Latentní trestná činnost v podnicích průmyslu komerční bezpečnosti

Latent crime enterprises in the commercial security industry

Bc. Jaromír Polášek

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jaromír POLÁŠEK**
Osobní číslo:	**A09388**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Latentní trestná činnost v podnicích Průmyslu komerční bezpečnosti**

Zásady pro vypracování:

Cíl: Najít aktivní způsoby ochrany podniků PKB proti vnitřní latentní kriminalitě.

1. **Vyhodnotit dosud páchanou trestnou činnost zaměstnanců podniků PKB.**
2. **Popsat a zanalyzovat tuto trestnou činnost.Stanovit příčiny a upozornit na důsledky této činnosti.**
3. **Chyby v personální politice podniků PKB.**
4. **Formy a metody odhalování této trestné činnosti.**
5. **Spolupráce se státní administrativou dosud a v budoucnosti.**
6. **Návrhy aktivních opatření**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, František. Ochrana bezpečnosti podniku, Praha: Eurounion, 1996. ISBN 80-86445-04-6.**
2. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. 1. vyd. UTB Zlín 2004, 123s.**
3. **ČÍRTKOVÁ, Ludmila. Policejní psychologie. 1.vyd. Nakladatelství Aleš Čeněk,2006, 310s., ISBN 80-86898-73-3.**
4. **PORADA, Viktor. Kriminalistika. 1.vyd. Akademické nakladatelství Cerm,2001,746s., ISBN 80-7204-194-0.**
5. **BRABEC, František. Hlídací služby. 1. vyd. Praha: Eurounion, 1995. 259 s. ISBN 80-85858-12-6.**

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

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

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce se věnuje latentní kriminalitě v podnicích průmyslu komerční bezpečnosti. V úvodní části je tato kriminalita definována a jsou zde také popsány nejčastější způsoby, příčiny a podmínky jejího páchání. Poté zde popisuji personální politiku a formy a metody odhalování latentní kriminality. Závěrečná část patří výsledkům mého bádání, rozboru případů a návrhům aktivních opatření proti vnitřní latentní kriminalitě v podnicích průmyslu komerční bezpečnosti.

Klíčová slova: latentní kriminalita, soukromé a bezpečnostní služby, hospodářská kriminalita, průmysl komerční bezpečnosti

ABSTRACT

This work focuses on latent crime enterprises in the commercial security industry. In the introductory part of this crime are defined and described the most common ways to causes and conditions for its perpetration. Then I describe the personnel policies and forms and methods of detection of latent crime. The final section includes the results of my research, analysis and proposals in cases of active measures against internal latent crime in the commercial security industry companies.

Keywords: latent crime, privacy and security services, economic crime, the commercial security industry

Tímto bych chtěl poděkovat svému vedoucímu diplomové práce JUDr. Vladimíru Lauckému za odborné znalosti, připomínky a rady, které mi poskytoval při vypracovávání mé práce. Dále bych rád poděkoval všem bezpečnostním agenturám, které se nebály odpovídat na mé dotěrné dotazy.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Ve své práci se budu zabývat latentní kriminalitou v podnicích průmyslu komerční bezpečnosti, kdy o tomto tématu nebyla publikována ani stránka a příliš se o něm nemluví. Jedním z důvodů je i možnost, že v případě odhalení utrpí pověst bezpečnostních agentur a tím i možnou ztrátu zakázek v budoucnu.

Latentní kriminalita v podnicích průmyslu komerční bezpečnosti se bude pohybovat jak u pracovníků na nižších pozicích, tak u pracovníků zařazených na řídících místech s možností napadnout ekonomické vazby a tím získat přístup k finančním hotovostem. Tyto a další možné způsoby rozkrádání budou rozebrány v další části.

Toto téma jsem si zvolil, protože jsem ve dvou bezpečnostních agenturách pracoval a toto prostředí je mi známé. Během psaní práce jsem také mohl využít kontaktů, které jsem při těchto brigádách získal.

Cílem této práce je najít aktivní způsoby ochrany pracovníků podniků průmyslu komerční bezpečnosti před možností páchání latentní kriminality. V této diplomové práci je také rozebráno, které nedostatky v personální práci vyúsťují v možnosti páchání latentní kriminality. Z tohoto důvodu použiji několik případů krádeží, které se mi podařilo vytěžit a v těchto případech poukáži na chyby, které usnadnily spáchání této trestné činnosti.

Při zpracování tohoto tématu byla největším problémem neochota některých bezpečnostních agentur, vyjadřovat se k problematice rozkrádání vlastními zaměstnanci.

Při vypracování diplomové práce jsem použil tři vědecké metody: Analýzu, kompilaci a syntézu. Metodu analýzy jsem použil v teoretické části práce a také při rozboru nejzávažnějších případů. Při sběru informací z internetu a médií bylo použito kompilace a při tvorbě závěru mi pomohla syntéza.

Práce je rozdělena na teoretickou část, což je prvních pět kapitol zaměřených na právní prostředí, způsoby rozkrádání v podnicích PKB, příčiny a podmínky páchání této činnosti, personální politiku podniků PKB a formy a metody odhalování latentní kriminality. Praktickou část tvoří poslední tři kapitoly, které obsahují výsledky dotazování bezpečnostních agentur, analýzu dosud páchané latentní kriminality a návrhy aktivních opatření, které by mohly zabránit páchání této kriminality.

I. TEORETICKÁ ČÁST

1 LATENTNÍ KRIMINALITA

Latentní kriminalita bývá často skloňována ve všech pádech a je předmětem dohadů, zda je či není ve skutečnosti páchána. Je to část kriminality, kdy vůbec nevyjde najevo, že byla spáchána závažná trestná činnost a proto se nestane předmětem trestního stíhání. Latentní kriminalita neodráží realitu objasňování trestných činů. Často značně zkresluje statistické údaje o zločinnosti, které shromažďují orgány činné v trestním řízení (jde o statistiky policejní, státního zastupitelství a soudní). Tyto evidence jsou hlavními prameny pro získávání poznatků o stavu a vývoji zločinnosti. Latentní kriminalita zahrnuje ty trestné činy, které vůbec nebyly spáchány tzn. ani nebyly oznámeny či zjištěny. Dále sem řadíme trestné činy, které sice byly policií zjištěny, ale nikdy nebyli vypátráni pachatelé, kteří je způsobili. Pod latentní kriminalitu spadají i ty případy, kdy došlo ke stíhání pachatele, ale z nejrůznějších důvodů nebyl vynesen odsuzující rozsudek. Rovněž sem patří případy, kdy se pachatel dopustil více trestných činů a není stíhán pro všechny trestné činy, ale jen pro některé z nich. Nikde nejsou evidovány přesná čísla nebo poměr latentní kriminality s kriminalitou obecnou. Jde pouze o odhady, ale v odborných kruzích zabývajících se latentní kriminalitou se zjišťuje, že tato zjištěnou kriminalitu několikanásobně převyšuje. [22]

Obecně se uvádí, že čím nižší je společenská nebezpečnost trestného činu, tím vyšší je jeho latence. Z tohoto důvodu latentní kriminalita zejména v oblasti hospodářské působí těmto organizacím velký problém. Proto, ať nečekají, že policie v oblasti soukromého majetku bude odhalovat tuto latentní kriminalitu. Toto je vždy věcí vedoucích hospodářských pracovníků, kteří musí dbát na to, aby majetek, kterým disponují, nebyl napadán jedinci, kteří působí v různých řídících funkcích.

V podnicích komerční bezpečnosti lze takovouto latentní trestnou činnost rozdělit [15]:

1) Vzhledem ke vztahu k poškozenému objektu:
   a) *Ve vztahu k zákazníkovi*- zde se jedná např. o drobné krádeže strážných, kteří mají naopak vykonávat dohled, případně hlídat objekty, zboží, materiály apod. Dále pak vynášení informací týkajících se zákazníka a jeho know-how. Případné odhalení takovéto kriminality je hrozbou pro podnik komerční bezpečnosti, neboť tato informace v rukou konkurence je velikou zbraní, poškozující solidnost a důvěryhodnost PKB.

b) *Ve vztahu k podniku komerční bezpečnosti*- krádeže zaměstnanců, vynášení informací z firmy a porušení mlčenlivosti, případně porušení ochrany osobních údajů.

2) Vzhledem ke způsobu provedení:
   a) Fyzické krádeže zboží, materiálu, finančních hotovostí, tištěných informací.
   b) Elektronické krádeže dat, a jiných stěžejních elektronických informací

1.1.1 Hospodářská oblast

V hospodářské oblasti je třeba zdůraznit význam soukromé detektivní činnosti v trestně právní oblasti. Jedná se především o vyhledávání latentní kriminality hospodářského charakteru v podniku.

Termín hospodářská (ekonomická) kriminalita má několik vrstev a v odborné literatuře bývá definována nejednotně. Pokud se hospodářské trestní právo chápe jen jako součást trestního práva, pak zahrnuje pouze trestné činy, které podrývají systém a fungování tržní ekonomiky. Tato hospodářská trestná činnost se opírá především o ustanovení trestního zákoníku. Vedle této hospodářské kriminality stojí ale delikty, které jsou sice mimo rámec vlastního hospodářského života, ale mají s ním souvislost (např. kontextovou, příčinnou, následkovou). Jde například o podvod, zpronevěru apod., které nejsou sice charakterizovány jako bezprostředně trestné činy ekonomické kriminality, ale velmi často s touto souvisejí a odehrávají se jak v občanské tak ekonomické rovině. [5]

Rozkrývání ekonomické kriminality v podniku je jednou z velmi složitých činností v rámci soukromě detektivních služeb. Spadá do oblasti ochrany ekonomických zájmů. Vzhledem k její složitosti a náročnosti nelze při její realizaci spoléhat jen na získané zkušenosti, dovednosti a návyky. Proto také pokud má soukromá detektivní činnost úspěšně působit v oblasti ochrany ekonomických zájmů a zejména pak v oblasti vyhledávání latentní ekonomické kriminality, musí vycházet z analýzy situací a jevů, které ekonomickou kriminalitu vyvolávají, způsobují a usnadňují. Musí se opírat o obecné poznatky kriminologické vědy, i o kriminologickou analýzu v daném podniku. V návaznosti na to je nezbytné provést analýzu a zkoumat situace, jevy a procesy, které

vznik ekonomické kriminality omezují nebo dokonce znemožňují a o ty se v soukromé detektivní činnosti opírat. [5]

Je třeba se zmínit také o existenci profesionální kriminality, kde lze vedle různých forem organizovaného zločinu řadit i tzv. kriminalitu bílých límečků, resp. white collar crime. Tento pojem zavedl v roce 1939 kriminolog Edwin H. Sutherland, když definoval hospodářský zločin jako jednání, které spáchala vážená, vysoce společensky postavená osoba v rámci svého povolání, využívajíc své důvěry vyplývající z jejího vysokého sociálního statutu a prestiže, náležející k této společenské vrstvě. [7]

Dnes je možné chápat trestnou činnost tzv. bílých límečků jako hospodářskou trestnou činnost, páchanou při výkonu profese představitelem legálního podnikaní, tj. obcházení pravidel a porušování zákonů v rámci výkonu profese na místě, které to umožňuje s cílem získat vyšší zisk. Jiná definice zase říká, že bílými límečky jsou středně a vysoce kvalifikované osoby, lidé s vysokou odpovědností, pravomocí, v důvěryhodném postavení. [7]

Nejzávažnějšími případy latentní kriminality jsou finanční krádeže, které mohou nejlépe provést právě vysoce postavení zaměstnanci, kteří mají potřebné informace a znalosti systému.

1.2 Právní prostředí

V souvislosti s latentní kriminalitou můžeme hovořit o tzv. podvodném jednání. To je možné označit jako loupež beze zbraně. Základem jsou nezákonné manipulace a jiná nežádoucí činnost využívající nepravdivé, upravené, neúplné či jinak zkreslené informace vedoucí k neoprávněnému obohacení osoby, která tuto činnost provádí. Takové podvodné jednání uvnitř podniku bývá důsledkem nepoctivého jednání zaměstnanců a to často vysoce postavených. Vždy jsou to lidé se znalostí systému a disponující informacemi. Tyto činy mají společné znaky, mezi které patří [17] :

- Podvodná jednání jsou prováděna beze zbraně
- Motivem je obohacení se
- Pachatel uvádí jiného v omyl nebo ho využije či zatají podstatné skutečnosti
- V současnosti se stále více využívají technologické vymoženosti

- Provedená podvodná operace se zprvu jeví jako standardní úkon
- Vysoká variabilnost
- Úspěšné případy představují vysoké škody a mají stoupající tendenci
- Podvodná jednání využívají nedostatky v kontrolní činnosti
- Jsou využívány i omezené možnosti sdílení informací mezi konkurenty či jinými subjekty
- Využívání nedostatků zákona

V souvislosti s latentní kriminalitou nás zajímá zákon č. 40/2009 Sb. trestního zákoníku, konkrétně část první, hlava II: Trestní odpovědnost:

- §13 Trestný čin
- §14 Přečiny a zločiny

Dále pak část druhá, hlava V: Trestné činy proti majetku:

- §205 Krádež
- §206 Zpronevěra
- §207 Neoprávněné užívání cizí věci
- §209 Podvod
- §228 Poškozování cizí věci
- §230 Neoprávněný přístup k počítačovému systému a nosiči informací

Část druhá, hlava VI: Trestné činy hospodářské

- §259 Vystavení nepravdivého potvrzení a zprávy

Co se týká zákonů a vyhlášek spojených s problematikou ochrany informací, je jich u nás několik set a proto se zaměřuji na dva hlavní, se kterými se běžně v životě setkáváme. Je to zákon č. 262/2006 Sb., zákoník práce, konkrétně hlava VIII :

- §316 Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance

A na závěr uvádím zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti.

1.2.1 Trestný čin - §13 zák. č. 40/2009 Sb.

(1) Trestným činem je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně.
(2) K trestní odpovědnosti za trestný čin je třeba úmyslného zavinění, nestanoví-li trestní zákon výslovně, že postačí zavinění z nedbalosti. [16]

1.2.2 Přečiny a zločiny- §14 zák. č. 40/2009 Sb.

(1) Trestné činy se dělí na přečiny a zločiny.
(2) Přečiny jsou všechny nedbalostní trestné činy a ty úmyslné trestné činy, na něž trestní zákon stanoví trest odnětí svobody s horní hranicí trestní sazby do pěti let.
(3) Zločiny jsou všechny trestné činy, které nejsou podle trestního zákona přečiny; zvlášť závažnými zločiny jsou ty úmyslné trestné činy, na něž trestní zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně deset let. [16]

1.2.3 Krádež - § 205 zák. č. 40/2009 Sb.

(1) Kdo si přisvojí cizí věc tím, že se jí zmocní, a

a) způsobí tak na cizím majetku škodu nikoliv nepatrnou,
b) čin spáchá vloupáním,
c) bezprostředně po činu se pokusí uchovat si věc násilím nebo pohrůžkou bezprostředního násilí,
d) čin spáchá na věci, kterou má jiný na sobě nebo při sobě, nebo
e) čin spáchá na území, na němž je prováděna nebo byla provedena evakuace osob,
bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty. [16]

1.2.4 Zpronevěra - §206 zák. č. 40/2009 Sb.

(1) Kdo si přisvojí cizí věc nebo jinou majetkovou hodnotu, která mu byla svěřena, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 větší škodu.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,

b) spáchá-li takový čin jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného. [16]

1.2.5 Neoprávněné užívání cizí věci - §207 zák. č. 40/2009 Sb.

(1) Kdo se zmocní cizí věci nikoli malé hodnoty nebo motorového vozidla v úmyslu je přechodně užívat, nebo

kdo na cizím majetku způsobí škodu nikoli malou tím, že neoprávněně takové věci, které mu byly svěřeny, přechodně užívá,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,

b) spáchá-li takový čin jako člen organizované skupiny, nebo

c) způsobí-li takovým činem značnou škodu. [16]

1.2.6 Podvod - §209 zák. č. 40/2009 Sb.

(1) Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 větší škodu.
(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,
b) spáchá-li takový čin jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,nebo
d) způsobí-li takovým činem značnou škodu. [16]

1.2.7 Poškozování cizí věci- §228 zák. č. 40/2009 Sb.

(1) Kdo zničí, poškodí nebo učiní neupotřebitelnou cizí věc, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 na věci svědka, znalce nebo tlumočníka pro výkon jejich povinnosti,

c) spáchá-li takový čin na věci, která požívá ochrany podle jiného právního předpisu, nebo

d) způsobí-li takovým činem značnou škodu. [16]

1.2.8 Neoprávněný přístup k počítačovému systému a nosiči informací -§230 zák. č.40/2009 Sb.

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo

b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) způsobí-li takovým činem značnou škodu,

d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo

e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem. [16]

1.2.9 Vystavení nepravdivého potvrzení a zprávy §259 zák. č.40/2009 Sb

Kdo jménem banky nebo jiného podnikatele oprávněného k provozování finanční činnosti podle jiného právního předpisu vystaví jinému nepravdivé potvrzení o jeho finanční situaci nebo jeho majetkových poměrech, nebo kdo jako auditor vystaví jinému nepravdivou zprávu auditora nebo nepravdivé potvrzení o finanční situaci nebo majetkových poměrech, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti. [16]

1.2.10 Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance §316 zák. č.262/2006 Sb.

(1) Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.
(2) Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.
(3) Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění. [24]

1.2.11 Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy. Zabezpečené oblasti se podle nejvyššího stupně utajení utajované informace, která se v nich ukládá, zařazují do kategorií:

a) Vyhrazené
b) Důvěrné
c) Tajné
d) Přísně tajné

Zabezpečené oblasti se podle možnosti přístupu k utajované informaci zařazují do tříd:
a) třída I, kdy vstupem do této oblasti dochází k seznámení s utajovanou informací,
b) třída II, kdy vstupem do této oblasti nedochází k seznámení s utajovanou informací.

Za naplňování zákona č. 412/2005 Sb. je zodpovědný Národní bezpečnostní úřad. Do náplně činností NBÚ patří bezpečnostní prověrky, certifikace informačních systému a kryptografických prostředků atd. Zákon spolu s řadou vyhlášek představuje ucelenou soustavu na ochranu zvláštního druhu informací. Jsou zde podrobně popsány požadavky na bezpečnost v jednotlivých oblastech. [10]

2 ROZKRÁDÁNÍ V PODNICÍCH PKB

Podniky průmyslu komerční bezpečnosti se nijak neliší od ostatních podniků, pokud se jedná o rozkrádání firemního majetku vlastními zaměstnanci. Latentní kriminalita je problém, jehož opomíjení může mít často pro firmu nedozírné následky a proto je nutno tento problém neustále sledovat a řešit. V případě malého náznaku je nutno vyvozovat okamžité závěry tak, aby se předešlo spáchání závažné kriminality.

2.1 Způsoby rozkrádání

Mezi nejčastější způsoby latentní kriminality v podnicích PKB patří :

2.1.1 Peněžní krádeže

Nejzávažnější činy páchané zaměstnanci podniků průmyslu komerční bezpečnosti jsou peněžní krádeže. V žebříčku největších krádeží v historii samostatné České republiky jsou na prvních příčkách právě ty, které způsobili tehdejší nebo bývalí zaměstnanci bezpečnostních agentur. Ti denně přicházejí při převozech do styku s obrovskými sumami peněz. Mnohdy mají přístup i do podnikového trezoru a to jsou ve firmě zaměstnáni třeba jen krátce. Jedním z mnoha důvodů, které jsou rozebrány v této práci, je zřejmě i to, že bezpečnostním agenturám brání ve vyšší prověrce zaměstnanců ustanovení zákona 101/2000Sb. o ochraně osobních údajů. V současnosti stačí mimo jiné doložit výpis z rejstříku trestů. Ten je ale možné po určité době nechat vymazat. Do firmy tak v krajním případě může být přijat i dříve trestaný člověk, který má třeba tři zahlazené tresty. Situace je taková, že příliš velký plat nemůže očekávat a v případě, že mu denně projdou rukama doslova miliony, bude jeho pokušení ke krádeži veliké. Je ale také dost možné, že do agentury už s úmyslem krást nastupoval.

