nebo jen části informací v nich, bývají nedozírné, někdy nenahraditelné (Ivanka, 2009). To si začínají mnohé organizace a instituce uvědomovat, zejména s rozšiřujícími se možnostmi využívat výpočetní techniku. Současně se ovšem problém ochrany informací většinou zužuje na jejich zabezpečení a úpravě v těchto prostředcích, postupně integrovaných do počítačových sítí.

4.1 Mezinárodní patentová ochrana

V současnosti stále více nabývá na významu způsob, jak chránit v zahraničí technická řešení, která jsou výsledkem tvůrčí činnosti. Technická řešení, pokud splňují podmínky stanovené příslušnými právními předpisy, je možno chránit patentem. Ochrana vynálezů má teritoriální charakter a každý stát v platném právním předpise stanovuje, za jakých podmínek lze udělit ochranu na vynález a v čem tato ochrana spočívá. Z toho vyplývá, že v případě, že má vynálezce zájem chránit vynález i mimo území ČR, je nutno, aby podal přihlášku vynálezu také v těch státech, kde hodlá získat na své řešení ochranu.

Další výlučnou ochranou technických řešení, která je rychlá a finančně méně náročná, je osvědčení na užitný vzor. Užitný vzor není celosvětově rozšířen tak jako ochrana patentem, ale je možno jej chránit v řadě zemí, kde jsou však také určité právní odlišnosti. Je možno tedy na technické řešení získat i ochranu užitným vzorem v těch státech, kde tento druh ochrany existuje.

Z uvedeného vyplývá, že ochrana průmyslových práv je poskytována pouze na území státu, kde o ni bylo požádáno, zaplaceny poplatky a po nezbytném, často i velmi zdlouhavém řízení. Zpravidla je přihláška vynálezu/užitného vzoru podávána poprvé v zemi, kde je původce občanem nebo kde má sídlo podnikatelský subjekt, který uplatňuje právo na ochranu. Od tohoto data prvního podání se začíná podle Úmluvy o ochraně průmyslového vlastnictví počítat 12měsíční lhůta pro podání přihlášky na shodné technické řešení v zahraničí. Pokud totiž přihlašovatel v této lhůtě podá shodnou přihlášku, pohlíží se na ni, jako by byla podána v den podání první přihlášky (právo přednosti – priorita).

Přihlašovatel tedy má od podání prioritní přihlášky omezený čas – 12 měsíců – na rozhodnutí, ve kterých státech bude žádat o ochranu a také o jaký druh ochrany bude žádat. Při přihlašování do zahraničí pak má přihlašovatel několik možností jak postupovat. První možností je národní cesta. Tato cesta je vhodná, pokud přihlašovatel hodlá získat ochranu v jednom nebo v málo státech. Vyžaduje to odbornou pomoc a přihlašovatel musí být zastoupen zástupcem, který je oprávněn zastupovat před příslušným patentovým úřadem. Přihlašovatel musí v určených lhůtách předložit překlady přihlášky a zaplatit příslušné poplatky. Potom v průběhu řízení dojde pravděpodobně k výměně názorů mezi úřadem a přihlašovatelem prostřednictvím stanoveného zástupce.

Celé řízení je tedy poměrně nákladné a přihlašovatel nemá jistotu, že skutečně dojde k udělení ochranného dokumentu. Další možností zahraniční ochrany je cesta

regionální ochrany. Při této cestě se zahájí řízení podáním jediné přihlášky, průzkumové řízení probíhá u jediného, regionálního úřadu a v kladném případě končí udělením regionálního patentu. Udělený regionální patent pak platí buď automaticky ve všech smluvních státech regionální úmluvy, nebo je třeba požádat v designovaných zemích o validaci. Jedná se o evropský patent, eurasijský patent, patent OAPI a patent ARIPO. Evropský patent se uděluje pro státy Evropské unie a přidružené. V evropské přihlášce je zahrnuta designace všech smluvních států, ale ve státech, kde má udělený evropský patent nakonec platit, je potřeba učinit odpovídající úkony, spojené s jeho validací. Eurasijský patent platí automaticky ve všech smluvních státech úmluvy a vydává se v ruštině. Regionální patent OAPI (frankofonní státy Afriky) platí pro všechny členské státy úmluvy. Regionální patent ARIPO (anglofonní země Afriky) – při podání přihlášky se vyžaduje designace států, ve kterých se hodlá získat ochrana, a registrace regionálního patentu vyžaduje schválení členských států.

Třetí cestou je pak cesta mezinárodní přihlášky podle Smlouvy o patentové spolupráci (PCT). Podle této Smlouvy podání jediné mezinárodní přihlášky a v jediném jazyce znamená podání přihlášky ve všech státech, které jsou k datu podání mezinárodní přihlášky smluvními státy Smlouvy. I když na konci mezinárodního řízení nedochází k udělení ochranného dokumentu, na mezinárodní přihlášku je provedena mezinárodní rešerše a případně i mezinárodní předběžný průzkum – průzkum patentovatelnosti. Přihlašovatel tak má dostatek informací a dost času na to, aby se rozhodl, zda zahájit národní řízení ve státech, kde hodlá získat ochranu (Hošková, 2010).

4.1.1 Smlouva o patentové spolupráci

Smlouva o patentové spolupráci (Paten Cooperation Treaty – PCT) byla uzavřena v r. 1970, novelizována v r. 1979 a upravena v r. 2001. Je otevřena pro smluvní státy Pařížské úmluvy na ochranu průmyslového vlastnictví (1883). Dokument o ratifikaci nebo přístupu ke Smlouvě musí být uložen u generálního ředitele Světové organizace duševního vlastnictví (WIPO). Smluvní státy uzavřely tuto smlouvu, protože si přály přispět k pokroku vědy a techniky, zdokonalit ochranu vynálezů, zjednodušit a zhospodárnit získání ochrany pro vynálezy tam, kde je požadována ochrana ve více státech, usnadnit a urychlit přístup veřejnosti k technickým informacím obsaženým v listinách popisujících nové vynálezy a podpořit a urychlit hospodářský pokrok rozvojových zemí přijetím opatření ke zvýšení účinnosti jejich národních nebo regionálních právních systémů pro ochranu vynálezů, a to poskytováním snadno přístupných informací o existenci technických řešení a usnadnění přístupu ke stále vzrůstajícímu rozsahu moderní techniky. Smlouva umožňuje získat patentovou ochranu

na vynález současně v každém z velkého počtu států (142 k 1. únoru 2010) podáním „mezinárodní“ patentové přihlášky. Takovou přihlášku lze podat kýmkoliv, kdo je občanem smluvního státu nebo v něm má sídlo. Může být obecně podána u národního patentového úřadu smluvního státu, jehož je přihlašovatel občanem nebo v něm má sídlo, nebo, podle volby přihlašovatele, u Mezinárodního úřadu WIPO v Ženevě (Hošková, 2010).

Přihlašovatel může podat mezinárodní přihlášku také u Evropského úřadu (EPO), Euroasijského úřadu (EAPO), Africké regionální organizace průmyslového vlastnictví (ARIPO), Africké organizace duševního vlastnictví (OAPI), pokud je občanem nebo má sídlo ve státu, který je smluvním státem těchto dohod o udělování regionálních patentů. Řízení podle PCT sestává ze dvou hlavních fází. Začíná podáním mezinárodní přihlášky a končí (v případě příznivého výsledku pro přihlašovatele) udělením řady národních a případně regionálních patentů. Proto se v rámci řízení podle PCT užívají výrazy „mezinárodní“ a „národní“ fáze řízení.

Mezinárodní fáze řízení sestává (v případě, že je úplná) ze čtyř hlavních kroků, z nichž tři nastávají automaticky, a pro poslední se přihlašovatel může rozhodnout sám. Národní fáze řízení pak probíhá u těch národních nebo regionálních úřadů, kde přihlašovatel hodlá získat ochranný dokument, podle jejich platného práva. První krok mezinárodní fáze řízení spočívá v podání mezinárodním přihlášky přihlašovatelem. V druhém kroku se mezinárodní přihláška podrobí tomu, co se nazývá „mezinárodní rešerše“. Tato rešerše se provádí jedním z větších patentových úřadů, ustanovených Shromážděním PCT jako Orgán pro mezinárodní rešerši (ISA). Výsledkem rešerše je „zpráva o mezinárodní rešerši“, tj. seznam citací takových zveřejněných dokumentů, které by mohly ovlivnit patentovatelnost vynálezu nárokovaného v mezinárodní přihlášce. Současně ISA připraví písemný posudek na patentovatelnost.

Zpráva o mezinárodní rešerši a písemný posudek Orgán pro mezinárodní rešerši postoupí přihlašovateli, který se může včas rozhodnout, jestli by raději neměl svou přihlášku vzít zpět, a to zejména tehdy, pokud z této zprávy nebo posudku vyplývá, že je udělení patentu nepravděpodobné. Pokud není mezinárodní přihláška vzata zpět, nastane třetí krok, kdy je mezinárodní přihláška spolu se zprávou o mezinárodní rešerši zveřejněna Mezinárodním úřadem (IB). Písemný posudek se nezveřejňuje. Celý postup podle PCT má pro přihlašovatele, patentové úřady a širokou veřejnost mimořádné výhody:

- přihlašovatel má až 18 měsíců navíc oproti řízení bez použití PCT, aby přemýšlel o vhodnosti získání ochrany v zahraničí, jmenoval místní patentové zástupce v každém státu, připravil potřebné překlady a zaplatil národní poplatky; je si jistý, že pokud je jeho přihláška v podobě předepsané PCT, nemůže být zamítnuta na základě formálních nedostatků žádným určeným úřadem během národní fáze řízení o přihlášce; na základě zprávy o mezinárodní rešerši nebo písemného posudku, může zhodnotit s přiměřenou pravděpodobností naději na udělení patentu na svůj vynález; a přihlašovatel má možnost během mezinárodního předběžného průzkumu upravit mezinárodní přihlášku a dát ji do pořádku před řízením u určených úřadů,

- práce na rešerši a průzkumu národních (regionálních) patentových úřadů se mohou významně redukovat nebo skutečně omezit díky zprávě o mezinárodní rešerši, písemnému posudku a případně mezinárodnímu předběžnému průzkumu, který doprovází mezinárodní přihlášku,

- protože je každá mezinárodní přihláška zveřejněna spolu se zprávou o mezinárodní rešerši, třetí strany jsou v lepší pozici formulovat dobře podložený názor na patentovatelnost nárokovaného vynálezu.

Dále může nastat volitelný čtvrtý krok, kdy přihlašovatel může požádat o provedení mezinárodního předběžného průzkumu (průzkumu patentovatelnosti), který končí vyhotovením zprávy o mezinárodním předběžném průzkumu (zpráva o patentovatelnosti), ze které přihlašovatel získá ještě podrobnější informace o pravděpodobnosti udělení požadovaného ochranného dokumentu (Hošková, 2010).

4.2 Získávání informací a pronikání do informačních systémů

Lze říci, že v současné době se většina informací rozvědného charakteru získává technickými prostředky, zejména pomocí satelitů, pozemních odposlouchávacích či pozorovacích stanovišť, až po užití této techniky jednotlivci (Požár, 2010). Zbytek je doplňován klasickými formami získávání informací, tj. prostřednictvím lidí, agentů, jejich prací uvnitř zájmových objektů (zcizování informací opisem, kopírováním, vlastním odposlechem atd.).

4.2.1 Získávání informací v automatizovaných informačních systémech

V oblasti automatizovaných informačních systémů, tedy při využívání výpočetní techniky, se problém nedovoleného získávání informací dostal až k naplňování ustanovení trestního zákoníku, tedy k páchání trestné činnosti tak, že mluvíme již speciálně o počítačové kriminalitě.

Do této oblasti např. patří (Strategie ISCS, 2009):

- mapování technického nebo programového vybavení, dat nebo komunikačních zařízení, tj. nejen fyzické odcizení nebo poškození technického prostředku, ale zejména na něm uloženého programu a dat (informací). Mohli bychom sem zahrnout i tzv. logické bomby, aktivující se za určitých podmínek, viry, dálková mazání dat apod.,
- neoprávněné užívání počítače či komunikačního zařízení, tj. zneužívání cizího počítače nebo počítačové technologie kompetentní obsluhou, ale v neprospěch jejího majitele, zpracováním zcela jiných úloh za úplatu pro jiného odběratele,
- neoprávněný (nelegální) přístup k datům s cílem získat utajované informace. V tomto případě však asi musíme odlišit profesionální počítačovou špionáž (vojenskou, hospodářskou, politickou apod.) od působení tzv. hackerů. Jejich cílem je pronikání vlastních schopností k prolomení ochrany a většinou nikoli materiální zisk spočívající v získání obsahu utajovaných informací. To je zájmem profesionálů. Nevylučujeme však, že činnost hackerů může být spojena s jinou trestnou činností, nebo využita jinými subjekty,
- krádež technických prostředků, tj. počítače, jeho příslušenství, programového vybavení, komunikačního zařízení i vlastních dat. Prostá krádež je jasná, motiv a cíl může odhadnout a zjistit. Složitější je to s okopírováním programů nebo dat. Jedná se spíše o počítačové pirátství, mimochodem u nás značně rozšířené, zejména mezi amatéry, ale i v profesionální sféře,
- úmyslná změna v programech a datech (eventuálně i v technickém zapojení), vložení virů, jiných programů, počítačová defraudace apod.,
- zneužití počítačových prostředků k páchání jiné trestné činnosti, tzn. neoprávněná a úmyslná manipulace s daty, např. stavy ve skladu, tržby, nemocenské pojištění, úprava dokladů apod. Tohoto způsobu se využívá snadněji než při úpravě dokladů papírových,
- jiné podvody páchané v souvislosti s výpočetní technikou, kdy např. programátor vytvoří v rámci pracovního poměru v kolektivu program a po okopírování ho prodá pod vlastním jménem.

Útočníky mohou být:

- amatéři, kteří se do informačního systému dostanou přes náhodně objevená zranitelná místa,
- hackeři, usilující prokázat své mimořádné schopnosti úmyslným prolomením ochrany systémů,
- profesionální zločinci, kteří vedou útok v podstatě „neomezenými prostředky". Například může jít o zájem cizí mocnosti (špionáž, zejména průmyslová nebo obchodní), silného konkurenčního podniku, teroristy, mafií apod.

Důsledkem útoků na informace a informační systém může být:

- znehodnocení částečné nebo úplné,
- pozměňování částečné nebo úplné (a tím znehodnocení),
- znehodnocení či zneužití krádeží,
- zneužití neoprávněným využíváním,
- zneužití podsunutím falešné informace,
- dočasná nebo trvalá ztráta informace.

4.3 Průmyslová špionáž

Nezřídka se setkáme také s různými aférami týkající se průmyslové špionáže. Tyto praktiky však zdaleka nejsou výsadou politické scény. Dnes již spadají do soukromého obchodu a podnikání. Když jde o velké peníze, každý se snaží chránit a k tomu potřebuje informace. To je ovšem velmi drahé. Průmyslová špionáž se rovněž zdaleka netýká jen velkých podniků, koncernů nebo výzkumných ústavů. Jakmile totiž podnik dosáhne určitého významu, je ve skutečnosti nezbytně nutné, a ostatně normální, aby byl neustále informován o činnosti a stavu trhu své konkurence. Aby se tato žízeň po informacích ukojila, stačí udělat jen malý krůček a už se od informací obecně známých dospěje ke zprávám získaným nedovoleným způsobem.

Nejdůležitější informací je zjistit, jaká je základní strategie konkurence. To se týká trhu, výstavby, financí. Důležité jsou rovněž informace, jaké jsou u konkurence pracovní vztahy, jaký má úvěr u banky, její trh apod. Stále větší důraz se v současnosti klade na včasné zjištění připravovaného snížení cen u konkurenční firmy a na to, jaký výrobek dá na trh v příštím roce.

Je ovšem samozřejmé, že prostředky, kterých se k získání informací použije, budovu úměrné významu toho, co je v sázce. Na nižší úrovni to může být člověk nebo skupina, ale i podnik (organizace) touží získat informace a profitovat z nich. Na vyšší

úrovni pak může pracovat specializovaný a odborně řízený aparát. Někdy se průmyslová špionáž stává speciální součástí marketingu (Vymětal, 2005). Proto ochraně dat je třeba věnovat pozornost již v období projekce informačního systému, jak bylo v předcházejících kapitolách doloženo, a samozřejmě v době jeho běžného užívaní. Obecně je ale pravdivé, že ochranná opatření jednak poněkud ztěžují činnost provozovatelů a jednak zvyšují náklady. Ty by měly být úměrné škodám, které by mohly vzniknout, a proto se obecně považuje za rozumné věnovat 10-20 % celkových nákladů na informační systém k zabezpečení jeho ochrany.

4.3.1 Únik důležitých informací

Při hodnocení jakýchkoli úniků nebo zneužití informací se ukazuje, že nejslabším článkem v celém systému ochrany je lidský faktor. Navíc ještě, nejrizikovějším faktorem úniku informací se jeví vlastní zaměstnanci. Odhaduje se, že např. 80 – 90 % případů porušení ochrany informací je způsobeno právě jimi. Pokud se přidá jejich nespokojenost, zloba nebo pomstychtivost, riziko se ještě zvyšuje. To rovněž narůstá s koncentrováním pravomocí. Například jestliže je správce informačního systému současně bezpečnostním manažerem. Jiným faktorem jsou bývalí zaměstnanci, jejichž funkce souvisela s provozem informačního systému.

Někdy mají možnost se seznamovat s řadou skutečností i externí pracovníci, protože jsou za určitých okolností bráni jako „vlastní lidé“. Toho všeho lze využívat k prolomení bezpečnosti informačního systému (Kostka, 2006). Tak např. zaměstnanec ve výpovědi nebo nespokojený, který má zlost na svého zaměstnavatele, může udělat podniku hodně škody. Stává se často „velmi silným“ anebo dokonce vstupuje „do služeb“ konkurence. Dokonce v některých případech vznikne zárodek pozdější systematické špionáže jen pouhým náhodným „únikem“ informací, kterého se pracovník neúmyslně dopustil. Nejsnadnějším a bezpochyby nejběžnějším postupem při získávání informací je zastupování a nahrazování určitého příslušného zaměstnance. Stačí např. odvést konkurentovi poslíčka a potom, za nějaký čas, mu přihrát náhradu, což ovšem bude již špion.

