# Komerční zpravodajství v soukromých bezpečnostních službách

Competitive intelligence in the private security services

Vladimír Stojaspal

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Vladimír STOJASPAL** |
| Osobní číslo: | **A09607** |
| Studijní program: | **B 3902 Inženýrská informatika** |
| Studijní obor: | **Bezpečnostní technologie, systémy a management** |
| Téma práce: | **Komerční zpravodajství v soukromých bezpečnostních službách** |

Zásady pro vypracování:

1. Zpracujte rešerši literatury, která se vztahuje ke zvolenému tématu.
2. V rámci východiskové hypotézy specifikujte zkoumaný problém, vymezte soukromé bezpečnostní služby v historických souvislostech, včetně aktuálních právních aspektů (fenomenologie, etiologie).
3. Vymezte a analyzujte specifika komerčního (nestátního) zpravodajství v soukromých bezpečnostních službách.
4. Definujte metody, formy a prostředky, spojené s komerčním (nestátním) zpravodajstvím.
5. Vymezte potřebné profesní a psychologické a etické požadavky bezpečnostního pracovníka v oblasti komerčního (nestátního) zpravodajství – dispozice pro výkon bezpečnostních činností.
6. Prezentujte vlastní návrhy postupu, využitelné v praxi při defenzivním, ofenzivním zpravodajství.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:


1. BRABEC, František. Technologie detektivních činností. UTB: UTB, 2009. ISBN 978-80-7318-780-4.
2. BRABEC, František. Soukromé detektivní služby. Praha: EUROUNION, 2009. ISBN 805-58-5816-9.
3. LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. UTB: UTB, 2010. ISBN 978-80-7318 -889-4.
4. KAMENÍK, J., BRABEC, F. a kol.: Komerční bezpečnost (Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur). ASPI, Praha 2005
5. STRAUS, J. Kriminalistická technika. Plzeň : Aleš Čeněk, s.r.o., 2007.
6. KLOUDA, P. Moderní analytické metody. Ostrava: Pavel Klouda, 2003.


| | |
|---|---|
| Vedoucí bakalářské práce: | PhDr. Mgr. Stanislav Zelinka<br>Ústav bezpečnostního inženýrství |
| Datum zadání bakalářské práce: | 24. února 2012 |
| Termín odevzdání bakalářské práce: | 25. května 2012 |

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
*děkan*

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

## ABSTRAKT

Hlavním cílem bakalářské práce je vypracovat a zhodnotit komerční zpravodajství v průmyslu komerční bezpečnosti. Jedná se o důkladné seznámení s daným problémem jak z hlediska psychologického, etického, tak i z hlediska právních aspektů a platných zákonů České Republiky.

V teoretické části jsou vypracované pro toho téma důležité pojmy, formy, metody, subjekty a objekty, spjaté s komerčním zpravodajstvím defenzivním i ofenzivním.

V praktické časti bakalářské práce je uveden praktický postup při výkonu komerčního zpravodajství.


Klíčová slova: komerční, zpravodajství, bezpečnost, průmysl.


## ABSTRACT

The main objective of this thesis is to work out and to evaluate commercial coverage in the commercial security industry. It is about a thorough explanation with the problem in terms of psychological, ethical, and in terms of legal aspects and the applicable laws of the Czech Republic.

In the theoretical part there are the important concepts, forms, methods, subjects and objects, associated with the commercial coverage - defensive and even offensive, which are worked out.

In the practical part of the thesis a practical procedure for the performance of commercial coverage is given.


Keywords: Commercial, coverage, security, industry.

Tímto bych chtěl poděkovat za všechny poskytnuté informace a konzultace s tím spojené panu PhDr. Mgr. Stanislavu Zelinkovi jako vedoucímu práce.

**Prohlašuji, že**

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

**Prohlašuji,**

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

Ve Zlíně …….……

podpis diplomanta

# OBSAH

# ÚVOD

Komerční zpravodajství jako konkurenční boj v průmyslu komerční bezpečnosti je celek, kde se klade jako základní otázka či myšlenka snaha vést konkurenční boj pomocí forem a metod tímto celkem formulované. Jenom díky této činnosti můžeme být konkurenceschopní, shromažďovat informace a data, abychom byli vždy o krok vpřed, a tím získali výhodu, kterou ostatní nemají. V případě, že se jedná o ucelenou organizaci jednající ve prospěch jednotlivce, hovoříme zde o zpravodajské činnosti. K dosažení cíle je základem znalost a základem znalosti je informace v jakékoli její podobě.

Už od počátku obchodování ve všech podobách bylo považováno za to nejcennější udržet si svá obchodní tajemství, své know-how. Dnešní moderní trh je zaplaven návalem navzájem si konkurujících firem a každá z nich se snaží udržovat si technologický náskok, své výrobní a provozní tajemství, a tím i maximalizovat své zisky. Momentální rozvoj na poli informačních a komunikačních technologií nám umožňují neomezené zdroje informací v podobě dat na internetu.

Komerční zpravodajství se zaměřuje na veřejné a neveřejné zdroje, z nich čerpá a shromažďuje znalosti, aby je mohlo využít ve svůj prospěch, k zisku. U veřejných zdrojů uvádíme, že 80% získaných informací pochází právě z těchto zdrojů, zbylých 20% informací pochází z tzv. šedé zóny. Je tady využíváno technických prostředků a čerpání informací z neveřejných zdrojů. Přitom respektuje všechny platné právní ustanovení, které z této činnosti vyplývají a kterými se musí řídit. Z etického hlediska se jedná o odcizení informací, znalostí a jejich následné využití.

Pro vypracovávání této bakalářské práce jsem se snažil seznámit s danou problematikou co nejpodrobněji a to pomocí odborných publikací a poznatků, které jsem získal během studia.

# I. TEORETICKÁ ČÁST

# 1 VYMEZENÍ PROBLEMATIKY

## 1.1 Informace

V nejobecnějším slova smyslu můžeme informaci brát jako stav a proces v něm probíhající. Informace odstraňuje neurčitost celku. Ve vědě se informací rozumí sdělení, komunikovatelný poznatek, který usnadňuje volbu rozhodnutí. Informace se dělí z hlediska informační hodnoty na:

- Primární – nezkreslená a autentická fakta, vedoucí přímo ze zdroje, např. tiskové konference, vládní dokumenty, projevy, výroční zprávy, osobní pozorování.
- Sekundární – přechází z primárních informací, avšak nejsou totožné, jedná se o zkrácené nebo subjektivně vynaložené informace.

Norbert Wiener definuje informaci jako: "*Obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním*". [7]

## 1.2 Komerční zpravodajství

Pojem komerční zpravodajství (dále KZ) realizuje vědomé a systematické zásady práce s informacemi a následný proces jejich přeměny, to vše se děje mimo rámec orgánů státu a jejich institucí.

Je to označení procesu, který se používá k získávání a interpretaci informací pro usnadnění rozhodování subjektů KZ. Snaží se najít a získat výhodu nad konkurenční výhodou protivníka. Jedná se o metody a běžně užívané postupy komerčních zpravodajských služeb v prostředí jejich pravomocí. KZ pracuje s těmito základními druhy pojmů:

- Data – popis libovolné skutečnosti nebo její interpretace.
- Informace – soubor dat relevantní k nějakému konkrétnímu problému.
- Znalost – výsledek porozumění významu informace.

- Zpravodajství – znalost převedená do použitelné podoby pro konkrétní rozhodnutí.

Tento postup, proces se v dnešní moderní době neobejde bez podpory a znalosti dalších vědních oborů, jako jsou informační a komunikační technologie, psychologie, kriminalistika, managementu, a právních oborů.

Dříve bylo zpravodajství zejména státního druhu, např. špionáže, státní tajné služby atd., to se v dnešní době stále více přesouvá do komerčního sektoru za účelem zisku. [1]

## 1.3 Komerční zpravodajství nebo špionáž

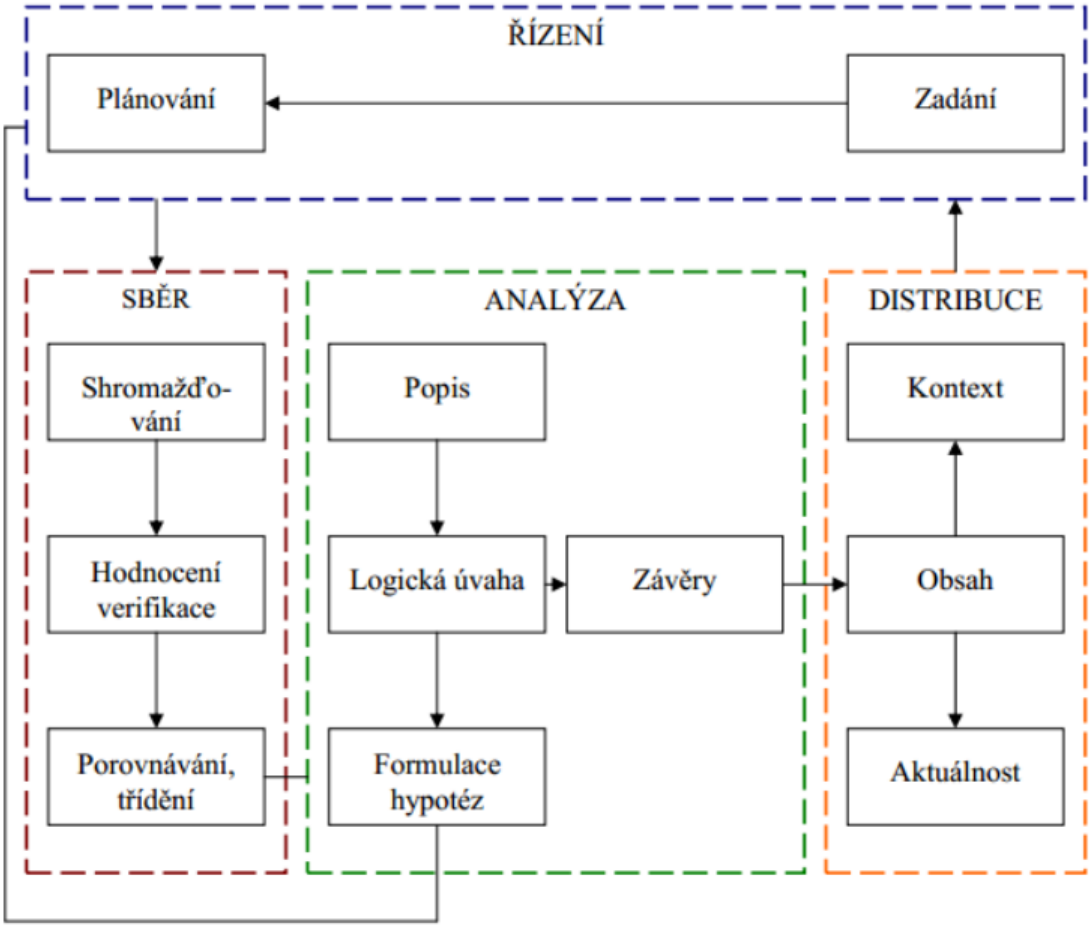
Kde jsou hranice mezi průmyslovou špionáží a komerčním zpravodajstvím? Poměrně velká část lidí – laiků v těchto dvou pojmech nevidí žádný rozdíl, a je to pro ně stále jedno a to samé – špionáž. Až 80 % informací získává zpravodajství z veřejně přístupných zdrojů, portálů, k metodám špionážní detekce se přistupuju jen v krajních případech.

Rozdíl mezi průmyslovou špionáží a komerčním zpravodajstvím se liší dle postupu shromažďování informací. Nejnovější metody, které využívají moderní technologie a se kterými pracují výhradně profesionálové, jsou využívány dle zákonů.

# 2 PROCES KOMERČNÍHO ZPRAVODAJSTVÍ

Základním předpokladem přeměny informací ve znalost a tvorbu využitelných znalostí je neustálá cirkulace otázek a odpovědí. Tento proces nazýváme zpravodajský proces. Dělíme ho na čtyři pilíře a to:

- Řízení.
- Sběr, hodnocení a třídění informací.
- Analýza a interpretace dat.
- Distribuce zprávy.




*Obr. 1. Zpravodajský cyklus. [2]*

Jednotlivé fáze na sebe postupně navazují a výsledný produkt činností je celek dělby práce uvnitř organizace a odráží se i vnitřním organizačním členění. Proto má pojem

zpravodajský cyklus důležitou roli při řízení zpravodajských organizací. Zpravodajská činnost začíná tehdy, je-li zadán úkol – požadavek, na dosud nezískané, avšak potřebné informace.

Začíná se plánováním prvního postupu směřujícího k zákazníkovi: odkud, kam a za kolik. Následuje sběr informací, a to utajeným nebo neutajeným postupem, vlastním know-how zpravodajské služby. Získané informace se musí vhodným způsobem zpracovat. Po důkladné analýze dat vzniká **zpravodajská informace**, ta už přináší přidanou hodnotu. Výsledkem je produkt, který je předán původnímu tazateli.