Dalším možným případem peněžních krádeží může být vrátný, který má v náplni práce mimo jiné vybírání poplatků například za vjezd vozidel do objektu. Při nedostatečné kontrole si může část poplatků nechávat a přilepšovat si tak ke svému platu. To může činit také pomocí vydávání nepravdivých potvrzení.

Podobným, avšak daleko hůře odhalitelným případem je kriminalita vedoucích pracovníků, tzv. bílých límečků. Tyto druhy zločinnosti často nevyplývají z potřeb uspokojení individuálních potřeb (podrobněji v další kapitole), ale stávají se jistou formou

podnikání- zločinných podnikatelských aktivit. Je to vysoce latentní činnost, která je těžce odhalitelná.

2.1.2 Krádeže materiálu

Snad v každé větší firmě se někdy setkali s tímto problémem a ani bezpečnostní agentury nejsou výjimkou. Podniky zabývající se například instalací poplachových systémů můžou mít problém s rozkrádáním montážního materiálu. Kde není hlídán a evidován doslova každý šroubek, je odcizení pro zaměstnance velikým lákadlem. Platí to zejména pro montéry, protože ostatní zaměstnanci by si s takovým materiálem pravděpodobně nevěděli rady. Riziko hrozí i při samotné montáži, kdy montér některý komponent nenainstaluje a ponechá si ho. Pokud to není na první pohled patrné, později se bude krádež dokazovat jen těžko. Zaměstnanci také mohou zneužívat různé nástroje potřebné pro montáže, které si berou pro vlastní potřebu domů. Poté je opotřebované vrátí na své místo a nikdo si ničeho nevšimne.

2.1.3 Krádeže firemních zakázek

Značnou možnost latentní kriminality umožňují také tzv. "vedlejší pracovní aktivity a vazby" pracovníků PKB, kdy právě zde uplatňují zkušenosti získané v PKB, zneužívají informace, eventuálně používají výstroj, výzbroj a kradený materiál.

Pokud má firma například rozjednanou zakázku na zabezpečení nějakého objektu, může se stát, že jeden i více zaměstnanců se s možným zákazníkem tajně domluví a zakázku provedou soukromě. Zákazník poté s firmou přestane komunikovat a peníze jdou do kapes nepoctivých zaměstnanců. Dalším možným případem je, že si zaměstnanci takový kšeft s potencionálním zákazníkem sami dohodnou a vystupují jménem firmy, avšak ta o takovém jednání nemá ani ponětí. Práce může být provedena i s materiálem, který jí byl ukraden.

Může se také objevit snaha některého z vedoucích pracovníků převést činnosti, které zpracovává na sebe a tzv. se trhnout. To může být doprovázeno i snahou zlákat k odchodu ostatní zaměstnance a založit si třeba vlastní firmu, ale takové pokusy končí většinou neúspěchem.

2.1.4 Krádeže výzbroje, výstroje, střeliva

Výzbroj a střelivo se většinou neustále předávají z jednoho zaměstnance na druhého, proto by případné zmizení bylo hned zaznamenáno. Veškeré pohyby zbraní a střeliva musí být ze zákona evidovány. Horší je to v případě, že se nějakou dobu nepoužívají, anebo jsou pouze uskladněny pro budoucí použití. V trezoru může být větší množství nábojů, ale každý den se bere do rukou třeba jen jeden zásobník. Bez důsledné kontroly není možné přesně dokázat, kdy a kým mohly být uskladněné náboje zcizeny. Pokud je ve firmě uskladněno větší množství výstroje a ta není řádně evidovaná a hlídaná, může si zaměstnanec odnést například služební bundu, z té odpárat nášivky a poté ji užívat jako svou vlastní.

Obr. 1 *Krádeže výzbroje, výstroje a střeliva [27]*

2.1.5 Zneužívání služebních vozidel k osobním účelům

Zaměstnanci mohou zneužít služebních vozidel a vědomi si toho, že pár desítek najetých kilometrů navíc si nikdo nevšimne, vyřizují mnohdy i v pracovní době své osobní záležitosti. Při doplňování paliva na čerpací stanici mohou také část natankovat do svého vlastního kanystru. Při nedůsledném kontrolování jim to může procházet léta.

2.1.6 Zneužívání služebního telefonu

Vyřizování soukromých hovorů služebním telefonem je už běžná záležitost. Ačkoliv způsobů, jak nepoctivého zaměstnance zjistit je spousta, protože se při měsíčních vyúčtováních neobjeví většinou příliš vysoká a podezřelá částka, vedení si této skutečnosti nevšímá nebo ji toleruje. Horší je to v případě, kdy je k soukromým hovorům zneužíván telefon, který má sloužit výhradně ke komunikaci například mezi centrálním dispečinkem a výjezdovou skupinou. V krajním případě může díky obsazenému telefonu dojít k daleko větším škodám než jen k vyššímu účtu za telefon. Další možný způsob zneužívání telefonů rozebírám na konkrétním případu v další kapitole.

2.1.7 Počítačová kriminalita a zneužití know how

V dobách hospodářského útlumu a propouštění zaměstnanců značně stoupá počet krádeží cenných firemních dat a informací, které můžeme nazývat pojmem know-how. V obecném pojetí představuje know-how výrobně technické poznatky, které nejsou obvykle výsledkem vědecké nebo tvůrčí činnosti. Jedná se zejména o dlouhodobé zkušenosti s optimálním průběhem určité technologie a procesu. Zahrnuje nesporně celou řadu zkušeností nabytých především z široké oblasti techniky, ale i obchodu a podnikání. Často bývají tímto výrazem označovány výrobní zkušenosti, technická pomoc nebo technická informace.

Bez vědomí majitelů či vedení firem se kopírují přísně tajné informace, například databáze zákazníků, strategické plány, technologické koncepty, průzkumy či výzkumy. Krádeží cenných dat se snaží zaměstnanci zvýšit svoji hodnotu na trhu práce. I jinak loajální zaměstnanci mají tendenci si z firmy odnést informace, které by mohly být zajímavé pro potencionální zaměstnavatele anebo pro ně samotné, pokud chtějí například podnikat sami na sebe. Nejvíce to jistě hrozí u zaměstnanců, kteří z firmy odcházejí, nebo jim aspoň hrozí možnost výpovědi. Riziko navíc představují i zaměstnanci, jimž reálně propuštění nehrozí. Ti si vytvářejí často pouze pojistku pro případ, že by si museli hledat nové místo. Možností je také, že se důvěrné informace pokusí zaměstnanec prodat konkurenci.

Další, i když ne tak závažný způsob, jak okrást podnik, může být zneužívání internetu v pracovní době. Zaměstnanci si místo práce vyřizují osobní záležitosti, navštěvují sociální sítě apod. Nevěnují se svojí práci, za kterou jsou placeni, a tím pádem

se dá říci, že svou firmu okrádají. Zájmem každého zaměstnavatele je, aby zaměstnanec využil pracovní dobu co nejefektivněji a nezneužíval pracovní prostředky poskytnuté mu za účelem plnění pracovních povinností zaměstnavatelem.

2.1.8 Krádeže krmiva pro psy

Služební psi bývají většinou velká plemena, která spotřebují ročně desítky kilogramů krmiva. To může být uskladněno v místech, kde mají všichni zaměstnanci přístup a tak nemusí být problém po částech si ho domů odnášet a z podnikových zdrojů živit vlastního psa. Obvykle ale toto činí přímo zaměstnanec, který je krmením psů pověřen.

2.1.9 Krádeže čisticích prostředků

V podnicích PKB se zejména pro provádění průmyslových úklidů nakupují speciální čisticí prostředky. Nákupy můžou probíhat třeba jednou ročně a to ve velkém množství, kdy jde cena i do milionů. Při takových objemech se na spotřebu příliš nehledí a tak nemusí být problém, občas si pár takovýchto drahých prostředků přivlastnit.

Obr. 2 *Čisticí prostředky pro průmyslové úklidy [29]*

2.2 Metody páchání latentní kriminality

U zaměstnanců PKB se vzhledem k jejich povolání nepředpokládá, že by měli ve velkém rozkrádat majetek podniku a právě to je jejich výhoda. Mnohdy může být

zaměstnanec zlákán minimálními bezpečnostními opatřeními. Když ví, že se na něj prakticky nemůže přijít, zabrání mu v krádeži snad jen jeho svědomí.

Způsoby páchání a utajování hospodářské kriminality lze podle různých kritérií klasifikovat. Pro detektivní odhalování latentní hospodářské (ekonomické) kriminality má význam zejména třídění [5] :

a) Podle předmětu zájmu pachatele:

- Rozkrádání naturální (např. rozkrádání materiálu)
- Rozkrádání finančních prostředků
- Rozkrádání nehmotného majetku (informací, know how)

b) Podle toho, zda majetek, dotčený kriminalitou, byl řádně evidován či nikoliv:

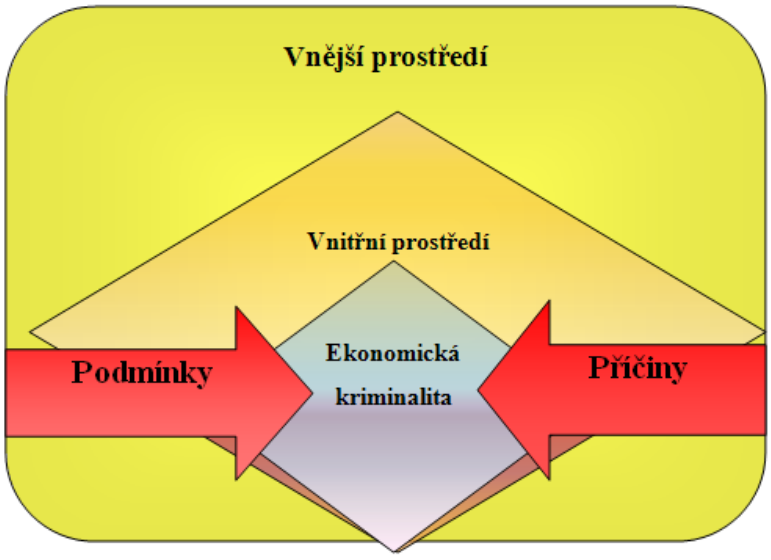
1. Rozkrádání majetku zapsaného do evidence v příslušných dokladech, které lze dělit na:
   - rozkrádání které se projeví v bilanci podniku v podobě schodku
   - rozkrádání, které se neobjeví v bilanci podniku

2. Rozkrádání majetku nezapsaného do evidence v příslušných dokladech podniku:
   - Předpoklady pro únik hodnot z evidence jsou zpravidla předem vytvářeny a připravovány a to rozmanitými způsoby, formami či metodami a činnostmi.

Samostatnou oblast tvoří rozkrádání finančních prostředků. Zejména odhalování latentních forem tohoto rozkrádání je značně obtížné a vyžaduje vysokou speciální odbornou způsobilost soukromých detektivů působících při ochraně ekonomických zájmů. Je třeba, aby takovýto soukromý detektiv měl vedle obecné odborné způsobilosti také způsobilost ekonomickou (účetní). Tato kriminalita může být zakrývána i administrativními účetními machinacemi, což velmi ztěžuje její odhalení.

3 PŘÍČINY A PODMÍNKY PÁCHÁNÍ KRIMINALITY

Významným momentem z hlediska příčin a podmínek zejména ekonomické kriminality je správná volba forem, metod a prostředků jejího rozkrývání a postihu. Velmi záleží v této souvislosti na osobní a místní znalosti soukromého detektiva. Osobní a místní znalost z hlediska soukromé detektivní činnosti má velký význam i v širším pohledu a to z hlediska včasné a účinné prevence. Nedostatky v této oblasti nahrávají vzniku zločinnosti vůbec a ekonomické kriminality zvláště. Prohlubují i latenci této kriminality. Některé příčiny a podmínky ekonomické kriminality se znásobují v důsledku rozvoje a rozšiřování mezinárodních ekonomických vztahů. V této souvislosti je třeba počítat i se skutečností, že s rozvojem mezinárodních ekonomických vztahů jde ruku v ruce i vytváření organizací mezinárodního ekonomického zločinu. S tím jsou pak pochopitelně spojené i značně ztížené podmínky a komplikace rozkrývání latentní ekonomické kriminality. Samozřejmě že cesta není v omezování mezinárodních ekonomických styků, ale v mezinárodní spolupráci soukromých detektivních služeb. [5]



Obr. 3 *Příčiny a podmínky*

3.1 Zločinnost a technika

Je třeba se zmínit i o podmínkách a příčinách patřících do technické oblasti. Zde je možné uplatnit dva pohledy. Na jedné straně rozvoj techniky rozšiřuje zájem pachatelů o

její získání a využívání a na straně druhé zdokonalování technických prostředků ovlivňuje ekonomickou zločinnost přímo a to jak v oblasti:

- Samotného páchání ekonomické zločinnosti, kdy vznikají nové formy zločinnosti např. při pronikání do počítačových sítí a databází, využívání zpravodajské techniky pachateli ekonomické zločinnosti či prostředky sloužící k snadnějšímu pronikání a překonávání překážek, nové možnosti účetních machinací, nové možnosti falšování účetních dokladů a zejména účetních databází apod.
- Prevence (ztěžování a znemožňování páchání ekonomické zločinnosti), stejně jako je využití technických prostředků v procesu rozkrývání latentní ekonomické zločinnosti (např. vysoce účinné zabezpečovací systémy)

Při výběru a stanovení forem, metod a prostředků v rámci konkrétních případů rozkrývání latentní ekonomické zločinnosti musí soukromý detektiv vycházet ze zásady, že tyto formy a metody soukromé detektivní činnosti musí v daném konkrétním případě svým obsahem reagovat na příčiny a podmínky páchání ekonomické zločinnosti. Současně musí alespoň z části mít schopnost tyto příčiny a podmínky ekonomické kriminality omezovat a odstraňovat. Jde tedy o schopnost využít těchto kriminogenních faktorů pro vlastní proces soukromé detektivní praxe při rozkrývání latentní ekonomické zločinnosti. [5]

3.2 Příčiny vzniku trestné činnosti tzv. bílých límečků

Za typické způsoby páchání trestné činnosti bílých límečků lze v našem případě považovat např. podvody různého druhu, zpronevěry, zneužívání důvěrných informací k vlastnímu obohacení nebo nedodržování předpisů o vedení účetnictví.

Příležitostí k páchání trestné činnosti (bílých límečků) je hlavně v dnešní době dostatek. Příležitost je také základní podmínkou k páchání této trestné činnosti. Obvykle nejde o „kriminalitu z materiální nouze“, poctivost a loajalita je ohrožena takovými příležitostmi, které slibují, že uspokojí následující trojlístek motivů: [6]

- Vylepšení společenské prestiže a postup na společenském žebříčku
- Výrazné vylepšení materiální situace
- Trvalé zajištění „dobré existence“

Typickou vlastností pachatelů je pocit, že jejich práce není dostatečně oceňována, pocit převahy (nad zaměstnavatelem, policií), pocit beztrestnosti a neodhalitelnosti. Pokud by pachatelé věnovali stejnou energii a vynalézavost legálnímu podnikání, byli by jistě mimořádně úspěšní.

Charakteristické znaky pachatelů této trestné činnosti již vyplývají z definic uvedených v první kapitole. Jedná se o osoby zpravidla vážené, výše společensky postavené, využívající své důvěry vyplývající z jejich vysokého společenského statutu a prestiže, náležející k této společenské vrstvě. V našem případě se jedná vždy o osoby bez kriminální minulosti, pokud se ovšem do bezpečnostní agentury nedostaly díky zahlazeným trestům ve výpisu rejstříku trestů.

K typickým osobnostním charakteristikám pachatelů často patří např. odvaha hraničící až s hazardem, cílevědomost, vytrvalost, vypočítavost, touha po majetku, společenském uznání a po moci, citová chladnost, bezohlednost, bezcitnost, sklony k velikášství, egoismu atd. Pachatelem hospodářské trestné činnosti (potažmo trestné činnosti bílých límečků) je dnes nejčastěji rafinovaný, vzdělaný, dobře situovaný člověk s kombinačními schopnostmi, nicméně jeho představivost funguje někdy jednosměrně. Z tohoto důvodu takoví pachatelé nejsou často schopni ani ochotni pochopit nemorálnost a trestnost svého činu a jeho odhalení považují za smůlu v obchodech nebo za spiknutí okolí. V případě odhalení je jejich obranou tvrzení o nespravedlivém stíhání, vyhrožují svými kontakty a v případě potřeby své hrozby plní. [12]

3.3 Sociálně psychologické aspekty

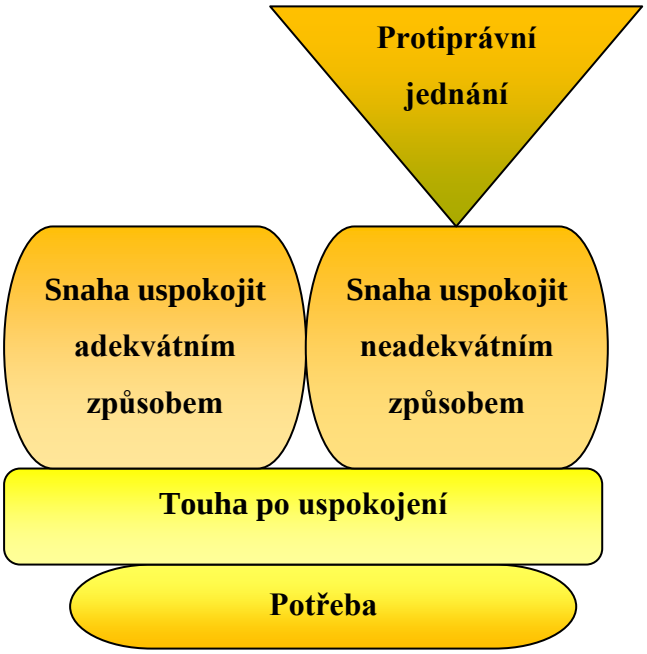
V sociálně psychologické oblasti se jedná, v souvislosti s páchaním hospodářské kriminality, o uplatňování touhy lidí (pachatelů) po uspokojení vyšších potřeb (např. touha po pochopení, seberealizaci, vyniknutí jistoty, společenském styku a jiné další rozsáhlé individuální duchovní hodnoty). Tyto jsou pak závislé na dalších psychologických faktorech (úrovni vnímání, pozornosti, představ, fantazie, myšlení apod.). Nedostatečné uspokojování individuálních potřeb může vyvolat různé typy nepřiměřeného chování. [5]

První projevy mohou být relativně nevinné, ale neuspokojování individuálních potřeb vede velmi často k vzniku rozhodnutí uspokojit tyto potřeby neadekvátním

způsobem a začít páchat trestnou činnost či jiné formy protiprávního jednání. Proto i když se zdá, že to spolu zdánlivě nesouvisí, jsou soukromé detektivní prověrky osob (periodické zaměstnanců) pro potřeby personální práce prvým krokem v procesu odhalování latentní kriminality v podniku. [12]

Neuspokojená potřeba zaměstnance podniku je velmi silným a významným motivačním faktorem v rozhodnutí začít páchat zločinnost. Neuspokojená individuální potřeba může být proto velmi často deformujícím faktorem. Proto zjištění takovýchto okolností může být velmi významným momentem pro zaměření pozornosti tímto směrem ze strany soukromé detektivní kanceláře či detektiva.