Je také velmi snadné dát vynálezci nebo autorovi významného projektu či objevu najevo zájem o jeho práci a nabídnout mu licenci. Při rozhovoru, který následuje, jakmile se naváže kontakt, často stačí směrovat otázky v debatě k informaci o základních principech, které chceme poznat. Jiný způsob spočívá v tom, že se inzerátem nabídnou skvělé podmínky specialistům z toho či onoho oboru a ti, kteří se přihlásí, dají potom v rozhovoru tazateli dostatek informací o věcech, které ho zajímají. Nelze konečně ani vyloučit postup, kdy firma „koupí“ hostesku, sekretářku nebo jiného

zaměstnance a přijme je, aby mluvili. Taková korupce jde často ruku v ruce s vydíráním. Člověk, kterého plánovitě přivedeme do kompromitující situace, rychle pochopí, že musí přijmout podmínky obchodu, které se nabízí. Zvláště v mafiánských kruzích mnoho variant na vybranou není.

Dle Kostky (1996, s. 2) lze hodnotu rizika pro konkrétní nebezpečí vyjádřit následující rovnicí:

RIZIKO (NEBEZPEČÍ) = ZRANITELNOST * PRAVDĚPODOBNOST * KRITIČNOST

Zranitelnost je veličina charakterizující snadnost napadnutí (osob, informací nebo majetku), dostupnost chráněného zájmu apod., *pravděpodobnost* je veličina, která charakterizuje statistickou pravděpodobnost výskytu daného nebezpečí v konkrétním místě, lokalitě, sociálním prostředí apod. a nakonec *kritičnost* je veličina charakterizující vliv dané nebezpečné události na konkrétní subjekt, zákazníka.

Charakterizuje míru dopadu události na ziskovost subjektu případně na jeho další existenci. Uvedená rovnice umožňuje kvantifikaci míry rizika a umožňuje tak seřadit jednotlivá rizika podle jejich významu, podle míry ohrožení firmy.

4.3.2 Získávání a úniky informací

Vogeltanz (1996, s. 8) uvádí, že *„Fyzická ochrana informací a prvků informačních a komunikačních technologií je důležitým aspektem, který do značné míry ovlivňuje velikost rizika ztráty, poškození, neoprávněné manipulace, nedostupnosti apod., citlivých informací, které mají životní význam pro úspěšnou ekonomickou činnost organizace.“*

Kdykoliv podnik přijímá nového zaměstnance na citlivé místo, vždy vyvstávají dvě otázky:

- nepracoval nový zaměstnanec už u konkurence,
- a nemá v konkurenčním podniku nějakého příbuzného.

Souběžně s rozšiřováním počtu zaměstnanců organizace, zapojovaných do informačního proudu na všech úrovních řízení, rostou příležitosti a možnosti destrukce informací a dat, jejich využití pro vlastní prospěch, získání vnějším subjektem a zvyšují se důsledky poruch informačních toků v neprospěch dané organizace (Vogeltanz, 1996).

Někteří lidé se specializují na to, že mění zaměstnání a přitom z podniku odnášejí spoustu důvěrných informací. Rovněž prodejní oddělení si zaslouží mimořádnou pozornost. Ve skutečnosti zde může konkurence získat i podrobnosti o

zásobování surovinami, o vlastnících, sběratelsko-dodavatelských vztazích, síti obchodních zástupců apod. Často lze předpokládat, že některé otázky kladené kupujícími mohou být zaměřeny na získávání informací pro konkurenci.

Všeobecně je důležité, aby se zaměstnanci nechlubili příliš úspěchy svého podniku, nevydávali žádné významné dokumenty a nikdy nediskutovali o důvěrných otázkách na veřejných místech. Velmi dobře informované služby v podniku jsou zpravidla pracoviště marketingu či reklamní oddělení. Tato by měla velmi pozorně sledovat vše, co má být zveřejněno prostředky masové komunikace. Rovněž se tato oddělení musí vyhýbat šíření předčasných informací, která by upozorňovala či jinak vyvolávala aktivitu konkurence.

Konečně lze upozornit na některé zásady používané na různých tiskových konferencích, trzích, veletrzích, výstavách apod. Jde zejména o to, aby tiskové konference byly připraveny a neodbočovaly od daného tématu. Důležitá sdělení tisku, rozhlasu a televize by měl prověřit právník, eventuálně bezpečnostní manažer pracující pro podnik. Nikdy by se neměly nechávat expozice nebo výstavní stánek bez dohledu odpovědného zaměstnance. Je třeba požadovat od reklamní agentury, která pro podnik pracuje, aby ničila nebo odevzdávala všechny podklady nebo dokumenty, jichž se nemá použít (fotografie, nákresy, texty apod.). Pokud jde o návštěvy, je nutné dbát, aby jména členů delegací byla známa předem a nepouštěli jsme hosty do blízkosti chráněných míst. Většina úspěšných firem získává bohatství informací např. z odborných časopisů, majetkových analýz i z výročních zpráv konkurence, protože malé společnosti nebo vývojová organizovaná oddělení odhalují více ze své technologie, než je jim milé, protože potřebují publicitu. Konkurenční společnosti mohou také sdílet informace shromážděné „třetí stranou“. Proto je nutno vedle ochrany vlastních zaměstnanců, střežit případné „špiony“, odhalovat je nějakým způsobem v jejich působišti, zabránit jim v činnosti a dohnat je k tomu, aby se dopustili nějakého činu, který bude mít za následek policejní zásah a zadržení.

Jinými zdroji jsou např. tiskové výstupy, a to zejména proto, že obsahují informace přístupné bez dalších technických prostředků. Praxe bývá taková, že použité výstupní, podkladové dokumenty často slouží pro psaní dalších poznámek, a to nejen vlastním zaměstnancům, ale často i jejich rodinám. Papír je přece drahý a proč ho kupovat, když se u nás v práci stejně vyhazuje.

Smejkal (1996, s. 15) uvádí, že *„nejsnadnějším a tedy asi nejrozšířenějším způsobem obohacování se prostřednictvím počítačů je manipulace s daty (např. stavy ve skladu, tržby, nemocenské pojištění a stavy pracovníků, plnění plánu, stav účtů atd.)*.

Ochrana zálohovacích médií, ač obsahují cenné informace, je značně podceňována, a to nejen z hlediska důvěrnosti nebo integrity, ale i z hlediska dostupnosti. Často je záložní, magnetické médium nečitelné, a tudíž i nepoužitelné nebo je uloženo na nevhodném místě, takže naopak dojde k jeho zničení či zneužití. „Vadné disky“ se vyhazují, aniž se je někdo pokusí opravit. A přitom data jsou na nich po určitou dobu zachována a tedy i dosti čitelná. Mohou být tedy přehrána.

4.3.3 Informační systém a možnost jeho napadení

Využitím systémové metodiky lze určit prvky systému ochrany vlastnictví, na nějž mohou eventuální pachatelé útočit, a to fyzické vlastnictví, nehmotné statky, osoby fyzické i právnické. *Fyzické vlastnictví*, tj. majetek, je souhrn věcí, práv a závazků, náležejících určitému subjektu, a to majetek movitý, nemovitý i činnosti a jejich produkty. *Nehmotné statky* chápeme jako práva (autorská, patentová), znalosti, vědomosti (know how), zkušenosti, záměry (plány), ale také informace a data. *Osoby fyzické*, tj. subjekty práva, mají způsobilost k právům a povinnostem, a *osobami právnickými* jsou společenské útvary (organizace), jímž byla právním řádem přiznána způsobilost vystupovat vlastním jménem v právních vztazích a mající majetkovou odpovědnost z těchto vztahů vznikající. Je to vlastně souhrn fyzickým osob tvořících vlastní organizaci se všemi právními i osobními vztahy mezi sebou a okolím.

Všechny tři prvky v systému ochrany vlastnictví jsou v dialektické jednotě. Mají mezi sebou sice různé vztahy, ale vzájemně se podmiňují a hlavně informace o nich jsou nebo mohou být předmětem zájmu nepovolaných osob. Již z toho vyplývá, že při ochraně vlastnictví je třeba zajišťovat její komplexnost a rovněž z hlediska prevence je nezbytné věnovat pozornost všem třem prvkům a vytvářet k nim současně potřebné opatření (Strategie ISCS, 2009). Vlastnictví jako vztah osob k majetku je ovšem jen jednou stránkou systému jeho ochrany. Je to jakýsi statický pohled. Osoby i majetek je třeba využívat k činnosti a vytváření dalších hodnot. Proto využijeme systémového přístupu k dalšímu rozboru.

4.3.4 Ohrožování a možnosti napadení informačního systému

Moderní doba přinesla potřebu rychlé a mnohem dokonalejší informovanosti. Elektronika musela proniknout i sem. A pronikla i v době různých skandálů, kdy např. firma dodávající odposlouchávací technické zařízení, které možnost použití odposlechu prvním podnikatelem eliminovala. Již zmíněný konkurenční boj na jakékoli úrovni podnikání v nových podmínkách však přinesl fakt, že informace jsou zbožím. Platí se

nejen za jejich získání, ale rovněž za jejich ochranu stejně jako se platí za jiné zboží (Koch, 2010).

V současné době se drtivá většina zpracovaných informací získává technickými prostředky, zejména pomocí satelitů, pozemních odposlouchávacích či pozorovacích stanovišť, až po užití této techniky jednotlivci. Zbytek je doplňován klasickými formami získávání informací, tj. prostřednictvím osob, jejich prací uvnitř zájmových objektů (zcizování informací opisem, kopírováním, vlastním odposlechem atd.)

Z hlediska způsobu ohrožení informačního systému se rozlišují dva druhy:

a) úmyslné – sem patří zejména vyzvídání, odposlouchávání, tzv. počítačové pirátství (pronikání do informačního systému s cílem data získat nebo je změnit, eventuálně je zničit), ohrožení systémů počítačovými viry aj. V rámci trestné činnosti na intonačních systémech automatizovaných hovoříme o počítačové kriminalitě.

b) nedbalostí – způsobené rovněž lidským faktorem (např. chybami operátorů), chybnými vstupními daty, chybami programového vybavení, selháním hardware, prostředím (výpadek proudu, přírodní katastrofa aj.)

Další rozvoj a rozšiřování užití výpočetní techniky, které vede k vytváření a užívání počítačových sítí obzvláště nese s sebou nutnost ochrany informací. V dnešním globalizovaném světě, kde počítačové sítě jsou již bohatě rozvinuty, jsou osobní počítače chápány čím dál více jako prostředky všestranné komunikace. A to nejen uvnitř státu, ale i na mezinárodní úrovni. Prakticky kdokoli, kdo má osobní počítač se může zapojit do sítě a účastnit s „elektronické“ diskuse po komunikačních kanálech. Vytvářejí se tak vlastně jakési diskusní kluby na nejrůznější témata.

Zapojení se do počítačových sítí neomezuje vzdálenost, ani odbornost či tématický zájem. Jejich vznik je spontánní, ale podstatné je, že již jen samotné sledování diskusí, zejména odborně zaměřených (např. o ochraně informací či pronikání do informačního systému) je obrovským informačním přínosem. Na zadanou otázku totiž přicházejí odpovědi prakticky z celého světa. Získávají se tak celosvětové zkušenosti. Kontakt s touto sítí je možný prakticky ze všech míst naší republiky. Omezovat nás mohou pouze finanční prostředky, nikoli technické (Požár, 2010).

Výše uvedené prvky systému činnosti, nebo z jiného pohledu informačního systému, mohou být napadány různými způsoby. Ty lze dělit na dva základní:

a) fyzicky – působením silou, jehož následkem je poranění či smrt osoby, poškození nebo ztráta věci, zařízení, produktů, informací,

b) intelektuálně – napadání slovní, činnosti protiprávní (např. poškozování obchodního jména, pomluva, aj.), získání informací k vlastnímu prospěchu apod.

Výše byl popsán útok pachatele z vnějšího prostředí. Je třeba ale také uvažovat o útoku z prostředí vnitřního. Ten bude uskutečňovat vždy osoba – zaměstnanec v podobě vyzrazování. V daném okamžiku nekomplikujme vztahy zavedením zprostředkovatele (nastrčeného prostředníka), ale zde podtrhujeme významnost lidského faktoru. Hlavním činitelem, který ohrozí nebo napadne informační systém nebo jeho produkt je člověk, který:

- uskutečňuje produktivní (materiální i nemateriální) činnost,
- daný systém napadá fyzicky nebo intelektuálně,
- využívá nebo zneužívá jeho výsledků opět v podobě materiální nebo i informační.

Motivace pachatele je však problém sám o sobě, který je třeba vykládat i z psychologického hlediska.

4.3.5 Ochrana informací a informačního systému

Ochrana informačních systémů je upravena zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a dále též vyhláškou č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy Souhlasíme-li s pojetím ochrany vlastnictví, jak bylo vyjádřeno výše, pak komplex ochrany informačního systému by měl zahrnovat:

a) bezpečnost osob, a to bezpečnost klientů i vlastního personálu při:

- násilných případech (teror, loupež)
- požáru
- haváriích a katastrofách
- běžné činnosti (bezpečnost práce)

b) bezpečnost majetku, a to majetku klientů i vlastního při:

- násilných případech
- nenásilných případech (krádeže)
- požáru
- haváriích a katastrofách
- běžné činnosti

c) bezpečnost informací, a to informací o klientech i vlastních při:

- narušení spolehlivostních faktorů
- neúmyslném působení vlastního personálu
- úmyslném působení vlastního personálu a osob

Ochranou informačního systému rozumíme komplex organizačních (administrativních i režimových), technických, programových a sociálně-personálních opatření s cílem minimalizace možných ztrát informací v daném systému vznikajících a obíhajících. *„S rozsáhlostí informačního systému roste počet napadnutelných míst a ta původní zůstávají“* (Němejc, 1996, s. 18).

V jakémkoli podniku mohou vznikat následující druhy škod:

a) přímé ztráty – vyzrazení obchodních záměrů, výsledku výzkumu či možnosti uplatnění výsledku, důsledky nelegálních informací či obnovení výroby v důsledku nuceného přerušení výroby či expedice zboží aj. Tedy škody nejen v materiální, ale i v duchovní podobě.
b) nepřímé ztráty – ztráty dobrého jména podniku, protože nebyly dodrženy dohodnuté podmínky a tím finanční ztráty aj.

V rámci ochrany informačního systému je třeba dbát na ochranu nejen dat, ale i programů, které zpracování dat, řízení výroby či celého podniku ovlivňují. Proto ochraně veškerého vlastnictví je třeba věnovat pozornost již v období projekce informačního systému a samozřejmě v době jeho běžného užívání. Je také pravdou, že ochranná opatření jednak poněkud ztěžují činnost provozovatelů a jednak zvyšují náklady. Ty by tedy měly být dle Němejce (1996) úměrné škodám, které by mohly vzniknout, a proto se obecně považuje za rozumné věnovat 10-20 % celkových nákladů na informační systém k zabezpečení jeho ochrany.

Problémem je ovšem stanovení hodnoty a ceny informací dat uložených nebo obíhajících v informačním systému. *„Z pohledu bezpečnosti není možné implementovat a udržovat úspěšný bezpečnostní program, jestliže nejsou předem identifikována aktiva organizace“* (Pekárek, 2007, s. 73). Fyzická a softwarová aktiva se nejčastěji oceňují podle jejich ceny, přesněji řečeno, ceny jejich náhrady v případě poškození nebo zničení. Data však tímto způsobem oceňovat nelze. Lze sice připustit, že je možné ocenit například nějakou databázi tak, že vyčíslíme náklady na její rekonstrukci v případě zničení. To je sice možné a dokonce potřebné udělat, v žádném případě to však neodráží všechna hlediska jejich hodnoty. Jedná se především o požadovanou dostupnost, věrohodnost a důvěrnost dat. Uvedené hodnoty je nutno ocenit jinak. Nejlépe je to

možné udělat s využitím hodnocení následků různých hledisek hrozeb. Těmito následky může být například ztráta dobrého jména, ohrožení bezpečnosti osob, porušení právních norem, porušení důvěrnosti osobních údajů, vyzrazení obchodního tajemství, přímé finanční ztráty a v neposlední řadě i přerušení aktivit organizace tím, že služby informačního systému nebudou dostupné.

Uvedené hodnocení však nelze provést exaktně, a musí být využito srovnávacích testů na bázi expertního průzkumu. K tomu je třeba získat názory různých respondentů opírající se o společnou stupnici hodnot (shodné scénáře). Výsledkem jsou pak určité, řekněme bodové hodnoty umožňující nejméně uspořádat datová aktiva podle jejich významnosti (citlivost) a tedy i ceny. Podaří-li se navíc vhodným způsobem porovnat finanční vyjádření fyzických a softwarových aktiv s výsledky expertního hodnocení datových aktiv, pak nejenže lze uspořádat všechna aktiva, ale také vyjádřit finančně cenu veškerých, tedy i datových aktiv, což by jinak nebylo možné. Softwarová aktiva je možné hodnotit kombinací obou uvedených způsobů.

Všeobecná ochranná opatření by měla zahrnovat (Strategie ISCS, 2009):

- vytváření celkové ochranné (bezpečnostní) politiky podniku či instituce,
- zajišťování fyzické ochrany objektů, majetku (fyzického vlastnictví), osob a informací (nehmotných statků),
- programově-technická opatření v automatizovaných informačních systémech, týkající se software, hardware, řádné vedení potřebné dokumentace, protivirová opatření apod.,
- organizačně-personální opatření, k nimž patří např. přesné a jasné vymezení funkcí, kompetence, režimu na pracovištích, úrovně pracovníků a další.

Z hlediska ochrany jednotlivých objektů (prvků systému) pak lze rozlišovat následující druhy opatření:

- organizační (organizační řád, pracovní řád, technologické postupy),
- administrativní (předpisy, pokyny, směrnice apod.),
- režimové (pokyny pro činnost v krizových situacích),
- právní (preventivní, represivní),
- fyzické (předpisy stavební, elektronické, vzduchotechnické a další)
- technická (pro HW i SW),
- personální (pro výběr a výchovu personálu) a sociálně-psychologické.

To vše můžeme shrnout pod všeobecný pojem bezpečnostní management, tj. komplexní řízení ochrany vlastnictví.