## 2.1 Charakteristika jednotlivých fází

### 2.1.1 Fáze první – Řízení

Zadávání úkolů, definice problému a definování požadavků se zdá být jednoduchým úkonem, ale realita bývá opakem. Plánování vyžaduje koordinaci času s jednotlivými procesy. Mezi první kroky plánování musíme zařadit, zda jsme správně porozuměli zadanému úkolu. Dále je třeba odpovědět na základní otázky. Jedná se o vymezení otázek na získání informací.

- Kdo, jak, pro koho.
- Cíle zadání.
- Vznik samotného problému.
- Kolik prostředků je možné čerpat.
- Jaké jsou hranice řešeného problému.
- Jak výsledek distribuovat.

Důležitým faktorem se stává plánování. Jedná se o určení priorit, patří sem akviziční politika zdrojů informací, tzn. vymezení množství dat, výběru a ceny. Při práci u větších organizací platí též plánovaní lidského faktoru, dále technologie, databáze a součásti na řízení nákladů spojených se zpracováním jednotlivých zadání. [1,2]

### 2.1.2 Fáze druhá – Sběr informací

Pro získání informací se používají nejrůznější metody a ty lze získat z různých zdrojů. Jednotlivým metodám se říká disciplíny sběru. Nejjednodušší členění zpravodajských zdrojů:

- Zdroje veřejně dostupné – Otevřené zdroje (Open Sources).
- Zdroje utajované – (Cover sources).

Zdroje utajované a její metody se dále dělí na:

- Získané kontaktem – od lidí.
- Získané na dálku – technickými prostředky.

Sběr informací je nedílnou součástí celku a bývá taktéž přeceňován, což má za následek zbytečné zvyšování nákladů na potřebnou techniku a zdroje informací. Také v této fázi dochází k ověření přijaté zprávy, její spolehlivosti a platnosti. To platí u informací starých a u zdrojů, u kterých nedošlo k jejich ověření.

**Hodnocení informací**

Další nedílnou součástí je hodnocení spolehlivosti dosavadních informací. Každá informace se hodnotí dle pravdivosti a věrohodnosti obsahu i zdroje. Hodnocení probíhá metodou 4x4, zde se každé informaci přiřadí odpovídající kód, který tvoří písmena A – D a číslice 1 – 4. Kódové označení, které se používá:

Hodnocení A – D, u zdrojů:

A. Nejsou pochyby o věrohodnosti a pravdivosti nyní, ani tomu nebylo dříve.
B. Zdroj v předchozích případech byl z většiny spolehlivý.
C. Zdroj v předchozích případech byl z většiny nespolehlivý.
D. Zdroj nebyl dosud ověřený, jsou pochyby o pravdivosti a věrohodnosti.

Hodnocení 1 – 4, u informací:

1. Informace je bez výhrad uvedena jako pravdivá.
2. Informace je zdroji osobně známá.
3. Informace je zdroji osobně neznámá, ale je potvrzena jinou již známou informací.
4. Informace je zdroji osobně neznámá a nemůže být potvrzena

Při sběru a pořizování zpravodajských informací, je důležité pravidlo: „*Co bylo řečeno, je pravda důležité; ještě významnější však je, kdo to řekl*“. [3]

### 2.1.3 Fáze třetí – Analýza a interpretace dat

Fáze analýzy je nejdůležitější fází, zde se prvotní surové informace mění do konečné zprávy (finished intelligence). Při analýze jsou původní data rozebírána na prvky a součásti. Systematicky se seskládají do potřebného svazku během syntézy. Analytický proces spočívá v několika krocích:

- Ohodnocení vstupní informace.
- Následná analýza informace.
- Integrace informací.

V této fázi se vytváří množství hypotéz a ty slouží buďto jako podpora výsledků, nebo jejich vyvrácení, vznikají na základě shromáždění existujících informací nebo informací doplňujících. Na hypotézy se musí nahlížet jako vedlejší jevy. To, co nás nejvíce zajímá, je aktuální stav informací.

**Předběžná zpráva**

Data, která se interpretují, je nutno sanitizovat – odpojit od údajů, které by vedly k originálnímu původu. Důvodem je ochrana vlastních zdrojů od získané informace. Příprava a schvalování výstupních dat ze zpravodajské činnosti je možnost pro důkladnou kontrolu a posouzení, zda je vše v pořádku a zda nevykazuje nežádoucí kvalitu.

Výsledek analýzy se jeví jako předpověď, či závěr. Je to hypotéza situace o současném stavu, ze kterého lze vycházet po provedení konkrétních rozhodnutí, ale stále

jsou zde přítomná rizika. Výsledky se zpracovávají různým způsobem, nejčastěji se jedná o strategický nebo operativní postup. Dalšími analýzami jsou považovány analýzy rizik a hrozeb. [1,2]

### 2.1.4 Fáze čtvrtá – Distribuce zprávy

Zpráva je distribuována za velmi pečlivého dohledu. Zprávy předávané uživatelům mohou být odpovědí na jejich požadavky, avšak zákazník nemusí být vždy spokojen. Je to způsobeno tím, že zpravodajství je proces s nejistými a probabilistickými výsledky.

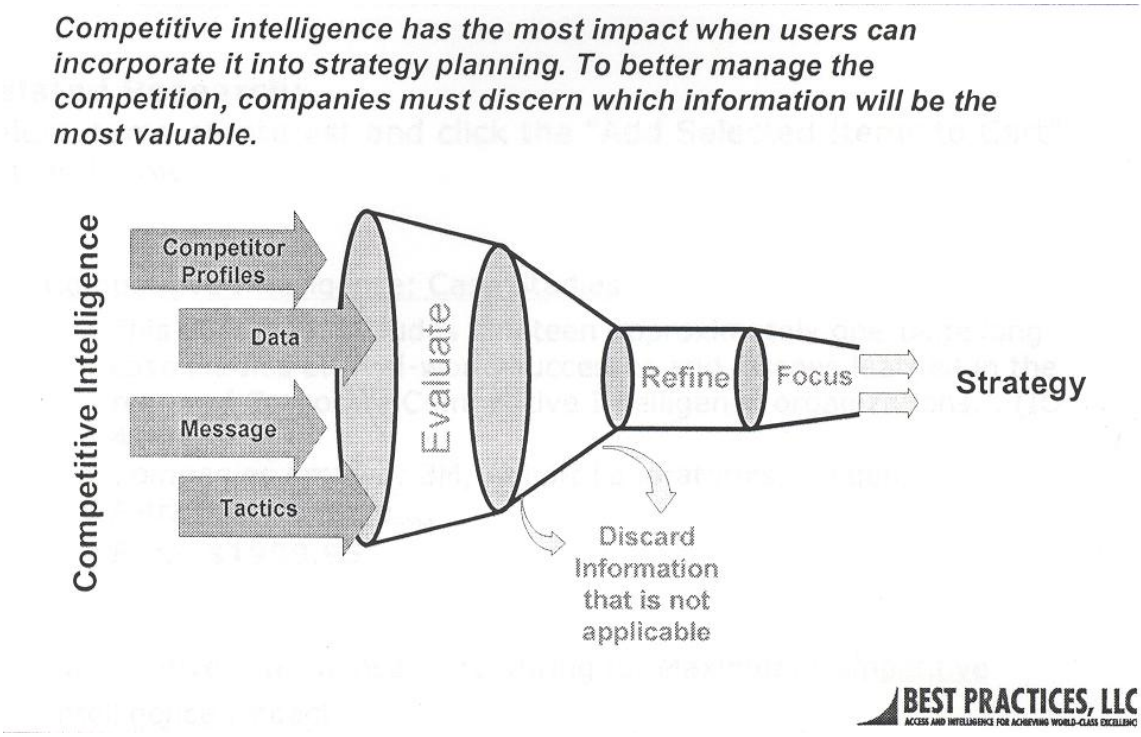
Výsledky procesu komerčního zpravodajství jsou:

- Avíza – upozornění.
- Analýza – prezentace závěrů.
- Reporty – souhrn informací a jejich dílčí závěry.

Je taktéž důležité, aby tyto informace byly předány v požadovaném časovém intervalu, kdy jsou poznatky aktuální. Jak se zpráva distribuuje, je individuální, záleží také na technickém vybavení. [1]

# 3 FORMY A METODY KOMERČNÍHO ZPRAVODAJSTVÍ

Mnohé organizace a podniky zjistili, že se bez komerčního (konkurenčního) nemohou obejít. Přijali fakt, že komerční zpravodajství je vyzbrojuje zbraní a potřebnými argumenty pro vlastní strategickou práci.




*Obr. 2 Základní koncept KZ. [8]*

Jistá americká společnost pro komerční zpravodajství definovala formy této činnosti takto:

- Komerční poznatky jsou důležité pro vedení podniku, pro jeho rozvoj a často i pro jeho přežití,
- občasné formy a neformální metody jsou neadekvátní,
- zdroje informací a poznání musí pocházet z veřejně přístupných zdrojů, musí být eticky přijatelné a legální.

Jak a kde získat potřebné informace o konkurenci? Je třeba vyloučit nelegální postupy, v některých případech dokonce víc a vyloučit postupy neetické, které jsou v rozporu s dobrými mravy.

Základní formy komerční zpravodajství jsou:

- Ofenzivní komerční zpravodajství.
- Defenzivní komerční zpravodajství.
- Vlivové komerční zpravodajství.

Komerční zpravodajství využívá činnosti infomačních a zpravodajských služeb. Distribuce informací pochází z otevřených zdrojů. Tyto formy využívají speciálně zaměřené kanceláře, firmy, ale i fyzické osoby, které získávají přehled nad okolím. Bezpečnostní charakter je specifická složka komerčního zpravodajství a je realizována dle uvážení. [4, 5]

## 3.1 Vymezení metod

Komerční zpravodajství je komplexní formou soukromé detektivní činnosti, která naplňuje cíle managementu znalostí a realizací jejích rozhodnutí.

V České republice se touto činností zabývají podniky průmyslu komerční bezpečnosti, které vlastní licenci na provozování detektivních činností. V jistém smyslu se tedy dá hovořit o činnosti soukromého detektiva jako o činnosti informačních a zpravodajských kanceláří. Proto i dané metody vychází z detektivní činnosti. [18]

## 3.2 Informační zdroje

Každá metoda je úzce spojena s typem informačních zdrojů – publikovatelné zdroje, nepublikovatelné zdroje. Metody, jak už bylo řečeno, by měli využívat legálního způsobu získávání informací. Příklady informací: internetové stránky, katalogy, noviny).

Zdroje informací, které jsou publikovatelné:

- k dispozici prostřednictvím informačních systémů,
- jsou veřejně přístupné,
- mají elektronickou a tištěnou podobu,
- např. statistika, patent, konferenční zpráva, výroční zpráva.

Některé informace nejsou běžně dostupné, ale měly by být, protože jsou veřejnými objekty. Tyto informace se musí shromažďovat za pomocí speciálních metod a forem.

Zdroje informací, které jsou nepublikovatelné:

- Burzovní zprávy,
- účetní a pokladní uzávěrky,
- trh, v němž je popsáno průmyslové odvětví,
- právní a legislativní dokumenty.

Zdroje, které se často neudávají, mohou být označovány jako polo-publikovatelné, nebo též „šedá literatura“. Tyto zdroje informací jsou velmi důležitou složkou ve zpravodajské sféře, ale materiály v této kategorii nejsou publikovány způsobem, jakým tomu bylo u publikovatelných a nepublikovatelných zdrojů. [5,7]

## 3.3 Využívané metody

### 3.3.1 Pozorování objektů

Jedna z nejčastějších metod, a zároveň nejjednodušší, je osobní pozorování. Jedná se o metodu ochrany osob a majetku a taktéž o pozorování klíčového zájmu. Užitek z této metody lze vyjádřit její bezprostředností a operativností. Tuto činnost může vykonávat každá fyzická osoba.

Jako další možnost pozorování můžeme zvolit cestou elektroniky. Jedná se o využití bezpečnostní techniky k ochraně osob a majetku. Mluvíme zde spíše o CCTV. [1,2]

### 3.3.2 Detektivní pátrání

Je též jednou ze základních pilířů forem detektivní činnosti. Informace se hledají dnes a denně spolu s osobními věcmi nebo osobami. Tato metoda je běžně realizovaná Integrovanými záchrannými složkami, jako je Policie České republiky (dále PČR).

