Komerční zpravodajství jako aktivní prostředek ochrany know-how

Copmetitive intelligence as active form of know-how protection

Tomáš Banský

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tomáš BANSKÝ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Komerční zpravodajství jako aktivní prostředek ochrany know-how**

Zásady pro vypracování:

1. **Zpracujte manuál pro managery PKB k metodě využití konkurenčního zpravodajství v boji proti krádežím know-how.**
2. **Pojem a metody KS.**
3. **Formy a metody práce soukr.detektiva na úseku konkurenčního zpravodajství.**
4. **Využití možností Živnostenského zákona.**
5. **Ofenzívní postupy v ochraně know-how.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JUDr. Laucký, V., Technologie komerční bezpečnosti I. Zlín: Univerzita TomášeBati, 2010, 81 s., ISBN 978-80-7318-889-4**
2. **JUDr. Laucký, V., Technologie komerční bezpečnosti II. Zlín: Univerzita Tomáše Bati, 2004, 122str., ISBN 80-7318-231-9**
3. **Hurta, Josef,. Management bezpečnostního inženýrství /. Vyd. 1. Zlín : Univerzita Tomáše Bati, 2006. 172 s. : ISBN 80-7318-412-5 (brož.).**
4. **Kameník, Jiří,. Komerční bezpečnost : soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur /. Vyd. 1. Praha : ASPI, 2007. 338 s. : ISBN 978-80-7357-309-6 (brož.).**
5. **Laucký, Vladimír,. Speciální bezpečnostní technologie /. 1. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 223 s. : ISBN 978-80-7318-762-0 (brož.).**
6. **Brabec, František. Soukromé detektivní služby /. 1. vyd. Praha : EUROUNION, 1995. ISBN 8085858169.**

Vedoucí bakalářské práce: **JUDr. Vladimír Laucký**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Bakalárska práca sa zaoberá komplexným problémom komerčného respektíve konkurenčného spravodajstva s hlavným zameraním na defenzívne konkurenčné spravodajstvo, ochranu know-how ,obchodného tajomstva a citlivých údajov. Cieľom práce bolo vytvoriť manuál určený pre manažérov priemyslu komerčnej bezpečnosti o využívaní konkurenčného spravodajstva pre ochranu know-how.

V teoretickej časti sú za týmto účelom spracované dôležité pojmy, metódy a formy využívané pri komerčnom spravodajstve.

V praktická časť je zameraná na skompletovanie postupov pri komerčnom spravodajstve so zameraním na ochranu know-how ale i popísanie ofenzívneho spravodajstva vzhľadom k lepšiemu pochopeniu akým formám musí defenzívne spravodajstvo čeliť. Praktická časť taktiež poskytuje základný prehľad spravodajskej techniky ako i protiopatrenia oproti nej.

Kľúčové slová: Know-how, obchodné tajomstvo, komerčné spravodajstvo, defenzívne spravodajstvo, spravodajská technika.

ABSTRACT

The bachelor work is dealing with komplex problem of commercial or compmetitive intelligence mainly aimed on defensive copmpetitive inteligence, know-how, bussines secret and crucial informations protection. Main task of this work was develop manual for commercial security managers about using commercial inteligence for know-how protection.

In theoretical party are for this purpose processed methods, techniques and important concepts in commercial intelligence problematics.

Practical part is focused on completation of commercial intelligence methods aimed on know-how protection, but also on inscription of offensive intelligence in case of better understanding of defensive intelligence problems. Practical part also presents brief look on survey intelligence technology and counter measures against it.

Keywords: Know-how, bussines secret, commercial intelligence, defensive intelligence, survey technology.

Rád by som poďakoval vedúcemu bakalárskej práce pánovi Judr. Vladimírovi Lauckému za poskytnuté materíaly a potrebné konzultácie pri zpracovaní tejto bakalárskej práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Snaha o zistenie informácií o výrobe a fungovania konkurencie je stará ako obchodovanie samo. Už v dávnej histórii sa obchodníci snažili o získanie kritických informácií konkurencie aby si zaistili konkurenčnú výhodu nad inými obchodníkmi.

Od polovice 20 storočia môžeme hovoriť o presune metód spravodajskej činnosti z rúk štátnych spravodajských služieb do komerčného sektoru a o začiatku formovania komerčného spravodajstva tak ako ho poznáme dnes.

Moderný ekonomický a podnikateľský trh je preplnený agresívnou konkurenciou a rýchlymi zmenami trendov a technológií. Kvôli snahe o maximalizáciu zisku sa spoločnosti snažia akýmkoľvek spôsobom získať nad svojou konkurenciou výhodu. Jednou z najlepších a najnebezpečnejších foriem boja s konkurenciu sa stala práca s informáciami a znalosťami. Tomuto trendu napomáha i extrémne rýchly rozvoj na poli informačných technológií a stále rýchlejšia výmena informácií. Takéto vedomosti môže využiť manažment firmy k vylepšovaniu svojich stávajúcich produktov a služieb alebo k aktívnemu oslabovaniu, destabilizácii alebo dokonca ničeniu svojej konkurencie.

Tieto trendy mali pozitívny vplyv na vývoj komerčného spravodajstva a dali vzniknúť pojmom ako sú Competitive intelligence, bussines inteligence a pod. Všetky podnikateľské subjekty už dnes chápu cenu informácie. Komerčné spravodajstvo sa stalo bežnou súčasťou podnikateľského sektoru či už za účelom získavania informácií (ofenzívne spravodajstvo) alebo vlastnej obrany firmy (defenzívne spravodajstvo).

Táto bakalárska práca je zameraná na objasnenie pojmov komerčného spravodajstva a o zostavenie manuálu pre manažérov priemyslu komerčnej bezpečnosti v rámci ochrany know-how, obchodného tajomstva a citlivých údajov spoločnosti.

I. TEORETICKÁ ČASŤ

1 ÚVOD DO PROBLEMATIKY

1.1 Know-how a jeho zákonná úprava

Obchodný zákonník ČR upravuje pojem know-how nepriamo a to v § 17 obchodného zákonníku, konkrétne v rámci právnej úpravy obchodného tajomstva. Obchodné tajomstvo tvorí všetky skutočnosti obchodnej, výrobnej či technickej povahy súvisiacej s podnikom, ktoré majú skutočnú alebo aspoň potencionálnu materiálnu či nemateriálnu hodnotu. Tieto skutočnosti sú v príslušných obchodných kruhoch nedostupné a podnikateľ by mal podľa svojej vôle dané skutočnosti utajiť a odpovedajúcim spôsobom toto utajenie chrániť. V právnej sfére ČR nie je know-how ako už bolo spomínané vyššie priamo definované na rozdiel od SR kde je tento pojem definovaný v zákone č. 188/1994 Zb., o ochrane hospodárskej súťaže kde je uvedené že know-how sú výrobno-technické , obchodné skúsenosti. Preto je v právnej praxi ČR interpretácia toho čo know-how je a čo nie značne komplikovanejšia. Pojmy obchodného tajomstva a know-how nie je možné medzi sebou zamieňať, pretože sa nejedná o identické pojmy. Obchodné tajomstvo je totižto osobitým inštitútom obchodného práva, pričom know-how je jeho možným predmetom. Know-how môže existovať samostatne bez toho aby bolo súčasťou obchodného tajomstva a taktiež môže byť majetkom fyzickej alebo právnickej osoby v zmysle §2 Obch. Z. Vymedzenie pojmu know-how vzhľadom k vynálezom, priemyselným zdrojom a zlepšovacím návrhom môžeme povedať, že vynálezy ktoré sú predmetom špeciálnej ochrany v zmysle zákona č. 527/1990 Sb., i vynálezoch a zlepšovacích nápadoch môžeme v právnom zmysle považovať za know-how. Táto definícia však platí len na vynálezy, ktoré sú chránené patentom.

1.2 Komerčné spravodajstvo

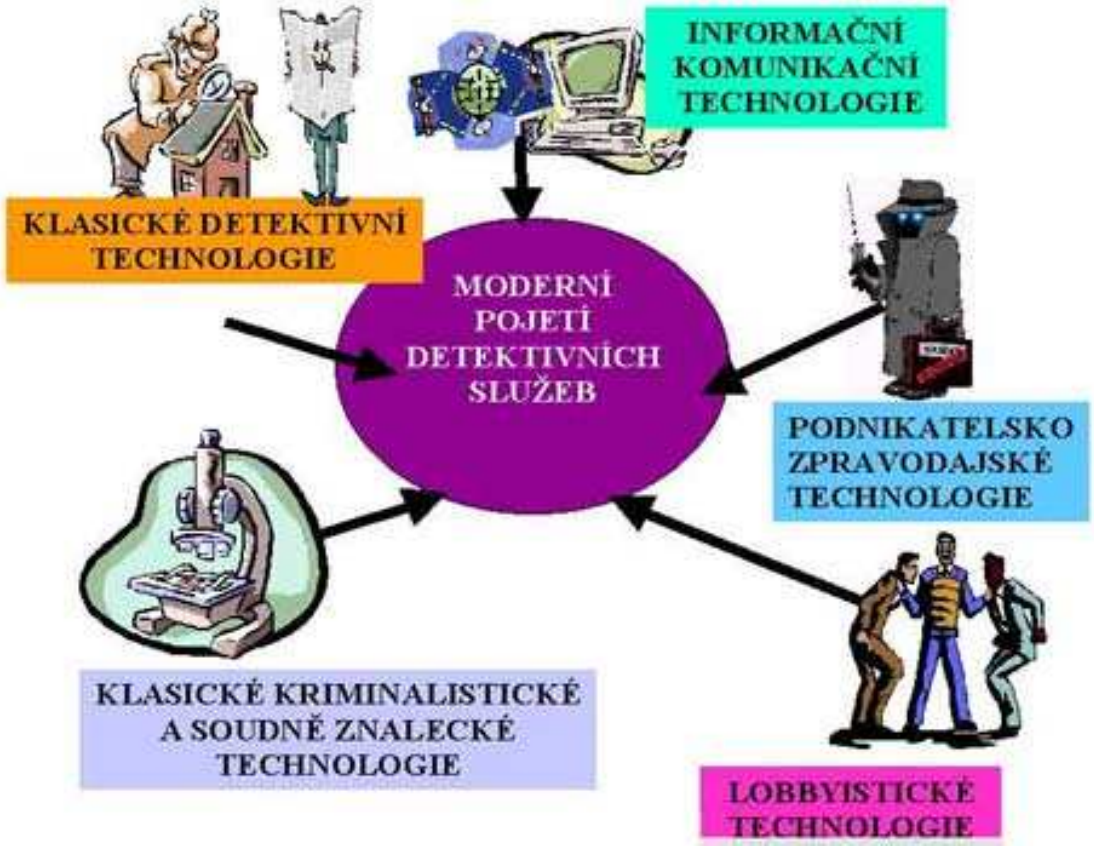
Komerčné spravodajstvo predstavuje realizáciu vedomého a systematického uplatňovania práce z informáciami a proces ich premeny v znalosť a to mimo rámec štátnych orgánov a inštitúcií. Ide vlastne o získavanie , spracovávanie a využívanie relevantných informácií pre potreby ochrany, rozhodovania a presadzovania spoločenských, politických a ekonomických záujmov, procesov a aktivít. Spravodajstvo bývalo vždy doménou hlavne štátnych tajných služieb, informačných služieb, špionáže, kontrašpionáže a pod. Ale na poli moderného podnikateľského trhu sa spravodajstvo stále viac presúva do komerčného sektoru. Pod pojmom komerčného spravodajstva rozumieme produkty a služby ktoré sú

potrebné k zaisteniu funkčného procesu spravodajskej činnosti v komerčnom sektore. Tento proces sa v dnešnej dobe nezaobíde bez znalosti veľkého množstva rôznych oborov hlavne v oblasti informačných technológií, kriminalistiky, detektívnej praxe , psychológie , práva a manažmentu.

Formy komerčného spravodajstva :

- Spravodajský servis – tento druh spravodajskej činnosti prevádzkujú firmy, organizácie atd. sami a pre vlastnú potrebu
- Komerčné spravodajstvo - jedná sa o činnosť špecializovaných organizácií, kancelárií, agentúr apod. Ktoré túto formu spravodajské činnosti zabezpečujú zmluvne na komerčnom základe.

Obe tieto formy komerčného spravodajstva reagujú na konkrétny dopyt trhu a smerujú k získaniu záujmových informácií a spracovaniu záujmových informácií na znalosť. Klientmi , zadávateľmi alebo zákazníkmi pri tom môžu byť : občania, organizácie, inštitúcie, občianske a profesné združenia, politické strany a hnutia, podnikateľské subjekty a pod.



Obr. 1 Moderní pojetí D.S.

1.3 Spravodajstvo

Spravodajstvo predstavuje je súhrn technológií (formy, metódy a prostriedky) a schopnosť vyhľadávania, spracovania a distribúcie znalostí a poznaní. Súhrn relevantných informácií k záujmovému problému predstavuje znalosť. Súhrn znalostí v širších súvislostiach predstavuje poznanie. Hlavnou úlohou spravodajstva je spracovanie dát a informácií do podoby relevantných informácií vo vzťahu k riešenému problému a teda vytvoriť znalosť. Súhrn znalostí a ich usporiadanie do súvislostí vytvorí poznanie . Prezentovanie poznania klientovi v zrozumiteľnej forme je vlastne produktom komerčného spravodajstva.

Spravodajstvo sa realizuje v nasledujúcich krokoch :

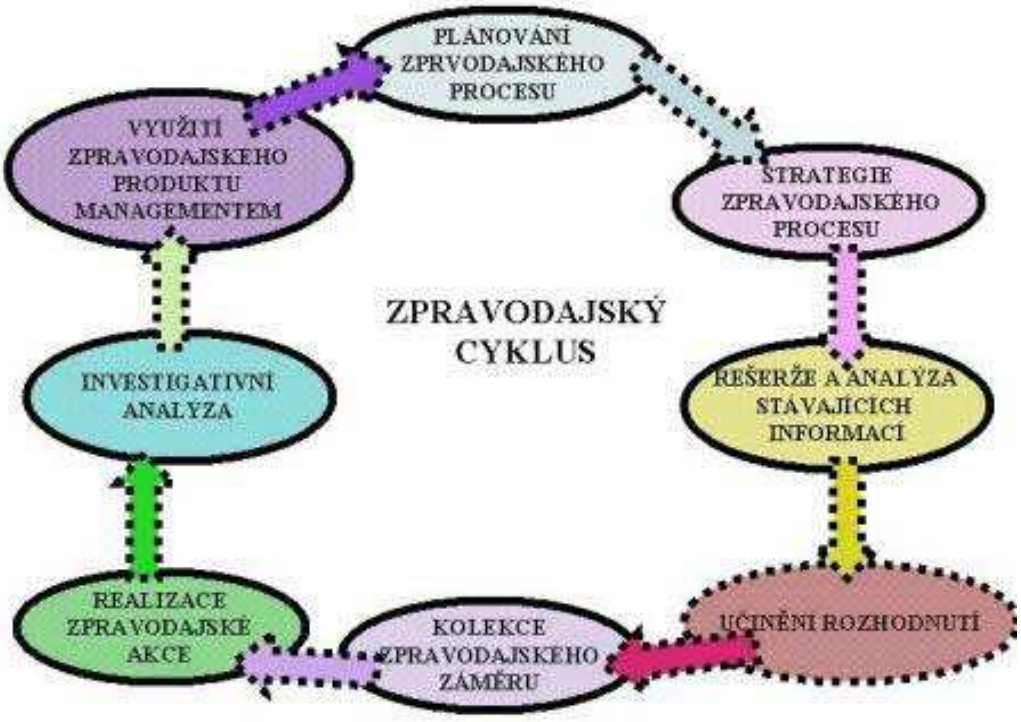
- Operatíva: Spravodajská operatíva predstavuje schopnosť efektívneho vyhľadania dát a ich následné spracovanie na informácie. Výsledným produktom operatívy je teda informácia.
- Taktika: Spravodajská taktika predstavuje schopnosť pochopenia informácií a za použitia spravodajskej technológie analýzy ich relevantný výber a premenu na znalosť a schopnosť prezentácie znalostí v podobe zrozumiteľnej pre užívateľa. Výsledkom taktiky je teda znalosť.
- Stratégia – Spravodajská stratégia teda predstavuje technológie a schopnosti hľadať a spracovať znalosti v ich vzájomných súvislostiach. Výsledkom tohto procesu je poznanie.

Spravodajstvo predstavuje neustále sa opakujúce a na sebe nadväzujúce cykly. Hovoríme teda o spravodajskom cykle. Spravodajský cyklus je tvorený neustále pokračujúcimi a vzájomne na seba nadväzujúcimi spravodajskými procesmi. Medzi jednotlivými procesmi prebieha spravodajské riadenie.

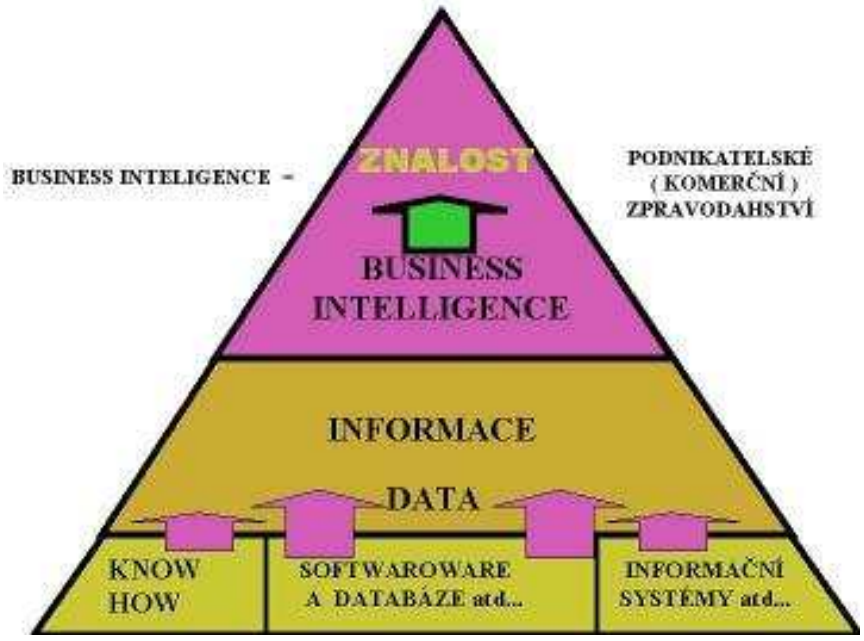
Spravodajské riadiace postupy obsahujú :

- Definovanie potrieb
- Spravodajské plánovanie
- Tvorbu operatívy, taktiky a stratégie spravodajského procesu
- Rešerše a analýzu stávajúcich informácií, znalostí a poznaní
- Učinenie rozhodnutia o realizácii spravodajského procesu a jeho zámeroch a cieľoch stanovenia kolekcie spravodajského zámeru.

