Defenzívne komerčné spravodajstvo – vrcholová technológia detektívnej činnosti

Defensive commercial intelligence - top technology of detective activity

Bc. Zdenka Straková

Diplomová práca
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2007/2008

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Zdenka STRAKOVÁ**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Defenzivní komerční zpravodajství – vrcholová technologie detektivní činnosti.**

Zásady pro vypracování:

1. **Zpracování rešerše literatury, která se vztahuje k tématu DP**
2. **Vymezení – definování pojmu komerční zpravodajství jako vrcholová technologie detektivní činnosti**
3. **Vymezení – definování metod, využívaných při získávaní komerčních informací**
4. **Analýza a syntéza (využití) komerčních informací získaných investigativní analýzou v kontextu činnosti SBS**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Strategické řízení firemních informací : teorie pro praxi, M. Keřkovský, M. Drdla, Praha 2003**
2. **Bezpečnost pro firmu, úřad, občana, BRABEC, F. a kol., Public History, Praha 2001**
3. **Základy teorie policejně bezpečnostní činnosti II., doc. JUDr. Antonín Filák, CSc a kol., Police history, Praha 2006**
4. **Základy kriminologie a trestní politiky, Josef Kuchta, Helena Válková a kolektiv, Praha 2005**

Vedoucí diplomové práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav elektrotechniky a měření

Datum zadání diplomové práce: **22. února 2008**

Termín odevzdání diplomové práce: **4. června 2008**

Ve Zlíně dne 22. února 2008

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

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práca sa zaoberá komerčným spravodajstvom. Značná pozornosť je venovaná hlavne defenzívnemu komerčnému spravodajstvu, teda prostriedkom na ochranu vlastných dát, informácií a poznatkov.

V teoretickej časti je popísaný vývoj komerčného spravodajstva v Českej republike a vo svete. Pozornosť je tu venovaná i zákonu o súkromnej bezpečnostnej službe v Slovenskej republike a problému s prijatím zákona v Českej republike.

Praktická časť poskytuje prehľad spravodajskej techniky, ktorá predstavuje technické prostriedky určené pre skryté získavanie a záznam informácií, ale zameriava sa i na vyhľadanie a ochranu proti nasadeniu odpočúvacej techniky.

Kľúčové slová:

Komerčné spravodajstvo, defenzívne komerčné spravodajstvo, spravodajstvo, informácie, odpočúvacia technika, odpočúvanie.

ABSTRACT

The diploma thesis deals with commercial intelligence. The considerable attention is dedicate especially defensive commercial intelligence, instruments on protection own data, information and know-how.

The theoretical part describes development commercial intelligence in the Czech Republic ant in the world. The attention is dedicated to law about private safety service in the Slovak Republic and problem whit acceptance to law in the Czech Republic.

The practical part presents a survey intelligence technology, which presents facilities intended for hidden acquisition and record information, but it is focused on detection and protection against listening device.

Keywords:

Commercial intelligence, defensive commercial intelligence, intelligence, information, listening device, tapping.

Rada by som touto cestou poďakovala vedúcemu diplomovej práce PhDr. Mgr. et Bc. Stanislavovi Zelinkovi za odborné vedenie, cenné rady a pripomienky, ktoré mi pri vypracovaní diplomovej práce poskytol.

Prehlasujem, že som na diplomovej práci pracovala samostatne a použitú literatúru som citovala. V prípade publikácie výsledkov, ak je to uvoľnené na základe licenčnej zmluvy, budem uvedená ako spoluautor.

V Zlíne …….

Podpis diplomanta

OBSAH

ÚVOD

Jedným z najvýznamnejších problémov začiatku 21. storočia sú otázky bezpečnosti. Veľmi často sa zabúda na význam súkromnej detektívnej (podnikateľsko-spravodajskej) ochrany ekonomických záujmov.

Je veľkou chybou, keď majitelia rôznych hodnôt nedoceňujú význam súkromnej bezpečnostnej ochrany ekonomických záujmov. U podnikateľských subjektov veľmi často panuje nesprávny názor, že sú dostatočne zabezpečené technickým zabezpečením svojich objektov, poprípade si najali strážnu službu. K ochrane ekonomických záujmov by mal podnik pristupovať zodpovedne. Ochrana ekonomických záujmov vyžaduje komplexný prístup, ktorý je oveľa širší ako technická či fyzická ochrany objektov. Významným faktorom, ktorý ovplyvňuje prosperitu, konkurenčnú schopnosť, teda efektívnosť podnikania každého podnikateľského subjektu, je schopnosť predvídať a riešiť krízové situácie, schopnosť odolávať rizikám a nástrahám, a to ako vonkajšieho, tak vnútorného charakteru. V procese zaisťovania bezpečnostnej ochrany ekonomických záujmov je nutné venovať prvoradú pozornosť tzv. vnútornej ochrane. Vnútornú ochranu predstavuje špeciálna, detektívna či operatívna ochrana. Patrí sem ochrana personálnej bezpečnosti, ochrana obchodnej bezpečnosti, vyhľadanie latentnej ekonomickej kriminality, zhromažďovanie informácií o dôkazoch pre súdne spory a správne jednania, ochrana informácií, dát, počítačových systémov, ochrana technológie a iného majetku podniku.

V poslednej dobe sa i v Českej republike vedľa klasických spôsobov súkromnej detektívnej ochrany ekonomiky začína, rovnako ako v štátoch s rozvinutou tržnou ekonomikou, uplatňovať i oblasť tzv. podnikateľského (komerčného) spravodajstva.

Odpoveďou na otázky, ako si má podnik uchovať a chrániť svoje vlastné tajomstvo je defenzívne (obranné) komerčné spravodajstvo. Dôležitou súčasťou moderného poňatia komplexnej bezpečnosti je ochrana proti nasadeniu odpočúvacej techniky. Hlavným dôvodom pre ochranu proti odpočúvaniu je ochrana informácií, s ktorými podnik manipuluje. Základom je využitie prístrojov na vyhľadávanie odpočúvacej techniky a prístroje na ochranu proti odpočúvaniu.

Táto práca si kladie za cieľ prehľadne a systematicky ukázať problematiku spojenú s defenzívnym (obranným) komerčným spravodajstvom. Jedným zo stanovených cieľov je poskytnutie podrobného prehľadu odpočúvacej techniky i prístrojov na ochranu proti odpočúvaniu. Ďalším cieľom práce je poukázanie na trendy vývoja komerčného spravodajstva v Českej republike.

I. TEORETICKÁ ČASŤ

1 PODNIKATEĽSKÉ SPRAVODAJSTVO

Spravodajstvo je pojem, ktorý vyjadruje proces získavania informácií a postupy a spôsoby práce s informáciami. Spravodajstvo vzniklo a po dlhú dobu bolo doménou štátnych tajných služieb, ale v súčasnosti sa stále viac presúva do privátnej (civilnej) oblasti, hlavne do sféry ekonomickej. Pre vyspelé podnikateľské subjekty sa stále výraznejšie stáva potrebnou súčasťou ekonomických, ale i spoločenských a politických procesov.

Produktom podnikateľského spravodajstva z vonkajšieho hľadiska, tj. voči konkurenčným subjektom, je buď zabránenie konkurencii získať informácie umožňujúce kvalifikované rozhodnutie, alebo dodanie dezinformácií, ktoré neumožňujú konkurencii kvalifikované a správne rozhodnutie, alebo oboje. Produktom podnikateľského spravodajstva z vnútorného (vlastného podnikového) hľadiska sú informácie vo forme znalostí umožňujúcich správne a kvalifikované rozhodnutie. Z hľadiska riadenia podnikateľského spravodajstva je potom veľmi dôležité, aby osoba zodpovedná za podnikateľské spravodajstvo bola súčasťou najužšieho vedenia. Pritom nezáleží na tom, či spravodajstvo je zaisťované podnikovým útvarom spravodajstva, alebo či je zaisťované zmluvne na komerčnom základe cez súkromnú detektívnu službu. Podstatné je ale to, že v podnikateľskom subjekte musí byť v najvyššom manažmente osoba zodpovedná za danú činnosť.[1]

Úlohou podnikateľského spravodajstva je odpovedať na nasledujúce otázky:

1) Ako si má podnikateľský subjekt uchovať svoje vlastné tajomstvo (dôverné a utajované skutočnosti) „v tajnosti“. Za najdôležitejšiu je nutné považovať ochranu svojich dôverných informácií, dát, počítačových a komunikačných systémov. Získavanie informácií o konkurencii by bolo k ničomu, keby sme neboli schopní ochrániť svoje vlastné informácie. Účinná ochrana vlastných informácií, dát a počítačových systémov musí mať východiskový základ v prevedení dôkladnej komplexnej bezpečnostnej analýzy.
2) Aký bude spôsob zhromažďovania informácií potrebných pre vlastné podnikanie (informácie o trhu, informácie o konkurencii apod.). Zhromažďovanie informácií

[1] BRABEC, František. Zpravodajství jiné než v televizi: Podnikatelská spravodajská činnost. *Profit Speciál*., roč. 2001, č. 11, s. 3

o konkurencii by malo mať pevne stanovené pravidlá, ktoré musia vychádzať z istého etického kódexu. Ak u ochrany vlastných informácií, dát, počítačových a komunikačných systémov spravidla nehrozia riziká porušenia zákona ani etiky, u zhromažďovania informácií o konkurencii táto otázka nie je úplne jednoznačná a jasná. Nehrozia riziká pri zhromažďovaní informácií z verejne dostupných (otvorených) zdrojov. Pomerne značné riziká sú však u využívaní špecifických foriem, metód a prostriedkov konkurenčného spravodajstva. Preto je potrebné sa v podniku touto otázkou veľmi podrobne zaoberať a stanoviť presné pravidlá. Súčasťou konkurenčného spravodajstva je i získavanie informácií marketingového charakteru, kde sú rizika o niečo nižšie.[2]

3) Ako získané informácie využiť pre ovplyvnenie vlastných podnikateľských aktivít, konkurenčných firiem, obchodných partnerov apod. Je potrebné stanoviť postup využívania získaných informácií, inak by boli získané informácie k ničomu. V podnikateľskom subjekte je nutné spracovať a realizovať systém informačných tokov, systém spracovania a systém využitia informácií v rámci ovplyvňovacej funkcie – vplyvného pôsobenia.

Podnikateľské spravodajstvo sa odohráva v troch smeroch:

- personálna bezpečnosť, ochrana vlastných informácií, dát, počítačových a komunikačných systémov podniku, čiastočne i ochrana proti vplyvovému spravodajstvu konkurencie. Ide o obrannom spravodajstve. V tejto oblasti spravodajstva sa spravidla nevyskytujú žiadne problémy. Ide o svojpomocnú, úplne legitímnu a oprávnenú ochranu vlastných záujmov, spravidla teda vlastných ekonomických záujmov.
- získavanie, zhromažďovanie, triedenie a analýza, syntéza a interpretácia informácií potrebných pre podnikania vrátane informácií o konkurencii, marketingových informácií apod. Tu hovoríme o ofenzívnom (aktívnom) spravodajstve.
- systém opatrení a protiopatrení k ovplyvňovaniu vlastných krokov, krokov obchodných partnerov, krokov konkurencie, krokov štátnej správy apod. Tu sa používajú názvy vply-

[2] BRABEC, František. Zpravodajství jiné než v televizi: Podnikatelská spravodajská činnost. *Profit Speciál*., roč. 2001, č. 11, s. 3

vové spravodajstvo. Zvlášť dôležitý je program zameraný na protiopratrenia proti komerčnému spravodajstvu zo strany konkurencie.

2 ČESKO A SVET

Podnikateľské spravodajstvo nadobúda v tuzemsku na význame. Z hľadiska metodologického a koncepčného je treba v ČR vytvoriť platformu, na ktorej základe sa začne s cieľavedomým budovaním národnej stratégie a koncepcie podnikateľského spravodajstva. V českej republike je istou platformou České spoločenstvo podnikateľského spravodajstva a managementu znalostí, ktoré je členom Central & East Europen BI & KM Community.

Národná stratégia podnikateľského spravodajstva by sa mala stať neoddeliteľnou súčasťou štátnej informačnej politiky a jej cieľom by malo byť:

- pri vykonávaní konkurenčného spravodajstva presadzovanie etických zásad v súlade so svetovým štandardom (osveta, obmedzovanie informačného monopolu apod.),
- vytváranie podmienok pre ľahký a rovný prístup k otvoreným informačným zdrojom (sprístupnenie informácií z otvorených zdrojov na internete, výuka spracovania informácií na školách apod.,
- zaistenie legitímnej ochrany národných ekonomických záujmov proti vykonávaniu komerčného spravodajstva zo strany iných zemí a národných zoskupení a koordinácie vykonávania národné komerčné spravodajstvo vo svete.

K dosiahnutiu cieľov podnikateľského spravodajstva je potrebné:

- v manažmente podnikov zmeniť predstavu, čo spravodajstvo je čo a nie. Manažéri na všetkých úrovniach musia pochopiť, že konkurenčné spravodajstvo existuje, aby poskytlo tvorcom firemnej politiky včasné informácie a analýzy, ktoré umožňujú vytvárať rozhodnutia založené na informovanosti a znalostiach a zároveň podporiť firemnú stratégiu a operácie bez rizík informačných, technologických a iných únikov,
- prehodnotenie firemnej vízie a posilnenie i kritické prehodnotenie firemných vízií. Manažéri na všetkých úrovniach musia byť pripravení akceptovať a reagovať na zmeny.
- vyvinúť celopodnikový mechanizmus konkurenčného spravodajského systému, aby tento bol nielen efektívny, ale hlavne aby sa v plnej miere stal nedielnou súčasťou vytvárania strategických, operatívnych i čiastkových rozhodnutí. Je nutné, aby spravodajská kolekcia zaujala svoje miesto v rámci kontextu správne definovanej firemnej politiky, ich

strategických, operačných a taktických cieľov. K zaisteniu úspechu nestačí neštruktura-lizované spravodajské projekty.

