Detektivní činnost v procesu obranného nestátního zpravodajství

Detective operations in defensive non-state intelligence

Zdeněk Krist

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Zdeněk KRIST**
Osobní číslo:	**A08348**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Detektivní činnost v procesu obranného nestátního zpravodajství**

Zásady pro vypracování:

1. **Pojednejte o detektivním zpravodajství jako jedné z forem soukromé detektivní činnosti.**
2. **Popište technologie v obranném komerčním (nestátním) zpravodajství.**
3. **Komerční obranné zpravodajství při zajišťování: personální bezpečnosti, informační bezpečnosti, bezpečnosti Know – How.**
4. **Obranné zpravodajství jako prostředek proti vlivovému a ofenzivnímu zpravodajství konkurence.**
5. **Uveďte praktický příklad řešení komerčního obranného zpravodajství.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, František. Technologie detektivních činností. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 160 s. ISBN 978-80-7318-780-4.**
2. **BRABEC, František. Bezpečnost pro firmu, úřad, občana. Praha : Public History, 2001. 400 s. ISBN 80-86445-04-6.**
3. **BRABEC, František. Soukromé detektivní služby. 1. vyd. Praha : Eurounion, 1995. 63 s. ISBN 80-85858-16-9.**
4. **LAUCKÝ, Vladimír. Speciální bezpečnostní technologie. 1. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 223 s. ISBN 978-80-7318-762-0.**
5. **KAMENÍK, Jiří; BRABEC, František. Komerční bezpečnost : soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Vyd. 1. Praha : ASPI, 2007. 338 s. ISBN 978-80-7357-309-6.**

Vedoucí bakalářské práce: **JUDr. František Brabec**
Ústav bezpečnostního inženýrství

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

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Bakalářská práce se zaměřuje na problematiku nestátního zpravodajství. V práci je kladen důraz především na obranné nestátní zpravodajství a jeho řešení pomocí jedné z forem detektivní činnosti – detektivního zpravodajství.

Teoretická část popisuje detektivní zpravodajství, jeho úlohu v nestátním zpravodajství, některé právní aspekty týkající se detektivního zpravodajství, technologie využívané v této oblasti a využití v obranném nestátním zpravodajství.

V praktické části je nastíněna iluzorní situace, na které je ilustrováno možné řešení pomocí obranného zpravodajství.

Klíčová slova: nestátní zpravodajství, detektivní zpravodajství, obranné zpravodajství

ABSTRACT

Bachelor work focuses on the issue of non-state intelligence. In particular, the work deals with non-state intelligence and his solution by a form of detective activity - detective Intelligence.

The theoretical part describes the detective intelligence, the role use non-state intelligence, some legislation aspects related to the detective intelligence, the technology used in the field and use in the defensive non-state intelligence.

The practical section outlines the illusory situation, which is illustrated with a possible solution to defensive intelligence.

Keywords: non-state intelligence, detective intelligence, defensive intelligence

Rád bych touto cestou poděkoval panu JUDr. Františku Brabcovi, za odborné vedení, cenné rady a připomínky, které mi poskytl při vypracovávání této práce. Dále bych chtěl ještě poděkovat rodině, blízkým a kamarádům za jejich podporu při mém studiu.

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

Zpravodajství doprovází lidstvo od nepaměti, jeho počátky můžeme datovat do nejranějších dob lidské kultury, kdy bylo třeba zjišťovat počty, pohyb a úmysly nepřátelských vojsk, ale také zdokonalovat své výrobní technologie na základě poznatků z cizích kultur. Současně ale také vzniklo tzv. kontra-zpravodajství neboli obranné (defenzivní) zpravodajství, jehož účelem je naopak utajování informací, před cizími zpravodajskými útvary.

V moderním světě, kdy dobu ovládají informační technologie a kdy je nutno okamžitě reagovat na nové trendy společnosti, jsou důležitým prvkem informace. Práce s informacemi se stala doménou dnešní doby. Hustota a rychlost informací se neustále zvyšuje a stávají se tak klíčovým nástrojem nejen ekonomické sféry. Jejich ochrana nevyžaduje pouze perfektní technické zabezpečení, ale také vyžaduje režimová opatření. Neméně důležitou oblastí je i vlastní personální bezpečnost. Jednoduše řečeno, bezpečnost vyžaduje komplexní přístup, jinak je neúčinná.

Detektivní zpravodajství hraje důležitou roli v personální bezpečnosti. Nezbytné je dále při vyhledávání latentní kriminality. Uplatnění najde též při ochraně informací a dat. Neměla by se opomenout klíčová role detektivního zpravodajství při zajišťování bezpečnosti v obchodních vztazích, ochraně před nežádoucím působením ofenzivního a vlivového zpravodajství konkurence, využití najde ale také v dalších oblastech.

Tato bakalářská práce si klade za cíl uvést čtenáře do oboru nestátního zpravodajství a seznámit jej s využitím detektivních činností v této oblasti. Pozornost je věnována převážně obrannému nestátnímu zpravodajství, které tvoří základ pro ofenzivní a vlivové zpravodajství.

I. TEORETICKÁ ČÁST

1 DETEKTIVNÍ ZPRAVODAJSTVÍ JAKO PRVEK K NAPLŇOVÁNÍ NESTÁTNÍHO ZPRAVODAJSTVÍ

V roce 2008 byla vydána novela živnostenského zákona (č. 274/2008 Sb.), která přesunula obsah soukromé detektivní činnosti z nařízení vlády 469/200 Sb., do živnostenského zákona do § 6a odst. 2. Obsahem služeb soukromých detektivů podle § 6a odst. 2 je poskytování služby spojené s hledáním majetku a osob, zjišťování skutečností, které mohou sloužit jako důkazní prostředky v řízení před soudem nebo správním orgánem, získáváním informací týkajících se fyzických nebo právnických osob nebo jejich majetkových poměrů, získáváním informací v souvislosti s vymáháním pohledávek, vyhledáváním protiprávních jednání ohrožujících obchodní tajemství, sběr dat a jejich vyhodnocování pro subjekty, které prokážou právní záměr. Tento souhrn činností je v uvedeném živnostenském zákoně pod hlavičkou Koncesovaná živnost služby soukromých detektivů.

Soukromých detektivních služeb se využívá v nestátním zpravodajství, to je pojem, který JUDr. František Brabec popisuje jako soubor komerčního zpravodajství (probíhá na komerční bázi, tedy smluvně pro jiné organizace) a zpravodajského servisu (na nekomerční bázi, slouží pouze pro potřebu vlastní organizace). Nestátní zpravodajství také subsumuje pojem konkurenční zpravodajství (Competitive inteligence) v ekonomické oblasti, někdy se též používá výraz komerční zpravodajství. Forma, kterou je vykonáváno nestátní zpravodajství se jmenuje detektivní zpravodajství, tedy jedna z forem detektivní činnosti. [1]

1.1 Právní aspekty soukromé detektivní činnosti

Základním kamenem k vykonávání soukromé detektivní činnosti je znát legislativu státu. Neznalostí legislativy se soukromý detektiv vystavuje riziku porušení zákona. Zde je uveden stručný popis některých důležitých právních aspektů spojených s detektivní činností:

Listina základních práv a svobod (č. 2/1993 Sb.)

Listina základních práv a svobod se stala právní normou, od níž se odvozují a odvíjejí další právní úpravy. Listinu práv a svobod je proto nutno chápat jako právní normu vyšší právní síly. Důležitým článkem, v této ústavní normě, pro soukromou detektivní činnost je článek 17, kterým je každému občanovi poskytováno právo na informace. Toto právo se tedy z občana přenáší i na právnické osoby tj. podniky, organizace. Opatřovat informace na ochranu svých práv a svých oprávněných zájmů, mohou přímo oprávněné fyzické osoby nebo se mohou v této činnosti nechat zastupovat jinou fyzickou či právnickou osobou. Na druhou stranu je touto normou i omezován, jde zejména o čl. 7 (nedotknutelnost osoby a jejího soukromí), čl. 12 (nedotknutelnost obydlí), čl. 10 (ochrana lidské důstojnosti, osobní cti, dobré pověsti, nedovolené zasahování do soukromí neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o osobě).

Listina základních práv a svobod tudíž svými ustanoveními determinuje rozsah a obsah soukromé detektivní činnosti, rozsah, možnosti a využití postupů soukromého detektiva. Tyto hranice musí mít soukromý detektiv neustále na mysli a musí jim přizpůsobovat veškerou svou činnost. [3][10]

Občanský zákoník (č. 40/1964)

Významnou právní normou, která rovněž determinuje soukromou detektivní činnost, je občanský zákoník.

- § 6

  „…jestliže hrozí neoprávněný zásah do práv bezprostředně, může jej ten, kdo je takto ohrožen, přiměřeným způsobem odvrátit…“

- § 11

  „…fyzická osoba má právo na ochranu své osobnosti, zejména života, zdraví, občanské cti, jakož i svého jména a projevů osobní povahy…“

- § 22

  „…zástupce je ten, kdo je oprávněn jednat za jiného a jeho jménem. Ze zastoupení vznikají práva a povinnosti přímo zastoupenému…“

- § 123

  „…vlastník je v mezích zákona oprávněn předmětem svého vlastnictví držet, užívat, požívat jeho plody a nakládat s ním…“
- § 126

  „…vlastník má právo na ochranu proti tomu, kdo do jeho vlastnických práv zasahuje…“
- § 414

  „…každý je povinen počínat si tak, aby nedocházelo ke škodám na zdraví, na majetku, na přírodě a životním prostředí…“
- § 417

  „… komu hrozí škody, je povinen k jejímu odvrácení zakročit způsobem přiměřeným okolnostem ohrožení…“
- § 418

  „… kdo způsobil škodu, když odvracel přímo hrozící nebezpečí, které sám nevyvolal, není za ni odpovědný, ledaže bylo možno toto nebezpečí za daných okolností odvrátit jinak anebo jestliže je způsobený následek zřejmě stejně závažný nebo ještě závažnější než ten, který hrozil…“
- § 419

  „…Kdo odvracel hrozící škodu, má právo na náhradu účelně vynaložených nákladů a na náhradu škody, kterou přitom utrpěl, i proti tomu, v jehož zájmu jednal, a to nejvýše v rozsahu odpovídajícím škodě, která byla odvrácena…“
- § 420

  „…Každý odpovídá za škodu, kterou způsobil porušením právní povinnosti…“ [3][11]

Občanský soudní řád (99/1963 Sb.)

V občanském soudním řízení jsou účastníci povinni podle § 120 odst. 2 občanského soudního řádu „…označit důkazy, jimiž lze objasnit skutkový stav věci…“ Mají-li účastníci řízení takovou povinnost, můžou si tyto informace opatřit sami nebo je nechat opatřit například soukromou detektivní kanceláří. § 123 umožňuje „…vyjádřit se k návrhu na předložené důkazy a ke všem důkazům, které byly provedeny…“ Aby tak mohli účastníci občanskoprávního řízení učinit, musí mít

rovněž právo důkazy soustředit nebo sám si je opatřit, požadovat jejich akceptování a realizaci. .[3] [12]

Trestní zákoník (40/2009 Sb.)

V souladu s § 29 trestního zákona o nutné obraně a § 28 trestního zákona o krajní nouzi jsou ustanoveny podmínky tzv. obranných prostředků (obranných zákroků) soukromého detektiva při výkonu soukromé detektivní činnosti. Tyto obranné zákroky by však měli být v činnosti soukromého detektiva zcela výjimečné. [3] [13]

Trestní řád (141/1961 Sb.)

V souladu s § 76 odst. 2 trestního řádu může soukromý detektiv, stejně jako kterýkoliv jiný občan, „…osobu, která byla přistižena při trestném činu, zadržet, je-li to nezbytné třeba k zajištění její totožnosti, k zamezení útěku nebo k zajištění důkazů. Je však povinen zadrženou osobu neprodleně předat státnímu zástupci, vyšetřovateli, orgánu policie nebo u příslušníka ozbrojených sil správci posádky…“ [3] [14]

Rizika právní odpovědnosti soukromého detektiva

- § 7 tr. zákona – příprava k trestnému činu
- § 8 tr. zákona – pokus trestného činu
- § 105 tr. zákona – vyzvědačství
- §§ 106 a 107 tr. zákona – ohrožení utajované skutečnosti
- § 128 tr. zákona – zneužití informací v obchodním styku
- § 164 tr. zákona – podněcování
- § 165 tr. zákona – schvalování trestného činu
- § 166 tr. zákona – nadržování
- § 167 tr. zákona – nepřekažení trestného činu
- § 168 tr. zákona – neoznámení trestného činu
- § 206 tr. zákona – trestný čin pomluvy
- § 209 tr. zákona – poškozování cizích práv
- § 231 tr. zákona – omezování osobní svobody
- § 235 tr. zákona – trestný čin vydírání, v souvislosti s vymáháním pohledávek

- § 237 tr. zákona – trestný čin útisku
- § 238 tr. zákona – porušení domovní svobody
- § 239 tr. zákona – porušení tajemství dopravovaných zpráv

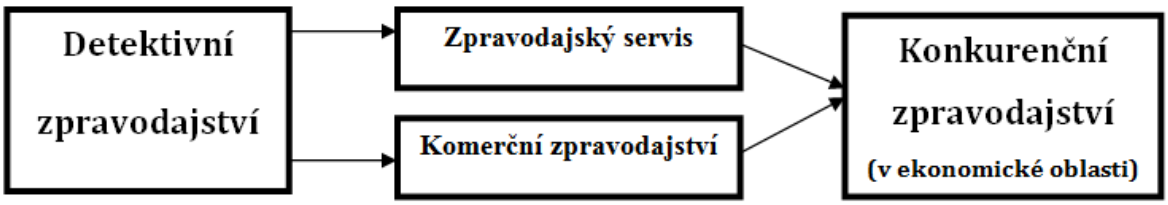
1.2 Detektivní zpravodajství

Jak už bylo zmiňováno, nestátní zpravodajství je v podstatě realizováno prostřednictvím soukromé detektivní činnosti, jejíž jednou z forem detektivní činnosti je i detektivní zpravodajství. Detektivní zpravodajství je významnou formou detektivní činnosti a její úloha spočívá především v:

- systematickém vyhledávání a získávání dat a informací s konkrétním zaměřením a s využitím rozličných metod a prostředků soukromé detektivní činnosti
- shromažďovaní a třídění dat a informací podle zadaných požadavků zákazníka
- investigativní analýze shromažďováním dat a informací s využitím metod analýzy, dedukce, indukce a logiky
- syntéze analyzovaných dat a informací a jejich přeměna na relevantní informace, tedy znalosti
- zpracování znalostí do podoby požadované zákazníkem (klientem), včetně dodržení zásad legalizace získaných znalostí a jejich distribuce zákazníkovi.