Jde o významný poznatek pro typování potencionálních pachatelů v zájmovém prostředí, k nimž jsou pak zaměřovány nebo z jejich okolí jsou typovány a získávány informační zdroje. Pokračující navršování neuspokojených individuálních potřeb mohou být motivačními řetězci k páchání podvodů, zpronevěry, prostého rozkrádání apod. K působení faktoru touhy se často připojuje i působení psychických nedostatečností a poruch. Velmi pestrá škála příčin a podmínek zločinnosti pak pramení ze sociální oblasti, tj. ze vztahů mezi lidmi či zaměstnanci navzájem. [5]



Obr. 4 *Uspokojení potřeb*

3.4 Kriminologické aspekty

Kriminologie charakterizuje zločin jako vědomé chování nebo jednání, které ohrožuje, v našem případě, ekonomické zájmy. Zločin – zločinnost jsou výsledkem vztahu mezi lidmi, mezi pachatelem a vlastníkem apod. Objektem zločinu může být jak člověk, tak majetek, jak hmotný, tak nehmotný majetek, práva a oprávněné zájmy apod. V detektivní práci je velmi důležité si ujasnit podstatu případu, který má detektivní kancelář (soukromý detektiv) řešit. Tomu je pak také třeba přizpůsobit další postupy, volit formy, metody, prostředky a síly detektivní činnosti. [5]

Kriminologie nám může dát odpověď na otázku: Kdo je pachatelem latentní kriminality? Vychází se ze základního kriminogenního poznání, že zločincem se člověk nerodí, ale stává se jím pod vlivem různých zejména společensko-ekonomických, ale i psychologických a sociálních faktorů. Z hlediska soukromě detektivní ochrany ekonomických a dalších bezpečnostních zájmů je významnou skutečností to, že ekonomický čin nese pečeť a stopy osobnosti pachatele. Proto také při rozkrývání ekonomické či hospodářské zločinnosti je třeba se zabývat takovými problémovými okruhy jako je [5]:

a) Zkoumání genetického programu osobnosti (zajímá nás rodinné prostředí apod.);
b) Zkoumání sociálního programu osobnosti (jaké má osoba představy o svých pozicích a své roli);
c) Sociální zkušenosti osobnosti (jde o to v jakém prostředí osoba procházela v různých životních etapách, jde o sociální zkušenosti osoby);
d) Působení okolního prostředí v současnosti;

Kriminologie zkoumá také kriminogenní osobnosti z hlediska způsobu jejich činnosti a zaměření. Jde o typy [12] :

a) **Příležitostné**, které využívají zejména příležitosti ke spáchání protiprávního jednání
b) **Cílevědomé**, které svou zločinnost zpravidla předem připravují
c) **Plánovité**, které postupují podle předem připraveného plánu a získaných informací

d) **Strategické**, které se zpravidla již vlastní protiprávní a trestné činnosti samy osobně neúčastní, ale spíše zločin připravují, organizují a nechávají jeho vykonání jiným osobám zločineckého gangu

e) **Recidivisté**, pro něž se zločin stává životním stylem. I když u ekonomické zločinnosti je míra recidivy menší než u obecné zločinnosti, přesto ji nelze vyloučit.

Další oblastí kriminologie je odpověď na otázku, zda je možné zločinu předcházet nebo mu dokonce zabránit? A pokud ano jakým způsobem? Způsobů zabraňování v páchání hospodářské kriminality může být celá řada. Nejdůležitější je však prevence, kdežto represe by měla být podpůrná. Represe nastupuje teprve tam, kde neuspěla prevence, a došlo ke spáchání trestné hospodářské kriminality. Ze strany soukromých detektivních služeb však o represi nelze vůbec hovořit, neboť tyto nejsou součástí státního donucovacího (represivního) aparátu. Proto i z tohoto pohledu je nutno rozkrývání latentní kriminality považovat za jistý stupeň prevence boje s ekonomickou zločinností. Včasné odhalení latentní kriminality a předání případu k dalšímu postupu orgánů činných v trestním řízení, má velký preventivní význam. Jednak zabraňuje v pokračování takovéto kriminality a dále působí preventivně vůči případným potencionálním pachatelům. [5]

Jak už jsem psal výše, v podmínkách tržní ekonomiky si musí vyhledávání latentní ekonomické kriminality zajistit samotný podnik. Policie řeší jen případy registrované kriminality a provádí odhalování a rozpracování těch případů ekonomické kriminality, které bezprostředně poškozují zájmy státu. Rozkrývání ekonomické kriminality v podniku spadá do ochrany ekonomických zájmů, ale samozřejmě zapadá i do komplexní ochrany představované konkurenčním zpravodajstvím. Vzhledem k její složitosti a náročnosti, nelze při její realizaci spoléhat jen na získané zkušenosti, dovednosti a návyky. Musí se vycházet z analýzy situací a jevů, které ekonomickou kriminalitu vyvolávají, způsobují a usnadňují, tedy z kořenů hospodářské kriminality. Musí se opírat o obecné poznatky kriminologické vědy, i o kriminologickou analýzu v daném podniku. V návaznosti na to je vhodné provést analýzu a zkoumat situace, jevy a procesy, které vznik ekonomické kriminality omezují, znesnadňují nebo dokonce znemožňují a o ty se v soukromé detektivní činnosti opírat. Soukromí detektivové zpravidla zabezpečují nebo realizují informační proces týkající se zejména jevů, majících

znaky zločinnosti-ekonomické kriminality. Proto také úspěšnost jejich práce ve značné míře závisí na tom, jak budou využívat bohatých zkušeností, jež poskytuje kriminologie, jako nauka o podstatě zločinu, jeho stavu, dynamice, struktuře, příčinách a podmínkách vzniku a existence, kriminogenních osobnostech a způsobech ekonomické kriminality. [12]

4 PERSONÁLNÍ POLITIKA PODNIKU PKB

4.1 Osoba personalisty

Vzhledem k náročné pozici, kterou personalisté ve firmách zaujímají, a k množství rolí, které plní, je důležité naučit se používat vybrané techniky, které umožní jednak dostát všem pracovním úkolům, jednak ochránit vlastní psychickou stabilitu. Personalista by měl být aktivním hybatelem chodu podniku, měl by dobře zvládat zátěžové situace, nejasnost pozic a rolí, konfliktní či problémové situace, kterým může ve své každodenní praxi čelit.

Kromě znalosti svých konkrétních pracovních povinností a úkolů a kontinuálního vzdělávání v příslušných oblastech řízení lidských zdrojů by se zřejmě měl orientovat v psychologických aspektech pracovní komunikace, ve variantách, jež zde - a to zvláště v zátěžových situacích - nastávají, měl by znát příčiny jejich projevů a možnosti zacházení s nimi. Dále je vhodné, aby si byl vědom svých vlastních mechanismů jednání, vyplývajících ze struktury jeho vlastní osobnosti, popřípadě aby pracoval na jejich poznání a vědomém zacházení s nimi, což mu zajistí i v zátěžových, nejasných či konfliktních situacích možnost volby a změny, na rozdíl od lidí, kteří jednají výhradně instinktivně, opakují své - byť často nepříliš fungující - stereotypní vzorce a v jejich důsledku se dostávají do složitých či někdy zdánlivě bezvýchodných situací. [25]

Osoba personalisty je součástí celkového procesu řízení firmy, jsou partnery v podnikání. Personální obsazenost personálního útvaru a jeho organizace záleží na každé individuální firmě, neexistuje totiž žádná norma, podle které bychom mohli zjistit ideální počet personalistů na počet zaměstnanců. Přihlíží se tedy k firemní velikosti, typu prováděných prací, typu zaměstnanců a samozřejmě i k důležitosti, která je připisována personálním pracovníkům.

Co se týká role vedoucího pracovníka personálního útvaru, je nutné říci, že je členem nejvyššího firemního vedení. Proto je důležité, aby měl jednak teoretické znalosti z oboru, tak i praktické zkušenosti, aby důkladně znal problematiku dané firmy a podporoval dosažení jejích cílů, aby uměl čelit stresovým situacím, určoval si priority a případně vytvářel podnikové strategie. [25]

Znalost podniku a kultury	Rozumí: 1. podnikovému prostředí, konkurenčním tlakům, jimž podnik čelí, a hybným silám vysokého výkonu, 2. klíčovým činnostem a procesům v podniku a jak tyto činnosti a procesy ovlivňují podnikové strategie, 3. podnikové kultuře (základní hodnoty a normy), 4. jak personální politika a praxe ovlivňuje výkon podniku, a snaží se o jejich správné uplatňování.
Strategické schopnosti	1. Usiluje o účast při formulování podnikové strategie a přispívá k vytváření této strategie, 2. přispívá k vytváření jasné vize a souboru jí odpovídajících hodnot pro podnik, 3. vytváří a realizuje promyšlené, logické a vzájemně propojené personální strategie odpovídající podnikové strategii, 4. chápe význam měření lidského kapitálu, zavádí systémy měření a zabezpečuje, aby byly správně používány.
Efektivnost organizace	1. Přispívá k analýzám a diagnózám problémů souvisejících s lidmi a navrhuje praktická řešení, 2. pomáhá formovat zdroje pro podnik tím, že zabezpečuje, aby měl potřebnou kvalifikovanou, oddanou a angažovanou pracovní sílu, 3. pomáhá formovat schopnosti podniku v oblasti procesů tím, že zavádí takové systémy práce, které vedou k optimálnímu využívání lidí, 4. přispívá k vytváření a rozvoji procesů řízení znalostí.
Interní konzultování	1. Analyzuje a diagnostikuje problémy související s lidmi a navrhuje praktická řešení, 2. používá intervenční styl k uspokojení potřeb klientů; podle potřeby hraje roli katalyzátoru, usnadňovatele nebo experta, 3. používá procesů konzultování k řešení problémů a záležitostí souvisejících s lidmi, 4. koučuje klienty, aby se vyrovnali se svými problémy, předává dovednosti.
Poskytování služeb	1. Předvídá požadavky a uzpůsobuje a provádí podle nich své služby, 2. poskytuje účinné a nákladově efektivní služby v každé oblasti řízení lidských zdrojů, 3. rychle a účinně reaguje na žádost o personální služby, pomoc a radu, 4. posiluje pravomoci liniových manažerů, aby mohli rozhodovat v personálních záležitostech, ale podle potřeby je vede.
Soustavný odborný rozvoj	1. Soustavně zdokonaluje a rozšiřuje své odborné znalosti a dovednosti, 2. hledá vzory nejlepší praxe v personální práci, 3. udržuje si přehled o novinkách v řízení lidských zdrojů, 4. udržuje krok s výzkumem v oblasti řízení lidských zdrojů a jeho praktickými důsledky.

Tab. 1 *Přehled ideálních vlastností personalisty [1]*

4.1.1 Styly komunikace

Pro zvládnutí náročných situací, vyplývajících z některých rolí, je vedle výše zmiňovaných poznatků důležité, aby se personalista učil zvládat, podobně jako jiní manažeři, různé styly komunikace či jejich strategie. K těmto stylům může patřit podobně jako ke stylům výchovy model [1] :

a) **autoritativní či direktivní**, přenášející požadavky „shora" a vyžadující jejich plnění,
b) **demokratický**, založený na respektování požadavků většiny,
c) **liberální**, jenž může být velmi tvořivý a ponechává velký prostor jednotlivci, avšak pokud současně není doprovázen zásadami „komunitní" týmové práce, může vést k chaosu či rozkladu.

4.1.2 Modely řízení lidí

Ve vztahu k řešení konkrétních situací a požadavků s nimi spojených, jakož i s ohledem na konkrétní jednotlivce, s nimiž se dostává personalista do styku, lze pak modely řízení lidí a přístup k nim rozdělit na [1]:

· **model mužský**, který je spíše dominantní, sebeprosazující, aktivní, opírající se o využívání analýz, statistik, racionálních argumentů, využívající metod přesvědčování (potažmo tlaku či nátlaku), apelující při interakci na rozum a „rozumnost" řešení situací,

· **model ženský**, přizpůsobivější a méně direktivní, opírající se více o naslouchání, naladění se na potřeby partnerů, o „pravohemisferické či celostní" hodnocení situace v její verbální i mimoverbální podobě, apelující více na sociální a emocionální potřeby účastníků či hodnoty jako je sounáležitost, kvalita společného prožívání apod.

4.2 Metody práce

Personální práce v soukromých bezpečnostních agenturách zahrnuje podle JUDr. Brabce [2] :

4.2.1 Personální plánování

Je to okruh činností vedoucího pracovníka či specializovaného personální pracovníka směřujících k výpočtu fondu potřebné práce podle rozsahu zakázek soukromých bezpečnostních služeb a výpočet potřebného počtu pracovníků podle profesní specializace.

4.2.2 Získávání a výběr pracovníků

U soukromé bezpečnostní agentury nesmí probíhat náborem, ale výběrem. Výběr pracovníků musí být prováděn v souladu s požadavky zákona kladenými na pracovníky soukromých bezpečnostních služeb, které je možno rozdělit do několika skupin:

- odpovídající věk
- spolehlivost a bezúhonnost
- vhodnost pracovníka s ohledem na jeho psychické vlastnosti a schopnosti
- vhodnost pracovníka s ohledem na jeho zdravotní stav
- vědomosti a dovednosti, jimiž je naplněna odborná způsobilost

V procesu výběru pracovníků má konečné a rozhodující slovo výkonný ředitel, ale musí mít možnost se vyjádřit i vedoucí pracovníci nižších stupňů řízení, kterým bude pracovník podřízen. Proces výběru by měl zahrnovat:

- vyhodnocení dotazníku a životopisu
- základní orientační test charakterizující osobnost uchazeče
- vyhodnocení dokumentace
- potvrzení o zdravotní způsobilosti
- o dosaženém vzdělání a jiných dovednostech, vědomostech a zkušenostech
- závěrů psychologických vyšetření
- výpisu z rejstříku trestu
- hodnocení z předchozích zaměstnání apod.
- vyhodnocení testů fyzické zdatnosti
- dotaz na stanovisko policie, popřípadě na obecním úřadě na zprávu o pověsti

Toto je ovšem ideální stav, který jak se dočtete v praktické části, u většiny agentur bohužel neexistuje.

4.2.3 Školení a výcvik pracovníků

Školení pracovníka musí proběhnout ještě před jeho zařazením do výkonu služby a to ve všech oblastech, které se dotýkají jeho práce. Například základní právní znalosti pracovníka SBS, etika práce, základy bezpečnosti a ochrany zdraví při práci atd.
Vyhláška 16/2009 Sb. O obsahu a rozsahu kvalifikace pro výkon fyzické ostrahy a služby soukromého detektiva také mimo jiné upravuje i podmínky pro získání odborné způsobilosti zaměstnance podnikatele provozujícího koncesovanou živnost ostraha majetku a osob nebo koncesovanou živnost služby soukromých detektivů. Dále upravuje způsob provádění zkoušky a její obsahovou náplň.

4.2.4 Hodnocení pracovníků

Pravidelné a průběžné hodnocení je významným momentem motivace pracovníka SBS. Hodnocení musí být konkrétní, objektivní a musí v závěru stanovit úkoly k odstranění zjištěných nedostatků. Závěry musí být konkrétní, časově ohraničené a požadavky nesmí být přemrštěné a nerealizovatelné. Hodnocení může být také psychologické, ale vždy záleží na správném zadání pro psychologa. Psychologické hodnocení by mělo obsahovat psychologickou charakteristiku, stanovisko k psychologické způsobilosti pro službu v SBS a pro funkci, kterou by mohl zastávat a doporučení pro individuální práci s pracovníkem

4.2.5 Vedení personální dokumentace

U každé soukromé bezpečnostní agentury musí být vedena a po dobu nejméně pěti let po skončení pracovního poměru archivována personální dokumentace na pracovníka. To může být z hlediska latentní trestné činnosti později důležité, neboť se na ni často přijde až po velmi dlouhé době, kdy už zaměstnanec nemusí ve firmě pracovat.

4.2.6 Formování příznivých pracovních vztahů

Formování příznivých pracovních vztahů patří k nedílné činnosti každého vedoucího pracovníka a personalisty. Je třeba pod ním chápat i formování a přizpůsobování vnitřního a vnějšího pracovního prostředí. Pracovníci, kteří jsou ve svém zaměstnání spokojeni, mají mnohem menší sklony k páchání trestné činnosti.

4.2.7 Rozmisťování a ukončení pracovního poměru

Rozmisťování pracovníků nesmí být nahodilé, ale musí jít o propracovaný systém vycházející ze znalosti a hodnocení pracovních míst a ze znalosti a hodnocení pracovníků

4.2.8 Průzkum trhu práce

Průzkum trhu práce dává přehled o nabídce a poptávce pracovních sil (možnostech výběru pracovníků) pro soukromou bezpečnostní agenturu. Soukromé bezpečnostní služby mají specifický charakter a ne každý člověk vyhovuje pro práci v soukromé bezpečností agentuře. O to významnější je průzkum trhu práce a úzká spolupráce s úřady práce.

4.2.9 Personální informační systém

Mezi soukromými bezpečnostními agenturami by měl být vybudován informační personální systém, který by znesnadnil nekvalitním a problémovým pracovníkům fluktovat mezi jednotlivými agenturami. Zabrání to různým excesům ve výkonu soukromých bezpečnostních služeb.

4.3 Psychotesty

Pro přijetí zejména na specializované pozice může být výhodné použití psychotestů. Dříve se této metody poměrně hojně využívalo, bohužel dnes už se od ní z časových i finančních důvodů upouští. Účelem psychotestů je odhadnout, který z uchazečů bude pravděpodobně v daném zaměstnání úspěšný. Nejprve je třeba o

kandidátovi nashromáždit co nejvíc relevantních údajů, poté tyto informace odpovědně zvážit a nakonec dospět k rozhodnutí, zda mu dané místo nabídnout, nebo nenabídnout. Zpravidla je absolvují až ti uchazeči, kteří postoupí do vyšších kol výběrového řízení, tedy nejdříve po prvotním výběru uchazečů na základě zaslaných životopisů. Testy si mnohdy vytvářejí agentury samy. Setkat se lze i s testy, které může zadávat a vyhodnocovat pouze vystudovaný psycholog. Jedině on je oprávněn provádět psychologická a psychodiagnostická vyšetření v pravém slova smyslu. Takové testy jsou součástí např. výběrových řízení na vysoce specializované pozice.

4.4 Požadavky na zaměstnance bezpečnostních agentur

Živnostenský zákon stanoví v příloze č.3 podmínku bezúhonnosti všech zaměstnanců. Bezúhonnost dokládá uchazeč o zaměstnání výpisem z rejstříků trestů – ve většině případů je vyžadováno, aby tento výpis nebyl starší než 3 měsíce.
Mezi další požadavky na uchazeče o zaměstnání v soukromých bezpečnostních službách patří zejména:

1) dosažení minimálně 18 let věku
2) odpovídají zdravotní stav – doložený potvrzením lékaře
3) minimální požadované vzdělání – zpravidla minimálně vyučen

Pro jednotlivé kategorie práce, na které jsou uchazeči přijímáni, mohou být stanovena rovněž další kritéria, jako např. odborná kvalifikace – např. doložení znalosti cizího jazyka, zbrojní průkaz, prověrka Národního bezpečnostního úřadu, psychodiagnostické vyšetření apod. U cizinců, jejichž zaměstnání v soukromých bezpečnostních službách není ničím neobvyklým, je vyžadován trvalý pobyt v ČR, výpis z rejstříků trestů ze země původu a znalost českého jazyka.