- zaistiť personálne obsadenie a vybavenie podnikateľského spravodajstva a tiež funkčný systém zberu informácií.

Je potrebné poznať možnosti a význam problematiky podnikateľského spravodajstva. Z toho sa potom odvíja schopnosť podniku uspieť a ochrániť si vlastné informácie.

3 DEFENZÍVNE (OBRANNÉ) SPRAVODAJSTVO

Defenzívne (obranné) spravodajstvo sa využíva k obrane vlastných dát, informácií a poznatkov tak, aby bola zminimalizovaná miera ich zverejnení a možnosť konkurencie ich využiť v boji proti našej firme. Defenzívne spravodajstvo, sa zaoberá analýzou informácií vytvorených vo firme, ich zverejňovaním a ochranou. Tento typ konkurenčného spravodajstva je použiteľný iba v prípade, že sú pracovníci a pracovisko súčasťou firmy (MILLER, 2001) a nehrozí žiadne riziko zverejnení kritických informácií. Tieto služby tak nie sú bežnou súčasťou ponuky brokerských konzultačných firiem. Ďalej je predpokladom úspešného fungovania obranného spravodajstva zvláštna výsada tohto pracoviska, ktoré musí mať prístup k všetkým dôležitým informáciám v podniku a musí tak byť mimo a nad ostatnými časťami podniku, pod ktoré býva niekedy aktívne konkurenčné spravodajstvo zaradené (najčastejšie sa jedná o marketingové alebo obchodné oddelenie). Tento typ spravodajstva je tak vývojovo vyššie než aktívne spravodajstvo a je používaný u veľmi veľkých, hlavne nadnárodných firiem, firiem s veľkou patentovou aktivitou (najčastejšie u firiem v chemickom alebo farmaceutickom priemysle) a ďalších.

Tri základné aktivity defenzívneho spravodajstva sú (NOLAN, 2005):[3]

1. Bezpečnostné protiopatrenie je tradičné fyzické zabezpečenie aktivít firmy. Patrí sem zabezpečenie vchodov, brán, skladov, pracovníci ochranky, apod.

2. Prevádzková bezpečnosť sa stará nie priamo o tajné informácie, ale o odkazy na tajné informácie. V bežnom obchodnom styku sú signály o tajných informáciách bežne produkované, tomu sa nedá zabrániť. Táto aktivita by sa dala považovať za protiklad zbierania indícií o konkurencii. Ide tak vlastne o snahu zabrániť súperom - konkurencii čítať indície vytvorené našou firmou.

3. Protirozvedné spravodajstvo je zamerané na objavenie a neutralizáciu protivníkových spravodajských aktivít.

[3] 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.70

Postup ochrany firmy, jej dát, informácii a procesov, rovnako ako strategických zámerov sa dá vyjadriť piatimi body (DeGENARO, 2005):

- identifikovať kritické informácie
- analyzovať hrozby
- analyzovať zraniteľnosť
- odhadnúť riziko
- nasadiť vhodné prostriedky obrany

Defenzívne spravodajstvo musí plniť viac rôznych, navzájom však prepojených úloh. Okruh úloh spojených s informačnou bezpečnosťou:

a) *Personálna bezpečnosť*. Ide o ochranu informačných systémov z hľadiska konkrétnych udalostí spôsobených pracovníkmi, a to predovšetkým z pohľadu prevencie. Personálna bezpečnosť musí byť zaisťovaná jednak detektívnymi previerkami budúcich zamestnancov podniku a jednak periodickými detektívnymi previerkami stávajúcich zamestnancov podniku.

b) *Režimová bezpečnosť*. Ide o vytvorenie bezpečnostných pravidiel z hľadiska zásad práce s informáciami, dátami, komunikačnými a počítačovými systémami. Je to veľmi významný prvok prevencie. Nestačí však iba existencia pravidiel, ale je samozrejme tiež nutné kontrolovať ich dodržovanie a v prípade ich porušenia i realizovať odpovedajúce opatrenia.

   Režimová bezpečnosť zahrňuje:

   - režim práce s písomnosťami,
   - režim ukladania dátových médií
   - vymedzenie okruhu osôb pre prácu s výberovými, dôvernými a utajovanými informáciami a dátami,
   - opatrenia pre prípad mimoriadnych udalostí apod.

c) *Bezpečnosť technických prostriedkov*. Ide o ich výber a spoľahlivosť, kontrolu prístupu k týmto prostriedkom, ochranu pred elektromagnetickým zariadením a elektrostatickou elektrinou apod.

d) *Bezpečnosť programových prostriedkov*. Je potrebné zaistiť kontrolu prístupu k ním, autentickosť a identifikáciu užívateľa, rozdelenie právomocí medzi užívateľov, výber a spoľahlivosť programov apod. Bezpečnosť programových prostriedkov spočíva:

   - v ochrane proti vírom,

- v obrane proti zneužitiu programového vybavenia

e) *Bezpečnosť dát*. Ide o ochranu dát v súboroch a databázach, či už elektronických či písomných, o ochranu proti chybám a vírom, o zvláštnu ochranu citlivých dát, o autorizáciu a rozlíšenie prístupu k dátam a databázam.

f) *Fyzická bezpečnosť*. Ide o ochranu informácií, dát, komunikačných a počítačových systémov proti neoprávnenému prístupu k ním, protiprávnemu vniknutiu do priestorov, kde sa nachádzajú.

g) *Bezpečnosť komunikačných systémov a ciest* predstavuje predovšetkým ochranu väzieb medzi jednotlivými časťami komunikačných a počítačových systémov.

h) Aktívna ochrana proti úniku informácií a dát, hlavne proti špionáži zo strany konkurencie, tj. proti aktívnemu súťaživému či konkurenčnému spravodajstvu. Ide o systém opatrení, smerujúcich k získaniu informácií o aktívach konkurenčných útvarov (agentúr) zaoberajúcich sa konkurenčným spravodajstvom.

   Patria sem tieto okruhy:

   - v rovine personálnej bezpečnosti ide o to zabrániť, aby zamestnanci podniku boli kontaktovaní a vyťažovaní konkurenciou; aby boli zamestnávaní zamestnanci konkurencie vo vlastnom podniku (fingované zamestnanie); aby informácie boli konkurenciou získavané za využitia korupcie či formou vydierania,
   - v rovine ochrany proti útokom na bezpečnosť informácií, dát, komunikačných a počítačových systémov zvonku ide o to zabrániť priamej krádeži počítačových nosičov informácií alebo ich nelegálne kopírovanie; zabrániť technickému získavaniu informácií z počítačových sietí; zabrániť špeciálnymi technickými prostriedkami (šumové generátory) odpočúvaniu vyžarovaniu počítačových monitorov,
   - v rovine odpočúvania a sledovania nelegálnymi prostriedkami ide o zaistenie a využitie ochrany proti odpočúvaniu audio, video, audiovideo a ďalších špeciálnych prostriedkov spravodajskej techniky konkurencie,
   - v rovine priameho narušenia vlastníckych práv ide napr. o ochranu proti vlámaniu za účelom krádeže dokumentov a iných nosičov informácií,
   - v neposlednej rade sem patrí i rovina získavania informácií o útvaroch konkurencie zaoberajúcich sa súťaživým, či konkurenčným spravodajstvom.

i) *Aktívna ochrana proti dezinformáciám a proti pôsobeniu vplyvového spravodajstva konkurencie*. Táto ochrana vyžaduje premyslený systém opatrení smerujúcich k rozloženiu dezinformačných kampaní a opatrenia obmedzujúce pôsobenie vplyvové-

ho spravodajstva konkurencie. Ide hlavne o rôzne akcie k narušeniu konkurenčných aktivít typu public relation a o vlastné aktivity tohto typu apod.

Ak majú byť všetky tieto úlohy naplnené, musí byť ochrana informácií chápaná v komplexnom - systémovom poňatí. Špecialisti na informačnú bezpečnosť sa preto musia vedieť orientovať v nasledujúcich činnostiach:

- činnosť metodologická a koncepčná,
- činnosť bezpečnostne organizačná, bezpečnostne režimová a bezpečnostne technologická,
- činnosť spočívajúca v presadzovaní a uplatňovaní informačnej bezpečnosti - bezpečnostných postupov a opatrení,
- činnosť spojená s bezpečnostnými informačnými auditmi,
- činnosť v oblasti personálnej,
- činnosť v oblasti technických riešení.

Pri definovaní požiadavkou na ochranu informácií je treba vychádzať zo skutočnosti, že existujú dve možnosti úniku informácií:

- nespoľahlivosť a zlyhanie ľudského faktora,
- nespoľahlivosť a zlyhanie technických systémov (vrátane softwarových subsystémov)

V prvej rade je potrebné si odpovedať otázky typu:

- Ktoré informácie, dáta, počítačové a komunikačné systémy je potrebné považovať za dôverné či inak utajované, aké sú hlavné elementy takto utajovaných informácií a prečo?
- Ako dlho je potrebné určité informácie a dáta uchovávať v tajnosti a prečo?
- Čo je už známe (alebo o čom možno predpokladať, že by už mohlo byť známe) a prečo?
- Ktoré podnikové útvary a ktoré osoby v nich sú alebo budú s daným okruhom informácií, dát a projektov zoznámené a v akom rozsahu a prečo je to nutné?
- Ktoré podnikové útvary a ktoré osoby v nich majú prístup do počítačového alebo komunikačného systému, v akom rozsahu a prečo?
- Ktoré osoby spadajú do okruhu manažérov – pracovníkov vytvárajúcich rozhodnutia, stratégiu, obchodnú politiku, pracujú na výskume či vývoji?

3.1 Obranné spravodajstvo ako prevencia

Prevencia musí byť čo najefektívnejšia. Predovšetkým by mala ísť cez hospodárne využitie už existujúcich síl a prostriedkov. Potom je úplne nepodstatné, či sú preventívne opatrenia realizované vlastnými silami a prostriedkami podniku, alebo prostredníctvom zmluvne zaistených súkromných detektívnych kancelárií a špeciálnymi prostriedkami technických služieb. Pre ich optimálne zaistenie však je obvykle efektívne využitie vhodnou kombináciou uvedených možností.

Požiadavka efektivity týchto opatrení sa premieta do odborného posúdenia možných strát a nákladov na ich elimináciu. Ukazuje sa, že čiastkové riešenie je menej efektívne než riešenie komplexné. Javí sa preto ako potrebné, aby u každého podniku bol spracovaný a realizovaný systém komplexných opatrení zaistený jeho bezpečnosti, ktorý musí zahrnúť komplexnú bezpečnosť objektov, komplexné zaistenie informácií, dát, počítačových a komunikačných systémov a komplexné zaistenie bezpečnosti ostatných oprávnených záujmov.

Veľmi vážnou chybou, ktorej sa podniky veľmi často dopúšťajú, je formálne zaistenie bezpečnosti. Obvykle si najmú súkromnú detektívnu službu, prípadne si zriadi vlastný operatívny bezpečnostný – spravodajský – útvar, a obvykle si i zaistí technické zabezpečenie objektov.

Medzi personálnu bezpečnosť podniku patria hlavne dva okruhy úloh:

a) Stanovenie a dôsledné vyžadovanie realizácie režimových opatrení, a to samozrejme vrátane kontroly ich dodržovania. V tejto súvislosti je potrebné predovšetkým riešiť:
   - ktorí pracovníci, v ktorej dobe a kam majú prístup, aký je spôsob vstupu pracovníkov do podniku a do jeho vybraných objektov a aký je spôsob odchodu z nich,
   - aký je režim pohybu zamestnancov v podniku a v jeho vybraných objektoch
   - to isté pre návštevy vrátane kontroly ich pohybu,
   - systém plánov pre prípad rôznych mimoriadnych (krízových) situácií.
b) Efektívna personálna politika podniku. Podniky vedia, že základom efektívneho a bezpečného fungovania každého podniku je zodpovedný výber uchádzačov o zamestnanie a priebežné komplexné hodnotenie zamestnancov. Je ale potrebné pristupovať nielen

z odborného, ale i bezpečnostného hľadiska. Iba taký prístup smeruje k odstráneniu príčin a podmienok negatívnych javov.

Informácie, ktoré sú výsledkom detektívneho vyšetrovania (napr. o fungovaní rodiny uchádzača či zamestnanca, čo robia rodičia, súrodenci, manželia, akú má uchádzač povesť v bydlisku či predchádzajúcom zamestnaní, jeho minulý i súčasný život, spôsob trávenia voľného času, okruh priateľov, majetkové pomery apod.), môžu byť pre podnik veľmi dôležitým vodítkom pri rozhodovaní o prijatí či neprijatí, pri rozhodovaní o pracovnom zaradení apod. Informácie získané detektívnymi vyšetrovaniami dokresľujú celkovú vierohodnosť, seriózнosť a spoľahlivosť uchádzača o zamestnanie alebo už zamestnaného pracovníka. Tieto informácie môžu vykresliť prípadné bezpečnostné riziká spojené so zamestnancom.