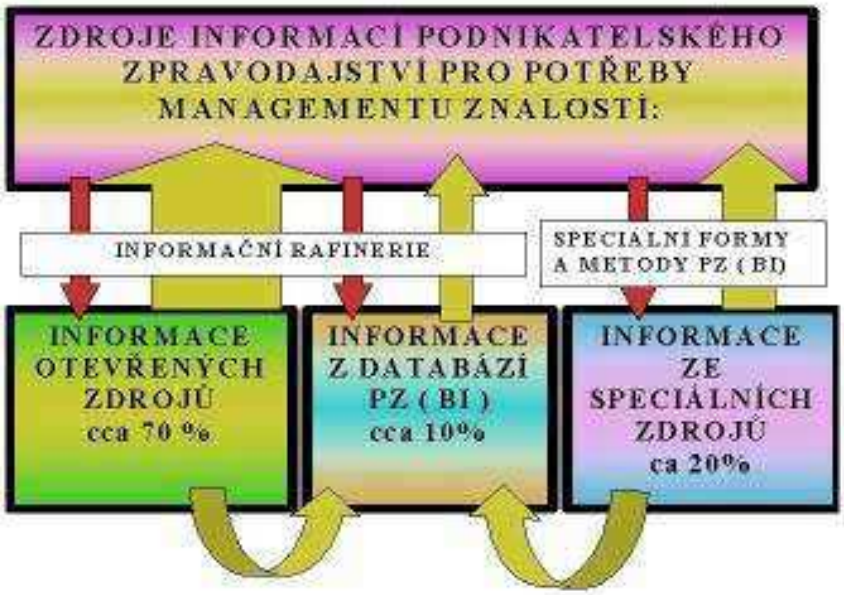
Obr. 2 Spravodajský cyklus



Obr. 3 Spravodajský cyklus – 2



Obr. 4. Vznik znalosti



Obr. 5. Zdroje KS

1.4 Spravodajské technológie

Spravodajstvo chápeme ako informačný produkt a teda ako produkt znalosti a poznania (ako produkt má svoj obsah, formu a aktuálnosť) a taktiež ako proces respektíve cestu od získaných dát k znalosti a poznaniu .

Ako proces sa skladá z nasledujúcich krokov respektíve fáz :

- **Riadenie** : riadenie spravodajskej činnosti predstavuje identifikáciu informačných potrieb a stanovenie priorít. Jedná sa o vytvorenie a správne definovanie otázok a stanovenie cesty k dosiahnutiu odpovedí.
- **Zber** : ide o cielené využívanie informačných zdrojov.
- **Analýza** : Spravodajská analýza predstavuje interpretáciu informácií v kontexte informačných potrieb vo vzájomných súvislostiach, vo vzťahu k riešenému problému, vo vzťahu k odpovedi a taktiež vo vzťahu k odpovedi na položené otázky čiže v kontexte docielenia znalosti o danom probléme vychádzajú z definovaných otázok.

- **Distribúcia** : distribúcia spravodajskej znalosti a spravodajského poznania vyžaduje včasné doručenie klientovi vo forme ktorej klient dokáže porozumieť. Táto znalosť musí mať vysoký stupeň aktuálnosti aj za cenu straty kvality. Distribúcia informácie respektíve znalosti nesmie byť zdržovaná kvôli dosiahnutiu maximálnej kvality za cenu straty aktuálnosti pretože i vysoko kvalitné informácie ktoré sú distribuované oneskorene strácajú svoju aktuálnosť a sú teda nevhodné k použitiu.

1.4.1 Spravodajské technológie obsahujú:

- **Technológie práce s otvorenými informačnými zdrojmi**, ktoré nazývame taktiež ako sekundárne zdroje . Jedná sa o metódy ako rafinovanie informácií z otvorených zdrojov pre získavanie informácií využiteľných bez rizika kompromitácie a potreby legalizácie a pod. Využívajú sa nasledovné kroky:
    - Zmapovanie záujmovej právnickej alebo fyzickej osoby, udalosti, situácie ,okolnosti, javu a pod. Z hľadiska vzájomných vzťahov a súvislostí .

- **Rýchle získanie relevantných informácií o záujmovom subjekte**, udalosti, skutočnosti atd. zo sekundárnych zdrojov ako je napríklad internet , média , iné verejne dostupné databázy a ďalšie komerčné zdroje.
- **Rýchle spracovanie všetkých získaných základných informácií formou tematických kontextových a prechodových rešerší** a využitie týchto informácií pri monitoringu záujmového subjektu, udalosti, skutočnosti a javu.
- **Rozkrytie vzájomných väzieb a súvislostí**. Jedná sa hlavne o väzby na ďalšie firmy či fyzické osoby, politické strany, organizácie atd. do potrebnej úrovne.
- **Získanie ďalších potrebných údajov pre nasledovné šetrenia a pre rozhodnutie o využití špeciálnych spravodajských postupov, pre plánovanie spravodajského postupu a podobne.**
- **Doplnenie relevantných informácií do diagramu** vzťahovej poprípade vývojovej analýzy a ich názorná prezentácia klientovi pričom je vhodné využiť grafickej vzťahovej alebo vývojovej analýzy
- **Využitie získaných znalostí a poznatkov** a taktiež doposiaľ realizovaných rešerší a analýz pre realizáciu ďalších spravodajských opatrení za využitia primárnych zdrojov informácií, investigatívnych postupov, pokiaľ je to nutné.

- **Technológie kvalifikovaného využitia primárnych** (prvotných) zdrojov a informácií pre investigatívu, vyhľadávanie a zhromažďovanie informácií z týchto zdrojov.
- **Technológie a analýzy informácií s využitím spravodajských technológií**.
  - Vypracovanie tematických rešeršou – ich hlavným účelom je rýchle a komplexné zmapovanie informačného poľa okolo osoby, organizácie ,javu atd. s dôrazom na zohľadnenie určitého charakteru či kontextu informácií .
  - Vypracovanie kontextovej rešerše – ich hlavným účelom je vyhodnotenie resp. sledovanie informácií o určitej problematike s dôrazom na konkrétny spôsob využitia týchto informácií.

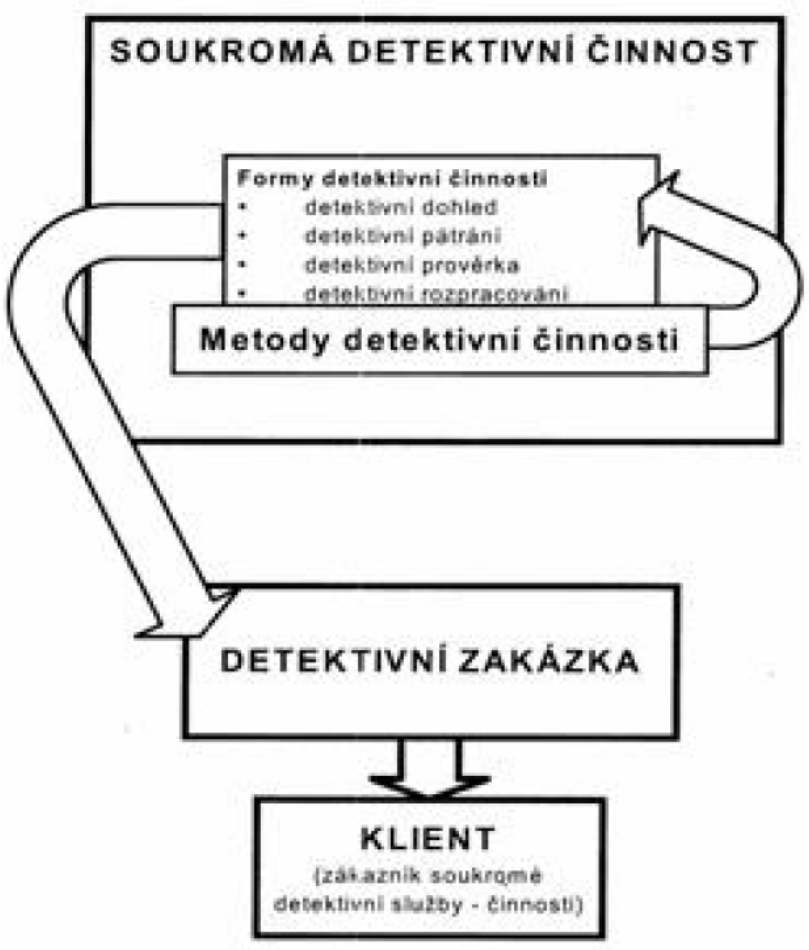
- Vypracovanie prehľadových monitoringov – ich hlavným účelom je odkrytie väzieb a súvislostí vo veľkom množstve informácií.
- Vypracovanie analýz - ich hlavným účelom je interpretácia nazbieraných dát ktoré sú relevantné k problému zadanému klientom. Príkladom analýz sú :
  - Situačná analýza – rozkrytie vzťahov fyzických a právnických osôb, pozícia záujmového objektu v určitom projekte.
  - Vývojová analýza - pozícia záujmového objektu na určitom teritóriu a taktiež vývoj v čase
  - Kontextová analýza – analýza k určitému problému a jeho vzájomné súvislosti a vzťahy.
  - Komplexná analýza – geografické rozloženie a časový priebeh záujmového objektu.

- **Technológie spracovania informácií na využiteľné znalosti a poznania .**
  - Spracovanie záverečnej analýzy v zákazníkom zadanej forme (texty, grafy, vzťahové a vývojové analýzy , atď.), ktorá obsahuje relevantné a verifikované informácie získané prostredníctvom primárnych a sekundárnych zdrojov.

1.5 Konkurenčné spravodajstvo (competitive inteligence – CI)

Pojem konkurenčné spravodajstvo alebo „competitive Inteligence“ sa v ČR zaužíval pod prekladom „konkurenční zpravodajství“. Jedná sa o činnosti , respektíve procesy slúžiace pre získavanie a následnú interpretáciu informácií , ktoré sú následne využívané pre rozhodovanie subjektov v konkurenčnom prostredí trhu za účelom dosiahnutia, udržania alebo zvýšenia konkurencieschopnosti firmy. Pri získavaní informácií sa používajú postupy a metódy bežne používane spravodajskými službami avšak za predpokladu, že budú rešpektované právne a etické pravidlá platné pre komerčné prostredie.

Pojem competitive inteligence môžeme definovať ako proces, ktorý zahŕňa zber, vyhodnocovanie, analýzu a distribúciu informácií, ktoré sa týkajú zadaného problému a ich výsledkom je poznatok vyjadrený vo forme umožňujúci stanoviť najlepší postup v riešení tohto problému.



Obr. 6 Súkromná detekívna činnosť

1.6 Business Inteligence

Jedná sa o súhrn metód a postupov pre zlepšenie rozhodnutí pri podnikaní za využitia dostupných faktov a dát, ktoré sa nachádzajú v informačných systémoch. Cieľom tohto procesu je spracovanie čo možno najpresnejších predpovedí vývoja v podnikaní na základe skúseností a odhadov, ktoré sú aplikované na informácie zhromaždené z rôznych relevantných zdrojov.

1.7 Živnostenský zákon a jeho vzťah ku KS

Súkromné bezpečnostné služby (SBS) nie sú v ČR zákonom priamo upravené a tak je podnikateľská činnosť v priemysle komerčnej bezpečnosti (PKB) prevádzkované na základe Živnostenského zákona č. 455/1991 Sb., . Tento zákon upravuje podmienky vstupu do podnikateľskej sféry SBS z hľadiska štátnej regulácie podnikania. SBS poskytujú služby na komerčnom základe a k tomu využívajú právne možnosti poskytované ústavou ČR, občianskym, obchodným zákonníkom a taktiež živnostenským zákonom. Činnosť PKB upravuje jedine tento zákon a zaraďuje ich medzi koncesovanú živnosť. V oblasti koncesovaných živností sa pre účely PKB využívajú obory : výuka a výcvik v streľbe zo zbraní ,poskytovanie telekomunikačných služieb, vývoj, výroba, úprava, preprava , nákup, predaj, požičiavanie , úschova a znehodnocovanie vojenských zbraní, streliva a prevádza strelníc. V oblasti viazaných živností sa pohybujeme v oblasti oborov : poskytovanie služieb v oblasti bezpečnosti a ochrany zdravia pri práci, psychologické poradenstvo, projektová činnosť, montáž, opravy, revízie a skúšky vyhradených elektrických zariadení.

Hlavné činnosti PKB v koncesovaných živnostiach :

- Poskytovanie technických služieb k ochrane majetku a osôb
- Služby súkromných detektívov
- Podniky zaisťujúce ostrahu majetku a osôb

1.8 Zákon č. 101/2000 Sb o ochrane osobných údajov

Jedná sa o významný zákon vzhľadom k problematike konkurenčného spravodajstva. Tento zákon upravuje prístup k informáciám a ochranu osobných údajov o fyzických osobách. Ochrana osobných údajov má tak vysokú prioritu, že bol zriadený samostatný úrad pre ochranu osobných údajov. Zákon sa nevzťahuje na osobné údaje, ktoré sú spracovávané štátnymi orgánmi, orgánmi územnej samosprávy alebo inými orgánmi úradnej moci ako taktiež fyzické a právnické osoby. V § 4 , pís. B je definovaný pojem citlivé údaje. Za citlivé údaje sú považované údaje o národnostnom, etickom alebo rasovom pôvode, politických postojoch, členstve v politických stranách alebo hnutiach prípadne odborových alebo zamestnaneckých organizáciách, náboženstve, filozofickom presvedčení, trestnej činnosti, zdravotnom stave a sexuálnom živote. Jedná sa hlavne o údaje intímne a súkromné ktoré by pohli poškodiť osobu na ktorú sa vzťahujú.

2 FORMY A METÓDY VYUŽÍVANÉ V KOMERČNOM SPRAVODAJSTVE

Súkromná detektívna činnosť je realizovaná prostredníctvom foriem a metód súkromnej detektívnej činnosti.

Formou súkromnej detektívnej činnosti rozumieme:

- Charakteristiku všeobecných cieľov, ktoré majú byť súkromnou detektívnou činnosťou dosiahnuté v konkrétnom prípade v procese realizácie súkromnej detektívnej činnosti.
- Formuláciu všeobecných cieľov, ktoré majú byť v procese súkromnej detektívnej činnosti dosiahnuté.

Význam foriem súkromnej detektívnej činnosti spočíva v tom, že pomáhajú súkromnému detektívovi už od začiatku správne stanoviť a vytýčiť ďalšie zameranie postupu, správnu voľbu metód a prostriedkov súkromnej detektívnej činnosti a ukazujú mu tendencie vývoja skúmaného problému. [6]

2.1 Detektívny dohľad

Súkromne detektívny dohľad je formou súkromnej detektívnej činnosti spočívajúci v súhrne úkonov a opatrení využívajúcich rôznych metód súkromnej detektívnej činnosti, metód kriminalistiky, metód kriminológie, sociológie a radu forenzných disciplín, metódy policajnej praxe apod.

Jedná sa o :

a) priebežné zhromažďovanie informácií o objektoch (osobách, firmách, apod.) a to najmä:
   - Pre potreby personálnej práce,
   - Pri ochrane proti úniku informácií a dát,
   -Pri získavaní informácií marketingového charakteru alebo prípadne konkurenčného charakteru.
   b) činnosť hotelových detektívov (vrátane reštauračných a zábavných zariadení), činnosť detektívov obchodného domu, obchodov, trhovísk, apod.

c) ochranné a obranné doprovody (napr. preprava peňažných hotovostí a cenností, kamiónovej prepravy atď.), ktoré sú vykonávané skrytým spôsobom.

d) osobná ochrana osôb (bodyguarding).

e) detektívny dohľad nad dodržiavaním verejného poriadku pri športových, kultúrnych udalostiach.

f) detektívny dohľad nad dodržiavaním verejného poriadku a bezpečnosti v peňažných ústavoch.

g) detektívny dohľad nad dodržiavaním verejného poriadku a bezpečnosti v podnikoch, úradoch, inštitúciách a organizáciách. [6]

2.2 Detektívne pátranie po osobách a veciach

Jedným zo základných druhov súkromnej detektívnej činnosti je detektívne pátranie po osobách a veciach. Pátranie po osobách a veciach môže byť spravidla tiež realizované paralelne s pátraním Polície ČR. Detektívne pátranie je forma kriminalisticko-detektívnej praxe, ktorú tvorí súhrn vzájomne zladených činností, úkonov a opatrení za využitia celej škály metód súkromnej detektívnej činnosti, zameraných na hľadanie a zistenia hľadaného objektu. Objektom detektívneho pátrania môžu byť osoby či veci. [6]

Detektívne pátranie sa delí na pátranie:

- Po osobách,

- Po veciach, vrátane vozidiel.

2.3 Detektívna previerka

Detektívnu previerku chápeme ako proces aktivít súkromného detektíva s využitím metód a prostriedkov, ktorých cieľom je overenie pravdivosti alebo nepravdivosti informácií o osobe, udalosti, skutočnosti apod., či doplnenie alebo získanie informácií o nových osobách a skutočnostiach, ktoré sú predmetom zákazky súkromnej detektívnej služby. [6]

V rámci detektívnej previerky sa môže jednať o:

a) overovanie určitých informácií, domnienok, hypotéz, dôkazných prostriedkov a pod.
b) zistenie povesti osôb a ďalších informácií o osobe, ako je napr. :

- Miesto zamestnania,

- Majetkové pomery,

- Zistenie režimu dňa a pod.

c) zistenia a preverenia dodržiavania režimu ochrany informácií

d) preverenie a získanie základných informácií o právnických i fyzických osobách v podnikateľskej sfére

e) preverenie marketingových informácií

2.4 Detektívne rozpracovanie

Detektívne rozpracovanie možno charakterizovať ako najzložitejšiu formu súkromnej detektívnej činnosti. Vyžaduje systematický, cieľavedomý, plánovaný a komplexný prístup súkromnej detektívnej kancelárie (agentúry), prípadne súkromného detektíva. Detektívne rozpracovanie sleduje zistenie objektívnych informácií o priebehu istých záujmových situácií alebo udalostí. Detektívne rozpracovanie máva spravidla dlhodobejší charakter. Celý proces detektívneho rozpracovania je nutné chápať ako cyklus úkonov, postupov, rozhodnutí a opatrení. [6]

Tento cyklus v sebe zahŕňa:

a) vymedzenie problému,

b) analýzu (vyhodnotenie) informácií, stôp a pod, ktoré sú k dispozícii,

c) stanovenie detektívnych verzií,

d) rozhodovanie o ďalších krokoch, využitie metód, síl a prostriedkov,

e) plánovanie jednotlivých krokov a využitie jednotlivých metód,

f) organizácia priebehu realizácie detektívneho rozpracovania,

- Motivovania,

- Stimulovanie,

- Operatívne riadenie,

g) hodnotenie výsledkov postupu detektívneho rozpracovania vrátane analýzy získaných informácií a vyvodzovanie dôsledkov k detektívnom verziám

h) ukončenie jedného cyklu predstavuje začatie cyklu nového.

Plán detektívneho rozpracovania, ktorý má charakter písomného materiálu, by mal obsahovať:

a) zhodnotenie situácie,

b) vytýčenie jednotlivých detektívnych krokov a ich preverenie,

c) určenie osobnej zodpovednosti a termínu plnenia,

d) výsledok plnenia.

Detektívne rozpracovanie sa uplatňuje najmä v prípadoch:

a) smerujúcich k odhaleniu páchateľa trestného činu alebo iného protiprávneho konania,

b) smerujúcich k odhaleniu skrytej trestnej činnosti alebo iného protiprávneho konania,

c) smerujúcich na zabezpečeniu skutkového stavu pre rôzne administratívne alebo súdne kauzy, smerujúcich k získaniu dôležitých informácií.

Fáza detektívneho rozpracovania:

a) fáza formulácie problému,

b) fáza vlastného plánovania detektívneho rozpracovania:

- Priebežná analýza získaných informácií,
- Vytyčovanie a previerka detektívnych verzií,
- Priebežné dopĺňanie plánu podľa vzniknutej situácie.

c) fáza realizácie detektívneho rozpracovanie:

Najčastejšie ide o metódy:

- Detektívneho informačného prieniku,
- Detektívneho vyťažovanie,
- Detektívneho pozorovania,
- Detektívne prehliadky miesta skutku či udalosti atď.