Detektivní zpravodajství je forma, která směřuje k naplňování nestátního zpravodajství, které se skládá z:

- *zpravodajského servisu*, pokud se jedná o činnost pro vlastní organizaci, pro kterou výsledný zpravodajský produkt slouží
- *komerčního zpravodajství,* které je prováděno specializovanou firmou pro jinou firmu, poskytováno na komerční bázi (na smluvním základě).



Obr. 1. Detektivní zpravodajství – inspirace JUDr. Brabec [1]

Zpravodajský servis a komerční zpravodajství v ekonomické oblasti tvoří konkurenční zpravodajství.

Detektivní zpravodajství se realizuje stejně, jako zpravodajství obecně v následujících krocích:

- *operativa = informace*:

zpravodajská operativa představuje schopnost vyhledat data a zpracovat je na informace, schopnost, pomocí zpravodajských technologií vyhledávání, naleznout informace.

- *taktika = znalosti*:

zpravodajská taktika představuje schopnost pochopení informací a za využití zpravodajské technologie analýzy, jejich relevantní výběr a přeměnu na znalost a schopnost prezentace znalosti v podobě přístupné pro uživatele – toho, kdo rozhoduje.

- *strategie = poznání:*

zpravodajská strategie představuje technologie a schopnosti vyhledat a zpracovat znalosti ve vzájemných souvislostech.

Detektivní zpravodajství je třeba chápat jako:

- *informační produkt* – produkt znalosti a poznání, který má svůj obsah, formu a aktuálnost

- *Informační proces*, tedy cestu od dat a informací ke znalosti a poznání;
  Jako proces skládající se z následujících kroků - fází:
  - *Řízení* – řízení zpravodajské činnosti představuje identifikaci informačních potřeb a stanovení priorit. Jde o vytvoření a správné definování otázek a stanovení cesty k dosažení odpovědí.
  - *Sběr* - jde o cílené využívání různých informačních zdrojů.
  - *Analýza* - zpravodajská analýza představuje interpretaci informací v kontextu informačních potřeb, které jsou ve vzájemných souvislostech a ve vztahu k řešenému problému, tedy ve vztahu k odpovědi na položené otázky – v kontextu docílení znalosti o daném problému vycházejícím z definovaných otázek.

- *Distribuce* - distribuce zpravodajské znalosti a zpravodajského poznání vyžaduje včasné doručení k uživateli, který rozhoduje, a to v jeho využitelné formě.

Informace – znalost – poznání jsou využitelné, pokud jsou aktuální. Aktuálnost musí mít přednost před kvalitou. Ztráta aktuálnosti informace – znalosti – poznání nesmí být ohroženo zdlouhavou distribucí, jen aby bylo dosaženo nejvyšší kvality. I vysoce kvalitní informace – znalosti – poznání ztrácející aktuálnost a jsou bezcenné, pokud jsou distribuované s opožděním.

Detektivní zpravodajství představuje neustále se opakující a na sebe navazující cykly. Zpravodajský cyklus je tvořen pravidelnými a navzájem na sebe navazujícími zpravodajskými procesy, mezi kterými probíhá zpravodajské řízení.
Zpravodajské řídící postupy obsahují:

- definování potřeb,
- zpravodajské plánování,
- tvorbu operativy, taktiky a strategie zpravodajského procesu,
- shrnutí a analýzu stávajících informací, poznaní a znalostí,
- kolekce zpravodajského záměru, to je rozhodnutí o realizaci zpravodajského procesu a jeho záměrech a cílech. [2]

Detektivní zpravodajství tedy patří do forem soukromé detektivní činnosti stejně jako:

- detektivní pátrání
- detektivní dohled
- detektivní prověrka
- detektivní vyšetřování (rozkrývání či rozpracování)

1.3 Další formy detektivních činností

1.3.1 Detektivní dohled

Detektivní dohled je forma soukromé detektivní činnosti spočívající v souhrnu úkonů a opatření, využívajících různé metody soukromé detektivní činnosti, směřujících ke kontrole dodržování žádoucího stavu a k včasnému zjištění stavů, které jsou v rozporu se stavem žádoucím a k včasnému přijetí účinných opatření k opětovnému nastolení stavu žádoucího. Detektivní dohled zahrnuje:

a) Průběžné shromažďování informací o objektech (osobách, firmách apod.), a to zejména:
- při personální práci
- při ochraně před únikem informací
- při získávání informací marketingového a konkurenčního charakteru apod.

b) Činnost hotelových detektivů (včetně restauračních a zábavních zařízení, kasin, heren apod.)

c) Činnost detektivů obchodních domů, obchodů apod.

d) Detektivním dohledem jsou rovněž ochranné a obranné doprovody osob, peněžních hotovostí a jiných cenností prováděné skrytým způsobem,

Detektivním dohledem jsou i tzv. „ochranky“ osob. [4]

1.3.2 Detektivní pátrání

Detektivní pátrání je forma kriminalisticko-detektivní praxe, kterou tvoří souhrn vzájemně sladěných činností, úkonů a opatření, za využití celé škály metod soukromé detektivní činnosti, zaměřených k nalezení a zjištění hledaného objektu. Objektem detektivního pátrání mohou být osoby či věci (včetně motorových vozidel). Detektivní pátrání je modifikací pátrání uplatňovaného v kriminalisticko-bezpečnostní praxi. Tato modifikace je dána možnostmi a zvláštnostmi soukromé detektivní praxe. [4]

1.3.3 Detektivní prověrka

Detektivní prověrku chápeme jako proces činností soukromého detektiva s využitím metod a prostředků soukromé detektivní činnosti, jehož cílem je ověření pravdivosti či nepravdivosti informací o osobě, události, skutečnosti apod. či doplnění

nebo získání informací o nových osobách a skutečnostech, jež jsou předmětem zakázky soukromé detektivní služby.

V rámci detektivní prověrky se může jednat o:

a) ověření určitých informací, domněnek, hypotéz, důkazních prostředků apod.
b) zjištění pověsti osoby a dalších informací o osobě, jako např.:
   - místo zaměstnání
   - místo bydliště či bydlišť
   - majetkové poměry apod.
   - zjištění režimu dne apod.
c) zjištění a prověření dodržování režimu ochrany informací
d) prověření a získání základních informací o právnických osobách i fyzických osobách v podnikatelské sféře apod.
e) prověření marketingových informací.

Ve vztahu k formě detektivního rozpracování jde o jednodušší formu detektivní činnosti. [4]

1.3.4 Detektivní rozpracování

Detektivní rozpracování je vysoce kvalifikovanou formou soukromé detektivní činnosti a představuje profesionálně kvalifikovaný výkon činností soukromého detektiva, jejichž cílem je získat a shromáždit, vyhodnotit a interpretovat ucelené informace a důkazní prostředky o určitých skutečnostech, skutkových dějích, o zločinnosti nebo kriminalitě, o fyzických i právnických osobách.

Tyto informace a důkazní prostředky mohou být významné pro:

a) oblast občanskoprávních vztahů
b) oblast rodinně-právních vztahů
c) oblast obchodně-právních vztahů
d) oblast trestně právních vztahů, zejména:
   - informace a důkazy pro oblast obhajoby, zpravidla v součinnosti s advokátem obviněného
   - jako nadstandardní služby (standardní služby jsou poskytovány ze zákona orgány činnými v trestním řízení), klient si však může na

komerčním základě objednat soukromé detektivní služby ke zpracování případu

e) oblasti ochrany informací a ochrany před tzv. firemní špionáží
f) další oblasti podnikatelské činnosti a podnikatelských aktivit
g) detektivní rozpracování v jiných zájmových oblastech [4]

1.4 Nestátní zpravodajství

Nestátní zpravodajství představuje realizaci vědomého a systematického uplatňování zásad práce s informacemi a proces jejich přeměny ve znalost a to mimo rámec státních orgánů a institucí. To v sobě obsahuje získávání, zpracování a využívání relevantních informací - znalostí, které se používají v ochraně, v rozhodování a v prosazování společenských, politických a ekonomických zájmů, procesů a aktivit. V minulosti bylo zpravodajství doménou různých tajných zvědů, státních tajných služeb apod. V současné době, zhruba od druhé poloviny 20. století, se stále více přesouvá do nestátní sféry. V souvislosti se zpravodajstvím je řeč o procesu, resp. o produktech a službách, které jsou pro zajištění tohoto procesu potřebné. Zpravodajství se dnes ovšem již neobejde bez znalostí z celé řady oborů, zejména informatiky, informačních technologií, psychologie, práva a managementu. [1]

1.4.1 Obranné zpravodajství

Zabezpečení komplexní ochrany vlastní organizace, instituce či podniku je základní stavebním kamenem každého zpravodajství. Bez zabezpečení vlastní ochrany nemohou být účinná ani opatření ofenzivního či vlivového zpravodajství (lobbingu).

Obranné (defenzivní) zpravodajství se využívá k obraně vlastních dat, informací a poznatků tak, aby byla míra jejich zveřejnění a možnost konkurence je využít co nejmenší. Obranné zpravodajství, se zabývá analýzou informací vytvořených ve firmě, jejich zveřejňováním a ochranou. [1]

Obranné zpravodajství řeší především:

- zajišťování personální bezpečnosti, režimové ochrany, technickou bezpečnost objektů, softwarovou bezpečnost
- zajišťování komplexní informační bezpečnosti
- zajišťování ochrany technologických procesů, především know-how, vynálezů, zlepšovacích návrhů, výzkumu, vývoje
- zajišťování bezpečnosti v obchodních vztazích
- aktivní ochranu proti dezinformacím a působení vlivového zpravodajství konkurence
- aktivní ochranu proti ofenzivnímu zpravodajství konkurence [5]

1.4.2 Ofenzivní zpravodajství

Někdy také označované jako „aktivní zpravodajsko-konkurenční průnik". Ofenzivní zpravodajství je logickým pokračováním často již prováděného pasivního monitoringu informací. Řeší převážně:

- zajišťování informací potřebných pro podnikání (průnik do managementu znalostí).
- zajišťování informací marketingového charakteru
- zjišťování cílených informací o konkurenci
- zjišťování informací o potřebných technologiích
- zjišťování informací o know-how, výzkumu a vývoji [5]

Ofenzivní zpravodajství využívá jak legálních, pololegálních, tak i nelegálních prostředků.

Za legální prostředky lze považovat např.:

- informace z otevřených zdrojů
- najímání bývalých zaměstnanců konkurence za účelem využití jejich obecných schopností a zkušeností z práce u konkurence. Je si ale potřeba uvědomit s tím spojená rizika (informační bezpečnost atd.)
- získávání a udržování si zkušených smluvních zaměstnanců na vedlejší pracovní poměr či dohodu pracovní činnosti z řad zaměstnanců konkurence (podobná rizika jako u předchozího bodu).

Za pololegální (konspirativní) lze považovat:

- získávání informátorů v prostředí konkurence
- pronikání informátorů do prostředí konkurence

Za nelegální lze považovat:

- telefonní, datové a další odposlechy
- nabízení úplatků a další formy korupce [1]

1.4.3 Vlivové zpravodajství

Představuje proces, kde soukromý detektiv vytváří (prosazuje) vhodné prostředí a podmínky pro realizaci rozhodnutí subjektu (zákazníka). Také bývá označované jako lobbying. Lobbying sám o sobě je zcela legální činnost v západním světě často používaná a v angloamerickém světě bussinesu zcela běžná, pokud ovšem ctí určité zásady a nepřerůstá ve vulgární nátlak, podplácení, vyhrožování a podobně. Lobbying může být jak obchodní - podnikatelský, tak i politický. Lobbying je uskutečňován především početnou a vlivná zájmovou skupinou, která prostřednictvím svých zaměstnanců, či k této činnosti specializovaných osob (např. právníků, advokátů), vytváří stálý nátlak na státní administrativu, poslance, senátory a ostatní politiky, ministry, členy státní byrokracie a výkonné moci včetně prezidenta, za účelem ovlivňování jejich rozhodnutí či konání, ve prospěch této skupiny. [5]

2 TECHNOLOGIE NESTÁTNÍHO ZPRAVODAJSTVÍ

Nejzákladnějšími formami nestátního zpravodajství, jak bylo již na začátku práce zmiňováno, jsou - komerční zpravodajství (na komerční bázi, smluvním základě) a zpravodajský servis (výsledný zpravodajský produkt slouží pouze pro vlastní organizaci). Tyto dvě formy jsou, ale vykonávány zejména prostřednictvím detektivního zpravodajství, tedy jedné z forem detektivní činnosti.