5 Příčiny a důvody úniku, ztrát a zneužívání informací

Z obsahu předcházejících kapitol je možné vyvodit, že informaci chápeme jako nehmotný statek, zboží či výrobek, „surovinový zdroj“, výrobní nástroj, projekt dalšího postupu, databanku, systém komunikace a konečně i jako objekt, na jehož užívání nebo ochranu má podle Listiny základních práv a svobod (nebo Ústavy) právo každý občan. Současně bereme v úvahu, že informace může být získávána a využívána racionálním, zákonným či nekonfliktním způsobem, ale také na druhé straně, že se může stát objektem, předmětem a nástrojem zločinu. Je třeba si rovněž uvědomit, že informace je základní podmínkou fungování všech systémů, tj. biologických, sociálních, ekonomických, právních, politických, mezinárodních, vědeckých, řídících, technických apod. Proto také ochrana informací je značně složitější a obtížnější než fyzická a technická ochrana objektů a osob. Její nehmotný charakter a individuální variabilita, zvyšuje možnosti úniku, manipulace, rychlé změny obsahu i „majitele“, deformace a zneužití.

Z tohoto důvodu je užitečné zabývat se těmito otázkami i z hlediska kriminologie jako vědy o podstatě zločinu, jeho stavu, struktuře a dynamice, příčinách a podmínkách vzniku a přežívání, kriminogenní osobnosti (pachatele, ale i oběti) a způsobech jejího překonávání (formou prevence i represe). Kriminologie se zabývá relevantních skutečností a informací, stop a důkazů, a to s cílem jejich dalšího využití především v trestním procesu (Ivanka, 2009).

Je třeba vycházet ze skutečnosti, že ve společnosti existují určité sociálně-patologické jevy, včetně zločinnosti (kriminality). Ty jsou charakterizovány touhou i rozhodnutím zmocnit se, zneužít, poškodit či zničit materiální i duchovní vlastnictví, omezit či zcela znemožnit uplatňování základních práv a svobod občanů.

Vedle této úmyslné a často cílevědomé činnosti některých deviantních jednotlivců a skupin, vznikají značné škody občanům a celé společnosti i v důsledku neodpovědnosti, nezájmu, nedbalosti, lhostejnosti, alibizmu a dalších negativních sociálně-psychologických jevů a vlastností. *„V současnosti se řada útoků vyznačuje nízkou technickou náročností, ale vysokou technickou zdatností útočníků“* (Vokůrková, 2006). O tom, jestli se jedná o činy trestné nebo přestupky rozhoduje úmysl, intenzita a výše škody.

Z kriminologického hlediska je zajímavé věnovat se také vztahu množství a kvality informací k příčinám a podmínkám kriminality různého druhu a v různých oblastech. Tedy projevům poruchového, nežádoucího fungování systémů společenských, právních, vědeckých, politických, technických apod.

Lze říci, že nedostatek informací může u lidí, ať jednotlivců, skupin nebo celé společnosti vyvolat stress, frustraci. Obecně hlad po informacích. Tyto stavy jsou značně významnou příčinou i podmínkou opatřování si informací, mimo dalších věcí a prostředků, „za každou cenu“, tj. krádežemi, loupežemi, nákupní horečkou, „vekslováním“, zneužíváním postavení nebo věcí apod. Nedostatek informací o fungování různých systémů pak zaviňuje poruchy v provozu a také havárie. Nedostatek a nesrozumitelnost právních a řídicích informací může být příčinou a podmínkou nezákonnosti, bezpráví a zneužívání postavení. To se v podstatě vztahuje i na neurčitost informací.

Rozpornost nebo různé deformace informací mají zpravidla za následek narušení základních informačních a organizačních vazeb ve společnosti a tím vznik příčin a podmínek zločinnosti (Porada, 1998). Tato rozpornost a deformace ovšem může být i úmyslně zneužívána v politickém boji, dezorientaci v pracovních i dalších sociálních skupinách. Zneužívá se často i v reklamě (nekalá soutěž, klamavá reklama apod.).

Rovněž tak může vyvolávat příčiny a podmínky kriminality přemíra (nadbytek) informací. Nejen, že může dojít k zahlcení informačního systému a tím narušení normálního chodu, ale také k jeho havárii. Ve společnosti (zejména při masovém a neustálém působení prostředků masové informace) může docházet jednak k tzv. „vymývání mozků“ (brainwashing), tj. vytváření si předpokladů k manipulaci s lidmi (ohrožování základních práv). Na druhé straně pak přílišná frekvence některých informací, může mít za následek růst mravnostní, násilné, hospodářské i jiné kriminality (viz působení televizních seriálů, akčních či pornofilmů, apod.), včetně kriminality „informační“.

Množství a kvalita informací může konečně vytvářet příčiny a podmínky pro dezorientaci systémů (zejména jedinců, skupin i celé společnosti) a pro davové chování a paniku. Ty pak mají velmi často za následek zejména násilnou, majetkovou a hospodářskou kriminalitu. Z uvedeného vyplývá, že předmětem ochrany musí být i kvantitativní a kvalitativní stránky informace. Čírtková (2006) uvádí, že… „vazba *mezi socializací a anonymitou poškozených - dobře socializovaní pachatelé poškozují spíše anonymní oběti, u defektně socializovaných je tomu naopak, a vazba mezi socializací a výší zisku z kriminální činnosti - pachatelé s nedostatečnou socializací jsou připraveni ke kriminálnímu jednání i u vyhlídek na nižší kořist.“*

Výše uvedené faktory se mohou stát tedy bezprostředními příčinami zločinnosti v oblasti informací anebo podmínkami, které páchání zločinu v této oblasti umožňují nebo usnadňují. Při tomto populárním vysvětlení základních příčin a podmínek

ohrožujících informaci ovšem nelze vyloučit, že některé z nich mohou mít objektivní charakter. Tedy, že jsou nezávislé na vědomí nebo vůli lidí, což jsou dosud neprobádané jevy a procesy, A naopak, že jiné jsou zcela závislé na vůli, ochotě, poznání, jednání lidí tedy subjektivního charakteru.

5.1 Informace a zločin

Ohrožení informací a zločinnost v této oblasti může mít různou podobu. Může to být důsledek živelných, technologických, technických či programových a organizačních chyb a faktorů. Hovoří-li se o zločinu v této oblasti, je tím myšleno úmyslné, vědomé nebo i nedbalostní jednání určitého subjektu (jedince, skupiny, organizace atp.), jehož následky jsou škody určitého rozsahu. Ty pak mohou být jak duchovní, fyzické či materiální podoby. V této kapitole, vzhledem k poslání a rozsahu nebudu zvláště uvádět přestupky, ale jen vybrané trestné činy, vyjmenované v zákonu č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „trestní zákoník“), v nichž informace působí nebo vystupují jednou jako objekt či předmět, jindy jako nástroj zločinu.

Každý náš občan, a to jak fyzické osoby, tak i právnické, je také spotřebitelem informací. Proto i v této oblasti může docházet k trestným činům různé povahy a nebezpečnosti v oblasti poškozování spotřebitele ve smyslu ust. § 253 trestního zákoníku. Pachatel poškozuje spotřebitele tak, že mu neposkytne informace dostatečně kvalitní nebo úplné, zatají významné informace, požaduje nepřiměřené ceny. To se může projevit nejen v nízké kvalitě informačních nosičů (médií), neposkytnuté možnosti reklamace a záruky, ale také kladení nepřiměřených překážek při vyžadování a využívání osobních údajů a nepřiměřené (neoprávněné) cenzuře hromadných sdělovacích prostředků. Takže informace se stává jednak předmětem, jednak nástrojem trestného činu.

Významným příkladem, kdy se informace může stát nástrojem trestného činu, jsou případy porušení předpisů o pravidlech hospodářské soutěže (§ 248 trestního zákoníku). Jde o jednání, které je v rozporu s normami a předpisy upravujícími soutěž v hospodářském styku nebo zvyklostmi soutěže i v jiných oblastech společenského života, které poškozuje dobrou pověst, ohrožuje chod nebo rozvoj podniku (organizace) soutěžitele. Může jít o jakékoli činy, které by mohly způsobit záměnu s podnikem a jeho výrobky, obchodní či jinou činnost soutěžitele. Rovněž tak se jedná o podání falešných informací (údajů) při provozování obchodu, které by mohly poškodit pověst podniku, výrobků a činnosti soutěžitele. Konečně jde i o používání údajů a tvrzení, které by

mohly veřejnost uvádět v omyl (nekalá, klamavá reklama), hanění a pomlouvání výrobků atp.

Naproti tomu typickým příkladem, kdy informace je předmětem trestného činu krádeže ve smyslu ust. § 205 trestního zákoníku, a to jak při krádeži prosté či vloupáním nebo loupeži dle ust. § 173 trestního zákoníku. Podstatou tohoto činu je, že pachatel užije násilí nebo pohrůžky bezprostředního násilí v úmyslu zmocnit se cizí věci. V našem případě to může být krádež informací v různé podobě a na různých médiích. Podobně se může stát informace objektem trestného činu v případě zpronevěry dle § 206 trestního zákoníku, kdy pachatel si přisvojí cizí věc (informaci nebo nosič, systém, která mu byla svěřována a způsobí škodu na cizím majetku. Zvláště nebezpečné je, když tento čin spáchá osoba, která má povinnost hájit zájmy poškozeného.

Informace jako nástroje trestného činu se často používá v různých případech podvodu (§ 209 trestního zákoníku). Pachatel zde sebe či jiného ke škodě cizího majetku obohatí tím, že uvede někoho v omyl nebo využije něčího omylu a způsobí tak jinému škodu. Častým jevem, jehož podstatou je zneužití dílčích, nepravdivých či zkreslených informací, je pomluva ve smyslu ust. § 184 trestního zákoníku. V tomto případě pachatel sděluje nepravdivé údaje, které způsobují, že je ohrožována vážnost občana u spoluobčanů, mohou jej poškodit v zaměstnání, narušit jeho rodinné vztahy nebo mu způsobit jinou vážnou újmu. Podobně se může pachatel dopustit takového činu tím, že uvedenou nepravdivou informaci vydá tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

Z hlediska zneužívání informací je rovněž vážným činem šíření poplašné zprávy ve smyslu ust. § 357 trestního zákoníku. Poplašnou zprávou (informací) se rozumí taková zpráva, která je svým obsahem způsobilá vyvolat nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa tím, že rozšiřuje poplašnou zprávu, která je nepravdivá. Trestným činem je úmyslné rozšiřování této falešné informace. Rovněž se takového činu dopouští ten, kdo poplašnou zprávu sdělí podniku, organizaci, policejnímu či jinému státnímu orgánu nebo hromadnému sdělovacímu prostředku. Je s podivem, přece však reálné, že informace se může stát prostředkem i nástrojem zločinu i v oblastech a činnostech, kde pobíhají procesy boje proti zločinnosti.

Takové případy se nezřídka stávají při poškozování cizích práv dle ust. § 181 trestního zákoníku. K tomuto dochází zpravidla v tom případě, že pachatel uvede někoho v omyl, využije něčího omylu anebo se vydává při činu za veřejného činitele. Zákonem jsou chráněna zejména nemajetková práva jednotlivce např. v oblasti rodinných vztahů, pracovních práv, v podnikání apod. Bohužel se s takovými případy

můžeme setkat velmi často a pachateli mohou být vedoucí pracovníci, personalisté, podnikatelé úředníci, ale i policisté, kteří úmyslně zkreslují požadované vysvětlení nebo nejsou ochotni splnit požadované oprávněné úkony. Mohou to být i různí „proradci“, kteří sledují především své osobní zájmy.

Podobně dochází ke zneužití informací (k jejich deformaci) v případech křivého obvinění dle ust. § 345 trestního zákoníku a křivé výpovědi a nepravdivých znaleckých posudků podle ust. § 346 trestního zákoníku. Základem je zde úmysl pachatele nebo účastníka jednání lživě obvinit jiného s cílem způsobit jeho stíhání či způsobit mu škodu. Podstatou tohoto trestného činu je, že občan oznámí orgánům činným v trestním řízení, jiné fyzické či právnické osobě, že se dopustily nebo dopouští činností, které jsou v rozporu se zákonem. Může však jít také o sdělení pochybností jiným orgánům nebo i soukromým osobám, jestliže pachatel jedná se záměrem, aby se toto sdělení dostalo do rukou orgánů činných v trestním řízení.

Není rozhodující, za jakých okolností a jakou formou je oznámení či sdělení učiněno. Může se tak stát i v rámci vlastní obhajoby. Je lhostejné, jestli pachatel jednal z vlastního popudu nebo své sdělení učinil z podnětu někoho jiného. Přitom však obvinění musí být lživé a musí směrovat vůči konkrétní osobě (fyzické či právnické). Není třeba, aby tyto osoba byla označena jménem. Stačí uvedení okolností, z nichž lze spolehlivě dovodit, o kterou konkrétní osobu se jedná. Tedy křivé obvinění může směrovat i vůči více osobám.

Křivé výpovědi a nepravdivého znaleckého posudku se pak může dopustit svědek, tlumočník nebo znalec před soudem, státním zástupcem, policejním orgánem, vyšetřovatelem, vyšetřovací komisí atd. Čin spáchá tím, že uvede nepravdu, neúplné nebo nepravdivé informace o okolnosti, která má význam pro zjištění jeho rozhodnutí, nebo takovou okolnost (informaci) zamlčí a tím způsobí škody.

V řadě případů bývají informace získávány, zpracovávány a zneužívány za účelem vydírání (§ 175 trestního zákoníku). Podstatou tohoto zločinu je, že pachatel násilím nebo pod pohrůžkou bezprostředního násilí nebo jiné těžké újmy nutí jinou osobu, aby něco konala, opominula nebo trpěla. Právě ve vydírání se stávají získané a zneužité informace nejčastějším nástrojem zločinu. Tyto informace jsou často opatřovány nelegálním způsobem, dovedně zkreslovány a zneužívány v obchodním styku, v politice i při nekalé soutěži. Právě zde je zvýrazněn požadavek ochrany informace před únikem a zneužitím.

Zvláštní pozornost zasluhují otázky zločinnosti při tvorbě a fungování a využívání informačních systémů, informačních vazeb a prvků, nosičů informací a jejich

rozšiřování. Často dochází k poškozování a zneužívání záznamu na nosiči informací. Trestný čin spočívá v tom, že pachatel získá (často i oprávněně) přístup k nosiči informací, informace však neoprávněně rozmnožuje při nedodržení kvality, popř. pozmění částečně její obsah. Rovněž tak, jestliže nosič záměrně poškodí nebo zcela zničí, učiní neupotřebitelným, učiní zásah do technického nebo programového vybavení informačního systému (počítače) s cílem způsobit jinému škodu anebo získat neoprávněný prospěch (§ 230, 231 a 232 trestního zákoníku).

K ohrožení informačních zdrojů, nosičů, systémů a vazeb dochází také v souvislosti s porušením tajemství dopravovaných zpráv (§ 182 trestního zákoníku), ohrožením utajované informace (§ 317, 318 trestního zákoníku) a zneužití informace a postavení v obchodním styku (§ 255 trestního zákoníku). Podstatnou zločinnosti je zde to, že kdo v úmyslu opatřit sobě nebo jinému výhodu nebo prospěch neoprávněně užije informace dosud nikoli veřejně přístupné, kterou získal při výkonu svého zaměstnání, povolání, postavení nebo své funkce a jejíž zveřejnění podstatně ovlivňuje rozhodování v obchodním styku, a uskuteční nebo dá podnět k uskutečnění smlouvy nebo operace na regulovaném trhu s investičními nástroji nebo na organizovaném trhu se zbožím, bude potrestán. V této souvislosti lze také uvažovat o zneužívání tzv. „strategických informací“ a vazbách na organizovaný zločin ve smyslu § 107 trestního zákoníku, před kterým nejsou chráněni ani významní státní a političtí činitelé a osoby úřední.

Špionáž, a to jak hospodářská, průmyslová, technická vědecká, tak politická a vojenská, je snad nejvážnější a nejsložitější formou zločinnosti v oblasti informačních systémů. Zde se ovšem jedná i využívání speciálních a komplexních způsobů získávání informací, informačních kombinací a her, i vytváření složitých způsobů utajování informací a jejich přenosu. Také prostředky ochrany jsou zde zpravidla velmi složité a komplexní.

Dále také nelze při výčtu trestných činů v oblasti informací zcela přehlédnout některé zdánlivě okrajové záležitosti, jako je porušování autorských práv (§ 270 trestního zákoníku) a neoprávněné nakládání s osobními údaji (§ 180 trestního zákoníku). V případě porušování autorských práv jde zejména o nerespektování či zamlčování autora jako zdroje informací nebo neoprávněné rozmnožování nosičů informací (Šámal, 2009).

Ochrana osobních dat je jedním z práv občanů. Jestliže někdo neoprávněně sdělí nebo zpřístupní údaje o jiném shromážděné v souvislosti s výkonem veřejné správy, svého povolání, zaměstnání nebo funkce, dopouští se trestného činu. Totéž platí i poskytne-li tyto uniformace nebo údaje neoprávněně prostředkům hromadné informace.

Dále je též podstatné uvést, že možnosti vzniku zločinu v oblasti práce s informacemi jsou zde uvedeny z tohoto důvodu, že každý občan, fyzická či právnická osoba se může stát jeho obětí. Ale při absenci alespoň obecné znalosti tohoto přehledu se také může, třeba i nevědomky, stát pachatelem nebo spolupachatelem.

5.2 Příčiny a podmínky zločinnosti v oblasti práce s informacemi

Vznik a přežívání (někdy i nové jevy) zločinnosti v oblasti práce s informace, jsou zvláště v této oblasti charakterizovány složitými kauzálními vazbami. Přitom za příčinu považujeme dlouhodobě či momentální působení různých vnějších i vnitřních faktorů na jednotlivce, skupinu či společnost vyvolávajících tomu odpovídající chování, jednání či reakci. Vedle toho za podmínku lze považovat určitou situaci, která umožňuje nebo ztěžuje, či dokonce znemožňuje určité chování, jednání nebo skutky. Při zkoumání zločinnosti však zejména vidíme úlohu aktivního subjektu (člověka jednice, skupiny, společnosti), jehož chování není zcela deterministické, tedy zákonité či předpověditelné, a také ovlivňuje charakter, sílu a rozsah následku. Tyto skutečnosti musíme brát v úvahu na rozdíl od projektování a modelování technických či matematických (kybernetických) systémů a jejich chování.