Detektívnej rozpracovanie sa vlastne odohráva v krokoch:

- Priebežná analýza novo získaných informácií,
- Vylučovanie či overovanie detektívnych verzií a tvorba nových,
- Aktualizácia plánu detektívneho rozpracovanie, stanovenie nových úloh a opatrení na preverenie vytýčených detektívnych verzií. [6]

2.5 Detektívne dokumentovanie

Detektívne dokumentovaní je forma súkromnej detektívnej činnosti, ktorej cieľom je súkromnou detektívnou činnosťou získané informácie tzv. zlegalizovať (spracovať ich do podoby prístupnej verejnosti) a zakonzervovať ich do dlhodobej podoby pre dlhodobé využitie. V procese detektívneho dokumentovania, súkromný detektív využije radu kriminalistických, taktických i technických metód. [6]

Detektívne dokumentovaní členíme podľa hľadiska nadväznosti:

a) detektívne dokumentovania v nadväznosti na iné formy detektívnej činnosti:
   - Detektívne dokumentovanie je pokračovanie iných foriem súkromnej detektívnej činnosti,
   - Detektívne dokumentovanie nadväzuje na detektívnu previerku a tiež na detektívne pátranie.

b) detektívne dokumentovanie bez nadväznosti na iné formy súkromnej detektívnej činnosti:

- Spravidla na objednávku advokáta, podnikových alebo komerčných právnikov zabezpečuje súkromná detektívna agentúra technické spracovanie informácií o dôkazoch a stopách,

- Tiež sa môže jednať o dlhodobé alebo krátkodobé monitorovanie záujmových informácií a ich technické spracovanie do požadovanej podoby.

Členenie detektívneho dokumentovania z hľadiska použitých prostriedkov detektívneho dokumentovania:

a) písomná dokumentácia:

- Nadobudnutie fotokópií rôznych dokumentov,
- Nadobudnutie fotokópií rôznych archívnych materiálov,
- Obstaranie nových písomností, napr. čestné vyhlásenie, znalecké posudky apod.

b) fotodokumentácia:

- Fotodokumentácia udalostí,
- Fotodokumentácia javov,

- Fotodokumentácia kriminalistických stôp,

- Fotodokumentácia činnosti osôb,

- Fotodokumentácia archiválií apod.

c) audiodokumentace : Ide o nadobudnutie zvukových záznamov na audio média. Z hľadiska ďalšieho využitia je vhodné obsah záznamu zdokumentovať aj písomnou formou.

d) video či filmová dokumentácia : Jedná sa o dokumentovaní dôležitých skutočností, predovšetkým dejového charakteru, na filmové alebo video média.

e) vecné dokumentácie:

Jedná sa o zabezpečenie predmetov a stôp (napríklad sadrových odliatkov, daktyloskopických odtlačkov apod.) pre potreby dokazovania v súdnych kauzách alebo v správnych konaniach. [6]

3 METÓDY SÚKROMNEJ DETEKTÍVNEJ ČINNOSTI

Metódou súkromnej detektívnej činnosti rozumieme typový postup smerujúci k naplneniu a realizácii niektorej z foriem súkromnej detektívnej činnosti. V rámci súkromnej detektívnej činnosti využívame metódy, kriminalistických, forenzných (psychológia, kriminológia, pedagogika, sociológia, atď.), modifikované metódy činnosti polície, najmä kriminálnej polície.

Rozdiel medzi formou a metódou súkromné detektívne činnosti možno charakterizovať tak, že forma je vonkajším výrazom obsahu typovej skupiny súkromnej detektívnej zákazky, zatiaľ čo metóda je napĺňaním jej obsahu. U formy ide o zovšeobecnenie určitého obsahového charakteru zákazky, naproti tomu u metódy sú uznávané, zovšeobecnené, profesijné (všeobecné, špeciálne a kriminalistické) postupy, ktoré umožňujú naplnenie jednotlivých cieľov. [6]

3.1 Detektívna kombinácia

Pod pojmom detektívna kombinácia rozumieme podrobne naplánovaný a plánovite realizovaný súbor úloh súkromné detektívnej činnosti. Tieto opatrenia na seba navzájom nadväzujú a vzájomne sa podmieňujú s cieľom získať pre daný prípad súkromnej detektívnej činnosti dôležité informácie. Ide o informácie záujmovom objekte a predmetu súkromného detektívneho pôsobenia, získaného v rámci rôznych foriem súkromnej detektívnej činnosti (atď.), pričom jednotlivé úkony sú realizované s využitím vhodne a účelne volených metód súkromnej detektívnej činnosti.

Detektívne kombinácia ako metóda súkromnej detektívnej činnosti predstavuje model systémového prístupu k riešeniu problémových okruhov súkromnej detektívnej činnosti. Táto metóda je založená na využití všeobecných, najmä psychologických metód, a to najmä metódy reflexívnych hier a asertívneho správania, čo v rôznych kombináciách v sebe obsahuje ďalšie čiastkové metódy súkromnej detektívnej činnosti. Podstatou detektívnej kombinácie je vyvolanie určitého prostredia a určitej situácie s cieľom vyvolať reakciu záujmového objektu, ktorý je detektívnymi metódami monitorovaný a zaznamenávaný. [6]

Detektívna kombinácia vedľa ďalších všeobecných metód využíva ako metódu špecifický spôsob modelovania, ktoré medzi metódami vedeckého prístupu na skúmanie alebo riešenie problému zaujíma veľmi dôležité miesto. V procese prípravy a riešenia detektívnej kombinácie zastávajú významné miesto také všeobecné metódy, ako je metóda indukcie, dedukcie, analýzy, syntézy, analógia atd. Detektívna kombinácia možno do určitej miery považovať za istý spôsob aplikácie reflexívnych alebo spravodajských hier a taktiež aj za prípustný stupeň aktivizácie záujmového prostredia či záujmovej osoby.

Zjednodušene možno povedať, že detektívne kombinácia spočíva vo vyvolaní situácie, na ktorú očakávame nejakú reakciu, kedy potom nasleduje zaregistrovanie takýchto reakcií, ich vyhodnotenie a interpretácia vo vzťahu k riešenému problému. Výber jednotlivých metód uplatňovaných v rámci detektívnej kombinácie a postupnosť ich použitia je daná charakterom príslušnej formy súkromnej detektívnej činnosti. Detektívna kombinácia, ako komplexná alebo súhrnná metóda súkromnej detektívnej činnosti, môže byť použitá aj ako submetóda inej komplexnej metódy súkromnej detektívnej činnosti, ako napríklad metódy detektívneho informačného preniknutia, metódy detektívnej dezinformácie atd.

Ak hovoríme o metóde detektívnej kombinácie ako o istej aplikácii reflexívnych alebo spravodajských hier, máme na mysli, že istá metóda alebo skupina metód slúžia v rámci detektívne kombinácie ako podnet k vyvolaniu reakcie záujmového objektu súkromnej detektívne činnosti a využitia ďalšie metódy, alebo skupiny metód slúžia na registráciu predmetnej reakcie. K registrácii reakcií v rámci detektívnej kombinácie je potom frekventovanou metódou napríklad detektívneho pozorovania.

Dobre pripravená a prepracovaná detektívna kombinácia je v rámci súkromnej detektívnej činnosti veľmi efektívnou metódou, a preto je tiež táto metóda pomerne často využívaná. Je potrebné povedať, že metóda detektívne kombinácie je v praxi skúsených súkromných detektívov v rade prípadov uplatňovaná inštinktívne, bez toho by si súkromný detektív uvedomoval, že využíva tejto komplexnej metódy.

V tomto prípade súkromný detektív vlastne reaguje na vznikajúci situáciu, ktorá je odozvou jeho predchádzajúcich krokov, a podľa nej volí ďalšie kroky. Ak máme ale hovoriť ako o metóde súkromnej detektívnej činnosti, predpokladá sa jej uvedomelého využívania, teda jej jednotlivé kroky sú vopred naplánované, a to vrátane vyvodenia istých predpokladov. [6]

V tomto smere má detektívna kombinácia rad spoločných rysov s detektívnou verziou a procesom jej overovania alebo vylučovania. Uvedomelé využívanie tejto komplexnej metódy súkromnej detektívnej činnosti zvyšuje efektívnosť jej využitia a tým aj celkovú efektívnosť naplňovania príslušnej realizovanej formy súkromnej detektívnej činnosti. Jednou zo základných zásad v procese detektívnej kombinácie zohráva zásada rýchlosti a ofenzívnosti. Jej realizácia si preto vyžaduje kvalitne premyslieť a pripraviť postup riešenia prípadu a vykonávanie vhodných detektívnych opatrení. Detektívnej kombináciou sa rozumie ofenzívny postup súkromného detektíva s využitím priaznivej situácie a detektívnej legendy s cieľom zabezpečiť zistenie a zadokumentovanie dôležitých skutočností a informácií pre realizáciu iných detektívnych opatrení a úkonov ako predpokladov vytvorenia potrebných podmienok pre ďalší postup a úspešné naplnenie niektorej z foriem, v konkrétnom prípade realizácie súkromnej detektívnej činnosti.

Pri detektívnej kombinácii sú do prirodzenej objektívne vzniknutej situácie vnášané umelé prvky, ktoré sú oprávnené ovplyvniť ako túto situáciu, tak i jednanie a správanie osôb, ktoré sú objektom detektívneho záujmu. Pri voľbe a využitie umelých prvkov je potrebné dbať na to, aby tieto prvky spĺňali nasledujúce požiadavky:

- Umelé prvky musia čo najlepšie a najvierohodnejšie nadväzovať na normálne vzniknutú situáciu, musí s ňou splynúť a nesmie byť nápadné,

- Musia byť vytvorené na základe dobrej znalosti charakteristiky osôb, pre ktoré je umelo vytvorená situácia určená,

- Vnesenie týchto prvkov do objektívne existujúcej situácie musí zostať utajené nielen pred osobami v detektívnom záujme, ale aj ďalšími nepovolanými osobami,

- Situácia upravená umelo vyvolanými prvky nesmie negatívne pôsobiť na ďalšie osoby pohybujúce sa v danom čase v danom priestore, kde tieto umelé prvky pôsobia,

- V žiadnom prípade nepripustiť, aby tieto prvky provokovali záujmové osoby k páchaniu protispoločenský a nezákonné činnosti. [6]

Detektívna kombinácia ako zložitý model systémového prístupu k riešeniu zadaného problému si vyžaduje prevedenie celej rady na seba nadväzujúcich detektívnych opatrení a úkonov. Preto tiež nie je možné kvalitnú detektívnu kombináciu uskutočniť bez veľmi kvalitnej a detailnej prípravy, pri ktorej je potrebné vychádzať z nasledujúcich odporúčaní:

- Dôkladne analyzovať situáciu,
- Vytýčiť ciele detektívnej kombinácie a zvoliť spôsob ich vykonania,
- Plánovito vykonávať detektívne úkony a opatrenia,
- Stanoviť a zosúladiť umelé prvky a priebeh detektívnej kombinácie,
- Zabezpečiť trvalú kontrolu priebehu detektívnej kombinácie.

3.2 Detektívne informačné preniknutie

Pre kvalifikovaný výkon súkromnej detektívnej činnosti, pre získavanie kvalitných informácií a najmä pri realizácii detektívneho rozpracovania, detektívneho dohľadu atď. je nevyhnutné vybudovanie informačných zdrojov. Detektívne informačný preniknutie je ďalšia z komplexných metód súkromnej detektívnej činnosti. S ohľadom na skutočnosť, že informačná činnosť je jednou zo základných smerov detektívne činnosti, je táto metóda jednou z najvýznamnejších. Smeruje k vytvoreniu vhodnej situácie pre dlhodobejšie získavanie záujmových informácií, zo záujmových prostredia a od záujmových osôb. [6]

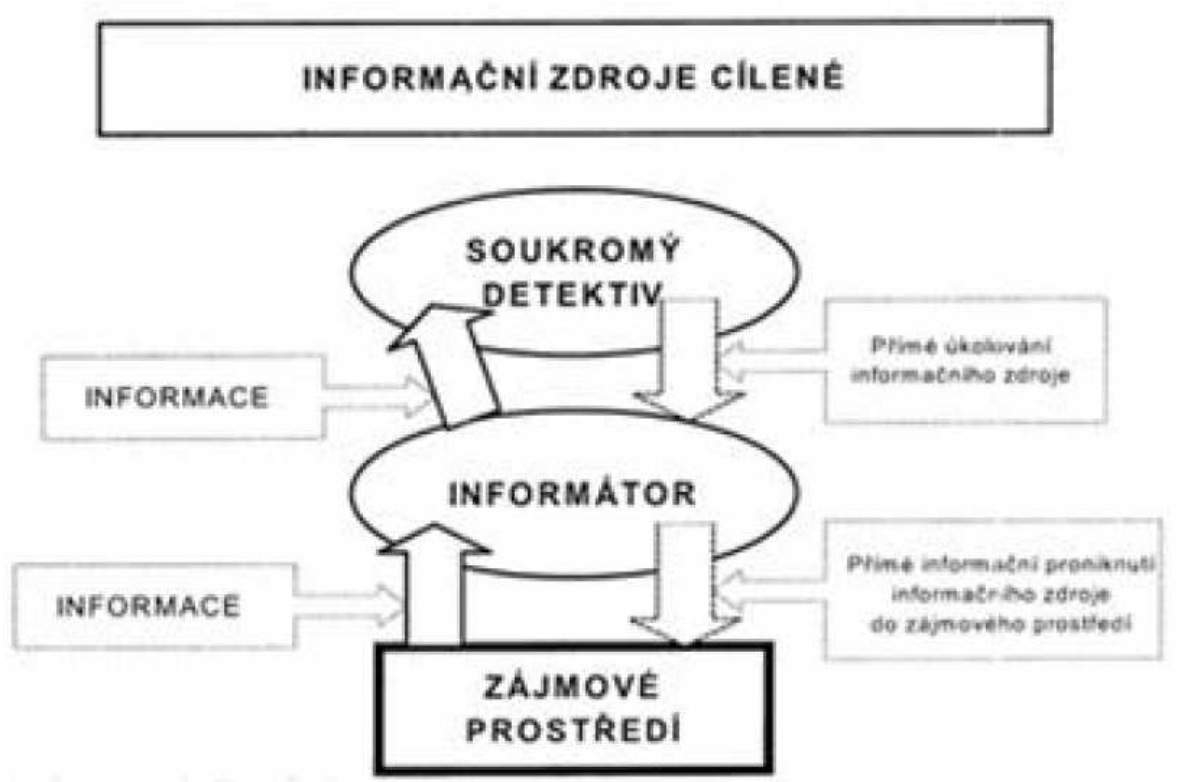
Pri výklade problematiky detektívneho informačného preniknutia je potrebné vychádzať zo základnej skutočnosti, že súkromná detektívna činnosť je komerčná činnosť alebo vlastná činnosť podnikateľského subjektu, úradu inštitúcie či organizácie. Nejde teda o činnosť štátneho donucovacieho aparátu, a preto tiež nemožno k informačnému preniknutiu využívať niektorých prístupov nimi používaných. Ďalej je potrebné vychádzať z úplne nezvratnej skutočnosti, že informácie sú tovarom, a to veľmi cenným tovarom.
Teória a prax policajnej činnosti a činnosti tajných služieb v súvislosti s ťažbou informácií rozlišuje: [6]

- Informačné zdroje získané na základe ich presvedčenia,
- Informačné zdroje získané na materiálnom základe,
- Informačné zdroje získané na podklade kompromitujúcich materiálov.

Získavanie informačného zdroja v rámci súkromnej detektívnej činnosti na podklade kompromitujúcich materiálov síce nemožno vylúčiť, ale tento prístup sa neodporúča. Oveľa lepšie je získanie informačného zdroja (informátora) ako platenú službu, teda na materiálnom základe tzn., že osoba bude ochotná stať sa informátorom súkromného detektíva za finančnú odmenu. Informácie sú pre informačný zdroj tovarom a tovarom sú aj pre súkromného detektíva. Každá informácia má svoju hodnotu (cenu) vyjadriteľnú peňažnou hodnotou. [6]

Informačné zdroje môžu byť v rámci súkromnej detektívnej činnosti delené ako:

- Informačné zdroje cielené-jedná sa o zdroje získavané a vyťažovanie ku konkrétnej osobe a najčastejšie ku konkrétnemu prípadu detektívneho rozpracovania.



Obr. 7. Informačné zdroje cielené

- Informačné zdroje pozičné - jedná sa o informačné zdroje v určitom prostredí, svoje plné opodstatnenie majú tieto informačné zdroje v rámci komerčného spravodajstva. [6]

Obr. 8 Informačné zdroje pozičné

Požiadavky na informačné zdroje:

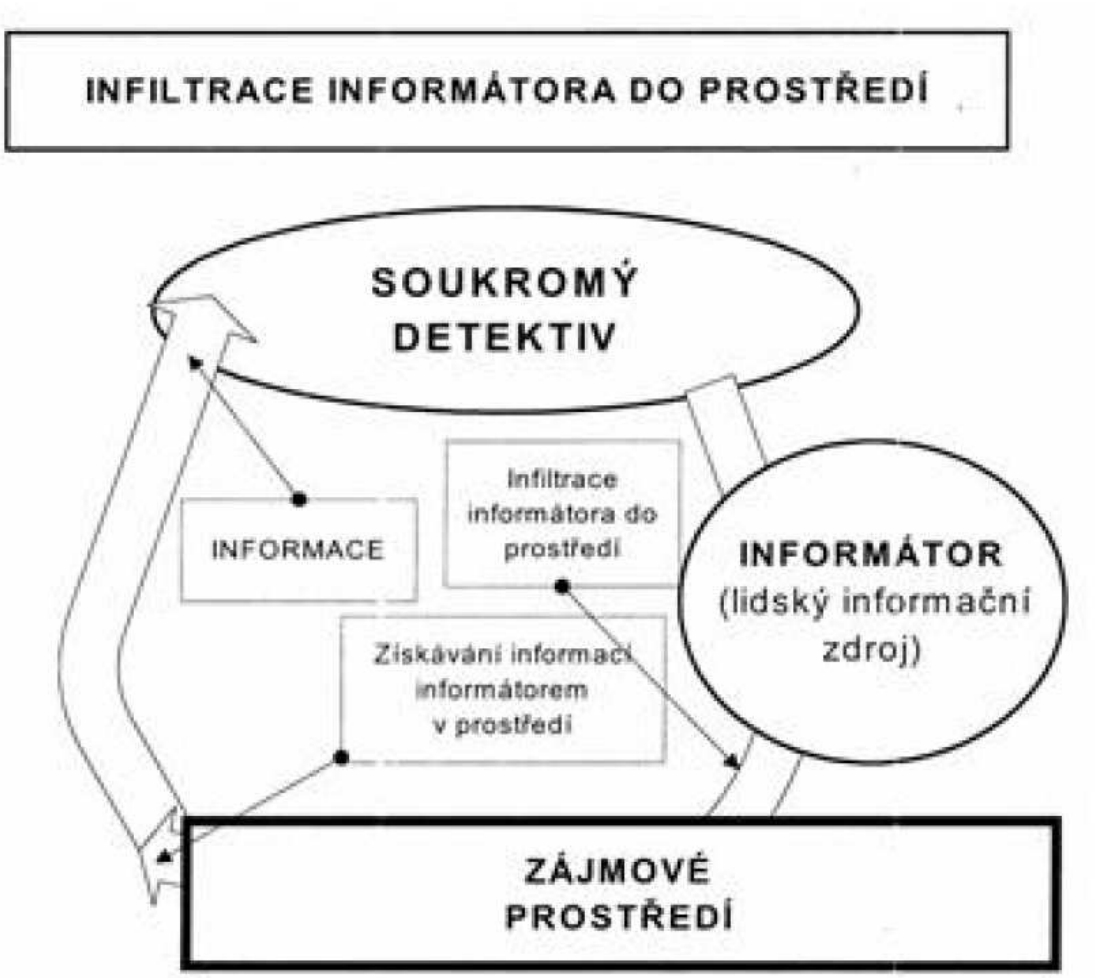
- Vhodnosť,
- Schopnosť,
- Spoľahlivosť.