Technologiemi ve zpravodajství rozumíme využívání forem, metod a prostředků, potřebných k vyhledávání, zpracovávání a distribuci výsledných znalostí (poznání). Dá se tedy říci, že technologie umožňují vyhledávat data a zpracovávat je v informace, tyto informace pomocí pochopení informací a za využití zpravodajské analýzy přeměňovat ve znalost a chápat znalosti ve vzájemných souvislostech, což představuje poznání.

Zpravodajské technologie můžeme rozdělovat podle typu zdroje získávání informací na zdroje:

2.1 Technologie práce s primárními zdroji

Jde o využití speciálních detektivních metod a prostředků s cílem využívání těchto zdrojů informací pro investigativní postup, který nám umožní vyhledávání a shromažďování informací od těchto zdrojů. Pro práci s primárními zdroji je důležitá znalost tzv. sociálního inženýrství, nebo též sociotechniky.

2.1.1 Sociotechnika

Sociotechnikou, nebo-li sociálním inženýrstvím, můžeme nazývat činnost, při které dochází k přesvědčování a ovlivňování lidí, s cílem oklamat osobu, tak že vyzradí nebo provede určité úkony k vyzrazení požadovaných informací.

Pojem lze chápat i jako metodu (postup) zpravodajských pracovníků při získávání informací z primárních zdrojů speciálními zpravodajskými postupy za využití psychologických, pedagogických a sociologických znalostí. Nejznámějším představitelem sociálního inženýrství je Kevin Mitnick.

Sociotechnický proces se skládá ze čtyř kroků:

1. *Postup* - Začíná od analýzy volně přístupných informací jako jsou katalogy, finanční zprávy, patentové přihlášky, články v odborném tisku, obsah internetových stránek, ale také i obsah popelnic
2. *Budování vztahu a důvěry* - Používání vnitřních informací, vydávání se za někoho jiného, zmiňování jmen, která oběť zná, žádosti o pomoc nebo vyvolání dojmu autority.
3. *Využití důvěry* - Žádost o informaci nebo činnost, adresovaná oběti. Zmanipulování oběti, aby sama žádala o pomoc.
4. *Využití informace* - Pokud je získána informace, je to pouze dalším krokem přibližujícím útočníka k cíli, vrací se k předcházejícím bodům cyklu tak dlouho, dokud nedosáhne svého cíle.

Kroky, které učinily sociotechnický útok účinným:

1. Znalost – znalost prostředí, znalost jmen a telefonních čísel manažerů a významných pracovníků organizace, instituce, společnosti či firmy apod.
2. Znalost terminologie
3. Prezentace sebe sama – prezentuje sebe sama v duchu připravené legendy.

Možné způsoby sociotechnického postupu:

- *Odhalit „díru" v zabezpečení*, obvykle jím bývá člověk. Pro sociotechnika (detektiva, zpravodajce) a jeho postupy ovlivňování jsou velmi vhodné a žádané osoby s projevy egoismu, sklony k pasivitě, nedbalosti, korupci apod.. To jsou nejvýznamnější „díry" v informační bezpečnosti.

- Jako nevyčerpatelným zdrojem informaci jsou také zaměstnanci v restauraci. V tomto směru jsou pro sociotechnika velice zajímavé *restaurace v blízkosti podniku*, kam zaměstnanci docházejí. Stačí si sednout do jejich blízkosti a poslouchat. Restaurace v blízkosti zájmového objektu, kam zaměstnanci docházejí, jsou z hlediska informační bezpečnosti obrovskou dírou v zabezpečení informační bezpečnosti. Prakticky každý v takovémto případě je vystaven riziku sociotechnického útoku.

- K nositeli informace nebo jiné osobě mající nebo usnadňující přístup k informacím, *být zdvořilý*.

- Připravit si a použít vhodnou *legendu* k dosažení svého cíle;

- *Využít psychologické, pedagogické a sociologické ovlivňování* ke zmanipulování objektu zájmu. Proces ovlivňování se odehrává tím, že sociotechnik působí na složitou strukturu osobnosti jedince, jejíž stránky jsou vzájemně spjaty a navzájem se ovlivňují. Sociotechnik působí na motivační sféru osoby, a tím ovlivňuje a utváří její postoje (ochotu spolupracovat, ochotu poskytnout informace či výhodu apod.). Působí přes potřeby, zaměření a zájmy osobnosti oběti. Mechanismus ovlivňování často znamená řešit i rozporuplné situace. Lidmi obsluhujícími systém jsou osoby s přístupem k informačním systémům a lidé - nositelé informací.

- Zjistit si, ujasnit si, připravit si a *používat správnou terminologii*. Přitom se sociotechnik zaměřuje na zájmy, očekávání, představy a problémy oběti.

- *Zformulovat si věrohodné otázky* nebudící podezření objektu zájmu. Zájmové otázky je třeba propašovat k zájmovému objektu mezi otázkami nezájmovými a možná i bezvýznamnými, které slouží k získání a udržení si důvěry. Hledá a vytváří vazbu mezi potřebami a problémy oběti na straně jedné a cíli a potřebami sociotechnika na straně druhé. Sociotechnik zaujímá stanovisko k potřebám, překážkám, potížím oběti a formuluje stanovisko k jejich řešení v duchu svých cílů a potřeb. Přitom volí správnou technologii sociotechnického postupu.

- Sociotechnik *předem předpokládá, že se setká s podezíravostí nebo odporem* a je vždy připravený na překonání bariér nedůvěry. Dobrý sociotechnik plánuje svůj útok jako šachovou partii, předvídá otázky, které může oběť klást, a připravuje si patřičné odpovědi.

- Zaváhá-li protějšek, mít připravenou a použít vhodnou *legendu k odpoutání podezření* a odpoutání pozornosti zájmového objektu, a tak zbavit protějšek opatrnosti.

- *Být trpělivý* a tzv. „ netlačit na pilu“. V této souvislosti se objevuje pojem „spálené zdroje“ – tzn., když dopustí, aby oběť poznala, že má na ní být podniknut útok. Tehdy pravděpodobně upozorní ostatní pracovníky a vedení o tom, že útok nastal. V takovém případě bude těžké tento zdroj ještě někdy využít

- *Všímat si maličkostí*, které ukazují na ochotu či neochotu zájmového objektu ke „spolupráci“.

- Sociotechnik manipuluje lidmi i tím, že předstírá, že od nich sám *pomoc potřebuje*. Vychází přitom z předpokladu, že lidé dokážou soucítit s jinými lidmi, kteří se ocitli v tísni.

- Úspěšným trikem sociotechniky je psychologický *trik spočívající v oblečení*. Obleče-li se sociotechnik tak, aby vypadal jako vrcholový manažer, který si hodně vydělá, „otevírá mu to dveře„. Maličkosti vytvářejí dojem. Oblek, kravata, náležitý účes a dobrý střih dokážou svést mnohé.

- Při snaze dostat se nepozorovaně do zájmového objektu je účinný starý trik – *vmísit se do davu.* Při vcházení do budovy či procházení vrátnicí „nalepit se“ k nějaké skupince a projít jako by k ní patřil. Nesmí dát najevo obavy nebo dokonce strach, musí se chovat suverénně.

- Ne příliš vkusným a pravděpodobně i etickým, ale o to účinnějším a efektivním je *věnovat pozornost odpadkům* a odpadkovým košům a smetištím. Tento způsob hledání informací je docela bezpečný, riziko je nevelké a zisk může být ohromný, snad jen koupení osob, které se zabývají úklidem, zvětšuje riziko nesení nějakých důsledků. Také výzvědné služby léta používají tuto metodu. Sociotechnik najde v odpadkových koších hodně zajímavých věcí - informace o struktuře firmy, plánech apod. Tyto detaily se mohou zdát lidem z dané organizace nedůležité, ale pro útočníka jsou velmi cenné. Obyčejně si nikdo nebo jen málokdo dělá velké starosti s tím, co vyhazuje do koše doma, a o to méně v zaměstnání.

- Velice úspěšnou sociotechnickou metodou je *„zastrašení“*. Nejedná se ale o vydírání, ale jde o zastrašení při zachování požadavku dodržení právních norem. Jde v podstatě o ovlivnění pomocí autority. Uvádění jmen jiných zaměstnanců je obvykle používáno pro vyvolání dojmu, že máme blízké kontakty s osobou ve firmě vysoce postavenou. Oběť ochotněji něco udělá pro člověka, který zná někoho, koho ona zná. Zastrašení pomocí odvolání se na autoritu funguje zejména tehdy, když oběť zaujímá poměrně nízké postavení v podniku. Použití jména důležité osoby nejenže oslabuje přirozený odpor a podezíravost, ale ještě posiluje ochotu pomoci. Sociotechnik ví, že tento podvod funguje nejlépe, když používá jméno osoby s vyšším postavením, než je bezprostřední nadřízený dané osoby. Tento trik je obtížný v případě malých firem. [1]

2.1.2 Zpravodajské vytěžování osob

Obr. 2 Metoda zpravodajského vytěžování [1]

Vytěžování osob je základní metodou zpravodajské práce směřující k získání rozličných informací (např. informace o politickém či společenském dění, informace vědeckého či technického charakteru marketingového charakteru, informací o konkurenci a dalších informací apod.) potřebných pro různé oblasti rozhodování. Jde v podstatě o řízený rozhovor s využitím znalostí a metod psychologie včetně psychologické metody asertivního chování.

Zpravodajské vytěžování probíhá ve 3 fázích:

1. Zajištění kontaktu s vytěžovanou osobou
    a. Bližší poznání vytěžované osoby
    b. Navázání kontaktu
2. Monologická část (vytěžované osoby)
3. Dialogická část (kladení a zodpovídání otázek)

Pro tuto metodu je důležité vědět, zda:

- Zda je vytěžovaná osoba *bývalým zaměstnancem* cílového objektu. Případně jestli odešla sama nebo byla vyhozena
- Zda se jedná o spokojeného či *nespokojeného zaměstnance* cílového objektu. Případně vědět důvod její nespokojenosti

Pokud se osoba cítí nedoceněna, ukřivděná a podobně poškozená, pak je vhodné získat důvěru vytěžované osoby (podporovat ji, že jí bylo ukřivděno apod.) a motivovat ji satisfakcí, tím že poskytne cílené informace.

Tyto informace mají velký vliv na volbu vhodné sociotechnicky a jejího dalšího postupu.

Mezi objekty sociotechnického vytěžování osob jsou zejména:

- Manažeři konkurenčních podniků
- Rodinní příslušníci, přátelé a známí manažerů konkurenčního podniku [1]

2.1.3 Zpravodajské informační proniknutí

Velký význam pro kvalifikovaný výkon nestátní zpravodajské činnosti, k získávání kvalitních informací a při realizaci zpravodajských. Jedná se o cílevědomý přístup k získávání cílově zájmových informací budováním informačních zdrojů. Tato metoda je velice úzce spojena se zpravodajským vytěžováním osob, ke kterému dochází mezi zpravodajským pracovníkem (soukromým detektivem realizujícího zpravodajskou činnost) a jeho informátorem - informačním zdrojem.

Zpravodajské proniknutí může být vykonáváno i přímo samotnými zpravodajskými pracovníky, kteří mají velké znalosti o získávání informací. Spíše ale využívají tzv. „obchodníků s informacemi“ (informátoři), protože jsou často postupy velmi obtížné z hlediska dodržování zákona a etiky. Pro úspěšné získávání informací, by měl soukromý detektiv seznámit informátora také s některými sociotechnickými praktikami.

Rozdělení informačních zdrojů dle jejich typu:

- Lidské informační zdroje
- Technické informační zdroje

Mezi důležité vlastnosti informačních zdrojů patří především jejich:

- Vhodnost

  Představuje schopnost zdroje pohybovat se v zájmové oblasti, případně v oblasti zájmové osoby. U technických zdrojů je tato vlastnost ovlivněna určitými technickými parametry zařízení.

- Schopnosti

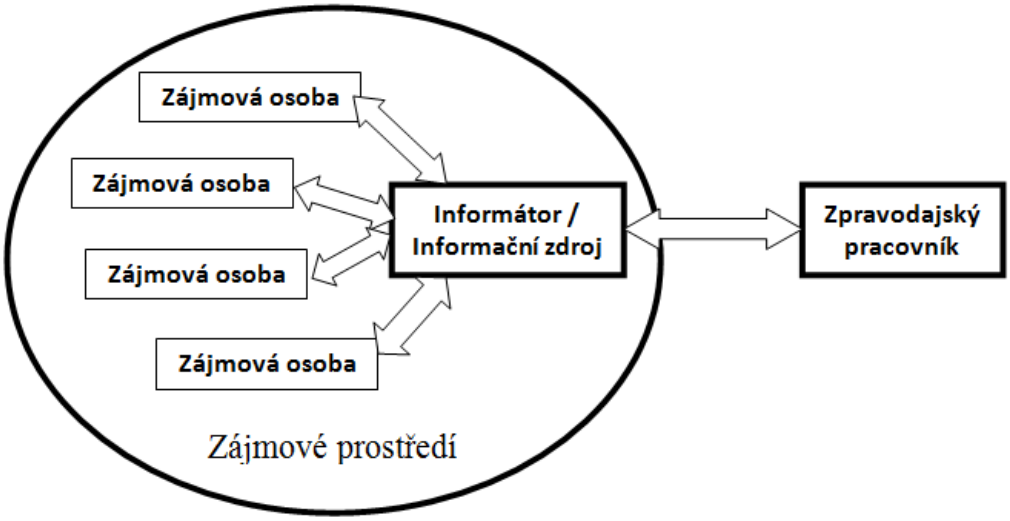
  Opírá se o psychickou výbavu umožňující navazovat kontakty, získávat informace, rozpoznávat podstatné informace od nepodstatných, objektivně informace hodnotit. U technických zdrojů je opět ovlivněno parametry zařízení.