V praxi sa stretávame s dvoma druhmi vyšetrovania zamestnancov:

1. Detektívne previerky zamestnancov. V tomto smere je samozrejme nutné vymedziť okruh osôb, ktoré budú podrobované preventívnym periodickým previerkam, ako často a v akom rozsahu. Zvlášť významné to je tam, kde sa pracuje s utajovanými a dôvernými informáciami alebo kde existujú iné zvýšené bezpečnostné riziká (napr. sektor bankovníctva, poisťovníctva, vývoja a výskumu). Z právneho hľadiska je potrebné tento okruh osôb vymedziť v organizačnom a pracovnom poriadku a spravidla i v pracovnej zmluve.
2. Psychologické vyšetrenie uchádzačov o zamestnanie a periodické preventívne psychologické vyšetrenia vybraného okruhu zamestnancov. Hlavné využitie poznatkov psychológie v praktickej činnosti personálnej práce v podniku môžeme vidieť hlavne v troch oblastiach:
   a) pri výbere pracovníkov a zisťovanie ich spoľahlivosti a pracovnej spôsobilosti pre výkon práce,
   b) pri výcviku pracovníkov aktivačne participačnou metódou, vrátane výcviku zvládnutia stresových situácií,
   c) pri využití niektorých špeciálnych psychofyziologických metód previerky.

   Všetky tri oblasti sa vzájomne doplňujú a tesne sa dotýkajú komplexného zaistenia bezpečnosti podniku. Významným prínosom tu môže byť objektivizácia psychologických vyšetrení pomocou fyziodetekcie, čo umožní ľahko odhaliť nevedomé či zámerné skrý-

vané charakteristiky skúmanej osoby. Takýmto skvalitnením personálneho výberu či bezpečnostných previerok záujmových skupín pracovníkov nesporne dochádza k významnému kladnému preventívnemu pôsobeniu, predovšetkým v oblasti kriminality.

4 TECHNICKÁ OCHRANA OBJEKTU

Technická ochrana predstavuje systémy a komponenty, pomocou ktorých sa vytvárajú relatívne stále podmienky brániace nepovolaným osobám vniknúť do chráneného objektu, ale tiež systémy signalizujúce vznik požiaru alebo signalizačné systémy informujúce o zmenách rôznych stavov, ktoré môžu viesť k havárii.

Technická ochrana, predovšetkým elektronická technická ochrana, predstavuje realizáciu metód ochrany objektov:

a) metóda technickej ochrany – spočíva v montáži rôznych technických zábran, brániacich v napadnutí objektu či preniknutiu nepovolaných osôb do chráneného priestoru. Táto ochrana býva spravidla kombinovaná s metódami elektronickej ochrany. Technická o elektronická ochrana môže iba spomaliť či sťažiť postup nepovolanej osoby, ale nemôže ju zastaviť či odvrátiť, to možné iba pomocou metód fyzickej ochrany.

b) metóda elektronickej ochrany – táto metóda je vysoko efektívna a účinná, ale opäť za predpokladu, že je spojená s uplatňovaním metód fyzickej ochrany. Ide o systémy:

- elektronickej zabezpečovacej signalizácie – EZS**,**
- elektronickej požiarnej signalizácie – EPS**,**
- elektronickej signalizácie rôznych stavov**.**

c) metóda elektronického pozorovania – touto metódou je zaisťovaná ochrana objektov s využitím elektronických systémov. Ide o elektronické pozorovanie s využitím videokamier a ďalších technických prostriedkov elektronického dohľadu či o elektronické dokumentačné prostriedky.

d) metóda režimových opatrení – táto metóda je na rozhraní medzi metódami technickej a technicko-elektronickej ochrany objektov a fyzickej ochrany. Pokiaľ ide o organizačné režimové opatrenia zaisťované fyzickou silou (pracovníkmi), ide o metódu fyzickej ochrany. Pokiaľ je táto metóda realizovaná technickými prostriedkami (napríklad rôznofarebné pracovné odevy rozlišujúce zamestnancov, výstražné tabuľky,...), ide o metódu technickej ochrany.

Technickú ochranu (pasívnu ochranu) objektov možno rozdeliť na:

- mechanické prostriedky ochrany**,**
- elektronické technické prostriedky.

4.1 Mechanické prostriedky ochrany

Mechanickou ochranou rozumieme súbor mechanických a technických prostriedkov, zariadení a komponentov, ktoré svojou konštrukciou znemožňujú ich jednoduché prekonanie. V technickej ochrane sú nezastupiteľné, ich inštalácia šetrí sily fyzickej ochrany a svojou odolnosťou pri prekonávaní vytvárajú časovú rezervu v postupe páchateľa a tým umožňujú zorganizovať kvalifikovaný zákrok.

Z hľadiska účelu, použitého materiálu a konštrukcie je mechanických prostriedkov technickej ochrany veľmi veľké množstvo. Ich druhy, rozmery a vlastnosti sú determinované požiadavkami využitia.

Mechanické prostriedky môžeme klasifikovať podľa rôznych hľadísk. Takýchto hľadísk členenia mechanických technických prostriedkov ochrany si môžeme stanoviť celú radu, a to podľa aktuálnosti ich využitia. V tejto súvislosti si môžeme urobiť delenie podľa druhových predstaviteľov. Druhových predstaviteľov možno deliť z rôznych pohľadov a kritérií podľa:

- mechanickej odolnosti, tuhosti a pevnosti**,**
- použitých konštrukčných prvkov a prevedení**,**
- úpravy k zvýšeniu odolnosti**,**
- spôsobu inštalácie.

Mechanické prostriedky sa používajú k:

- isteniu všetkých kritických miest v objekte, hlavne vstupov**,**
- vytváraniu oddeľujúcich bezpečnostných bariér a stien**,**
- vytváraniu úschovných miest**,**
- zaisťovaniú a dodržovaniú režimu a režimovanie.

4.2 Elektronické technické prostriedky ochrany

Úlohou elektronických technických prostriedkov je plnenie úloh:

a) **preventívnych** – prevencia elektronickej technickej ochrany spočíva už v samotnom fakte ich existencie a využitia. Viditeľné umiestnenie ich niektorých prvkov z 80% odvracajú potencionálnych páchateľov od úmyslu v danom objekte uskutočniť pripravovanú trestnú činnosť. Pri ochrane objektu zabezpečovacími elektronickými systémami

je potrebné podľa stupňa rizikovosti voliť i stupeň kvality takýchto systémov, poprípade zvolenie i násobenia rôznych systémov.

b) **podporne informačných** – tieto úlohy vo svojom dôsledku:
   - podporujú mechanickú ochranu tým, že signalizujú kde dochádza k narušeniu obvodového plášťa (šetrí sily fyzickej ochrany)**,**
   - sťažujú alebo znemožňujú neoprávnený pohyb v priestore**,**
   - zefektívňujú fyzickú ochranu tým, že signalizujú, kde dochádza k narušeniu obvodového plášťa (šetrí sily fyzickej ochrany)**,**
   - urýchľujú a skvalitňujú zákrok fyzickej ochrany, tým, že umožňujú vizuálnu kontrolu celého objektu, hlavne kritických miest**,**
   - informujú o iných skutočnostiach nevyhnutných pre zaistenie ochrany**.**

c) **dokumentačných** – dokumentácia má zvláštny význam pre orgány činné v trestnom konaní a poisťovňu. Rozsah prvkov elektronickej ochrany v základnom prevedení je tvorený:
   - zariadením EZS (elektronickou zabezpečovacou signalizáciou)**,**
   - zariadením EPS (elektronickou protipožiarnou signalizáciou – dohľadové videokomunikačné systémy)**,**
   - inými technickými zariadeniami podporujúcimi ochranné hľadisko**,**
   - súbor mechanicko-zábranných komponentov eliminujúcich kritické miesta.

Elektronické systémy a prvky môžeme členiť do nasledujúcich skupín:
- ústredne,
- čidlá,
- optické a akustické prvky,
- elektronické zámky,
- vstupné systémy,
- tiesňové hlásiče,
- ochrana rozvodov,
- systémy a prvky prepravy cenností,
- systém ochrany vozidiel,
- prvky osobnej ochrany.

Významnou súčasťou elektronických systémov ochrany sú pulty centralizovanej ochrany, ktoré môže byť prevádzkované:

- Políciou ČR,
- obecnými (mestskými) políciami,
- súkromnými bezpečnostnými agentúrami, ktoré spravidla súbežne zabezpečujú i výjazdové (zásahové) hliadky pre prípad narušenia objektu,
- pultmi centralizovanej ochrany.

V súvislosti s elektronickou ochranou objektov je potrebné si uvedomiť dve významné skutočnosti:

- výhodou EZS je ich neutrálnosť,
- efektívnosti a účinnosti elektronickej ochrany možno dosiahnuť iba v náväznosti na fyzický faktor, tj. fyzickú ochranu.

4.2.1 Elektronická zabezpečovacia signalizácia

Ide o elektronické systémy slúžiace k včasnej signalizácii nežiaduceho stavu, vniknutiu alebo pokusu o vniknutie do stráženého priestoru alebo iné nežiaduce činnosti narušiteľa.

Samočinne alebo prostredníctvom ľudského činiteľa urýchľuje predanie tejto informácie určenej osobe k ďalšiemu opatreniu. Je tvorené:

- sústavou čidiel a tiesňových hlásičov,
- prenosovou trasou poplachového signálu,
- riadiacou jednotkou (ústredňou) opatrenou ovládacím panelom, informačnou a zapisovacou jednotkou,
- príslušenstvom.

Normy zabezpečovacej techniky kladú rôzne požiadavky na zaistenie objektov EZS. Z tohto pohľadu je rozlišovaná:

- ochrana kľúčová,
- ochrana priestorová celoplošná,
- ochrana plášťová,
- strážení na uzatvorenie,

- stráženie na uzamknutie,
- stráženie na priechod,
- stráženie na preraz.

Veľmi významnými komponentmi EZS sú detektory (čidlá):

a) detektory pohybu
   - infradetektory pasívne a aktívne,
   - ultrazvukové,
   - duálne čidlá.
b) čidlá kontroly kľudového stavu
c) ochrana skla
d) detektory vibrácií
e) snímače osobnej ochrany
f) vstupné systémy a elektronické zámky
g) autoalarmy

4.2.2 Elektronická požiarna signalizácia

Elektronická požiarna signalizácia slúži k signalizácii vzniku ohniska požiaru a jeho rozširovanie na ďalšie priestory.

Celý tento systém je tvorený subsystémami:

- detektory (čidla, hlásiče) požiaru,
- ústredňa (riadiaca jednotka),
- doplňujúce zariadenie a príslušenstvo.

Detektory (čidlá, hlásiče) požiaru je možné rozlíšiť na:

a) optické hlásiče dymu
b) plamenné hlásiče dymu
c) tepelné hlásiče požiaru
d) ionizačné hlásiče dymu
e) lineárne hlásiče dymu
f) kombinované hlásiče

4.2.3 Dohľadové a dokumentačné systémy

Dohľadové a dokumentačné prostriedky spočívajú v tom, že prostredníctvom videokamier (videokamerových systémov) je realizovaný tzv. diaľkový elektronickooptický dohľad nad určitými vybranými objektmi či priestormi. Dohľad je realizovaný pomocou pracovníkov fyzickej ochrany, ktorí sledujú situáciu v týchto priestoroch na monitoroch. Táto situácia môže byť pre potreby dokumentačné ďalej zaznamenávaná na videorekordéroch. Videosystémy sú tvorené:

a) kamerovým subsystémom (jednotlivé kamery alebo systémy rozmiestnených kamier):
   - pevných alebo pohyblivých,
   - čiernobielych alebo farebných.
b) monitorovým systémom:
   - jednotlivý monitor s možnosťou prepínania na rôzne videokamery,
   - delené monitory,
   - sústava viacerých monitorov.
d) záznamovými systémami:
   - videorekordéry,
   - počítač s tlačiarňami s možnosťou vyhotovenia tlače obrázku apod.
e) ďalšie pomocné a doplnkové systémy

5 ODPOČÚVANIE A PRÁVO

Dohoda o ochrane ľudských práv a základných slobôd

Je zjavne najvýznamnejším dokumentom, ktorý poskytuje ochranu súkromia človeka. Táto dohoda vo svojom článku 8 stanoví, že každý má právo na rešpektovanie svojho súkromného života, obydlia a korešpondencie, pričom štátny orgán nemôže do výkonu tohto práva zasahovať okrem prípadov, kedy je to v súlade so zákonom a potrebné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu zeme, predchádzanie nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných.[4]

Listina základných práv a slobôd

Článok 13

Nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uložených v súkromí, alebo posielaných poštou alebo iným spôsobom, s výnimkou prípadov a spôsobov, ktoré stanoví zákon. Tak isto sa zaručuje tajomstvo správ predávaných telefónom, telegrafom alebo iným podobným zariadením.[5]

Odpočúvanie a záznam telekomunikačnej prevádzky

§ 88 Trestného poriadku

1. Ak je vedené trestné konanie pre obzvlášť závažný úmyselný trestný čin alebo iný úmyselný trestný čin, ku ktorému stíhaniu zaväzuje vyhlásená medzinárodná zmluva, môže predseda senátu a v prípravnom konaní na návrh štátneho zástupcu sudcu nariadiť odpočúvanie a záznam telekomunikačnej prevádzky, pokiaľ je dôvodné predpokladať, že týmto budú odhalené významné skutočnosti pre trestné konanie. Vykonávanie odpočú-

---

[4] *E-law : Úmluva o ochraně lidských práv a základních svobod a další smluvní dokumenty na tuto Úmluvu navazující* [online]. c2007 [cit. 2008-05-12]. Dostupný z WWW: <http://www.e-law.cz/zakony/euumluva.htm>

[5] *Business center.cz : Zákon č. 2/1993 Sb. - Listina základních práv a svobod* [online]. c1998-2008 [cit. 2008-05-13]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/listina-zakladnich-prav-a-svobod/>.

vania a záznamu telekomunikačnej prevádzky medzi obhajcom a obvineným je neprípustné. Ak policajný orgán pri odpočúvaní a zázname telekomunikačnej prevádzky zistí, že obvinený komunikuje so svojím obhajcom, je povinný odpočúvanie ihneď prerušiť, záznam o jeho obsahu zničiť a informácie, ktoré sa v tejto súvislosti dozvedel nijak nepoužiť.