Spoľahlivosť informačného zdroja v sebe kumuluje:

- Pravidelnosť informácií: ide o vysoký stupeň pravdepodobnosti, že osoba poskytujúca informácie ich bude odovzdávať v požadovanom čase, že osoba bude dodržiavať dohodnuté termíny kontaktov a že bude dodržiavať zásady konšpirácie,
- Pravdivosť informácie: ide o vysoký stupeň pravdepodobnosti, že osoba odovzdávajúci informácie bude odovzdávať skutočné a pravdivé informácie, že bude informovať akým spôsobom a z akých zdrojov boli informácie získané a že nebude odovzdávať dezinformácie,
- Objektívnosť informácií: objektivita informácie predovšetkým predpokladá vysoký stupeň pravdepodobnosti, že ľudský informačný zdroj bude v záujmovej sfére pristupovať objektívne na získavanie informácií, tj nebude ich ani prikrášľovať, ani přičerňovat, bude odlišovať získané informácie a svoje úvahy a vývody.
- Dôveryhodnosť osoby-informačného zdroja: ide o vysoký stupeň pravdepodobnosti, že osoba poskytujúca informácie nebude tzv. dublovať. Že bude schopná si spoločenské prostredie alebo u záujmových osôb získavať dôveru.

V rámci informačného preniknutia je možné informačný zdroj rozdeliť v podstate dvoma spôsobmi: [6]

a) informačný zdroj je získaný alebo už existuje a je infiltrovaný do záujmového prostredia alebo k záujmovej osobe.



Obr. 8. Infiltrácia informátora do prostredia

b) informačný zdroj je vytipovaný zo záujmového prostredia či okolia záujmové osoby a je získavaný z tohto prostredia.

Obr. 9. Získanie informátora z prostredia

Metódu detektívneho preniknutia je potrebné považovať za veľmi náročnú a náročnú na profesionalitu súkromného detektíva. Pre proces získavania ľudského informačného zdroja a následne v procese jeho kontroly sú využívané ďalšie metódy súkromnej detektívnej činnosti. Ide najmä o metódu detektívne kombinácie, metódu detektívneho pozorovania, všeobecné metódy modelovania atd. [6]

3.3 Detektívna dezinformácia

Detektívne dezinformácie predstavuje metódu súkromnej detektívnej činnosti slúžiace k infiltrácii účelovo formulovanej a zámerne infiltrovanej nepravdivej správy do záujmového prostredia súkromnej detektívnej činnosti. Táto zámerná infiltrácia nepravdivej správy sleduje určitý konkrétny cieľ, ktorý je determinovaný potrebami súkromnej detektívnej činnosti.

Dezinformácia všeobecne znamená prienik nepravdivej správy. Detektívna dezinformácia je jednou z významných metód súkromnej detektívnej činnosti. Pri použití detektívnej dezinformácie je treba postupovať obozretne. Použitie metódy detektívnej dezinformácie je nutné dôkladne zvážiť i z hľadiska, či nedôjde k naplneniu skutkovej postavy niektorého trestného činu, napríklad šírenia poplašnej správy apod. s ohľadom na ciele súkromné detektívnej činnosti, na rozdiel od spravodajské činnosti, v ktorej sa uplatňuje ako jedna z metód spravodajskej dezinformácie, nie je detektívne dezinformácia v bežnej detektívnej činnosti príliš frekventovaná. V rámci súkromnej detektívnej činnosti nadobúda na význame s postupne sa rozvíjajúcim komerčným spravodajstvom. Môže pripadať do úvahy aj v niektorých prípadoch realizácie detektívneho rozpracovanie atd. Metóda detektívnej dezinformácia má rad spoločných rysov s metódou detektívne legendy, ale je na vyššom stupni; detektívne legenda je jednou z metód, ktoré detektívne dezinformáciu využíva. Na rozdiel od detektívnej legendy je detektívna dezinformácia vyšším stupňom infiltrácie nepravdivej správy a tiež je zložitejšia jej realizácie. Rovnako ako u detektívnej legendy je potrebné, aby časť dezinformujúcej správy bola pravdivá a tvorila základ detektívnej dezinformácie. Detektívna legenda je vlastne súčasťou detektívnej dezinformácie. Táto pravdivá časť dezinformácie a od nej sa odvíjajúca detektívne legenda tvoria základ detektívnej dezinformácie a sledujú určitý cieľ. Má za úlohu urobiť detektívnu dezinformáciu ako celok vierohodnou pre objekt, prostredie, osobu, ktorá je v záujme súkromnej detektívnej činnosti. Ak by detektívne dezinformácie nebudila dojem vierohodnosti, bola by bezcenná a jej infiltrácie k záujmovému objektu súkromnej detektívnej činnosti by bola nemožná, prípadne by priniesla opačný výsledok, než aký je sledovaný. Dezinformácie by sa tak stala pre zámery súkromné detektívnej činnosti bezcennou.

O detektívnej dezinformácii hovoríme ako o komplexnej metóde preto, že k realizácii tejto metódy je využívané ďalších metód súkromnej detektívnej činnosti. Ide najmä o

využitie metódy detektívneho informačného preniknutia a už spomínané metódy detektívnej legendy. Metóda detektívneho informačného preniknutia slúži na vytvorenie nosiča dezinformácie infiltrovaného do záujmového prostredia detektívnej činnosti. V tejto súvislosti sa vo spravodajskej a policajnej práci hovorí o vplyvovej agentúre a v rámci súkromnej detektívnej činnosti o vplyvových informátoroch - dezinformátoroch, ktorý môžu infiltráciu dezinformácie vykonávať vedome alebo nevedome. Najideálnejšie pre infiltráciu detektívnej dezinformácie je informátor, ktorý bol získaný ako informátor pre získavanie informácií, pričom sa o ňom súkromný detektív presvedčil, že tzv. dubluje, nedá to však poznať a využíva takéhoto informátora ako dezinformátora. Naproti tomu metóda detektívne legendy slúži ako základ dezinformácie. Priebeh detektívnej dezinformácie je potom spravidla monitorovaný-kontrolovaný ďalšími detektívnom metódami. Detektívna dezinformácia ako metóda súkromnej detektívnej činnosti sa odlišuje od detektívneho ovplyvňovania tým, že detektívny lobbing je širšieho obsahu. Detektívny lobbing je cieľom súkromnej detektívnej činnosti, naopak detektívna dezinformácia je jedným z prostriedkov - jednou z metód slúžiace k dosiahnutiu detektívneho ovplyvnenie, nie je ale metódou jedinou.

Metóda detektívneho informačného preniknutia v rámci detektívnej dezinformácie má osobitné postavenie. Spravidla jeden informátor-dezinformátor slúži na infiltrovanie dezinformácie do prostredia, ktoré je v záujme súkromnej detektívnej činnosti. Okrem toho ďalší informátor slúži na získavanie informácií o odozve detektívnej dezinformácie v záujmovom prostredí. Ide o zabezpečení tzv. spätnej informačnej väzby. [6]

Detektívna dezinformácia prebieha v niekoľkých fázach:

- Uvedomenie si zámeru sledovaného dezinformácie,
- Formulovanie detektívne dezinformácie,
- Vytipovanie dezinformačných nosičov a informačných zdrojov,
- Plán priebehu realizácie detektívnej dezinformácie,
- Vlastná realizácia detektívnej dezinformácie,
- Prienik nosiča dezinformácie a informačných zdrojov do záujmového, prostredia, ktorý je cieľovým objektom dezinformácie,
- Odovzdanie dezinformačných správ nosičmi dezinformácie,

- Infiltrácia dezorientačnej správy do záujmového prostredia,

- Získavanie spätnej väzby,

- Vyhodnotenie účinnosti infiltrovanej dezinformácie,

- Analýza informácií,

- Interpretácia informácií,

- Plán korekcie detektívnej dezinformácie,

-Korekcia priebehu detektívne dezinformácie a cyklus pokračuje opakovaním jednotlivých fáz.

3.4 Detektívna osobná ochrana

Metóda osobnej ochrany - bodyguard spočíva v zaistení bezpečnosti osôb a majetku. Jedná sa o špecifickú metódu detektívnej činnosti, ktorá je na rozhraní s ochranou majetku a osôb, tj. fyzickou ochranou alebo strážnou službou. Je vhodné porozmýšľať, či ide o súkromnú alebo komplexné metódu alebo o formu súkromnej detektívnej činnosti. V tomto prípade je hranica medzi metódou a formou značne strmá. Pretože osobné ochranu osôb - bodyguard chápeme z hľadiska foriem ako súčasť detektívneho dohľadu, potom osobné ochranu chápeme ako metódu. Ako komplexnú metódu ju chápeme preto, že v jej rámci sú využívané ďalšie metódy súkromnej detektívnej činnosti, a to metóda pozorovania, metóda extrakcie apod., nekonzistentnosti v posúdení, či ide o metódu alebo formu, potom vyplýva z toho, že jednotlivú úkonom tejto metódy je spravidla aj detektívne previerka osoby, čo je forma súkromnej detektívnej činnosti. [6]

Praxe a od nej odvodené teórie osobnej ochrany- bodyguard rozlišuje nasledujúce spôsoby osobné ochrany:

- osobná ochrana s predchádzajúcou prípravou:

Pre výkon osobnej ochrany vykonávané súkromnú detektívnu službou s predchádzajúcou prípravou je treba sa predovšetkým zaoberať:

- Osobnosťou chránenej osoby,

- Trasou pohybu či miestom pobytu,

- Operatívne bezpečnostnou situáciou na trase presunu alebo miestom pobytu chránenej osoby,

- Vozidlom presunu osoby z hľadiska výhod a nevýhod a z hľadiska bezpečnosti a ochrany bezpečnosti osoby.

- osobná ochrana bez predchádzajúcej prípravy:

Pre osobnú ochranu chránenej osoby, je ak treba ju zabezpečovať bez predchádzajúcej prípravy, je potrebné si aspoň na začiatku zistiť a v priebehu dopĺňať:

- Informácie o chránenej osobe,

- Rámcový program chránené osoby,

- Riziká nebezpečenstvo napadnutia chránenej osoby apod.

3.5 Detektívne osobné pátranie

Detektívne osobné pátranie je potrebné chápať ako sústavnú činnosť súkromného detektíva realizovanú pre každodenné činnosti. Jedná sa o najčastejšie používanú kombinovanú metódu súkromnej detektívnej činnosti. V jej rámci súkromný detektív priamo a bezprostredne užíva všetky detektívne prostriedky a postupy za účelom získania informácií, informácií o dôkazoch, veciach a písomnostiach, ktoré by v budúcnosti mohli slúžiť ako dôkazy apod. Ide teda o jeden zo spôsobov využívaných súkromnými motívmi v napĺňaní obsahu jednotlivých foriem súkromnej detektívnej činnosti. Detektívne pátranie plní špecifickú funkciu v rámci realizácie okrem detektívnej činnosti. Detektívnemu osobnému pátraniu rovnako ako každému systému prináleží aj tu množina prvkov, ktorými sú jednotlivé ďalšie metódy súkromnej detektívne činnosti, a to vrátane metód kombinovaných, prostriedky, pomocnej sily, ktorej integráciou sú nové vlastnosti, ktoré jednotlivé prvky, z ktorých sa systém skladá, samy o sebe nemajú.

Z tohto pohľadu je možné detektívne osobné pátranie považovať za prioritnú a najvýznamnejšiu kombinovanú metódu súkromnej detektívnej činnosti. Detektívne osobné pátranie je metódou činnosti každého jednotlivého súkromného detektíva, ide o jeho každodennú činnosť. Rovnako ako každej metóde, vrátane systémov sociálnych, prislúcha i kombinovanej metóde detektívnemu osobnému pátraniu určité znaky[6]:

- Zlostnosť,

- Súbor špecifických prvkov,

- Špecifický charakter integrácie s okolím.

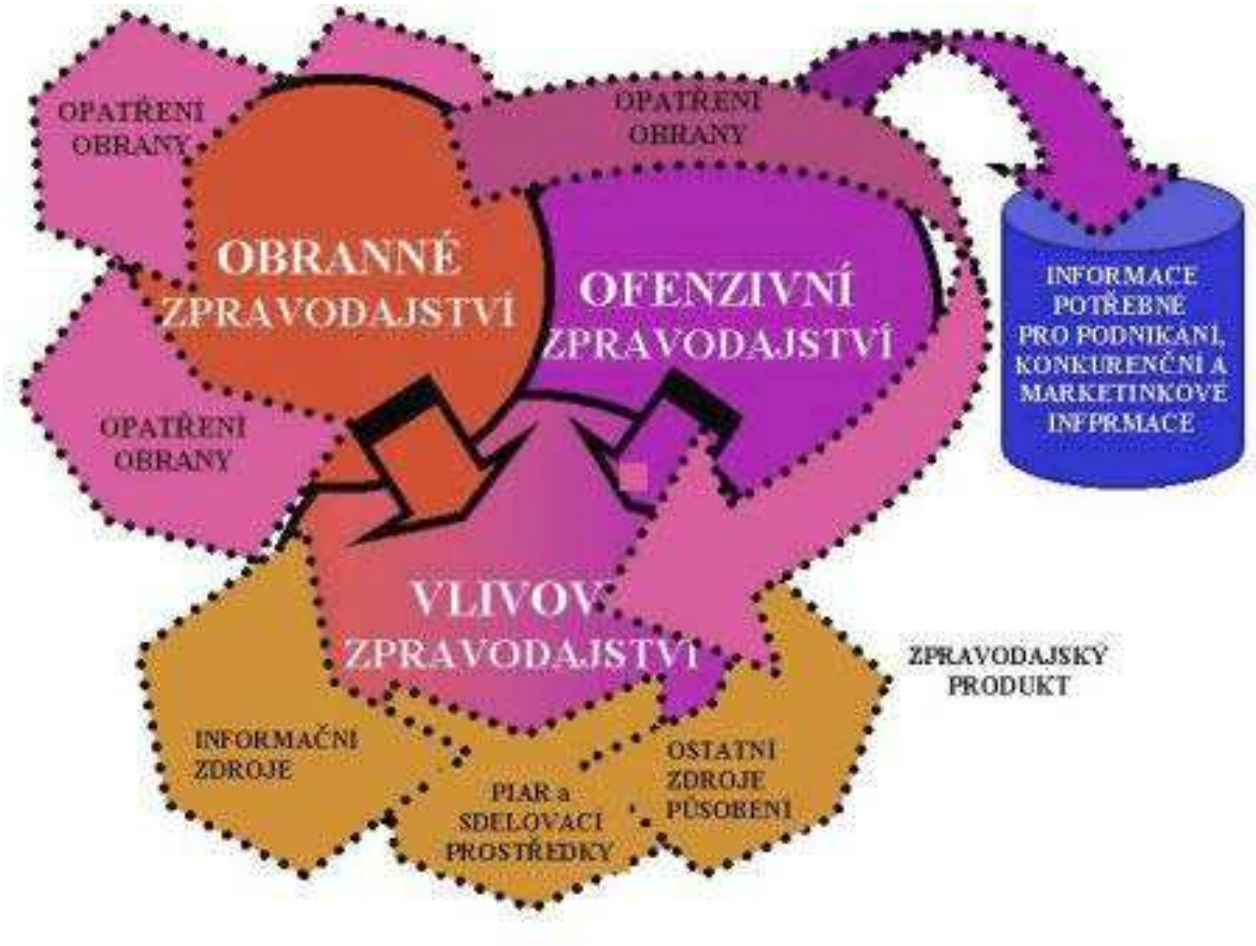
Súkromný detektív pri detektívnom osobnom pátraní využíva najmä nasledujúcich metód súkromnej detektívnej činnosti:

- Detektívne pozorovanie,
- Detektívne vyťažovanie,
- Detektívne vyťažovanie a vyhodnocovanie evidenciou, registráciou, archívov a pod,
- Detektívne vyhodnocovanie dokumentov,
- Vyšetrovacie metódy hodnotenia stop apod.

Detektívne osobné pátranie využíva súkromný detektív najmä na dosiahnutie nasledujúcich cieľov:

- Na získanie informácií a aktualizáciu operačnej situácie, k prehĺbeniu a doplneniu osobnej a miestnej znalosti,
- Na získanie prvotných informácií pre rozhodovanie v procese prípravy a realizácie ďalších metód súkromnej detektívnej činnosti,
- Na získanie spätnej väzby prípravy a realizácie krokov, úkonov a opatrení súkromné detektívnej činnosti,
- K priamemu naplňovaní jednotlivých foriem súkromnej detektívnej činnosti, v ich jednotlivých konkrétnych prípadoch. [6]

4 FORMY KOMERČNÉHO SPRAVODAJSTVA



Obr. 10. Formy KS

4.1 Obranné spravodajstvo

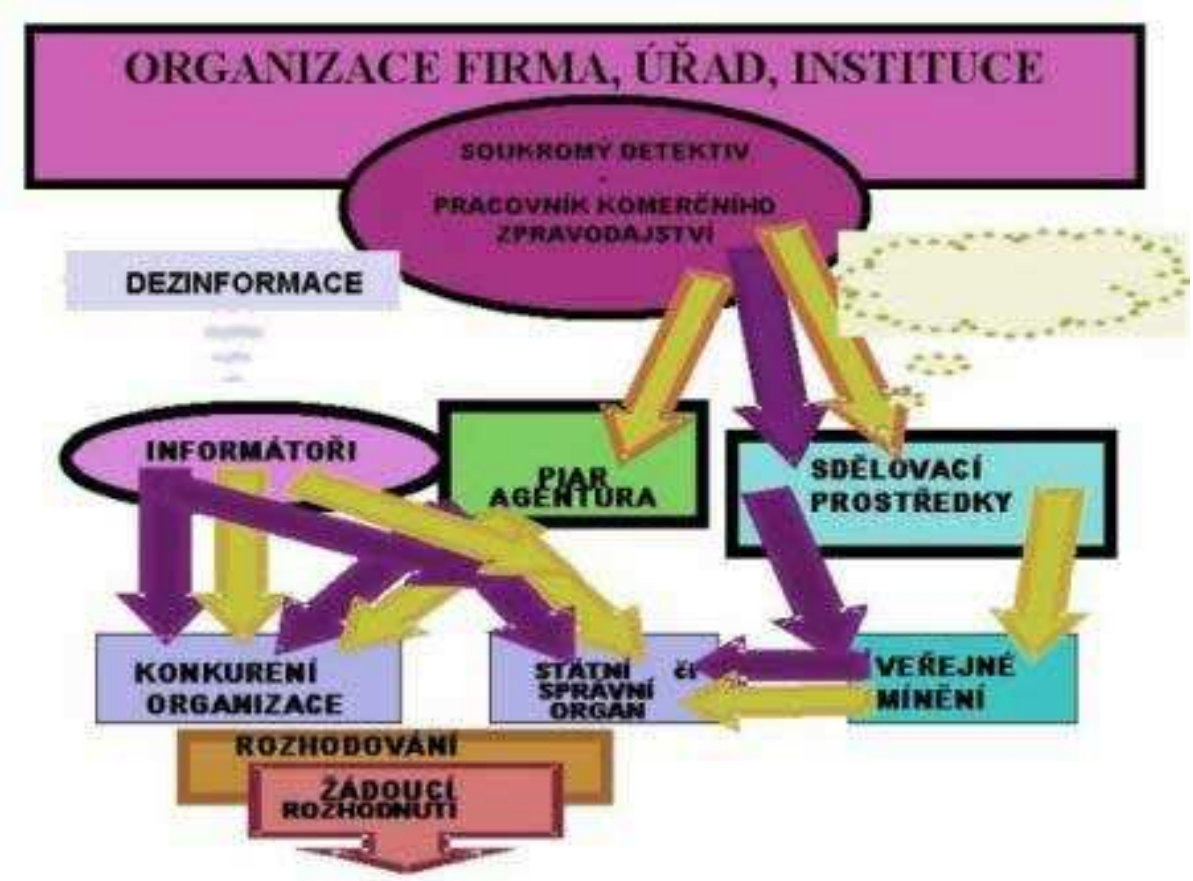
Obranné konkurenčné spravodajstvo predstavuje spôsoby a metódy, ktoré sa využívajú pri ochrane záujmovej firmy. Môžeme tiež nazvať ako defenzívne konkurenčné spravodajstvo.