### 3.3.3 Detektivní prověrka

Metoda, která zasahuje do všech ostatních. Je též jednou ze základních forem soukromé detektivní služby nebo komerčního zpravodajství. Tato metoda shromažďuje, představuje a interpretuje relevantní informace o:

- soustředění se na chování cílových osob v současné době i v minulosti,
- důkazech a informacích, které jsou v této metodě prověřovány

### 3.3.4 Detektivní rozpracování

Metoda, která svou komplexností a složitostí patří mezi nejsložitější metody. K plnému rozpracování a naplnění se používá i jiných forem detektivní činnosti. Přístup k formě musí být plánovaný, systematický, cílevědomý a komplexní. Metoda má uzavřený charakter a obsahuje:

- Vymezení problému,
- analýzu informací, které vyplívají z vymezených problémů,
- vymezení a rozhodování se v krocích, metodách a prostředcích k ověření, nebo vyvrácení detektivní verze,
- následuje ověřování jednotlivých verzí,
- detektivní rozpracování musí vyústit v nějaký konkrétní výsledek a je vhodně interpretován. [12,14]

### 3.3.5 Detektivní dokumentování

Všechny informace, které se nám dostanou do „rukou“ je nutno řádně dokumentovat, je to proces legalizace a zpracování do podoby přístupné veřejnosti. Musí být též na úrovni právních předpisů a platných norem. Postup evidence informací a příprava k předání klientovi:

- Vysvětlení postupu detektivního dokumentování,
- analýzou důkazů, činnosti osob ze všech dokumentů a jejich podobách,
- upřesnění postupu ukládání dat a ostatních příloh v souvislosti s platnou legislativou,

- v rámci zákona 101/2000Sb. o ochraně osobních údajů, je nutné prokázat oprávněnost výsledků, detektivního dokumentování,
- dokumenty předané klientovi musí splňovat právní legislativy. [2,14]

### 3.3.6 Detektivní vytěžování

Touto metodou detektivní činnosti směřujeme k získávání informací, které potřebujeme. Metodu detektivního vytěžování využívají profesionálové individuálně, přístup k metodě zvažuje každý zvlášť. Sama o sobě je tato metoda stěžejní, nezastupitelná, ale náročná z psychologického hlediska. Nutnost pochopit osobnost vytěžované osoby s sebou nese řadu otázek a sociální odpovědnosti:

- Osobní kontakt – zvládnutí navázání komunikace, odborná terminologie a znalost procesu komunikace,
- vytěžovaná osoba vám musí důvěřovat – nalezení vzájemného kontaktu a adekvátní přístup,
- dbát na psychologické a etické hlediska informací od vytěžované osoby – věrohodnost zprávy (informace).

Oblasti detektivního vytěžování jsou rozprostřeny do nejrůznějších odvětví a jejich zaměření je pestré:

- Vytěžování svědků a podezřelých osob,
- vytěžování poškozených osob,
- vytěžování osob s odbornou způsobilostí,
- vytěžování lidí z nejbližšího okolí místa činu,
- vytěžování lidí – správců databází a informačních center,
- vytěžování osob z marketingu a personalistiky. [2,14]

#### *3.3.6.1 Detektivní vytěžování evidencí*

Veřejná místa jako jsou registry a evidence, mají velký význam z pohledu zdrojů informací. V těchto místech je velmi složitá otázka legality, proto je nutné tyto evidence a registry rozdělit:

- Veřejně přístupné – po zaplacení poplatku má do databáze právo vstoupit každý,
- neveřejné,
- důvěrné,
- utajovaného charakteru.

Všechny tyto body jsou velmi vzácným zdrojem informací, ale není prioritní otázkou získat informace týkající se utajovaného charakteru, protože porušuje platné zákony České republiky, zvláště potom trestního zákoníku. [2,14]

### 3.3.7 Detektivní informační proniknutí

Pro zkvalitnění metod, jako jsou detektivní prohlídka či detektivní rozpracování, je důležité získání a vybudování informačních zdrojů. Tato metoda je komplexní a kombinovatelná z pohledu ostatních metod. Jedná se o základní skutečnost detektivní činnosti a jednu z nejvýznamnějších. Souhrnný přehled směru informačního proniknutí:

- Jedná se cílevědomý přístup pro získání informace,
- jedná se o komerční činnost,
- nejedná se o státní donucovací prostředek,
- informace jsou zbožím, a to velmi ceněným.

Zdroje informací mohou být stavěny jako cílené informační zdroje, zdroje, které jsou vytěžované ke konkrétním cílům či případům.

Metodu je také nutno brát jako velice obtížnou a náročnou na odbornou způsobilost a profesionalitu. Proces získávání informátorů a nadcházející proces jejich kontroly je spojován s dalšími detektivními metodami. [2,14]

### 3.3.8 Detektivní kombinace

V této metodě hraje roli plánování a následná realizace souboru úkolů, které mají za cíl získat pro daný případ soukromého detektiva či zpravodajce relevantní informace. Informace o cílovém objektu a předměty detektivního působení.

Detektivní kombinace jako metoda představuje model systémového řízení přístupu k řešení problémových okruhů. Jde o využití obecných, avšak zejména psychologických metod, reflexivních her. Podstatou je vyvolání prostředí a jisté situace s cílem vyvolat reakci zájmového, prověřovaného jedince. [2,14]

### 3.3.9 Technická ostraha a ochrana

Technická ostraha a ochrana míst a prostorů spjatých s podnikovou činností. Technickou ostrahu můžeme rozdělit dle technických principů, podle kterých pracuje, ale i podle předmětů, které mají chránit, dle nebezpečí nebo rizika, které stanovují normy.

Dle předmětu, které mají technické prostředky chránit, jsou určeny:

- Prostředky k ochraně života a zdravý fyzické osoby – neprůstřelné vesty, auta,
- prostředky k ochraně majetku – řadíme sem systémy PTZS a jednotlivé prvky MZS,
- prostředky k ochraně informací – generátory šumu, trezory.

Podle rizika a nebezpečí, jenž mají technické prostředky chránit, rozeznáváme:

- Prostředky pro ochranu proti útoku pachatele, jsou to všechny bezpečnostní prostředky, protipožární signalizace, tísňové hlásiče, mechanické zábranné systémy, kamerové systémy atd.
- Prostředky pro ochranu před živelnými pohromami, jsou to zejména detekční zařízení – jejich smysl je včasné varování vznikající nebo hrozící situace.
- Prostředky pro ochranu proti průmyslovým haváriím, jsou to zejména detekční zařízení a monitorovací stanice ke včasnému varování, před

blížícími se mi událostmi. Jedná se o různé typy havárií – ropné úniky, úniky plynů a zdravý škodlivých látek.

- Prostředky pro ochranu časové nouze – sem řadíme systémy signalizace, na které musí obsluha reagovat v určitém časovém intervalu, jinak systém automaticky provede vypnutí či odpojení systému.

Můžeme tedy říct, že se jedná o plné využití všech bezpečnostních technických prostředků a faktorů. [1,2,17]

### 3.3.10 Využití zákonů k ochraně

Tyto metody se využívají zvláště za předpokladu splnění podmínky nutné obrany a krajní nouze. Jde o jednoznačnou a i nejasnou problematiku fyzické ochrany a ostrahy. Využívání těchto metod se doporučuje tam, kde to za daných okolností případ vyžaduje. Před použitím těchto paragrafů by mělo předcházet promyšlení, zda ji lze využít. Pouze při provádění zákroku obranného charakteru je nutno dodržovat tento postup:

- Způsob provedení zákroku by měl být co nejšetrnější, aby nevznikla újma na zdraví ani jedné zúčastněné osobě,
- pokud nějaká osoba jedná protiprávně, varovat ji předem, že proti ní směřuje zákrok,
- je-li potřeba, po provedení zákroku poskytnout první pomoc,
- ohlásit situaci na příslušném místě PČR,
- po skončení zákroku zajistit svědky, pokud jsou a dovoluje nám to situace, až do příjezdu PČR.

## 3.4 Informační činnost

Pod informační činností se skrývá **analytická činnost**, která nabírá na mimořádné pozornosti. Jedná se o činnost manažerů a jejich přístup k analytické práci při využití svých schopností – psychologických či fyziologických. Analýza pracuje na rozboru celku rozdělením na jednotlivé prvky s cílem podívat se na řešení problému.

Informační činnost je významná vzhledem:

- K rozvoji průmyslu komerční bezpečnosti,
- ovlivnění vývoje i specializace a profesionalitě.

Je to proces studia podstaty věci, který se využívá pro rozhodnutí a plánování v průmyslu komerční bezpečnosti. [7]

# 4 ROZDĚLENÍ FOREM KZ

V celku komerčního zpravodajství působí celkem tři ucelené formy, které vystupují jako formy komerčního zpravodajství. Každá tato forma je specificky rozpoznatelná od dalších tím, jak naplňuje svůj účel a pro co je primárně určena. Jedná se jak o ochranu informací, tak i o zisk informací pro účel zisku a konkurenceschopnosti, která vede k rozvoji ekonomiky. Základní dělení komerčního zpravodajství je následující:

- Defenzivní KZ
- Ofenzivní KZ
- Vlivové KZ

Pod každou formou se najde ucelený postup a zpravodajský proces odpovídající jednotlivým formám.

## 4.1 Defenzivní komerční zpravodajství

Defenzivní neboli obranné zpravodajství se využívá k ochraně dat a informací, které si chce a hodlá daný objekt ochránit před ztrátou a případným využitím v jejich neprospěch. Jedná se o možnou minimalizaci zveřejňování interních citlivých dat a jejich následné zneužití. Tato forma se zaměřuje na analýzu informací, které byly vytvořeny u daného objektu či firmy, jejich zveřejňováním a ochrannou. Možnosti této obrany spíše využívají větší firmy a také organizace, které pracují s větším množstvím patentů, jejich sestrojováním a distribucí.

Na druhou stranu můžeme také říct, že defenzivní zpravodajství využívají i organizace, které o této problematice nemají téměř žádné informace. Reagují na základě principu ochrany své činnosti a drží v tajnosti informace, které brání za každou cenu. Ztráta těchto informací může mít za následek úplnou ztrátu postavení firmy na trhu nebo může způsobit újmu nenahraditelné škody. Místa, kde se informace setkávají s rovinnou činnosti obranného komerčního zpravodajství, jsou následující:

- Fyzická bezpečnost podniku, možnost odcizení dat, umístění odposlouchávacích zařízení, sabotáže, ale i ochrana před vlastními zaměstnanci a jejich možnosti zasahovat bez příslušného osvědčení do centrálního informačního zdroje podniku.

- Technické zabezpečení informací, sem přímo spadá sféra zařízení na kontrolu proti odposlechům, kontrola přístupu k umístění dat (např. biometrická ochrana, šifrování dat).
- Ochrana před lobbingem – jedna z možností útoku na podnik pomocí další formy komerčního zpravodajství, a to vlivovým zpravodajstvím. Tento potencionální útok pomocí lobbingu se těžce odhaluje a ochrana před ním je taktéž velmi složitá. Můžeme sem také zařadit principy sociálního inženýrství, jehož rozmach v posledních letech roste.
- V poslední řadě je to režimová bezpečnost. V daném problému organizace se řeší způsob, jakým budou lidé postupovat při ochraně organizace, řadíme sem činnosti v oblasti administrativy a činnost lidí uvnitř organizace, sledování pohybu osob přicházejících zvenčí a výstupy informací a dat z organizace.

### 4.1.1 Bezpečnostní politika

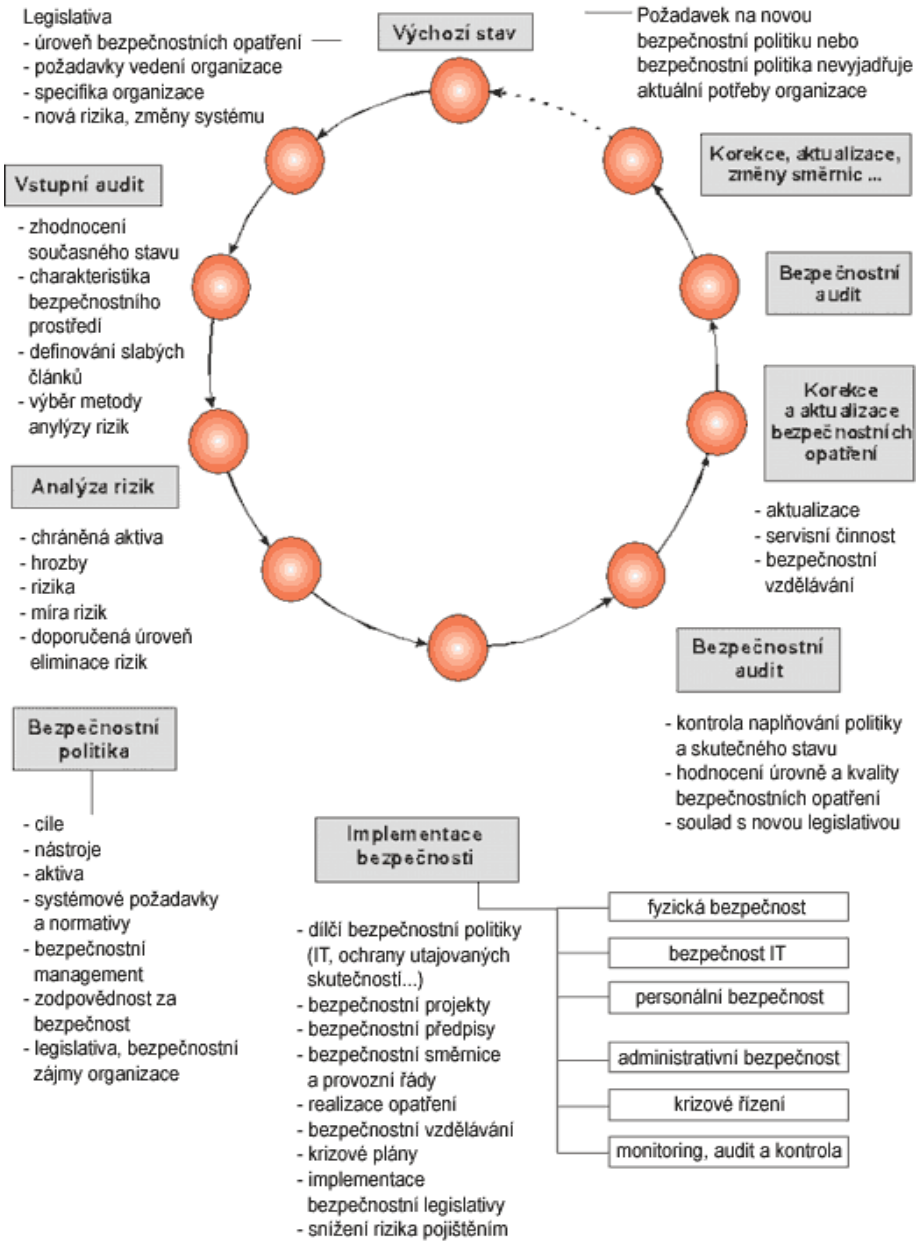
Bezpečnostní politika podniku/organizace v sobě zahrnuje pokyny, podle kterých se řídí celé personální uspořádání organizace včetně lidí, kteří tuto bezpečnost řídí. Je základním dokumentem, který stanovuje strategii a zásady bezpečnosti jak v informačním prostředí, tak i v personálním uspořádání.