Bez pochopení následujících příčinných souvislostí, nelze úspěšně ani koncipovat prevenci zločinnost v oblasti informací, tím méně promýšlet efektivní ochranu informací. I když nelze při fungování lidského organismu, jak uvádí Brechlerová (2007), vyloučit řadu „vnitřních informačních procesů“, např. biologických, filozofických apod., vycházíme ze skutečnosti, že v převážné a podstatné části lidského života (zejména duchovního) probíhají informační procesy v oblasti psychiky. Tím se člověk také podstatně liší od jiných živých i neživých systémů.

Potřeba informací je tedy jednou ze základních potřeb existence a činnosti člověka. Její upokojování nebo neuspokojování může být jednou ze základních příčin zločinnosti v oblasti práce s informacemi. Pochopitelně, že zde působí řada psychických faktorů jako je úroveň vnímání, myšlení (intelekt), schopnost postihnout podstatu, smysl a význam informací jako podnětu či schopnosti získávání a využívání informací, typ temperamentu, vůle, charakteru. Pod vlivem shora uvedených faktorů může vzniknout napětí nebo frustrace (hlad po informaci). Jedinec se pak rozhoduje, že si opatří informace za každou cenu, zvláště vidí-li možnost výhodného uplatnění této nebo jiné informace. *„Nejsnazší útok je ve velké organizaci, kde se lidé navzájem neznají a kde je možno třeba zavolat novému zaměstnanci a přes něj se pokusit získat informace“* (Brechlerová, 2007).

Na druhé straně pak přemíra informací (inflace) snižuje schopnost výběru (diferenciace, selekce) a tím zvyšuje nebezpečí neopatrného zacházení a zneužití a někdy i k neracionálnímu rozšiřování okruhu nositelů informací a zvyšování nebezpečí úniku k nežádoucím subjektům.

Nelze konečně přehlédnout i některé volní vlastnosti jedinců, jejich nedostatečnou vůli udržet informace v tajnosti a podléhajících přílišné sdílnosti. Jako nežádoucí podmínky z hlediska psychologického je přílišná benevolence při zjišťování „drobných nedostatků“ v práci s informacemi, nedostatečná režimová opatření vyplývající z nepěstování a neupevňování návyků, slabá personální práce při výběru nositelů závažných informací apod. Nelze podcenit ani nebezpečí vyplývající z nedodržování poznatků psychologie práce, které mohou mít za následek únik, deformace a zneužívání informací. Vzhledem ke společenskému charakteru člověka můžeme také hovořit o některých sociálně-psychologických příčinách a podmínkách vzniku zločinu v informačních systémech a procesech. Důvodem zde může v prvé řadě být neuspokojení (frustrace) sociálně-psychologických potřeb jednotlivců či skupin. Jde zejména o uplatnění akceptování osobnosti ze strany jiných lidí nebo skupin, potřeby uznání, sociální komunikace, seberealizace (potřeby vyniknout), apod. (Přibyl, 2009).

Trvalejší neuspokojování uvedených potřeb pak může vyvolat touhu po deformování či účelovém informování v podobě pomluv, poškozování cizích práv, vydírání, podvodu, někdy i poškozování cizí věci (např. grafity), nekalé soutěže, klamavé reklamy atd. Přibyl (2009) uvádí, že… „zhruba *dvě třetiny propuštěných zaměstnanců mají přístup do systémů i po ukončení pracovního poměru. Přitom by měli být bez pardonu odstřiženi v minutě rozvázání pracovního poměru…“* Neukojení některých sociálně psychologických potřeb však může vést u některých jedinců ke zvýšené potřebě sdílnosti. Potřebují si postěžovat, ohromit svými informacemi (chlubivost) a tím se dopouštějí vyzrazování informací. Nebo se také příliš podřizují autoritě. Tím vzniká další možnost zneužívání v informační činnosti (vyzvídání, špionáž apod.). Rovněž tak snížená míra solidarity s vedením organizace a konfliktní situace s pracovním kolektivem mohou vést k úniku a zneužívání informací jako k aktu lhostejnosti či pomsty.

Mezi významnými sociologickými příčinami a podmínkami kriminality jsou:

- zařazení (pozice a role) jednice ve skupině a společnosti,
- složení, velikost, charakter formálních a neformálních skupin (cíle a její potřeby),
- charakter a kvalita vůdců (jejich formální i neformální autorita).

5.3 Vliv lidského faktoru z kriminologického hlediska

Výchozím momentem úlohy lidského faktoru je určitá analýza vývoje (minulosti) osobnosti z hlediska jeho sociálního programu a zkušenosti, které mohou být motivací ke zločinu. Jestliže člověk prožíval dosud svůj život v podmínkách, kdy nebyly respektovány základní společenské hodnoty (jako je zejména vztah k vlastnictví, vzájemná důvěra a solidarita, pravdomluvnost a osobní odpovědnost, ochrana práv jiných), pak je potenciální možnost, že takto bude zacházet s informacemi, které mu budou zpřístupněny. Rovněž tak, jestliže jeho sociální program a zkušenost výrazně akcentuje snahu obohatit se, preferovat otázku „Co z toho bude mít?“, snahu za každou cenu odstranit konkurenci atp., skrývá se v něm nebezpečí zneužívání informací.

Obdobně důležitou je kriminální minulost osobnosti, a to zejména z hlediska její občanské a trestní bezúhonnosti. Zda se již osoba nedopustila nějakého nežádoucího činu na přecházejícím působišti z nedbalosti nebo úmyslně. Zda nešlo o činy spojené s ochranou informací, zda dokonce nejde o recidivistu v oblasti poškozování a zneužívání informací. Za šedesáti až osmdesáti procenty incidentů v informačních systémech stojí interní uživatelé (Přibyl, 2009)

Častá fluktuace pracovníků na úseku informací může vytvořit podmínky zanášení informačních šumů do pracovních kolektivů a do informačních systémů. Takový stav pracovní morálky umožňuje danému pracovníkovi snáze a kvalifikovaně proniknout do informačního systému, zneužít nebo zničit jej. Došlo zde k získání nežádoucí „kvalifikace“, která může být spíše na škodu informacím a informačním systémům. Základem vzniku příčiny a podmínky se může stát i nedokonalá personální práce při výběru, rozmisťování a hodnocení lidí.

5.4 Preventivní opatření ve fázi projektování informační činnosti

Ochrana informací z hlediska kvality, deformací, úniku či zneužití má ve fázi projektování nesmírný význam. Podcenění může znamenat zcizení celého projektu nebo jeho základní myšlenky. Dle Kudělky (2009) *„Informace jsou jedním z nejcennějších aktiv firmy, a proto kontrola přístupu k těmto informacím tvoří důležitou součást každodenních operací organizace.“* To by mohlo vést k zavedení projektu s předstihem ze strany konkurence jeho zpochybnění nebo deformaci v neprospěch autora

(zadavatele). Hlavním subjektem všech preventivních opatření je tedy autor nebo zadavatel projektu.

Východiskem je sběr, soustředění a uspořádání vstupních informací, při kterém musíme dbát (případně si ověřit) pravdivosti a hodnoty, použitelnosti, případně aktuálnosti atd. Je třeba vyvarovat se přílišné důvěřivosti a podléhání nadšení (nezdravý optimismus). Ne všechna nabízená know-how jsou reálná a dobrá. Ve většině navrhovaných opatření hraje tedy rozhodující úlohu zadavatel nebo autor projektu. Vstupní informace je třeba doplnit o průzkum trhu a informace o činnosti konkurence. Jinak můžeme být ohrožen celkový úspěch projektu.

Je vhodné vybírat základní, ne příliš široký okruh projektantů a všem předávat jinak celkový ideový projekt, jednak diferencovaně nezbytné dílčí, konkrétní informace. Je tomu tak proto, aby rozsah informací u jednotlivce nebyl příliš velký, jehož pomocí by mohl proniknout do hloubky projektu, ale také, aby celková koncepční práce zůstala v rukou vedoucího – zakladatele projektu. Tím se sníží riziko úniku informací. Je i vhodné již nyní řešit otázky hmotné či jiné zainteresovanosti projektů a jejich motivaci pro solidaritu se zakladatelem či iniciátorem projektu. Tvrdíková (2001) uvádí, že *„Volba přístupu k projektování, vhodného pro konkrétní podmínky v dané firmě či instituci, hraje také významnou roli. Právě zvolený přístup k projektování informačního systému může ovlivnit konkurenceschopnost firmy, protože rozhoduje o rychlosti zavedení změn.“*

Důležité je zamezovat frustraci projektů z nedostatku informací na straně jedné a na druhé straně nepřipouštět přílišné „zahlcení“ informacemi, které by mohlo mít za následek podcenění nebo únik informací z nedbalosti. Nutno provádět odpovědnou selekci a třídění nezbytných informací pro projektování – postupně zavazovat projektanty povinností mlčení o informacích, které zpracovávají a související s projektem. *„Kvalita ošetření lidského faktoru v návrhu ovlivňuje produktivitu člověka, který pracuje s informačními technologiemi, a spolehlivost celého informačního systému, rozhoduje o jeho celkové pružnosti a adaptabilitě“* (Tvrdíková, 2001). Také je vhodné sledovat sociologické faktory, tj. přirozené formování vůdců (dominantních osobností), tvorbu neformálních vztahů mezi jednotlivými projektanty s cílem zabránit:

- konfliktům ve skupině,
- přílišnému vlivu dominantních jedinců, které by mohly mít negativní následky v práci s informacemi (utajování, deformace, nepravdivost, nepodloženost, zveličování zásluh), a v konečném důsledku i únik informace, zneužití a tak ohrožení celého projektu.

Prostupujeme a postupně upřesňujeme a aplikujeme platné právní normy, které podmiňují vznik a fungování projektu, přepracujeme vlastní organizační normy pro fungování systému. S tím současně řešíme právní ochranu i vlastních projektů (autorské právo). Se speciální ochranou informací v procesu projektování je vhodné začít hned na počátku, a to v souvislosti s náležitostmi:

- zpracování, a manipulace s projektovou dokumentací,
- se způsoby a prostředky fyzické, technické, autorského a další ochrany celkového projektu i jeho částí.

Z hlediska budoucího rozvoje systému (zavádění, provoz, reorganizace, fúze, likvidace) je užitečné současně s projektováním zpracovat prognózu, ke kterým negativním jevům nebo procesům může dojít. Z ní lze pak vycházet jak při projektování tak i dalších etapách činnosti a fungování systému (s důrazem na ochranu informací a výsledků práce). Na této prognóze by se měli podílet všichni účastníci projektu (např. formou brainstormingu).

5.4.1 Fáze zavádění systému a procesů

Pro tuto fázi je typické rozšiřování počtu subjektů jako např. nositelů, organizátorů, zpracovatelů, ale také objektů zpracování informací. Proto při organizování vlastní ochrany informací musí docházet k dělbě práce. Kvalitní základy v ochraně informací (zejména pak v přijatých preventivních opatřeních) se pozitivně odrazí v následných procesech. Prevence začíná již při výběru a nákupu technologií techniky, které v sobě zahrnují některé preventivní opatření (ochranná zařízení) proti úniku, poškození, deformaci či zničení informací. Kocan (2011) uvádí, že *„Velmi důležité je prověřování bezpečnostních a organizačních pravidel uvnitř firmy a u jednotlivých členů týmů. Většina bezpečnostních incidentů pochází směrem zevnitř, od zaměstnanců a ostatních lidí mající přístup k interním zdrojům společnosti.“* Odpovědnost zde mají jednak projektanti, ale zejména vedení organizace (podniku).

Proto je třeba odpovědně a ostražitě vybírat dodavatele nebo subdodavatele, partnery a v pozdější době i odběratele (zákazníky) z hlediska jejich korektnosti, spolehlivosti, včetně ostražitého předávání informací a záměrů. Zde může vedení organizace využívat jednak vlastních pracovníků, jednak i civilních bezpečnostních služeb (detektivů) anebo odborných poradců, vlastních či externích (Skalický, 2003).

Skalický (2003, s. 13) dále také uvádí, že *„Tok informací uvnitř projektového nebo podnikového prostředí a výměna informací s okolním prostředím je důležitou součástí projektového nebo podnikového managementu.“* Rozsah a intenzita ohrožení informací také závisí na výběru, rozmisťování a úkolování zaměstnanců. Za tímto účelem již ve fázi zavádění systému a procesů cíleně a postupně vybíráme budoucí zaměstnance. V každém případě bude třeba prověřit občanskou a trestní bezúhonnost, ale také např. přílišnou přecházející fluktuaci, jako předpokladů případného zneužití informací. Nelze rovněž podcenit prověrky, eventuálně doplnění důkazů odborné způsobilosti, jako prevence následné „poruchovosti“ pracovních (informačních) procesů. Doplnění je možno provádět formou zaškolování či doškolování, v němž budou již problémy a otázky ochrany informací obsaženy. V této činnosti musí sehrát rozhodující úlohu personalisté, personální útvary nebo odborní poradci.

Distribuce informací obsahuje poskytování informací účastníkům projektu ve vhodném čase. Vymezení informačních vazeb z hlediska jejich směru, kapacit kvality je dalším preventivním opatřením. Zde musíme zejména sledovat a vymezit, kdo bude výchozím bodem (nositelem a předavatelem) informací a ke které budou směrovat i zpětné vazby. Stanovíme také nezbytné množství informací, které musí mít jednotlivé subjekty či objekty. Přitom dbáme nebezpečí zahlcení nebo nedostatku informací ve vztahu k dané funkci a poslání prvku systému. Tato opatření se zavádějí a realizují na všech stupních systému (Skalický, 2003).

V této souvislosti nelze přehlédnout sociologické vazby vznikající mezi zaměstnanci. Jde zejména o vytváření neformálních skupin či postupné formování vůdců, které mají značný vliv na informační procesy (komunikace), a to jak z hlediska množství, kvality, tak z hlediska prospěchu či neprospěchu systému. Zde mají nezastupitelnou úlohu všichni vedoucí pracovníci. Vedoucí projektu musí najít individuální vztah k pracovníkům, a to jak formální, tak neformální (Skalický, 2003).

V návaznosti na předcházející kroky začínáme u formování pracovních kolektivů a typování vůdců (formálních a neformálních, pozitivních, negativních), na které posupně přenášíme stále větší množství a vyšší kvalitu (podrobnější, složitější) informací a zavazujeme je k odpovědnosti za jejich ochranu. To provádějí všichni vedoucí pracovníci. Postupně a cílevědomě řešíme otázky hmotné (ekonomické) i nehmotné zainteresovanosti zaměstnanců či skupin, jako předpokladu loajality a solidarity s podnikem i jako předpokladu zvýšené ochrany informací. Významnou úlohou zde má vedoucí podniku, ekonomická a personální pracoviště.

Řešíme postupně celkový systém právní ochrany systému i jednotlivých informací, ale i zaměstnanců. V tomto smyslu aplikujeme platné právní normy i jejich novely, ale podle potřeby vytváříme i nové interní normy. Pozornost je třeba věnovat přílišnému množství a časté rozpornosti těchto norem, aby nedocházelo k zahlcení a narušení systému a vazeb. Často je výhodné pro plnění tohoto úkolu angažovat stálého právníka nebo využívat právních poradců, kteří pochopili povahu systému a jsou připravení řešit případné spory uvnitř i vně systému (Skalický, 2003).

Konečně je užitečné doplnit a zpřesnit prognózu některých negativních jevů v ochraně informací, k nimž může dojít. Přitom zainteresovat zejména řídicí a bezpečnostní pracovníky k zavádění např.

- kontrolních týmů,
- systému fyzické, technické, popř. jiné ochrany objektů i vlastních informačních médií, dokumentů, počítačů atd.,
- speciálních ochranných opatření, kódování, šifrování, manipulace, režimová opatření.

5.4.2 Fáze běžného procesu systému

V této fázi zcela dominují ochranná opatření kontrolního charakteru a následují doplňující nebo pozměňující (reorganizační, zdokonalující, nápravná) opatření a kroky. Jedná se jak o dílčí nápravná opatření, tak i o významnější zásahy do organizace i procesů. Z psychologických hledisek jde zejména o zvyšování autority kontrolních procesů pochopení jejich nezbytnosti, ale také efektivnosti z hlediska zjednání nápravy, tj. odstranění nedostatků nebo alespoň zmírnění dopadů. Tato kontrolní opatření by měla být nástrojem motivace pracovních procesů (pozitivní motivace) i procesů ochrany informací. Značný význam zde mají různé formy a způsoby rozborů zjištěných nedostatků, ale také způsobů odstranění formou služebních porad, besed, odborných seminářů či iniciativních akcí (schůzí, besed) neformálních skupin (Skalický, 2003).

Paralelně s uvedenými opatřeními je významné dále sledovat a upevňovat pozitivní neformální vztahy a podporovat autoritu formálních i neformálních vůdců. Tuto povinnost mají všichni vedoucí pracovníci. Přitom však je třeba pozorně sledovat případy negativních jevů, vznik opozičních, konflikty vzbuzujících skupin či znevažování autority, které by mohly být příčinou narušování informačních toků uvnitř systému a úniku informací mimo pracoviště, podnik apod.

Dále je třeba rozvíjet a zdokonalovat formy ekonomické i sociální zainteresovanosti zaměstnanců s cílem neustále udržovat a prohlubovat pocity

sounáležitosti a solidarity se systémem (podnikem) a ochotou aktivně zasáhnout v případech možného ohrožení. *„Závažným hrozivým faktem, který není rozumné přehlížet, je skutečnost že více než čtyři pětiny útoků na informační systémy a data v nich uložená jsou klasifikovány jako vnitřní útoky. Ne všechny jsou vědomě cílené přímo zaměstnanci - jejich část je zapříčiněna nedbalostí či neúmyslnou pomocí“* (Stranyánek, 2001). Nelze přehlédnout také význam uplatnění a plnění přijatých právních norem, jejich zpřesňování a v závislosti na situaci i jejich účinky. Opět zde využíváme buď vlastních právníků, nebo právních poradců. Nelze zdokonalování ochrany s orgány činnými v trestním řízení. Pro zdokonalování ochrany informací uvnitř vlastního podniku má nemalý význam sledování vývoje v této oblasti a také u jiných objektů (konkurence) a pohotové zavádění nových prvků (psychologických, sociologických, ekonomických, právních, organizačních, technických apod.) Tato činnost by měla být záležitostí většiny zaměstnanců. Nelze ani podcenit zpřesňování prognóz možných způsobů ohrožení informací, a to za účasti řídicích pracovníků, ale i bezpečnostních pracovníků (orgánů). Stejně tak bude důležité sledovat, jestli nedochází k úmyslnému pronikání dezinformací organizovanému konkurencí. Z hlediska zabezpečení ochrany informací proti úniku, zneužití, deformací zničení nelze konečně podcenit ani nebezpečí působení politických konfliktů mezi zaměstnanci (popř. vedoucími pracovníky), ale také vliv alkoholu a drog. V této oblasti je potřeba takový vliv minimalizovat. To je povinností všech zaměstnanců, ale zejména personálních pracovišť v současnosti s vedením podniku. *„Vlastní krádež dat může mít i zcela nevinnou podobu - pár vytištěných papírů s citlivými informacemi (majícími charakter obchodního tajemství). Avšak s rostoucím objemem elektronicky uchovávaných dat se jedná především o hrozící problém vynášení dat v elektronické podobě“* (Stranyánek, 2001).