Dále je nutné, aby zaměstnanci byli odborně způsobilí. Způsobilost pro zaměstnance bezpečnostních agentur (příloha č. 5 živnostenského zákona) – zaměstnanci musí absolvovat kurz (osvědčení) osobou akreditovanou Ministerstvem školství, mládeže a tělovýchovy, dále osobou autorizovanou Ministerstvem vnitra (vyhláška č. 16/2009 Sb.). Platnost tohoto kurzu (osvědčení), se prodlužila z 5 na 10 let. Datum povinnosti dokládat živnostenskému úřadu zmíněný kurz (osvědčení), zůstal nezměněn – tedy nejpozději do

1.1.2012. Dále již nebude možno, doložit odbornou způsobilost vzděláním v oboru bezpečnostním, právním nebo obdobném.

4.5 Chyby v personální politice

Činnost soukromých bezpečnostních agentur, které nevěnují dostatečnou pozornost personální práci, včetně dlouhodobé stabilizace pracovníků, se dá hodnotit jako krátkozraká a nebezpečná. Firmy, které nevěnují pozornost personální práci a stabilizaci svých pracovníků, ohrožují dobré jméno soukromých bezpečnostních služeb jako celku, protože jak už jsem psal, trestná činnost pracovníků PKB vysoce ohrožuje pověst bezpečnostních agentur, kterým hrozí také pokles zakázek. [4]

Poměrně častým nešvarem v personální práci je skutečnost, že vedení agentury při sjednávání zakázky deklaruje vysoký stupeň a odborné způsobilosti pracovníků, ač skutečná situace je odlišná. Dalším nešvarem bývá, že vedení soukromé bezpečnostní služby při poskytování služeb pro zákazníka nasadí v prvé etapě skutečně kvalifikované a připravené pracovníky, ale postupně je nahrazuje méně kvalifikovanými nebo zcela nekvalifikovanými. Dobré jméno se ztrácí velice snadno, ale daleko obtížnější je si ho vybudovat. [4]

V personální politice musí platit zásada, že za personální činnost zodpovídá ve svém rozsahu každý, kdo řídí. Statutární personální pravomoc má však výkonný ředitel soukromé bezpečnostní agentury a v přiměřeném rozsahu jeho zástupce, popřípadě zástupci, pokud jsou v soukromé bezpečnostní agentuře zřízeni. U středně velkých agentur jde zpravidla o:

- zástupce pro výkon služby
- zástupce pro personální práci

Velmi častým prohřeškem, se kterým se personalisté setkávají, jsou úpravy životopisů. Potvrzují to i zkušenosti společností, které se zabývají hledáním a výběrem vedoucích pracovníků. Nejčastěji se objevují nepravdivé údaje o vzdělání, znalostech cizích jazyků, trestní minulosti, počítačové gramotnosti a důvodech odchodu z předchozích

zaměstnání. Chybou personalistů bývá, že si takové údaje mnohdy neověřují. Je možno využít i prověření zaměstnanců, o kterém se více rozepisuji v další kapitole.
Personalisté můžou vybírat zaměstnance na základě toho, kdo je nejlepším při osobním pohovoru nebo kdo se nejvíce blíží představám vybírajícího o novém spolupracovníkovi. Je ale nutné vybrat skutečně důvěryhodného člověka, který je schopen zvládnout stanovené cíle a ne toho, který má jen dobře naučené odpovědi na standardní otázky

Mezi další možné chyby, které se vyskytují v personální politice patří**:**

- Nekompetentní lidé ve vedoucích funkcích
- Nefunkční popřípadě komplikovaná firemní struktura
- Špatně fungující vnitřní komunikace, při níž vázne zpětná vazba
- Chybná strategie vypracovaná k dosažení stanoveného cíle
- Nízká produktivita práce
- Nedokonale propracovaný, případně žádný systém vzdělávání
- Špatný systém odměňování a dalších motivačních složek

4.6 Spolupráce se státní administrativou

Podle § 35 zákona o zaměstnanosti (č. 435/2004 Sb.) je každý zaměstnavatel povinen do 10 kalendářních dnů oznámit příslušnému úřadu práce (jakákoliv) volná pracovní místa a jejich charakteristiku. S tím souvisí i následná povinnost nejpozději do 10 kalendářních dnů oznámit obsazení těchto míst. Volnými pracovními místy se rozumí nově vytvořená nebo uvolněná místa, na která zaměstnavatel zamýšlí získat zaměstnance. Lhůta pro oznámení počíná běžet dnem následujícím po vytvoření, uvolnění nebo obsazení pracovního místa.

Zkušenosti z bezpečnostních agentur bohužel potvrzují, že Úřady práce neplní řádně svou funkci. Například zahlcují personální oddělení nevhodnými uchazeči a to takovými, kteří o práci vůbec nemají zájem a jde jim jen o razítko nebo dokonce dříve trestanými, kteří už vůbec nemají v bezpečnostní agentuře co dělat. V nejbližší době zřejmě k žádné změně nedojde a připravovaný zákon o bezpečnostních agenturách tuto situaci asi také nezlepší.

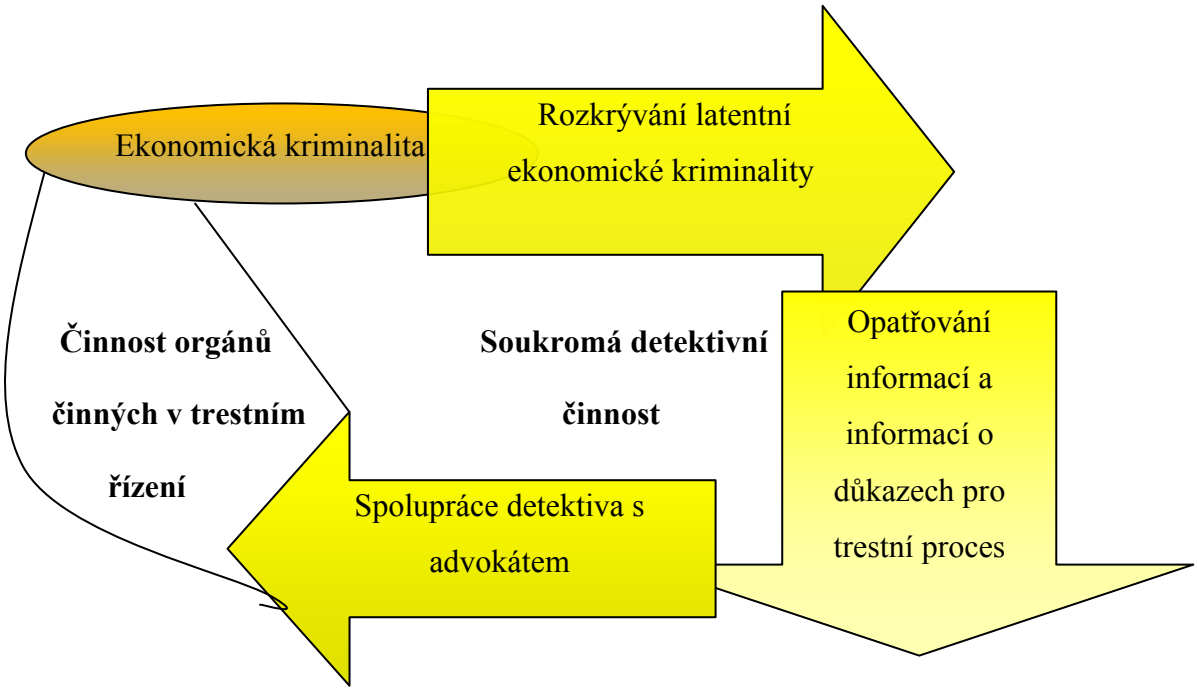
5 FORMY A METODY ODHALOVÁNÍ LATENTNÍ KRIMINALITY

5.1 Rozkrývání latentní kriminality

K charakterizování detektivních služeb uvnitř podniku uvádím definici uvedenou v publikaci Komerční bezpečnost, kterou je možné chápat i v případě prostředí Podniků komerční bezpečnosti:

Detektivní služby charakteru vnitřní ochrany jsou službami uvnitř podniku, organizace či instituce a jsou vykonávány vlastními zaměstnanci příslušného podniku a pro jejich vlastní potřeby. Jde o vnitřní bezpečnostní útvary využívající ve své činnosti forem, metod a prostředků soukromé detektivní činnosti. [11]

Činnost soukromého detektiva uskutečňovaná v procesu rozkrývání latentní kriminality není ve své podstatě ničím jiným než procesem poznání určitých jevů. Poznávat vlastnosti či podstatu těchto jevů znamená poznávat jejich vzájemné působení, formy jejich pohybu a změny. Výsledkem tohoto zkoumání v procesu rozkrývání latentní kriminality jsou informace o těchto jevech, které mají různou podstatu a hodnotu. Z hlediska zaměření na využívání informací získávaných v procesu rozkrývání latentní kriminality hovoříme o zabezpečení informací pro zabezpečení budoucího dokazování. Tyto informace můžeme pak nazývat informacemi z neprocesních zdrojů. [5]



Obr. 5 *Rozkrývání latentní ekonomické kriminality*

Informace získávané v procesu rozkrývání ekonomické zločinnosti soukromými detektivy jsou právě informace z neprocesních zdrojů. Soukromý detektiv nemůže provádět dokazování protiprávního jednání, neboť není součástí státního donucovacího aparátu-orgánů činných v trestním řízení, ale získává pouze informace potřebné pro příští dokazování. Informace z neprocesních zdrojů získané v rámci rozkrývání ekonomické zločinnosti mohou mít jednak charakter orientačních informací a jednak charakter informací sloužících v dalším procesu dokazování orgány činnými v trestním řízení. To ale neznamená, že by soukromý detektiv v procesu rozkrývání nemohl zajistit podklad, které právě v budoucím procesu dokazování orgány činnými v trestním řízení mohou posloužit jako důkazy. Takto může pořídit například fotodokumentaci, videozáznam nebo třeba záznam docházkového systému, o kterém jsem psal v případě zneužívání telefonů ve druhé kapitole. [5]

V rámci odhalování latentní hospodářské kriminality se jedná o různé útoky proti majetku podniků. Jako jedna z velmi nebezpečných forem se jeví krádeže jak hmotného (materiál, výstroj,výzbroj, čistící prostředky…) tak nehmotného majetku (know-how, databáze zákazníků apod.) Je třeba si uvědomit skutečnost, že v podmínkách tržní ekonomiky se policejní orgány či další orgány činné v trestním řízení nezabývají skrytou kriminalitou v podniku. Ze zákona mají povinnost zabývat se tzv. oznámenou kriminalitou a u latentní ekonomické kriminality jen těmi případy, které bezprostředně ohrožují zájem státu. Latentní kriminalitou se musí zabývat buď přímo sám vlastník, nebo vedoucí pracovníci (management) podniku. Jedná se zpravidla o zneužití pracovního zařazení či postavení zaměstnanců nebo dokonce skupin takovýchto pracovníků. Tito pachatelé jsou zpravidla označováni jako vnitřní pachatelé. Většinou bývají zařazeni na úseku hospodaření s hmotnými, finančními i nehmotnými prostředky, kteří tohoto svého postavení zneužijí k vlastnímu obohacení na úkor majetku podniku. Tito pachatelé se mohou zmocnit svěřeného hmotného či nehmotného majetku přímo, formou zpronevěry, nebo nepřímo pomocí různých machinací s účetními či jinými finančními doklady, kdy rozkrádání má formu podvodu. Obtížnost odhalování latentní kriminality spočívá především v tom, že se v této oblasti způsoby rozkrádání neustále mění. Pachatelé využívají k svému obohacování nedostatků, které existují v zabezpečení takovéhoto nehmotného či hmotného majetku anebo nedostatků v manipulaci s takovýmto majetkem (převozy cenin). Každá změna v podniku sebou ihned přináší nové možnosti rozkrádání. Způsoby rozkrádání se mění i tak, jak se pachatelé této zločinnosti seznamují s prací

bezpečnosti, kontrolních orgánů a v neposlední řadě i činností soukromých detektivů. Pachatelé neustále hledají a zdokonalují možnosti zakrývání této kriminality. [5], [18]

5.2 Formy a metody soukromé detektivní činnosti

Význam forem soukromé detektivní činnosti spočívá v tom, že pomáhají soukromému detektivovi již od počátku stanovit a vytyčit další zaměření vlastního postupu, správnou volbu metod a prostředků soukromé detektivní činnosti a ukazují mu tendence vývoje zkoumaného problému. [3]

V našem případě nás zajímají jen ty formy a metody detektivní činnosti, které lze dobře použít při rozkrývání kriminality v Podnicích průmyslu komerční bezpečnosti. Jedná se zejména o formy:

- Konkurenční zpravodajství
- Detektivní rozpracování a dokumentování
- Detektivní prověrka

Z metod je výhodné použití:

- Detektivní vytěžování osob
- Detektivní vytěžování evidencí, registrací, databází a archivů
- Detektivní monitorování (pozorování)
- Detektivní osobní pátrání
- Metoda fyziodetekce

5.2.1 Konkurenční zpravodajství

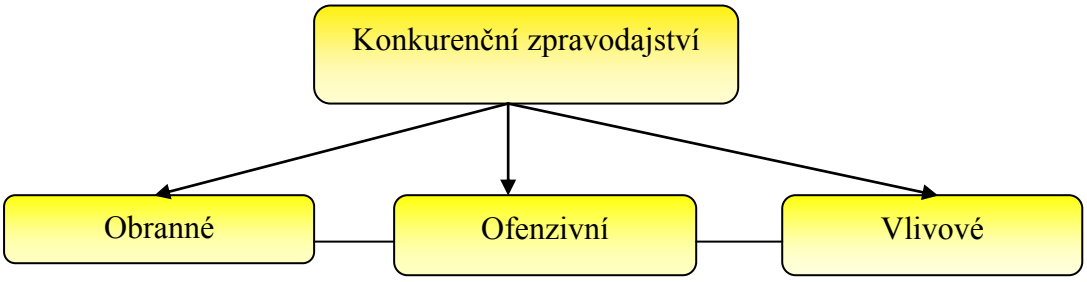
Konkurenční zpravodajství, někdy také uváděno jako nestátní zpravodajství, je forma práce průmyslu komerční bezpečnosti zaměřená do zpravodajské oblasti. V podmínkách České republiky se touto činností zabývají podniky průmyslu komerční bezpečnosti mající licenci na provozování detektivní činnosti. Můžeme tedy říci, že jde o určitou formu práce soukromého detektiva. Služby soukromých detektivů jsou služby

spojené s hledáním majetku a osob, zjišťováním skutečností, které mohou sloužit jako důkazní prostředky v řízení před soudem nebo správním orgánem, získáváním informací tykajících se osobního stavu občanů, fyzických nebo právnických osob, nebo jejich majetkových poměrů, získáváním informací v souvislosti s vymáháním pohledávek, vyhledáváním protiprávních jednání, ohrožujících obchodní tajemství. Konkurenční zpravodajství lze dělit v podstatě na tří základní okruhy [14]:

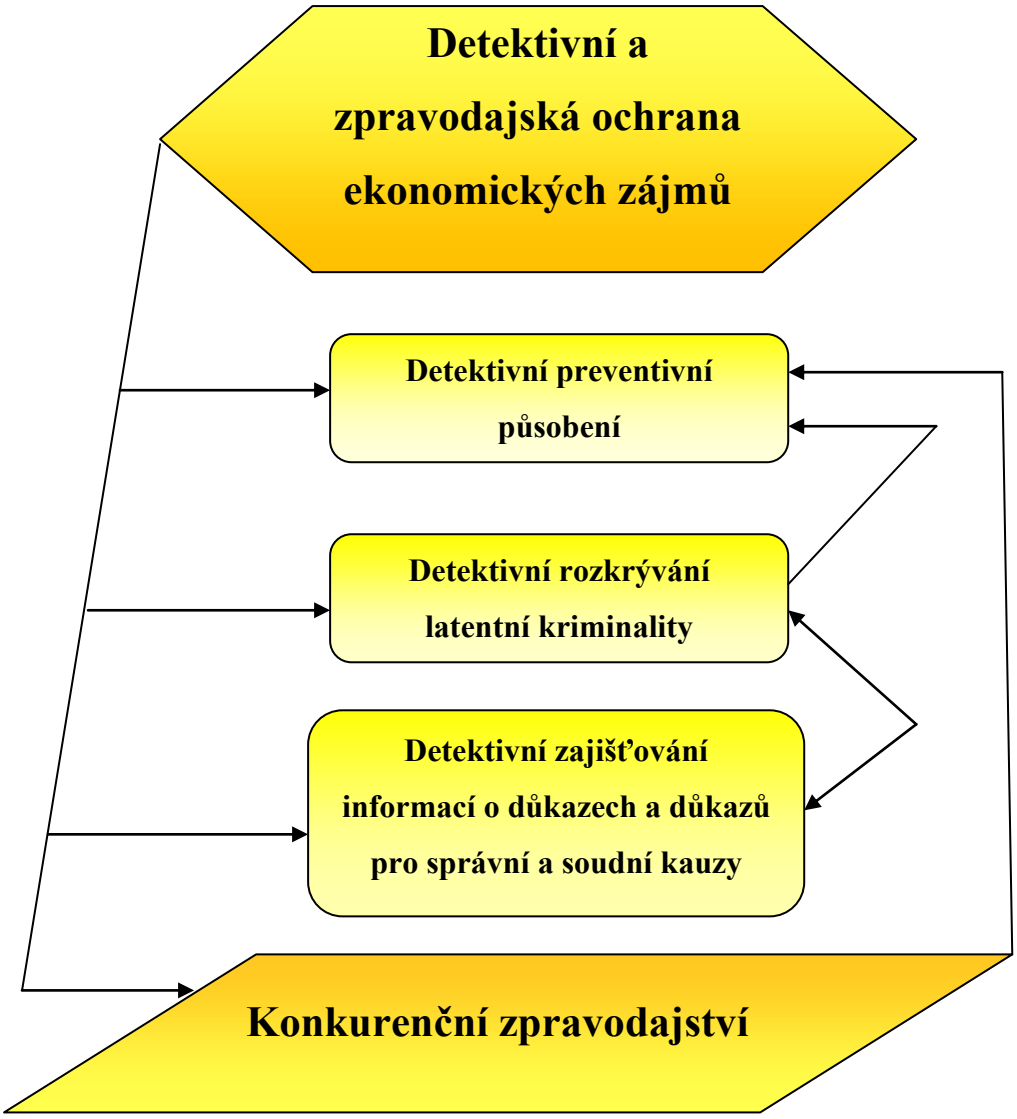
a) *Obranné zpravodajství* – jedná se především o ochranu informací, personální bezpečnost, ochrana komunikačních systému a dat, zajišťování ochrany technologických procesů, zajišťování bezpečnosti v obchodních vztazích, aktivní ochrana proti dezinformacím a působení vlivového zpravodajství konkurence, aktivní ochrana proti ofenzivnímu zpravodajství konkurence. Zjednodušeně se dá říci, že jsou to způsoby a metody, kterými podnik chrání sám sebe.

b) *Ofenzivní zpravodajství* – jedná se o zajišťování informací potřebných pro podnikání, zajišťování informací marketingového charakteru, zjišťování cílených informací o konkurenci, zjišťování informací o potřebných technologiích, zjišťování informací o know-how, výzkumu, vývoji, vynálezecké a zlepšovatelské činnosti v příslušných oborech průnikového zájmu.

c) *Vlivové zpravodajství* – někdy také označované jako lobing. Lobby je početná, většinou vlivná zájmová skupina, která prostřednictvím svých zaměstnanců, či k této činnosti specializovaných osob, vytváří stály nátlak na státní administrativu, poslance, senátory a ostatní politiky, za účelem ovlivňování jejich rozhodnutí či konání ve prospěch této skupiny.