Bezpečnostní politika se řídí normou ISO/IEC 27001 a ISO/IEC 27002, kde se definují cíle organizace při zajištění bezpečnosti z řad personální bezpečnosti, fyzické bezpečnosti a prostředí bezpečnosti, řízení přístupů, vývoj a údržba konfigurovaných systémů, podmínkou je soulad s požadavky daného předpisu. Další podmínkou bezpečnostní politiky je stanovení organizační struktury, která bezpečnost řídí, dohlíží na ni a také preferuje. Na tyto pozice se dosazují facility manažeři. Předpis bezpečnostní politiky by měl obsahovat:

- Výklad předpisů bezpečnostní politiky organizace,
- dodržování požadovaných norem,
- režimovou ochranu a vzdělání v bezpečnosti informací,
- definici bezpečnosti informací společně s jejím cílem,

- přímý odkaz na bezpečností dokumentaci, která podporuje bezpečnostní politiku organizace.

Bezpečnostní politika přináší do organizace jasně formulované základní principy řízení informační bezpečnosti. Všichni účastníci budou znát svá práva, povinnosti a základní odpovědnost. S tím je spojena povinnost při práci s informacemi. Uplatňování bezpečnostní politiky je na základě vypracovaného dokumentu v prostředí informačního systému organizace. Zavedení bezpečnostní politiky přináší vyšší prestiž a hodnocení nezávislou třetí stranou. [3,6]




*Obr. 3. Schéma bezpečnostní politiky organizace. [6]*

### 4.1.2 Bezpečnostní analýza

Cílem bezpečnostní analýzy v PKB zaměřené na defenzivní komerční zpravodajství je správné vyhodnocení rizik spojených s ochranou informací uvnitř organizace. Je nutné hrozby pojmenovat, identifikovat tak, aby výsledná zpráva byla přínosem pro organizaci. Bezpečnostní analýza je prováděna na základě současných nejlepších norem a standardů používaných v oblasti bezpečnosti. Počítáme i s analýzou rizik, a to s **hrubou úrovní**, analýza je prováděna a vytvářena na základě všeobecných standardů, bere v úvahu hodnotu celkového systému, zpracovaných informací a rizika činnosti celé organizace. Dalším typem analýzy je **neformální přístup**. Metoda je zde prováděna neformálně, pragmaticky, využívá znalosti a zkušenosti jednotlivců v rámci organizace.

Následuje analýza pomocí **kombinovaného přístupu**, jedná se o kombinaci předchozích vstupních analýz, kdy se provádí nejprve počáteční analýza na hrubé úrovni pro všechny stupně systému. Tyto jsou hodnoceny jako významné pro činnost organizace. Pokud je možnost vysokých rizik, měla by tato zpráva být podstoupena **podrobnému přístupu**. Je to analýza rizik spojená s identifikací a odhadem velikosti jednotlivého rizika pro organizaci. Také se zde provádí zkouška nepříznivých dopadů a nežádoucích událostí na činnost organizace a pravděpodobnost jejího výskytu.

Bezpečností analýza se vztahuje nejen k informačnímu bezpečí, ale z pohledu zabezpečení i k hmotnému majetku. To se týká zabezpečení objektů jako celku, výrobního zařízení, ochrany života a zdraví v cílovém objektu, ale taky výrobků a zásob. [6,16]

### 4.1.3 Postup bezpečností analýzy

Zde se vychází z procesu plánování, kdy je nejdůležitější určení cílů a priorit, kterých chceme dosáhnout ke kvalitní bezpečnostní analýze. Z hlediska priorit se jedná zvláště o:

- Stanovení rizik bezpečnosti,
- časový úsek,
- finanční prostředky,
- posouzení hrozeb – zejména těch, které se jeví jako reálné,
- návrh konkrétního zabezpečení,

- návrh bezpečnostní politiky organizace,
- návrh dalšího postupu.

#### *4.1.3.1 Kvalitativní a kvantitativní analýza*

Kvalitativní analýzou rozumíme rozbor všech možných rizik v určeném časovém úseku. Vychází z událostí, které organizace už v minulém období trápily a snaží se podobným věcem předejít. Na to navazuje analýza příčin, která zkoumá následek a událost, která k tomuto následku vedla. Hledí se na časový úsek mezi těmito částmi. Další částí kvalitativní analýzy řešíme otázku lidských zdrojů, zkoumají se chyby při činnosti v různých sférách zaměření jedinců. Jedná se o analýzu lidské činnosti při podnikání.

Kvantitativní analýza je úvodní činnost v analytické analýze a klade si za cíle minimální oblast zaměření a identifikovat možnou hrozbu a míru rizika, které by mohlo vzniknout. Jedná se o rychlý přehled provozního nebezpečí. Kvantitativní analýza se stala primární činností při kontrole bezpečnostních událostí v informačních systémech. [16]

### 4.1.4 Bezpečnostní projekty

Bezpečnostní projekt volně navazuje na bezpečností analýzu a ve svém principu nám má předložit návrh zabezpečení v souladu s právními předpisy a normami. Měl by být svým obsahem dostačujícím podkladem pro všechny potřebné kroky, které by organizace měla učinit, a to v určitém časovém úseku, kdy stále platí vypracovaná bezpečnostní analýza. Projekt zohledňuje návrh přijetí bezpečností politiky organizace a svým obsahem je přínosem pro celkovou bezpečnost. V souladu s bezpečnostním a právními předpisy se projekty komerčního zpravodajství rozdělují podle zaměření na:

- Obecné,
- projekt fyzické – personální ochrany organizace,
- projekt elektronické ochrany organizace,
- projekt detektivní ochrany organizace. [14,16]

### 4.1.5 Personální bezpečnost organizace

Personální bezpečnost klade důraz na ochranu před lidským faktorem. Dává si za cíl eliminovat chyby, které způsobují interní pracovníci, jako např. krádeže, podvody, nebo zneužívání prostředků organizace ve svůj vlastní prospěch. Tato část defenzivní komerční zpravodajské činnosti pojednává o nejrizikovějším faktoru uvnitř organizace. Personální bezpečnost začíná již při samém přijetím zaměstnance do organizace.

Zde nastupuje zpravodajská činnost, aby vypátrala a přezkoumala informace o této osobě a zohlednila jeho spolehlivost a loajálnost v případě, kdy má zaměstnanec přímý přístup k informacím, které chceme chránit před konkurencí. Zaměstnanci, kteří budou mít přístup k utajovaným informacím, musí podstoupit bezpečnostní prověrku a musí být seznámeni se smlouvou o mlčenlivosti. [6]

### 4.1.6 Bezpečnost informace

Jedná se o ochranu údajů před neoprávněným přístupem, u počítačových sítí je to řešeno nastavením příslušných práv osobě, která s těmito informacemi pracuje. Bezpečnost informací v rámci dobře zvoleného technického prostředku. Uživatel těchto dat šířených v interní síti organizace je povinen zabezpečit své přístupové místo v době své nepřítomnosti, a to způsobem odhlášení ze systému, nebo vypnutí zařízení, v němž je tato informace uložena. Nesmí však narušit bezpečnost svým vlastním jednáním. Jakékoli narušení musí být bezodkladně hlášeno vedoucímu pracovníkovi bezpečnostního managementu (ve větších organizacích faciliti manažer).

Jedná se o ochranu know-how, patentů, výrobních tajemství, ale také důležitých firemních jednání, setkání akcionářů, výroční schůze či dalších cenných a důležitých dokumentů a kontaktů.

Zpravidla jde o ochranu místnosti před odposlechem či sledováním, „nabouráním do počítače“ – ochrana před hrubou silou. V případě počítačů je nejrozšířenějším způsobem ochrany dat šifrování a uchovávání, je-li to nezbytné, mimo veřejnou síť a internetem.

Při ochraně před odposlechem místnosti, mobilního zařízení, automobilu je nezbytné využít technických prostředků, které jsou k tomuto účelu stvořeny a které se

aktivně využívají nejen ve státní správě, kde jsou ve větší míře používány, ale také při interních schůzích podniku či osobní schůzce.

## 4.2 Ofenzivní komerční zpravodajství

Ofenzivní komerční zpravodajství je základem při získávání informací o osobě, objektu či organizaci. Ve své činnosti se zabývá získáváním, shromažďováním, tříděním a analýzou informací, které jsou potřebné ke konkurenčnímu boji, popř. k navýšení vlastní převahy nad konkurencí a maximalizování zisku. Spadají sem všechny informace o konkurenci a trhu. Za cíl si také klade snížení míry neurčitosti pro daný problém při rozhodování. Může být hlavní příčinou zahájení aktivního útoku na konkurenci za účelem získání strategické výhody na trhu.

Ofenzivní zpravodajství je pokračování pasivního monitoringu informací, který v sobě zahrnuje pouze fáze sběru a distribuce informací. Postup ofenzivního zpravodajství je vázán na používání technických prostředků pro snaží získání dat, přitom ale není spojeno s konkrétní technologií. Jedná se o individuální přístup zpracovávání informací.

Základem této činnosti jsou prvky založené na detektivní činnosti jako sledování, získávání a vyhodnocování velkého množství dat ze širšího spektra informačních zdrojů. To už dnes téměř nelze provádět bez příslušných technických prostředků. Podstatou ofenzivního zpravodajství jsou postupy, pomocí kterých dosahujeme:

- Odhalení strategie konkurenční organizace a následné využití těchto znalostí ve vlastní prospěch jak u celé organizace, tak i u jedince,
- zajištění informací marketingového charakteru,
- škála informací důležitých pro rozhodování organizace v procesu podnikání.

Informace získané v průběhu činnosti ofenzivního zpravodajství také aktivně napomáhají i vlastní obraně podniku. Cesty, kterými jsme získali informace od konkurence, bychom měli dobrým způsobem ošetřit i ve vlastní organizaci, aby konkurence nevyužila našich vlastních postupů ve svůj prospěch.

Ve prospěch tohoto typu komerčního zpravodajství je též důležitým faktorem časový úsek, ve kterém je činnost vykonána, správné zadání úkolů je polovina úspěchu. V části plánování popisujeme konkrétní informaci, které chceme dosáhnout a na kterou se

chceme soustředit, abychom dosáhli správně zodpovězených hledaných odpovědí. Ofenzivní zpravodajství čerpá ze zdrojů informací, jak už bylo řečeno v úvodu, komerčního zpravodajství pouze z veřejně dostupných informací a z detektivní činnosti s využíváním technických prostředků. [17,18]

### 4.2.1 Zisk informací

Klíčovou částí v oboru komerčního zpravodajství je samozřejmě zisk informací. Praktiké a technické zázemí nám umožňují využití rozdílných způsobů a strategií pro získávání důležitých informací. Můžeme hovořit o informačních aktivitách firemního zpravodajství, které lze označit za veřejné a legální zdroje:

- Jsou to informace z otevřených veřejných zdrojů,
- vlivové zpravodajství – lobbing zaměstnanců,

až tam, kde legální činnost jde stranou a nastupuje odvětví, které se pohybuje na hraně zákona. Je to jednání neetické a téměř ilegální. Patří sem:

- veřejně dostupné odposlechy,
- informační proniknutí s využíváním praktik sociálního inženýrství
- a korupce.