Ochrana informácií a celkovej bezpečnosti podniku je komplexný a systémový problém. Nejedná sa o využitie len jednej metódy ale o komplikovaný systém ochrany tvorený množstvom subsystémov. Cieľom je komplexne zabezpečiť bezpečnosť podniku.

Obranné respektíve defenzívne pojatie konkurenčného spravodajstva je vlastne reakcia firmy na už vzniknutú situáciu na trhu, a to tak, že daná spoločnosť je prinútená reagovať na momentálne hrozby prípadne reagovať na vzniknutú príležitosť.

- Bezpečnostná politika podniku – jedná sa o súhrn pravidiel pre dosiahnutie stanovených cieľov pri ochrane informácií, bezpečnosti, majetku a osôb. Tvorí

základ pre efektívne využitie všetkých bezpečnostných opatrení a jej presadenie je nevyhnutné pre ich správne fungovanie. Z hľadiska riadenia podniku sem patria informácie o ohrození podniku, stanovenie bezpečnostných, odborných, prevádzkových i obchodných rizík, návrhy a koncepcie k ochrane podniku v rámci technických, technologických, organizačných, personálnych a informačných problémov. Stanovenie bezpečnostnej politiky podniku je jedným z najdôležitejších dokumentov podniku a je taktiež súčasťou riadiacich dokumentov manažmentu.



Obr. 11. Obranné spravodajstvo

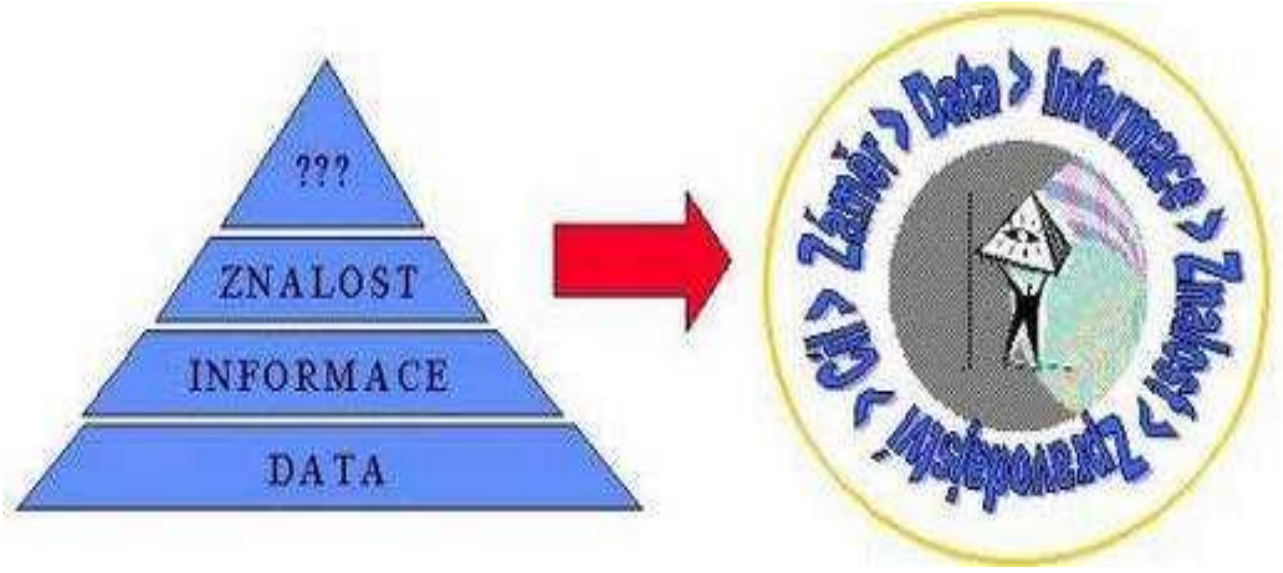
4.2 Ofenzívne konkurenčné spravodajstvo

Býva často označované ako ofenzívne alebo útočné konkurenčné spravodajstvo. Podstatou aktívneho konkurenčného spravodajstva je využitie spravodajských postupov, metód a prostriedkov k odhaleniu stratégie, citlivých inforamácií, know-how, obchodného tajomstva a pod. konkurenčných firiem a ich následné využitie pre potreby a k získaniu konkurenčnej výhody vlastnej spoločnosti.

Informácie pochádzajúce z tohto druhu spravodajskej činnosti môže využiť vedenie firmy počínajúc strednými manažérmi k pristúpeniu opatrení proti konkurencii, ochrane vlastných záujmov a zámerov. Pri ofenzívnom spravodajstve je dôležité presne špecifikovať oblasť záujmu aby sa mohli operatívny pracovníci sústrediť na hľadanie relevantných informácií.

Pri ofenzívnom konkurenčnom spravodajstve je veľmi dôležité riadiť sa etickými a právnymi zásadami aby sa predišlo možnému nelegálnemu konaniu, pretože množstvo metód výhodných a vhodných pre konkurenčnú špionáž sú v rozpore zo zákonom.

Ofenzívne pojatie konkurenčného spravodajstva znamená vytvoriť spravodajskú aktivitu či iniciatívu za účelom dosiahnutia svojich cieľov, predstáv a zámerov a svojim tlakom ovplyvniť marketingový trh tým, že konkurenčné spoločnosti sú prinútené jednať a tým nútiť konkurenčné firmy k činnostiam , ktoré neumožnia uskutočnenie ich cieľov a zámerov , ktoré by mohli ohroziť činnosť našej spoločnosti.



Obr. 12 Ofenzívne spravodajstvo

4.3 Vplyvové konkurenčné spravodajstvo (lobbing)

Vplyvové konkurenčné spravodajstvo je súbor metód, činností a foriem, ktorých cieľom je formou ovplyvňovania, nátlaku, dezinformácií ale aj prostého presvedčovania a prezentácie informácií dosiahnuť priaznivej situácie a podmienok pre rozhodnutie podnikateľských subjektov. Je to vlastne komunikácia za účelom zistenia presných úmyslov daných osôb, spoločnosí atd. a poprípade ovplyvnenie zámerov osôb, spoločností atd. v prospech klienta.

Túto činnosť vykonávajú prezentačne zdatné osoby, ktoré majú talent ovplyvniť záujmovú osobu behom veľmi krátkeho času. Využívajú sa hlavne metódy presvedčovania a argumentácie, demonštratívne metódy a dezinformácie.

II. PRAKTICKÁ ČASŤ

5 OCHRANA KNOW-HOW POMOCOU DEFENZÍVNEHO SPRAVODAJSTVA

Agresívna situácia dnešnej podnikateľskej sféry si vyžaduje mimoriadnu pozornosť a dôslednosť v ochrane know-how, obchodného tajomstva a iných pre spoločnosť dôležitých alebo citlivých informácií. Pre efektívnu ochranu musia byť prevedené opatrenia krátkodobého, stredne-dlhého a dlhodobého charakteru. Významnú časť zastupujú najmä režimové opatrenia technické prostriedky a taktiež služby súkromných detektívov so špecializáciou na poli prenikania do priestorov záujmu. Jedným z najnebezpečnejších aspektov v probléme ochrany know-how je využitie rôznych foriem odposluchov. Tomuto problému sa čelí najmä prísnymi režimovými opatreniami a obranno- technickými prehliadkami .

5.1 Aktívne a pasívne formy defenzívneho spravodajstva

Cieľom defenzívneho spravodajstva je snaha o minimalizáciu zverejnenia pre firmu citlivých dát a informácií , ktoré sa snaží získať a následne využiť pre svoj osoh konkurencia. Defenzívne spravodajstvo je súhrn foriem a metód ktorých cieľom je efektívna kontrola a analyzovanie informácií vzniknutých v spoločnosti, kontrola ich zverejňovania a taktiež ich samotnou ochranou. Oddelenie spoločnosti zaoberajúce sa defenzívnym spravodajstvom by malo byť samostatné a nemalo by spadať pod napr. marketingové alebo obchodné oddelenie ako je tomu v bežnej praxi.

Základné aktivity defenzívneho spravodajstva :

- **Technické zabezpečenie ochrany informácií** – Jedná sa o klasické zabezpečenie spoločnosti ako napríklad MZS, EZS, fyzická ostraha objektu, CCTV, ACS, atd.

- **Bezpečnosť emitovania informácií** – Jedná sa o snahu kontrolovať, minimalizovať a filtrovať informácie vytvorené domovskou spoločnosťou, resp. Minimalizovať možnosti zneužitia informácií konkurenciou.

- **Aktívne defenzívne spravodajstvo –** Jedná sa o protirozvedné spravodajstvo alebo inak povedané kontrašpionáž. Cieľom je lokalizovať a zabrániť konkurenčnej spravodajskej aktivite.

5.2 ochrana know-how za využitia aktívneho defenzívneho spravodajstva

Podstatou aktívneho defenzívneho spravodajstva je súbor postupov či už sa jedná o metódy, formy alebo prostriedky , ktorými je možné odhaliť konkurenčnú spravodajskú aktivitu. Ide o systém opatrení snažiacich sa zabrániť konkurenčnému ofenzívnemu spravodajstvu. Informácie získané za využitia aktívneho defenzívneho spravodajstva o činnosti, stratégii a cieľoch konkurenčnej snahy o spravodajskú činnosť sa využijú pre potreby nastavenia a stratégie obranného spravodajstva firmy. Na základe takto získaných informácií je možné efektívnejšie voliť opatrenia, využívať detektívnej dezinformácie a pod. . K aktívnemu defenzívnemu spravodajstvu sú využívané metódy ofenzívneho spravodajstva s pozmeneným cieľom záujmu – cieľom spravodajskej činnosti totiž nie je obchodné tajomstvo, know-how, utajované skutočnosti a pod. Konkurenčnej firmy ale práveže jej oddelenie ofenzívneho spravodajstva prípadne spravodajská agentúra, kancelária, spoločnosť konkurenčnou firmou najatá.

Vzhľadom k tomu, že sú využívané hlavne formy ofenzívneho spravodajstva je nutné dodržovať legálnosť a etiku nášho jednania .

5.2.1 Metódy aktívnej ochrany know-how

Pri aktívnej ochrane know-how využívame rôznych metód súkromnej detektívnej činnosti a metód používaných pri komerčnom spravodajstve. Jedná sa hlavne o metódy, ktoré sa využívajú pri ofenzívnom spravodajstve, respektíve ofenzívnom konkurenčnom spravodajstve ale s tým rozdielom, že cieľové informácie nie sú z oboru výrobných tajomstiev, know-how, obchodného tajomstva a pod. konkurenčných firiem. Zameriavame sa práveže na oddelenie konkurenčného spravodajstva iných firiem prípadne na firmy ktoré tieto spravodajské služby konkurenčným firmám poskytujú. Hlavným cieľom aktívneho defenzívneho spravodajstva je monitorovanie spravodajskej činnosti konkurencie, zisťovanie ich stratégie, dezinformovanie a akékoľvek narušenie procesu konkurenčnej spravodajskej činnosti. Všetky tieto zámery , metódy a procesy sledujú ochranu záujmov vlastnej spoločnosti.

Pri aktívnej ochrane know-how (taktiež obchodného tajomstva, citlivých informácií atd.) využívame informácií z primárnych a sekundárnych zdrojov.

- Informácie získané z primárnych informačných zdrojov : Tieto informácie sú získavané za použitia metód a prostriedkov spravodajskej práce. Využívajú sa rôzne druhy metód a foriem súkromnej detektívnej činnosti a spravodajských technológií ktoré sú popísané v teoretickej časti práce. Ide napríklad o detektívne pozorovanie, informačné preniknutie atd.
- Informácie získané zo sekundárnych informačných zdrojov : Informácie sú získavané z médií, internetu, veľtrhov , voľne dostupných produktov konkurencie atd.

Metódy, ciele a okruhy aktívneho defenzívneho spravodajstva :

- **Využitie metód súkromnej detektívnej činnosti:** využitie detektívnych foriem a metód popísaných v teoretickej časti práce (najmä ofenzívneho spravodajstva) pre aktívne získavanie informácií o konkurenčnom spravodajstve, jeho stratégií, zámeroch a cieľoch.
- **Zabezpečenie personálnej bezpečnosti:** Jedná sa o zabezpečenie bezpečnosti a lojality stávajúcich zamestnancov spoločnosti. Cieľom je zabrániť kontaktovaniu, vyťažovaniu, vydieraniu a uplácaniu stávajúcich zamestnancov firmy ale taktiež zabrániť prieniku konkurenčných agentov do našej spoločnosti (hlavne vo forme fingovaného zamestnania).
- **Aktívne vyhľadávanie konkurenčnej spravodajskej techniky:** Jedná sa o proces vyhľadávania konkurenčnej spravodajskej techniky za pomoci špeciálnych metód, technológií a techniky k tomu určenej.
- **Aktívne zabránenie používania konkurenčnej spravodajskej techniky:** Jedná sa o využitie špeciálnej techniky určenej na aktívne rušenie už nainštalovanej spravodajskej techniky.
- **Aktívna ochrana proti dezinformáciám:** Jedná sa o aktívne narušovanie konkurenčných dezinformačných kampaní.
- **Aktívna ochrana proti lobbingu (vplyvového spravodajstva) konkurencie:** Jedná sa o narušenie konkurenčných public relations (PR) kampaní.

5.3 Ochrana know-how za použitia pasívneho defenzívneho spravodajstva

5.3.1 Režimové opatrenia

Jedná sa o zavedenie systému režimových opatrení v rámci podniku alebo objektu ktorých cieľom je usporiadanie vzťahov medzi zamestnancami, ich činnosťami a právami za účelom minimalizovania prieniku nežiaducich osôb do záujmových oblastí. Pri obmedzení pohybu zamestnancov a osôb po pracovisku spolu s identifikáciou jednotlivých osôb v dôležitých priestoroch za použitia napr. Rôznych druhov priepustiek, časových obmedzení, priestorových obmedzení osobných obmedzení pre vstup, farebné odlíšenie oblečenia pre vstup a zdržovanie sa vo vyhradených priestoroch, vstup a výstup určitým priestorom , vstup cez priepust alebo filter. Takéto režimové opatrenia značne sťažujú inštaláciu odpočúvacieho vybavenia, ktorá býva často náročná, taktiež sťažuje nepozorovanú infiltráciu nežiaducim osobám do objektu. Pri režimových opatreniach je dôležité dodržovanie kľúčového režimu, identifikácia a kontrola osôb (vrátane servisných alebo upratovacích služieb) , pravidelné obranno-technické prehliadky (OTP) ako aj náhodné OTP, utajenie termínu OTP, využitie bezpečnostných systémov v záujmových priestoroch. [5]

5.3.2 Obranno-technická prehliadka (OTP)

Pre dosiahnutie maximálnej efektivity je nutné OTP prevádzať v pravidelných intervaloch, napr. raz za štvrťrok alebo polrok, taktiež je vhodné vykonať prehliadku v náhodnom termíne. Prvým krokom OTP je zabránenie prenikaniu konkurenčného spravodajstva , tento krok pozostáva z vyhľadávania technických prostriedkov špionáže za pomoci špeciálnej techniky. Druhým krokom je organizačné a technické zabezpečenie už ošetreného záujmového priestoru proti opätovnému infikovaniu odpočúvacím alebo monitorovacím zariadením. [5]

Druhy OTP : - Fyzická prehliadka

- Rádiová prehliadka
- Kontrola nelinearít

5.3.3 Taktické zásady OTP

- zahájenie prehliadky v čase, kedy sa predpokladá aktivácia odpočúvacích zariadení (napríklad v priebehu rokovania)
- niektoré odpočúvacie zariadenia môžu byť diaľkovo ovládané a predstieranie rokovania nám môže zabezpečiť aktiváciu týchto prostriedkov
- všetky následné prehliadky by sa mali vykonávať v náhodných intervaloch,
- vyhľadávanie sa musí vykonávať skrytým spôsobom. Porady s kolegami, alebo technikmi, fingované začatia prehliadky, nastavenie prístrojov, lokalizácia zariadení nesmie dať tomu, kto odpočúvanie vykonáva informáciu o realizácii OTP alebo o jeho odhalení.
- úspech pri vykonávaní prehliadky je závislý na vybavení, odborných vedomostiach a svedomitosti, ktorá je vyhľadávaniu venovaná.
- Ak si prehliadku vykonávate sami je nutné sa pred vlastným začatím vyhľadávania dôkladne sa zoznámiť s jednotlivými detekčnými metódami a možnosťami prístrojov. Tieto nácviky vyhľadávania je potrebné vykonávať tajne a zásadne na bezpečných miestach
- Najväčšiu pozornosť je potrebné venovať oblasti, kde sa odohrávajú dôležité rozhovory (za písacím stolom, blízko telefónneho prístroja). Najväčšie množstvo odposluchov bude umiestnených v okruhu 7m z dôvodu dobrého hlasového príjmu
- Je potrebné vytvoriť vhodné podmienky pre prehliadku, zatiahnuť všetky závesy – (eliminácia možnosti pozorovaní), zapnúť všetky svetlá a niektoré ďalšie prístroje z dôvodu vytvorenia bežného pracovného prostredia.

5.3.4 Dátová bezpečnosť

Jedná sa o zabezpečenie počítačových sietí a dát či už softwarovej alebo hardwarovej úrovni. Cieľom je vytvorenie takého informačného systému, ktorý minimalizuje možnosť úniku a zneužitia informácií a v prípade, že by takýto stav nastal o čo najskoršie napravenie problému a vystopovaniu vinníka. Bezpečnosť je chápaná ako komplexné zaistenie systému. Záujmovú oblasť predstavuje prístup do systému, editácia hodnôt a dát , vytváranie záloh, antivírovú ochranu a ďalšie aspekty daného informačného systému.

Bezpečnostný informačný systém definujeme ako systém chrániaci informácie behom ich vstupu, spracovania, uloženia, prenosu a výstupu proti strate dostupnosti, integrity a dôveryhodnosti.

Je nutné si uvedomiť, že pri zabezpečovaní informačných systémov nie je možné dosiahnuť úplnej bezpečnosti, len mieru pre nás akceptovateľného rizika.