2. Príkaz k odpočúvaniu a záznamu telekomunikačnej prevádzky musí byť vydaný písomne a odôvodnený. Súčasne v ňom musí byť stanovená doba, počas ktorej bude odpočúvanie a záznam vykonávaný, a ktorá nesmie byť dlhšia ako šesť mesiacov. Túto dobu môže sudca predĺžiť vždy na dobu ďalších šiestich mesiacov. Opis príkazu sudca bez odkladu pošle štátnemu zástupcovi. Odpočúvanie a záznam telekomunikačnej prevádzky vykonáva pre potreby všetkých orgánov činných v trestnom konaní Polícia Českej republiky.
3. Bez príkazu podľa odstavca 1 môže orgán činný v trestnom konaní nariadiť odpočúvanie a záznam telekomunikačnej prevádzky, alebo ho vykonať i sám, a to aj vtedy, ak je vedené trestné konanie pre trestný čin neuvedený v odstavci 1, pokiaľ s tým účastník odpočúvacej stanice súhlasí.
4. Ak má byť záznam telekomunikačnej prevádzky využitý ako dôkaz, je treba k nemu pripojiť protokol s uvedenými údajmi o mieste, čase, spôsobe a obsahu vykonaného záznamu, ako aj o osobe, ktorá záznam vykonala. Ostatné záznamy je treba zničiť, spoľahlivo uschovať a v protokole založenom do spisu poznamenať, kde sú uložené. V inej trestnej veci ako je tá, v ktorej bolo odpočúvanie a záznam telekomunikačnej prevádzky vykonané, je možné záznam použiť ako dôkaz vtedy, pokiaľ je i v tejto veci vedené trestné stíhanie pre trestný čin uvedený v odstavci 1 alebo ak s tým súhlasí účastník odpočúvanej stanice.
5. Pokiaľ pri odpočúvaní a zázname neboli zistené skutočnosti významné pre trestné konanie, je nutné záznamy predpísaným spôsobom zničiť.[6]

---

[6] *Business center.cz : Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)* [online]. c1998 - 2008 [cit. 2008-04-03]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/trestni_rad/>.

6 DETEKTÍVNE SPRAVODAJSTVO

Detektívne spravodajstvo predstavuje významnú formu súkromnej detektívnej činnosti, ktorej úloha spočíva v:

- **systematickom vyhľadávaní a získavaní** dát a informácií s konkrétnym zameraním a s využitím rozličných metód a prostriedkov súkromnej detektívnej činnosti,
- **zhromažďovaní a triedení** dát a informácií podľa presne stanovených požiadaviek zákazníka
- **investigatívnej analýze** zhromažďovaných a vytriedených dát a informácií s využitím všeobecných metód, ako je analýza, dedukcia, indukcia a a s využitím metód logiky a logických postupov,
- **syntéze** analyzovaných dát a informácií a ich transformácie na relevantné informácie,
- **znalosti**,
- **spracovanie znalostí do klientom požadovanej podoby**, vrátane dodržania zásad legalizácie získaných relevantných informácií a distribúcia znalosti klientovi.

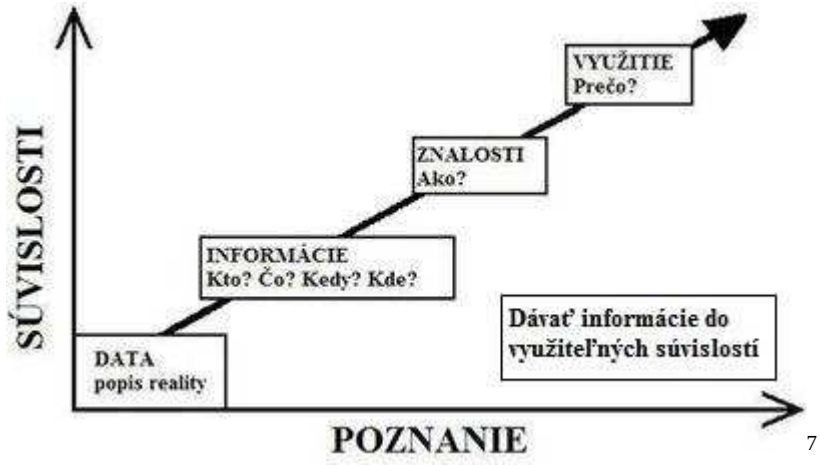
Detektívne spravodajstvo má nasledujúce kroky:

- **operatíva = informácia**. Spravodajská operatíva predstavuje schopnosť vyhľadať dáta a spracovať ich na informácie, schopnosť pomocou spravodajských technológií vyhľadanie a nájdenie informácií,
- **taktika = znalosti**. Spravodajská taktika predstavuje schopnosť pochopenia pomocou spravodajskej technológie analýzy informácie, ich relevantný výber a premenu na znalosť a schopnosť prezentácie znalosti v podobe zrozumiteľnej pre užívateľa (klienta),
- **stratégia = poznanie**. Spravodajská stratégia predstavuje postup využívania jednotlivých technológií a schopnosti vybrať a spracovať znalosti vo vzájomných súvislostiach.

Detektívne spravodajstvo je potrebné chápať ako:

1. **Informačný produkt** – produkt znalosti a poznania, ktorý pozostáva z obsahu, formy a aktuálnosti.
2. **Proces od dát a informácií k znalosti a poznaniu**, ako proces, ktorý sa skladá:
    - **Riadenie** spravodajskej činnosti predstavuje identifikáciu informačných potrieb a stanovenie priorít. Základným východiskom je vytvorenie a správne definovanie otázok a stanovenie spôsobov a ciest k dosiahnutiu odpovedí.

- **Zber** je účelové a cielené využívanie rôznych informačných zdrojov a rôznych metód súkromnej detektívnej činnosti a iných metód zberu informácií, ako napríklad vyťažovanie informácií z otvorených zdrojov.
- **Spravodajská analýza** predstavuje výklad informácií v spojení informačných potrieb vo vzájomných súvislostiach a vo vzťahu k riešenému problému.
- **Distribúcia** informácií získaných z rôznych informačných zdrojov vyžaduje včasné doručenie k užívateľovi, ktorý rozhoduje o tom, a to v jemu použiteľnej podobe.



[7]

Informácie – znalosť – poznanie sú využiteľné ak sú aktuálne, teda ich aktuálnosť musí mať prednosť pred kvalitou. Strata aktuálnosti informácie – znalosti – poznania nesmie byť ohrozená zdĺhavou distribúciou, len aby bolo dosiahnutej maximálnej kvality. Vysokokvalitné informácie – znalosti – poznania strácajú aktuálnosť a sú bezcenné ak sú distribuované s oneskorením.

Detektívne spravodajstvo predstavuje neustále sa opakujúce a na seba nadväzujúce cykly. Spravodajský cyklus je tvorený pravidelnými a navzájom na sebe nadväzujúcimi spravodajskými procesmi, medzi ktorými prebieha spravodajské riadenie. Spravodajské riadiace postupy obsahujú:

- definovanie potrieb,

[7] *obrázok prevzatý z:* KAMENÍK, Jiří, BRABEC, František. *Komerční bezpečnost : Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. 1. vyd. Praha : ASPI, a.s., 2007. ISBN 978-80-7357-3.

- spravodajské plánovanie,
- tvorbu operatívy, taktiky a stratégie spravodajského procesu,
- zhrnutie a analýzu terajších informácií, poznaní a znalostí,
- kolekcia spravodajského zámeru, čo je rozhodnutie o realizácií spravodajského procesu a jeho zámeroch a cieľoch.

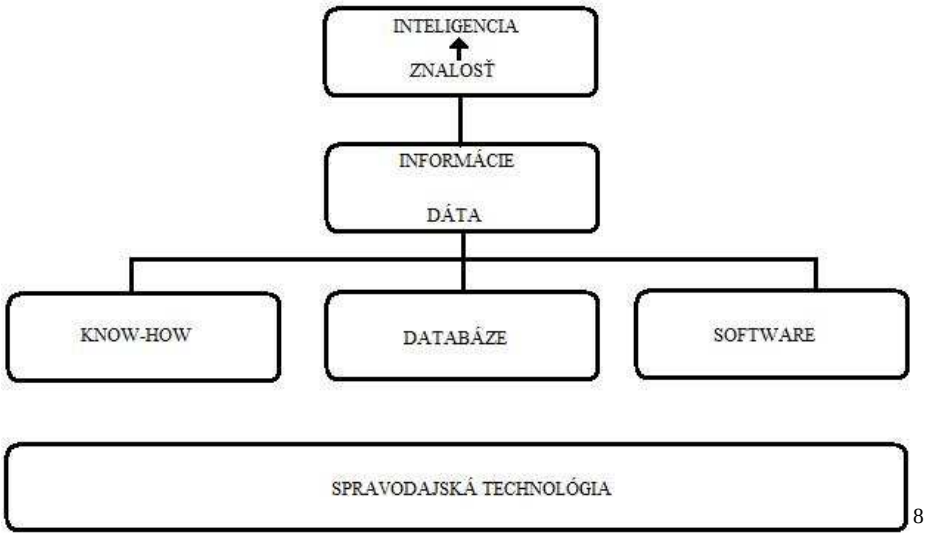
6.1 Investigatívna analýza

Investigatívna analýza informácií predstavuje spracovanie informácií za účelom pochopenia určitej situácie, jej príčin a možných následkov, s cieľom dosiahnuť znalosti o riešenom probléme.

Hlavným účelom investigatívnej analýzy je interpretácia pochopenia významu rozhodujúcich informácií k určitému definovanému zámeru a ich názorná prezentácia v kontexte cieľov, kľúčových oblastiach a úloh, na ktorých je zámer závislý.

6.2 Detektívna spravodajská technológia

Táto technológia sa využíva pri získavaní spravodajských produktov (znalostí).



[8]

[8] *obrázok prevzatý z:* KAMENÍK, Jiří, BRABEC, František. *Komerční bezpečnost : Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. 1. vyd. Praha : ASPI, a.s., 2007. ISBN 978-80-7357-3.

Technológia spravodajskej práce

Spracovanie informácií z otvorených zdrojov pre získanie informácií, ktoré budú využiteľné bez rizika poškodenia a potreby legalizácie vyžaduje:

- zmapovanie činnosti osoby (fyzickej alebo právnickej), udalosti, situácie z hľadiska vzájomných vzťahov a súvislostí;
- rýchle získanie podstatných informácií o subjekte, prostredí, skutočnosti zo všetkých dostupných zdrojov;
- rýchle spracovanie všetkých získaných informácií do prehľadnej podoby a využitie týchto informácií pri priebežnom sledovaní subjektu, prostredia alebo skutočnosti,
- odhalenie vzájomných väzieb a súvislostí (na ďalšie firmy, fyzické osoby, atd.) do potrebnej úrovne;
- získanie ďalších potrebných informácií pre plánovanie a rozhodovanie využitia spravodajského postupu a procesu;
- doplnenie podstatných informácií
- využitie získaných poznatkov a znalostí pre uskutočnenie spravodajských opatrení pomocou využitia primárnych zdrojov informácií.

6.3 Spravodajské informačné preniknutie [9]

Metóda spravodajského informačného preniknutia je jednou z najvýznamnejších ale tiež veľmi náročnou z činností spravodajských pracovníkov – súkromných detektívov. Ide v podstate o získanie ľudských informačných zdrojov a prácu s nimi s cieľom získať informácie k záujmovým osobám a zo záujmového prostredia k určitým záujmovým situáciám, javom, udalostiam a pod. Súčasťou metódy spravodajského informačného preniknutia je i metóda spravodajského vyťažovania osôb – spravodajský pracovník, ľudský informačný zdroj nielenže vytvára, ale tiež, a to je najdôležitejšie k získaniu informácií, i vyťažuje.

---

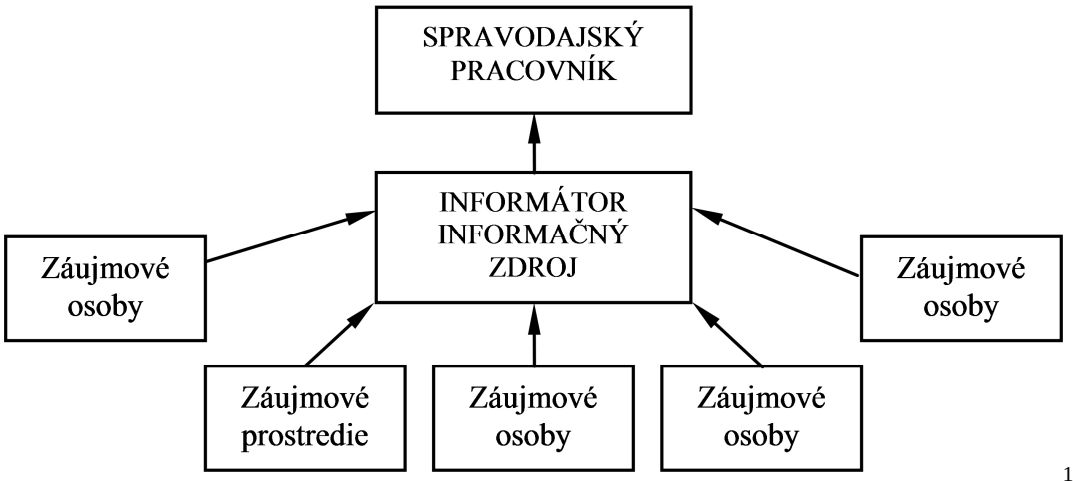
[9] KAMENÍK, Jiří, BRABEC, František. *Komerční bezpečnost : Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. 1. vyd. Praha : ASPI, a.s., 2007. ISBN 978-80-7357-3. s. 242.