- Spolehlivost zahrnuje:
  - Pravidelnost informací
  - Pravdivost informací
  - Objektivita (nezkreslování) informací
  - Důvěryhodnost zdroje

Rozdělení informačních zdrojů dle způsobu získávání informací:

- **Poziční**

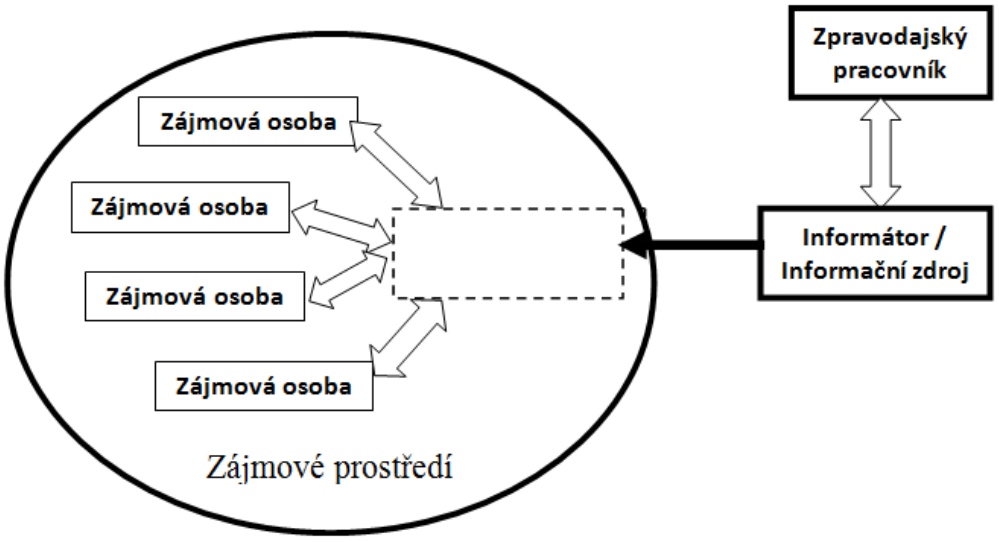
  Informační zdroj je vytipován ze zájmového prostředí či okolí zájmové osoby (osob) a je teprve jako informátor získáván.



Obr. 3 Zpravodajské informační proniknutí-poziční, inspirace JUDr. Brabec [1]

- **Cílově zaměřené**

  Informační zdroj je získáván jako vyhovující osoba, která bude podávat informace, následně je infiltrována do zájmového prostředí nebo k zájmové osobě



Obr. 4 Zpravodajské informační proniknutí-cílové, inspirace JUDr. Brabec [1]

Rozdělení informačních zdrojů dle jejich získání:

Teorie a praxe policejní činnosti a činnosti tajných služeb, ale i nestátního zpravodajství v souvislosti se získáváním informací rozlišuje:

- informační zdroje získané na základě jejich přesvědčení (na ideovém základě);
- informační zdroje získané na materiálním základě (např. finanční odměna);
- informační zdroje získané na podkladě kompromitujících materiálů.

Získávat informační zdroje v rámci nestátní zpravodajské činnosti na podkladě kompromitujících materiálů sice nelze zcela vyloučit, ale nedoporučuje se tento přístup. Jednak zpravodajský pracovník nestátního zpravodajství nemá možnosti jako policie či tajné služby, na straně druhé použití kompromitujících materiálů by mohlo být hodnoceno jako vydírání. To je třeba mít vždy na mysli. Je také málo pravděpodobné, že by někdo byl ochoten poskytovat informace zpravodajskému pracovníkovi ze svého přesvědčení.

Je proto nejpravděpodobnější získání informačního zdroje – informátora, jako placenou službu, tedy na materiálním základě. To znamená, že osoba bude ochotna stát se informátorem - informačním zdrojem soukromého detektiva za finanční odměnu. Tím se informace stanou pro informační zdroj zbožím a zbožím jsou i pro soukromého detektiva. Každá informace má svou hodnotu vyjádřenou v peněžní hodnotě.

Metodu zpravodajského proniknutí je třeba považovat za velice obtížnou a náročnou na profesionalitu zpravodajského pracovníka. Pro proces vytipování, získávání informátora, případně jeho zavedení do prostředí a následně jeho kontroly, jsou využívány další metody nestátní zpravodajské činnosti. Jde zejména o metodu zpravodajské kombinace, metodu zpravodajského pozorování, obecné metody modelování apod. [1]

2.1.4 Zpravodajské pozorování (monitoring)

Je velice frekventovaná metoda pro pracovníky nestátního zpravodajství, která zaujímá společně se zpravodajským vytěžováním klíčovou roli. Je také součástí dalších zpravodajských metod, zejména zpravodajského pátrání, se kterým se v obecné rovině prolíná.

Monitoring může být prováděn podle pohybu:

- Staticky
- Dynamicky

Vizuální kontroly podle utajení monitoringu:

- Otevřeným způsobem
- Skrytým způsobem

Skryté monitorování je převážnou částí této metody. Důvodem utajování postupu sledujícího detektiva není jeho tajuplnost, ale významná účelnost zjištění objektivní pravdy, skutečného chování sledovaného objektu. Pokud by sledovaná osoba o této metodě věděla, prováděla by účelově zastírací činnost, která však není předmětem šetření.

Sledovaným zájmovým objektem může být:

- Osoba (popř. skupina osob)
- Prostor (popř. neživé objekty)
- Probíhající děj

Cíle detektivního pozorování:

- zmapování denního režimu zájmové osoby;
- zmapování styků - styková báze
- zjištění významných informací o jednání a chování zájmového objektu
- zjištění a zadokumentování a tím potvrzení předpokládané činnosti zájmového objektu, která je podstatou objednávky zákazníka;
- zjištění významných informací o podezřelých zájmových prostorách (případně neživých objektech), jež jsou v zájmu soukromé detektivní činnosti,

Monitoring slouží zejména k:

- potvrzení již známých poznatků o osobě či jiném objektu;
- vyvrácení těchto poznatků;
- získání nových upřesňujících a doplňujících poznatků a dalších informací;
- získání zcela nových poznatků, které rozšiřují poznatkovou bázi.

Fáze detektivního pozorování:

- příprava (rekognoskace terénu, ve kterém má být osoba tzv. "vystavena"- monitorována, převzata k monitorování)
- realizace (zajištění utajení, možnosti bezprostředního kontaktu a kontroly nad jednáním osoby, pořizování dokumentace)
- shromáždění a třídění poznatků (informací), získaných v průběhu monitorování (zpracování pořízených audio, video a foto záznamů)
- doplnění neúplných informací o údaje z jiných zdrojů
- analýza a interpretace informací a jejich využití v rámci jiných metod a forem soukromé detektivní činnosti
- zpracování zprávy a dokumentace pro klienta

Zásadní chyby při zpracovávání zprávy:

- nepřesného popisu osoby, situace v místě a čase
- abstrahování dalších údajů, které nebyly prokazatelně zjištěny a jsou zanášeny do skutečně pozorovaného děje
- komentování zjištěných skutečností dle vlastního názoru [1]

2.1.5 Zpravodajské osobní pátrání

Zpravodajské osobní pátrání je třeba chápat jako soustavnou činnost nestátního zpravodajství realizovanou v jeho každodenní činnosti, která je nejčastěji užívanou komplexní metodou nestátního zpravodajství. V jejím rámci zpravodajský pracovník přímo a bezprostředně užívá veškeré zpravodajské prostředky, způsoby a postupy za účelem získání informací, věcí a písemností, které by v budoucnu mohly sloužit jako relevantní informace vedoucí ke znalosti apod. Zpravodajskému osobnímu pátrání, stejně jako

každému systému, přísluší určitá množina prvků (subsystémů), jimiž jsou jednotlivé další metody nestátní zpravodajské činnosti.

Využívání zpravodajského osobního pátrání zahrnuje další zpravodajské metody:

- zpravodajské pozorování;
- zpravodajské vytěžování osob;
- zpravodajské vytěžování a vyhodnocování dokumentů z evidencí, registrací, archivů a databází;
- kriminalistické metody vyhodnocování stop apod.

Zpravodajské osobní pátrání využívá zpravodajský pracovník, zejména k dosažení následujících cílů:

- k získání informací a k aktualizaci operativní situace a k prohloubení a doplnění osobní a místní znalosti;
- k získání prvotních (výchozích) informací pro rozhodování v procesu přípravy a realizace dalších metod zpravodajské práce;
- k získání zpětné vazby (informací o průběhu a efektivnosti) přípravy a realizace kroků, úkonů a opatření nestátní zpravodajské činnosti (o průběhu přípravy a realizace jednotlivých metod);
- k přímému naplňování nestátní zpravodajské činnosti; [1]

2.1.6 Zpravodajská legenda

Zpravodajskou legendu je třeba chápat jako nepravdivé, smyšlené podání s pravdivými prvky, která je pro danou chvíli neprověřitelná ze strany osoby, na kterou má působit a kterou má ovlivnit ve prospěch zpravodajského pracovníka či jeho informačního zdroje. Úspěšná zpravodajská legenda musí vycházet z objektivně existující situace působící na osobu, jíž je určena. Vychází tedy z hluboké znalosti detektiva o popisované situaci, objektu, člověku, protože musí působit hodnověrně. Pravdivé prvky musí být ze strany osoby, proti níž legenda směřuje, lehce ověřitelné, případně známé. Naopak smyšlené prvky musí být v daném okamžiku neprověřitelné nebo velmi těžce prověřitelné.

Není možné akceptovat jako legendu náhodné, situační užití nepravdy, která má shodou náhod pro daný účel úspěch. V tomto případě může jít jen o dobrou reakci zpravodajského pracovníka či duchapřítomnost, nikoliv však o cílevědomě utvořenou legendu. Jde o náhodnou dezinformaci.

Cílem legendy je zajistit krytí pracovníka zpravodajské činnosti či jeho informátora, jím využívaných metod nebo užitých prostředků. Tato zpravodajská metoda je významnou speciální metodou nestátního zpravodajství.

Detektivní legenda musí splňovat požadavky:

- Věrohodnost
  musí tedy ve svém základu vycházet z objektivní reality (skutečnosti) a její navršení teprve může obsahovat nepravdivé nebo polopravdivé skutečnosti (informace);
- Účinnost
  musí mít schopnost svým obsahem ovlivnit jednání, myšlení a smýšlení zájmové osoby či skupiny zájmových osob. Vytvořená legenda musí skýtat záruku, že osoba (či skupina osob), jíž je určena, bude přijatým sdělením natolik ovlivněna, že bude jednat tak, jak detektiv předpokládá, aby tak mohl realizovat postupy potřebné k řešení a vyřešení případu.
- Neprověřitelnost
  Neprověřitelnost nepravdivé části legendy v daném čase a na daném místě [1]

2.1.7 Zpravodajská kombinace

Jedná se o naplánovaný a plánovitě realizovaný soubor úkolů nestátních zpravodajských činností, které na sebe vzájemně navazují a vzájemně se podmiňují s cílem získat pro daný případ zpravodajské činnosti relevantní informace.

Tato metoda je založena na využití obecných, zejména psychologických metod, a to zejména metody reflexivních her a asertivního chování, a v různých kombinacích v sobě absorbuje další dílčí metody zpravodajské činnosti.

Podstatou zpravodajské kombinace je vyvolání řízených a záměrných podnětů do určitého zájmového prostředí a určité zájmové situace s cílem vyvolat reakci zájmového objektu či celého zájmového prostřední, která je dalšími zpravodajskými metodami sledována a zaznamenávána.

Při přípravě a realizaci kombinačního zpravodajství se využívá zejména metod:

- Indukce,
- Dedukce,
- Analýzy,
- Syntézy,
- Analogie, atd.

Zjednodušeně lze říci, že zpravodajská kombinace spočívá ve vyvolání situace, na níž očekáváme nějakou reakci, která je zaznamenána a posléze zpracována.

Vysoké efektivnosti této metody lze dosáhnout dobrým promyšlením, kvalitním propracování postupu řešení a uplatňování vhodných zpravodajských opatření.

Umělé prvky, které jsou vnášeny do přirozených situací, za účelem vyvolání cílených reakcí, by měly splňovat podmínky:

- Splynutí umělých prvků se situací, tak aby působily věrohodně
- Vytvořeny na základě charakteristiky cílových osob
- Utajení vnesených umělých prvků, před cílovými osobami i jejich širokým okolím
- Nesmí negativně působit na další osoby, které v dané době na daném místě působí
- Nesmí cílové osoby provokovat k páchání trestné či protiprávní činnosti

Zpravodajská kombinace jako složitý model systémového přístupu k řešení zadaného problému vyžaduje provedení celé řady na sebe navazujících zpravodajských opatření a úkonů. Proto také není možné kvalitně zpravodajskou kombinaci uskutečnit bez velmi kvalitní a detailní přípravy, při níž je nutno vycházet z následujících doporučení:

- Důkladná analýza situace
- Určit cíle a zvolit způsob jejich naplnění

- Plánovitě provádět zpravodajské úkony a opatření
- Stanovit a sladit umělé prvky s průběhem zpravodajské kombinace
- Trvalá kontrola průběhu [1]

2.1.8 Zpravodajská dezinformace

Zpravodajská dezinformace představuje metodu nestátní zpravodajské činnosti sloužící k infiltraci účelově formulované a záměrně nepravdivé zprávy do zájmového prostředí (osobě, objektu) zpravodajské činnosti. Tato záměrná infiltrace nepravdivé zprávy sleduje konkrétní cíl, který je determinován potřebami zpravodajské práce.