V některých případech se nelze vyhnout i sledování některých zaměstnanců, kteří projevují „mimořádný zájem“ o některé významné informace, které nejsou v jejich kompetenci. Zejména, jestliže se jedná o pracovníky, jejichž minulost, personální kvality a pracovní výsledky dávají předpoklad ke vzniku podezření z úniku (prodeje, předávání) informací mimo systém. To je povinností všech zaměstnanců, popř. speciálních bezpečnostních pracovníků. Zvýšenou bdělost konečně musíme zachovávat i při styku s obchodními partery, konkurencí, ale také zahraničními hosty.

6 Metodika zabezpečení ochrany utajovaných informací

Účelem této kapitoly je vytvořit konkrétní metodiku pro plnění úkolů vyplývajících ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a prováděcích právních předpisů Národního bezpečnostního úřadu (dále jen „NBÚ“) v konkurenčním prostředí, a to zejména v oblasti personální, administrativní a fyzické bezpečnosti, registru utajovaných informací a certifikaci informačních systémů. Metodika zabezpečení ochrany utajovaných informací je vytvořena tak, aby byla univerzálně použitelná jak pro orgány státní správy, tak i pro subjekty podnikatelské sféry.

6.1 Právní předpisy

Oblast ochrany utajovaných informací a bezpečnostní způsobilosti je upravena těmito právními předpisy:

a) zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, (dále jen „zákon“)

b) zákonem č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,

c) nařízením vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací

d) vyhláškou č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení, nakládajících s utajovanými informacemi a o certifikaci stínicích komor

e) vyhláškou č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací,

f) vyhláškou č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací,

g) vyhláškou č. 526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamu písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti),

h) vyhláškou č. 527/2005 Sb., o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o

vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti),

i) vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků,

j) vyhláškou č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

6.2 Stupně utajení

Utajované informace se klasifikují do těchto stupňů utajení:

a) PŘÍSNĚ TAJNÉ, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,
b) TAJNÉ, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,
c) DŮVĚRNÉ, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,
d) VYHRAZENÉ, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.

Dále se také utajované informace klasifikují na cizí moci poskytnuté České republice, nebo utajované informace cizí moci, k jejichž ochraně se Česká republika zavázala.

6.3 Druhy zajištění ochrany utajovaných informací

Ochrana utajovaných informací je zajišťována zejména:

- 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,
- administrativní bezpečností, která je tvořena systémem opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,
- fyzickou bezpečností, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat,

- 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.

6.4 Povinnosti při ochraně utajovaných informací

Mezi obecné povinnosti při ochraně utajovaných informací patří zejména to, že:

- každý je povinen neprodleně odevzdat nalezenou utajovanou informaci nebo utajovanou informaci získanou v rozporu s tímto zákonem anebo osvědčení fyzické osoby, osvědčení podnikatele, osvědčení fyzické osoby pro cizí moc nebo osvědčení podnikatele pro cizí moc Úřadu, policii nebo zastupitelskému úřadu České republiky,
- každý, kdo měl nebo má přístup k utajované informaci, je povinen zachovávat o ní mlčenlivost a nesmí k ní umožnit přístup neoprávněné osobě,
- každý, kdo podal žádost o provedení bezpečnostního řízení (§ 94 zákona), je povinen neprodleně oznámit Úřadu změny údajů, které jsou v ní uvedeny,
- každý je povinen při výkonu státní kontroly Úřadem plnit pokyny kontrolního pracovníka při provádění neodkladných opatření (§ 144 odst. 1 zákona),
- odevzdat do pěti dnů své Osvědčení, jehož platnost zanikla (§ 56 odst. 1 písm. b), f) a g) zákona), tomu, kdo jej vydal,
- neprodleně písemně oznámit tomu, kdo Osvědčení nebo Osvědčení fyzické osoby pro cizí moc vydal, ztrátu nebo odcizení svého Osvědčení nebo Osvědčení fyzické osoby pro cizí moc,
- neprodleně oznámit Úřadu změny údajů, které byly uvedeny v její Žádosti o vydání osvědčení fyzické osoby (§ 94 odst. 2 písm. a), c) a d) zákona) nebo v Žádosti o vydání osvědčení fyzické osoby pro cizí moc,
- neprodleně oznamovat tomu, kdo provedl její poučení, porušení povinností stanovených tímto zákonem (§ 9 odst. 1 nebo §11 odst. 2 zákona),
- účastnit se proškolení (§ 67 odst. 1 písm. b) zákona).

6.5 Administrativní bezpečnost

Informace, která naplňuje znaky § 3 a § 4 zákona a je uvedena v seznamu utajovaných informací (Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací), uvedeném v prováděcím předpisu, musí být evidována v jednacím protokolu.

Utajovaná informace se eviduje v určených administrativních pomůckách:

a) jednací protokol pro evidování utajovaného dokumentu,
b) pomocný jednací protokol pro zaznamenávání pohybu utajovaného dokumentu uvnitř organizace,
c) manipulační kniha pro zaznamenávání utajovaného dokumentu při jeho vytváření, přebírání a předávání osobou, která utajovaný dokument vytváří nebo které byl utajovaný dokument předán k vyřízení; do manipulační knihy se zapisují i utajované dokumenty, které byly zapůjčeny prostřednictvím zápůjční knihy a ty, které byly převzaté mimo organizaci a předávané k zaevidování do jednacího (případně pomocného jednacího) protokolu (zpravidla zásilky),
d) doručovací kniha pro zaznamenávání předání utajovaného dokumentu mezi jednotlivými organizacemi, případně mimo organizaci,
e) zápůjční kniha pro zaznamenávání zápůjček již uloženého utajovaného dokumentu,
f) kontrolní list pro stupně utajení DŮVĚRNÉ a vyšší pro vedení přehledu osob, které se s obsahem utajovaného dokumentu seznámily, aniž jej převzaly,
g) sběrný arch pro rozšíření evidenčního záznamu v jednacím protokolu v případě evidování většího počtu utajovaných dokumentů k jedné věci,
h) poznámkový sešit nebo kniha, do kterých se zaznamenávají poznámky nebo dílčí utajované informace.

Jednací a pomocné jednací protokoly, manipulační knihy a poznámkové sešity nebo knihy musí být autentizovány dle § 3 odst. 3 vyhlášky č. 529/2005 Sb. Seznamovat se s utajovanou informací nebo vytvářet utajovaný dokument může pouze zaměstnanec, který je držitelem Oznámení pro stupeň utajení VYHRAZENÉ nebo Osvědčení pro stupně utajení DŮVĚRNÉ nebo TAJNÉ a je poučen. Každý zaměstnanec, který obdrží utajovanou zásilku, je povinen nechat ji zaevidovat do jednacího (případně pomocného jednacího) protokolu a zapsat ji do své manipulační knihy. Vyskytne-li se u doručené zásilky závada (například poškození obálky nebo nesouhlasí-li počet listů), zaeviduje se zásilka podle skutečného stavu, neprodleně se vyrozumí bezpečnostní ředitel nebo jím pověřená osoba. Zaměstnanec, který zásilku převzal, sepíše záznam, jehož kopii odešle odesilateli. V případě, že byl utajovaný dokument určen jinému adresátovi, příjemce jej zaeviduje a zašle správnému adresátovi nebo vrátí odesilateli (§ 11 odst. 1 – 3 vyhlášky č. 529/2005 Sb.).

Zaměstnanec, který vytváří utajovaný dokument, si vyžádá číslo jednací z jednacího protokolu a zaznamená jej ve své manipulační knize. Na první stranu vytvářeného utajovaného dokumentu v listinné podobě se uvádí název organizace, číslo jednací, stupeň utajení, datum vyhotovení, číslo výtisku, počet listů, počet utajovaných a neutajovaných příloh a počet jejich listů, případně počet utajovaných a neutajovaných příloh v nelistinné podobě a jejich druh, v souladu s ust. § 15 -17 vyhlášky č. 529/2005 Sb. Listy utajovaného dokumentu musí být průběžně číslovány a sešity nebo jinak pevně spojeny (každý list bez ohledu na formát je považován za jeden list). Čistopis utajovaného dokumentu se vyhotovuje v počtu výtisků uvedeném v rozdělovníku. Zaměstnanec, který vyhotovuje čistopisy, neprodleně zničí vadné a nadbytečné výtisky tak, aby byla znemožněna jejich rekonstrukce a identifikace utajované informace, kterou obsahovaly. Na výtisku utajovaného dokumentu, který je určen k uložení, vyhotoví rozdělovník a záznam (Vzor stanoven v příloze č. 9 vyhlášky č. 529/2005 Sb.).

Stupeň utajení se vyznačí na utajovaném dokumentu v listinné formě v horní a dolní části uprostřed, a to na každé straně utajovaného dokumentu, takto:

a) VYHRAZENÉ a v čísle jednacím zkratku V,
b) DŮVĚRNÉ a v čísle jednacím zkratku D,
c) TAJNÉ a v čísle jednacím zkratku T.

Na utajovaný dokument v nelistinné podobě vyznačí údaje na popisném štítku nebo jiným vhodným způsobem. Vyznačení stupně utajení musí být zachováno po celou dobu trvání důvodu utajení, bez souhlasu původce nebo poskytující cizí moci nesmí být stupeň utajení změněn nebo zrušen. Zaměstnanec, který vytvořil utajovaný dokument, je povinen prověřit nejméně jednou za pět let ode dne vzniku dokumentu, zda důvod utajení trvá. Pominul-li důvod utajení nebo byl-li stanoven neoprávněně, zrušení nebo změnu stupně utajení vyznačí na utajovaném dokumentu a tuto skutečnost oznámí neprodleně písemně všem adresátům, kterým byl dokument zaslán. Ti vyznačí na utajovaném dokumentu zrušení nebo změnu stupně utajení přeškrtnutím původního tak, aby zůstal čitelný, případně vyznačí nový stupeň utajení. Provedení změny musí být potvrzeno záznamem na utajovaném dokumentu s uvedením důvodu, data provedení, jména, příjmení a podpisu osoby, která změnu provedla. O změně nebo zrušení stupně utajení se v příslušné administrativní pomůcce provede záznam dle §6 odst. 2 a 3 vyhlášky č. 529/2005 Sb.

Při předpokládaném větším počtu utajovaných dokumentů k jedné věci může zaměstnanec založit k příslušnému číslu jednacímu sběrný arch, do kterého zapisuje

dokumenty v pořadí, ve kterém jsou doručeny nebo ve kterém vznikly. Sběrný arch se uzavírá každoročně k 31.12., pokud však obsahuje dokument, jehož vyřízení přesáhne do nového kalendářního roku, lze uzavřít tento sběrný arch až po vyřízení dokumentu. V případě, že věc pokračuje i v novém kalendářním roce, založí k ní zaměstnanec sběrný arch s novým číslem jednacím a uzavřený sběrný arch z minulého kalendářního roku k němu připojí. Takto je možné pokračovat opakovaně. Sběrný arch je součástí spisu a ukládá se společně s ním, kopie sběrného archu se ukládá u jednacího protokolu, rovněž s ním se i vyřazuje. Na sběrný arch se vyznačí takový stupeň utajení, který má utajovaný dokument nejvyššího stupně utajení v něm zaevidovaný; lze do něj zapisovat i neutajované dokumenty, pokud se týkají téže věci. Opis, kopie, výpis nebo překlad utajované informace stupně utajení VYHRAZENÉ mohou být vyhotoveny bez souhlasu přímo nadřízené osoby, u písemností stupně utajení DŮVĚRNÉ nebo TAJNÉ je nutný písemný souhlas přímo nadřízené osoby (§19 vyhlášky č. 529/2005 Sb.) může být zapsán přímo na utajovaném dokumentu nebo na samostatném listu; je-li zapsán na samostatném listu, stává se součástí utajovaného dokumentu).

Utajovanou informaci lze přepravovat nebo přenášet pouze v přenosných schránkách nebo v uzavřeném obalu v závislosti na jejím stupni utajení a na jejím nosiči; přepravovat ji lze pouze prostřednictvím kurýrní služby nebo držitele poštovní licence. Převzetí utajované informace příjemce potvrdí podpisem (§20 – 23 vyhlášky č. 529/2005 Sb.). Utajovaná informace se v průběhu zpracování a po vyřízení ukládá v zabezpečené oblasti, případně v úschovném objektu podle bodové hodnoty nejnižší míry zabezpečení zabezpečené oblasti. Po vyřízení se utajovaný dokument předává osobě pověřené vedením jednacího protokolu k uložení. Na utajovaný dokument, který byl doručen z jiné organizace, uvede před uložením zaměstnanec, který jej vyřizoval, skartační znak a rok skartačního řízení, potvrzený podpisem nadřízeného. Takto upravený dokument předá osobě, pověřené vedením jednacího (případně pomocného jednacího) protokolu. Ta vyhotoví na utajovaný dokument záznam (vzor stanoven v příloze č. 9 vyhlášky č. 529/2005 Sb.), uloží jej do úložny utajovaných dokumentů a tuto skutečnost vyznačí v jednacím (případně pomocném jednacím) protokolu. Uložený utajovaný dokument lze zapůjčit na nezbytně nutnou dobu, zapůjčení a vrácení zaznamenává osoba pověřená vedením jednacího protokolu v zápůjční knize, vypůjčené dokumenty se v lednu každého kalendářního roku vrací pro účely provedení fyzické kontroly dle § 25 vyhlášky č. 529/2005 Sb.

Vyřazování utajovaných dokumentů zajišťuje nejméně tříčlenná skartační komise. Při vyřazování utajovaných dokumentů ve skartačním řízení se postupuje podle

zvláštního předpisu (Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, vyhláška č. 646/2004 Sb., o podrobnostech výkonu spisové služby) a platného skartačního řádu dané organizace. Nadpočetné výtisky může zničit mimo skartační řízení bezpečnostní ředitel organizace nebo osoba jím pověřená a osoba pověřená vedením jednacího (případně pomocného jednacího) protokolu, jejich zničení potvrdí podpisy v rozdělovníku na výtisku určeném k uložení.

6.6 Fyzická bezpečnost

Pro zabezpečení ochrany utajovaných informací v rámci fyzické bezpečnosti se určují objekty, zabezpečené oblasti a jednací oblasti.

Opatřeními fyzické bezpečnosti jsou:

a) ostraha,
b) režimová opatření,
c) technické prostředky.

Míra zabezpečení jednací oblasti a zabezpečené oblasti opatřeními fyzické bezpečnosti se určuje pomocí bodových hodnot těchto opatření v závislosti na vyhodnocení rizik; bodové hodnoty a nejnižší míra zabezpečení jsou stanoveny právním předpisem (Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků). Opatření fyzické bezpečnosti nebo kombinace více těchto opatření musí odpovídat alespoň nejnižší míře zabezpečení jednací oblasti nebo zabezpečené oblasti a stanoví se v závislosti na vyhodnocení rizik a na stupni utajení utajovaných informací, které jsou v jednací oblasti pravidelně projednávány, nebo na kategorii zabezpečené oblasti. Ověření, zda jednotlivá použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti ochrany utajovaných informací, provádí provozovatel průběžně, nejméně však každých 12 měsíců. Pro potřeby vyhlášky NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků je provozovatelem objektů dané organizace ředitel, popřípadě jím pověřená osoba. Postup při určení objektů, zabezpečených oblastí a jednacích oblastí a způsob ověření opatření fyzické bezpečnosti stanoví bezpečnostní ředitel vnitřním pokynem.

6.7 Bezpečnost informačních systémů

Útvar organizace, který o certifikaci informačních systémů požádá, předkládá v jejím průběhu na žádost Úřadu dokumentaci nezbytnou pro její provedení. Zjistí-li Úřad způsobilost IS k nakládání s utajovanými informacemi, vydá certifikát IS, který obsahuje:

a) evidenční číslo certifikátu,
b) identifikaci držitele certifikátu,
c) datum vydání a dobu platnosti certifikátu,
d) stupeň utajení utajovaných informací, pro který byla způsobilost IS ověřena,
e) přílohu certifikátu IS tvoří certifikační zpráva, která obsahuje zásady a podmínky pro používání IS.

Nakládat s utajovanou informací lze pouze v IS, který byl certifikován Úřadem a písemně schválen do provozu odpovědnou osobou; schválení IS do provozu oznámí odpovědná osoba, prostřednictvím bezpečnostního ředitele, písemně do 30 dnů od tohoto schválení Úřadu. Schválení IS do provozu (akreditaci) provádí komise stanovená odpovědnou osobou, na návrh bezpečnostního ředitele, která porovnává, zda schvalovaný IS odpovídá skutečnostem uvedeným v certifikační zprávě a bezpečnostní dokumentaci IS. Bližší postup při certifikaci IS stanoví bezpečnostní ředitel vnitřním pokynem.

6.8 Bezpečnostní politika

Bezpečnostní politika, přijatá vedením organizace, slouží jako návod a podpora k zavedení a zachování bezpečnosti informací. Ze strany vedení organizace je proto nutné zveřejnit jasné prohlášení k zavedení bezpečnosti informací v organizaci. Tento vrcholný dokument tvoří špičku pyramidy dokumentů, která pokrývá všechny aspekty IS od těchto zásad až po technické popisy. Platí zde následující pravidlo: každý koncept uvedený v bezpečnostní politice musí být v podřízených dokumentech konkretizován anebo musí být rozpracován.