Ofenzivní zpravodajství ke své činnosti v dnešní době využívá především internet. Je to místo, kde se zisk informací jeví jako nejjednodušší a nejrychlejší. Pokud ten, kdo provozuje zpravodajský servis, ví, co má hledat a kde to hledat, můžeme říct, že všechny informace uložené v této síti nejsou v bezpečí. Vyhledávání přes internet se realizuje pomocí webových vyhledávačů, internetových adres či internetových katalogů. Profesionál v tomto oboru je tedy nepostradatelný pomocník při hledání informací.

Ve sběru informací pomocí internetového vyhledávače, kde vyhledáváme klíčová slova, se snažíme zaměřit na informace objektivním pohledem a každou informaci si ověřujeme, snažíme se také o minimalizaci vyhledaných webových stránek z důvodu zpřehlednění práce informátora. [7,12]

Jednoduchým způsobem zisku informací je také nákup informací. Zde využíváme služeb odborníků, kteří s těmito informacemi přichází denně do kontaktu, má o nich kvalitní znalosti a záznamy. Jedná se o neetický a zákonem postihnutelný proces zisku

informací. Dle zákona 40/2009 Sb. trestního zákoníku se korupce přímo nevyskytuje, ale je možné ji brát jako: „*Trestné činy proti pořádku ve věcech veřejných*“ a to: [18]

- § 331 o přijetí úplatku,
- § 332 o podplácení,
- § 333 o nepřímém úplatkářství,
- § 334 o společném ustanovení, které vymezuje pojmy úplatek a obstarávání obecného zájmu.

### 4.2.2 Komerční informace

Jedná se o odvětví informací, které se týkají hlavní činnosti podniků a organizací, mají tržní hodnotu a na jejich získání (taktéž i ochraně) má organizace zájem. Získávání těchto informací má vliv na konkurenčním poli trhu, kde podnik získá značnou výhodu díky těmto druhům informací.

Komerční informace jsou data, které úzce souvisí s typem podnikání, druhem výroby a technologickými postupy organizace a též s patentovými vynálezy. Další ryze cenná data se pohybují v rámci zákona o osobních údajích. Jsou to informace o trestních řízeních, identifikačních údajích, bankovních institucích, spisy vyšetřovatelů apod.

## 4.3 Vlivové zpravodajství

Vlivové zpravodajství neboli lobbingové zpravodajství je souborem metod a forem působících na lidský faktor v organizaci. Ovlivňuje vývoj akcí, které jedinec koná na „vlastní pěst“, taktéž se sem zařazují kroky obchodních partnerů a konkurence samotné. V podstatě se jedná o prosazení zájmů třetí osoby, která chce získat interní informace a snaží se jich dosáhnout jinou cestou než přes ofenzivní komerční zpravodajství. Lobbing působí nejčastěji těmito metodami:

- Cílené metody na fyzickou osobu uvnitř organizace s využitím argumentů,
- sociální inženýrství,
- asertivní a demonstrativní metody,
- dezinformace.

K této činnosti přispívají značným dílem také veřejnoprávní média, která slouží jako prostředek k ovlivnění osoby. Děje se to pomocí cílených sdělovacích prostředků, které jsou našemu záměru blízké.

### 4.3.1 Lobbing a jeho techniky

Jak bylo zmíněno, lobbing působí v těchto sférách:

- Cílené metody na fyzickou osobu uvnitř organizace s využitím argumentů. Je založena na zpracování informací, které jsou věrohodné, je to metoda, která je účinná a významově nejjednodušší. Tuto metodu může využívat jak soukromý detektiv, tak i management organizace.
- Sociální inženýrství volně navazuje na předchozí metodu, ale s tím rozdílem, že je mnohem více propracovaná a je do ní zapojeno více osob. Jedna osoba může působit důvěryhodně na osobu cílenou a tato osoba, bez ohlédnutí na základní bezpečnostní předpisy organizace, vydá informace, které jsou důvěrné a mohou způsobit újmu nejen jemu, ale i celé organizaci.
- Asertivní a demonstrativní metody, se zaměřují na kampaně, výstavy, veletrhy, exkurze apod.
- Dezinformace představuje metodu detektivního původu. Slouží k rozptýlení nepravdivé zprávy, ke zmatení konkurence. Je základem jedné z metod detektivní činnosti a rovněž komerčního zpravodajství. Dezinformace volně znamená zkreslenou či jinak upravenou informaci, která má uvézt druhý subjekt v omyl. [1,2,5]

# 5 SUBJEKTY A OBJEKTY KOMERČNÍHO ZPRAVODAJSTVÍ

Proces vyhledávání informací je navázán na základní subjekty informačního průmyslu. Pro výklad základních vztahů mezi těmito subjekty se užívá tento příklad se třemi následujícími prvky:

- Producenti a tvůrci informací a informačních systémů,
- poskytovatelé informačních systémů
- a uživatelé informací a informačních systémů.

Tyto skupiny subjektů užívají architekturu informačního průmyslu. V praxi jsou vztahy mezi jednotlivými subjekty značně mnohonásobné a komplikovanější. Velmi časté jsou spoje mezi producenty a poskytovateli, kdy tyto dva subjekty bývají označovány za jeden, což má za následek zjednodušování informačních systémů (např. databáze). Taktéž se v praxi vyskytuje model, kdy zprostředkovat informačního toku bývá označen společně s uživatelem a následně s odpovědností za autorská práva. [1,2,10]

## 5.1 Producenti a poskytovatelé informací

Mezi instituce, které podporují a produkují elektronické informační zdroje, patří:

- Producenti a vydavatelé primárních dokumentů (česká a zahraniční nakladatelství), producenti z řad oborových informací (management, matematika, …),
- distributoři a prodejci,
- dále to jsou služby dodávání dokumentů (knihovny),
- bibliografické a referátové služby,
- instituce státní správy a samosprávy (ministerstva v ČR),
- specializované informační instituce.

## 5.2 Databázové centra

Z hlediska vyhledávání informací je jedním z hlavních cílů skupina provozovatelů databázových center. Tato centra poskytují značnou škálu sofistikovaných nástrojů

vyhledávaní informací. Příkladem může být databázové centrum Dialog, které je komplexním provozovatelem informačních systémů se snadným nástrojem na vyhledávání. Pokrok v sofistikovaném vyhledávání informací je natolik pokročilý, aby umožňoval agregátorům volný přístup k informacím. Databázová centra lze rozdělit podle různých kritérií jak podle velikosti, tak i podle cílového subjektu. Databázová centra podle rozdělení dle velikosti:

- Velká – obsahují stovky databází,
- střední – obsahují desítky databází,
- malá – obsahují jednotky databází.

A podle oborového zaměření:

- Centra určená dle konkrétního oboru,
- centra polytematická – inženýrské obory,
- univerzální. [5]

## 5.3 Uživatelé informací

Mezi uživatele (subjekty) komerčního zpravodajství patří osoby výdělečně činné a zabývající se komerčním zpravodajstvím, dále komerční zpravodajské kanceláře a detektivní kanceláře. Spadá sem také oblast skrytých subjektů komerčního zpravodajství, které ke své činnosti využívají lobbingu: [9,18]

- PR agentury a kanceláře,
- reklamní agentury a kanceláře,

Typickými uživateli komerčního zpravodajství jsou:

- Politické strany a hnutí,
- bankovní instituce,
- živnostenské společnosti,
- bezpečnostní agentury,
- státní sektor.

# 6 PLATNÉ ZÁKONY V KOMERČNÍM ZPRAVODAJSTVÍ

Zákonů a právních předpisů, které se dotýkají přímo nebo jen okrajově práce s informacemi či informačními systémy, je mnoho. Jedná se také o instituty svobodného přístupu k informacím a ochraně osobních údajů nebo také o institut mlčenlivosti, o právní úpravy utajovaných informací a zvláštních skutečností.

## 6.1 Vymezení zákonů

- *„**Zákon č. 513/1991 Sb.** – Obchodní zákoník.“*
- *„**Zákon č. 63/1991 S.** – Ochrana hospodářské soutěže.“*
  a) *§ 16 Zákona č. 63/1991 Sb. – Výrobní tajemství.“*
- *„**Usnesení ČNR č. 2/1993 Sb.** – Vyhlášení listiny základních práv a svobod, jako součástí ústavního pořádku ČR.“*
- *„**Zákon č. 412/2005 Sb.** – Ochrana utajovaných informací a bezpečnostní způsobilost.“*
- *„**Zákon č. 240/2000 Sb.** – Krizové řízení.*
  a) *§ 2 pís. D a § 27 Zákona 240/2000 Sb.“*
- *„**Zákon č. 101/2000 Sb.** – Ochrana osobních údajů.“*
- *„**Zákon č. 106/1996 Sb.** – Svobodný přístup k informacím.“*

Další instituty o utajovaných informacích jsou především zvláštní skutečnosti, obchodní tajemství, ochrana průmyslových práv, autorská práva, mlčenlivost, svobodný přístup k informacím a ochrana osobních údajů. [10,17,18]

## 6.2 Zvláštní skutečnost a obchodní tajemství

Tento státní institut byl zřízen kvůli zákonu 240/2000 Sb. o krizovém řízení a stanovuje pravomoc státních orgánů, jejich práva a povinnosti. Taktéž stanovuje práva a povinnosti fyzických a právnických osob při přípravě a v době krizové situace. [18]

## 6.3 Obchodní tajemství a mlčenlivost

Dle platného právního předpisu ČR do obchodního tajemství zahrnujeme veškeré skutečnosti obchodní, výrobní a technické – vše co souvisí s povahou podniku. Problematika obchodního tajemství, je zákonem ustanovena v těchto paragrafech: § 17, § 44, § 51. Další předpisy určují normy z oblasti průmyslové ochrany – patenty aj.

Mlčenlivost je v našem právním systému deklarována v konkrétních právních vztazích jako tajemství, a to lékařské, poštovní, osobní. Předmětem ochrany jsou zpravidla konkrétní informace o údajích občanů. Ochrana je zcela v zájmu jednotlivců. Tento institut lze definovat jako okruh osob, které mají povinnost zachovávat mlčenlivost, a skutečnosti tímto zákonem chráněné. Povinnost mlčenlivosti je také upravena v zájmu utajovaných informací, a to přímo zákonem. Zákon hovoří o tom, že je povinnost nesdělovat utajovanou informaci osobě, která nemá oprávnění se s touto informací dostat do styku. [14]

## 6.4 Svobodný přístup k informacím

Právo každého jedince je získat od státu a jeho orgánů informace, týkají-li se jeho činnosti (státní zakázky). Přístup k informacím musí být sdělen bez odmítnutí s odvoláním na skutečnost, že osoba, která se těchto informací snaží dosáhnout, nemá na záležitosti zvláštní zájem. Poskytování informací dle tohoto zákonu je dvojí na:

- Žádost od žadatele, a to písemně, nebo nahlédnutí včetně pořízení duplikátu s požadovanou informací,
- zveřejnění informace přímo od instituce, která tuto skutečnost má ve svém držení, a to na veřejně přístupné místo, např. internet.

# 7 PSYCHOLOGICKÉ A ETICKÉ ASPEKTY PRACOVNÍKA KZ

## 7.1 Psychologické požadavky

Osoba pracující v odvětví komerčního zpravodajství by měla vynikat jistými rysy a předpoklady pro výkon v povolání detektivní činnosti. Měla by přesně a správně vnímat a rozlišovat situace, které vznikají v jejím okolí a prostředí a měla by být schopna dlouhodobé koncentrace ve stavu pozornosti. Musí se také umět rychle zorientovat v dané situaci, popř. prostoru. Mezi další schopnosti řadíme také anticipaci – předvídání vývoje řešené situace, a to jak u detektivní činnosti, tak u informačního zkoumání a plnění svých povinností jako zpravodajce. Minimální požadavky na pracovníka KZ jsou:

- Rozvinutá sociální oblast:
  - schopnost vytvoření příznivého prvního dojmu,
  - navázání konverzace a její následné udržení,
  - zvládání asertivních technik a praktického jednání.
- Zachování emoční stability.
- Vyrovnání se s psychickou zátěží.
- Vysoká psychická odolnost.