Dezinformace obecně znamená průnik nepravdivé zprávy. Je jednou významných metod nestátního zpravodajství, a to v rovině ofenzivního, obranného i vlivového. Při jejím použití je třeba postupovat obezřetně a použití metody zpravodajské dezinformace je nutné důkladně zvážit i z hlediska, zda nedojde k naplnění skutkové podstaty trestného činu šíření poplašné zprávy, pomluvy apod. V rámci běžné zpravodajské činnosti připadá v úvahu zejména s realizací metody zpravodajského informačního proniknutí, a zvláště pak v rámci zpravodajské kombinace – zpravodajských her. Významné místo zaujímá při realizaci vlivového zpravodajství - lobbyingu.

Zpravodajská dezinformace má mnoho společného s metodou zpravodajské legendy. Je však na vyšším stupni z hlediska četnosti použitých nepravdivých prvků, z hlediska doby trvání její neprověřitelnosti a obvykle ovlivňuje skupinu více osob. Zpravodajská legenda je nedílnou součástí i v rámci zpravodajské dezinformace. Na rozdíl od zpravodajské legendy je zpravodajská dezinformace složitější při jejím uplatnění. Stejně jako u zpravodajské legendy je třeba, aby část dezinformační zprávy byla pravdivá a tvořila základ zpravodajské dezinformace. Tato pravdivá část dezinformace, stejně jako u zpravodajské legendy, tvoří základ dezinformace a sleduje určitý cíl. Má za úkol učinit zpravodajskou dezinformaci jako celek věrohodnou pro objekt (prostředí, osoby), vůči kterému působí. Pokud by zpravodajská dezinformace nebudila dojem věrohodnosti, byla by bezcenná a její infiltrace k zájmovému objektu nestátní zpravodajské činnosti by byla nemožná, případně by přinesla opačný výsledek, než jaký je sledován. Dezinformace by se

tak stala pro záměry nestátního zpravodajství bezcennou a mohla by tzv. „nahrát na smeč konkurenci“.

V souvislosti se zpravodajskou dezinformací hovoříme o jejím využití v rámci dalších metod - jako například detektivního informačního proniknutí, zpravodajské kombinace, ale i v rámci zpravodajského vytěžování apod. Metoda zpravodajského informačního proniknutí slouží jako nosič dezinformace infiltrované do zájmového prostředí, ale také může sloužit jako příprava ke zpravodajskému informačnímu proniknutí. V souvislosti s průnikem dezinformace vůči zájmovému objektu (prostředí) pomocí zpravodajského informačního průniku se ve zpravodajské a policejní práci hovoří o vlivové agentuře (vlivovém informačním nosiči) či o vlivových informátorech – dezinformátorech, kteří mohou infiltraci dezinformace provádět vědomě či nevědomě. Nejideálnější pro infiltraci detektivní dezinformace je informátor, který byl získán jako informátor pro získávání informací, o němž se zpravodajský pracovník přesvědčí, že pracuje na dvě strany, nedá to znát a využívá takového informátora jako dezinformátora. Touto cestou se přes informátora dostává dezinformace ke svému cíli.

Metoda zpravodajské legendy slouží tehdy, pokud ji použijeme jako zakrytí cesty - „zástěrky“ pro přenos dezinformace, která slouží k zakrytí cíle dezinformace i samotné dezinformace. Průběh zpravodajské dezinformace je pak zpravidla sledován dalšími zpravodajskými metodami, čímž se stává součástí zpravodajské kombinace. Zpravodajská dezinformace, jakožto metoda nestátní zpravodajské činnosti, se odlišuje od zpravodajského ovlivňování (lobbyingu) tím, že zpravodajský lobbying je cílem i zpravodajské dezinformace. Přitom zpravodajská dezinformace bývá i součásti vlivového zpravodajství.

Metoda zpravodajského informačního proniknutí s využitím zpravodajské dezinformace má zvláštní postavení, které spočívá v:

- infiltraci jedním či několika dezinformátory
- kontrole odezvy účinku dezinformace v zájmovém prostředí. Jde o zabezpečení tzv. zpětné informační vazby.

Zpravodajská dezinformace probíhá v několika fázích:

- příprava zpravodajské dezinformace :
- uvědomění si záměru sledovaného dezinformací;
- formulace dezinformačního obsahu ;
- plánování zpravodajské dezinformace;
- vytipování dezinformačních nosičů a informačních zdrojů;
- plán průběhu realizace zpravodajské dezinformace;

Vlastní realizace zpravodajské dezinformace:

- proniknutí nosiči dezinformace a informačními zdroji do zájmového prostředí, jenž je cílovým objektem dezinformace ;

- předání dezinformačních zpráv nosiči dezinformace ; (nosičem nemusí být vždy informátor – dezinformátor, ale může se jednat třeba i o fingovaný telefonní hovor, vhodnou tiskovou zprávu apod.)
- infiltrace dezorientační zprávy (dezorientačního chování – obsahu dezinformace) do zájmového prostředí (k objektu dezorientace);
- získávání zpětné vazby;

Vyhodnocení účinnosti infiltrované dezinformace;

- analýza informací (zpětných vazeb);
- interpretace informací (zpětných vazeb);
- plán korekce dezinformace;

Korekce průběhu zpravodajské dezinformace nastává v případě, že dezinformace v některých bodech nesplnila své cíle. Cyklus pokračuje opakováním jednotlivých fází.[1]

2.1.9 Zpravodajská obhlídka místa

Pro pracovníka nestátního zpravodajství je velmi důležitá orientace v terénu (regionu, prostoru apod.), v němž zajišťuje zpravodajskou činnost. Z tohoto pohledu je pro něho velmi významná místní a osobní znalost.

Můžeme v této souvislosti hovořit o rekognoskaci terénu budoucí realizace zpravodajské činnosti, ale také o kriminalistickém zajištění místa trestného činu a kriminalistické obhlídce místa trestného činu či jiného protiprávního jednání souvisejícího se zpravodajským zájmem.

Zpravodajská obhlídka místa může tedy sloužit především a zejména k:

- rekognoskaci místa, v němž bude probíhat realizace některých z dalších metod zpravodajské činnosti. Jde o obhlídku sloužící pro potřeby plánování a přípravy akcí nestátního zpravodajství.
- vyhledávání a zajišťování stop a jiných nosičů (médií) důkazních prostředků, resp. stop a předmětů, které by v další fázi činnosti mohly být soudem či správním orgánem použity jako důkazy. Zejména v rámci komplexní zpravodajské ochrany organizace, instituce, úřadu či podnikatelského subjektu mohou být zajišťovány informace o důkazech, důkazy a další informace potřebné pro správní a soudní kauzy.
- sloužící k vlastní přímé realizaci zpravodajské činnosti, např. při zpravodajském informačním průniku, při pátrání po osobách a věcech, které jsou v zájmu zpravodajské činnosti apod. [1]

2.2 Technologie práce se sekundárními zdroji

Technologie práce se sekundárními informačními zdroji neboli otevřenými zdroji. Skládá se z následujících kroků:

- *zmapování* zájmové právnické či fyzické osoby, události, situace, okolnosti, jevu apod. Z hlediska vzájemných vztahů a souvislostí (např. obchodních vztahů, politických či společenských vazeb apod.);
- *rychlé získání relevantních informací* o zájmovém subjektu, události, skutečnosti, jevu, prostředí apod. z otevřených (sekundárních) zdrojů jako jsou média, internet a další veřejně dostupné databáze a doplnění informací z dalších komerčních zdrojů.
- *rychlé zpracování* všech získaných základních informací formou tématických, kontextových a přehledových rešerší a využití těchto informací při monitoringu zájmového subjektu, události, skutečnosti nebo jevu apod.;
- *rozkrytí vzájemných vazeb a souvislostí* (vazeb na další firmy či fyzické osoby, politické strany, organizace, instituce apod.) do potřebné úrovně;
- *získání dalších potřebných údajů* pro následná šetření, pro rozhodnutí o využití speciálních zpravodajských postupů, pro plánování zpravodajského procesu apod.;
- *doplnění relevantních informací* do diagramu, vztahové popřípadě vývojové analýzy a jejich názorná prezentace, vhodná je grafická prezentace pomocí vztahové nebo vývojové analýzy;
- *využití získaných znalostí a poznatků* (relevantních informací) a dosud provedených rešerší a analýz pro realizaci dalších zpravodajských opatření za využití primárních zdrojů informací (investigativních postupů), pokud je toto požadováno. [1]

2.2.1 Zpravodajské vyhodnocování dokumentů

Metoda detektivního vyhodnocování dokumentů a otevřených zdrojů je v rámci nestátní zpravodajské činnosti jednou z významných metod. Písemné dokumenty jsou významnými nositeli informací a v řadě případů mohou v dalším procesu zpravodajské činnosti posloužit jako významný zdroj výchozích informací.

K vyhodnocování dokumentů může docházet z celé řady hledisek, nás především zajímá hledisko:

- jejich obsahu, kdy půjde o:
    - dokumenty hovořící k meritu zjišťované zpravodajské záležitosti (věci)
    - dokumenty podpůrné, svědčící svým obsahem nepřímo o dalším zpravodajském postupu
- podle jejich formy:
    - mající schopnost být listinnými zdroji informací ve zpravodajském zájmu, případně důkazními prostředky;
    - dokumenty prokazující totožnost, stav apod.;
    - protokoly osvědčující úředně zkoumanou skutečnost, osobu
    - osobní dopisy a obdobné písemnosti mající vztah ke zkoumanému zpravodajskému zájmu, ke zkoumané osobě či skutečnosti;
    - technické, účetní a jiné dokumenty a dokumentace;
    - ostatní spisové materiály, které mají alespoň taktickou hodnotu.

- z hlediska jejich pravosti:
  posouzení z hlediska pravosti dokumentu provádí zpravodajský pracovník pouze zběžně. Ke konečnému verdiktu o pravosti se obrátí nejlépe na soudního znalce.

Každý dokument je třeba posuzovat z hlediska jeho:

- informační hodnoty :
- objemu informací obsažených v dokumentu;
- obsahu informací a jejich vztahu k zájmové osobě, události apod.;
- objektivity informací apod.
- aktuálnosti informací

Důkazní hodnoty:

- Mají schopnost se stát procesní cestou důkazem
- Nemají schopnost být použity jako případný důkaz (mají schopnost pouze taktickou)

Dokumenty jsou v nestátní zpravodajské činnosti velmi významné především proto, že mají obvykle stabilní schopnost být zdrojem velkého množství významných informací i posloužit jako listinné důkazy. Proto je třeba také dokládat jejich pravost a původ. [1]

2.2.2 Zpravodajské vytěžování evidencí, registrů a archivů

Databáze, evidence a registry jsou velmi významným zdrojem informací, bez nichž se zpravodajská práce nemůže obejít. Velice složitá je však otázka legality vstupu pracovníků nestátního zpravodajství (soukromých detektivů zajišťujících zpravodajskou činnost) do některých státními orgány a úřady vedených a zpravovaných archivů, evidencí a registrací - databází.

Z tohoto pohledu je třeba databáze, evidence a registrace členit na :

- veřejně přístupné;
  jedná se o evidence a registrace, do nichž má ve své podstatě po zaplacení příslušného správního poplatku přístup každý občan;
- neveřejné;
  - sloužící jen pro interní potřebu (např. soukromé katalogy sbírek)
  - důvěrné (např. finanční výkazy)
  - utajovaného charakteru (z hlediska zákona je jejich vytěžování zakázáno).

Zpravodajský pracovník (soukromý detektiv zajišťující zpravodajskou činnost) by neměl usilovat o získání informací, které mají charakter utajovaných skutečností, neboť v opačném případě naplňuje skutkovou podstatu trestného činu, a vystavuje se trestnímu stíhání.

V současné době je velmi významným zdrojem informací i ve vztahu k evidencím a registracím internet. Z internetu je možno získat mnoho cenných informací jak o organizacích, institucích, úřadech, podnikatelských subjektech a jejich aktivitách, ale i o fyzických osobách, o věřitelích a dlužnících a další významné informace. Velmi významné jsou tiskové – press zprávy (informace) např. z ANOPRESSU, ČTK, ČEKIA a podobných placených databází. Ty mohou posloužit i jako výchozí informace pro přípravu a realizaci zpravodajské sociotechniky. [1]

2.2.3 Vedení a vyhodnocování zpravodajských databází

Vedení zpravodajských databází, byť by se mohlo zdát jako jednoduchá záležitost, opak je pravdou. Hlavní problém spočívá v tom vyrovnat se s požadavky zákona č. 101/2000 Sb. na ochranu osobních údajů, či se zákonem 412/2005 Sb. o utajovaných skutečnostech.

Pokud se podaří vyrovnat se s uvedenými úskalími zmíněných zákonů, samotné zpracování relevantních informací do počítačových databází je již jednoduché. Existuje celá řada softwarových programů pro tvorbu databází a vyhledávání v nich. [1]

2.2.4 Zpravodajské dokumentování

Zpravodajské dokumentování je metoda zpravodajské činnosti, jejímž cílem je získané informace v procesu zpravodajské činnosti zachovat, zpřístupnit (podávat je ve srozumitelné podobě) a umožnit klientovi je využít pro jím plánované postupy v různých procesech rozhodování, ale i v správních a soudních kauzách. V procesu zpravodajského dokumentování využije zpravodajský pracovník, soukromý detektiv realizující nestátní zpravodajství jako jednu z forem detektivní činnosti, řady obecných i kriminalistických taktických i technických metod.

Písemná dokumentace :

- pořízení fotokopií (zpravidla úředně ověřených) různých dokumentů;
- pořízení nových písemností např. čestná prohlášení (s úředně ověřeným podpisem),
- popisy technických řešení
- znalecké posudky apod.

Fotodokumentace:

- fotodokumentace událostí;
- fotodokumentace jevů;

- fotodokumentace kriminalistických stop;
- fotodokumentace činnosti osob;
- fotodokumentace archiválií apod.