Obr. 6 *Roviny konkurenčního zpravodajství*



Obr. 7 *Detektivní a zpravodajská ochrana ekonomických zájmů*

Zejména obranné neboli defenzivní zpravodajství může být nápomocné v případě ochrany podniku před rozkrádáním vlastními zaměstnanci. Využívá se pro ochranu vlastních dat, informací a poznatků tak, aby byla minimalizována možnost jejich zneužití. V souvislosti s konkurencí to může znamenat ochranu před počítačovou kriminalitou, kdy zaměstnanec, který chce zvýšit svou hodnotu na trhu práce, vynese informace, které může konkurenční podnik zužitkovat. Toto se děje hlavně pokud zaměstnanci reálně hrozí výpověď nebo se chystá podnik sám opustit.

Obranné zpravodajství musí plnit více úloh, které jsou ale navzájem propojené. Okruh úloh spojených s informační bezpečností [19] :

a) *Personální bezpečnost* – jde o ochranu informačních systémů z hlediska konkrétních událostí způsobených zaměstnanci a to především z pohledu prevence. Personální bezpečnost musí být zajišťována jednak detektivními prověrkami budoucích zaměstnanců podniku a jednak periodickými detektivními prověrkami stávajících zaměstnanců podniku.

b) *Režimová bezpečnost* – Jde o vytvoření bezpečnostních pravidel z hlediska zásad práce s informacemi, daty, komunikačními a počítačovými systémy. Je to velmi významný prvek prevence. Nestačí ale jen existence pravidel a samozřejmě je nutné kontrolovat jejich dodržování a v případě jejich porušení realizovat odpovídající opatření.

   Režimová bezpečnost zahrnuje:

   - Režim práce s písemnostmi
   - Režim ukládání datových médií
   - Vymezení okruhu osob pro práci s výběrovými, důvěrnými a utajovanými informacemi a daty
   - Opatření pro případ mimořádných událostí apod.

c) *Bezpečnost technických prostředků* – Jde o jejich výběr a spolehlivost, kontrolu přístupu k těmto prostředkům, ochranu před elektromagnetickým zařízením a elektrostatickou elektřinou apod.

d) *Bezpečnost programových prostředků* – Je potřebné zajistit kontrolu přístupu k nim, autentizaci a identifikaci uživatele, rozdělené pravomocí mezi uživatele, výběr a spolehlivost programů apod.

Bezpečnost programových prostředků spočívá:

- V ochraně proti virům
- V obraně před zneužitím programového vybavení

e) *Bezpečnost dat* – Jde o ochranu dat v souborech a databázích, ať už elektronických nebo písemných, o ochranu proti chybám a virům, o zvláštní ochranu citlivých dat, o autorizaci a rozlišení přístupu k datům a databázím

f) *Fyzická bezpečnost*- Jedná se o ochranu informací, dat, komunikačních a počítačových systémů proti neoprávněnému přístupu k nim, protiprávnímu přístupu do prostorů, kde se nacházejí

g) *Bezpečnost komunikačních systémů a cest* – představuje především ochranu vazeb mezi jednotlivými částmi komunikačních a počítačových systémů.

h) *Aktivní ochrana proti úniku informací a dat* – hlavně proti špionáži ze strany konkurence. Jde o systém opatření směřujících k získání informací o aktivech konkurenčních podniků. Patří sem tyto okruhy:

- V rovině personální bezpečnosti jde o to zabránit, aby zaměstnanci podniku byli kontaktováni a vytěžováni konkurencí, aby byli zaměstnáváni zaměstnanci konkurence ve vlastním podniku (fingované zaměstnání), aby informace byli konkurencí získávány formou korupce nebo vydírání.
- V rovině ochrany proti útokům na bezpečnost informací, dat, komunikačních a počítačových systémů zvenku. Jde o to zabránit přímé krádeži počítačových nosičů informací anebo jejich nelegálnímu kopírování a zabránit technickému získávání informací z počítačových sítí.
- V rovině přímého narušení vlastnických práv jde např. o ochranu proti vlámání za účelem krádeže dokumentů a jiných nosičů informací.

Pokud mají být všechny tyto úlohy splněné, musí být ochrana informací chápána v komplexně-systémovém pojetí. Specialisti na informační bezpečnost se proto musí umět orientovat v následujících činnostech:

- Činnost metodologická a koncepční
- Činnost bezpečnostně organizační, bezpečnostně režimová a bezpečnostně technologická,
- Činnost spočívající v prosazování a uplatňování informační bezpečnosti
- Činnost spojená s bezpečnostními informačními audity
- Činnost v oblasti personální
- Činnost v oblasti technických řešení

Při definování požadavků na ochranu informací je třeba vycházet ze skutečnosti, že existují dvě možnosti úniku informací:

- Nespolehlivost a selhání technických systémů
- Nespolehlivost a selhání lidského faktoru (zejména v našem případě)

V prvé řadě je ale potřeba odpovědět si na otázky typu:

- Které informace, data, počítačové a komunikační systémy je potřebné považovat za důvěrné nebo jinak utajované, jaké jsou hlavní elementy takto utajovaných informací a proč?
- Jak dlouho je potřebné data a informace uchovávat v tajnosti a proč?
- Které podnikové útvary a které osoby v nich budou s danými informacemi seznámené, v jaké rozsahu a proč je to nutné?
- Které podnikové útvary a které osoby v nich mají přístup do počítačového anebo komunikačního systému, v jakém rozsahu a proč?
- Které osoby spadají do okruhu manažerů-pracovníků vytvářejících rozhodnutí, strategii, obchodní politiku apod. ?

5.2.2 Detektivní rozpracování a dokumentování

Detektivní rozpracování je možné charakterizovat jako nejsložitější formu soukromé detektivní činnosti či činnosti bezpečnostního manažera (soukromé detektivní kanceláře či bezpečnostního managementu podnikatelského subjektu). Vyžaduje systematický, cílevědomý, plánovitý a komplexní přístup soukromé detektivní kanceláře (útvaru bezpečnostního managementu podnikatelského subjektu) případně soukromého detektiva či bezpečnostního manažera. V procesu detektivního rozpracování (rozkrývání, vyšetřování) se ale zpravidla na činnosti podílí více soukromých detektivů. Je využívána celá škála metod soukromé detektivní činnosti, které probíhají v různých vypracovaných algoritmech. Metoda detektivního rozpracování by ve svém závěru měla přejít do procesu realizace metody detektivního dokumentování. [5]

V procesu detektivní rozpracování sehrává významnou roli plán detektivního rozpracování, který má charakter jistých cyklů. Plán detektivního rozpracování je významným dokumentem detektivní činnosti v procesu detektivního rozpracování, který

řeší i otázky součinnosti a spolupráce v rámci daného procesu. Celý proces detektivního rozpracování je nutno chápat jako cyklus úkonů, postupů, rozhodování a opatření apod. Tento cyklus v sobě zahrnuje :

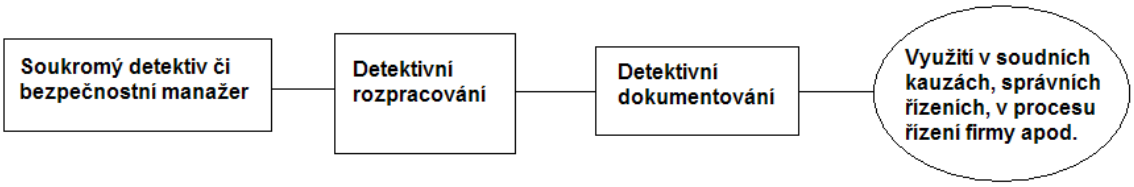
- vymezení (vytýčení) problému ;
- analýzu (vyhodnocení) informací, stop apod. které jsou k dispozici;
- vytýčení (stanovení) detektivních verzí;
- rozhodování o dalších krocích a využití metod, sil a prostředků;
- organizace průběhu realizace detektivního rozpracování;
- motivování - stimulování - operativní řízení;
- hodnocení výsledků postupu detektivního rozpracování;
- ukončení jednoho cyklu představuje započetí cyklu nového.

Detektivní rozpracování se vlastně odehrává v krocích :

- průběžná analýza nově získaných informací;
- vylučování či ověřování detektivních verzí a tvorba nových;
- aktualizace plánu detektivního rozpracování, stanovení nových úkonů a opatření k prověření vytýčených detektivních verzí;

Detektivní rozpracování lze považovat za jakousi kombinovanou formu soukromé detektivní činnosti, protože v jejím rámci jsou realizovány i jiné formy a metody např. detektivní prověrka, pátrání, dohled, průběžné dokumentování apod. [5]

Obr. 7 *Detektivní rozpracování 1*



Obr. 8 *Detektivní rozpracování 2*

5.2.3 Detektivní prověrka

Detektivní prověrka je také jednou z forem soukromé detektivní činnosti.

Může se jednat o:

- Prověrku pověsti osoby (z hlediska solventnosti, majetkových poměrů, osobních a rodinných poměrů),
- Prověrku zájmového prostředí (z hlediska výskytu negativních skutečností či osob),
- Prověrku režimu činnosti osob a jejich kontaktů,
- Prověrku podnikatelského subjektu či jiné organizační struktury
- Prověrku událostí, děje. [11]

Zaměstnavatelé by si měli uvědomovat, že jedním z nejlepších způsobů jak snižovat latentní kriminalitu uvnitř podniku na minimum je prověřovat minulost potencionálních uchazečů o místo, předtím než je přijmou.

V posledních letech se prosazuje po vzoru Spojených států i v evropských zemích jako součást náboru a kariérního růstu tzv.“pre-employment screening“. Doslovně přeloženo - prověření před zaměstnáním.

Skutečné prověřování zaměstnanců zatím v České republice rozvinuté není, ale zvláště v bezpečnostních agenturách by mělo být prověřování nutností. Je nutné snížit na minimum rizika spojená s přijetím nového pracovníka, či povýšení stávajícího pracovníka, může to ušetřit značnou finanční sumu. Pokud agentura disponuje vlastními detektivy, celý

proces může uskutečnit vlastními silami, což je nejlevnější a jediný možný způsob, protože těžko by si agentura mohla najmout konkurenční firmu pro prověření zaměstnanců.

Stupeň prověřování bývá odvislý od pracovního zařazení a pozice zaměstnance ve firmě, jakožto i od druhu a míry rizika souvisejícího s výkonem jeho funkce. Prověrka sestává z jednotlivých úkonů, jako je např. prověrka trestní minulosti, ověření pravdivosti o minulých zaměstnáních včetně zjištění referencí, o vzdělání a praxi v oboru, rodinných poměrech atd. U vyššího stupně přichází na řadu i prověrka pověsti v místě bydliště a prověření rodinných příslušníků. U nejvyššího stupně se již jedná např. o prověření bezdlužnosti nebo o detektivní prověrku, se zaměřením na zjišťování a pozorování volnočasových aktivit. Toto nejnáročnější prověřování je prováděno se zaměřením na zjištění rizika nevhodného okruhu přátel, kontaktních osob z jiných nebo konkurenčních firem, míry požívání alkoholu a drog. Zároveň se věnuje pozornost veškerým činnostem, které by mohly mít negativní vliv na výkon zaměstnání a finanční situaci prověřovaného (hraní hazardních her, automatů apod.). Je na zaměstnavateli, zda upozorní prověřovaného na možnost prověřování jeho osoby nebo zda zvolí prověrku utajovanou. Toto posouzení je záležitostí taktiky a účelu za jakým je prověrka prováděna. Pro prověřování některých údajů je ale nutná plná moc od prověřovaného. [30]

V rámci detektivní prověrky využívá detektiv celé škály metod soukromé detektivní činnosti:

- Detektivní vytěžování osob
- Detektivní pozorování
- Detektivní vytěžování evidencí, registrací, archivů apod.
- Detektivní osobní pátrání

Jakákoliv prověrka, byť sebekvalitnější, však nesejme z podniku zodpovědnost za konečné rozhodnutí. Ale činit rozhodnutí se znalostí všech okolností je vždy snazší a přesnější, než skok do tmy.

5.2.3.1 Detektivní vytěžování osob

Soukromý detektiv se zejména zaměřuje na vytěžování osob z okruhu:

- Bydliště prověřované osoby,
- Pracoviště prověřované osoby, a to včetně minulých zaměstnání,
- Míst, která prověřená osoba navštěvuje s ohledem na její zájmy a zvyklosti

Nelze vyloučit ani okruh osob v příbuzenském vztahu k prověřované osobě (zejména rodiče, sourozenci apod.).

Metoda detektivního vytěžování je ze strany soukromého detektiva řízený rozhovor s dotazovanou osobou. Tuto metodu je třeba považovat za základní postup detektivní práce, který je pro soukromého detektiva nezastupitelný. Metoda detektivního vytěžování směřuje k získání informací a představuje složitý proces, který je určován aktivní činností soukromého detektiva jako řídícího subjektu v sociální komunikaci a interakci s osobou vytěžovanou.

Detektivní vytěžování může probíhat nejenom s osobami z okruhu prověřované osoby, ale také se samotnou prověřovanou osobou. Zkušený detektiv může poznat už během rozhovoru, jestli je osoba nějakým způsobem podezřelá a zda je nutné ji důkladněji prověřit. Může se ptát například na otázky týkající se jeho životopisu a tak zjistit určité nesrovnalosti.

Detektivní vytěžování by mělo probíhat ve třech základních fázích [11] :

a) *Kontaktní část vytěžování* – Úkolem soukromého detektiva jako subjektu je blíže poznat vytěžovanou osobu jako objekt vytěžování. Jedná se o to, aby byl navázán kontakt a aby si soukromý detektiv v procesu nezávazného rozhovoru získal důvěru vytěžované osoby. Dalším krokem je navázání vhodné situace k budoucí komunikaci o předmětu vytěžování.

b) *Monologická část vytěžování* – Tato část spočívá v souvislém vylíčení událostí, skutečností, chování, jednání vytěžovanou osobou, aniž by jí do toho soukromý detektiv zasahoval. Monolog je volnou spontánní výpovědí vytěžované osoby.

c) *Dialogická část detektivního vytěžování* – Dialogická část spočívá v kladení otázek soukromým detektivem a v odpovědích vytěžované osoby na kladené otázky. Tato

fáze má za účel doplňujícími otázkami dotěžit relevantní informace, které nám vytěžovaná osoba ve svém monologu nesdělila.

Detektivní vytěžování je v případě ochrany před latentní kriminalitou důležité zejména pro potřeby personální práce.

5.2.3.2 Detektivní monitorování

Metoda detektivního monitorování (pozorování, sledování) je další z velmi významných a stěžejních metod soukromé detektivní činnosti. Jedná se o metodu velice frekventovanou, která má pro soukromou detektivní činnost vedle detektivního vytěžování klíčové postavení. Detektivní pozorování prováděné jako vizuální kontrola zájmové osoby může být prováděna [11] :

a) *Otevřeným způsobem* – a to staticky nebo dynamicky

b) *Skrytým způsobem* – a to rovněž staticky nebo dynamicky, přičemž zájmovým objektem může být:

- Zájmová osoba nebo skupina osob
- Prostor či jiné neživé objekty
- Probíhající skutkový děj

Skryté monitorování je převážnou částí této metody. Pokud by totiž sledovaná osoba o této metodě věděla, prováděla by účelově zastírací činnost. Monitorování slouží zejména:

- K potvrzení již známých poznatků o osobě či jiném subjektu,
- K vyvrácení takovýchto poznatků
- K získání nových upřesňujících poznatků a dalších informací,
- K získání zcela nových poznatků, které rozšiřují poznatkovou bázi

Detektivním pozorováním soukromý detektiv získává poznatky o:

- Pohybu osoby,
- stycích osoby,

- režimu dne osoby,
- jednání a chování osoby,
- situaci a činnosti v zájmových prostorách.

5.2.3.3 Detektivní vytěžování databází, evidencí, registrací a archivů

Databáze, evidence a registrace jsou velmi významným zdrojem informací, bez nichž se soukromá detektivní činnost nemůže obejít. Velice složitá je však otázka legality vstupu soukromého detektiva do některých evidencí a registrací. Z tohoto pohledu je třeba tyto databáze, evidence a registrace rozdělit na:

a) *Veřejně přístupné* – jedná se o evidence a registrace, do nichž má ve své podstatě po zaplacení příslušného správního poplatku přístup každý občan;

b) *Neveřejné* :

- Sloužící jen pro interní potřebu (např. soukromé katalogy sbírek)
- Důvěrné (např. finanční výkazy)
- Utajovaného charakteru (z hlediska zákona je jejich vytěžování zakázáno)

Celý systém těchto evidencí a registrací je pro detektivní činnost významným zdrojem informací. V každém případě by soukromý detektiv neměl usilovat o získání informací, které mají charakter utajovaných skutečností, neboť v opačném případě naplňuje skutkovou podstatu trestného činu a vystavuje se trestnímu stíhání. Z tohoto pohledu je také velmi významné, aby připravovaný zákon o provozování soukromých bezpečnostních činností v ustanoveních týkajících se detektivní činnosti vymezil oprávnění soukromého detektiva při výkonu jeho činnosti a aby tato problematika byla řešena i s ohledem na zákon č. 101/2000 Sb., o ochraně osobních údajů. V současné době je velmi významným zdrojem informací i ve vztahu k evidencím a registracím internet. Z internetu je možno získat mnoho cenných informací, jak o podnikatelských aktivitách, tak o fyzických osobách a další významné informace. [11]

5.2.3.4 Detektivní osobní pátrání

Detektivní osobní pátrání je třeba chápat jako soustavnou činnost soukromého detektiva realizovanou v jeho každodenní činnosti. Jedná se o nejčastěji užívanou komplexní metodu soukromé detektivní činnosti. V jejím rámci soukromý detektiv přímo a bezprostředně užívá veškeré detektivní prostředky, způsoby a postupy za účelem získání informací, informací o důkazech, věci a písemnosti, které by v budoucnu mohly sloužit jako důkazy apod. Při detektivním osobním pátrání se využívá zejména metody [11] :

- Detektivní pozorování,
- Detektivní vytěžování,
- Detektivní vytěžování a vyhodnocování dokumentů z evidencí, registrací, archivů,
- Kriminalistické metody vyhodnocování stop.

5.2.4 Detektivní ochrana

Detektivní ochranu je možno chápat jako ochranu osob – bodyguarding, nebo v našem případě jako detektivní ochranu majetku. Na rozdíl od služeb ochrany majetku a osob, která se vykonává ve stejnokroji, je soukromá detektivní ochrana vykonávána v občanském oděvu. Hlavní rozdíl je ale v odlišnosti využívaných metod a prostředků.

Podle publikace Komerční bezpečnost JUDr. Kameníka a JUDr. Brabce [11] je soukromá detektivní ochrana formou soukromé detektivní činnosti spočívající v souhrnu úkonů a opatření využívajících různých metod soukromé detektivní činnosti, metod kriminalistiky, metod kriminologie, sociologie, psychologie a řady forenzních disciplín, metod policejní praxe, směřujících ke kontrole dodržování žádoucího stavu. Dále sloužících k včasnému odhalení nebezpečných odchylek od žádoucího stavu a současně přispívajících k včasnému přijetí opatření, a tím opětovnému nastolení bezpečnosti chráněného subjektu. Jedná se o průběžné shromažďování informací o objektech (osobách,firmách a jejich majetku apod.), a to zejména:

- Pro potřeby personální práce
- Při ochraně proti úniku informací a dat
- Při získávání informací marketingového charakteru a konkurenčního charakteru

V našem případě jsou významné zejména informace pro potřeby personální práce a pro ochranu informací a dat – know-how.