Psychické vytížení člověka při práci je značné a stupňuje se mírou zodpovědnosti a nepravidelnosti konané činnosti. Stresové situace působí na celý organismus jedince a snižují schopnost vnímat a řešit situace, ve kterých by za normálních okolností zcela uspěl a neudělal sebemenší chybu. Pracovník KZ je taktéž osoba s nezbytnou psychologickou složkou – fantazie. Fantazie vychází ze znalostí, které člověk nabyl řešením daného problému, ale zatím nezná všechna fakta vedoucí k vyhodnocení dané situace. Je to schopnost vnímání a vyobrazení znalostí, např. schéma, výkres, plánek… [15]

## 7.2 Sociálně-psychologické vlastnosti

Rozvoj osobnosti v prostředí vykonávané činnosti, v mezilidském kontaktu je v interakci se sociálním prostředím a má svůj vrozený původ v genetickém základu

jedince. Mezi základní vlastnosti sociálně-psychologických vlastností patří **sociální inteligence**:

- Jedná se o jednu ze složek struktury inteligence jedince, je v harmonickém souznění se schopnostmi empatie, společenského taktu, mírou diplomacie, citlivosti a umění komunikace, což je jedna z nejpodstatnějších věcí z pohledu psychologie na aspekt pracovníka komerčního zpravodajství. Lidé s nízkou sociální inteligencí nejsou vhodní pro výkon povolání, kde se poměrná část práce soustřeďuje na komunikaci s lidmi.
- Dalším aspektem je povaha osobnosti – extrovert a introvert, dominance a submisivita. Tyto aspekty jsou rozhodující u volby vedoucího pracovníka a naopak podřízeného. Dominantní lidí se mnohem více hodí na řídící pozice než submisivní lidé.
- V neposlední řadě mluvíme o konformitě a autonomii závislosti na sociálním okolí. Pracovníci KZ, u kterých je povaha konformní, se snaží být cílevědomí, ale svojí činností se spíše straní práce v sociálním prostředí a mají destruktivní, nebo v opačném případě konstruktivní vlohy. [13,15]

## 7.3 Etické aspekty

Etické aspekty a požadavky nejlépe shrnuje etický kodex člena hospodářské komory ČR. „*Člen komory České republiky je součásti silného podnikatelského seskupení, které společnými silami pracuje na zkvalitnění podmínek pro podnikání. Jako člen této instituce se při své činnosti zasazuje o dodržování právních předpisů České republiky, Zákona č. 301/1992 Sb., o Hospodářské komoře České republiky a Agrární komoře České republiky, v platném znění, platných vnitřních norem, smluvních závazků, pravidel správné a uznávané praxe a dále uvedených etických zásad.*“ [17] Taktéž se řídí etickým kodexem České komory detektivních služeb, který v přepisu zní:

- pracovník či organizace mají neustále usilovat o zvyšování uznání a respektu svého profesního sdružení,
- pracovník či organizace mají neustále usilovat o vysokou profesionalitu práce,

- pracovník či organizace mají vykonávat svoji profesi vždy s tuzemským i mezinárodním právem a profesní etikou,
- pracovník či organizace mají poskytovat pravdivé a relevantní informace o sobě a své firmě,
- pracovník či organizace mají respektovat požadavky na výkon povolání detektivní činnosti a zachovávat důvěrné informace,
- pracovník či organizace mají svou preventivní činností předcházet situacím, ve kterých by mohlo docházet ke konfliktům zájmů,
- pracovník či organizace mají být ve své činnosti seriózní a poskytovat pouze pravdivé závěry,
- pracovník či organizace mají prosazovat tento etický kodex ve své vlastní detektivní kanceláři, mezi členy ČKDS a mezi všemi ve své profesi,
- pracovník či organizace mají být loajální ke své detektivní kanceláři a mají dodržovat její politiku,
- pracovník či organizace mají taktéž propagovat profesi soukromého detektiva a profesního sdružení živnostenského společenstva HK ČR ČKDS. [14,17]

# II. PRAKTICKÁ ČÁST

# 8 VYUŽITÍ TECHNICKÝCH PROSTŘEDKŮ V KZ

Dnes už technika dospěla do bodu miniaturizace natolik, že můžeme využívat technických prostředků opravdu hojně. Velikost dnešních odposlechových zařízení se rovná velikosti kancelářské sponky a její ukrytí v daném objektu není žádný problém.

## 8.1 Problematika odposlechů

Právní systém České republiky umožňuje použití odposlechů na osoby, které jsou podezřívané z páchání trestné činnosti, u kterých je zvýšené riziko vyzrazení utajované informace, nebo u vyšetřovaných osob na svobodě, je to možnost ovlivnění svědků a případná manipulace se soudním přelíčením. Další použití odposlechů je potom na vlastní pěst soukromého detektiva, fyzické nebo právnické osoby a nese to s sebou riziko porušování základní listiny práv a svobod tak, jak ji uzákonila Ústava České republiky.

Mezi nejrozšířenější odposlechy dnes patří prostředky využívající GSM mobilní signál. Je to prostředek bezdrátového odposlechu, jenž k přenosu dat využívá mobilní síť a je schopen neomezeného dosahu, stává se proto předním a nejvíce využívaným odposlechem.

GSM odposlechy jsou jedny z mnoha druhů odposlechových zařízení, které využívají řadu různých technologií, velikostí a systémů. Komerční zpravodajství využívá těchto systémů dle své formy. U ofenzivního komerčního zpravodajství se aktivně tyto odposlechy nasazují do praxe a přináší zisk ve formě informací. U defenzivního komerčního zpravodajství se naopak používají systémy, které pomáhají tyto odposlouchávací zařízení odhalovat. Značný důraz se klade na obranně technickou prohlídku (OTP), která je rozebrána v následujících kapitolách. [4]

## 8.2 Ofenzivní KZ v praxi

Odposlech jako technický prostředek ofenzivního KZ nám slouží jako nástroj, pomocí kterého získáváme zdroje informací, které nám za daných podmínek nikdo nepředá a chrání si je. Využití moderních odposlouchávacích zařízení má velkou výhodou v tom, že zařízení může být zabudováno do předmětu a odposlouchávací zařízení se stává pro okolní pozorovatele neviditelný. Daný předmět se může jevit jako předmět běžné potřeby, např.

propisovací pero. Technických prostředků je velká škála, těch nejpoužívanějších je několik:

- GSM odposlouchávací modul,
- odposlech mobilního telefonu,
- laserové odposlouchávací zařízení,
- linkové, drátové odposlechy,
- rádiové odposlechy,
- skrytá kamera,
- mikro diktafony,
- štěrbinové a speciální mikrofony,
- VHF vysílače.

### 8.2.1 GSM odposlouchávací modul

Slabinou tohoto přístroje je napájení, má svou vlastní baterii, ale ta vydrží pouze po určitou dobu. Je také možnost napájet tato zařízení ze sítě, což nám umožňuje nepřetržitý provoz, ale snižuje úroveň krytí. Aktivní odposlouchávací zařízení mají dosah přibližně 10 m a napájení z baterie je omezeno na 6-8 hodin, v pohotovostním režimu vydrží cca 6 dní. Pracuje na běžných mobilních frekvencích a má velmi vysokou citlivost zaznamenávaného zvukového klipu. Další nevýhodou je poměrně velká pořizovací cena, která se běžně pohybuje nad horní hranicí dvaceti tisíc korun. [18]


*Obr. 4. GSM odposlouchávací modul. [5]*

### 8.2.2 Laserové odposlechy

Laserový odposlech pracuje na principu mechanického vlnění. Snímá na velké vzdálenosti – většinou skleněnou plochu (okno), kde probíhá událost, kterou chceme „slyšet“. Velkou vzdáleností rozumíme jednotky v řádu kilometrů. Skládá se z optického zaměřovače s kvalitním zesilovačem zvuku a ekvalizérem. Princip je takový, že hlas, který rozechvěje okolní prostor určitou frekvencí, je přístrojem zachycen. Tyto frekvence se následně namodulují na odražený laserový paprsek a přijímačem se získává potřebná hlasová informace. Toto je nejčistší forma odposlechu. V praxi se aplikuje velmi obtížně a její nevýhodou je celková náročnost instalace. [18]

*Obr. 5. Laserový odposlech. [5]*

### 8.2.3 Odposlech mobilního telefonu

Odposlechy mobilních telefonů můžeme rozdělit na dvě základní skupiny. První probíhá přes mobilního operátora a uskutečňuje se na základě soudního povolení, jedná se tedy o činnost legální a využívá ji Policie ČR. Princip je jednoduchý. Každý mobilní telefon má unikátní identifikační číslo IMSI a každý hovor, který je uskutečněn přes tento identifikátor, se automaticky sleduje.

Druhá varianta je odposlech mobilních telefonů přes tzv. GSM interceptory. Jde o zařízení, které pomocí GSM antén a speciálního softwarového zařízení sleduje mobilní frekvence v okruhu několika stovek metrů a může současně sledovat několik telefonů. Software, který je nejznámější, se nazývá Aghata. [4,18]

### 8.2.4 Radiové odposlechy

Jedná se o miniaturní frekvenčně stabilizovaný vysílač za účelem odposlechu jednání, schůzky. Vyzařovací schopnost až 300 metrů od místa vysílače. Vysílací frekvence

je 433 MHz a jedná se o VKV (velmi krátké vlny). Napájení je dvojího způsobu, a to buď baterií, nebo běžným napájením ze sítě. Vysílač je velmi malé velikosti a lze ho snadno ukrýt. Přijímacím zařízením může být potom jednoduché zařízení jako sluchátka či vysílačka naladěná na pracovní frekvenci vysílače. [18]

*Obr. 6. Radiový odposlech. [5]*

### 8.2.5 Skryté kamery

Pro získání optického záznamu informace se v problematice ofenzivního komerčního zpravodajství hovoří o použití skrytých mikrokamer, u nichž velikostí a nenápadností nejde rozeznat, že předmět je určen k této činnosti.

U kamerových systémů je v dnešní době používáno k výrobě a praktickému používání těch nejnovějších a nejmodernějších technologií. Velikost objektivu kamery je v průměru 1 mm, ale i při této velikosti zařízení nahrává záznam o HD rozlišení. Tomuto systému také odpovídá cena. Běžně se pohybuje nad hranicí deseti tisíců korun. [4]


*Obr. 7. Mikro kamerový systém. [5]*

## 8.3 Defenzivní KZ v praxi

Defenzivní komerční zpravodajství úzce souvisí s bezpečnostní politikou podniku, bezpečnostní analýzou. Její hlavní prioritou je ochrana informací a monitorování informace, pokud se s ní pracuje na úrovni, kdy by její únik znamenal pro danou organizaci velkou újmou.

Ochrana informací by měla být primárním úkolem každého, kdo informace a data veřejně, ale i neveřejně, zveřejňuje. Ochranou myslíme takové kroky zabezpečení, v nichž by se předešlo ztrátě informace a následné újmě způsobené právě touto ztrátou.

Jedná se o ochranu know-how, patentů, výrobních tajemství, ale také důležitých firemních jednání, setkání akcionářů, výroční schůze či dalších cenných a důležitých dokumentů a kontaktů.

Zpravidla jde o ochranu místnosti před odposlechem – Obranně technická prohlídka (OTP) – či sledováním, „nabouráním do počítače“ – ochrana před hrubou silou. V případě počítačů je nejrozšířenějším způsobem ochrany dat šifrování a uchovávání, je-li to nezbytné, mimo veřejnou síť a internetem.

Při ochraně před odposlechem místnosti, mobilního zařízení je nezbytné využít technických prostředků, které jsou k tomuto účelu stvořeny a které se aktivně využívají nejen ve státní správě, kde jsou ve větší míše používány, ale také při interních schůzích podniku, či osobní schůzce.

### 8.3.1 Obranně technická prohlídka

Obranně technická prohlídka by se měla provádět před každým důležitým zasedáním, poradou, setkáním v rámci organizace, kde se předpokládá, že hrozí únik informací nebo na programu jednání budou zveřejňovány informace, které by v případě úniku mohly způsobit újmu chráněnou zákonem, nebo důležité informace organizace. Tato prohlídka je soubor postupů a pravidel pro zabezpečení místnosti. Můžeme při tom využít profesionální firmu, nebo pokud je ve vedení organizace bezpečností manažer, může tuto prohlídku za předpokladu, že je vybaven dostatečných technických zázemím, udělat sám. Při této prohlídce bychom měli postupovat následovně:

- Zahájení prohlídky v čase, kdy se předpokládá uvedení odposlouchávacích zařízení do činnosti.
- Zahájení fiktivní porady, aby se odhalili případné nedostatky při provádění OTP.
- Všechny prohlídky by měly být prováděny v náhodných časových intervalech, aby nebylo možné využít časové monotónnosti ve prospěch pachatele.
- Vyhledávání a detekce musí být prováděny skrytě, aby se předešlo odhalení provádění této prohlídky a ztráty efektivnosti. Jedná se o nastavení přístrojů, poradu s kolegy a techniky, vlastní zahájení prohlídky.
- Využití správných technických prostředků, vybavení a k tomu potřebné znalosti, které jsou důležité pro vykonání této činnosti.
- Věnovat se oblasti, která je pro dané odposlouchávací zařízení cílová – dosah jednotlivých odposlouchávacích zařízení (kvůli kvalitnímu zvukovému záznamu).
- Vytvoření podmínek pro zahájení prohlídky. Zamezit možnost případného pozorování – zatažení závěsů u skleněných ploch a vytvoření prostředí pro běžnou pracovní činnost.