Pri získavaní spravodajských pracovníkov je potrebné dbať na:

- vhodnosť informačného zdroja, ktorá je daná jeho možnosťami pohybovať sa a zdržovať sa v blízkosti záujmových osôb a v záujmovom prostredí, teda možnosťami získavať záujmové informácie;
- schopnosť informačného zdroja, ktorá sa opiera o jeho psychickú výbavu umožňujúcu nadväzovať kontakty, získavať informácie, rozpoznávať podstatné informácie od nepodstatných, objektívne informácie hodnotiť;
- spoľahlivosť informačného zdroja, ktorá je charakterizovaná jeho lojalitou voči spravodajskému pracovníkovi, teda odôvodneným predpokladom, že styk so spravodajským pracovníkom nevyzradí záujmovým osobám a v záujmovom prostredí, že bude spravodajského pracovníka včas a objektívne informovať o získaných informáciách, že neodovzdá záujmovým osobám a záujmovému prostrediu informácie o tom, o čo sa spravodajský pracovník zaujíma;

Spravodajské informačné preniknutie môžeme deliť na:

- pozičné informačné zdroje – také, ktoré sa nachádzajú v určitom záujmovom prostredí a z tohto odovzdávajú informácie;



[10]

[10] *obrázok prevzatý z:* KAMENÍK, Jiří, BRABEC, František. *Komerční bezpečnost : Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. 1. vyd. Praha : ASPI, a.s., 2007. ISBN 978-80-7357-3.

- cielené informačné zdroje – cielene prenikajú do záujmového prostredia či k záujmovým osobám s cieľom získať konkrétne zamerané informácie.

Typický užívatelia neštátneho spravodajstva sú spravidla:

- public relation agentúry,
- bankové domy,
- investičné spoločnosti a kapitálové spoločnosti,
- komerčné subjekty (zahraničné i domáce)
- advokátske kancelárie,
- bezpečnostné agentúry – hlavne služby ochrany majetku a osôb,
- štátny sektor.

Detektívne spravodajstvo, ako jedna z foriem súkromnej detektívnej činnosti, naplňuje obsah:

- spravodajstva, tzn. ofenzívneho spravodajstva,
- kontraspravodajstva, tzn. z časti obranného spravodajstva. Kontraspravodajstvo je získavanie a vytváranie znalostí o spravodajskej činnosti konkurencie. Obranné spravodajstvo je ale naplňované ďalšími formami súkromnej detektívnej činnosti, ako napríklad detektívna previerka, detektívne vyšetrovanie a rozkrývanie.

7 ZÁKON O SÚKROMNEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE

Dňa 1. 1. 2006 nadobudol v Slovenskej republike účinnosť zákon číslo 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti)

Zákon o súkromnej bezpečnosti upravuje:

1. poskytovanie služieb v oblasti súkromnej bezpečnosti
2. výkon štátneho dozoru Ministerstvom vnútra Slovenskej republiky a kontroly Policajným zborom v oblasti súkromnej bezpečnosti.

Súkromná bezpečnosť sa prevádzkuje ako súkromná bezpečnostná služba (ďalej len "bezpečnostná služba") alebo ako technická služba na ochranu majetku a osoby (ďalej len "technická služba").

Bezpečnostnou službou sa rozumie:

1. strážna služba
2. detektívna služba
3. odborná príprava a poradenstvo.

Fyzická osoba alebo právnická osoba prevádzkuje bezpečnostnú službu pre iné osoby alebo ako vlastnú ochranu. Bezpečnostnú službu možno prevádzkovať na základe licencie na prevádzkovanie bezpečnostnej služby.

Žiadosť o udelenie licencie na prevádzkovanie bezpečnostnej služby, vlastnej ochrany alebo technickej služby sa podáva osobne krajskému riaditeľstvu, pričom fyzická osoba alebo zástupca právnickej osoby pri podaní žiadosti o udelenie licencie preukáže svoju totožnosť občianskym preukazom alebo iným dokladom preukazujúcim totožnosť.

O udelení licencie rozhoduje krajské riaditeľstvo Policajného zboru na základe žiadosti fyzickej alebo právnickej osoby, príslušné podľa miesta trvalého bydliska fyzickej osoby alebo sídla právnickej osoby.

Licencia na prevádzkovanie bezpečnostnej služby sa vydáva na desať rokov, ak zákon o súkromnej bezpečnosti neustanovuje inak.

Licencia na prevádzkovanie bezpečnostnej služby je verejná listina a je neprevoditeľná.

Podmienky udelenia licencie na prevádzkovanie bezpečnostnej služby fyzickej osobe (§11 zákona o súkromnej bezpečnosti)

Krajské riaditeľstvo udelí licenciu na prevádzkovanie bezpečnostnej služby fyzickej osobe, ak tomu nebráni záujem vnútorného poriadku a bezpečnosti a ak :

a. je občanom členského štátu Európskej únie, občanom iného zmluvného štátu dohody o Európskom hospodárskom priestore alebo občanom Švajčiarskej konfederácie,
b. dosiahla vek 21 rokov,
c. má spôsobilosť na právne úkony v plnom rozsahu,
d. je bezúhonná,
e. je spoľahlivá,
f. je zdravotne spôsobilá,
g. má požadovanú odbornú spôsobilosť.

Uvedené podmienky musí spĺňať aj prokurista, vedúci organizačnej zložky podniku a vedúci zahraničnej osoby.

Ak fyzická osoba nemá pobyt na území Slovenskej republiky, musí ustanoviť zodpovedného zástupcu. Zodpovedný zástupca musí spĺňať vyššie uvedené podmienky a musí byť v pracovnoprávnom vzťahu k prevádzkovateľovi: to neplatí ak je ním manžel (manželka) prevádzkovateľa.

Podmienky udelenia licencie na prevádzkovanie bezpečnostnej služby právnickej osobe (§12 zákona o súkromnej bezpečnosti)

1) Krajské riaditeľstvo udelí licenciu na prevádzkovanie bezpečnostnej služby právnickej osobe, ktorá je spoľahlivá (§ 14 ods. 1 písm. g zákona o súkromnej bezpečnosti), ak tomu nebráni záujem vnútorného poriadku a bezpečnosti a:
   a) fyzická osoba alebo fyzické osoby, ktoré sú jej štatutárnym orgánom alebo členmi štatutárneho orgánu, spĺňajú podmienky ustanovené v § 11 ods. 1 zákona o súkromnej bezpečnosti,
   b) fyzická osoba, ktorá má najmenej 15 % majetkový podiel v právnickej osobe, spĺňa podmienky ustanovené v § 11 ods. 1 písm. d) a e) zákona o súkromnej bezpečnosti,
   c) z obchodného mena právnickej osoby nevyplýva, že plní úlohy verejnej správy.

2) Podmienky ustanovené v § 11 ods. 1 musí spĺňať aj prokurista, vedúci organizačnej zložky podniku a vedúci podniku zahraničnej osoby.
3) Ak osoba podľa odseku 1 písm. a) alebo vedúci podniku zahraničnej osoby nemá pobyt na území Slovenskej republiky, musí mať právnická osoba, ktorá žiada o udelenie licencie na prevádzkovanie bezpečnostnej služby, ustanoveného zodpovedného zástupcu. Zodpovedný zástupca musí spĺňať podmienky ustanovené v § 11 ods. 1 zákona o súkromnej bezpečnosti a musí byť v pracovnoprávnom vzťahu k prevádzkovateľovi.

Vzdelanie (§ 17 zákona o súkromnej bezpečnosti)

Požiadavku ustanoveného vzdelania na prevádzkovanie strážnej služby spĺňa osoba, ktorá má ukončené úplné stredné vzdelanie alebo úplné stredné odborné vzdelanie.
Požiadavku ustanoveného vzdelania na prevádzkovanie detektívnej služby a odbornej prípravy a poradenstva spĺňa osoba, ktorá:

- získala vysokoškolské vzdelanie druhého stupňa v študijnom odbore právo alebo v oblasti bezpečnostných služieb alebo v týchto odboroch získala vedecko-pedagogický titul docent alebo profesor,
- je držiteľom osvedčenia o vykonaní kvalifikačnej skúšky alebo
- získala vysokoškolské vzdelanie druhého stupňa v inom študijnom odbore ako právo alebo v oblasti bezpečnostných služieb a získala špecializované policajné vzdelanie a vykonávala bezpečnostnú prax v ozbrojenom bezpečnostnom zbore najmenej desať rokov a čas od skončenia vykonávania tejto praxe nie je dlhší ako päť rokov.

Technická služba

Technickú službu možno prevádzkovať na základe licencie na prevádzkovanie technickej služby.
O udelení licencie na prevádzkovanie technickej služby rozhoduje krajské riaditeľstvo na základe žiadosti fyzickej osoby alebo právnickej osoby. Licencia na prevádzkovanie technickej služby sa vydáva na dobu desať rokov, ak tento zákon neustanovuje inak.
Licencia na prevádzkovanie technickej služby je verejná listina a je neprevoditeľná.

Podmienky udelenia licencie na prevádzkovanie technickej služby (§ 70 zákona o súkromnej bezpečnosti)

1. Fyzická osoba, ktorá žiada o udelenie licencie na prevádzkovanie technickej služby, musí spĺňať podmienky ustanovené v § 11 ods. 1 písm. a) až e) a g) s tým, že § 11 ods. 2 a 3 platí rovnako.
2. Právnická osoba, ktorá žiada o udelenie licencie na prevádzkovanie technickej služby, musí spĺňať podmienky ustanovené v § 12 s tým, že fyzické osoby uvedené v § 12 ods. 1 písm. a), ods. 2 a 3 nemusia spĺňať podmienku zdravotnej spôsobilosti
3. Na posudzovanie bezúhonnosti a spoľahlivosti sa vzťahujú § 13 a 14.
4. Odborne spôsobilou je osoba, ktorá:
   a. získala vysokoškolské vzdelanie aspoň prvého stupňa v príslušnom študijnom odbore a má aspoň jednoročnú prax v tomto odbore alebo
   b. má stredoškolské vzdelanie v príslušnom odbore ukončené maturitnou skúškou a má aspoň dvojročnú prax v tomto odbore alebo
   c. má ukončené stredné odborné vzdelanie v príslušnom odbore a má aspoň trojročnú prax v tomto odbore.
5. Odbornú spôsobilosť osoba preukazuje dokladom o vzdelaní a potvrdením o praxi.

7.1 Najdôležitejšie zmeny

- Vymedzuje sa nový druh bezpečnostnej služby, ktorým je odborná príprava a poradenstvo.
- Režim povoľovania, kontroly a výkonu technickej služby sa podriaďuje novej právnej úprave, technická služba prestáva byť koncesovanou živnosťou a stáva sa licenčným podnikaním na základe licencie udelenej príslušným krajským riaditeľstvom Policajného zboru.
- Upravuje sa požiadavka odbornej spôsobilosti na prevádzkovanie a výkon bezpečnostnej služby a člení sa podľa obtiažnosti.
- Zavádzajú sa dva druhy preukazov odbornej spôsobilosti:
  - typu S pre osoby poverené výkonom fyzickej ochrany a pátrania
  - typu P pre osoby poverené výkonom fyzickej ochrany, pátrania, odbornej prípravy a poradenstva a pre prevádzkovateľov.
- Ustanovuje sa povinnosť označiť sídlo prevádzkovateľa, miesto činnosti fyzickej osoby a prevádzku obchodným menom na viditeľnom a verejne prístupnom mieste a motorové

vozidlo používané na preverenie signálu poplachového systému čitateľným nápisom "ZÁSAHOVÉ VOZIDLO". Na toto označenie je ustanovená lehota do 30. júna 2006.

- Sprístupňujú sa informácie z informačného systému súkromnej bezpečnosti.

8 PROBLÉMY S PRIJATÍM ZÁKONA O SBS V ČR

8.1 Legislatívna história SBS

Po novembri 1989 bol vznik a vývoj súkromnej bezpečnosti v Českej republike rôznorodý. Služby ochrany a majetku (strážne služby) nadviazali predovšetkým na činnosť Závodných stráži. Technické zabezpečovacie služby mali svojich predchodcov v rôznych elektronických a zámočníckych družstvách, ale i u služby ochrany objektov, ktorá sa vyvíjala od druhej polovice 70. rokov minulého storočia v rámci Verejnej bezpečnosti ako súčasť Zboru národnej bezpečnosti. Zložitejšia situácia bola u súkromných detektívnych služieb.

V Československej republike (dnes Českej republike) prvé súkromné detektívne služby vznikli už v období tzv. prvej republiky, kedy existovalo i v Československu niekoľko významných súkromných detektívnych kancelárií. K prerušeniu činnosti súkromných detektívnych kancelárií došlo v období okupácie – protektorátu Čechy a Morava – a na Slovensku v období tzv. Slovenského štátu. K istej obnove došlo po oslobodení Československa v roku 1945. Úplný útlm nastal po roku 1948. Na sklonku osemdesiatych rokov 20. storočia, bolo síce pripustené drobné podnikanie, ale súkromné detektívne služby do okruhu povolených činností drobného podnikania nespadali. Po roku 1989 museli služby súkromných detektívov začať od úplného základu, na rozdiel od už spomínaných služieb ochrany majetku a osôb.

Súkromné bezpečnostné služby a detektívne agentúry začali po novembri 1989 vznikať na podklade Vládneho nariadenia 1/1988 Zb., o podpore drobného podnikania, a vo svojej činnosti, pokiaľ sa jednalo o postupy – povinnosti a oprávnení, sa v podstate opierali o Vyhlášku FMV 135/83 Zb., o ochrane majetku v socialistickom vlastníctve, ktorá upravovala činnosť strážcov a závodných stráží. Zrušením tejto vyhlášky zákonom č. 333/1991 Zb., o federálnej polícií, stratili hlavne služby ochrany majetku a osôb právny základ vlastného výkonu činnosti. Dnes sa postupy služieb ochrany majetku a osôb riadia niekoľkými ustanoveniami trestného zákona a trestného poriadku (§13 tr. z. – nutná obrana, §14 tr. z. – krajná núdza, § 76 odst. 2 tr. poriadku – predvedenie osoby) a opierajú sa o občiansky

zákonník, hlavne o ustanovenia a svojpomoci (§ 6, § 11, §123, § 126, §415, § 417, § 418), ustanovenie o predchádzaniu škody (§ 151), ustanovenie o zastúpení (§ 22).