5.2.5 Metoda fyziodetekce

Jedná se o metodu sledování činnosti nervové soustavy a s tím spojených fyziologických projevů. Tato metoda umožňuje snímat, vyhodnocovat a zaznamenávat hodnoty určitých fyziologických změn, které jsou vyvolané reakcemi vyšetřované osoby na vnější podněty. Tyto fyziologické změny vyvolané emocionálním napětím, stresem nebo bolestí nelze vědomě ovlivnit. Takovou stresovou situací může byt i vhodně položená otázka, kterou se člověk cítí byt ohrožen, a proto odpovídá lživě. Snímáním fyziologických projevů lze tedy odhalit, zda konkrétní osoba mluví pravdu vzhledem k předmětu vyšetřování.

Obecně můžeme říci, že se k fyziodetekci v bezpečnostní komunitě používají tzv. detektory lži. Nejsou to však detektory lži v pravém slova smyslu, nedetekuje se zde přímo lež, ale změna emočního napětí vyvolaná lží. Změnu emočního napětí může vyvolat strach, pocit viny, úzkost, stres apod. a k odhalení těchto pocitů slouží zařízení v podobě [9] :

a) *Polygrafického vyšetření* – Polygraf pracuje na principu zaznamenávání fyziologických změn, jako je změna krevního tlaku, odpor kůže, změna tepu, dýchání, svalového chvění apod. To znamená, že k měření dochází pouze na nižší hierarchické úrovni struktury lidských vlastností a dispozic. Úspěšnost polygrafu se udává na 60–90 %. Tato hodnota není zcela uspokojivá a to z důvodu možnosti oklamání daného zařízení.

b) *Analýza hlasu* – Sleduje odraz průběhu psychické reakce na změnách v oblasti hlasivek. Pro detektivní a zpravodajskou činnost vhodný především tím, že tento postup je možno použít bez vědomí osoby a stačí pouze na skrytý nejlépe digitální magnetofon nahrát řízený rozhovor s vytěžovanou osobou a tento záznam vyhodnotit na přístroji analýzy hlasu.

c) *Termovize jako prostředek fyziodetekce* – sleduje odraz průběhu psychické reakce na změně teploty těla. Rovněž termovizi je možno použít skrytým způsobem a

registrovat odezvy průběhu psychických reakcí na kladené otázky na periferii organismu, v tomto případě na změny teploty těla

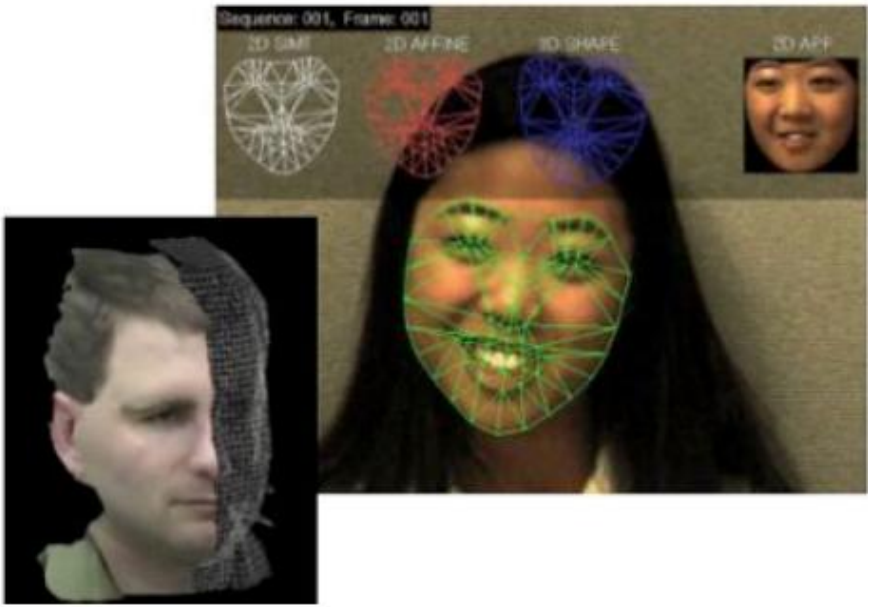
d) *Aktivaciometr* – Při detekci lži aktivaciometrem se detekuje na všech hierarchických skupinách tzn. že se sledují nejen fyziologické projevy na periferii organismu, ale také aktivace mozkových center. Díky těmto vlastnostem je aktivaciometr schopen zaznamenat i ty nejmenší změny emocionálního stavu člověka. Jeho úspěšnost odhalení lživé reakce vyšetřované osoby se odhaduje na 90-97 %. Přístroj aktivaciometr lze použít nejen k detekci lži, ale i k individuálnímu medicínskému a psychologickému vyšetření v institucích všeobecného i speciálního vzdělávání, v armádě, v ozbrojených složkách, ve školství, ale také v personalistice. S přístrojem aktivaciometr mohou pracovat osoby bez speciálního vzdělání. Aktivacimetr je tzv. „user-friendly", tedy uživatelsky nenáročný a k jeho obsluze běžnému člověku postačí přiloženy manuál nebo výukový program na CD, který je vždy součástí balení přístroje.

Obr. 9 *Aktivaciometr AC-9K [9]*

e) *Technologie vrstvení hlasu (LVA)* - Tato nová technologie byla přímo vyvinuta pro detekci lži. Detekuje a měří emoční obsah lidského hlasu. Jedná se o nové zařízení patentované izraelskou společností Nemesysco. Nepracuje na principu analýzy stresu v hlase, ale na unikátním principu změny hlasu vyvolaného změnami mozkové činnosti. LVA využívá okamžiku změny hlasu, které jsou vyvolány různými typy mozkové činnosti. Pomocí spektrální analýzy se zde sledují okamžité změny ve volných vlnových délkách řeči. Tímto způsobem LVA detekuje určité

anomálie v mozkové činnosti způsobené emočním napětím projevujícím se v řeči člověka. Můžeme říci, že LVA analyzuje „třasy mozkové činnosti.“ Tyto třasy se projevují při zvýšeném pocitu stresu a nelze je vědomě člověkem ovlivnit.

f) *Čtečka myšlenek* - Čtečka myšlenek, na které pracují američtí vědci z Carnegie Mellon University v Pittsburgu, se nazývá FAST (Future Attribute Screening Technology). Toto zařízení je schopno na dálku snímat různé fyziologické projevy člověka i jeho mozkovou funkci a do jisté míry předvídat jeho nekalé úmysly. Skenery tohoto zařízení by měli byt schopné bezkontaktně detekovat psychicky stav člověka. Tělo člověka, který je pod vysokým emočním napětím, samovolně vysílá signály jako je tep, rychlost dechu, pohyb očí, krku, mimiku obličeje, teplotu těla a „ošívání se“. Zařízení FAST je schopné tyto signály vyhodnotit a zjistit tak jestli osoba není pro společnost nějakym způsobem nebezpečná.



Obr. 10 *Snímání obličeje senzory FAST [9]*

g) *Infračervený detektor – tvář strachu* - Snímání „tváře strachu“ se provádí pomocí infrakamery s vysokou rozlišitelností. Při snímání tváře jsou vyslýchané osobě pokládány otázky, na něž odpovídá ano či ne, podle stejného principu jako u polygrafního vyšetření. Tvář je zde snímána infračervenou kamerou, která podrobně sleduje krevní oběh ve tváři vyslýchané osoby. Kamera dokáže

zaznamenat i nejmenší změny v prokrvení tváře. Při každé odpovědi je zhotoven snímek prokrvení obličeje. Emoční napětí, neboli lež se projevuje zvýšeným prokrvením, které lze tímto zaznamenat. Tato metoda se vyvíjí v Institutu detektoru lži (Polygraph Institute) při ministerstvu obrany USA. Hlavním šéfem je zde Andrew Ryan, který tuto metodu dokonce testuje na vlastních zaměstnancích. Raynův detektor je bezdotykový, vyslýchaná osoba tedy ani nemusí vědět, že byla podrobena vyšetření detektorem lži.

Obr. 11 *Průběh fyziodetekce [5]*

V České republice se k fyziodetekčnímu vyšetření na poli kriminality stále využívá přístroj polygraf. Toto zařízení je dle mého názoru zastaralé, má nízkou spolehlivost a disponuje jím u nás hlavně policie. Otázky sice sestavuje zkušený detektiv, což by v prostředí podniků PKB zřejmě nebyl problém, ale k vyhodnocení je nutno opravdových odborníků z řad lékařů a psychologů.

Pro rozšíření i do podniků komerční bezpečnosti by mohly přispět přístroje, které by bylo možno dobře využít při personální práci. Například aktivaciometr je na obsluhu

mnohem méně náročnější a teoreticky by mohl být využíván personalisty či detektivy k odhalení nebezpečných úmyslů potencionálních zaměstnanců nebo k odhalení nepravd v jejich životopisech. Tento přístroj má ale stejně jako polygraf nevýhodu, že k němu musí být člověk připojený. Proto by mohlo být využíváno bezkontaktního snímání pomocí nových zařízení, jako je např. analyzátor vrstvení hlasu LVA, čtečka myšlenek FAST nebo infračervený detektor - Tvář strachu. Podobných přístrojů se vyvíjí celá řada. Výhodnou u nich je, že lze osoby snímat, aniž by věděly, že jsou kontrolovány. Bezkontaktní detekce je velmi rychlá a podezřelé osoby můžou být vyhodnoceny téměř okamžitě. Takový detektor pochopitelně neoznačuje přímo zločince, ale dává určitou informaci o podezřelé osobě, kterou je třeba dále prověřit. Toho by mohli využívat detektivové v podnicích PKB.

V současné době je to ale ještě poměrně nereálné vzhledem k finančním nákladům. Zřejmě by byla vhodná i nějaká právní úprava takového problému. Do budoucna by ale tyto přístroje mohly být významnou zbraní v boji proti latentní kriminalitě jak v podnicích PKB tak v ostatních podnikatelských subjektech, firmách či asociacích.

II. PRAKTICKÁ ČÁST

6 ZHODNOCENÍ SOUČASNÉHO STAVU

Pro vypracování této práce bylo nutností získat názory přímo z praxe. Od počátku jsem se obával, že se agentury nebudou chtít podělit o názory na toto citlivé téma a tyto obavy se později vyplnily. Kdo by se také chválil s tím, že se u něj v podniku krade nebo vyzrazoval opatření, kterými se liší od konkurence. Nejprve jsem se pokoušel kontaktovat bezpečnostní asociace, ale z došlých odpovědí jsem musel uznat, že otázky, které jsem pokládal, nebyly příliš šťastně zvoleny. Počáteční neúspěchy mě ale neodradily a po úpravě otázek jsem se snažil kontaktovat majitele firem písemně, telefonicky i osobně. Celkem jsem kontaktoval přes 40 bezpečnostních agentur a osob pohybujících se v průmyslu komerční bezpečnosti a odpovědi se mi podařilo získat od:

PhDr. Michala Fábery, dříve ředitele bezpečnostní agentury Group 4 Securitas, dnes majitele firmy Orange Group a.s., dále pak od agentur:

Čechymen s.r.o. ; Informační a bezpečnostní agentura s.r.o. ; S&S Securitas s.r.o.; bezpečnostní agentura Martina Růžičková s.r.o. ; NSC Security; S.O.S. a.s. Olomouc; D.I.SEVEN a.s.; MOBA, spol.s r.o. ; Alwas Maty Security, s.r.o.;

6.1 Výsledky

V prvé řadě jsem v bezpečnostních agenturách zjišťoval jejich zkušenosti s jednotlivými druhy rozkrádání. Zajímavé případy, které se mi podařilo vytěžit, uvádím v následující kapitole.

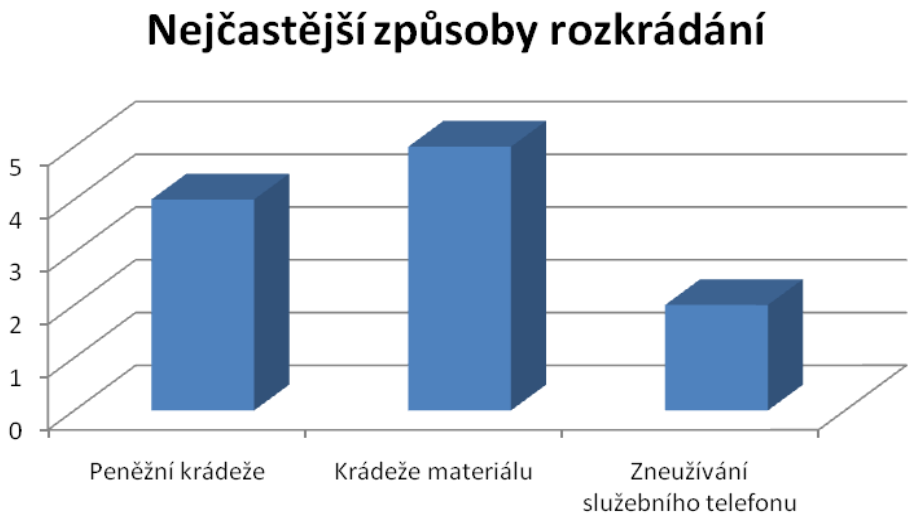
Žebříčku krádeží v mém průzkumu vévodily krádeže materiálu. Hlavním důvodem je zřejmě snadnost jeho vynesení, případně nízké zabezpečení. Objevují se jak krádeže montážního materiálu, tak různých předmětů, které se dají prodat ve sběrných surovinách. Agentury mají také velké problémy s krádežemi zboží ve střežených objektech, zejména obchodních domech, já jsem se ale ve své práci zaměřoval hlavně na majetek podniků PKB, ačkoliv návrhy aktivních opatření uvedené v této práci mohou vyřešit i tento problém.

Druhým nejčastějším případem byly peněžní krádeže. Ty jsou nejzávažnější a pro podnik mohou mít likvidační charakter. Díky panu PhDr. Fáberovi, který pracoval jako ředitel Group 4 Securitas, se mi podařilo získat podrobnosti o tehdejších

mnohamilionových krádežích. Jinak ale žádná z oslovených agentur nepřiznala větší krádež finanční hotovosti v řádech milionů, kterou by spáchal jejich zaměstnanec. Většinou se jednalo o menší částky, které mizely ze šaten, nebo si strážní nechávali část poplatků, které vybírali například za parkování.

Třetím nejčastějším případem bylo zneužívání služebních telefonů. V další kapitole je jeden zajímavý případ, který se mi podařilo vytěžit. Další případy nebyly tak závažné a vedení nad ním často mávlo rukou, protože se nejednalo o větší částky.

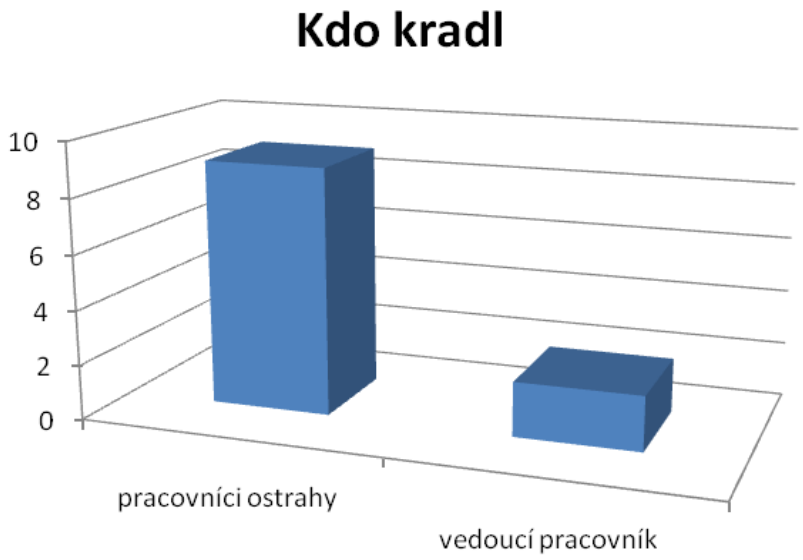
Co se týká dalších způsobů rozkrádání, objevil se jeden případ krádeže firemní zakázky. Zneužívání služebních vozidel se žádné neobjevilo, důvodem může být i to, že většina agentur již využívá GPS lokátorů. Nejsem si ale jist, zda dostatečně využívají jejich možností a pravidelně provádějí kontrolu. Mnoho důležitých věcí totiž není v agenturách kontrolováno. Například čisticí prostředky pro velké průmyslové úklidy jsou nakupovány dopředu a částky jdou do milionů, majitelé při takovém množství nehledí na to, jestli se pár kusů ztratí. Žádná z agentur také nepřiznala počítačovou kriminalitu. Důležité informace mají většinou zabezpečeny pouze heslem.



Graf 1 *Nejčastější způsoby rozkrádání*

V devíti agenturách se setkávali nebo stále ještě setkávají s krádežemi u strážných nebo jiných pracovníků ostrahy, z toho ve dvou odhalili krádež vedoucího pracovníka. Agentura, která by neměla žádné problémy s rozkrádáním vlastními zaměstnanci se neobjevila, některé přiznaly potíže velké, jiné pouze minimální.

Překvapivě se žádný z majitelů nezmiňoval o krádeži z řad uklízeček, sekretářek apod. Montéři, kteří jsou schopni zužitkovat kradený materiál, se také ve výsledcích neobjevili. Tedy až na jednoho, který ale povýšil mezi vedoucí pracovníky a jeho případ je zmíněn v další kapitole.

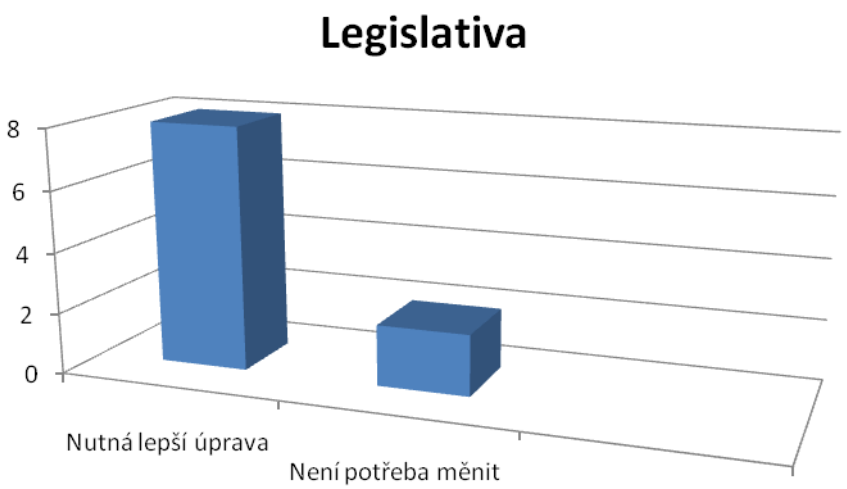


Graf 2 *Nejčastější pachatelé krádeží*

Dále jsem zjišťoval, zda jsou majitelé bezpečnostních agentur spokojeni se současným stavem jejich zabezpečení proti kriminalitě zaměstnanců. Podle očekávání většina z dotázaných odpověděla, že za současného stavu dělají vše proto, aby kriminalitě zamezili. Využívají široké škály technických i režimových opatření jako je například klíčový režim, kamerové a přístupové systémy, pochůzkové systémy apod. Pouze jedna agentura mi sdělila, že neustále snižování cen v tomto sektoru má u nich za následek také nižší frekvenci preventivních opatření (např. kontrolní činnost vedoucích pracovníků). Ačkoliv tento problém tíží všechny z oslovených agentur, ty ho ale zmínili v jiných souvislostech.

Graf 3 *Spokojenost s opatřeními proti kriminalitě zaměstnanců*

Co se týká legislativy, většina agentur považuje za nutnost zákon o bezpečnostních službách. Některé by ocenily zejména možnost kontroly opisu rejstříku trestů, protože při současném stavu, kdy se kontroluje pouze výpis, může být do agentury přijat i dříve trestaný člověk. Objevily se také dva názory, že pokud se komerční bezpečnost dělá slušně, není třeba, aby byla jakkoliv speciálně legislativně upravována, postačí stávající úprava. To ostatně platí v každém oboru.