Dokument „Bezpečnostní politika“ by se měl dotýkat těchto témat:

- Definice bezpečnosti informací, všechny její cíle a oblast použití, stejně jako důležitost bezpečnosti jako mechanizmu, který umožňuje společné používání informací;
- Strukturní popis řízení rizik;

- Prohlášení managementu o záměru podpořit cíle a principy bezpečnosti informací;
- Stručné vysvětlení bezpečnostní politiky, principů, norem a požadavků na shodu, které jsou pro organizaci obzvlášť důležité, např.:

- dodržování zákonných předpisů a smluvních požadavků,
- požadavky na výcvik v oblasti bezpečnosti,
- zabránění a identifikace virů a jiného škodlivého softwaru,
- řízení kontinuity činnosti organizace,
- důsledky při porušení bezpečnostních směrnic.

- Definování obecných a specifických kompetencí pro všechny aspekty řízení bezpečnosti informací, včetně ohlašování bezpečnostních incidentů;
- Odkazy na dokumentaci, která politiku podporuje, např. podrobné bezpečnostní politiky a postupy pro specifické informační systémy nebo bezpečnostní pravidla, která musí uživatelé dodržovat.

Tento dokument by měl být k dispozici všem uživatelům v organizaci ve formě, která je pro cílovou skupinu relevantní, přístupná a srozumitelná. Níže se pokusme takovou bezpečnostní politiku vytvořit na příkladu Celní správy ČR.

6.8.1 Bezpečnostní politika Celní správy ČR

Předmětem této bezpečnostní politiky je informační systém tvořený na bázi informačních a komunikačních technologií (dále jen „ISCS“), který Celní správa ČR (dále jen „CS“) vytváří a využívá k provádění svých zákonných činností. Pro potřeby řízení provozu je ISCS z dislokačního a funkčního hlediska členěn na subsystémy (dále jen „subISCS“) a pro potřeby řízení bezpečnosti ISCS na bezpečnostní domény (dále jen „BD“). Informace do ISCS začleněné a prezentované počítačovými daty (dále jen „data“) nesmí být informacemi utajovanými podle Zákona č.412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti; tato data je nutné chránit před ztrátou důvěrnosti, integrity a dostupnosti.

Bezpečnostní politika ISCS (2007) (dále jen „BP ISCS“) vychází z usnesení vlády České republiky ze dne 19. října 2005 č. 1340 o Národní strategii informační bezpečnosti České republiky a o zřízení Výboru pro informační bezpečnost České republiky. BP ISCS je by měla být zpracována v souladu s ČSN ISO/IEC 17799. Právní

rámec BP ISCS vytvářejí předpisy EU, právní předpisy ČR, usnesení vlády České republiky a ČSN.

6.8.2 Význam ochrany ISCS

ISCS je důležité chránit před riziky úmyslné i neúmyslné nevhodné lidské činnosti, dále před riziky chyb, poruch a havárií jeho technologického vybavení a neposlední řadě před riziky působení přírodních sil. Předcházení uvedených rizik umožní eliminovat jejich negativní dopady jak na veřejnost, tak na zájmy státu i zájmy CS. Velký význam má ochrana ISCS při začlenění CS mezi subjekty moderních veřejných elektronických služeb, v případě CS na úseku cel a daní.

6.8.3 Účel a cíle bezpečnostní politiky

BP ISCS je zásadním dlouhodobým a koncepčním bezpečnostním programem ISCS. Účelem BP ISCS je stanovit organizaci systému řízení bezpečnosti ISCS a organizaci bezpečnostního systému ISCS, jakož i stanovit odpovědnost organizačních útvarů i služebních funkcionářů CS při řízení bezpečnosti a provádění ochrany ISCS. Dále pak stanovit zásady řízení personální, technologické a fyzické bezpečnosti ISCS. Cílem BP ISCS je vytvoření systému řízení bezpečnosti ISCS a vytvoření bezpečnostního systému ISCS v souladu se zásadami této bezpečnostní politiky, a to na všech organizačních úrovních CS.

6.8.4 Vymezení pojmů

Pro účely tohoto návrhu bezpečnostní politiky se rozumí

- *aktivy ISCS* data, počítačové programy, výpočetní a komunikační technologie, napájecí a klimatizační systémy,
- *aplikací ISCS* uživatelský počítačový program vytvořený na zakázku CS a užívaný výhradně v ISCS,
- *bezpečností ISCS* stav tohoto informačního systému, kdy je zachována dostupnost, integrita i důvěrnost jeho i informací v něm začleněných,
- *bezpečnostním systémem ISCS* komplex opatření k zajištění požadované úrovně bezpečnosti tohoto informačního systému,
- *kritickými aktivy ISCS* taková aktiva, jejich ohrožení by mělo vysoký nebo velmi vysoký negativní dopad na CS,
- *kritickou činností v ISCS* taková činnost, která by mohla ohrozit provozuschopnost nebo bezpečnost ISCS,

- *krizovou situací ISCS* bezpečnostní událost, při níž jsou ohrožena kritická aktiva ISCS a ohrožení nelze odvrátit běžnou činností celníků a občanských zaměstnanců CS (dále jen „zaměstnanci CS“),
- *krizovým řízením ISCS* souhrn činností věcně příslušných organizačních útvarů a zaměstnanců CS zaměřených na řízení rizik, krizových situací, kontinuity a obnovy provozu ISCS,
- *ochranou ISCS* ochrana poskytovaná tomuto systému pro zachování dostupnosti, integrity a důvěrnosti jeho i informací v něm začleněných,
- *personálem ISCS* zaměstnanci CS, kteří jsou pracovníky úseků informatiky nebo pracovníky informační podpory na všech organizačních úrovních CS,
- *rolemi* činnosti, které je nutno vykonávat a pro které je možno, avšak obvykle není účelné nebo možné vytvářet samostatná služební či pracovní místa,
- *systémem řízení bezpečnosti ISCS* lidské síly, postupy a procedury určené k řízení jednotné a efektivní ochrany ISCS,
- *úseky informatiky CS* organizační útvary CS nebo jejich organizační součásti podílející se na výstavbě a provozu ISCS,
- *zvláštními informačními systémy CS* informační systémy užívané pro citlivé specifické činnosti CS; může se jednat i o systémy poskytnuté třetími stranami.

6.8.5 Věcná příslušnost

Tato bezpečnostní politika je určena pro ISCS. Je důležité ji dodržovat i v informačním systému veřejné správy (dále jen „ISVS“) CS. V případě potřeby a v přiměřeném rozsahu může být využita i pro zvláštní informační systémy užívané v CS, včetně informačních systémů CS nakládajícími s utajovanými informacemi podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále jen „IS/OUI“). Tato bezpečnostní politika je pro zaměstnance CS závazná. Pro smluvní dodavatele a externí uživatele ISCS je závazná pouze v rozsahu oboustranně schválených smluvních bezpečnostních podmínek. Je-li touto bezpečnostní politikou stanovena odpovědnost, povinnosti či práva organizačního útvaru CS v roli subjektu systému řízení bezpečnosti ISCS nebo subjektu bezpečnostního systému ISCS, rozumí se tím odpovědnost ředitele nebo vedoucího tohoto organizačního útvaru; související povinnosti a práva jím přitom mohou být delegovány na jednoho či více pracovníků jemu podřízeného organizačního útvaru CS.

6.8.6 Organizace bezpečnosti ISCS

Organizace bezpečnosti stanoví organizaci systému řízení bezpečnosti ISCS a organizaci bezpečnostního systému ISCS, včetně účasti a odpovědnosti organizačních útvarů CS, služebních funkcionářů CS, rolí a odborných orgánů v systému řízení bezpečnosti ISCS a v bezpečnostním systému ISCS. Organizační strukturu ISCS tvoří role, představující činnosti v oblasti správy, vývoje, výstavby a provozu tohoto informačního systému. Jsou jimi zřizovatel ISCS, provozovatel ISCS, provozovatel subISCS, správce ISVS CS, správce aplikace ISCS, personál ISCS a uživatel ISCS. Výkon, odpovědnost a oblast působnosti rolí uvedených v odst. 1 nutno stanovit vnitřními akty řízení CS, zejména Provozním řádem ISCS. Subjekty systému řízení bezpečnosti ISCS jsou organizační útvary CS, služební funkcionáři a zaměstnanci CS ustavení do rolí správce bezpečnosti ISCS a správce BD ISCS.

6.8.7 Role v systému řízení bezpečnosti ISCS

Rolemi v systému řízení bezpečnosti ISCS jsou role správce bezpečnosti ISCS a správců BD ISCS. Správce bezpečnosti provádí správu bezpečnosti ISCS, přičemž zejména:

- provádí správu bezpečnostních předpisů ISCS,
- metodicky řídí správu BD ISCS,
- organizuje a provádí kontrolu bezpečnosti ISCS,
- metodicky řídí bezpečnost IS/OUI v rámci jejich výstavby a provozu v CS,
- organizuje a provádí audit ochrany ISCS,
- řídí systém dálkové poplachové signalizace CS (dále jen „DPS CS“),
- provádí podporu správy systémů ochrany ISCS.

Správci BD ISCS zejména:

- podílejí se na správě bezpečnostních předpisů ISCS,
- organizují a provádějí kontrolu bezpečnosti v BD ISCS,
- podílejí se na metodickém řízení bezpečnosti IS/OUI v rámci jejich výstavby a provozu v CS,
- organizují a provádějí audit ochrany v BD ISCS,
- podílejí se na řízení systému DPS CS v BD ISCS,

- podílejí se na provádění podpory správy systémů ochrany ISCS v BD ISCS.

Pro jednotné a efektivní metodické řízení bezpečnosti IS/OUI jsou určena pravidla metodického řízení bezpečnosti IS/OUI CS.

6.8.8 Odborné orgány v systému řízení bezpečnosti ISCS

Odborným poradním orgánem správce bezpečnosti ISCS je bezpečnostní skupina, security group, (dále jen „SG2“) tvořená určenými pracovníky a externími konzultanty. V případě potřeby je SG2 správcem bezpečnosti ISCS rozšířena o správce BD ISCS.

SG2 zejména:

a) zpracovává návrhy bezpečnostních předpisů ISCS, provádí revize a aktualizace schválených bezpečnostních přepisů ISCS,

b) podílí se na metodickém řízení správy BD ISCS, zvláště formou aktuálního informování a bezpečnostního školení správců BD ISCS,

c) připravuje podklady a účastní se kontrol bezpečnosti ISCS,

d) zpracovává typovou bezpečnostní dokumentaci IS/OUI, účastní se akreditace těchto informačních systémů a provozních kontrol jejich bezpečnosti,

e) připravuje podklady, účastní se nebo provádí audit ochrany ISCS,

f) provádí bezpečnostní školení správců pultů centralizované ochrany (dále jen „PCO“) systému DPS CS, kontrolu externích revizí tohoto systému a připravuje podklady pro jeho změny a rozvoj,

g) podílí se na podpoře správy systémů ochrany ISCS podle pokynů správce bezpečnosti ISCS,

h) plní další úkoly a činnosti v oblasti operativního řízení bezpečnosti ISCS podle pokynů správce bezpečnosti ISCS.

6.8.9 Organizace provádění ochrany ISCS

Subjekty bezpečnostního systému ISCS jsou organizační útvary CS, služební funkcionáři a zaměstnanci CS tvořící personál ISCS i zaměstnanci ustavení do rolí správce systému ochrany ISCS a administrátor systému ochrany bezpečnostní domény ISCS. Organizační útvary CS plní úkoly a vykonávají činnosti související s prováděním ochrany ISCS v souladu s Organizačním řádem CS. Odbory a samostatná oddělení GŘC realizují stanovená opatření BP ISCS konkretizovaná vnitřními akty řízení CS

vydanými k provádění BP ISCS. Celní ředitelství a celní úřady zajišťují ve vymezeném rozsahu ochranu subISCS CŘ.

Rolemi v bezpečnostním systému ISCS jsou role správců systémů ochrany ISCS a administrátorů systémů ochrany BD ISCS. Správci systémů ochrany ISCS zejména

- řídí vytváření a rozvoj systémů ochrany ISCS,
- zpracovávají pravidla provozu systémů ochrany ISCS,
- provádějí audit systémů ochrany ISCS,
- metodicky řídí ochranu BD ISCS.

Administrátoři systémů ochrany BD ISCS zejména

- podílejí se na vytváření a rozvoji systémů ochrany ISCS,
- zajišťují provoz systémů ochrany ISCS,
- podílejí se na auditu systémů ochrany ISCS.

Personál ISCS se podílí na vytváření, rozvoji a provozu systémů ochrany ISCS v rozsahu vymezeném vnitřními akty řízení CS vydanými k provádění BP ISCS nebo pravidly provozu systémů ochrany ISCS. Uživatelé ISCS jsou povinni dodržovat pravidla provozu systémů ochrany ISCS v rozsahu jim těmito pravidly vymezeném, k čemuž musí být pravidelně školeni.

Bezpečnost ISCS může být negativně ovlivněna činností třetích stran, externích uživatelů ISCS i smluvních dodavatelů technologie a služeb pro ISCS. Je nezbytné, aby smlouvy s třetími stranami obsahovaly bezpečnostní podmínky, jejichž plnění je kontrolováno a v případě negativních zjištění jsou přijímána odpovídající opatření.

Při vytváření, rozvoji a provozu systému řízení bezpečnosti ISCS a bezpečnostního systému ISCS nutno znát aktiva i rizika tohoto informačního systému a nutno stanovit a implementovat bezpečnostní opatření. Přehled bezpečnostních opatření ISCS, jejichž výběr pro konkrétní subISCS nebo aplikaci ISCS vychází z jejich rizikovosti.

Závěr

Jedním z nejdůležitějších úkolů konkurenčního zpravodajství je pomáhat manažerům, aby si uvědomili, že jejich myšlenkový model nemusí odpovídat realitě. Dlouhodobá prosperita podniku a její udržitelnost je určena jednáním okolí a nikoliv jen analýzou výsledků a jejich historického vývoje. Organizace by také měla zjišťovat a zaznamenávat jednotlivé měnící se faktory v jejím okolí a měla by se snažit nalézt pro organizaci významné faktory a vazby, důležité pro strategické rozhodování. Zvyšování konkurenceschopnosti je omezováno nedostatečnou dostupností kvalitních manažerských informací a nedostatečnou schopností je účinně využít. V současné globální ekonomice je třeba zaměření se na rozhodování v oblasti produktových strategií z externích informačních zdrojů a využívání intelektuálního kapitálu vlastních zaměstnanců. Dále je také jedním z problémů informační fragmentace, která omezuje dostupnost a využitelnost manažerských informací. K řešení tohoto problému je třeba využití vhodných nástrojů a metod znalostního managementu, a to právě konkurenčního zpravodajství.

Základem konkurenceschopnosti je správné rozhodování, správná a rychlá reakce na změny v konkurenčním prostředí. Faktem je, že podkladem pro správné rozhodnutí jsou správné informace. Zavedení Competitive Inteligence (CI) v organizacích zlepší především znalosti jejich manažerů předvídat změny na trhu, tahy konkurence a zmapování nových a potenciálních konkurentů. Využití veškerých metod CI umožní učit se z chyb druhých a zvyšovat tak svou doménu a kvalitu u vyřčených cílů. CI je vlastně uceleným systémem získávání informací a jejich zpracování. Mohli bychom nabýt dojmu, že CI je pouze synonymum pro vojenskou špionáž v komerčním světě. Avšak není tomu tak. Podkladem jsou pouze běžně dostupné informace. Úkolem CI je monitorovat co konkurence dělá a za pomoci takových informací sestavit předpověď co hodlá konkurence udělat, ještě před tím než to udělá. Jedná se tedy o předpovídání trendů a plánů konkurentů a o plánování naší vlastní strategie podnikání tak, abychom z budoucích událostí co nejvíce těžili ve svůj prospěch. Aby bylo CI úspěšné, je nutná integrace do stávající struktury podniku, aby rozhodovací procesy využívaly ve správný čas ty správné informace.

Stěžejním účelem zákona č. 106/1999 Sb. je zajištění ústavního práva na informace fyzických osob, a to práva na takové informace, které mají k dispozici státní orgány, orgány územní samosprávy, jakož i další veřejné instituce a další subjekty, které rozhodují na základě zákona o právech a povinnostech fyzických a právnických osob v oblasti veřejné správy. Připomeňme si, že zákon č. 106/1999 Sb. je obecným a

komplexním předpisem, tedy že reglementuje každou hlavní právní stránku dotýkající se svobodného přístupu k veřejnoprávním informacím. Nedopadá jen na tu skupinu informací, která je komplexně upravena jiným předpisem, stanovuje obecný rámec přístupu k informacím veřejného sektoru s možností jejich dalšího využití.

Podnikání v současné době vyžaduje neustále nové tvořivé přístupy, které by naplnily stále rostoucí očekávání potenciálních zákazníků. Tyto moderní metody a trendy se nemohou vyhnout žádnému odvětví nebo segmentu trhu. Strategie představuje určení dlouhodobých základních cílů podnikatelského subjektu a určení nezbytných činností a zdrojů potřebných pro jejich dosahování. Účelem strategie je formulovat a prostřednictvím strategických cílů a s nimi spojených hrozeb popsat cílový obrat podnikání. Není podstatné tedy to, jak určit, jak podnik dosáhne svých cílů. To je úkolem především taktiky, složené z množství hlavních a vedlejších programů. Strategie vytváří rámec pro organizování a činnost. Úspěšná strategie by měla mít jednoduché, konzistentní a dlouhodobé cíle jednoznačně formulované. Pro úspěšnost strategie je dále nutné porozumění konkurenčnímu prostředí a znalost charakteru odvětví. Významná je také schopnost zhodnocení zdrojů, jejich potřeby a charakteru.

Strategie řešení konkurenčního boje je pro vrcholový management firmy velice složitou, náročnou a značně rizikovou záležitostí, vyžadující značné zkušenosti a vysokou úroveň znalostí. Konkurenční zpravodajství není pouze záležitostí bezpečnosti, ale představuje celý komplex. Konkurenčním zpravodajství je v podstatě komplexní konkurenční boj, který je vlastně ekonomickou válkou vedenou podnikateli o nové zákazníky, o nové trhy a o vyšší zisky. Bez systematického vyhodnocování informací dnes již nikdo není schopen využitelné příležitosti, reálné hrozby a důležité změny ani identifikovat a ani na ně adekvátně a včas zareagovat. Každá organizace by tak dnes měla zařadit konkurenční zpravodajství. Dále je třeba poukázat na fakt, že velké firmy musí díky své velké setrvačnosti včas odhalovat rizika a slepé cesty rozvoje, střední firmy musí usilovat o svoji pozici na trhu a vyhledávat příležitosti svého růstu a malé firmy musí odhalovat skulinky, kde se díky své pružnosti mohou uplatnit. Konkurenceschopnost závisí především na parametrech operační efektivnosti a na strategickém záměru organizace.