Istým pokrokom sa stalo v roku 1992 (zákon č. 455/1991 Sb., o živnostenskom podnikaní) zakotvenie služieb súkromných detektívov a podnikov zaisťujúcich ochranu majetku a osôb do živnostenského zákona, a to ako koncesované živnosti. Novelou potom pribudla i koncesovaná živnosť technické služby k ochrane majetku a osôb. Nie sú ale dostatočne riešené požiadavky u podnikov zaisťujúcich ochranu majetku a osôb, ale hlavne potom u služieb súkromných detektívov. Nedostačujúce sú požiadavky na odbornú spôsobilosť, ale hlavným hľadiskom je politický požiadavok vychádzajúci z kolektívnej viny, a to lustračné osvedčenie podľa zákona č. 451/1991 Sb. § 1 odst. 5 – ktorým sa stanovia niektoré ďalšie predpoklady pre výkon niektorých funkcií v štátnej orgánoch a organizáciách.

V legislatíve bolo ďalším pokrokom v sektore súkromnej bezpečnosti nariadenie vlády č. 469/2000Sb., ktoré definovalo obsah služieb:

- Poskytovanie technických služieb k ochrane majetku a osôb – *„Projektovanie, montáž, údržba, revízia a opravy elektronických zabezpečovacích systémov k ochrane majetku a osôb pred neoprávnenými zásahmi vrátane zabezpečovacích systémov a zariadení umožňujúcich sledovanie pohybu osôb v objektoch a ich okolí.“*
- Služby súkromných detektívov – *„Služby spojené s hľadaním majetku a osôb, zisťovaním skutočností, ktoré môžu slúžiť ako dôkazy pred súdom alebo správnym orgánom, získavanie informácií týkajúcich sa osobného stavu občanov, fyzických alebo právnických osôb alebo ich majetkových pomerov, získavanie informácií v súvislosti s vymáhaním pohľadávok.“*
- Podniky zaisťujúce ochranu majetku a osôb – *„Poskytovanie služieb spojených so strážením a ochranou hnuteľného a nehnuteľného majetku, stráž pri preprave peňazí, cenností či iného majetku, ochranou osôb a vymedzených záujmov, vyhodnocovaním bezpečnostných rizík a spracovaním plánov ochrany, prevádzkovaním pultov centrálnej ochrany.*

Žiaľ ide iba o vymedzenie obsahu jednotlivých služieb sektoru súkromnej bezpečnosti, ale nie je tu vyriešená otázky povinností a oprávnenia pri realizácií uvedených obsahov.[11]

8.2 Legislatíva sektoru SBS do budúcnosti

Z praxe sektoru súkromnej bezpečnosti a z kladných i záporných skúseností zo zahraničia je potrebné:

- Pre sektor súkromnej bezpečnosti prijať dva zákony, ktoré by súkromné bezpečnostné služby vyňali zo živnostenského zákona a vytvorili špecifickú právnu úpravu fungovania tohto sektoru. Ide o:
  - ***Zákon o službách ochrany majetku a osôb***, ktorý by riešil problematiku činnosti súčasných podnikov zaisťujúcich ochranu majetku a osôb a problematiku technických služieb k ochrane majetku a osôb.
  - ***Zákon o súkromných detektívnych službách a komerčnom spravodajstve***, ktorý by riešil problematiku činnosti súkromných detektívnych služieb, služieb komerčného spravodajstva a technických služieb k ochrane informácií, počítačových a komunikačných systémov.

V daných zákonoch je potrebné riešiť nielen požiadavky, ktoré sú kladené na prevádzkovateľa, ale hlavne požiadavky, ktoré sú kladené na pracovníkov (zamestnancov). Každý prevádzkovateľ i pracovníci by mali získať licenciu, a prevádzkovateľ ešte koncesiu, ktorá ho oprávňuje k podnikaniu v danom odbore.

- Aby zákony riešili odlišné požiadavky odbornej spôsobilosti:
  - U služieb ochrany majetku a osôb je potrebné riešiť odlišné požiadavky na fyzickú ochranu a technickú ochranu. Tiež odlišne riešiť požiadavky v rámci fyzickej ochrany.
  - Odlišné požiadavky musia byť kladené na prevádzkovateľov a pracovníkov (zamestnancov) súkromnej detektívnej činnosti a komerčného spravodajstva. Požiadavky na

[11] BRABEC, František. Problémy s přijetím zákona o SBS v ČR. *Security Magazín*. Listopad/Prosinec 2005., č. 11/12, s. 36-37

bežné súkromné detektívne činnosti zaoberajúce sa informáciami ohľadne partnerských vzťahov by boli podstatne menšie ako keď súkromný detektív pracuje pre advokáta a jeho mandanta pri zaisťovaní informácií o dôkazoch a dôkazov pre súdne kauzy. Rovnako odlišné je potrebné riešiť požiadavky u súkromných detektívov zaoberajúcich sa detektívnou ochranou ekonomických záujmov a aktivít podnikateľských subjektov a jej komplexnou podobou komerčnom spravodajstve v bezpečnostnom poňatí.

- Riešiť konkrétne povinnosti a oprávnenia pri výkone činnosti. Je tak naplňovaná požiadavka teórie práva spočívajúca v tom, že musí byť rovnovážny stav medzi povinnosťami a oprávneniami.

V prvej fáze by bolo potrebné náplne činnosti jednotlivých služieb sektoru bezpečnosti previesť z úpravy v nariadení vlády 469/2000 Sb., do podoby ustanovenia zákona v živnostenskom zákone.

- V zákonoch o týchto službách riešiť profesijnú komoru s povinným členstvom, podobne ako je tomu u advokácie, súdnych exekútorov a ďalších profesií. Táto komora by mala za úlohu i vydávanie licencií pre prevádzkovateľov, ich manažérov a pre pracovníkov. Živnostenské úrady by potom na základe licencie a splnení prípadných ďalších požiadaviek vydávali koncesiu k podnikaniu v danom odbore činnosti.

Ďalej by bolo vhodné, aby novelou živnostenského zákona (doplnením) bolo vydávanie licencií presunuté na autorizované živnostenské spoločenstvá príslušných odborov u Hospodárskej komory ČR.

Štátny dozor nad výkonom služieb súkromne bezpečnostného sektoru by malo vykonávať:

- Ministerstvo vnútra ČR prostredníctvom Polície ČR u služieb ochrany majetku a osôb;
- Ministerstvo spravodlivosti prostredníctvom štátnych zastupiteľstiev u súkromných detektívnych služieb a komerčného spravodajstva. Hlavným dôvodom je skutočnosť, že súkromný detektívi zaisťujú informačnú a dôkaznú podporu pre advokátov a ich mandantov. Pri dozore Polície ČR by pri činnosti v prospech obhajoby mohlo dochádzať ku konfliktom záujmov.

Súčasný stav v legislatíve sektoru súkromnej bezpečnosti je nežiaduci a vedie k problémom. Je žiaduce zriadenie komôr s povinným členstvom v tomto sektore činnosti. Chýba i dozor zo štátnej strany a zo strany živnostenského úradu kontrola vykazuje absenciu. Zamestnancom priameho výkonu služieb je venovaná malá alebo žiadna pozornosť pri získavaní odbornej spôsobilosti. Nápravu možno vidieť v licenciách pre priamy výkon zamestnania v týchto službách. V súkromnej bezpečnosti sa jedná o služby špecifické s istým dopadom do práv a oprávnených záujmov občanov a organizácie. Tento špecifický charakter týchto služieb vyvoláva požiadavku špecifickej legislatívnej úpravy.

II. PRAKTICKÁ ČASŤ

9 SPRAVODAJSKÁ TECHNIKA

Za spravodajskú techniku možno v širšom zmysle považovať technické prostriedky určené pre skryté získavanie a záznam informácií (audio, video či dátových). Ide predovšetkým o odpočúvanie, miniatúrne magnetofóny, fotoaparáty a videokamery, ale tiež nástroje pre konšpiratívnej prehliadky bytu (paklice) čí kontrolu korešpondencie ("nahrievačky", "čítačky"), prístroje pre nočné videnie (noktovízia, termovízia) atd.

Nemožno tiež vynechať prístroje pre spojenie (vysielačky, radary,...) a ďalšiu elektronickú a počítačovú výbavu slúžiacu k získavaniu informácií (nabúraniu počítačovej siete objektu záujmu atd.).

Jedným z najznámejších druhov operatívnej techniky je odpočúvanie. Obecne je rozšírené (predovšetkým z televíznych seriálov) slangové označenie - ploštica. Rádiová ploštica je však iba jeden z možných spôsobov realizácie odpočúvania. Za odpočúvanie možno považovať obecne každý technicky prostriedok slúžiaci k monitorovaniu, pripadne nahrávaniu rozhovoru. Rozlišujeme, či ide o priestorové odpočúvanie (monitorovanie rozhovoru v priestoroch) alebo o odpočúvanie rozhovoru či dát putujúcich po technických nosičoch - pevnej telefónnej linke, celulárnej telefónnej siete (mobilné telefóny), počítačové siete apod.

9.1 Základné rozdelenie odpočúvania

Za spravodajskú techniku možno považovať technické prostriedky určené pre utajené získanie a záznam informácií. Ide predovšetkým o rádiové vysielače bežne označované – „ploštice“, miniatúrne magnetofóny, miniatúrne videokamery, satelitné sledovanie, nahrávaciu a ďalšiu špeciálnu techniku.

Za odpočúvanie možno považovať každý technický prostriedok, ktorý slúži k monitorovaniu, prípadne k skrytému nahrávaniu zvuku a obrazu. Odpočúvanie môžeme rozdeliť do dvoch základných skupín:

a) priestorové odpočúvanie
b) odpočúvanie dát prenášaných po komunikačných linkách

Základné spôsoby odpočúvania:

1) odpočúvanie zvuku v miestnosti, v kancelárii, aute, na ulici atd.
2) snímanie zvuku z telefónneho vedenia
3) snímanie zvuku a obrazu
4) snímanie dát prenášaných po technickom vedení
5) bezkontaktné odpočúvanie počítačov
6) odpočúvanie rádiovej komunikácie

Základné spôsoby prenosu odpočutých informácií:

1) prenos signálu po metalickom vedení
2) prenos signálu pomocou rádiového signálu
3) prenos signálu pomocou optického vodiča
4) prenos signálu pomocou infračerveného lúču
5) prenos signálu pomocou laserového lúča

Ochrana prenášaných odpočutých informácií:

1) bez šifrovania
2) pomocou šifrovania
3) rýchlou zmenou kmitočtu
4) odosielanie informácií prerušovane, tj. po častiach

Základné spôsoby ukladania odpočutých informácií možno rozdeliť na 2 skupiny:

a) uloženie odpočutých informácií priamo v mieste odpočúvania
b) uloženie odpočutých informácií mimo priestor odpočúvania
   b1) v bezprostrednej blízkosti odpočúvaného priestoru
   b2) vo väčšej vzdialenosti od odpočúvaného priestoru

1) uloženie informácií na magnetickom kazetu (pásku)
2) uloženie informácií na videokazetu
3) uloženie informácií na HD počítača
4) uloženie informácií na pamäťové karty a iné záznamové zariadenia

Podľa spôsobu uloženia odpočutých informácií

1) analógové
2) digitálne

9.2 Základne typy odpočúvania

Miniatúrne rádiové vysielače ("ploštice", "ucha", "bezdrôtové mikrofóny"). Ich nasadenie je veľmi operatívne, ľahké a preto najčastejšie. V praxi ich existuje nepreberné množstvo. Možno ich rozlišovať podľa spôsobu napájania (doby prevádzky), režimu vysielania. druhu použitej modulácie, vysielacej frekvencie a výkonu, podľa veľkosti, spôsobu kamufláže, a podľa množstva ďalších technických kritérií (tie sú často prísne utajované). Tomuto širokému spektru odpovedá i obrovské rozpätie cien. Tie sa pohybujú od niekoľko sto korún u jednoduchých "strážidlo na deti" až po niekoľko desiatok tisíc za zariadenie kvalitné a komerčne najčastejšie používané až konečne po systémy špičkovej úrovne nasadzované napr. pri medzinárodnej špionáži. Cena takéhoto zariadenia musí všeobecne prevážiť hodnotu získaných informácií - tie môžu byť tiež často k "nezaplateniu".

Systémy kontaktného snímania vibrácií - tzv. stetoskopické mikrofóny slúžiace k odpočúvaniu zvonku miestnosti cez steny, dvere, okná, radiátory. Ide o elektronickú podobu "hrnčeku na stene" - pochopiteľné znateľne citlivejší.

Rádiostetoskopy - stetoskopy umožňujúce signál vysielať.

Systémy bezkontaktného snímania vibrácií - prevažne laserové odpočúvacie zariadenia - k prenosu informácie sa využíva koherencie laserového zariadenia najčastejšie v IR obore elektromagnetického spektra.

Linkové mikrofóny - využívajú k prenosu informácie metalické vedenie

Mikrofónné sondy - väčšinou subminiatúrne citlivé mikrofóny (často s nízkošumovým predzosilňovačom) umiestené skryte alebo kamuflovane s inou kabelážou.