Informačné systémy ich aktíva môžu byť cieľom pôsobenia rôznych nebezpečí. Môže sa jednať o ľudí, vrátane vlastných zamestnancov, udalosti spôsobené prírodnými javmi (požiar, voda, zásah blesku). Poruchy techniky (výpadok prúdu, porucha zariadenia). Ďalšou formou nebezpečenstva predstavujú agenti konkurenčnej spravodajskej činnosti, teroristi, organizovaný alebo samostatný kriminálnici a počítačový nadšenci. Od útočníka môžeme očakávať akýkoľvek druh útoku vrátene napríklad útoku na najsilnejšie miesto systému. Pri fyzickom poškodení systému bývajú následky okamžite identifikovateľné z dôvodu nefunkčnosti celého systému alebo jeho časti. Pri nelegálnom úniku informácií je ale situácia diametrálne odlišná, pokiaľ totižto nie sú informácie zjavne použité, je takmer nemožné dokázať vinu. Ďalším aspektom je to , že vlastník informačného systému je neochotný takýto únik alebo jeho rozsah priznať z dôvodu poškodenia povesti. [9]

Dátová bezpečnosť sa zabezpečuje radou protiopatrení, ktoré majú formu :

- Administratívnu – upravenie prístupových práv, editovanie dát
- Logickú – upravenie a natavenie prístupových práv
- Fyzickú – ochrana objektu, zabránenie prístupu nepovolaných o.
- Technickú - kryptografické systémy, diskové polia

5.3.5 Technická ochrana objektu

Jedná sa o klasické formy zabezpečenia objektu za použitia technických alebo systémových riešení bezpečnostného priemyslu ako sú :

- Mechanické zábranné systémy
    - Mreže
    - Zámky a bezpečnostné uzamykacie systémy
    - Závory
    - Rolety
    - Úschovné objekty
    - Ploty
    - Bezpečnostné dvere
    - Bezpečnostné fólie a sklá
- Elektrické a elektronické zabezpečovacie systémy
    - Elektrická zabezpečovacia signalizácia
    - Elektrická požiarna signalizácia
    - Systémy CCTV
    - ACS systémy
    - Perimetrické systémy
    - Zabezpečenie sietí a prostriedkov
    - Pulty centralizovanej ochrany (PCO)

5.3.6 Ochrana utajovaných informácií

Ochrana utajovaných informácií podlieha zákonu 412/2005 Sb o ochrane utajovaných informácií a o bezpečnostnej spôsobilosti. Jedná sa o také informácie, ktorých zverejnenie alebo použitie by mohlo poškodiť osobu fyzickú alebo právnickú, inštitúciu alebo štát. Záujem na chránení tejto informácie vyjadruje subjekt zavedením rôznych bezpečnostných opatrení vrátane stíhania osoby, ktorá informáciu scudzila, zneužila alebo zverejnila.

6 OPERATÍVNA (SPRAVODAJSKÁ) TECHNIKA VYUŽÍVANÁ V KOMERČNOM SPRAVODAJSTVE

Jedná sa o rôzne technické pomôcky určené alebo využívané pri spravodajskej činnosti. Do technických prostriedkov môžeme zaradiť techniku pre skryté získavanie informácií audieo, video alebo dátového charakteru. Môže sa jednať o odpočúvacie zariadenia, magnetofóny, videokamery, fotoaparáty atd. . ale taktiež sme patria technické pomôcky ako sú planžety na bezkľúčové otváranie zámkov, prístroje pre nočné videnie, termokamery atd.

Do kategórie spravodajských prostriedkov taktiež patria prístroje určené na komunikáciu a technickú výbavu pre získavanie informácií z informačných technológií, cieľového objektu atd.

Jedna z najnebezpečnejších foriem komerčného spravodajstva je odpočúvanie. Môžeme rozlíšiť či ide o odpočúvanie priestorové alebo o odpočúvanie konkrétneho rozhovoru, toku dát po rôznych druhoch sietí (telekomunikačná, GSM, Lan, atd.)

Riziká možného nasadenia operatívnej techniky za účelom komerčného spravodajstva je na dnešnom trhu kde prevládajú agresívne praktiky veľmi reálne. Ďalším elementom sú relatívne nízke postihy za napríklad odposluch osôb pretože v ČR je za trestný čin klasifikované len odpočúvanie telefónnych hovorov, zatiaľ čo akákoľvek iná forma odpočúvania je klasifikovaná len ako previnenie sa voči listine základných práv a slobôd občana. [5]

Spravodajskú techniku môžeme rozdeliť na :

- Akustické systémy
- Optické systémy
- Techniku na odposluch dát a monitorovanie informačných technológií

6.1 Akustické systémy

Jedná sa o technické systémy umožňujúce skrytý audio odposluch. Systém audio odposluchu je taký systém ktorý prevádza zvukové vlny rozhovoru na elektrické signály a vysiela ich pomocou rádiovĺn, drátového vedenia alebo svetelného lúča k prijímaču.

Využívajú sa :

- **Mikrofóny** : Ide o klasickú odposluchovú techniku, ktorej širšie využitie umožnili nové technológie a rozvoj nahrávacích systémov. Súčasná miniaturizácia v mikrofónovej technike umožňuje takmer neidentifikovateľnosť mikrofónu v miestnosti, vyžaduje však drôtové prepojenie a samozrejme prídavné elektronické zariadenia. Tiež inštalácia mikrofónov ako odposluchového zariadenie je neatraktívna, vyžaduje určité technické znalosti, hlavne potrebný čas pre ich skrytú montáž. K dosiahnutiu kvalitného odposluchu treba takisto vhodné umiestnenie mikrofónu. Čím bližšie je mikrofón u hovoriacej osoby, tým je odpočúvanie kvalitnejšie. Takisto nesmieme zabudnúť na akustiku miestnosti k vylúčeniu nežiaduceho brumu a takisto umiestnenie zdrojov sieťového napätia. [5]
    - Elektromagnetické mikrofóny
    - Piezoelektrické mikrofóny
    - Uhlíkové mikrofóny
    - Elektrostatické mikrofóny
    - Elektretové mikrofóny
- **Špeciálne mikrofóny :** Mimo klasické vyššie popísané druhy mikrofónov, ktoré sú bežne dostupné v obchodnej sieti sa k monitorovaniu miestnosti používa aj špeciálne upravených alebo skonštruovaných mikrofónov. Najznámejšie sú kontaktné mikrofóny. Princíp činnosti je jednoduchý - akustický tlak vznikajúci pri hovore v miestnosti rozochvieva múr, dvere a okenné tabuľky a pripojený mikrofón (Vlastne piezoelektrický kryštál) je schopný toto chvenie sňať. Kvalitné kontaktné mikrofóny snímajú vibrácie stien i niekoľko desiatok centimetrov hrubých. Prenosové vlastnosti pevných materiálov sú nevypočítateľné a treba skusmo nájsť na stene vhodné miesto, kde je počuteľnosť a zrozumiteľnosť hovoru najväčšia. Snímacia kvalita kontaktného mikrofónu možno vylepšiť predvŕtaním malej dierky do steny na strane počúvania a k mikrofónu prilepiť kúsok skrutky alebo klinca. [5]

- Akustický stetoskop
- Elektronický stetoskop
- Optický mikrofón

- **Diaľkové smerové mikrofóny:** Základným druhom diaľkových mikrofónov sú mikrofóny parabolické, založené na princípe parabolickej odrazovej plochy a koncentrácie akustickej energie do ohniska paraboly. Uvedený mikrofón má veľkosť a tvar bežnej satelitnej antény, iba v ohnisku paraboly nie je konvertor, ale kvalitný mikrofón spojený s citlivým zosilňovačom. Odporúčaná veľkosť paraboly je 70cm a účinok mikrofónu je do vzdialenosti asi l00m. Parabolický mikrofón však sníma všetky zvuky, ktoré sú na trase sledovania. Ideálne použitie mikrofónu je na otvorenom priestranstve s nízkym okolitým hlukom, napr. v parku, v lese, na lúke alebo na ihrisku. [5]
- **Zvláštne druhy odposluchu**
  - Laserový odposluch
  - Pasívny rezonátor
  - Kryštalický rezonátor
  - Mems rezonátor
- **Telefónne odposluchy:** Telefónne slúchadlo, respektíve telefónny prístroj, je vďačným miestom ukrývanie odpočúvacích zariadení. Telefón je takmer v každej kancelárii a každej domácnosti a je spravidla spojený s okolitým svetom štvoržilovým drôtovým vedením. Aj keď v súčasnej dobe prežíva boom bezdrôtový telefón, stále sú drôtové systémy v prevádzke. Pre odposluch je výhodné aj umiestnenie telefónneho prístroja blízko zóny, kde sa najčastejšie vedú rozhovory, najmä v kanceláriách firiem. Skrátka použitie telefónu, alebo drôtového alebo bezdrôtového, je ideálne riešenie. Telefónny prístroj je použiteľný na odpočúvanie dvoma spôsobmi. Môžeme priamo odpočúvať telefónny rozhovor alebo využiť telefónneho prístroja na monitorovanie miestnosti. [5]
- **Odposluch mobilných telefónov:** Je jasné, že príslušné technické prostriedky pre monitorovanie hovorov v mobilných sieťach v ČR existuje a sú v majetku privátnych firiem, často ani neregistrovaných, v asociáciách bezpečnostných služieb. Dozorné a kontrolné mechanizmy zodpovedných inštitúcií ani operátorov však nedisponujú zariadením, ktoré by umožnilo preukázať nasadenia odpočúvacích systémov v praxi. K odpočúvania v mobilnej sieti môže dôjsť buď

monitorovaním prevádzky operátora alebo aj vo vzduchu a následným dešifrovaním signálu, čo je technicky výrazne komplikovanejšia, avšak pre realizátora tejto činnosti ďaleko bezpečnejšia metóda. [5]

- **Drátový odposluch telefónnej linky:** Je evidentné, že v starých zástavbách môže byť, najmä v bývalých budovách firiem, ešte aj zostatková montáž drôtového odpočúvania, ktorá tu zostala pre nedostatok času ju odstrániť a ktorá môže byť opätovne využitá, pri jej náhodnom nájdení príslušnou odbornou firmou alebo jednotlivcom. Základný spôsob Odpočúvania telefónneho hovoru je priame napojenie citlivého zosilňovača alebo nahrávača na prívodnú linku označenú a / b, farebne je to hnedý a biely vodič. Technicky nie je podstatné, v ktorom mieste trasy telefónne linky sa na vedenie napojíte. Záleží iba na možnostiach prístupu k jednotlivým uzlom káblovej trasy (pozor teda pri organizovaní OTP a pri kontrole starých vedení v starých zástavbách teraz využívaných firmami). Musí sa však vždy ísť o vedenie prislúchajúce iba jednej telefónnej linke, a to tej, ktorú chceme monitorovať a kde je signál v analógovej podobe. Nemožno túto techniku použiť za koncentrátorom, kde dochádza k digitalizácii a kde sa zlučuje Niekoľko telefónnych liniek na jeden pár[5]

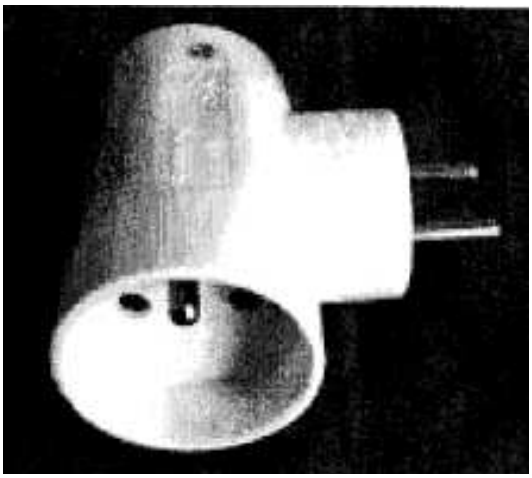
- **Rádiové systémy odposluchu telefónnej linky:** Nie vždy je možné napojiť sa na telefónne vedenia mimo odposluchový priestor. Potom nezostáva nič iného, než napojiť telefónnu linku priamo v účastníckej zásuvke alebo v telefónnom prístroji a skrytý nahrávač prepojiť drôtovým vedením. Pravidelná kontrola nahrávky nie je vhodná a preto sa volí spôsob, ktorý prenáša telefónny hovor vzduchom po rádiových vlnách. Používajú sa miniatúrne rádio vysielače. Miesto mikrofónu je tu ale adaptér napojený na telefónnu linku. Napájanie rádio vysielačov je možné z batérie, alebo možno použiť napätie 60V z telefónnej siete. Klasická telefónna ploštica je krabička s rozmermi približne 10x5x3mm s dvoma drôtiky na pripojenie. Telefónne vedenie nahrádza zdroj signálu, mikrofón, napájací zdroj aj anténu. Kvalitnejšie telefónne rádio vysielače sú dvojkanálové. Jeden kanál sníma a vysiela telefónny hovor, druhý sníma zvuky z miestnosti. Rádio vysielače môžeme napojiť na telefónnu linku dvoma spôsobmi. Paralelne, kedy sa telefónna linka rádio vysielača premostí, a sériovo, kedy je prerušený

prívodný drôt a drôt telefónne linky a prepoja sa cez vysielač. Paralelný spôsob zapojenia je premostenie dvoch aktívnych vodičov, pripojovacie drôtiky rádio vysielača sa napoja na hnedý a biely vodič (a,b drôt) telefónnej linky kdekoľvek po trase vedenia. Výhodou paralelného zapojenia proti sériovému je menšia spotreba prúdu (a tým aj menšia možnosť odhalenia). Má možnosť napojenia kdekoľvek na trase telefónne linky a pritom monitoruje akúkoľvek prípojku alebo podvojku, ktorá môže byť na linke trebárs aj dodatočne pripojená. Sériový spôsob využíva sériového zapojenia rádio vysielača, kedy sa prenáša biely (a drôt) vodiča a prepoja s rádio vysielačom. Pre typ zapojenia sa nemožno ľubovoľne rozhodnúť, každé zariadenie je určené vždy len pre jeden spôsob zapojenia na telefónne linku. U oboch zapojení je vysielač konštruovaný tak, že po zdvihnutí slúchadla začne automaticky vysielať rádiový signál. Pre napojenie a tým aj úkryt rádio vysielača sa môže u klasického telefónu zvoliť niekoľko možností. Napojenie môže byť vykonané priamo vo slúchadle, v telefónnom prístroji, v účastníckej zásuvke alebo v pobočkovej ústredni. Pre zamedzenie ľahkému odhaleniu telefónneho vysielača začali byť vyrábané priamo v tvare mikrofónu alebo slúchadlovej vložky, alebo v tvare súčiastok používaných v telefónnom prístroji. [5]

- **Záznamníky telefónnych hovorov:** Zaujímavý spôsob odpočúvania využíva záznamníky telefónnych hovorov umiestnené v odpočúvanom priestore, záznamníky v telefónnych a faxových prístrojoch. Ponúkajú možnosť vyberania odkazov diaľkovo, po telefónnej linke. Umožňujú jednoduchým stlačením tlačidla tónovej voľby prehrávať uložené vzkazy, vymazať dôležitú správu, popr. zmeniť váš vlastný nahovorený text. Staršie záznamníky sa pri každej takejto aktivácii linky ohlásili klasickým pípnutím, ale novšie prístroje sú predávané bez akustickej signalizácie. Niektoré odkazovače majú funkciu, ktorá umožňuje diaľkovo monitorovať priestor miestnosti, v ktorej je prístroj umiestnený. Je to vlastne obdoba nekonečného vysielača a slúži ku kontrole, či vo vašej kancelárii práve nepracujú zlodeji. Odkazovače telefónnych hovorov sú proti zneužitiu uvedených funkcií chránené prístupovým kódom. Využívajú systém DTMF (Dual Tone Multifrequency), ale získanie prístupového kódu nie je tak zložité. Stačí totiž, aby niekto zostal sám vo vašej kancelárii u prístroja a môže si na zadnej stene prečítať sériové, výrobné číslo alebo priamo prístupový kód. Stačí potom zájsť do predajne

s podobnými zariadeniami a vyžiadať si manuál tohto typu prístroja a tam si prečítať možné prístupové kódy. Inak firmy zaoberajúce sa nasadzovaním spravodajskej techniky všetky takéto manuály od novo vyvinutých i starších prístrojov dávno majú a priebežne si ich zaobstarávajú. Ak nie je prístup do odposluchového priestoru konkurenčnej firmy, je možné nájsť prístupový kód skusmo. Stačí vytočiť všetkých desať čísel a počúvať reakciu záznamníka. Ak sa nepodarí záznamník aktivovať, pristúpi sa k aktivácii pomocou dvojčíselného hesla. [5]

- **Maskovanie mikrofónov :**



Obr. 13 mikrofón maskovaný ako zástrčka

6.2 Vysielače

- **Rádiové vysielače:** Jednou z veľkých nevýhod mikrofónneho odposluchu je nutnosť dôkladného ukrytie kábla vedúceho od mikrofónu, alebo nutnosť použiť pre prenos alternatívne vedenie, napríklad vodovodného potrubia, prívodov kúrenia, klimatizácia apod. Možno tiež použiť aj existujúce "legálne“ vedenie. Takýto mikrofón môže byť však relatívne ľahko odhalený citlivým zosilňovačom, ktorý sa k tomuto rozvodu pripojí. Aby sa odstránili uvedené nevýhody, bolo skonštruované zariadenie pracujúce na princípe rádiového vysielača. Pre prenos signálu sa využíva pásma veľmi dlhých vĺn, spravidla 50kHz-400kHz a frekvenčne modulovaný signál. Nešíri sa však vzduchom, ale po vodičoch. Vysielacie zariadenia je o niečo málo väčšie ako samotný mikrofón, nie je však detekovateľné zosilňovačom, pretože pracuje v nehlasovom pásme. Na prijímacej strane je

zapojený dekodér, VKV prijímač a nahrávač, spravidla magnetofón. Veľmi dlhovlnné vysielače, nazývané tiež vysielače nosného prúdu, majú aj ďalšiu výhodu. Prenos akustického signálu z odposluchového priestoru môže byť uskutočnený po akýchkoľvek vodičoch, ktoré vedú z miestnosti, teda aj po vodičoch elektrickej signalizácie, intercomu, telefónu, faxu alebo dátovej linke. [5]

- **Vkv vysielače:** Použitie dlouhovlnných vysielačov pre prenos informácie z odposlechového priestoru čiastočne odstránilo nevýhody klasických mikrofónnych vedenie, ale problémy s náročnou inštaláciou zostávajú. Použitie tu vyžaduje starostlivú prípravu sv dnešnej dynamickej dobe je takéto riešenie trochu ťažkopádne. Výhodnejšie najmä pre krátkodobé monitorovanie priestoru je požití miniatúrnych rádiových vysielačov tzv. ploštíc. Soudobé ploštice sú už veľmi malé rozmerov, dajú sa ľahko kúpiť za prijateľnú cenu a ich inštalácia je veľmi rýchla, čo je napríklad zrejmé na ďalších stránkach, kde toto "tovar" uvádzam. Signál uvedeného zariadenia a tým aj odpočúvanej rozhovor je možné zachytiť na normálnom rádioprijímači v rozsahu VKV do vzdialenosti asi 100m. Pre serióznejšie prácu sa však používa zariadenie, ktoré vysí1á mimo rozsah VKV, aby nedošlo k jeho ľahkému odhalenie. Jedná sa o miniatúrne rádiové vysielače naladenej výrobcom mimo VKV prevádzku, spravidla v pásme 200MHz-400MHz. Počúvanie je možný kvalitným širokopásmovým komunikačným prijímačom, alebo možno kúpiť miniatúrny rádiový vysielač ako súpravu i s jednokanálovým miniprijímačom. K nemu sa dajú pripojiť slúchadlá a nahrávač (magnetofón). E1egantní a nenápadné riešenie spočíva v použití vysielača ladeného výrobcom tesne nad frekvenčný rozsah VKV, do pásma 110MHz-130MHz a prijímača walknanu / discman s upraveným prijímacím rozsahom. So slúchadlami na ušiach a s walkmanom za pasom nebudí nikto pozornosť a pritom možno počúvať a zároveň aj nahrávať zvuky z. odpočúvania prostoru93. Ak však niekto uvažuje o použití rádiového odposluchu, musí vziať do úvahy všetky technické špecifiká, aby vybrané zariadenia splnilo očakávané výs1edky. [5]