Jedná se o dokumentování významných skutečností a jevů v podobě fotografií, ať již jednotlivých či zpracovaných do fotodokumentace (fotodokumentačních svazků), pro další využití je třeba, aby k fotografiím či foto dokumentačním svazkům byla pořízena legenda obsahující zejména údaje:

- datum a čas pořízení;
- místo pořízení;
- vysvětlení, co fotografie zachycuje;
- kdo pořídil a proč;

U důležité fotodokumentace je vhodné, pokud to charakter postupu dovoluje, uvést svědky události či jevu a svědky vlastního pořízení fotodokumentace. Je vhodné fotodokumentaci v tomto směru doplnit i čestnými prohlášeními svědků.

audio-dokumentace :

Jedná se o pořízení zvukových záznamů na audio-média (magnetofonové pásky, CD, DVD nosiče). Z hlediska dalšího využití je vhodné obsah záznamu nebo alespoň jeho nejdůležitější pasáže zdvojit i písemným záznamem, neboť je již v praxi ověřeno, že některé nosiče (CD, DVD) jsou schopny uchovat záznam jen po dobu několika let (na rozdíl od magnetofonových pásků, které ani po 30-ti letech neztrácí svou audio-záznamovou hodnotu);

video dokumentace:

Jedná se o dokumentování významných skutečností, především dějového charakteru, na filmová či video média. Zejména u zpravodajské dokumentace, i bez návaznosti na jiné metody zpravodajské činnosti, může jít o zpracování různých filmových či video sestřihů významných událostí, skutečností. Rovněž v souvislosti s video (filmovou) dokumentací se doporučuje zpracovat písemné legendy a písemné popisy natočených skutečností, událostí a dějů a doplnit je čestnými prohlášeními, pokud to charakter zpravodajského postupu dovoluje, svědků událostí

či dějů. Video záznam je používán zejména tam, kde světelné podmínky nejsou vhodné pro fotodokumentaci.

věcná dokumentace:

Ve zpravodajské práci, jde zejména o zajištění různých vzorků, prototypů apod. Ale může se jednat i o zajištění předmětů a stop (např. sádrových odlitků, daktyloskopických otisků apod.) pro potřeby dokazování soudních kauzách či ve správních řízeních. Rovněž v těchto případech je vhodné doplnit tyto věcné důkazy a stopy čestnými prohlášeními svědků s úřadně ověřenými podpisy.

To, co je u dokumentací pořizovaných orgány činnými v trestním řízení, ale i v soukromé detektivní činnosti poměrně jednoduché, ve zpravodajské činnosti může být, s ohledem na její konspirativní charakter, značně složité. [1]

2.3 Technologie zpravodajské analýzy informací

Technologie zpravodajských analýz jsou využívány jak při práci s primárními informačními zdroji, tak i při práci se sekundárními informačními zdroji. Představuje nacházení a prezentaci souvislostí současně s využitím špičkových zpravodajských technologií.

- *Vypracování tematických rešerší*: jejich hlavním účelem je rychlé a komplexní zmapování „informačního pole“ kolem osoby, organizace či události se zohledněním důrazu na určitý charakter či kontext informací
- *Vypracování kontextové rešerše*: hlavním účelem kontextových rešerší a monitoringů je vyhodnocení, resp. sledování, informací o určité problematice s důrazem na konkrétní způsob využití těchto informací
- *Vypracování přehledových monitoringů*: Hlavním účelem přehledových monitoringů je:
    - odkrývat souvislosti skryté ve velkém množství dílčích informací a identifikovat signály tvořené trendy, periodicitami, shluky, či absencemi informací

  Tyto signály a souvislosti slouží:
    - pro včasnou reakci na změny představující možné příležitosti a rizika nebo na stav vypovídající o slabých či silných stránkách subjektů ovlivňujících definované cíle a záměry
- *Vypracování analýz*: Hlavním účelem analýz je interpretace (pochopení významu) informací relevantních k určitému definovanému záměru a jejich názorná prezentace v kontextu cílů, klíčových oblastí a úkolů, na nichž je záměr závislý. [1]

2.4 Prostředky nestátního zpravodajství

Z hlediska dokumentování výsledků zpravodajské činnosti a při posuzování některých specifických událostí, situací a okolností je nejen důležité dospět k pozitivnímu či negativnímu výsledku, který je třeba zadokumentovat, a tím uchovat pro další potřeby řešení věci. Dokumentovat je potřebné nejen exaktní výsledky, ale mnohdy i samotnou činnost zpravodajského pracovníka pro průhlednost a kontrolu ze strany klienta. [1]

2.4.1 Kriminalistické prostředky

Pro potřeby sběru a zpracování informací a převodu na relevantní informace - znalost má své zvláštní postavení i kriminalistická technika. Jako kriminalistická technika slouží univerzální prostředky i specializované prostředky, jejichž další výčet je jen příkladný, neboť by se o jejich užití mohla vytvořit samostatná publikace.

Kriminalistickou techniku ve zpravodajské činnosti je možné členit např. podle způsobu užití:

- Pro ohledání místa činu:

  I ve zpravodajské práci se vyskytne potřeba ohledat místo nějaké události, průběhu nějakého jevu, nebo prosté zajištění dokumentů a stop na nich apod.

  - Kufřík kriminalistické techniky:

    Jde zpravidla o kufříky sloužící k zajištění stop, ve zpravodajské práci se poměrně často vyskytne potřeba zajištění daktyloskopických stop (například z různých předmětů jako jsou sklenice apod.)

  - Měřidla:

    Ve zpravodajské práci je mnohdy třeba vypracovat náčrtky, či plánky a je třeba provádět různá měření a zaměření objektů, předmětů apod. K tomu se využívají běžná i speciální měřidla.

  - Rýsovací potřeby apod.:

    Pro vypracování plánků a náčrtků jsou třeba i různé psací a rýsovací potřeby. V poslední době dochází k jejich zpracování na počítačích s využitím různých grafických programů, kterých je celá řada.

- Pro kriminalistické expertízy:
  - Přístroje;

    I v rámci zpravodajské práce je třeba zajistit různé znalecké expertízy, k čemuž slouží různé kriminalistické i běžné přístroje.
  - Přípravky:

    V rámci nestátního zpravodajství při realizaci zpravodajské práce se používají i různé nástrahové prášky a jiné přípravky. Rovněž při provádění kriminalistických expertíz jsou potřebné různé přípravky, především chemické apod. [1]

2.4.2 Detektory

- detektory kovů a výbušnin apod.;

  V procesu zpravodajské činnosti je třeba se přesvědčit, zda na místě zpravodajského zájmu se nenacházejí výbušniny, zbraně a jiné kovové předměty. Je třeba např. použít detektory kovů k vyhledání různých předmětů ukrytých v zemi, ve stěnách apod.

  K tomu se využívá různých ručních detektorů kovu, případně rámových detektorů, které je možné připojit k PC a na něm sledovat podrobnější údaje kontroly. [1]

2.4.3 Prostředky zabezpečující základní činnosti

Jedná se o nejzákladnější prostředky sloužící k vykonávání zpravodajské činnosti.

- Dopravní

  Dopravní prostředky ve zpravodajské práci zaujímají významné místo. Mnohdy z konspirativních důvodů je třeba střídat vozidla různých typů a značek. To samozřejmě v soukromém sektoru – nestátní zpravodajské činnosti - sebou přináší jisté problémy. Řešit se to ale dá např. zapůjčením vozidel v půjčovnách.
- Spojovací [1]

  Spojení ve zpravodajské práci sehrává mimořádnou úlohu, proto se využívá mobilních telefonů, pevných linek popř. vysílaček.

- Počítačová technika a informační technologie
- Kancelářská technika a s ní související prostředky:
  Jedná se o kopírky, skenery, tiskárny k PC, kancelářské vybavení apod. [1]

2.4.4 Audiovizuální prostředky

- Fotoaparáty

  Fotografování je nedílnou součástí zpravodajské činnosti, kde je třeba fotografovat dokumenty, objekty, osoby apod.

- Videokamery

  Zpravodajská činnost často vyžaduje zachycení průběhu různých činností a dějů.

- Audio záznamníky
  Dokumentování rozhovorů a provedení se audio poznámek je také nedílnou součástí zpravodajské práce. [1]

2.4.5 Optické prostředky

- Dalekohledy

  Zpravodajská práce vyžaduje časté pozorování a mnohdy z důvodů utajení, pozorování na větší vzdálenosti.

- Přístroje pro noční vidění
  Zpravodajská činnost se neodehrává jen ve dne, ale i za snížené viditelnosti a také v noci. Jde především o speciální přístroje, většinou noktovizory.
- Lupy [1]

2.4.6 Bezpečnostní prostředky

Nejedná se o prostředky, které bezprostředně souvisejí se zpravodajskou činností, ale též o prostředky zabezpečující práci zpravodajského pracovníka (soukromého detektiva zabezpečujícího zpravodajskou činnost) ve výjimečných případech. Jde například o prostředky využitelné v souladu s § 29 trestního zákona o nutné obraně a § 28 trestního zákona o krajní nouzi. Jde například o prostředky:

- Osobní zbraně, elektrické paralyzéry, obranné spreje, obušky, svítilny, pouta [1]

2.4.7 Speciální prostředky k ochraně informací

- Telefonní a faxové šifrovací prostředky
- Generátory šumu
- Detektory a deaktivátory mobilních telefonů

  Zařízení pro vyhledávání a deaktivaci jak mobilních telefonů, tak elektronických zařízení pro odposlechy. [1]

2.4.8 Speciální zpravodajská technika

Jde o techniku, kterou se soukromou detektivní činností odhaluje, a tak zároveň bráníme zájmy klienta, před únikem relevantních informací. K tomu, aby bylo možno se bránit, tedy rozkrývat zločinnost v tomto směru, je třeba tyto prostředky znát a vědět o nich. Proti těmto prostředkům používaným ze strany konkurence, případně organizovaného zločinu, je třeba se bránit.

- Audiovizuální získávání informací
  - K osobní práci zpravodajského pracovníka

    jedná se o různé kamufly, které zpravodajský pracovník nosí při sobě a používá např. k nahrávání průběhu vytěžování osob. Může jít o zabudované skryté diktafony například v diáři. Může se ale jednat i o skrytý mikrofon s vysílačem a přijímačem, na kterém druhý zpravodajský pracovník kontroluje průběh vytěžování v reálním čase.
  - Další speciální technika

    Může se jednat například o miniaturní kamery s CCD či CMOS čipem, speciální mikrofonové vysílače a přijímače nebo externí hardwarová zařízení pro nahrávání telefonních hovorů [1]

3 OBRANNÉ ZPRAVODAJSTVÍ PŘI ZAJIŠŤOVÁNÍ INFORMAČNÍ BEZPEČNOSTI

První a nezastupitelnou zásadou, prvořadým požadavkem, základním atributem každého zpravodajství je zabezpečení komplexní ochrany vlastní organizace, instituce či podniku (společnosti, firmy). Bez zabezpečení vlastní ochrany organizace, instituce či podnikatelského subjektu nemohou být účinná ani opatření ofenzivního či vlivového zpravodajství. Obranné zpravodajství je nutno v rámci detektivní - zpravodajské ochrany realizovat i tam, kde nejsou realizována další opatření ofenzivního či vlivového zpravodajství. Nerespektování této zásady může způsobit, a zpravidla také dříve či později způsobí dané organizaci vážné problémy. [1]

Cíle obranného zpravodajství

- zabránit kontaktování a vytěžování zaměstnanců organizace, instituce či podnikatelského subjektu ze strany konkurence;
- zabránit případům fingovaným zaměstnáním zaměstnanců konkurence ve vlastní organizaci, instituci, či vlastním podnikatelském subjektu (vysílání zaměstnanců – zpravidla pracovníků útvarů ofenzivního či vlivového zpravodajství konkurence nebo pracovníků zpravodajství na smluvním základě – komerčních zpravodajských pracovníků) do organizace, instituce či podnikatelského subjektu - útok konkurence).
- zabránit získání informací konkurencí za využití korupce;
- zabránit získávání informací konkurencí formou vydírání apod.
- zabránit přímé krádeži počítačových nosičů informací nebo jejich nelegálnímu kopírování;
- zabránit technickému získávání informací z počítačových sítí;
- zabránit speciálními technickými prostředky (šumové generátory) odposlechům
- zabránit odposlouchávání a sledování nelegálními prostředky
- zabránit narušení vlastnických práv (vloupání za účelem krádeže informačních nosičů)
- zabránit získávání informací o útvarech konkurence, zabývajících se konkurenčním zpravodajstvím

- zabránit dezinformacím a působení vlivového zpravodajství konkurence

3.1 Oblasti obranného zpravodajství

- Personální bezpečnost :
  jedná se o ochranu informačních systémů z hlediska jednání a konkrétních událostí způsobených pracovníky, a to především z pohledu prevence. Personální bezpečnost musí být zajišťována jednak detektivními prověrkami budoucích (potencionálních) zaměstnanců podniku (společnosti, firmy, instituce, organizace apod.), jednak periodickými detektivními prověrkami stávajících zaměstnanců podniku.
- Režimová bezpečnost:
  jde o vytvoření bezpečnostních pravidel z hlediska zásad práce s informacemi, daty, komunikačními a počítačovými systémy. Jde o významný prvek prevence. Nestačí pouze existence pravidel, ale je zde nutnost kontroly jejich dodržování;
  Zahrnuje:
  - režim práce s písemnostmi;
  - režim ukládání datových médií;
  - vymezení okruhu osob pro práci s výběrovými, důvěrnými a utajovanými informacemi a daty;
  - opatření pro případ mimořádných událostí apod.
- Informační bezpečnost - bezpečnost dat a datových souborů:
  předpokládá ochranu dat v souborech a databázích, ať již elektronických či písemných, ochrana proti chybám a virům, zvláštní ochrana citlivých dat, autorizace a rozlišení přístupů k datům a databázím.