Dlhovlnné vysielače s prenosom po vedení (sú menej známe a o to nebezpečnejšie).

Smerové mikrofóny - priame odpočúvanie na diaľku pomocou špeciálnych mikrofonov s úzko smerovou charakteristikou. Ku zvýšeniu smerového účinku sa často používa parabolický reflektor.

Rádiové telefónne odpočúvanie - miniatúrne vysielače napojené na telefónne vedenie, ktoré vysielajú signál podobne ako priestorové ploštice. Existujú rovnako systémy, ktoré nevyžadujú priamy galvanický kontakt s telefónnou linkou (tzv. neinvazívne snímače).

Špeciálna nahrávacia technika (profesionálne záznamové systémy, upravené diktafóny s externými miniatúrnymi mikrofónmi, hlasovou aktiváciou VAS, dlhou dobou záznamu prípadne ďalšími funkciami).

Širokopásmové prehľadové prijímače - tzv. scannery pre zachytenie a dekódovanie rádiových signálov neverejných komunikácií - odpočúvanie mobilných telefónov, neverejných služieb apod. Dokonalejšie systémy môžu nielen telefónni rozhovor zachytiť, ale tiež zaznamenať, identifikovať volanú i volajúcu stanicu, čas, dĺžku rozhovoru apod.

Alternatívne spôsoby odpočúvania - niekde môžu byť zneužité na prvý pohľad regulárne zariadenie ako napr. dverné telefóny, modifikovaný reproduktor centrálneho (podnikového) rozhlasu apod., vstavané reproduktory v rádioprijímačoch apod. To úzko súvisí s maskovaním a kamuflážou.

9.3 Metódy informačného prieniku

Skrytá videotechnika - miniatúrne kamery s možnosťou bezdrôtového prenosu video a audio signálu.

Noktovízia a termovízia - veľmi jednoducho povedané noktovízia slúži k pozorovaniu za zníženej viditeľnosti alebo v tme (zosilňovač zvyškového svetla); termovízia sníma rozdielne teploty predmetu a prevádza ich do viditeľného spektra. Obidva systémy pracujú na odlišnom fyzikálnom princípe a môžu sa tak vhodne doplňovať.

Prostriedky fyziodetekcie - polygraf, analyzátory hlasu apod.

Doplnkové a účelové prostriedky - prídavné zosilňovače výkonu, meniče charakteristiky hlasu, telefónne sabotážne zariadenia apod.

Možnosti odpočúvania

Súčasná odpočúvacia technika je úžasne výkonná. V prvej rade je nutné si uvedomiť, že ten, kto má záujem o dôverné informácie a prenášané dáta, je ochotný vložiť do odpočúvacej techniky mnohokrát nemalé finančné prostriedky, a veľkú dávku vynaliezavosti. Je veľmi málo pravdepodobné, že by „plošticu“ odhalili niektorí zo zamestnancov organizácie bez akéhokoľvek technického vybavenia a skúseností v tomto odbore. Napriek tomu sa to môže podariť. Miniatúrne rádiové vysielače „ploštice“ vysielajú na vzdialenosť 25,50,150,200,500 a viac metrov. Pokiaľ je „ploštica“ napájaná z telefónnej siete, EZS alebo EPS, je životnosť takéhoto vysielača prakticky neobmedzená. Napichnutie telefónnej linky je určite ľahšie. Nie je potreba preniknúť do budovy organizácie, ale na linku sa možno pripojiť kdekoľvek na prenosovej ceste k telefónnej ústredne.

Profesionálne inštalované odpočúvanie telefónnej linky nemožno ľahko zistiť. Nevyvoláva ďalšie zvuky ani cvaknutie. Napriek tomu je na našom trhu technika, ktorá dokáže niektoré spôsoby odpočúvania telefónnej linky úspešne odhaliť. Pri prenose informácie do po telefónnych linkách je veľmi účelné používať šifrovací software. Pokiaľ priamo nezabráni v odpočúvaniu, môže ho nepríjemne skomplikovať. Na našom trhu je dostupná technika, ktorá umožňuje kvalitné šifrovanie prenášaných dát. Vždy je potrebné dbať na to, aby šifrovacia technika bola schválená pre používanie na území ČR. Niektoré „ploštice“ dnes prenášajú nielen zvuk, ale súčasne i kvalitný obraz. Pritom objektív má priemer len 2mm. Mnohokrát tieto skryté kamery fungujú ako kamery bezpečnostné, a pomohli tak pri odhalení páchateľov závažnej trestnej kriminality.

Životnosť „ploštíc“ je rôzna. „Ploštica“ môže byť v činnosti napríklad iba niekoľko málo hodín. To znamená, že je do určitého záujmového priestoru umiestnená niekoľko hodín pred dôležitou plánovanou poradou. Iné „ploštice“ sa sami uvedú do činnosti iba vtedy, keď sa v danom priestore hovorí. Ďalšie „ploštice“ sú obsluhované, zapínané a vypínané, diaľkovo. Iné „ploštice“ môžu byť pripojené priamo do zásuvky na 230V alebo k EZS a odpočúvané informácie posielajú priamo po napájacej siete. O niekoľko metrov ďalej je snímacia a záznamová technika. Iné „ploštice“ dokážu snímať nepatrné chvenie stien, radiátorov, nábytku, okenných tabúl atd. Iné sú umiestnené hlboko v stene a k okraji steny vedie iba slabá plastová trubička. Mnohé z „ploštíc“ nemožno zachytiť ani odhaliť bežným prijímačmi. Tu je nutné urobiť OTP – obranne technickú prehliadku. Prehliadky

požadovaných priestorov sa robia v dvoch fázach. Použitie veľmi drahej a špeciálnej techniky obsluhovanej špecialistami v tomto obore sa samozrejme premieta i do ceny za takúto prehliadku. Ale cena odcudzenia takýchto informácií býva často väčšia. O tom sa už presvedčili mnohé firmy i mnohí jednotlivci. Túto prehliadku môže robiť jedine firma, ktorá má dlhoročné skúsenosti a znalosti v tomto obore a je držiteľom potvrdenia NBÚ pre prácu s utajovanými skutočnosťami.

10 VYHĽADANIE ODPOČÚVACEJ TECHNIKY

Dôležitou súčasťou moderného poňatia komplexnej bezpečnosti je ochrana proti nasadeniu odpočúvacej techniky. Tejto problematike je nutné venovať značnú pozornosť. Hlavným dôvodom pre ochranu proti odpočúvaniu je ochrana informácií, s ktorými firma manipuluje.

V dôsledku rastu konkurencie v jednotlivých odvetviach podnikania rastie v poslednej dobe riziko úniku informácií, ktoré sú pre podnik dôležité. Používanie takýchto praktík je umožnené skoro úplnou beztrestnosťou. Český trestný zákon hovorí iba o odpočúvaní telefónnych rozhovorov ako o trestnom čine, ale všetky ostatné typy odpočúvania sú len porušením Listiny základných práv a slobôd občanov, teda spadajú do občiansko-právnych sporov. To však platí iba vtedy, ak sa podarí dopadnúť páchateľov týchto trestných činov. Preto by mala byť ochrana proti odpočúvaniu ďalším bezpečnostným opatrením, ktoré slúži k ochrane majetku spoločnosti. Pretože i akýkoľvek zabezpečovací systém má význam predovšetkým preventívny. V podnikoch, ktoré sa úspešne vyvíjajú by sa mala ochrana informácií stať štandardom, pretože hlavne únik dôverných informácií môže byť pre podnik katastrofálny.

Inštalácia ani získanie záznamu vo svojej podstate nie je trestným činom. Trestným činom je zneužitie získaných záznamov k páchaniu trestnej činnosti napríklad k vydieraniu. Ak inštaláciu robí tretia osoba je takmer nemožné odhaliť, ale predovšetkým potrestať páchateľa. Z tohto jednoznačne vyplýva záver, že každý občana firma si musí brániť svoj majetok a informácie sama.

10.1 Režimové opatrenia

Základom ochrany proti odpočúvania sú režimové opatrenia, ktoré majú minimalizovať riziko inštalácie odpočúvacích prostriedkov:

- kľúčový režim chránených priestorov,

- v preverovaných priestoroch sa doporučuje uskutočniť inštaláciu obranno-technických prostriedkov a zaviesť kontrolovaný pohyb osôb, vrátane upratovania a servisných činností.
- obranno-technické prehliadky robiť opakovane a pravidelne. Podľa činnosti spoločnosti i náhodnú kontrolu pred dôležitým jednaním.
- dať všeobecne najavo, že priestory sú zabezpečené proti odpočúvaniu a že sú v spoločnosti vykonávané pravidelná prehliadky,
- utajenie presného termínu prehliadky,
- dôsledne používanie elektronického zabezpečovacieho systému v kontrolovaných priestoroch.

10.2 Obranné prehliadky

Obranné prehliadky sú prostriedkom odhaľovania nasadenia prostriedkov odpočúvacej techniky. Veľké množstvo odhalených inštalácií je dôsledkom dobrej technickej znalosti pracovníkov firiem, ktoré sa špecializujú na obranné prehliadky.

Úspešnosť obranných prehliadok závisí na:

- technickom vybavení,
- skúsenostiach špecialistov,
- zložitosti prostredia nesadenia techniky,
- predpokladaná profesionálna a technická úroveň nasadenia operatívnej techniky.

Prvoradým predpokladom pre kvalitnú obrannú prehliadku je bezpečnostná spoľahlivosť firmy a jej špecialistov, ktorá prehliadku uskutočňuje.

10.3 Obranné technické prehliadky proti odpočúvaniu

Cieľom obrannej technickej prehliadky je odhalenie odpočúvacích prostriedkov, ktoré môžu byť v čase keď sa prehliadka uskutočňuje aktívne, alebo neaktívne.

10.3.1 Fyzická prehliadka

Fyzická prehliadka je nedielnou súčasťou obrannej technickej prehliadky miestností zameraná na odhalenie odpočúvacích prostriedkov umiestnených v sieťových rozvodoch, telefónnych zásuvkách, telefónnych aparátoch, vypínačoch.

Obr. 1: Fyzická prehliadka

10.3.2 Rádiová prehliadka

Rádiová prehliadka je zamarená na odhalenie všetkých činných rádiových prostriedkov detektorom RF poľa a na vytvorenie frekvenčnej mapy priestorov pomocou spektrálneho analyzátoru čo predstavuje zhotovenie zoznamu všetkých rádiových frekvencií, ktoré sa vyskytujú v kontrolovanom priestore (tj. aktívne prostriedky). Tento zoznam veľmi uľahčuje ďalšie prehliadky.

Obr. 2: Rádiová prehliadka

10.3.3 Kontrola nelinearity

Kontrola nelinearity je zameraná na vyhľadanie všetkých polovodičových súčiastok pomocou detektoru nelineárnych prechodov. Tento detektor využíva pre svoju činnosť základný predpoklad, že každý spravodajský prostriedok obsahuje aspoň jednu polovodičovú súčiastku. Táto kontrola je dôležitá z hľadiska nájdenia spravodajských prostriedkov, takých, ktoré sú diaľkove ovládané alebo také, ktoré si informácie uchovávajú vo svojej pamäti a po uplynutí periódy ich dokážu preniesť vo veľmi krátkom okamžiku alebo prenášajú informácie zo záujmového priestoru iným spôsobom. Predovšetkým v starších budovách sú týmto detektorom odhaľované i prostriedky, ktoré sú napájané zo sieťového rozvodu a sú zamurované.

Obr. 3: Kontrola detektorom nelineárnych prechodov

11 PRÍSTROJE NA VYHĽADÁVANIE ODPOČÚVANIA

Spektrálny analyzátor OSC-5000 DELUX OSCOR

Súprava mikropočítačom riadeného prijímača so spektrálnym analyzátorom v kompaktnom kufríku. Analyzátor je automatiky preladiteľný u audio systému v pásme 50 Hz - 15 kHz, u RF systému v pásme 10 kHz - 3 GHz a v IR spektre 10 kHz - 5 MHz, 850 - 1070 nm, porovnáva zvuky miestnosti s prijatým demodulovaným signálom a opticky alebo akusticky upozorňuje na odpočúvacie zariadenie. Prístroj zobrazuje prijatý signál na spektrálnom analyzátore, spracováva všetky druhy modulácií, má aktívne prepínanie antén (vrátane sondy na kontrolu magnetofónov), umožňuje kontrolu sieťových káblov a telefónnych liniek, obsahuje LCD videodispleje a trojbodový lokátor vyžarovaného signálu.

Obr. 4: Súprava prijímača so spektrálnym analyzátorom

Širokopásmový prijímač MRA-3 - Automatický pamäťový prijímač novej generácie

Špeciálny prijímač umožňujúci rýchle preladenie a následnú automatickú kontrolu kmitočtového spektra 42 až 2700 MHz. Jednotlivé signály možno vyladiť, počúvať, zmerať ich intenzitu a zachytenú frekvenciu. Celé rádiové spektrum možno uložiť do pamäte. Prepnutím do plne automatického režimu je v päťsekundových intervaloch každý prijímaný signál porovnávaný s pôvodným záznamom v pamäti. Prítomnosť nového signálu je indikovaná dvojstupňovým poplachom a zároveň je nový signál zapísaný do samostatnej poplachovej pamäte. Nastavenie prístroja cez LCD displej, pripočutie cez zabudovaný reproduktor alebo cez slúchadlový výstup.

Obr. 5: MRA-3

Detektor silného RF poľa RFDS-3 - Protiodpočúvacia detekčná a vyhľadávacia súprava

Protiodpočúvacia detekčná a vyhľadávacia súprava umiestnená v diplomat kufríku obsahuje vf detektor RFD-2 s teleskopickou anténou k automatickej detekcii najsilnejšieho blízkeho vysielača so zobrazením intenzity rádiového signálu v pásmu 1 MHz - 10 GHz.