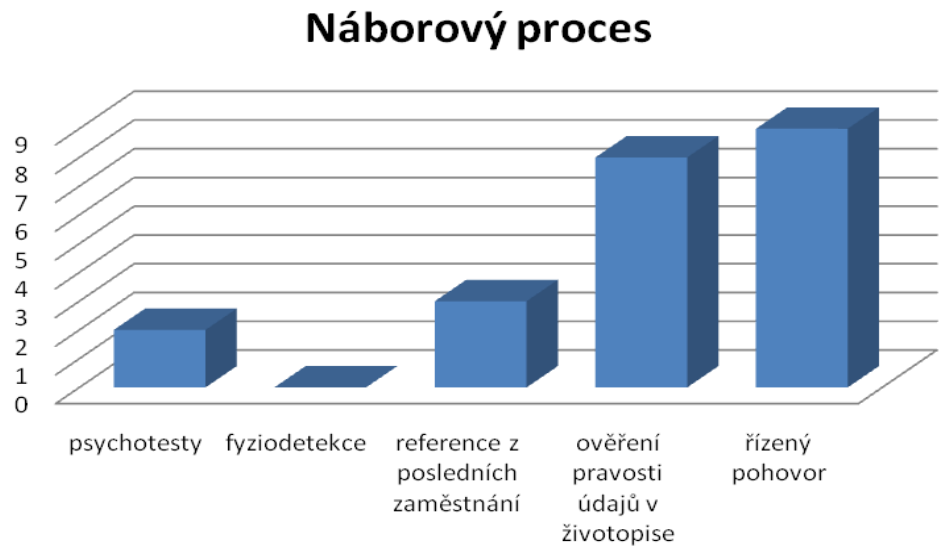


Graf 4 *Legislativa*

Jak už jsem psal výše, agentury tíží zejména nízké ceny v oboru komerční bezpečnosti. Některé uváděli jako hlavní příčinu určitou lehkost zahájení tohoto podnikání a při enormním tlaku zákazníků na nízkou cenu bezpočet úhybných i protizákonných manévrů ze strany firem za účelem dosažení co nejnižší ceny - zpětně pak ochota velkého množství zaměstnanců nechat se svými zaměstnavateli bezostyšně využívat. Z nízké ceny služby se odvíjí nízké mzdy pracovníků ostrahy a tudíž i jejich náchylnost si jakkoliv dále přivydělat.

Bezpečnostní agentura chce většinou rychle vydělat a nabere velký objem zakázek, aby byly větší zisky. Na provádění zakázek potřebuje zaměstnance za málo peněz a tak sáhne po lidech z úřadu práce, kteří jsou již delší dobu ve finanční tísni a budou pracovat a rádi za 55,- Kč hrubého s tím, že za záchyt zloděje mají třeba 100,- Kč (pokud toto vůbec dostanou). Tito lidé pak pracují jako zběsilí, aby si nějaké peníze vydělali a klidně odpracují i 250 hodin za měsíc. To ale není problém, problém je, že za 200 - 250 hodin dostanou mzdu 11-14.000,- Kč hrubého + za 10 záchytů 1.000,- Kč. Za tuto mzdu si majitel nemůže být jistý, zda mu tento člověk přijde druhý den do práce a musí mít zaměstnance, který jej každý den zkontroluje, jestli vůbec osoba přišla nebo někde nespí po druhé směně v jiném zaměstnání. Takováto sorta zaměstnanců pak nejčastěji krade, což ukázal i průzkum. Jeden z majitelů dokonce zažil situaci, kdy se zaměstnanec SBS za 5,000,- Kč nechal zbít a svázat a umožnil krádež zákazníkova zboží.

Od počátku jsem zastával názor, že největší vliv na kriminalitu zaměstnanců má jejich samotný výběr a následná kontrola doplněná dalšími opatřeními. To mi potvrdili i v bezpečnostních agenturách a tak jsem se zaměřil na samotný náborový proces a zjišťoval, jaké metody využívají.



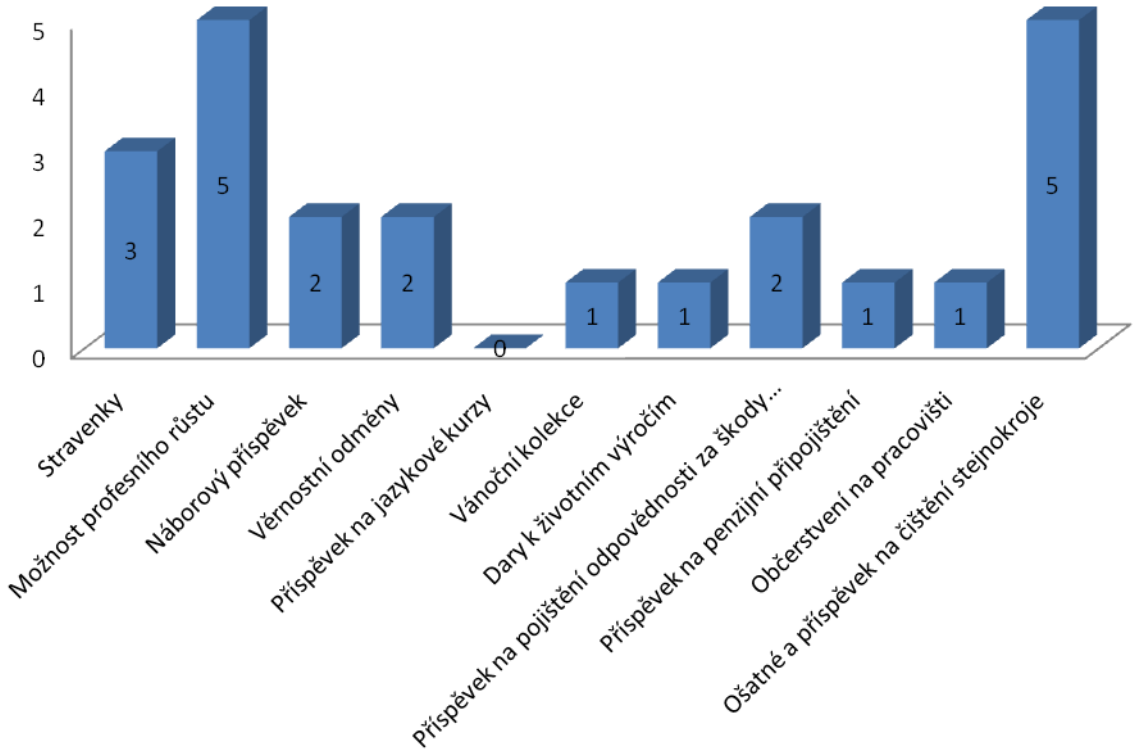
Graf 5 *Náborový proces*

Agentury nechtěly příliš dopodrobna rozebírat svůj náborový proces, ale z toho, co se mi podařilo zjistit, vyplývá, že řadové zaměstnance kontrolují na požadavky dané ze zákona, ale navíc toho mnoho nedělají. Obvykle každý zaměstnanec projde řízeným pohovorem, probíhá ověření údajů ze životopisu jako je nejvyšší dosažené vzdělání apod., ale jiné údaje jako minulá zaměstnání se nekontrolují. Jen ve třech agenturách požadují reference z posledních zaměstnání a to jen na vedoucích pracovnících. Při přijímání zaměstnanců na vedoucí pozice bývají agentury opatrné a většinou se snaží povýšit někoho ze stávajících zaměstnanců, který si problematikou prošel „od spoda“ a zná ji. Agentura zná jeho, jeho přístup k práci a jeho rezervy. Tím pádem je tento člověk respektován svými podřízenými, jelikož práci zná a nedá se jen tak zmanipulovat planými argumenty.

Metodu fyziodetekce v žádné agentuře nevyužívají a v nejbližší době ani nebudou. Psychotesty byly používány hlavně dříve, ale v současnosti už od nich agentury ustupují a pouze ve dvou z oslovených agentur je stále používají a to jen na prověřování zaměstnanců na vyšších pozicích, či na zaměstnance provádějící speciální a kvalifikované práce. Setkával jsem se s názorem, že psychotesty jsou jen indikací a bez celého dalšího systému prověřování včetně řízených pohovorů atd. jsou jen vyhazováním peněz, což je jistě pravda.

Jedna z oslovených agentur se trochu lišila od ostatních, protože se snaží zaměstnávat zejména cizince, jelikož s nimi mají jen dobré zkušenosti. Nejlepší zkušenosti mají s občany Uzbekistánu, jelikož ve chvíli kdy střeží objekt, je to „jejich“ území. Pokud se týká nedokonalé znalosti českého jazyka, tak tento hendikep vysoce zastiňuje kvalita vykonané práce. Pokud se týká ostatních cizinců blíže k české mentalitě, (např. Slováci, Ukrajinci) tak se zde procentuálně zvyšuje riziko laxního přístupu a výkonu práce. V ostatních agenturách mají nejlepší zkušenosti s bývalými pracovníky Policie ČR, Vězeňské služby a Armády ČR, ale ani u nich si nemůže být nikdo jistý, že žádný trestný čin nespáchají.

V poslední fázi průzkumu jsem zjišťoval, zda agentury využívají zaměstnaneckých výhod jako prostředku k motivaci zaměstnanců. Vzhledem k množství otázek, které jsem pokládal, už jsem tyto informace získával jen od pěti z oslovených agentur, kde byli majitelé nejochotnější.



Graf 6 *Zaměstnanecké výhody*

Ve všech pěti společnostech poskytují svým zaměstnancům ošatné a příspěvek na čištění stejnokroje, dále je u nich možnost profesního růstu v závislosti od výsledku hodnocení a plánu profesního rozvoje. Ve třech společnostech poskytují svým zaměstnancům stravenky, ale v jedné z nich od toho hodlají upustit. Dvě z agentur nabízejí náborový příspěvek za doporučení nového zaměstnance, věrnostní odměny či příspěvek na pojištění odpovědnosti za škody způsobené zaměstnavateli. Pouze jedna společnost nabízí příspěvek na penzijní připojištění, dary k životním výročím a vánoční kolekce. Jedna společnost nabízí také občerstvení na pracovišti ve formě výdejníků vody, ale u všech společností je možno občerstvit se vodou z kohoutku. Žádná z agentur nenabízí příspěvek pro zaměstnance na jazykové kurzy.

7 ANALÝZA DOSUD PÁCHANÉ LATENTNÍ KRIMINALITY

7.1 Výběr a rozbor zjištěných případů

Zaměstnanci bezpečnostních agentur mají na svém kontě celou řadu závažných případů, mezi které patří i ty největší krádeže v českých dějinách. První dvě podkapitolky jsou určeny krádežím finančních hotovostí, o kterých se mi podařilo zjistit informace z médií. Další případy jsem vytěžil od osob pracujících v průmyslu PKB.

7.1.1 Krádež 564 milionů

Zaměstnanec agentury František Procházka, který byl do krádeže podle policie zapojen, přišel v sobotu 1.prosince 2007 do práce. V pobočce na pražském Žižkově, kam agentura sváží a přepočítává tržby od svých klientů, měl směnu. Krátce poté, kolem devíti hodin ráno, přijela před bránu do podzemních garáží u domu bílá dodávka Volkswagen Transporter s registrační značkou 1L7 4973. Na první pohled se nelišila od aut, která agentura používá pro převoz peněz. Vůz byl však soukromý, patřil Procházkovi, který si ho koupil už v roce 2003. Právě Procházka ho totiž nedávno polepil samolepkami s logem bezpečnostní agentury, aby jeho auto vypadalo jako firemní. Dodávku řídil neznámý muž. Procházka už na něj čekal a bránu mu otevřel. Možná to zní divně, ale bylo to skutečně tak jednoduché. Nikdo si nevšiml něčeho podivného," řekl policista obeznámený s případem. Auto vjelo do útrob domu a zůstalo zde jen několik málo minut. Ty stačily na to, aby Procházka společně s řidičem naložili do vozu připravené balíky s bankovkami. Vůz pak odjel a Procházka se vrátil ke své práci. Vše vypadalo jako normální převoz peněz, kterých se každý den v pobočce odehraje několik. Aby krádež Procházka zamaskoval, zůstal v práci do konce směny. Odcházel až v sedm večer. Řidič dodávky nejel s penězi daleko. Ještě v Praze je přeložil do jiného auta. Protože balíky s penězi vážily několik set kilogramů, musel mu pomáhat někdo další. Procházka byl v té době stále v práci. [31]

Firma každopádně na rekordní krádež přišla až v neděli v poledne. Na policisty se lidé z agentury obrátili přesně ve 12 hodin 8 minut. Zloději tak měli dost času zmizet. V případu zůstává řada nejasných věcí. Odborníkům i policistům především vrtá hlavou, jak mohl Procházka přelstít bezpečnostní systém firmy. Mohl sice díky svému postavení do trezoru firmy, neměl však právo vpouštět auta do objektu.

Obr. 12 *Hlavní podezřelý*

Informace jsem se pokoušel získat z archivů, ale ty byly údajně zrušeny. Proto většina informací o případu pochází z médií, takže je možné, že spousta popisovaných událostí proběhla jinak a krádež jistě nebyla tak jednoduchá, jak vypadá. Co se týká osobnosti Procházky, určitě se nejedná o žádného psychopata, který by jednal zkratovitě. Celý čin byl velmi dobře zorganizovaný a zřejmě plánovaný delší dobu, než jsou 4 měsíce jeho působení ve firmě. Měl minimálně jednoho komplice, který byl viděn ve vozidle. Policie komplice následně dopadla, ale po čase byl propuštěn na kauci 10 milionů korun.Co je s Procházkou nyní, není pro tuto práci až tak důležité. Zajímá nás spíš, jak k tomu mohlo vůbec dojít?

Dění ve firmě navíc sledují bezpečnostní kamery. Před i po krádeži zřejmě musel vyřadit několik bezpečnostních mechanismů. Takže zůstává otázka, jestli mu nemohl pomoci i někdo další z firmy. Na případu pracuje i nadále speciální vyšetřovací tým, i když už ne tak početný jako na počátku kauzy.

Suma, která byla odcizena by byla asi pro většinu menších agentur naprosto likvidační. G4S je ale jedním z největších a nejsilnějších provozovatelů peněžního svozu. Jde o velmi silnou agenturu se zahraniční účastí, evropským i světovým rozšířením, pojištěním a zajištěním. Díky pojištění a svému postavení ustála tato bezpečnostní agentura i krádež půl miliardy korun. Nicméně její pověst výrazně utrpěla a všeobecně klesla také důvěra v bezpečnostní agentury.

Podařilo se mi získat rozhovor s PhDr. Michalem Fáberou, který dva roky před případem, pracoval jako ředitel bezpečnostní agentury Group 4 Securitas. Uvádím zde části rozhovoru, které se vztahují k tomuto případu:

Uvádí se, že podezřelý využil situace, kdy se mohl dostat do trezorové místnosti společnosti, tam vzal peníze v hotovosti, přemístil je do tašek a nechal je komplicem odvézt z budovy neznámo kam. Sám pak normálně zůstal v zaměstnání. Mohlo to být tak jednoduché?

Z informací, které mám, a mám je pouze z otevřených zdrojů, ten člověk tam byl sám. Jedno z prvních pravidel veškeré manipulace s hotovostí, ať je to soukromá agentura, ať je to banka, ať je to pošta, je, že u takovýchto manipulací musí být vždycky minimálně tři lidé. A ještě navíc tři lidé, kteří rotují, to znamená, nevědí dopředu, s kým dalším budou zrovna ve službě. To, že tam zůstal do konce směny, to je spíš otázka pro psychologa a otázka profilu toho člověka. On tím, že tam zůstal, nechal čas svým komplicům a oddálil možnost zjištění celé té činnost. Ale jak říkám, spíš než to, že tam zůstal do konce směny, mě zaráží to slovíčko sám. V trezorovém oddělení totiž musí být vždy tři zaměstnanci. Ani trezor není schopen odemknout jeden. Další lidé otevírají autu bránu.

Třídírna peněz se skládá ze tří částí: trezoru, kde jsou uložené peníze, vlastního přepočítávacího pracoviště a takzvaného "předtrezoří", kam zajíždí obrněný automobil. Procházkovo auto s falešnými logy G4S muselo při vjezdu nejspíš překonat hned několik kontrolních stanovišť – nejméně tři: bránu do budovy, pak takzvanou roletu, která se za vozem zavře, a prostor zvaný Interlock.

"Dveře" otevírá operační středisko. Pak si papíry řidiče ověří ještě obsluha trezoru. Auto totiž nakonec dorazí k zařízení připomínajícímu kolotoč rozdělený přepážkou. Na "kolotoč" se pokládají peníze. Tento okamžik museli zloději při krádeži dobře zkoordinovat – řidič musel mít jistotu, že se v dané chvíli shledá s Procházkou či komplicem.

Na otázku, zda případ vyšetřuje i sama bezpečnostní agentura PhDr. Fábera odpověděl:

Agentura sama interně vyšetřuje, ale především vyšetřuje pojišťovna. Experti z pojišťovny provádějí interní šetření, které se v podstatě týká toho, jak byly dodrženy procedury

stanovené té agentuře a jak fungovala interní technická opatření. Tam takovéhle případy vždy vycházejí z toho, že rizika v takovémto businessu jsou eliminována ve třech rovinách. Jedno riziko jsou lidé. V tomto případě, o kterém mluvíme, ten lidský faktor zřetelně selhal. Druhá rovina jsou technická a bezpečnostní zařízení typu kamerových systémů, mechanických zábran. Třetí rovina jsou procedury, jak se co dělá a jak se co má dělat. Zřejmě v tomto případě selhaly i ty další roviny, nebo alespoň jedna z nich

Je normální, že firma přijde na to, že jí chybí víc než půl miliardy korun až o den později?

Není to normální. Ale to zase souvisí pravděpodobně s tím informačním systémem založeným na lidském faktoru, protože ta diference byla zjištěna v okamžiku, kdy odešel ze služby zmíněný Procházka a nastoupil někdo jiný. A po čase zjistil, že v trezoru chybí peníze.

Existují nějaké statistiky, co se týče spolehlivosti zaměstnanců bezpečnostních agentur?

Pro mě to byl jeden z hlavních nástrojů řízení takovéto agentury, analýzy odchodovosti, důvodů odchodovosti, analýzy vnitřní trestné činnosti, nebo drobné trestné činnosti ve firmě a z toho vycházející manažerská opatření. A hlavně opatření vycházející do té řídící sféry, znovu říkám, protože tam je ... to základní jsou opravdu ony procedury. I člověk, který by měl sklony k páchání trestné činnosti, jestliže mu nevytvoříte příležitost, tak k té trestné činnosti nedojde. Protože tam je vždycky potřeba dvou věcí, záměr a příležitost. Máte-li záměr, nemáte-li příležitost, k ničemu nedojde. A naopak.

7.1.2 Další známé krádeže finančních hotovostí

154 milionů korun- 16.září 2002

Nejméně tři muži přepadli na Evropské třídě v Praze 6 vozidlo bezpečnostní agentury Group 4 Securitas, která právě odvážela ze Citibank a dalších objektů peníze. Lupiči byli ozbrojeni a měli výbušninu. Dva z nich byli oblečeni v uniformách zásahové policejní jednotky, jeden byl bez masky, druhý měl přes hlavu pletenou pruhovanou kuklu. Třetí byl v civilu a na hlavě měl karnevalovou masku s gumovým obličejem. Na místě činu

stála také bílá felicie s černým nápisem POLICIE. Při přepadení nebyl nikdo zraněn. Poslední, i když velice matnou stopou je to, že jeden z pachatelů mluvil špatně česky, pravděpodobně s ruským přízvukem. To však mohl předstírat, aby policii zmátl. Později byli dva z lupičů identifikování jako členové tzv. Berdychova gangu. Gang operoval v naší zemi od roku 1995. Jeho základní silou bylo napojení na policejní špičky, které jim dovolily využívat policejní taktiku, výstroj, zbraně, ale i doklady.Mozkem celého zločinného spojení je bývalý policejní informátor David Berdych, který vlastnil i bezpečnostní agenturu.