Česká celní správa, stejně jako celní správy ostatních států, má dva základní úkoly, kterými jsou ochrana a regulace domácího trhu formou výběru cla z dováženého zboží a dohled nad tím, aby toto zboží neohrožovalo životy nebo zdraví lidí, zvířat či rostlin. Vývoj ekonomické situace, včetně zahájení příprav na členství v EU, naléhavě vyžadoval, aby celní správa při plnění svých úkolů co nejvíce usnadňovala legální

mezinárodní obchod. Základní úkoly v oblasti zajištění ochrany trhu a bezpečnosti mezinárodního obchodu jsou v zásadě všem celním správám společné. Mezinárodní obchod se vždy dotýká minimálně dvou a zpravidla více celních správ a každá z nich má kontrolu jen nad částí celé obchodní operace. Z toho důvodu je nezbytné, aby celní správy vzájemně úzce spolupracovaly, a to na základě mezinárodních smluv, které poskytují právní rámec pro výměnu informací, předávání dokumentů a vzájemnou pomoc při šetřeních týkajících se porušování celních předpisů.

Ochrana informací je značně složitější a obtížnější než fyzická a technická ochrana objektů a osob. Její nehmotný charakter a individuální variabilita, zvyšuje možnosti úniku, manipulace, rychlé změny obsahu i „majitele“, deformace a zneužití. Nepochybně je však ztráta či získání informace i významným motivačním faktorem pro páchání kriminální trestné činnosti. Technická řešení, pokud splňují podmínky stanovené příslušnými právními předpisy, je možno chránit patentem. Ochrana vynálezů má teritoriální charakter a každý stát v platném právním předpise stanovuje, za jakých podmínek lze udělit ochranu na vynález a v čem tato ochrana spočívá. Z toho vyplývá, že v případě, že má vynálezce zájem chránit vynález i mimo území ČR, je nutno, aby podal přihlášku vynálezu také v těch státech, kde hodlá získat na své řešení ochranu. Složité společenské a ekonomické podmínky vedou nejen k ochraně jednotlivých informací, ale spíše k ochraně celých informačních systémů. Lze říci, že v současné době se většina informací rozvědného charakteru získává technickými prostředky, zbytek je doplňován klasickými formami získávání informací, tj. prostřednictvím lidí, agentů, jejich prací uvnitř zájmových objektů apod. Obecně je možno říci, že ochranná opatření jednak poněkud ztěžují činnost provozovatelů a jednak zvyšují náklady. Náklady by měly být úměrné škodám, které by mohly vzniknout, a proto je rozumné věnovat 10-20 % celkových nákladů na informační systém k zabezpečení jeho ochrany. Při hodnocení jakýchkoli úniků nebo zneužití informací se ukazuje, že nejslabším článkem v celém systému ochrany je lidský faktor. Nejrizikovějším faktorem úniku informací jsou vlastní zaměstnanci. Odhaduje se, že 80 – 90 % případů porušení ochrany informací je způsobeno vlastními zaměstnanci.

Na všech místech, spadajících pod plnění úkolů vyplývajících ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a prováděcích právních předpisů Národního bezpečnostního úřadu v konkurenčním prostředí, a to zejména v oblasti personální, administrativní a fyzické bezpečnosti, registru utajovaných informací a certifikaci informačních systémů, je třeba zpracovat konkrétní metodiku organizace. Metodika řeší oblast ochrany utajovaných informací a

bezpečnostní způsobilosti. Je třeba jasně stanovit povinnosti při ochraně utajovaných informací a seznámit s nimi všechny zaměstnance. Bezpečnostní politika tvoří špičku pyramidy dokumentů, která pokrývá všechny aspekty IS od těchto zásad až po technické popisy. Platí zde následující pravidlo: každý koncept uvedený v bezpečnostní politice musí být v podřízených dokumentech konkretizován anebo musí být rozpracován. Tento dokument by měl být k dispozici všem uživatelům v organizaci ve formě, která je pro cílovou skupinu relevantní, přístupná a srozumitelná.

Resumé

Rigorózní práce se zabývá konkurenčním zpravodajstvím a působením informací v podnikatelském prostředí, ale i státní sféře, jelikož informace bere na sebe roli významné strategické zbraně a do těchto odvětví významně zasahuje. Působení v dnešním globalizovaném světě vyžaduje neustále nové metody a přístupy. Bez těchto moderních metod a trendů se dnes neobejde žádná organizace. Informace mají, a budou mít, v dnešním světě klíčovou roli. Obzvláště v tržním mechanismu představují významnou výhodu pro soutěžící subjekty. Roste množství příležitostí a hrozeb, složitost vztahů mezi konkurenty a rychlost, s jakou se dění na trhu odehrává. Bez systematického vyhodnocování informací dnes již nikdo není schopen využitelné příležitosti, reálné hrozby a důležité změny ani identifikovat a ani na ně adekvátně a včas zareagovat. V této souvislosti dochází také k únikům, ztrátám a zneužívání informací. Na významu a nepostradatelnosti pro organizace nabývají také informační technologie, jež jsou a vždy budou nástrojem, který lidé mohou používat k tomu, aby lépe a efektivněji vykonávali to, co považují za potřebné či vhodné vykonávat. Kvalitativní změna je v tom, že možnosti tohoto nástroje radikálně mění naše dosavadní představy o tom, co je dosažitelné, schůdné a realizovatelné. Jelikož počátky konkurenčního zpravodajství mají kořeny v činnosti státní bezpečnosti a vojenských služeb, jsou proto v práci aplikovány metody a poznatky z mého působení v Celní správě České republiky, jakožto organizace, denně přicházející do styku s širokou sférou podnikatelské veřejnosti a dalšími orgány státní správy.

Díky fenoménu globalizace se konkurenční boje neustále vyostřují. Objevují se stále nové hrozby, kterým firmy musí čelit. Informace jsou dnes velmi ceněným a drahým zbožím. Informace jsou stavebním materiálem managementu znalostí a jeho rozhodovacích procesů. Úspěšnou firmu odlišuje od šedi průměru, jak dobře využívá informace. Prostředkem k dosažení managementu znalostí je konkurenční zpravodajství. Konkurenční zpravodajství není pouze záležitostí bezpečnosti, ale představuje celý komplex. Nejdůležitější role konkurenčního zpravodajství spočívá v podpoře tvorby a prosazování konkurenceschopné strategie. Současná globální ekonomika vyžaduje od organizací, které chtějí být konkurenceschopné, zaměření se na rozhodování v oblasti produktových strategií z externích informačních zdrojů a využívání intelektuálního kapitálu vlastních zaměstnanců. Klíčem k řešení problému informační fragmentace, která omezuje dostupnost a využitelnost manažerských informací, je využití vhodných nástrojů a metod znalostního managementu, zvláště potom konkurenčního zpravodajství.

Zavedení Competitive Inteligence (CI) v organizacích zlepší především znalosti jejich manažerů předvídat změny na trhu, tahy konkurence a zmapování nových a potenciálních konkurentů. Využití veškerých metod CI umožní učit se z chyb druhých a zvyšovat tak svou doménu a kvalitu u vyřčených cílů. CI je vlastně uceleným systémem získávání informací a jejich zpracování. Mohli bychom nabýt dojmu, že CI je pouze synonymum pro vojenskou špionáž v komerčním světě. Avšak není tomu tak. Podkladem jsou pouze běžně dostupné informace.

Další rozvoj a rozšiřování užití výpočetní techniky, které vede k vytváření a užívání počítačových sítí obzvláště nese s sebou nutnost ochrany informací. V současné době se problém ochrany informací většinou zužuje na jejich zabezpečení a úpravě v těchto prostředcích, postupně integrovaných do počítačových sítí. Ochraně dat je třeba věnovat pozornost již v období projekce informačního systému a samozřejmě v době jeho běžného užívaní. Ochrana informací se stává významným faktorem soudobého úspěchu či naopak neúspěchu organizace. Jestliže mají být podnikatelské informace dokonale a hospodárně ochráněny, nelze tuto činnost uskutečňovat amatérsky. Zejména, jestliže se jedná o uchování informací významných z hlediska perspektivy podniku, jeho strategie nebo informací aktuálně významně ovlivňujících chod dalších subjektů, je třeba zajistit profesionální úroveň ochrany.

Je skutečností, že ve společnosti existují určité sociálně-patologické jevy, včetně kriminality. Ty jsou charakterizovány touhou i rozhodnutím zmocnit se, zneužít, poškodit či zničit materiální i duchovní vlastnictví, omezit či zcela znemožnit uplatňování základních práv a svobod občanů. Nedostatek a nesrozumitelnost právních a řídicích informací může být příčinou a podmínkou nezákonnosti, bezpráví a zneužívání postavení. To se v podstatě vztahuje i na neurčitost informací. Množství a kvalita informací může konečně vytvářet příčiny a podmínky pro dezorientaci systémů. Ty pak mají velmi často za následek zejména násilnou, majetkovou a hospodářskou kriminalitu. Z uvedeného vyplývá, že předmětem ochrany musí být i kvantitativní a kvalitativní stránky informace. Informace se tedy může stát také nástrojem trestného činu. Ochrana osobních dat je jedním z práv občanů. Jestliže někdo neoprávněně sdělí nebo zpřístupní údaje o jiném shromážděné v souvislosti s výkonem veřejné správy, svého povolání, zaměstnání nebo funkce, dopouští se trestného činu. Totéž platí i poskytne-li tyto uniformace nebo údaje neoprávněně prostředkům hromadné informace.

Summary

The rigorous thesis deals with competitive reporting and the effect of information in the business environment, but also the state sphere, since the information takes on the role of major strategic weapons and to the industry. Significantly extends. In today's globalised world requires new methods and approaches are constantly.Without these modern methods and trends of today needs no other organization. The information they have and will have a key role in today's world. Especially in a market mechanism, constitute a significant advantage for competing entities. Growing quantity of opportunities and threats the complexi of the relationship between the competitors and the speed with which the action takes place on the market. Without a systematic evaluation of information today, no one is able to use the real threats and opportunities, important changes or identify and even to them adequately and timely to respond. In this context, it also leaks, loss and misuse of the information. On the significance and indispensability for the organization are also information technology, who they are and always will be the tool that people can use to make better and more efficiently pursued what he considered to be necessary or appropriate to carry out. Qualitative change is that the options for this utility to radically change our notions of what is achievable, feasible and achievable. Since the beginnings of the competitive intelligence activities are rooted in national security and military services are therefore in the work of the applied methods and knowledge from my time in the customs administration of the Czech republic, as an organization, daily coming into contact with a broad sphere of business to the public and other public authorities.

Thanks to the phenomenon of globalisation with the competitive fight constantly increasign. There are still a new threat, which the company must face. The information is very valuable and expensive goods. Information is material to the construction of knowledge management and it's decision-making processes. A successful company differs from the grey average, as well uses the information. Means to achieve the management of knowledge is competitive intelligence. Competitive intelligence is not only a matter of safety, but is the entire complex. The most important role of the competitive intelligence is to promote the creation and promotion of competitive strategy. The current global economy requires from the organisations that want to be competitive, focusing on the decision-making in the field of product strategies from external information sources and the use of the intellectual capital of it's own employees. The key to resolving the problem of fragmentation of information, which limits the availability and the availability of management information, is the use of appropriate

tools and methods of knowledge management, especially by competitive intelligence.

The introduction of Competitive Intelligence (CI) in organizations, in particular, to improve the knowledge of their managers to anticipate changes in the market, competition and mapping of new strokes and potential competitors. The use of any CI methods allow to learn from the mistakes of others and raise your domain and speaking for quality objectives. CI is actually a coherent system of collecting information and their processing. We could, that CI is only a synonym for military espionage in the commercial world. But it is not so. The basis are only commonly available information.

Further development and expansion of the use of computer technology, which leads to the creation and use of computer networks in particular, leads to the need for the protection of information. Currently the issue of protection of information usually narrows on their security and adjustment in these devices gradually integrated into the computer networks. Protect data attention is alredy in the design of an information system and of course at the time of it's current usage. Protection of information is becoming a significant factor in the success or failure of the existing organization. If they are to be bussiness information completely and economically protected, unable to carry out this activity. In particular if the retention of the respective of the company it's strategy or significantly affecting the operation of the information currently in the other bodies, it is necessary to ensure that the professional level of protection.

Is the fact that in a society there are certain socio-pathological phenomena, including crime. These are characterized by the desire and the decision to seize, misuse, damage or destroy both material and spiritual property, to limit or completely block the application of the fundamental rights and freedoms of citizens. The lack of legislation and control and the obscure nature of the information may be the cause and condition of lawlessness, injustice and the abuse of position. It relates essentially to the vagueness of the information. The quantity and quality of the information may finally create the causes and conditions for the disorientation of the systems. You then have very often result in a particularly violent, material and economic crimes. From the foregoing that the subject of protection must be quantitative and qualitative information page. Information may also become a tool of the offence. Protection of personal data is one of the rights of the citizens. If someone unduly communicate or make available data on another collected in connection with the performance of public administration, their profession, occupation or function, are guilty of the offence. The same applies if these uniformace or information unlawfully mail information resources.

Seznam použitých zdrojů

ABRHÁM, Josef. Klastry a rozvoj konkurenceschopnosti české ekonomiky. In *Současná Evropa a Česká republika*. Praha : VŠE, 2006. s. 230-246. ISSN 1211-4073.

BARTES, František; DOSTÁL, Vladimír . *Strategie konkurenčních střetů*. 1. Brno : PC-DIR Real, 1999. 137 s. ISBN 80-214-1496-0.

BENEŠ, M. Konkurenceschopnost a konkurenční výhoda. In: *Working Paper*. Praha : VŠE, 2006. s. 15. ISSN 1210-3292.

BERGER, P. I., LUCKMAN, T. *Sociální konstrukce reality*. 1. vyd. Brno : CKD, 1999. 216 s. ISBN 80-85959-46-1.

BERGMAN, Ofer, Ruth BEYTH-MAROM a Rafi NACHMIAS. The project fragmentation problem in personal information management. In: GRINTER, Rebecca. *CHI 2006*: *interact, inform, inspire : conference proceedings : Conference on Human Factors in Computing Systems : Montreal, Quebec, Canada, April 22-27*. New York, N.Y.: Association for Computing Machinery, c2006. DOI: 608063.

Bezpečnostní politika informačního systému Celní správy ČR. Praha : Celní správa ČR, 2007, 27 s.

BOCK, Wally. *Frequently Asked Questions about Business* Intelligence [online]. 2000 [cit. 2011-05-15]. Bockinfo. Dostupné z WWW: <http://www.bockinfo.com/docs/bifaq.

BRABEC, František. *Bezpečnost pro firmu , úřad, občana*. 1. Praha : Public History , 2001. 400 s. ISBN 80-86445-04-06.

BRABEC, František. *Komerční zpravodajství jako významná součást soukromé detektivní činnosti II.* In: Security Server, 2000. Dostupné on-line:
<http://www.securityserver.cz/article.asp?ArticleID=2>.

BRABEC, František. *Komerční zpravodajství jako významná součást soukromé detektivní činnosti III.* In: Security Server, 2000. Dostupné on-line:
<http://www.securityserver.cz/article.asp?ArticleID=2>.

BRECHLEROVÁ, Dagmar. Sociální inženýrství. *IT Systems* [online]. 2007, 3, [cit. 2011-04-06]. Dostupný z WWW: <http://www.systemonline.cz/it-security/socialni-inzenyrstvi.htm>. ISSN 1802-615X.

CAUSA, Orsetta; COHEN, Daniel. *Overcoming barriers to competitiveness* [online]. Paris : OECD, 2004 [cit. 2011-08-12]. Dostupné z WWW:
<http://www.oecd.org/dataoecd/37/56/34027373.pdf>.

Celní správa ČR. GENERÁLNÍ ŘEDITELSTVÍ CEL. *Http://www.celnisprava.cz/cz/Stranky/default.aspx* [online]. ver. 2.0.0.9/109. 2009 [cit. 2011-12-21]. Dostupné z: http://www.celnisprava.cz/cz/Stranky/default.aspx

CzechInvest : Agentura pro podporu podnikání a investic [online]. 20.1.2007 [cit. 2010-09-04]. <http://www.bockinfo.com/docs/bifaq.htm>.Průvodce klastrem. Dostupné z www:<http://www.czechinvest.org/data/files/pruvodce-klastrem-63.pdf>.

ČERVENKA, Jaroslav. *Svobodný přístup k informacím je jen iluzí* [online]. epravo.cz, 2001 [cit. 2011-08-05]. Dostupné z WWW: <http://www.epravo.cz/top/clanky/svobodny-pristup-k-informacim-je-jen-iluzi-3410.html>.

Česká republika. Nález Ústavního soudu: ze dne 22. března 2011 sp. zn. Pl. ÚS 24/10, o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), In: *94/2011*. 2011, 35/2011. Dostupné z: http://www.epravo.cz/_dataPublic/sbirky/2011/sb0035-2011.pdf

Česká republika. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, 77, s. 1-2.

Česká republika. Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. In *Sbírka zákonů, Česká republika*. 2005, 179, s. 30-45.

Česká republika. Vyhláška č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, 179, s. 46-60.

Česká republika. Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, 179, s. 61-66.

Česká republika. Vyhláška č. 526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamu písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti). In *Sbírka zákonů, Česká republika*. 2005, 179, s. 67-96.

Česká republika. Vyhláška č. 527/2005 Sb., o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti). In *Sbírka zákonů, Česká republika*. 2005, 179, s. 97-130.

Česká republika. Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy . In *Sbírka zákonů*. 2006, 172, s. 1-5.

Česká republika. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů, Česká republika*. 2005, 179, s. 131-167.

Česká republika. Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, 179, s. 168-179.

Česká republika. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, 11, s. 2-112.

Česká republika. Zákon č.106/1999 Sb., o svobodném přístupu k informacím. In *Sbírka zákonů*. 1999, 39/1999 Sb., s. 1-12.

Česká republika. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů. In *Sbírka zákonů*. 2000, 99, s. 1-23.

Česká republika. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, 76, s. 2-52.

Česká republika. Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, 143, s. 53-67.