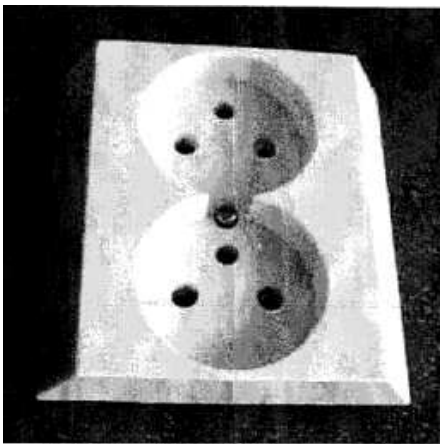
- **Nekonečné vysielače:** Vyššie opísané metódy telefónneho odpočúvania sú klasické spôsoby využitia telefónneho prístroja. Jeden zo známych systémov sa nazýva "nekonečný vysielač" alebo tiež "pískacie" alebo tiež "harmonická ploštica". Prvý

zo svojich názvov získal tým. že umožňuje monitorovať odposluchový priestor z ktoréhokoľvek miesta na Zemi, vlastne z nekonečnej vzdialenosti. Toto zariadenie, malá škatuľka s vlastným mikrofónom, sa zapojí na telefónnu linku v odpočúvanom priestore. Ako náhle je potrebné odposluch, môžete z ktoréhokoľvek iného telefónneho prístroja uvedené zariadenie aktivovať a počúvať zvuky v miestnosti. Nekonečný vysielač je vlastne diaľkovo, po telefónnej linke ovládané zariadenie. Nepotrebuje osobitné napájanie, ani aktívne nevysiela v rádiovom spektre. Celá súprava nekonečného vysielača sa skladá z dvoch prístrojov Jeden je v telefónnom prístroji, obsahuje mikrofón, zosilňovač, spínací systém a prijímač diaľkovej aktivácie. Druhý prístroj, veľkosťou, tvarom aj identifikáciou podobný vysielači tónovej voľby je určený na vysielanie tónového kódu pre aktiváciu zariadenia.. Mimo názov "nekonečný vysielač" alebo pískajúca ploštica sa môžete stretnúť i s pomenovaním "harmonická ploštica". Pôvodne sa totiž pre aktiváciu prijímača využívalo harmonického kmitočtu noty "C", to jest 440Hz. Pri použití tohto zariadenia sa vytočí číslo napichnutej telefónne stanice a pred vytočením posledného čísla sa začne vysielačom tónovej voľby do mikrofónu vysielať kódový signál. Na náprotivnej strane sa v okamihu ukončenia voľby aktivuje prijímač, telefón nevyzváňa a môže sa počúvať. Po položení slúchadla sa prístroj automaticky prepne do vyčkávacej polohy. Úspech pri aktivácii nekonečného vysielača závisí aj od typu telefónnej ústredne. Ak sa nestihne hneď po vytočení telefónneho čísla vyslať kódový signál , telefón zazvoní. [5]

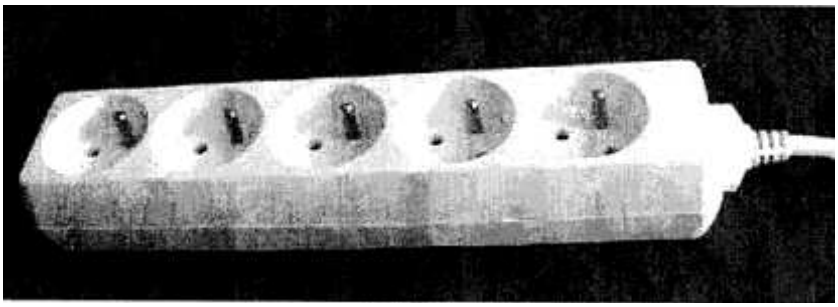
- **Špeciálne druhy vysielačov :** Miniatúrne rádio vysielače používané na odpočúvanie majú aj svoje nevýhody. Trvalé rádiové spojenie (Vysielanie) aj keď má dosah len niekoľko stoviek metrov, možno náhodne zachytiť na širokopásmovom komunikačnom prijímači, ktorý používajú rádioamatéri. Tento problém možno riešiť niekoľkými spôsobmi: Použitím špeciálneho druhu modulácie, obmedzením doby vysielania na nevyhnutne potrebnú dobu, znížením výkonu vysielača a použitím diaľkového ovládania. Nový spôsob modulácie využíva systém podnosnej frekvencie a dvojakej modulácie, kedy je hovorom modulovania dlhovlnné napr. 75KHz, výsledným signálom je potom hlavná nosná frekvencia, napr. 300MHz. Na prijímacej strane sa podobným spôsobom uskutočňuje dvojité demodulovanie. Ak je takýto signál zachytený na

širokopásmovom prijímači s bežnými druhmi prevádzky, nie je nemodulovaný a nie je ani počuť. Nevýhodou tohto spôsobu je veľká energetická náročnosť zariadenia. Drahšie rádio vysielače sú vybavované zariadením známym z reportážnych magnetofónov s označením skratkou VOX (Voice operatér). Systém VOX automaticky spustí vysielač iba pri dosiahnutí určitej hladiny akustického hluku v odposluchovom priestore. Systém VOX je výhodný pri dlhodobom monitorovaní a nahrávaní hovorov bez nutnosti trvalej obsluhy nahrávacieho zariadenia. VOX tiež znižuje možnosť náhodného zachytenia radiovysielania. Na sťaženie identifikácie a lokalizácie odpočúvania a tiež k predĺženiu životnosti napájacích zdrojov sú kvalitné a drahé rádio vysielacích vybavované diaľkovým ovládaním. Celé zariadenie sa predáva ako súprava s prijímačom a vysielačom diaľkového ovládania. Medzi najkvalitnejšie rádio vysielače patrí zariadenie, ktoré prijatý akustický signál vzorkuje, digitalizuje, ukladá do pamäte a vysiela ho komprimovaný v určitých časových intervaloch na dobu cca 0,5 sec. (Bursttransmitter). Prenosovým médiom informácie nemusia byť vždy len rádiové frekvencie. Pre prenos je možné využiť aj modulovaného infračerveného svetla alebo laserového lúča. U infračerveného prenosu je u hovoru z odposlechového priestoru monitorovaný infračervený lúč. Miesto klasickej drôtovej antény je tu vysielacie infradioda rovnako ako napr. u diaľkových ovládačov televízorov alebo videoprehrávačov. Prijímač, väčšinou umiestnený na statívu, je vybavený kvalitným teleobjektívom a snímacou infračervenou diódou pre zachytenie IR lúčov, optickým zameriavačom, zosilňovačom a niekedy aj ekvalizérom. Výhodou prenosu je jeho nezjistitelnost prístrojmi na meranie rádiového spektra. Nevýhodou je nutnosť zabezpečiť priamu optickú viditeľnosť medzi vysielačom a prijímačom. [5]

- **Príklady maskovania vysielačov :**



Obr. 14. Vysielač maskovaný ako zástrčka



Obr. 15. Vysielač maskovaný ako predlžovačka

Obr. 16. Maskovaný vysielač

6.3 Optické systémy

Jedná sa o technické systémy operatívnej techniky zabezpečujúce obrazový odposluch či už vo forme video záznamu alebo fotografií. Môžu zaisťovať i audio odposluch.

Využívajú sa :

- **Fotografické prístroje :** Fotografické prístroje prekonali značnú technickú zmenu a dnes sú nielen výkonné, čo do kapacity snímok, ale najmä miniatúrne ateda vhodné pre použitie skrytým spôsobom. Špionážne fotografie pre dokumentáciu osôb a jednotlivých tvárí sa vykonávajú malými fotografickými prístrojmi ukrytými do odevu, príručnej batožiny alebo vecí osobnej potreby. Bežne sú prístroje ukryté v zapaľovačoch, takže náhodný návštevník, ktorý vám pripaľuje cigaretu, môže zároveň fotografovať vašu tvár. Pri fotodokumentácii je však spravidla podstatné vyfotografovať osobu pri určitej činnosti. Používa sa väčších fotoaparátov, aby aj záznamový materiál mohol byť väčšieho rozmeru. Fotoaparáty sa používajú s pevným objektívom, fixnou clonou a tomu zodpovedajúci hĺbkou ostrosti. Uzávierka fotoaparátu je jednoduchá, podmienkou je minimálna hlučnosť, a je ovládaná skrytým spínačom. Pretáčanie filmu je riešené pružinovým pohonom natiahnutým pred začiatkom fotografovania. Obľúbené sú fotoaparáty značky ROBOT z Düsseldorfu. Najväčší rozpor pôsobí veľkosť fotoaparátu a filmu. Požiadavka je čo najmenšie telo fotoaparátu, ale čo najväčší rozmer filmu. Čím väčšie políčko filmu, tým sú aj kvalitnejšie fotografie. Aj vo fotografovaní ale nastupuje elektronika a ovládanie niektorých fotografických prístrojov je vykonávané elektronicky. V poslednej dobe je masový nástup digitálnych fotoaparátov. Tieto prístroje už nepoužívajú svetlocitlivý film, ale snímací čip a elektronickú pamäť. Tým je vyriešený problém s prevíjaním filmu, ale kvalita obrázku je závislá na kvalite snímacieho čipu. Tá je priamo úmerná počtu snímacích bodov vytvorených na čipe. Ako u väčšiny elektronických zariadení prebiehajú tu preteky jednotlivých konkurenčných výrobcov - kto dokáže ponúknuť trhu čip s čo najväčším počtom snímacích bodov, a tým aj čo najkvalitnejšie digitálne snímky. Vlastné digitálne snímky sa ukladajú na vstavané pevné pamäte alebo na vyberateľné pamäťové karty. Tie je možné čítať v čítačkách pripojených k počítaču alebo je možné snímky preťahovať pomocou kábla do počítača priamo z fotoaparátu ako z pevných pamätí. Ďalšie spracovanie a archivácia sa už odohráva

v PC. Neoddeliteľnou súčasťou fotoaparátu je objektív. Ten má tiež podstatný vplyv na kvalitu fotografie. To platí tak pre klasickú fotografiu, tak aj pre digitálnu. Ak chceme používať diaľkové fotografovanie, musíme byť vybavení kvalitným teleobjektívom a robustným statívom. S najmodernejšou technológiou je možné vytvárať kvalitné snímky na vzdialenosť mnohých kilometrov. Ak robíme fotografie z bežnej vzdialenosti, rádovo niekoľko metrov, a potrebujeme fotoaparát čo najviac skryť, je možné použiť ihlový objektív, a tým zmenšiť a lepšie zamaskovať otvor pre fotografovanie, alebo môžeme predĺžiť objektív svetlovodným káblom. Fotoaparát je potom ukrytý napríklad vo vrecku a niekolkomilimetrovým otvorom v preklopke sa môže fotografovať. Asi jedny z najdokonalejších fotografických zariadení pre diaľkovú fotografiu sú prístroje umiestnené na špionážnych satelitoch. Je pozoruhodné, že pomocou klasickej fotografickej metódy, tj. kvalitného objektívu a svetlocitlivého filmu, dosahovali ruské snímky z kozmu takej kvality, že to vyvolalo údiv aj u amerických odborníkov. Presnosť jedného až troch metrov u snímok z kozmu je rozlíšenie, o ktorom sa u klasickej fotografie mnohým len sníva. [5]

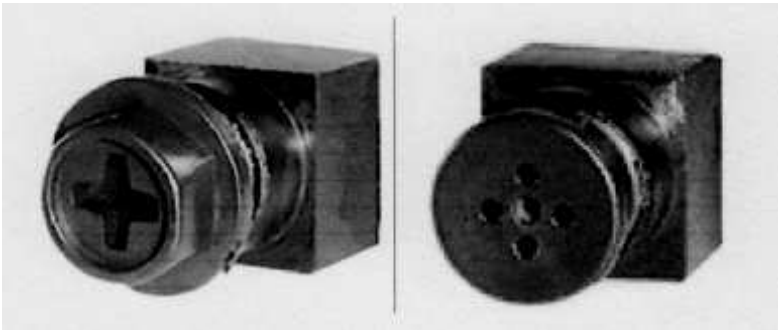
- **Videotechnika:** Doskové CCD kamery sú vyrábané v čiernobielom aj farebnom prevedení. Farebné sa ale používajú len v obmedzenej miere, pretože potrebujú oveľa viac svetla a nie sú citlivé v infračervenom spektre. To obmedzuje ich činnosť za šera, v noci a za zníženej viditeľnosti. Práve infračervená ožarovača sa používa na nepozorované osvetlenie scény pri monitorovaní v noci. Ľudské oko nič nevidí, ale čiernobiela kamera vidí takmer ako za dňa. Súčasne používané malé kamery, od priemyselných po policajnej a špionážne, sú osadené výhradne CCD čipmy. Kamery sú malé, s dobrou rozlišovacou schopnosťou, pevným objektívom, veľkou citlivosťou a spravidla s automatickou clonou a kompenzáciou protisvetla. Kvalitnejšie typy sú vybavené aj možnosťou výmeny objektívu. Sú veľkosti krabičky zápaliek, alebo dokonca kocky cukru, a umožňujú zabudovanie do rôznych predmetov. Ich použitie nie je teda viazané výlučne na otvory v stene. Pre objektív bežne používaných kamier stačí veľkosť otvoru asi 5-8mm, u dierkových (pinhole) objektívov asi 0,8-1mm. Kamery je možné zabudovať do nábytku, televízora, rádioprijímača, obrazov, rôznych plastík a dekoratívnych predmetov, hodín, kníh a hračiek. Vhodným miestom pre skrytú kameru sú osvetľovacie telesá,

požiarne a zabezpečovacie čidlá, krabice telefónnych rozvodov a rozvodov 220V. Kamery je možné ukryť do umelých kvetín, telefónov, faxov i počítačov. Pre ich ukrytie je limitujúcim faktorom veľkosť prístroja a veľkosť otvoru potrebného pre priechod svetelných lúčov do objektívu. Zmenšenie priemeru tohto otvoru sa dosahuje použitím dierkových objektívov alebo objektívov s predsunutým ohniskom. Kvalitným dierkovým objektívom stačí otvor s priemerom cca 0,8 mm, čo je napríklad papier prepichnutý ihlou. Uhol záberu v horizontálnej rovine je však obmedzený na max asi 60 °. Ak je žiaduci väčší uhol záberu, je nutné zvoliť objektív s bežnou šošovkou a následne ho zamaskovať. Osvedčila sa montáž za mriežku reproduktora, polopriepustné fólie, tkaniny s riedkou osnovou apod. Každá takáto montáž ale uberá na svetelnosti objektívu. Ďalšou možnosťou predĺženia objektívu je použitie svetlovodného kábla. Káble môžu byť pevné alebo pružné, dajú sa pretiahnuť malým otvorom v stene, sú ohybné bez straty kvality obrazu ale majú nižšiu svetelnosť. Aj u svetlovodných káblov platí, že pre špeciálne aplikácie je možné do jednej trubice zabudovať optický i akustický systém. Niektoré CCD kamery sú vybavené aj citlivými elektretovými mikrofóny, takže môžu okrem obrazu snímať aj zvuk. Výstupné signály zodpovedajú normám a môžu sa priamo zapojiť do videa a audiovstupov videorekordérov, monitorov alebo televízorov. Najprv je ale potrebné videosignál, prípadne audio signál, dopraviť z kamery na kľudné miesto a pripojiť k monitoru alebo videorekordéru. Prvý spôsob prenosu je káblom. Používajú sa, a tiež je to technicky najsprávnejšie, koaxiálne káble. Sú tienené a signál je možné viesť na veľkú vzdialenosť s relatívne malými stratami. Kábel však vyžaduje slušné zaobchádzanie, je väčšieho priemeru a nesmie sa príliš ohýbať. Tenký tienený kábel má zase väčšie straty. Ak privrieme oko nad technickým riešením, je možné viesť videosignál na malú vzdialenosť (asi do 50m) obyčajným tieneným viacžilovým oznamovacím káblom. Pri profesionálnych aplikáciách možno použiť aj Svetlovodné káble. Ten je veľmi tenký, nie je náchylný na rušenie a je možné ho viesť súbežne s rozvodmi sieťového napätia. Svetlovodný kábel je naozaj malý technický zázrak, ale ako napovedá názov, vedie len svetlo. Na začiatku aj na konci kábla musia byť prevodníky, optické konvertory. Videosignál je možné tiež viesť po krútenom dvojlinke, treba ale na strane kamery umiestniť vysielač signálu a na druhom konci drôtu jeho prijímač. [5]

U zabezpečovacích systémov sa používa pre automatizovaný prenos videosignálu bezpečnostných kamier prevodníky na telefónnu alebo ISDN linku. S troškou fantázie možno v takom prípade využiť optický odposluch v spojení s nekonečným vysielačom na telefónnej linke alebo s vysielačom nosného prúdu po sieťovom vedení. V poslednej dobe sa objavili tiež prenosy videosignálu po sieti mobilných telefónov GSM. Vďaka pomerne nízkej prenosovej rýchlosti tejto dátovej siete je ale výsledný videosignál roztrhaný do jednotlivých snímok. Tie sa obnovujú u čierno-bieleho obrazu asi 4x za sekundu a u farebného obrazu asi 2x za sekundu, a to ešte za predpokladu, že sa prenáša len obrazové body, kde došlo ku zmene, a nie statické pozadia. Pre bezdrôtového spojenia je možné použiť prevodník. Používajú sa schválené vysielače s vysielacou frekvenciou 2,4 GHz, pôvodne určené pre prenos signálu medzi videorekordérom a televízorom v domácnostiach a pre bezpečnostné systémy. Špeciálne aplikácie ale využívajú špeciálnej kamery aj špeciálne prevodníky. Vysielacia frekvencia je od 900MHz vyššie. Modulácia je spravidla frekvenčná, šírka pásma 5MHz a výkon vysielača od 100mW do 2W. U týchto špeciálnych aplikácií sa spravidla využíva aj šifrovanie videosignálu, aby nebolo možné jeho náhodné zachytenie a sledovanie. Ak sa podarí umiestniť kameru do priestoru, natiahnuť kábel alebo aktivovať vysielač, nastáva problém čo sa získaným videosignálu. Donedávna sa používal pomalobežný videorekordér (Time-lapse), kde je možné na jednu kazetu nahrať až 960 hodín záznamu. Ďalšiu možnosť ponúka digitalizácia obrazu. Digitálne videorekordéry sú už bežne dostupné u špecializovaných firiem s bezpečnostnou videotechnikou. Zakúpiť možno aj špeciálny HW a SW pre inštaláciu do PC. Miesto videorekordéra potom máme bežný počítač. Výhodou väčšiny digitálnych záznamových zariadení je, že už v sebe majú implementované niektoré funkcie, ktoré sa pri klasických analógových systémov riešili pridaním ďalších prístrojov. Jedná sa predovšetkým o videodetektor pohybu, kvadrátor či multiplexer, modem pre prenos videosignálu po sieťach JTS, GSM, ISDN, LAN apod. Ďalšou výhodou digitálnych systémov je jednoduchá archivácia záznamov, jednoduchšie vyhľadávanie nahratých udalostí, a nesporne aj vysoká kvalita záznamu. Nevýhodou je len vyššia obstarávacia cena u profesionálnych zariadení. Systémy určené pre inštaláciu do PC sú dokonca lacnejšie než zodpovedajúce prístrojové vybavenie pre analógové spracovanie a záznam videosignálu. [5]

- **Kamuflované minikamery :** jedná sa o maskovanie pre videotechniku.
  - Príklady maskovania :

Obr. 17. Maskovanie kamery za krabičku cigariet



Obr.18. Maskovanie kam. Za gombík a šroub

Obr.19. Maskovanie kam. za fľašu.