- Bezpečnost technických prostředků:
  jde o jejich výběr a spolehlivost, kontrolu přístupu k těmto prostředkům, ochranu před elektromagnetickým zářením a elektrostatickou elektřinou apod.

- Bezpečnost programových (softwarových) prostředků:
  je třeba, aby byla zajištěna kontrola přístupu k nim, autentičnost a identifikace uživatele, rozdělení pravomocí mezi uživateli, výběr a spolehlivost programů apod.;

Bezpečnost programových (softwarových) prostředků spočívá:

- v ochraně proti virům;
- v obraně proti zneužití programového vybavení (softwarového vybavení);
- v ochraně proti zničení či poškození softwarových (programových) vybavení.

- Bezpečnost komunikačních systémů a cest:
  představuje především ochranu mezi jednotlivými částmi komunikačních a počítačových systémů atd.;

- Fyzická bezpečnost:
  jde o ochranu informací, dat, komunikačních a počítačových systémů proti neoprávněnému přístupu k nim, proti protiprávnímu vniknutí do prostor, kde se nachází atd.

- Aktivní ochrana proti úniku informací a dat:
  proti podnikové či firemní špionáži = proti aktivnímu (soutěživému či konkurenčnímu zpravodajství): Jde o systém opatření směřujících k získání informací o aktivitách konkurenčních útvarů (agentur) zabývajících se konkurenčním (soutěživým) zpravodajstvím (informační pronikání do takovýchto útvarů či agentur). [1]

3.2 Ochrana informací

Základem udržení informačních a s tím úzce spojených i konkurenčních výhod, je nutnost patřičného zabezpečení vlastních informací a jejich komunikačních cest (informační databáze, komunikační, počítačové a informační systémy), před jejich zcizením, zneužitím, ale také jejich pozměněním. Nejedná se pouze o informace v elektronické podobě, jak by se mohlo na první pohled zdát, ale také o informace v papírové formě a také o znalosti zaměstnanců.

V současné době informačního rozkvětu mají informace velký význam v mnoha oblastech, především ale v oblasti ekonomické. Je tedy nutné vědět, že ochrana informací se netýká jen státu a jeho součástí, ale také firem, institucí a v neposlední řadě i běžných lidí.

Pokud bychom chtěli porovnávat informace, jako nehmotný majetek s majetkem hmotným, zjistíme, že pro nás mají informace mnohdy větší cenu než věci hmotné, je to dáno především tím, že ztráta (případně vyzrazení nebo zneužití) informací oproti ztrátě hmotného majetku, je často nenahraditelná. Ochranu informací můžeme tedy zařadit mezi klíčové aspekty dlouhodobého úspěchu organizace. Některé dnešní zákony dokonce nařizují, jak určité informace mají být chráněny (zák. o ochraně osobních údajů, zák. o utajovaných informacích apod.).

3.2.1 Informace, které je třeba chránit

Obchodní tajemství

Informace o provozech a provozních činnostech, technologiích know-how, obchodních aktivitách a podobně jsou ze strany konkurence velice žádanými informacemi. Jsou cenným zbožím, neboť mají vysokou užitnou, a tím i směnnou hodnotu. Zájmem každé organizace (každého subjektu, instituce, firmy, společnosti) by mělo být tyto informace – znalosti chránit jako významný majetek. Právní řád České republiky umožňuje chránit hmotný a nehmotný majetek před škodlivými útoky, které mohou mít formu rozkrádání, poškození, zkreslení, zneužití, ztráty nebo zničení. Ochranu upravuje jednak Obchodní zákoník, zákoník práce i trestní zákon (např. nekalá soutěž, zneužití informací v obchodním styku apod.)

Je také třeba, aby bylo obchodní tajemství upraveno v interních normách, a to:

- definováno a zajištěno jeho utajení (přijetím organizačních, režimových a technických opatření k zajištění ochrany)
- Sankcionováno porušení těchto interních norem podle pracovně-právních předpisů, zajištěn závazek mlčenlivosti zaměstnanců a odpovědnosti za škodu dle pracovně-právních předpisů a upozornění na možnost trestního stíhání případných pachatelů. Tento závazek, tj. odpovědnost za škodu a smluvní sankci při vyzrazení obchodního tajemství jinými subjekty (například obchodními partnery) je nutné formulovat v obchodní smlouvě.

Zvláštní skutečnosti

Institut „zvláštních skutečností“ zavedl do právního systému české republiky zákon č. 240/2000 sb., o krizovém řízení a změně některých zákonů (tzv. krizový zákon), a to v ustanovení § 27 zákona. K provádění činností v souvislosti s ochranou zvláštních skutečností zejména v oblasti personální a administrativní bezpečnosti, vydala Vláda ČR Nařízení vlády č. 462/2000 Sb., k provedení ustanovení § 27 odst. 8 a § 28 odst. 5 krizového zákona.

Zákon stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávných celků a práva a povinnosti právnických a fyzických osob při přípravě na krizové situace (mimořádné události). Z krizového zákona vyplývá, že organizace, u které se vyskytují písemnosti obsahující „zvláštní skutečnosti“ v oblasti krizového řízení (tj. listiny, nosná média a jiné materiály, které je obsahují) musí být stanoveným způsobem označeny a musí být dodržován zákonem požadovaný režim manipulace s nimi. Zvláštní skutečnosti jsou informace z oblasti krizového řízení, které by v případě zneužití mohly vést k ohrožení života, zdraví, majetku, životního prostředí nebo podnikatelských zájmů právnických osob nebo fyzických osob vykonávajících podnikatelskou činnost podle zvláštních právních předpisů (viz § 2 krizového zákona). Pracovníci organizace, kteří jsou oprávněni se seznamovat se zvláštními skutečnostmi, musí být zapsáni ve zvláštním seznamu, který schvaluje vedoucí zaměstnanec orgánu krizového řízení. Povinnost mlčenlivosti je stanovena všem, kteří jsou oprávněni se seznamovat se zvláštními skutečnostmi a všem osobám, které se s nimi seznámily při plnění úkolů krizového řízení.

V případě ochrany zvláštních skutečností je organizace povinna provést opatření požadovaná zákonem č. 240/2000 Sb., o krizovém řízení a dalšími normami, které zákon rozpracovávají, zejména pak Nařízením vlády č. 462/2000 Sb., a to vždy po projednání s příslušným orgánem krizového řízení.

Ochrana osobních a citlivých osobních údajů v organizacích nemá význam pouze pro občana (zaměstnance), kterého se týkají, ale mají obrovský význam z hlediska celkové i informační bezpečnosti organizace. Je třeba si uvědomit, že z hlediska celkové bezpečnosti a informační bezpečnosti zvláště je nejrizikovějším faktorem právě lidský faktor. Zajištění personální bezpečnosti se bezprostředně dotýká zajištění i ostatních bezpečnostních okruhů. Únik osobních údajů, zvláště pak citlivých osobních údajů, může posloužit konkurenci ke zneužití formou vydírání, korupce apod.

Osobní údaje a citlivé osobní údaje

Výchozím dokumentem upravující oblast ochrany informací obsahující osobní údaje je ústavní zákon č. 23/1991 Sb. ze dne 9. ledna 1991, kterým se uvozuje Listina základních práv a svobod. Do nedávné doby poskytoval ochranu osobních údajů zákon č.256/1992 Sb., o ochraně osobních údajů v informačních systémech, který byl zrušena nahrazen zákonem č. 101 /2000 Sb. o ochraně osobních údajů a o změně některých zákonů ze dne 4. dubna 2000 (od 1. června 2000 je zákon účinný). Ochrana osobních údajů je součástí evropské úmluvy o lidských právech a základních svobodách. Smyslem zákona je dosáhnout toho, aby se s osobními údaji občanů nakládalo jen podle stanovených pravidel, která odpovídají standardům Evropské unie. Zákon je v souladu s direktivou EU a Úmluvou Rady Evropy**.**

Tento okruh chráněných informací se tedy opírá o zákon 101/2000 Sb. – o ochraně osobních údajů. Ochrana osobních údajů je běžnou součástí života moderní demokratické společnosti. Ten, kdo má být chráněn, je jednotlivec, tj. fyzická osoba, o níž osobní údaje vypovídají. Tím, kdo má osobní údaje chránit je každý, kdo osobní údaje zjišťuje, zpracovává, případně uchovává a sděluje jiným subjektům.

Utajované informace

Zákon č. 412/2005 - Zákon o ochraně utajovaných informací a bezpečnostní způsobilosti. Vzhledem k charakteru činností prováděných organizací a v souvislosti s rozvojem podnikatelských aktivit může vzniknout potřeba požádat NBÚ o prověrku, a tím i nutnost zahájit budování ochranných procedur a opatření ve smyslu požadavků zákona, který utajované informace upravuje. Zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

Zákon vymezuje zejména informace, které je nutno v zájmu České republiky utajovat, a s tím související:

- způsob ochrany těchto skutečností (informací),
- působnost a pravomoc orgánů státu při výkon státní správy v oblasti ochrany utajovaných informací,
- povinnosti orgánů státu, práva a povinnosti fyzických a právnických osob, odpovědnosti za porušení povinností stanovených zákonem

- upravuje postavení Národního bezpečnostního úřadu (NBÚ),
- vytváří předpoklady pro vzájemné poskytování utajovaných informací v rámci Aliance,
- pojetí zákona zabezpečuje přesnou klasifikaci utajovaných informací, jejich ochranu a dispozici s nimi,
- určuje, kdo a za jakých podmínek se s utajovanými informacemi může seznamovat, stanoví takové ochranné mechanismy, které zajišťují na vysoké úrovni jejich bezpečnost. [1]

Utajované informace se člení na:

- přísně tajné
- tajné
- důvěrné
- vyhrazené [7]

Při zabezpečení potřebných informací se často přihlíží jen na technickou stránku zabezpečení, ale velice málo pak na stránku personální, jež bývá mnohdy nejslabším článkem v ochraně informací a nejen jich.

3.2.2 Detektivní zpravodajství při zajišťování informační bezpečnosti

Je nutné podotknout, že této stránce ochrany informační bezpečnosti je z pohledu organizací věnována velmi malá pozornost, při tom je tato oblast (personální bezpečnost) velice riziková. Detektivní zpravodajství v této oblasti působí při výběru a prověrky osob, pracujících s určitým typem informací, to zahrnuje i problematiku řešení otázek jejich odborné přípravy, ochrana těchto osob a také problematiku kontrolních činností spojených s dodržováním stanovených postupů při ochraně informací. Významnou úlohu v této problematice zaujímají prověrky loajality zaměstnanců a manažerů organizací.

Prověrky lze provádět dvěma způsoby a to:

- detektivně-zpravodajskými prověrkami zaměstnanců na významných pozicích a především středního a vyššího managementu.
- prověrky prostřednictvím psychologických auditů v personální sféře. V této souvislosti může významnou měrou přispět fyziodetekce. Ta může přispět k objektivizaci psychologických diagnostických metod a postupů, ale i formou zjišťování pravdomluvnosti s vazbou na loajalitu k organizaci.

Fyziodetekce

Principem fyziodetekce je vyvolávání psychických reakcí kladenými kritickými či nekritickými podněty, tyto reakce jsou zaznamenávány a nakonec je výsledek na základě zaznamenaných hodnot odborně zkoumán a interpretován.

Prostředky pro zkoumání fyziodetekce:

- *Polygraf* – někdy také populárně nazýván jako „detektor lži“. Přístroj zaznamenává několik fyziologických veličin (například krevní tlak, srdeční puls, dýchání, elektrický odpor kůže, velikost zornice oka apod.), když je člověku kladena série otázek. Vychází se z předpokladu, že vědomá lež vyvolá stresovou situaci, která se projeví měřitelnou změnou sledovaných údajů.
- *Analyzátor hlasu* - sleduje odraz průběhu psychické reakce na hlasivkách. Pro detektivní a zpravodajskou činnost je vhodný především tím, že je možno ho použít bez vědomí osoby a stačí pouze na skrytý kvalitní magnetofon (nejlépe digitální) nahrát řízený rozhovor s vytěžovanou osobou a tento záznam vyhodnotit na přístroji analýzy hlasu. I v řízeném rozhovoru jde o to klást kritické a nekritické otázky.
- *Termovize* - sleduje odraz průběhu psychické reakce na změně teploty těla. I termovize je možno použít skrytým způsobem a registrovat odezvy průběhu psychických reakcí na kladené otázky na periferii organizmu v daném případě změny teploty těla. [1]

II. PRAKTICKÁ ČÁST

4 MODELOVÝ PŘÍKLAD OBRANNÉHO ZPRAVODAJSTVÍ

Kapitola modelového praktického příkladu obranného zpravodajství obsahuje fiktivní situaci, na které je ilustrován postup obranného zpravodajství.

4.1 Zadání problému

Společnost A, dříve velice úspěšná s velice dobrými kontrakty, začíná upadat kvůli zakázkám, které jí stále častěji přebírá konkurenční společnost, jež je při nabídkách vždy o něco níže s cenou. Ředitel společnosti A má podezření, že někdo z jeho společnosti vyzrazuje důležité informace o jejich nabídkách konkurenční firmě. Ředitel se tedy rozhodl objednat soukromou detektivní kancelář, zabývající se konkurenčním zpravodajstvím, aby danou situaci prověřila.

V této části je potřeba si uvědomit, co je již známo a co je třeba zjistit, tedy stanovit si klíčové otázky, které by měly být řešeny. Ze zadání víme, že společnost A ztratila a ztrácí zakázky, které jí přebírá konkurenční společnost B. S touto situací je spjato podezření, že někdo ze společnosti A předává konkurenční společnosti důležité informace o nabídkách, tím přichází společnost A o zakázky a tím pádem i o zisky.