Ďalej obsahuje:

- externú sondu EXTSOND, ktorá zväčšuje rozsah až do 20 GHz s nastaviteľnou tyčou 2,4m pro kontrolu stropov
- špeciálny generátor WHG k vyhľadávaní priechodu neznámych vodičov
- linkový adaptér LTA pre odhalenie mikrofónnych, linkových a sieťových odpočúvacích prostriedkov
- slúchadlá a dve antény pre príjem generátoru.

Obr. 6: RFDS – 3

Prehľadové prijímače

AOR 8200 MK3 - Ruční VHF/UHF komunikační prijímač, 500kHz-3000MHz

Ruční prehľadný prijímač vhodný pro príjem všetkých analógových rádiových mikrofónov. Plynule laditeľný od 500 kHz do 3 GHz, 1000 pamätí frekvencií, 9 typov modulácií, inteligentný filter, jednoduchý spektrálny analyzátor, hmotnosť 340 g vrátane akumulátora, rozmery 61x143x39 mm. Možnosť napojenia na počítač, možnosť vloženia dekodéru.

Obr. 7: AOR 8200 MK3

ALINCO DJ-X30E

ALINCO DJ-X30E je malý a cenovo dostupný prehľadný prijímač, vhodný i k príjmu analógových rádiových mikrofónov. Kmitočtový rozsah je 100kHz - 1300MHz. Modulácia AM, NFM, WFM, 1000 pamätí, 16 krokov ladenia. Prijímač má päť režimov skenovania a vyhľadáva i CTCSS kmitočty. Rozmery sú 58x99x32 mm, hmotnosť 165g. Napájanie 2x AA články. Anténny konektor SMA, prijímač sa dá prepojiť s PC pomocou USB rozhrania.

Obr. 8: ALINCO DJ-X30E

Osobný detektor RF poľa - RVD

Vreckový detektor vysokofrekvenčného poľa so svetelnou a vibračnou indikáciou. Prístroj je vo vreckovom prevedení s vysokou citlivosťou. Je vybavený trojstupňovou filtráciou rušivých signálov a indikácií sily poľa pomocou rady 5 LED. Kmitočtový rozsah 0,2 až 4000 MHz s možnosťou voliť pásma HF 0,2 - 4000 MHz, VHF 40 - 4000 MHz a UHF 300 - 4000 MHz. Hradlo poplachové indikácie je pri +3 dB proti hodnote pozadia. Napájanie 9V batérie, rozmer 121x58x22 mm.

Obr. 9: RVD

Analyzátor telefónnych liniek DPA-7000 Talan - Analyzátor káblových vedení, vrátane digitálnych

Špeciálny analyzátor liniek a vedení Talan je určený k testovaniu všetkých elektrických a elektronických káblových rozvodov vrátane digitálnych telefónnych liniek. Prístroj okrem napätia, prúdu, kapacity, robí i demoduláciu digitálnych liniek, kontrolu RF spektra a meranie detektorom nelineárnych prechodov. U viačžilových vedení meria všetky vzájomné kombinácie párov vodičov. Uchováva namerané hodnoty pre následné porovnanie s inými meraniami. Odhalí akékoľvek elektronické zariadenie pripojené na kontrolované vedenie.

Obr. 10: DPA-7000 Talan

Detektor nelineárnych prechodov NJE-4000

Ľahký, s hmotnosťou 1,6 kg, skladací detektor nelineárnych prechodov na 2. a 3. harmonickou. Výkon vysielača regulovateľný od 14 mW do 1,4 W. Pracovná frekvencia 850 až 1005 MHz.. Vybavený bezdrôtovými IR slúchadlami.

Obr. 11: NJE-4000

Doplnkové a jednoúčelové prístroje

Borescop - Optický prístroj na prehliadanie neprístupných dutín

Sonda sa zasunie do dutiny vyvŕtaným otvorom. Používajú sa pevné alebo flexibilné borescopy. Pohľad je možný podľa typu použitého borescopa.

Obr. 12: Pevný a flexibilný borescop

VPC-64 - Kamera s monitorom na teleskopickej tyči

Zariadenie slúži k preskúmavaniu neprístupných priestorov. Na konci teleskopickej tyče je umiestnená čiernobiela nebo farebná kamera s možnosťou natáčania. V rukoväti tyče je LCD monitor.

Obr. 13: VPC-64

12 OCHRANA PROTI ODPOČÚVANIU

SNG - inteligentní šumový generátor

Umožňuje pripojenie až 100 piezokeramických akustických meničov, 2-12 nízkoimpedančných reproduktorov, alebo ich vzájomnú kombináciu. Účelom zašumenia je zaistiť ochranu priestoru proti všetkým formám snímania zvuku z okien, stien a pod. Šumová ochrana proti odpočúvaniu spočíva v priamom mechanickom zašumení miest, kde je možné zvuky snímať. Účinnosť SNG optimalizuje procesor, ktorý v automatickom režime analyzuje zvuky v miestnosti a zabezpečuje len takú úroveň zašumenia, ktorá je nutná v závislosti na hlasitosti konverzácie.

Obr. 14: SNG

Rušička parazitného vyžarovania PC

ZOD-301 - Generátor maskovacieho signálu pre ochranu počítačov

Umiestňuje sa vedľa počítača a pripojuje sa do rovnakej zásuvky ako počítač. Ochráni počítač vrátane periférneho zariadenia, ktoré je umiestnené v sférickom priestore o priemere 4m okolo generátoru.

Obr. 15: ZOD-301

Rušička mobilných telefónov

GSM-OUT Spy-Indikátor prevádzky mobilného telefónu GSM (pásmo 900 a 1800 MHz)

Zariadenie slúži k zaisteniu prítomnosti zapnutého mobilného telefónu GSM. Má optickú diódu (LED) a zvukovú signalizáciu. Dokáže rozlíšiť či sa odosiela SMS alebo prebieha hovor. Vo vnútri je umiestnené relé, ktoré môže spínať ďalšie zariadenie ako napríklad hlásič.

Obr. 16: GSM-OUT Spy

ZÁVER

Na záver možno skonštatovať, že podnikateľské (komerčné) spravodajstvo vnáša do podnikania na jednej strane niektoré inak nedostupné informácie, na strane druhej zvyšuje prostredníctvom defenzívneho spravodajstva ochranu vlastných informácií, vrátane tých, ktoré boli získané metódami komerčného spravodajstva. Je potrebné podotknúť, že určitým spôsobom ovplyvňuje toho, kto ovplyvnený má byť.

Práca sa snaží v hlavných kapitolách priblížiť problematiku komerčného spravodajstva s prihliadnutím na situáciu v Českej republike. Po načrtnutí všeobecnej problematiky, je jedna z kapitol venovaná hlavnej problematike diplomovej práce, vymedzeniu pojmu defenzívne (obranné) spravodajstvo, čo bolo jedným z cieľov práce. Tento typ spravodajstva je vývojovo vyššie než aktívne spravodajstvo a je používaný u veľmi veľkých, hlavne nadnárodných firiem, firiem s veľkou patentovou aktivitou a ďalších.

Práca popisuje i úlohu detektívneho spravodajstva, ktoré predstavuje významnú formu súkromnej detektívnej činnosti a je významným prvkom komerčného spravodajstva.

Ďalšie z kapitol pomáhajú pochopiť legislatívne podmienky spojené s problematikou odpočúvania a s problematikou prijatia zákona o súkromných bezpečnostných službách v Českej republike.

Problematike odpočúvania a hlavne prístrojom a prostriedkom na vyhľadanie odpočúvacej techniky je venovaná časť praktickej časti diplomovej práce. V podnikoch, ktoré sa úspešne vyvíjajú by sa mala ochrana informácií stať štandardom, pretože hlavne únik dôverných informácií môže byť pre podnik katastrofálny.

CONCLUSION

In conclusion is possible submit, that business (commercial) intelligence is bringing into business on one hand some inaccessible information, on the other hand increases by defensive commercial intelligence protecting own information, including information, which was acquired with method commercial intelligence. Is necessary to remark, that specific method is affecting of that, who affecting are to by.

Diplomas try in general chapters approach problems commercial intelligence with consideration on situation in Czech Republic. One of chapter is dedicating basic problems of diploma thesis, allocation concept defensive commercial intelligence, what was one of aims diploma. This type of intelligence is developmental higher than active intelligence and is used at extra large, primarily supranational companies, companies with big patent activity.

Diploma describes also work detective intelligence, which presents significant form private detective activities and is significant element of commercial intelligence.

Other from chapter helps understand legislative conditions connected with problems tapping and with problems receiving law about private security service in Czech Republic.

The Problems tapping and especially apparatus and resources on detection listening techniques are devoted part practical parts diploma thesis. In companies, which successfully develop, protect of information should become standards, because especially escape intimate information can be for company disastrous.

ZOZNAM POUŽITEJ LITERATÚRY

[1] BRABEC, František, vedoucí autorského kolektivu, LÁTAL, Ivo, MUSIL, Rudolf, URBAN, Miloš, VEJLUPEK, Tomáš, PILNÝ, Ivan. *Bezpečnost pro firmu, úřad, občana*. Praha : Public History, 2001. 400 s. ISBN 80-86445-04-06.

[2] BRABEC, František. Národní program konkurenčního zpravodajství (NPKZ) - historická příležitost. *Security Magazín*. 2003, č. 11/12, s. 47-49.

[3] BRABEC, František. Nestátní zpravodajství - primární zdroje. *Security Magazín*. 2007, č. 7/8, s. 48-51.

[4] BRABEC, František. Nestátní zpravodajství a jeho sekundární zdroje. *Security Magazín*. 2007, č. 5/6, s. 60-62.

[5] BRABEC, František. Podnikatelské (komerční) zpravodajství - vlivové zpravodajství (lobbing). *Security Magazín*. 2003, č. 1/2, s. 52-53.

[6] BRABEC, František. Problémy s přijetím zákona o SBS v ČR. *Security Magazín*. Listopad/Prosinec 2005., č. 11/12, s. 36-38.

[7] BRABEC, František. Zpravodajství jiné než v televizi: Podnikatelská spravodajská činnost. *Profit Speciál*., roč. 2001, č. 11, s. 2-13.

[8] *Business center.cz : Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)* [online]. c1998 - 2008 [cit. 2008-04-03]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/trestni_rad/>.

[9] *Business center.cz : Zákon č. 2/1993 Sb. - Listina základních práv a svobod* [online]. c1998-2008 [cit. 2008-05-13]. Dostupný z WWW: <http://business.center.cz/business/pravo/zakony/listina-zakladnich-prav-a-svobod/>.

[10] *Co je zpravodajská technika?* [on-line]. [cit. 2008-03-04]. Dostupný z WWW: <http://www.infosafe.cz/index.htm>.

[11] Detektory odposlechu [online]. 2007- [cit. 2008-01-14]. Dostupný z WWW: <http://www.detekce.com/technika_proti_odposlechu_odposlech.htm>.

[12] *E-law : Úmluva o ochraně lidských práv a základních svobod a další smluvní dokumenty na tuto Úmluvu navazující* [online]. c2007 [cit. 2008-05-12]. Dostupný z WWW: <http://www.e-law.cz/zakony/euumluva.htm>.

[13] KAMENÍK, Jiří, BRABEC, František. *Komerční bezpečnost : Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. 1. vyd. Praha : ASPI, a.s., 2007. ISBN 978-80-7357-3.

[14] LANDA, Jaroslav. Získávání a ochrana informací : Část 4 - Speciálni technika. *Security Magazín*. Prosinec 2005., č. 12, s. 43-45.

[15] *Ministerstvo vnútra Slovenskej republiky : Zákon číslo 473/2008 Zz. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene doplnení niektorých zákonov (zákon o súkromnej bezpečnosti).* [online]. 4.5.2008 [cit. 2008-05-17]. Dostupný z WWW: <http://www.minv.sk/legislativa/473sbs.htm>.

[16] *Odposlechy.com - Elektornické systémy* [online]. Copyright c1999 - 2008 [cit. 2008-01-13]. Dostupný z WWW: <http://www.odposlechy.com/>.

[17] *Odposlechy.cz* [online]. c2008 [cit. 2008-05-03]. Dostupný z WWW: <http://www.odposlechy.cz/law/sk.html>.

[18] *PROBIN s.r.o. - odposlech, šifrované telefony* [online]. c2001-2006 [cit. 2008-04-05]. Dostupný z WWW: <http://www.probin.cz/>.

[19] *Projekt Bibliografické citace* [online]. c2004-2008 [cit. 2008-05-03]. Dostupný z WWW: <http://www.citace.com/>.

[20] *SafeCom s.r.o.* [online]. c2007 Webczech spol s r.o. [cit. 2008-04-06]. Dostupný z WWW: <http://www.safecom.cz/>.

[21] 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.

[22] *Vyhledání štěnic, odposlechů, ochrana proti průmyslové špionáži, Ochrana proti nasazení operativní (odposlechové) techniky* [online]. c2003, 18.4.2003 [cit. 2008-04-07]. Dostupný z WWW: <http://www.fortunecity.com/business/investment/52/>.

[23] KUCHTA, Jozef, VÁLKOVÁ, Helena, a kolektiv. *Základy kriminologie a trestní politiky*. Praha : [s.n.], 2005. 576 s. ISBN 80-7179-813-4.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

SBS	Súkromná bezpečnostná služba.
EZS	elektronická zabezpečovacia signalizácia
EPS	elektronická protipožiarna signalizácia
GSM	Globálny Systém pre Mobilnú komunikáciu pôvodne však francúzsky „Groupe Spécial Mobile“
LED	Svetlo - vyžarujúca dióda pôvod z anglického Light-Emitting Diode
LCD	Light-Emitting Diode

ZOZNAM OBRÁZKOV