Prohlídka se zaměřuje na tyto formy odposlechů:

- Linkové a drátové odposlechy – tvoří jej vodič po konstrukci,
- dlouhovlnné odposlechy využívající rozvodnou síť 230V,
- analogové – rádiové odposlechy s otevřenou komunikací,

- scramblovaná šifrovaná odposlechová zařízení,
- odposlechy na diskrétních frekvencích,
- dálkově ovládané odposlechy GSM,
- odposlechy realizované přes mobilní telefony,
- nelegální přístupy do místních sítí LAN,
- odposlechy určené pro speciální nasazení.

### 8.3.2 Ochrana dat na PC

Ochrana stolního počítače či notebooku je v dnešní době dostupná a velmi potřebná, přihlédneme-li k počtu krádeží těchto zařízení. Defenzivní komerční zpravodajství musí počítat i s formou tohoto útoku a pokud se na PC nachází citlivá data, např. databáze zaměstnanců, v nichž jsou uloženy jejich osobní údaje, musí se typ ochrany zabezpečit příhodným způsobem. Můžeme přitom využít služby speciálních firem, které se na tuto problematiku zaměřují.

Firmy nabízí bezpečné a privátní pracovní prostředí na počítači s využitím nejrůznějšího softwaru (SW). Nabízí ochranu proti škodlivým SW jako viry, spyware atd., a to díky různým antivirovým programům a firewallům, znemožní, alespoň částečně, neoprávněného přístupu k PC, ochranu dat a optimální nastavení systému.

Běžné zabezpečení počítače v sobě zahrnuje nutnost šifrování dat a souborů. Jednotlivé metody šifrování, které jsou v dnešní době používány, jsou velmi komplexní a časový úsek, který by teoreticky pokryl dobu útoku na tato šifrovaná data, se rovná několika desítkám let, takže můžeme říct, že pro blízkou budoucnost jsou v bezpečí.

Další formou ochrany dat v PC před ztrátou je zálohování a archivace dat. Je to běžná ochrana uživatele před sebou samým nebo před případným poškozením hardwaru. Data jsou uložena v externím zařízením nebo na speciálních zálohovacích serverech, které poskytují za peněžní odměnu profesionální firmy.

### 8.3.3 Technické prostředky defenzivního KZ

Jak ofenzivní, tak i defenzivní komerční zpravodajství využívají ke své činnosti technických prostředků. Defenzivní zpravodajství se však na rozdíl od ofenzivního pomocí

těchto zařízení snaží odhalit případné odposlouchávací zařízení umístěné v cílovém objektu.

#### *8.3.3.1 Detektor nelineárních přechodů*

Tento technický prostředek se používá současně s OTP, aby se zjistilo, zda v cílené oblasti/místnosti nejsou umístěna odposlouchávací zařízení. Detektor se skládá ze dvou částí, a to vysílací a přijímací antény a vysílací a přijímací aparatury. Tyto antény jsou umístěny na konci teleskopické tyče a vysílací s přijímací technikou jsou umístěny ve skříince na druhé konci této tyče. Napájení je řešeno z akumulátoru, nebo ze sítě.

Princip tohoto detektoru je takový, že zařízení vysílá pulsní signál o frekvenci 900 MHz a přijímací anténa zachycuje odražené signály od předmětů a konstrukcí. Vyhodnocovací jednotka určuje typ zpětně zachyceného signálu, polovodičové součástky, které obsahují téměř všechny odposlouchávací zařízení, vydávají signál o 2. harmonické frekvenci a kovové konstrukce odráží signál o 3. harmonické frekvenci. Přístroj nás upozorní akustickým signálem, když zachytí odlišné frekvence, než jaké vyslal.

Výhoda tohoto detektoru je taková, že odhalí i staré a již nefunkční zařízení, takže můžeme zjistit, jestli daná místnost/objekt byla již dříve terčem komerčního zpravodajství. [4,18]

#### *8.3.3.2 Generátor bílého šumu*

Zařízení, které produkuje bílý šum na frekvenci 40 - 60 Hz a je to náhodný signál s konstantní výkonovou spektrální hustotou. Generátor má konstantní hlasitost pouze ve chvíli, kdy zaznamenává zvuk hovoru. Pro ideální rušení možných odposlechových zařízení se doporučuje umístění tohoto zařízení na místo zhruba ve stejné vzdálenosti od všech účastníků rozhovoru. Generátor šumu sníží kvalitu záznamu až o 95 %, což je pro záznam devastující. V pořízené nahrávce, která byla ovlivněna tímto generátorem, je těžké najít slova, kterým by bylo rozumět, a tím pádem se stává pořízený materiál nepoužitelný. Cena zařízení se pohybuje nad hranicí patnácti tisíc korun. [4]


*Obr. 8. Generátor bílého šumu. [5]*

#### *8.3.3.3 Kontrola mikrofonů, přímím poslechem*

U této metody se využívá jako technický prostředek citlivý zesilovač s velkým odporem. Odhalují se tak přímé napojení na telefonní linku, přístroj. Toto řešení najde i harmonické odposlechové zařízení, nebo nekonečné připojení na dráty telefonního rozvodu. Tato kontrola se provádí tak, že se zesilovač připojí na vedení tel. linky a pomocí sluchátka se poslouchají přenášené zvuky. Telefon, který nebyl nijak upraven externím zařízením, nevydává žádný audiosignál, takže pokud slyšíme zvuky, které vycházejí ze zabezpečované místnosti, znamená to, že telefonní linka byla upravena. Pro větší jistotu zabezpečení, sledujeme tyto linky dlouhodobě v neurčitých časových intervalech. [18]

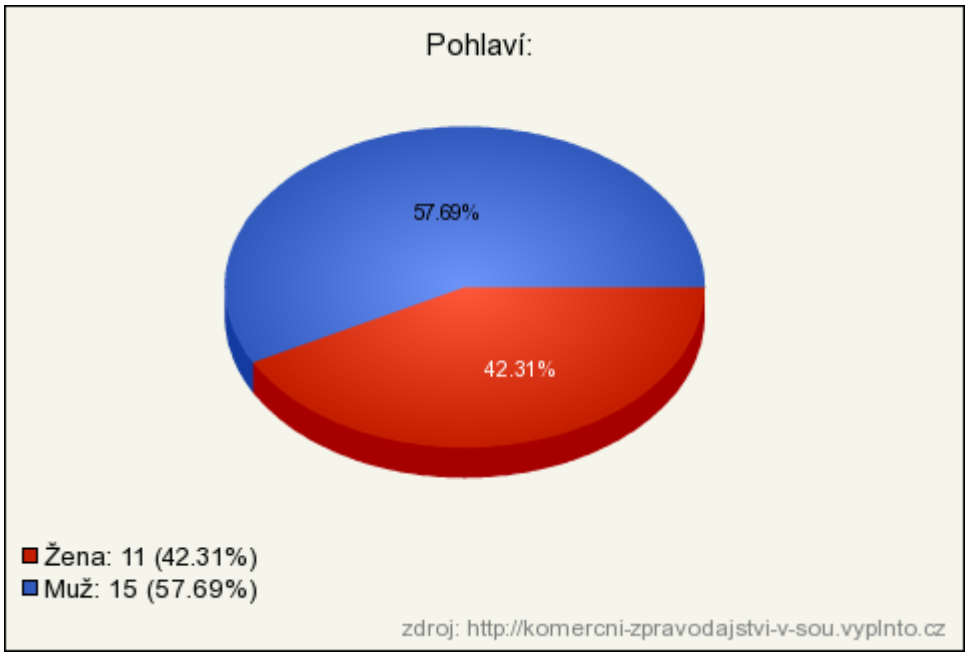
#### *8.3.3.4 Kontrola radiového spektra*

Tato metoda si klade za cíl odhalit radiová odposlechová zařízení, která jsou umístěna v chráněných prostorách. Jedná se o širokopásmový automatický přijímač s detekcí nejsilnějšího signálu. Měřící rozsah přístroje je dostačující, aby pokryl všechny frekvence, na kterých pracují dnešní odposlouchávací zařízení – běžné frekvence od 50 do 450 MHz. Ochrana se provádí rozeznáváním frekvenčního spektra v předem nadefinovaných frekvenčních pásmech pomocí paměťových radiových analyzátorů. [18]

# 9 DOTAZNÍK

Během vypracovávání bakalářské práce jsem se snažil zjistit, zda se lidé v mém okolí setkali s pojmem komerční zpravodajství, popř. zda těchto služeb využili. Dotazník byl anonymní a postavil jsem jej na devíti otázkách s možností výběru odpovědí ano/ne (se dvěma výjimkami) kvůli jednoduchosti a jednoznačnosti odpovědí. Dotazník má celkem 26 respondentů, z uvedených grafů vyplývá, jak dotázaní odpovídali. Níže jsou výsledky průzkumu na téma komerční zpravodajství v soukromých bezpečnostních službách:

## 9.1 1. Otázka – Pohlaví.




*Graf 1. Odpovědi na 1. otázku v %.*

## 9.2 2. Otázka – Setkali jste se s pojmem komerční zpravodajství?


*Graf 2. Odpovědi na 2. otázku v %.*

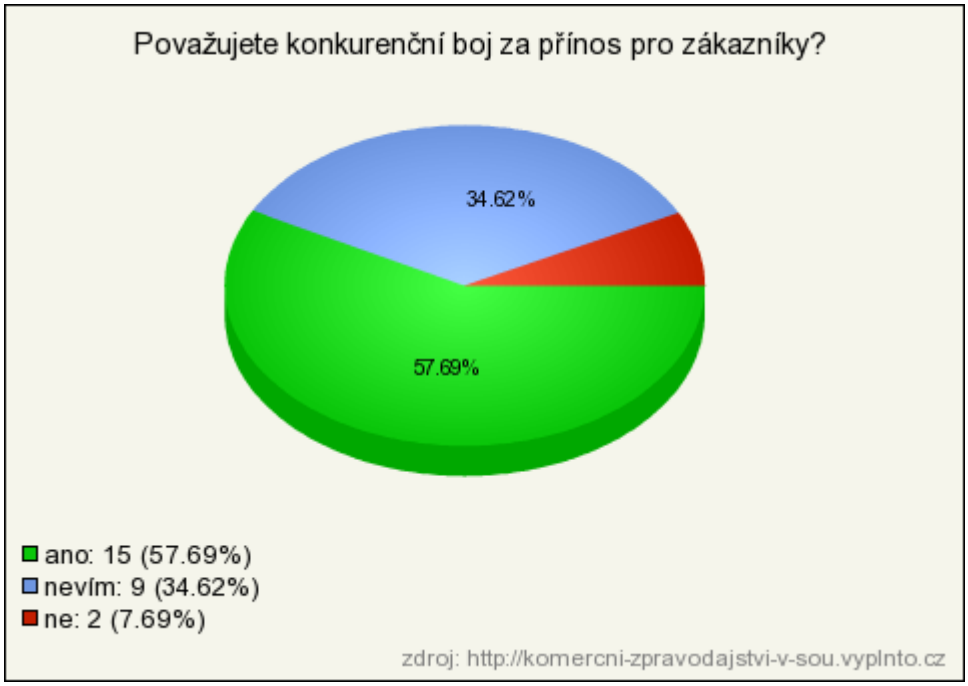
Z uvedeného grafu vyplývá, že 42% respondentů se nikdy nesetkalo s pojmem komerční zpravodajství. V úvodu této otázky jsem tázajícím nastínil význam pojmu komerční zpravodajství, aby se dalo na tuto otázku objektivně odpovědět.

## 9.3 3. Otázka – Jedná se podle Vás o špionáž?


*Graf 3. Odpovědi na 3. otázku v %.*

Jak vypovídá graf 3, odpovědi na tuto otázku jsou názorově různé, avšak ne chybné. Komerční zpravodajství pracuje s veřejnými zdroji informací, ale také se pohybují na hraně zákonů ČR.

## 9.4 4. Otázka – Považujete konkurenční boj za přínos pro zákazníky?




*Graf 4. Odpovědi na 4. otázku v %.*

Převážná většina respondentů se domnívá, že konkurenční boj je přínosem pro zákazníky.