4.2 Profil společnosti A

Název společnosti:	*společnost A*
Hlavní management společnosti:	*jména....*
Dodavatelé:	…
Spolupracující firmy:	…
Konkurenční společnosti:	*společnost B*

4.3 Stanovení cílů a vytvoření plánu

Než se začnou zjišťovat a zpracovávat informace je zapotřebí si nejprve uvědomit, čeho je potřeba dosáhnout a formulovat tak cíle. V nastíněné situaci je požadováno ředitelem společnosti A prošetřit úniky informací ke konkurenční společnosti B. Cílem tedy bude stanovit kudy, případně kým, jsou informace o zakázkách předávány společnosti B.

Společnost A si již nechala provést testy bezpečnosti jejich informačních systémů a ty ukázaly, že jejich systémy jsou poměrně dobře zabezpečeny a bylo by poměrně náročné tímto způsobem informace o zakázkách zjistit. Z toho vyplývá, že s největší pravděpodobností bude problém v personálu společnosti A. Nevyhnutelně nutné bude prověřit personál společnosti A a najít kdo a proč informace předává konkurenční společnosti B.

Před samotným získáváním informací je ale ještě potřeba si stanovit způsob, jakým budou informace získávány, zda budou získávány skrytě, bez vědomí vytipovaných osob či otevřeně, s jejich vědomím o šetření. Pro případný další postup a využití např. dezinformace, bude vhodnější postup pomocí skrytého šetření. Skryté šetření události má také výhodu tak, aby případně nedošlo k podezření z řad zaměstnanců, zejména vytipovaných osob, že se něco vyšetřuje a aby se tak zamezilo případnému zastírání ze strany šetřených zaměstnanců.

4.4 Sběr informací

Sběr informací je jedna z hlavních činností zpravodajského pracovníka. Nejjednodušším a nejméně rizikovým způsobem získávání informací je bezpochyby z otevřených neboli sekundárních zdrojů, ty by se měly maximálně využít. Na mysli zpravodajského pracovníka by však mělo být, že všechny takto získané informace nemusí být zcela pravdivé a proto je nutné rozlišovat jejich věrohodnost. Informace z primárních zdrojů, tedy takové informace, které nejsou běžně dostupné a je potřeba je získávat speciálními zpravodajskými postupy. Informace nabývané touto cestou jsou však velmi cenné díky jejich obtížnému získávání.

4.4.1 Vyhodnocení okruhu osob s přístupem k patřičným informacím

V této části bude věnována pozornost okruhu zaměstnanců společnosti A, kteří mají přístupu k informacím, které unikají z jejich společnosti. Přesněji řečeno, zjistit kdo má k těmto informacím přístup. Seznam okruhu osob s přístupem k požadovaným informacím by měl být vyhodnocen společně s ředitelem společnosti A, který má k těmto údajům přístup. V opačném případě by bylo potřeba tyto informace opatřit jinou, pracnější, cestou.

Bude třeba projít zápisy z jednání o kontraktech a prověřit, kdo všechno se mohl k těmto dostat. Velkým usnadněním by byl např. výpis všech přístupů do prostor, kde se cílené údaje nacházely, pokud takovým systémem společnost disponuje.

Pro další zúžení vytipovaného okruhu osob může napomoct fakt, že někteří zaměstnanci se mohou cítit nedoceněni nebo nespokojení a tak mohou být motivováni „přivýdělkem“ nebo tzv. satisfakcí vůči společnosti A.

Fáze vyhodnocování okruhu lidí může zahrnovat různé zpravodajské metody, např. zpravodajské vytěžování databází, zpravodajské hypotézy, zpravodajské analýzy…

4.4.2 Šetření kolem vytipovaných osob

Při šetření se musí vycházet ze stanovených cílů a podle toho také využívat vhodné zpravodajské metody. Jak již bylo zmíněno, postupovat se bude skrytě, tak aby nedošlo k případnému zastírání ze strany zaměstnanců. Během prověřování by měl být kladen důraz i na různé drobnosti, které mohou šetření posunout dále nebo lecos napovědět. Například prověření firemní komunikace, jako je firemní elektronická pošta nebo výpis telefonních hovorů, může poskytnout užitečné informace.

Nemusí však být dostačující sbírat informace pouze o společnosti A, ale je třeba se zaměřit i na konkurenční společnost, která společnosti A zakázky přebírá a zjistit potřebné informace o ní. Důležitými údaji budou jména vedení společnosti, ale i běžní zaměstnanci a spolupracující společnosti. To může pomoct při vytváření souvislostí mezi získanými informacemi.

Jako účinná metoda se v tomto případě jeví metoda zpravodajského pozorování (monitoring). Monitoring vytipovaným osob může přinést důležité informace o pohybu, jednání, ale hlavně o tom, s kým se šetřené osoby stýkají.

Monitoring by měl probíhat ve fázích:

- **příprava** zpravodajského pozorování – sledování
  To zahrnuje zejména rekognoskaci terénu, ve kterém má být osoba monitorována, popř. převzata k monitorování;

- **vlastní realizace** pozorování
  Představuje zajištění utajení, možnosti bezprostředního kontaktu a kontroly nad jednáním osoby, pořizování dokumentace;

- **shromáždění a třídění poznatků** – informací získaných v průběhu monitorování, Jedná se o zpracování pořízených audio, video a foto záznamů;

- **doplnění neúplných informací** o údaje z jiných zdrojů;

- **analýza a interpretace informací** a jejich využití v rámci jiných metod a forem soukromé detektivní činnosti;

- **zpracování zprávy a dokumentace** pro klienta.

S touto metodou jsou úzce spjaty další zpravodajské metody a to zpravodajská rekognoskace, zpravodajské dokumentování, zpravodajské vytěžování dokumentů atd.

4.5 Analýza získaných informací

Analýza informací má důležitou pozici ve zpravodajském systému. Analýza se různě prolíná více zpravodajskými fázemi. Jejím cílem je zjišťování smyslu získaných informací v daném kontextu se zadáním úkolu.

Získané informace je nutné také zhodnotit, podle toho z jakého pocházejí zdroje, jestli jim je možné zcela důvěřovat, či je jejich pravost pochybná.

4.6 Výsledek šetření

Výsledky vychází z důkladného prověření získaných informací. Jsou formulovány na úroveň vhodnou pro cílového uživatele, tak aby byl jasně zřejmý výsledek šetření a neobsahovaly tak zbytečné a příliš odborné údaje, kterým uživatel nemusí rozumět.

Zpravodajským pozorováním bylo zjištěno, že jeden zaměstnanec, ze stanoveného okruhu s přístupem k problémovým informacím, se stýká se zaměstnancem konkurenční společnosti B. Bylo navrhnuto vypracování dezinformačního materiálu společně s ředitelem společnosti A, vedoucí k ověření úniku informací skrz zaměstnance stýkajícího se s konkurencí.

4.7 Příprava dezinformačního plánu

Vytvoření dezinformačního materiálu kontraktu proběhlo v součinnosti zpravodajského pracovníka s ředitelem společnosti A. Dezinformační materiál byl vytvořen na základě již známých informací, na které bylo navázáno nepravdivými, ale těžce ověřitelnými, informacemi. Tento materiál byl vytvořen jako fiktivní nabídka ke kontraktu se společností C.

4.8 Monitoring působení dezinformačního plánu na konkurenční společnosti

Po vytvoření a uvedení dezinformačního plánu v činnost je monitorováno dění konkurenční společnosti B. Zkoumá se působení dezinformačního plánu. V případě, že dezinformace nesplní cíle, je třeba provést korekci a dezinformační cyklus provést znovu.

ZÁVĚR

Bakalářská práce je zaměřena na využití detektivních činností v oblasti nestátního zpravodajství. V úvodní kapitole jsou nastíněny některé důležité právní aspekty týkající se soukromé detektivní činnosti. Dále v téže kapitole je řešena problematika nestátního zpravodajství, které je členěno na ofenzivní, defenzivní (obranné) a vlivové zpravodajství, k jejichž naplňování slouží detektivní zpravodajství, jež je zde také popsáno.

Druhá kapitola práce je věnována zpravodajským technologiím, což je velice široká oblast. Mezi zpravodajské technologie jsou zařazeny technologie primárních informačních zdrojů, při nichž je využíváno speciálních metod k získávání informací, mezi které patří např. zpravodajský monitoring, zpravodajské informační proniknutí, zpravodajské vytěžování osob apod. Další využívanou zpravodajskou technologií jsou sekundární informační zdroje nebo také otevřené zdroje, tyto zdroje obvykle nevyžadují speciální postupy a informace z nich jsou většinou volně dostupné. Zvlášť jsou zařazeny zpravodajské analýzy, jež protkávají jak primární, tak i sekundární zpravodajské informační zdroje. Kapitolu zpravodajských technologií uzavírají technické prostředky užívané v této oblasti, v této části je uveden stručný přehled prostředků seřazených podle jejich typu.

Kapitola třetí popisuje využití obranného zpravodajství k ochraně informací. Ochrana informací je velmi široká problematika a kumuluje několik rovin bezpečnosti. S ochranou informací je úzce spjata bezpečnost know-how a taktéž i personální bezpečnost.

Práci zakončuje v praktické části modelový příklad fiktivní situace obranného zpravodajství. V situaci je nastíněn možný zpravodajský postup při jejím řešení. Řešení situace se skládá ze zadání problému, stanovení cílů, sběru informací, analýzy informací a dezinformace.

CONCLUSION

The thesis is focused on the use of detective activities in non-state intelligence. The introductory chapter is outlines some important law aspects relating to private detective activity. In the same chapter dealt with the issue of non-state intelligence, which is divided into offensive, defensive and lobby intelligence, detective intelligence is their implementation.

The second chapter is devoted to technology of intelligence which is a very wide area. Among technologies of intelligence are included the primary resources of information technologies, this resources are used of special methods for obtaining information, eg intelligence monitoring, intelligence penetration, intelligence mining of persons etc. Other used of intelligence technologies are secondary information resources or they also known as open resources, they not require special procedure and information from them are freely available. Intelligence analysis are classified like separate technologies, which penetrate both – technologies of primary resources and technologies of secondary resources too. Chapter of intelligence technologies conclude the technical instruments, used in this area, this part provides a brief overview of instruments sorted by their type.

The third chapter describes the use of defense intelligence to information protection. Information protection is very wide broad, which cumulated several layers of security. Information protection is closely linked with know-how protection and also personnel security.

The work concludes model example of defensive intelligence of fictional situation, in practical part. Situation is outlined a possible intelligence procedure for their solution. Solving of the situation is consists setting of problem, determination of goals, collection of information, information analysis and disinformation.

SEZNAM POUŽITÉ LITERATURY

[1] BRABEC, František. *Technologie detektivních činností*. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 160 s. ISBN 978-80-7318-780-4

[2] KAMENÍK, Jiří; BRABEC, František. *Komerční bezpečnost : soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. Vyd. 1. Praha : ASPI, 2007. 338 s. ISBN 978-80-7357-309-6

[3] BRABEC, František. *Bezpečnost pro firmu, úřad, občana*. Praha : Public History, 2001. 400 s. ISBN 80-86445-04-6

[4] BRABEC, František. *Soukromé detektivní služby*. 1. vyd. Praha : Eurounion, 1995. 19963 s. ISBN 80-85858-16-9

[5] LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie*. 1. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 223 s. ISBN 978-80-7318-762-0

[6] *Systemonline.cz* [online] 2005 [cit. 2011-04-14]. Dostupné z www: <http://www.systemonline.cz/clanky/reseni-informacni-bezpecnosti-1-cast.htm>

[7] *Národní bezpečnostní úřad* [online] 2011 [cit. 2011-04-20]. Dostupné z www: <http://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost/obecne-k-personalni-bezpecnosti/>

[8] *INFORUM* [online] 2001 [cit. 2011-04-25]. Dostupné z www: <http://www.inforum.cz/archiv/inforum2001/prispevky/vejlupek.htm>

[9] *Česká komora detektivních služeb* [online] 2011 [cit. 2011-04-2]. Dostupné z www: <http://www.ckds.cz/index.php?lid=CZ&nid=3729&oid=458863>

[10] *Bussiness.center.cz: Zákon č. 2/1993 Sb. - Listina základních práv a svobod* [online] 2011 [cit. 2011-04-20]. Dostupné z www: <http://business.center.cz/business/pravo/zakony/listina-zakladnich-prav-a-svobod/>

[11] *Bussiness.center.cz: Zákon č. 40/1964 Sb., občanský zákoník* [online] 2011 [cit. 2011-04-20]. Dostupné z www: <http://business.center.cz/business/pravo/zakony/obcanzak/>

[12] *Bussiness.center.cz: Zákon č. 99/1963 Sb., občanský soudní řád* [online] 2011 [cit. 2011-04-20]. Dostupné z www: <http://business.center.cz/business/pravo/zakony/osr/>

[13] *Bussiness.center.cz: Zákon č. 40/2009 Sb., trestní zákoník* [online] 2011 [cit. 2011-04-20]. Dostupné z www: <http://business.center.cz/business/pravo/zakony/trestni-zakonik/>

[14] *Bussiness.center.cz: Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)* [online] 2011 [cit. 2011-04-20]. Dostupné z www: <http://business.center.cz/business/pravo/zakony/trestni_rad/>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CD Kompaktní disk

DVD Digitální videodisk

PC Osobní počítač

CCD Elektronická součástka pro snímání obrazové informace

CMOS Elektronická součástka pro snímání obrazové informace

SEZNAM OBRÁZKŮ