Obr. 20 . maskovanie kamery za budík

Obr. 21. Maskovanie kamery za slúchadlá

Obr. 22. Maskovanie kamery za PIR senzor

- **Infrakamery:** Infrakamera je založená na meraní emitovaných tepelných lúčov o vopred definovanej vlnovej dĺžke a až z nich sa v prístroji vypočítava predpokladaná teplota objektu. Meranie je teda ovplyvnené druhom okolité zástavby, smerom merania, denný časom, vlastnosťami meraného materiálu a mnohými ďalšími vplyvmi, ktoré je nutné pri následnej interpretácii zohľadniť a brať do úvahy. [5]
- **Bezpečnostné kamery:** Štandardné bezpečnostné kamery sú zvyčajne vybavené snímacím prvkom CCD, lacnejší low-end kamery využívajú CMOS čip. Vďaka technickému pokroku v oblasti vývoja CCD obrazových prvkov sú skôr výhradne používané čiernobiele bezpečnostné kamery postupne nahradzované kamerami farebnými. Bezpečnostné kamery sa vyrábajú v najrôznejších prevedeniach: štandardné kamery s SK-závitom pre výmenný objektív, kompaktné kamery s vstavaným objektívom, pologuľovité dome-kamery pre montáž no strop, doskové kamery pre vstavanie do rôznych zariadení atď. Pre kamerové systémy s aktívnou obsluhou (operátorom) je možné využiť tzv. auto-dome kamery (inak tiež speed-dome kamery alebo fast-dome kamery), ktoré umožňujú vzdialené natáčanie, naklápanie a zoomovanie. [5]

- **Ccd kamery a video vysielače:** Veľmi populárne sú v poslednej dobe aj odpočúvania obrazu a zvuku súčasne. Je to možné vďaka značnej miniaturizáciu kamier i vlastných vysielačov. Miniatúrne doskové CCD kamery potrebujú iba priviesť napájanie a už z nich vychádza klasický videosignál, spracovateľný každým bežným zariadením s video vstupom. Pritom rozmer takejto kamery môže byť14x14x15mm a ako otvor pre objektív stačí kruhová dierka o priemere cca 1,5 mm. Miniatúrne video vysielače farebného alebo čiernobieleho obrazu a mono zvuku nie sú väčšie ako kocka cukru. Nevýhodou je však trochu väčšia energetická náročnosť než je u vysielačov iba na zvuk. Preto možno očakávať, že video ploštica bude nainštalovaná v nejakom elektrickom spotrebičmi trvalo pripojenom v sieti. [5]

- **Fotoaparáty:** Slúžia na zaznamenanie konkrétnej situácie, konkrétneho páchateľa. Teraz sa už používajú digitálne fotoaparáty. Väčšia prednosť sa v dnešnej dobe dáva nahraným dôkazovým materiálom pred fotografiami. [5]

- **Noktovízia:** Noktovízor je prístroj pre nočné videnie, ktorý je vybavený elektrooptickým meničom. Je to zariadenie, ktoré nepatrné množstvo svetla (fotony) dopadajúce na objektív zmení na elektrický signál (elektróny). Tieto zosilnené elektróny sú zrýchlené proti fosforovej doštičke, ktorá ich premení späť na viditeľné svetlo, teda nazelenalý obraz, ktorý vidíme skrz prístroj. (Najlepšie klasické ďalekohľady dokážu zosilniť zbytkové svetlo až 40 x, noktovízor to dokáže od 900x až do 35 000x) Pokiaľ noktovízor nemá k dispozícii žiadne zbytkove svetlo (mesiac, hviezdy), alebo ho je príliš málo, pomôže prisvietenie IR žiaričom, ktoré je pre ľudské oko neviditeľné, ale prístroj ho dokáže znásobiť a previesť na viditeľný obraz. IR žiarič je súčasťou prístroja a jeho výkon meriame v mW. Rozoznávame diodové a laserové IR žiariče. Laserové sa vyznačujú vyšším výkonom a možnosťou koncetrácie žiarenia na rôzne veľkú plochu.
- **Termovízia:** Termokamery umožňujú zobraziť infračervenú stopu telesa, tak aby ho bolo možné vidieť.

6.3.1 Technika na odposluch dát a monitorovanie informačných technológií

Jedná sa o operatívnu techniku zameranú na monitorovanie akejkoľvek formy počítačovej komunikácie, získavanie počítačových dát a vyťažovanie informácií zo zdrojov informačných technológií.

- **Odposluch dát:** Prenos audiosignálu tvorí iba časť informácií prenášaných komunikačnými prostriedkami. Súčasný prenos informácií telexovými, telefaxovými, telex a dátovými stroji po telefónnych linkách je vzhľadom k hustote prenosu dát ďaleko atraktívnejšie pre odposluch ako hlasová komunikácia. Faxové prístroje, a hlavne počítače, sú vďačnými zdrojmi informácií, pretože na malej ploche je sústredené veľké množstvo informácií s možnosťou relatívne jednoduchého prístupu. Nové spôsoby prenosu dát však sťažujú možnosti ich odpočúvania. Klasické telefónne káble sú nahradzované mikrovlnnými spojmi,

telefónne a dátové linky sú prenášané vzduchom av jednom mikrovlnnom spojmi je sústredených niekoľko stoviek kanálov. V káblovej technike sa prechádza na svetlovodné káble, kde sa ako prenosového média využíva svetelného lúča. Z hľadiska odpočúvania je komplikované aj samo napojenie na takýto kábel a problém je aj spätný prevod informácie do zrozumiteľnej formy. Odposluchové systémy sa v týchto prípadoch zameriavajú na koncové zariadenia a dôležité informácie sa získavajú priamo zo zdroja. [5]

- **Odposluch počítačov:** Rozvoj výpočtovej techniky konečne zasiahol aj našu republiku. Do počítačov sú ukladané databázové súbory a informácie o osobách zo všetkých odborov ľudskej činnosti. Od informácií o privatizácii až po zdravotný stav pacientov. Takmer všetky výrobné informácie sú firmami ukladané na pevné disky počítačov. Tie sú pre urýchlenie a zefektívnenie práce prepojované do lokálnych a diaľkových sietí a informácie sú prenášané pomocou modemu po telefónnych linkách. Informácie o zamestnancoch firmy, zákazníkoch, výrobnom sortimente a finančných záležitostiach sú natoľko citlivé, aby vedenie firmy venovalo určitý čas a finančné prostriedky na ich ochranu. Každý si však musí sám vyhodnotiť veľkosť nebezpečenstva a potenciálnu možnosť ohrozenia svojho počítačového systému. Ide napríklad o zálohovanie dát, spôsoby antivírusovej ochrany súborov a používanie legálne získaného SW vybavenie. U počítačových systémov hovoríme spravidla o prenikaní do systému za účelom získavania informácií. Tieto metódy sa nie vždy uplatňujú v komerčnej oblasti, sú pomerne nákladné a komplikované tak z technického, tak z organizačného hľadiska. Sú však zaujímavé a používajú sa, a to nielen v tajných službách. V počítačových systémoch sa však môžu uplatňovať aj metódy odpočúvania opísané v predchádzajúcich kapitolách. Sám počítač a monitor sú vhodné na ukrytie miniatúrneho rádio vysielača alebo vysielača nosného prúdu. Sú takmer trvalo napájané a máloktorý používateľ je schopný si ich všimnúť. [5]

- **Odposluch faxov:** K odpočúvaniu faxovej prevádzky sa používa podobná technika ako pri telefónnom prenose. Faxová informácie je po telefónnej linke prenášaná vo forme akustických tónov a tieto tóny sa môžu nahrávať a prenášať rovnakým

spôsobom ako ľudský hovor. Zachytená faxové informácie je spravidla nahrávaná na digitálny magnetofón a počítačovo spracovávané k ďalšiemu využitiu. K rozlúšteniu faxové správy už netreba žiadneho prídavného technického zariadenia, ale iba špeciálneho počítačového softvéru. Písacie stroje klasické i elektronické je tiež možné monitorovať. Každý stroj vydáva určité akustické zvuky zodpovedajúce úderom klávesov a je možné po následnom počítačovom spracovaní k týmto zvukom priradiť písmená. Elektronické písacie stroje s pamäťou a displejom možno monitorovať obdobným spôsobom ako počítače. [5]

- **Odposluch sms:** SMS správy sú vďaka svojmu charakteru ideálnym predmetom odpočúvania. Náklady na ich monitorovania sú nižšie ako pri odpočúvaní hlasovej komunikácie. Tiež je jednoduché SMS prechádzajúcou sietí odpočúvať podľa výskytu kľúčových slov. Sledovanie nemusí byť vykonávané len prostredníctvom operátora. SMS má trvalejší ráz ako hovor. Osoba, ktorá vstúpila do miestnosti chvíľu potom, čo ste ukončili telefonát, má minimálnu možnosť zistiť o čom ste hovorili. Doručená (prípadne i odoslaná) SMS ale zostane v telefóne tak dlho, kým si nespomeniete zmazať ju. Potom už len stačí vzdialiť sa na chvíľu od telefónu, a každý, kto je v tú chvíľu prítomný, si môže správy prezrieť. To isté platí samozrejme v prípade, že je prístroj odcudzený. Za bezpečnostnú slabinu SMS správ môžeme jednoznačne požadovať aj to, že možno ľahko zmeniť ich text alebo identitu odosielateľa. K napáchané škody postačí už jednoduché pridanie či uberanie predpony, ale útočník môže pokojne zmeniť kompletný text. U bežnej SMS si teda nemôžete byť nikdy stopercentne istí, kto je autorom a či správa dorazila v pôvodnom stave. Čo sa s ňou dialo na ceste od odosielateľa do vášho telefónu skrátka nemôžete vedieť. Z toho je zrejmé, že spoliehať na bežné SMS služby pri výmene dôverných údajov, je prinajmenšom rizikové. [5]

6.4 Odhalenie a znemožnenie fungovania spravodajskej techniky

- **Režimové opatrenia**
- **OTP**
  - **Fyzická prehliadka:** Jedná sa o prehliadku miestnosti alebo objektu, ktorú prevádzaná technikom. Úspešnosť takejto prehliadky závisí od skúseností a technických znalostí technika.
  - **Rádiová prehliadka:** Pri tomto type prehliadky sa využívajú technické prostriedky špecializované na odhalenie aktívnej rádiovej spravodajskej techniky. Využívajú sa spektrálne analyzéry pre vytvorenie mapy rádiového poľa (mapa aktívnych rádiových prístrojov) a detektory rádiových frekvencií.
  - **Kontrola nelinearít:** Jedná sa o prehliadku záujmovej oblasti za pomoci detektoru nelinearít, ktorý odhaľuje polovodičové súčiastky v spravodajskej technike. Týmto spôsobom je možné lokalizovať operatívnu techniku, ktorá je neaktívna alebo ukladá nazbierané dáta na pamäťové médium. Taktiež je možné odhalenie prostriedkov, ktoré používajú iný druh komunikácie alebo boli napríklad v budove umiestnené počas stavby a sú dokonalo skryté.

- **Generátory šumu:** jedná sa o aktívny prostriedok rušenia konkurenčnej spravodajskej techniky. Je vhodné ich inštalovať na okná, nepriehľadné žalúzie, rolety alebo závesy. Vhodné je ich kombinovať s akustickými meničmi.
  - **Analógový gen. Šumu :** U analógového generátoru šumí nedeštruktívne prerazený polovodičový prechod. Používajú sa k tomu buď Zenerove diódy, častejšie ale prechod medzi bázou a emitorom bežného bipolárneho tranzistora pólovaný v nepriepustnom smere. Jeho šumové spektrum je vyrovnanejšie. Tieto prechody však produkujú pomerne vyrovnaný biely šum, u ktorého len na veľmi nízkom konci spektra, skôr až v subsonický pásme, môže prevládnuť šum ružový. Nasledujúcim obvodom je preto hneď za predzosilňovačom integračný článok, respektíve, dolná priepusť, ktorá urobí z bieleho šumu ružový. Tento článok väčšinou nie je čistý integrátor, býva ešte trochu frekvenčne korigovaný, pretože nie je potrebný ani podzvukové ani nadzvukový šum, navyše "surové" spektrum medzi tým tiež nemusí byť vyvážené

úplne presne. Biely šum je náhodný signál s rovnomernou výkonovou spektrálnou hustotou. Signál má rovnaký výkon v akomkoľvek pásme zhodnej šírky. Napríklad pásmo široké 20Hz medzi 40 a 60Hz má rovnaký výkon ako pásmo medzi 4000 a 4020Hz. Pre. využitie bieleho šumu: · Biely šum je používaný v niektorých Sirénach pohotovostných vozidiel pre jeho schopnosť preniknúť ostatnými zvuky prostredia (napr. zvukom mestskej dopravy) a nezpôsobovať ozvenu, takže je ľahšie určiť smer, odkiaľ prichádza. · Biely šum môže byť použitý na zmätenie jedincov pred výsluchom (Brainwashing = vymývanie mozgu) a tiež ako súčasť techniky zmyslové deprivácie.· Prístroje, ktoré ho produkujú, sú predávané na ochranu súkromia pri konverzácii, podporu spánku a zamaskovanie hučanie v ušiach. Ružový šum tiež známy ako "1 / f šum" alebo "kmitajúci šum" je signál alebo proces s takým frekvenčným rozsahom, že výkonová frekvenčné hustota je priamo úmerná prevrátenej hodnote frekvencie. [5]

- **Digitálny gen. Šumu :** Druhý typ šumového generátora neprodukuje ani čisto náhodný signál, ale len pseudonáhodný. Ten vzniká na špeciálne zapojených a do seba zavazbených posuvných registroch, teda akýchsi logických integrovaných obvodoch. Ide teda o skoro nepravidelnú sériu obdĺžnikových impulzov. Z ich výstupov odoberaný signál prechádza kaskádou filtrov typu dolnej priepusty. Keď ho pustíte nahlas, počujete v ňom oproti predchádzajúcemu kovové strojovej zafarbenie. Ak odoberáte šum zo zvukovej karty, môže sa prehrávať buď nasamplovanú vzorku, alebo jeho hodnotu počíta počítač, opäť pseudonáhodné, nejakým vhodným programovým algoritmom. Maximálna výchylka signálu z šumového generátora, nech toho či onoho typu, je limitovaná napájacím napätím príslušného obvodu. Toto obmedzenie náhodnosti signálu nás ale netrápi, skôr naopak. Dôležitejšie je, či má taký šum vyrovnané frekvenčné spektrum. V princípe sú na tom všetky druhy generátorov rovnako. Záleží na precíznosti pripojeného frekvenčného filtra, u počítaného či samplovaného šumu na kvalite vzorke alebo výpočte. U analógového typu zapojenie sa šumiaca polovodičové prechody môžu

kus od kusu líšiť, takže je vhodné, ak je požiadavkou maximálna presnosť, každý takýto generátor, teda jeho filter, kus od kusu doladiť. Konštrukcia takéhoto generátora býva ale často najjednoduchšie. Druhým problémom ešte je, že analógový generátor je naozaj najviac dieťaťom prírody, a preto jeho stredná hodnota viac kolíše, a to osobitne na spodnom okraji spektra, v oblasti basov (nízke frekvencie). S tým je potreba pri práci počítať a jeho zobrazenie integrovať s dlhšou časovou konštantou. Z tohto dôvodu sa mi pre naše účely ako vhodnejšie javí ostatné z uvedených generátorov - pseudonáhodné, Samplovanie alebo vypočítaný. Ak ale používate komplexné továrenské zariadenia, nemôžete si zvyčajne taký detail vyberať. [5]

ZÁVER

Na záver môžeme konštatovať, že všetky druhy a formy komerčného, respektíve konkurenčného spravodajstva sú na dnešnom agresívnom a neustále súperiacom podnikateľskom trhu významnou časťou stratégie spoločnosti. Pre firmy a spoločnosti je kľúčová ochrana ich know-how, obchodného tajomstva a citlivých informácií pokiaľ chcú byť konkurencieschopné. Pri využívaní komerčného spravodajstva je vhodné využívať vyvážene všetkých troch typov (ofenzívne, defenzívne, lobbying) pre efektívne fungovanie spravodajskej činnosti.

Pri defenzívnom spravodajstve je vhodné využiť pasívnych aj aktívnych metód ochrany spoločnosti, pričom pasívne metódy sú nevyhnutné pre vlastnú ochranu spoločnosti a objektu a aktívne pre zhromažďovanie informácií o spravodajskej činnosti konkurencie a následnú správnu voľbu stratégie a protiopatrení, ktoré spoločnosť zaujme na ochranu svojho know-how, obchodného tajomstva a citlivých informácií.

V práci som vytvoril súhrn a objasnenie dôležitých pojmov komerčného spravodajstva, metód a foriem detektívnej činnosti potrebných pre vykonávanie komerčného spravodajstva a taktiež som v praktickej časti vytvoril základný manuál využívania metód, praktík a techniky potrebnej ku spravodajskej ochrane firemného know-how, obchodného tajomstva a citlivých informácií.

ZÁVER V ANGLIČTINE

In conclusion it is possible to submit, that all kinds and forms of commercial or competitive intelligence are in nowadays agressive and always competitive bussines market crucial part of company strategy. For companies is crucial to protect their know-how, bussines secret and important informations if they wants to be able to compete with other companies. For effective use of commercial intelligence is considerable idea to use all of its forms (defensive, offensive, lobbying).

In defensive intelligence is appropriative to use both active and passive forms, where passive form is aimed for actual protection of the company and active form is aimed for gathering informations about intelligence servis of concurence and following choose of strategy and countermeassures for protection of know-how, bussines secret and important inforamtions.

In this bachelor work i have created summary and precision of important terms of commercial intelligence, methods and forms of private investigative services needed for commercial intelligence proces and in practical part i have created basic manual for applying methods,forms and technologies for intelligence protection of know-how, bussines secret and important informations.

ZOZNAM POUŽITEJ LITERATÚRY

[1] JUDr. LAUCKÝ, Vladimír., *Technologie komerční bezpečnosti I*. Zlín: Univerzita TomášeBati, 2010, 81 s., ISBN 978-80-7318-889-4

[2] JUDr. LAUCKÝ, Vladimír., *Technologie komerční bezpečnosti II*. Zlín: Univerzita Tomáše Bati, 2004, 122str., ISBN 80-7318-231-9

[3] HURTA, Josef,. *Management bezpečnostního inženýrství* /. Vyd. 1. Zlín : Univerzita Tomáše Bati, 2006. 172 s. : ISBN 80-7318-412-5 (brož.).

[4] KAMENÍK, Jiří,. *Komerční bezpečnost : soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur* /. Vyd. 1. Praha : ASPI, 2007. 338 s. : ISBN 978-80-7357-309-6 (brož.).

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

[6] BRABEC, František. *Soukromé detektivní služby* /. 1. vyd. Praha : EUROUNION, 1995. ISBN 8085858169.

[7] ŠMEJKAL, Petr. *Úvod do problematiky Competitive Intelligence s přihlédnutím k situaci v ČR*. Brno, 2006. 99 s. Ústav české literatury a knihovnictví. Kabinet knihovnictví. Masarykova univerzita. Vedoucí diplomové práce Mgr. Břetislav Šimral.

[9] JAŠEK, ROMAN,. *Informační a datová bezpečnost*/. 1. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2006. 144 s. : ISBN 80-7318-456-7 (brož.)

[10] Doc. Ing. LUKÁŠ CSC., Ludě. *Bezpečtnostní systémy technologie a management : Sborník mezinárodní konference*. první. [s.l.] : Univerzita Tomáše Bati ve Zlíně, únor 2008. 261 s. ISBN 978-80-7318-605-0.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

KS Komerčné spravodajstvo

EZS Elektronické zabezpečovacie systémy

MZS Mechanické zábranné systémy

ACS Acces control system (systém kontroly vstupu)

OPT Obranno technická prehliadka

PCO Pult centralizovanej ochrany

SDS Súkromné detektívne služby

DS Detektívne služby

PKB Preimysel komerčnej bezpečtnosti

SBS Súkromá bezpečtnostná služba

EPS Elektrická požiarna signalizácia

VKV Veľmi krátke vlny

VDV Veľmi dlhé vlny

ZOZNAM OBRÁZKOV