## 9.5 5. Otázka – Využili jste služeb komerčního zpravodajství?


*Graf 5. Odpovědi na 5. otázku v %.*

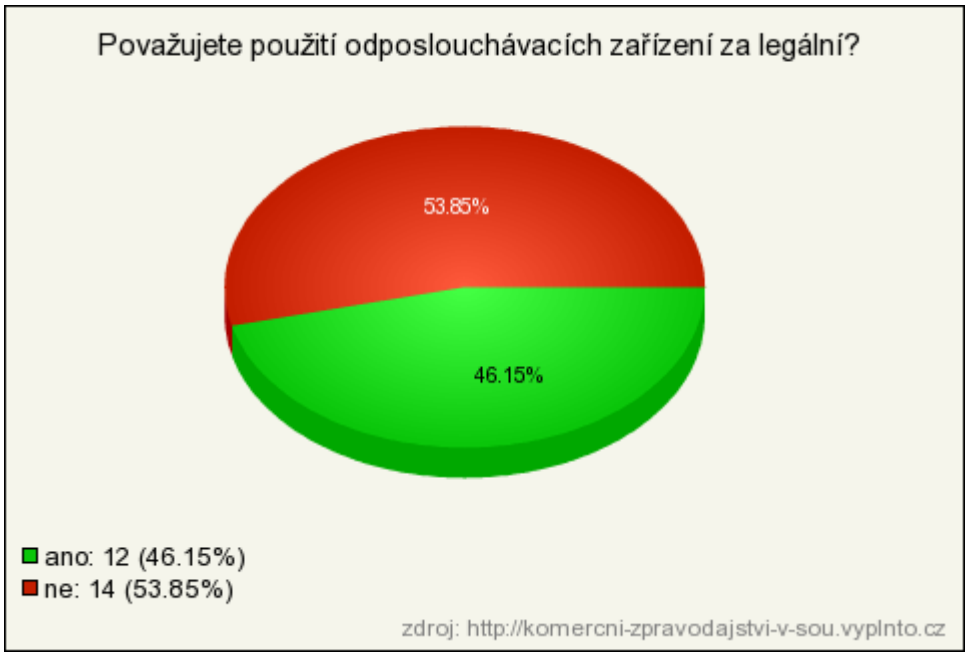
Z uvedeného grafu vyplývá, že 50 % respondentů (13 odpovědí z 26) nikdy nevyužilo komerční zpravodajství ve svůj prospěch nebo pro svou obranu.

## 9.6 6. Otázka – Stali jste se obětí komerčního zpravodajství?


*Graf 6. Odpovědi na 6. otázku v %.*

U této otázky bylo, dle vyhodnoceného průzkumu, 30 % respondentů, kteří se stali obětí komerčního zpravodajství, nerozlišoval jsem, zda ofenzivního nebo vlivového. Otázku jsem položil s vysvětlením, že obětí se stává člověk, který měl např. odposlouchávaný mobilní telefon nebo nevědomě vyzradil cenné (soukromé) informace.

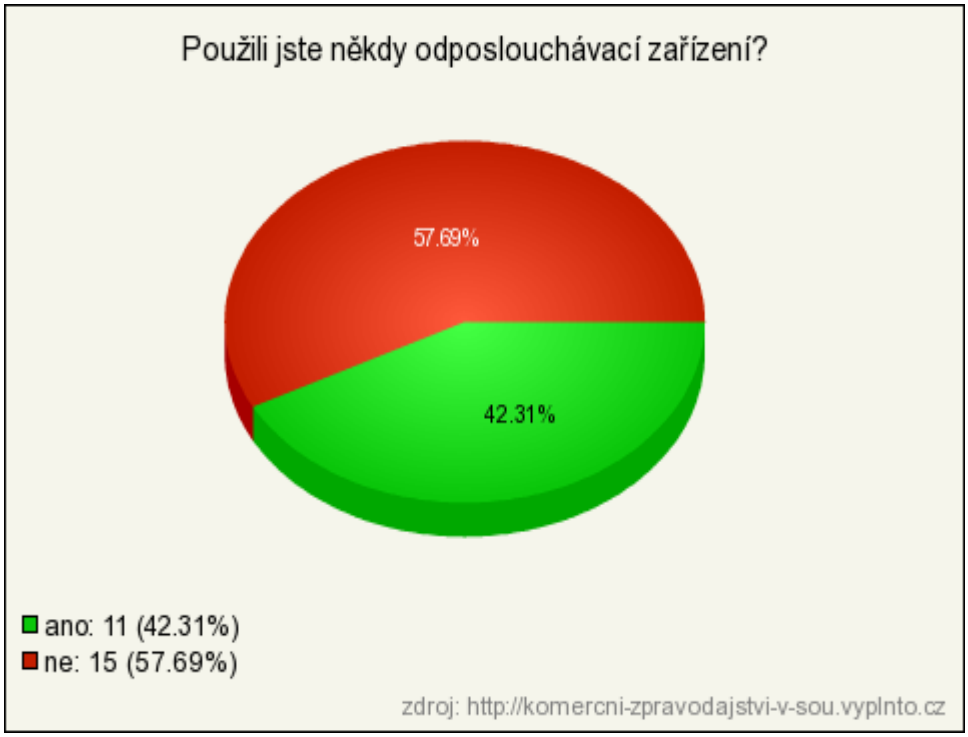
## 9.7 7. Otázka – Považujete použití odposlouchávacích zařízení za legální?




*Graf 7. Odpovědi na 7. otázku v %.*

Z 26 dotázaných respondentů považuje použití odposlouchávacích zařízení za legální 46%. Vychází z faktu, že použití odposlechů je možné pouze v případě, že soud dá oprávnění danou osobu sledovat.

## 9.8 8. Otázka – Použili jste někdy odposlouchávací zařízení?




*Graf 8. Odpovědi na 8. otázku v %.*

## 9.9 9. Otázka – Víte, jak se můžete bránit proti odposlouchávacím zařízením?


*Graf 9. Odpovědi na 9. otázku v %.*

## 9.10 Vyhodnocení dotazníku

Cílem dotazníku bylo zjistit, jak jsou lidé v mém okolí seznámeni a jestli souhlasí s problematikou komerčního zpravodajství. Dotazník byl neveřejný a rozšířil jsem ho mezi podniky v okolí mého bydliště a také mezi studenty. Výsledky dotazníku byly rozporuplné. Většina lidí je s tímto tématem seznámena, ale bohužel nezná základní myšlenku komerčního zpravodajství. Lidé, kteří se setkali s touto problematikou, neberou komerční zpravodajství jako činnost, která se rovná špionáži, ale ví, jak se proti této činnosti bránit. Vycházím ze surových dat, které jsem získal při vyhodnocení dotazníku.

# ZÁVĚR

Tato bakalářská práce řeší problematiku komerčního zpravodajství jako nástroje, pomocí kterého můžeme informace buďto získat, nebo o ně přijít. Komerční zpravodajství využívá metod, které úzce souvisí s používáním technických prostředků jak u defenzivního, tak i ofenzivního komerčního zpravodajství. Rozhodujícím faktorem, na který je kladen důraz, a to u všech forem, je čas. Včasné informace nám v této problematice pomáhají zvládat překážky, které bychom jinak jen těžce překonávali.

Využití komerčního zpravodajství je bohužel omezeno, a to kvůli nižšímu počtu lidí, kteří tuto problematiku znají. K tomuto závěru jsem došel po předložení dotazníku, ale i po diskuzi s podnikateli a organizacemi v místě svého bydliště. Pojem komerční zpravodajství jim byl známý, ale převážná část respondentů jej nedokázala vysvětlit.

Komerční zpravodajství je účinný nástroj, pomocí kterého můžeme dosáhnout na informace, jež potřebujeme pro konkurenční náskok, nebo opačně, pokud informace chceme co nejefektivněji chránit. Proto se v tomto případě také musí brát důraz na režimovou bezpečnost a bezpečnostní politiku podniku společně s bezpečnostní analýzou. V potaz musíme brát také psychologické a etické aspekty a požadavky na pracovníky, kteří tuto činnost vykonávají. Špatná psychika člověka a nedostatek loajality může mít za následek ohrožení bezpečnosti organizace a možný vpád vlivového komerčního zpravodajství ze strany konkurence, která by se mohla snažit využít takové situace ve svůj prospěch.

Podniky nebo jakékoli jiné organizace by neměly podceňovat význam komerčního zpravodajství a měly by se zaměřit zvláště na své interní bezpečností předpisy, tzn. přímo na bezpečnostní politiku podniku, ale i na řádné školení zaměstnanců v rámci režimové ochrany. Pokud je společnost zaměřena technologickým směrem, je také důležité, aby si chránila své know-how technickými prostředky, a pokud je to možné, i kryptografií a správným zabezpečením ethernetové sítě a všech počítačů, které by se mohly stát terčem potencionálního útoku.

# ZÁVĚR V ANGLIČTINĚ

This thesis solves the problem of commercial news as an aid by which we can either get information or to lose . The commercial news use the methods which are closely associated with the use of technical means for both defensive and offensive commercial news. The decisive factor that is emphasized, in all forms, is time. Timely information in this issue help us to manage the obstacles that we would´ve overcome hard otherwise.

The use of commercial news is unfortunately limited because of fewer people who know this issue . This is the conclusion I reached after submission of the questionnaire and after discussion with the entrepreneurs and the organizations in my home place. The concept of commercial news were known to them but the most of the respondents could not explain this concept .

The commercial news is an effective aid by which we can reach the information, we need for a competitive start, or oppositely if we want to protect the information as effectively as possible . Therefore in this case there are the regimed security and security policy of the company together with safety analysis on which must be taken the emphasis as well. We have to take the psychological and ethical aspects and requirements for personnel who perform this activity into consideration. Poor human psyche and the want of loyalty can result in a threat security of the organization and a possible invasion of commercial news from competitor who might try to benefit from the situation.

The companies or any other organizations should not underestimate the importance of commercial news and they should focus particularly on their internal safety regulations, i.e. directly on security policy of the company and also on proper training of employees within the regime of protection. If the company is geared towards technology it is also important to protect its know- how by technical means and if it´s possible even by cryptography and by proper security of internet network and all computers that could become potential target of attack.

# SEZNAM POUŽITÉ LITERATURY

[1] BRABEC, František. Technologie detektivních činností. První. UTB : UTB, 2009. ISBN 978-80-7318-780-4

[2] BRABEC, František, et al. Bezpečnost pro firmu, úřad, občana. Praha : Public History, 2001. ISBN 80864450406

[3] Co je konkurenční zpravodajství. Česká komora detektivních služeb [online]. 2012 [cit. 2012-04-05]. Dostupné z: http://ckds.cz/index.php?nid=3729&lid=CZ&oid=458863

[4] Odposlechy.com: Speciální technika a služby [online]. 1999-2012 [cit. 2012-04-08]. Dostupné z: http://www.odposlechy.com/odposlechova-a-nahravaci-technika

[5] PAPÍK, Richard. Competitive Intelligence, informační služby, Internet a informační profese. Ikaros [online]. 2001, roč. 5, č. 4 [cit. 7-05-2012]. Dostupný z: http://www.ikaros.cz/node/739. URN-NBN:cz-ik739. ISSN 1212-5075.

[6] *F.S.C. Bezpečnostní poradenství* [online]. 2005 [cit. 2012-05-22]. Dostupné z: http://www.fsc-ov.cz/produkt.php?id=101

[7] PAPÍK, Richard. Strategie vyhledávání informací a elektronické informační zdroje. Praha: Velryba s.r.o., Praha 9, 2011. ISBN 978-80-85860-22-1.

[8] JAŠEK, Roman. Komerční zpravodajství. UTB. Dostupné z: http://vyuka.fai.utb.cz/course/view.php?id=113. Prezentace.

[9] Laucký, Vladimír. Technologie komerční bezpečnosti I. UTB : UTB,2010. ISBN 978-80-7318 -889-4

[10] KAMENÍK, J., BRABEC, F. a kol.: Komerční bezpečnost (Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur). ASPI, Praha 2005

[11] STRAUS, J. Kriminalistická technika. Plzeň : Aleš Čeněk, s.r.o., 2007.

[12] KLOUDA, P. Moderní analytické metody. Ostrava: Pavel Klouda, 2003.

[13] Grafologie a Psychologie [online]. 2005 [cit. 2012-04-18]. Dostupné z: http://ografologii.blogspot.com/search/label/Psychologie%20osobnosti

[14] Česká komora detektivních služeb: Etický kodex CKDS [online]. 2012 [cit. 2012-05-10]. Dostupné z: http://www.ckds.cz/index.php?nid=3729&lid=cs&oid=458839

[15] MIŇHOVÁ, Jana. Základy Psychologie [online]. [cit. 2012-05-12]. Dostupné z: http://www.najmo.borec.cz/ZPS.pdf

[16] ŠMEJKAL, Petr. Competitive Intelligence s přihlédnutím k situaci v čr [online]. Brno, 2006 [cit. 2012-05-08]. Dostupné z: http://is.muni.cz/th/43262/ff_m_a2/Uvod_do_Competitive_Intelligence.txt. Diplomová práce. Masarykova Univerzita.

[17] BRABEC, František. ČESKÁ KOMORA DETEKTIVNÍCH SLUŽEB. Oborová příručka. 2. vyd. 2009.

[18] LAUCKÝ, Vladimír. Speciální bezpečnostní technologie. Zlín: UTB, 2009. ISBN 978-80-7318-762-0.

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

KZ Komerční zpravodajství.

OTP Obraně technická prohlídka.

SBS Soukromé bezpečnostní služby.

ČKDS Česká komora detektivních služeb.

GSM Global Sytem for Mobile comunnications.

CCTV Close Circuit Televisions.

PČR Policie České republiky

# SEZNAM OBRÁZKŮ

# SEZNAM GRAFŮ