ČÍRTKOVÁ, Ludmila. Finanční zločinci. *Psychologie dnes* [online]. 2006, 10, [cit. 2011-04-06]. Dostupný z WWW: <http://www.portal.cz/scripts/detail.php?id=20138>.

DEVITO, Joseph A. *Základy mezilidské komunikace*. 6. Praha : Grada, 2008. 512 s. ISBN 978-80-247-2018-0.

DOUCEK, Petr; NOVÁK, Luděk; SVATÁ, Vlasta. *Řízení bezpečnosti informací* . 1. Praha : Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7.

DRUCKER, Peter Ferdinand. *Nové reality*. 1. Praha : Management Press, 1995. 244 s. ISBN 80-85603-85-3.

EURO-INFO. Podľa správy EPÚ európske firmy zlyhávajú pri využívání patentových informácií. *Euro-Info*. 2003, 12.

Evropské společenství. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2006/24/ES ze dne 15. března 2006: o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES. In: *L 105/54*. Evropský parlament a Rada Evropské unie, 2006. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:CS:PDF

FULD, Leonard M. *What competitive intelligence is and is not!* [online]. Copyright 1996 2010 [cit. 2010-05-15]. Fuld&Company. Dostupné z www: <http://www.fuld.com/Company/CI.html>.

GARELLI, S. *Competitiveness of Nations: The Fundamentals* [online]. Copyright 1996 2010 [cit. 2010-05-15]. IMD World Competitiveness Yearbook. Dostupné z www: <http://www.imd.ch/research/centers/wcc/upload/Fundamentals.pdf.>.

GARSHOL, Lars Marius . Metadata? Thesauri? Taxonomies? Topic Maps!. *Ontopia* [online]. 2004, 10, 26, [cit. 2010-05-15]. Dostupný z www: <http://www.ontopia.net/topicmaps/materials/tm-vs-thesauri.html>.

GATES, Bill. Byznys rychlostí myšlenky. 1. Praha : Vydává Management Press, 1999. 356 s. ISBN 80-85943-97-2.

GERLOCH, A. (2004): *Teorie práva.* Plzeň: Aleš Čeněk s.r.o. ISBN 80-86473- 85-6.

GERLOCH, A. (2003): In HENDRYCH, D. a kol.: *Právnický slovník.* 2. rozšířené vydání. Praha: C. H. Beck. ISBN 80-7179-740-5.

HAS, Michael; MOLNÁR, Zdeněk. Využití map námětů pro tvorbu znalostní báze podnikatelských klastrů. In *Cesty ke zvyšování konkurenceschopnosti v soukromém i veřejném sektoru a vzdělávání*. Praha : Nakladatelství ČVUT, 2006. s. 15-22. ISBN 80-01-03597-2.

HELÍSEK, M. (2002): *Makroekonomie – základní kurs.* Praha: Melandrium. ISBN 80-86175-26-X.

HELMS, M. M.; ETTKIN, L. P.; MORRIS, D. J. Viewpoint : the risk of information compromise and approaches to prevention. *Journal of Strategic Information Systems*. 2000, 9, 1, s. 5-15.

HENDRYCH, D. a kol. (2003): *Právnický slovník.* 2. rozšířené vydání. Praha: C. H. Beck. ISBN 80-7179-740-5.

HOFFMAN, Constantine Von. Competitive Intelligence. *Harvard Business Review*. 1999, 4, 9, s. 6-7.

HOŘEJŠÍ, B., et al. (2008): *Mikroekonomie*. 4. rozšířené vydání. Praha: Management Press. ISBN 978-80-7261-150-8.

HOŠKOVÁ, Marta. *Mezinárodní patentová ochrana*. 2., aktualiz. vyd. Praha : Metropolitní univerzita Praha, 2010. 166 s. ISBN 978-80-86855-60-8.

Informační koncepce Celní správy ČR. Praha : Celní správa ČR, 2009. 22 s.

ISO/IEC 17799:2005 . *Information Security Management : Information Technology - Security techniques - Code of practice for information security management*. Geneva : International Organization for Standardization , 2005. 10 s. Dostupné z WWW: <http://www.rac.cz/rac/homepage.nsf/CZ/27002/$FILE/BS_ISO_IEC_27002_obsah.pdf

IVANKA, Ján. *Systematizace bezpečnostního průmyslu*. První. Zlín : Univerzita Tomáše Bati ve Zlíně Academia centrum, 2009. 86 s. ISBN 978-80-7318-863-4.

JIRÁSEK, J., A. Konkurenčnost. Vítězství a porážky na kolbišti trhu. Praha : Professional Publishing, 2001. 378 s. ISBN 80-86009-29-7.

JOHNSON, Gerry ; SCHOLES, Kevan. *Exploring Corporate Strategy : Text and Cases*. 7 edition . Norfolk : Prentice Hall Europe, 1998. 1120 s. ISBN 0-273-65112-9, 978-0273-6511-2-3.

KAHANER, Larry. *Competitive Intelligence : How to Gather, Analyze, and Use Information to Move Your Business to the Top* . New York : Touchstone, 1998. 304 s. ISBN 0-684-84404-4, 978-0-684-84404-6.

KALUŽA, Jindřich. *Informační systémy pro strategické řízení* . 1. Ostrava : Vysoká škola báňská - Technická univerzita, Fakulta ekonomická, 2010. 145 s. ISBN 978-80-248-2280-8.

KEŘKOVSKÝ, Miloslav; VYKYPĚL, Oldřich. *Strategické řízení : teorie pro praxi*. 2. Praha : C. H. Beck, 2006. 206 s. ISBN 80-7179-453-8.
KLÍMA, K. (2006): *Ústavní právo.* 3. vydání. Plzeň: Aleš Čeněk, s.r.o. ISBN 80- 7380-000-4.

KNAPP, V. (1995): *Teorie práva.* Praha: C. H. Beck. ISBN 80-7179-028-1.

KOCAN, Marek. Bezpečnost je třeba řídit : Základní atributy bezpečnostní politiky. *IT Systems* [online]. 2011, 1, [cit. 2011-04-09]. Dostupný z WWW: <http://www.systemonline.cz/it-security/bezpecnost-je-treba-ridit.htm>. ISSN 1802-615X.

KOCH, Miloš. *Management informačních systémů* . 3. Brno : Akademické nakladatelství CERM, 2010. 171 s. ISBN 978-80-214-4157-6.

KOLMAN, Petr. *Právo na informace*. 1. Brno : Masarykova univerzita, 2010. 216 s. ISBN 978-80-210-5135-5.

KOLMAN, Petr. Právo na informace, obchodní tajemství a vynakládání rozpočtových prostředků obce. epravo [online]. 2003, 1, [cit. 2011-07-09]. Dostupný z WWW: <http://www.epravo.cz/top/clanky/pravo-na-informace-obchodni-tajemstvi-a vynakladani-rozpoctovych-prostredku-obce-22072.html>.

KOSTKA, Vladimír. Informační bezpečnost v bezpečnostním systému . In JELÍNEK, Josef. *Ochrana dat a informací : sborník z odborného semináře konaného při příležitosti mezinárodní výstavy PRAGOALARM '96*. Praha : Family media, 1996. s. 2-5., Příl. čas.: Security magazín ; č. 3. 1996. ISSN 1210-8723.

KUBIŠTA, Václav. *Mezinárodní ekonomické vztahy*. 1. Praha : HZ Editio, 1999. 378 s. ISBN 80-86009-29-7.

KUDĚLKA, Tomáš. Jak efektivně řídit přístup k firemním informacím : Výsledky průzkumu identity & access managementu (IAM). *IT Systems* [online]. 2009, 12, [cit. 2011-04-06]. Dostupný z WWW: <http://www.systemonline.cz/it-security/jak-efektivne-ridit-pristup-k-firemnim-informacim.htm>. ISSN 1802-615X.

LÁTAL, Ivo. *Ochrana informací, dat a počítačových systémů*. 1. vyd. Praha: Eurounion, 1996, 238 s. ISBN 80-858-5832-0.

LIŠKA, Miroslav. *Matematické metody v podnikání* . 1. Ostrava : Vysoká škola podnikání v Ostravě, 2007. 95 s. ISBN 978-80-86764-73-3.

LOPEZ-CLAROS, Augusto. *The Global Competitiveness Report 2005-2006* [online]. Geneva : World Economic Forum, 2004-2005 [cit. 2011-08-12]. Dostupné z WWW: <http://insight.iese.edu/casos/Study_0035.pdf>.

LOPEZ-CLAROS, Augusto. *The Global Competitiveness Report 2005-2006* [online]. Geneva : World Economic Forum, 2005-2006 [cit. 2011-08-12]. Dostupné z WWW: <http://insight.iese.edu/casos/Study_0035.pdf>.

LOPEZ-CLAROS, Augusto. *The Global Competitiveness Report 2005-2006* [online]. Geneva : World Economic Forum, 2006-2007 [cit. 2011-08-12]. Dostupné z WWW: <http://insight.iese.edu/casos/Study_0035.pdf>.

MATES, Pavel. *Evidence, informace, systémy : právní úprava*. 1. Praha : Codex Bohemia, 1997. 263 s. ISBN 80-85963-27-2.

MATES, Pavel. *Ochrana osobních údajů*. 1. Praha : Karolinum, 2002. 73 s. ISBN 80-246-0469-8.

MINTZBERG, Henry. *The Strategy Process: Concepts, Context, Cases*. 4 edition. New Jersey : Prentice Hall, 2002. 489 s. ISBN 978-0130479136.

MLEZIVA, Emil. *Diktatura informací : jak s námi informace manipulují*. 1. Plzeň : Aleš Čeněk, 2004. 133 s. ISBN 80-86898-12-1.

MOLNÁR, Zdeněk. *Competitive Intelligence*. 1. Praha : Nakladatelství Oeconomica, 2009. 98 s. ISBN 978-80-245-1603-5.

NĚMEJC, Jiří. Zajištění informační bezpečnosti při přenosu dat technickými prostředky. In JELÍNEK, Josef. *Ochrana dat a informací : sborník z odborného semináře konaného při příležitosti mezinárodní výstavy PRAGOALARM '96*. Praha : Family media, 1996. s. 17-23., Příl. čas.: Security magazín ; č. 3. 1996. ISSN 1210-8723.

PAPÍK, Richard. *Competitive Intelligence a internet. Co je CI?* [online]. 2001 [cit. 2010-05-15]. Konjunktura. Dostupné z WWW: <http://www.konjunktura.cz/index.php3?w=art&id=41&s=&rub=44>.

PEKÁREK, Oldřich; ČÍŽEK, Vladimír. *Práce s agenturními a elektronickými informacemi* . 1. České Budějovice : Vysoká škola evropských a regionálních studií, 2007. 138 s. ISBN 978-80-86708-40-9.

PEPPER, Steve. The TAO of Topic Maps. Ontopia [online]. 2002, 04, [cit. 2010-05-15]. Dostupný z www: <http://www.ontopia.net/topicmaps/materials/tao.html>.

PORTER, Michael. *Competitive Strategy : Techniques for Analyzing Industries and Competitors* . 1 edition . New York : The Free Press, 1998. 397 s. ISBN 0-684-84148-7, 978-0684841489 .

PORTER, Michael. Competitive Advantage of Nations . New York : The Free Press, 1990. 896 s. ISBN 0-684-84147-9.

PORTER, Michael. *Konkurenční strategie : Metody pro analýzu odvětví a konkurentů*. Praha : Victoria Publishing, 1994. 403 s. ISBN 80-85605-11-2.

PORTER, M., SCHWAB, K., MARTIN, X. S. The Global Competitivenes Report 2007/2008 . Houndmills : Palgrave macmillan, 2008.

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

PRAHALAD, C. K.; HAMEL, Gary. The core competence of the corporation. *Harvard Business Review* [online]. 1990, May-June, [cit. 2010-05-15]. Dostupný z www: http://tleinc.com/PDFS/FILES/resources/The%20Core%20Competencies%20of%20the%20Corp.pdf

PREUSS, Karel. *Podnikatelské strategie*. Praha : Bankovní institut vysoká škola, 2008. 101 s. ISBN 978-80-7265-134-4.

PŘIBYL, Tomáš. Jak zastavit vnitřního nepřítele?. *IT SYSTEMS* [online]. 2009, 10, [cit. 2011-04-06]. Dostupný z WWW: <http://www.systemonline.cz/it-security/jak-zastavit-vnitrniho-nepritele.htm>. ISSN 1802-615X.

Rada pro výzkum a vývoj ČR, s. 102, 2008.

RYP, Petr. Informační proces jako součást systému velení a řízení. *Vojenské rozhledy*. 2009, 18, 4, s. 149-153. ISSN 1210-3292.

SCIP Code of Ethics for CI Professionals [online]. 2010 [cit. 2010-05-15]. SCIP. Dostupné z www: <http://www.scip.org/About/content.cfm?ItemNumber=578>.

SEDLÁČEK, Václav. *Management systému informační bezpečnosti - ISMS : studijní opora disciplíny* . 1. Třebíč : Vivat Academia, 2010. 96 s. ISBN 978-80-87385-05-0.

SKALICKÝ, Jiří. *Projektový management*. 3. Plzeň : Západočeská univerzita, 2003. 188 s. ISBN 80-7043-237-3.

SKLENÁK, V. a kol. (2001): *Data, informace, znalosti a Internet.* Praha: C. H. Beck. ISBN 80-7179-409-0.

SLABÝ, Jiří. Competitive Intelligence - poznejte své nepřátele. In *Cesty ke zvyšování konkurenceschopnosti v soukromém i veřejném sektoru a vzdělávání*. Praha : Nakladatelství ČVUT, 2006. s. 53-57. ISBN 80-01-03597-2.

SMEJKAL, Vladimír. Právní aspekty informační bezpečnosti . In JELÍNEK, Josef. *Ochrana dat a informací : sborník z odborného semináře konaného při příležitosti mezinárodní výstavy PRAGOALARM '96*. Praha : Family media, 1996. s. 9-17., Příl. čas.: Security magazín ; č. 3. 1996. ISSN 1210-8723.

SÖLVELL, Örjan; LINDQIST, Göran; KETELS, Christian. *The Cluster Initiative Greenbook* [online]. First edition. Stockholm : Ivory Tower AB, 2003 [cit. 2010-05-15]. Dostupné z www:<http://www.dps.tesoro.it/cd_cooperazione_bilaterale/docs/6.Toolbox/13.Supporting_documents/1.Cluster_methodologies_casoni/3.Learning_materials/5.Cluster_initiative_greenbook.pdf>. ISBN 91-974783-1-8.

STEINMETZOVÁ, Dana. *Bariéry konkurenceschopnosti* . Praha : Oeconomica, 2008. 162 s. ISBN 978-80-245-1444-4.

STRANYÁNEK, Tomáš. Jak zamezit krádežím firemních dat?. *IT Systems* [online]. 2001, 7-8, [cit. 2011-04-09]. Dostupný z WWW: <http://www.systemonline.cz/clanky/jak-zamezit-kradezim-firemnich-dat.htm>. ISSN 1802-615X.

Strategie ISCS. Praha : Celní správa ČR, 2009. 20 s.

STODOLA, Jiří. *Informace, komunikace a bytí : fragment realistické informační vědy*. 1. Brno : J. Stodola, 2010. 146 s. ISBN 978-80-254-7996-4.
Strategie ISCS. Praha : Celní správa ČR, 2009. 20 s.

ŠÁMAL, Pavel. *Trestní zákoník : komentář*. 1. Praha : C.H. Beck, 2009. 1285 s. ISBN 978-80-7400-109-3.

TONDL, Ladislav. *Technologické myšlení a usuzování*. Praha : Filosofia - AV ČR, 1998. 264 s. ISBN 80-7007-105-2.

TVRDÍKOVÁ, Milena. Příprava společnosti na zavádění a inovace IS : III. díl - Výběr dodavatele, řízení lidského faktoru při inovaci. *IT Systems* [online]. 2001, 12, [cit. 2011-04-06]. Dostupný z WWW: <http://www.systemonline.cz/clanky/priprava-spolecnosti-na-zavadeni-a-inovace-is-iii-dil-vyber-dodavatele-rizeni-lidskeho-faktoru-pri-inovaci.htm>. ISSN 1802-615X.

VÁGNER, Ivan. *Management z pohledu všeobecného a celostního*. 3. vydání. Brno : Masarykova univerzita v Brně, 2003. 603 s. ISBN 80-210-3536-6.

VEJLUPEK, Tomáš. Competitive Intelligence : vývoj a stav oboru. In *Cesty ke zvyšování konkurenceschopnosti v soukromém i veřejném sektoru a vzdělávání*. Praha : Nakladatelství ČVUT, 2006. s. 1-21. CD-ROM. ISBN 80-01-03597-2.

VEJLUPEK, Tomáš. Competitive intelligence : zpravodajské metody jako legální součást managementu. In JAROSLAV, Hujňák. *Žurnál Per Partes o managementu znalostí : znalosti v akci* . 1. Brno : Per Partes Consulting, 2002. s. 47-62.

VEJLUPEK, Tomáš. 2001. Firemní zpravodajský informační systém. In *Inforum 2001, 7. konference o profesionálních informačních zdrojích, 29. - 31. května 2001* [online]. [cit. 2007-05-02]. Dostupný z www: <http://www.inforum.cz/inforum2001/prispevky/vejlupek.htm>.

VOGELTANZ, Antonín. Hlídání dveří - nebo ochrana informací? . In JELÍNEK, Josef. *Ochrana dat a informací : sborník z odborného semináře konaného při příležitosti mezinárodní výstavy PRAGOALARM '96*. Praha : Family media, 1996. s. 6-8., Příl. čas.: Security magazín ; č. 3. 1996. ISSN 1210-8723.

VOKŮRKOVÁ, Lenka. Největší hrozby bezpečnosti IS/IT číhají uvnitř firmy. *Computerworld* [online]. 2006 [cit. 2010-10-15]. Dostupný z WWW: <http://businessworld.cz/cw.nsf/id/F2FE22A794D48549C1257109004FADE2>.

VYMĚTAL, Jan. *Informační zdroje v odborné literatuře* . 1. Praha : Wolters Kluwer Česká republika, 2010. 433 s. ISBN 978-80-7357-520-5.

VYMĚTAL, Jan, DIAČIKOVÁ, Anna, VÁCHOVÁ, Miriam. Informační a znalostní management v praxi . 1. vyd. Praha : LexisNexis, 2005. 399 s. ISBN 80-86920-01-1.