74 miliónů korun, 17. ledna 2008**:**

Členové posádky vozidla bezpečnostní agentury Fenix policii řekli, že byli při zastávce na Semilsku přepadeni ozbrojencem, který si vynutil vydání peněz. Podle policistů se však na činu, jenž se zřejmě odehrál v Hořicích na Jičínsku, podílela posádka vozidla. Pachatelé včetně řidiče vozidla byli odsouzeni - řidič na pět a další dva muži k deseti letům vězení. Nyní už bývalá ministryně spravedlnosti Daniela Kovářová loni v červnu přerušila pobyt ve vězení dvěma zlodějům odsouzeným za krádež 74 milionů korun. Policisté, žalobci i soudci ji tehdy před takovým krokem varovali. Peníze z loupeže se totiž nikdy nenašly. A proto se všichni obávali, že by mohli zloději zmizet. To se nakonec také stalo a dosud nejsou k nalezení.

37 miliónů korun, 8. března 2006:

Ozbrojený lupič přepadl v Jindřichově Hradci vůz bezpečnostní agentury převážející peníze z banky. Českobudějovický krajský soud poslal do vězení dva bývalé pracovníky bezpečnostní agentury za zpronevěru, a to na devět a 7,5 roku. Jejich údajný komplic byl osvobozen.

27 milionů korun - 16. září 2004:

Auto bezpečnostní agentury bylo prý přepadeno ve Frenštátě pod Radhoštěm na Novojičínsku. Vyšetřování ukázalo, že loupež fingovali dva zaměstnanci agentury, které soud odsoudil na sedm a 6,5 let. Pachatelé za necelých pět měsíců po loupeži stihli utratit asi milion korun.

24,7 milionu korun - 4. prosince 2003:

Zaměstnanec bezpečnostní agentury Securitas zinscenoval spolu s komplicem u Ostopovic na Brněnsku přepadení služebního vozu firmy. Při loupeži 24,7 milionu korun byl zavražděn třiadvacetiletý pracovník ochranky. Hlavní pachatel byl za loupežnou vraždu pravomocně odsouzen k 17 letům vězení.

23 milionů korun - 2. srpna 1995:

Skupina pachatelů odcizila z transportního vozidla bezpečnostní služby Fenix na cestě z Brna do Prahy peníze převážené České spořitelně. Krádež měli na svědomí pracovníci Fenixu a další lidé na ně napojení. V roce 1997 byl jeden z nich v nepřítomnosti odsouzen na 11 let. Dva zaměstnanci Fenixu dostali devět a 7,5 roku. [32]

Jak už jsem psal výše, popisy případů pocházejí z veřejně dostupných informací, do policejních spisů se mi bohužel nahlédnout nepodařilo. Byl jsem velice překvapen, že prakticky všechny největší loupeže nebo krádeže peněz v historii samostatné České republiky mají na svědomí tehdejší nebo bývalí zaměstnanci bezpečnostních agentur. Ani v jednom případě se nejednalo o žádné zkratové jednání a vše bylo pečlivě plánováno většinou více než jednou osobou. To jenom podtrhuje důležitost důkladného výběru zaměstnanců. V souvislosti s latentní trestnou činností hovoříme především o krádežích, protože probíhají skrytě a než dojde k jejich odhalení, uplyne často velmi dlouhá doba a na viníka se nemusí ani přijít.

U loupeží (§ 173) je však použito násilí a na čin je tím pádem upozorněno okamžitě, nejedná se proto o latentní kriminalitu. Přesto jsou výše uvedeny i některé případy loupeží, protože jsou prováděny zaměstnanci podniků PKB a tudíž se na ně můžou vztahovat opatření použitá v této práci.

7.1.3 120 tisíc korun- zneužití služebního telefonu

Podnik komerční bezpečnosti obdržel zakázku na střežení významné firmy, která tvořila zisk a neustále zaměstnávala nové pracovníky. Zakázka byla lukrativní a proto vedení podniku komerční bezpečnosti mělo zájem, aby bylo vše z hlediska ochrany

v pořádku. Byl zaveden kontrolní systém obchůzek tzv. PES (který jak později zjistíme byl velmi důležitý při rozkrytí latentní kriminality). Mimo jiné firma, která podnik střežila obsluhovala a přepojovala na ústředně telefonické hovory. Řediteli podniku komerční bezpečnosti volal pracovník, který měl na starosti ostrahu všech závodů a sdělil mi, že Telecom zaslal jeho firmě fakturaci za uskutečněné telefonní hovory ve výši 120 tisíc Kč. Okamžitě ze strany firmy byla faktura podniku uhrazena a započato šetření odhalení možných pachatelů.

1. Zjištěno, že nedopatřením při opravě ústředny pracovník Telecomu uvolnil další linku s možností vstupu do celostátní sítě.
2. Veškeré hovory byly uskutečněny na erotické služby
3. Linka byla použita vždy tenkrát, když druhý pracovník prováděl venkovní obchůzku po kontrolních bodech a na vrátnici zůstal muž, který telefonoval.
4. Obchůzkový systém PES umožnil analyzovat zpětně, kdo volal na erotickou linku.
5. Bylo zjištěno, že 75% hovorů uskutečnil hlavní pachatel a zbylá část hovorů byla rozdělena mezi dalších šest pachatelů.

Tito drobní pachatelé, kteří se dobrovolně doznali k používání telefonů, uhradili způsobenou škodu. Hlavní pachatel se k trestné činnosti nepřiznal, proto na něj bylo podáno trestní oznámení o spáchání trestného činu a celá věc se dostala k trestnímu soudu. Pachatel byl odsouzen na základě přesné analýzy s porovnáním obchůzkové činnosti podle elektronického systému a volání po telefonních linkách. Zde je ukázka toho, že pachatel konal bez zábran trestnou činnost, aniž by vedení firmy mělo jakoukoli informaci o jeho protiprávním jednání.

7.1.4 450 tisíc korun- neprověřený strážný

Majitel bezpečnostní služby, který nechce být z pochopitelných důvod jmenovaný, uvedl největší událost, která se mu v historii jeho podnikání stala.
Když po konkurenční bezpečnostní agentuře přebral střežení jedné administrativní budovy, její majitel mu doporučil, aby tam jeden tehdejší hlídač zůstal, protože prostředí zná a v práci je velmi dobře zaběhnutý.

Po dvaceti dnech budovu vykradli, přičemž škoda na odcizené hotovosti a majetku byla ve výši 450 000 korun. Hlídač byl podle policie pod vlivem alkoholu, přičemž některé dveře, které měli být poškozené, nejevily známky poškození. Doposud není jasné, jestli šlo o typické vloupání nebo o zinscenovanou krádež, v které měl prsty strážný se svým bývalým zaměstnavatelem nebo sám majitel budovy, který si nechal proplatit škodu.

Tento případ je dobrým příkladem latentní kriminality, protože ačkoliv se na krádež přišlo, nebyl zjištěn viník. Každopádně velký podíl na krádeži má hlídač, ať už v ní měl prsty nebo jen selhal ve výkonu povolání. To jenom dokazuje nutnost řádného prověření zaměstnanců, i pokud mají doporučení a praxi u bezpečnostních agentur, policie apod.

7.1.5 Zakázka načerno, neznámá finanční škoda

Bezpečnostní agentura měla rozjednanou s klientem zakázku na zabezpečení objektu a jeho následné připojení na PCO. Jeden ze zaměstnanců agentury ale tajně s klientem dojednal, že mu objekt zabezpečí sám a tudíž bude výsledná cena nižší.

Mezitím se ale bezpečnostní agentura začala zajímat, proč s nimi potencionální zákazník přestal komunikovat a vydala se k němu zjistit důvod. Jejich překvapení bylo veliké, když zjistili, že podle nálepek už objekt střeží, ačkoliv o tom nic nevědí. Po rozmluvě s majitelem objektu zjistili, že celý objekt zabezpečoval jejich zaměstnanec. Majitel ačkoliv dobře věděl, co se stalo, měl ještě tu drzost a zajímal se o možnost takto zabezpečený objekt připojit na PCO této agentury. Po zjištění takovýchto skutečností byl zaměstnanec propuštěn a údajně se ještě pokoušel zlákat k odchodu další zaměstnance, aby společně začali podnikat.

Tento případ je poměrně ojedinělý, ale ukazuje, že i vedoucí pracovníci můžou být schopni takovýchto podvodů. Lze tomu těžko zabránit, pokud má zaměstnanec důvěru vedení a takovouto činnost si sjednává ve svém volném čase. Pokud by ale tušil, že si agentura hlídá každého potencionálního zákazníka, jistě by se do toho nepouštěl, proto je i takováto činnost velmi důležitá.

7.1.6 650Kč, Krádež v obchodním domě

Strážný, který krade v obchodním domě, okrádá spíše samotný obchod než svou agenturu, ale v konečném důsledku to může způsobit škodu i samotné agentuře.

Zaměstnanec bezpečnostní agentury, kterému bylo přes padesát let a měl třicetiletou praxi u policie jako vyšetřovatel, plnil vzorně své pracovní úkoly a doslova vyčistil dvě prodejny od narkomanů a bezdomovců, kteří tam kradli. Do prodejny se opět vrátili normální zákazníci. Po určitém čase byla provedena náhodná kontrola a u tohoto vzorného zaměstnance bylo nalezeno zboží v hodnotě 650 Kč. Zřejmě se nejednalo o první případ, ale to mu již nešlo dokázat.

Nejedná se o žádnou závratnou sumu, ale tento případ ukazuje na to, že ani dobrý výběr zaměstnanců není zárukou, že se nic neztratí. Vždy je důležitá kontrola a další činnosti, které jsou podrobněji rozebrány v praktické části práce.

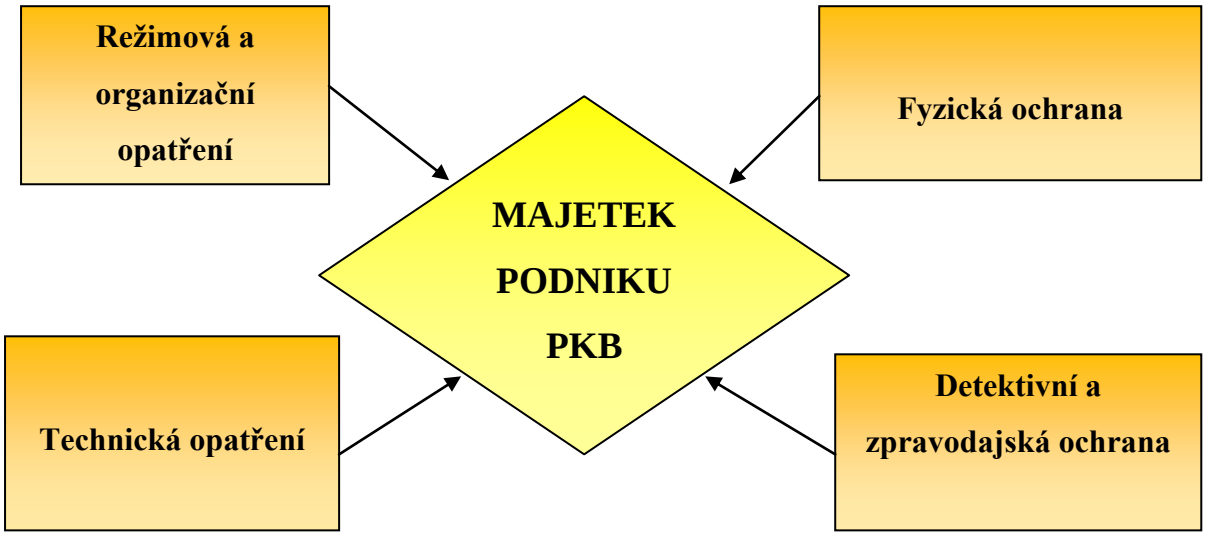
7.1.7 Krádeže materiálu vedoucím pracovníkem

Majitel bezpečnostní agentury se mi svěřil s jediným závažnějším případem, se kterým se ve své praxi setkal.

Zaměstnanec pracoval v agentuře několik let, žil sám, byl rozvedený a bezdětný. Měl důvěru vedení a postupem času se stal velitelem objektu. Nejspíš se ale dostal do situace, kdy si musel tzv. přilepšit. Postupem času se začaly ztrácet hliníkové předměty. Majitel s ním tuto situaci konzultoval a společně připravovali různé pasti na chycení zloděje. Krádeže ale pokračovaly a majitel se rozhodl, zkusit pátrat na vlastní pěst. V noci zůstal v objektu a zanedlouho chytil zloděje při činu. Krádeže páchal velitel objektu a majitel s ním rozvázal pracovní poměr dohodou.

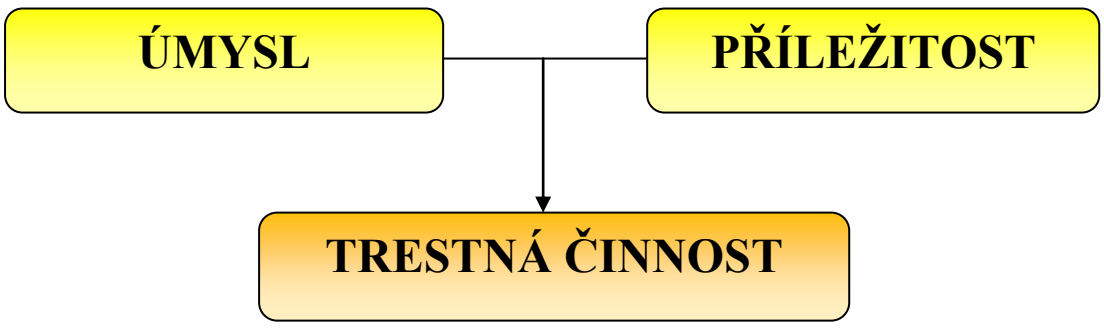
8 NÁVRHY AKTIVNÍCH OPATŘENÍ

Majetek podniku, ať už se jedná o know-how, finanční hotovost či materiál, by měl být chráněn kombinací opatření, které jsem uvedl na obrázku níže. Dodržování těchto opatření by mělo být kontrolováno, stejně jako by měli být kontrolováni sami zaměstnanci. Zaměstnance je ale třeba nejprve správně vybrat, aby už to mohlo zamezit případné kriminalitě. Všechna tato opatření se pokusím přiblížit v této závěrečné kapitole.

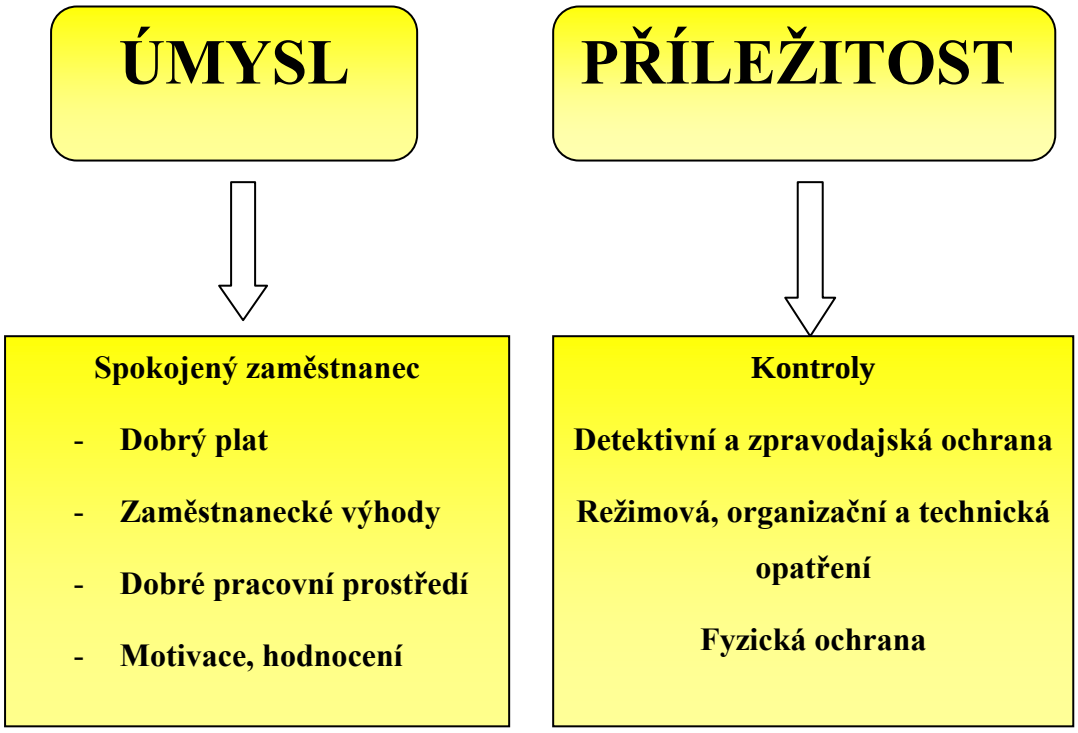


Obr. 13 *Ochrana majetku podniku*

Zaměstnanec potřebuje mít ke krádeži úmysl a příležitost. Když má úmysl a nemá příležitost, ke krádeži nedojde, to samé platí i obráceně. Proto v této části práce navrhuju opatření, která můžou zabránit jak úmyslu, tak příležitosti.



Obr. 14 *Podmínky spáchání trestné činnosti*



Obr. 15 *Jak zabránit trestným činům*

Aby neměl zaměstnanec úmysl krást, je důležité ho správně motivovat. Nejlepší motivací je bezesporu dobrý plat, ale zaměstnanec se musí také v práci cítit dobře, aby si jí více vážil, proto i pracovní prostředí a kolektiv má velký vliv.

Omezit příležitost ke krádeži lze různými technickými a režimovými opatřeními, pravidelnou i namátkovou kontrolou, případně za pomoci detektivní či zpravodajské ochrany a dalších vhodných opatření.

8.1 Výběr a přijetí zaměstnanců

V rámci personalistiky v podnicích PKB je vhodné uplatnit všechny metody, které jsem uváděl v kapitole o personální politice podniků, ale zde v praktické části uvádím podrobněji jen ty nejdůležitější, které mají podle mého názoru největší vliv na obranu před trestnou činnost zaměstnanců.

Prvním krokem v rámci prevence latentní kriminality je samotný výběr zaměstnanců. Pokud je potencionální uchazeč dobře prověřen, podstatně se sníží riziko, které pro podnik znamená.

8.1.1 Metody získávání pracovníků

Metod k získávání pracovníků je celá řada, uvádím zde ty nejčastější, které bezpečnostní agentury využívají:

- uchazeči se nabízejí sami;
- doporučení současného pracovníka organizace;
- přímé oslovení vyhlédnutého jedince;
- vývěsky;
- inzerce ve sdělovacích prostředcích;
- spolupráce s úřady práce;
- využívání služeb komerčních zprostředkovatelen;
- využívání počítačových sítí (internetu).

Z mého průzkumu vyplynulo, že úřadů práce sice agentury využívají, ale spokojeni s ním rozhodně nejsou. Důvodem je to, že zahlcují personální oddělení nevhodnými uchazeči a to takovými, kteří o práci vůbec nemají zájem a jde jim jen o razítko nebo dokonce dříve trestanými, kteří už vůbec nemají v bezpečnostní agentuře co dělat. Dalším způsobem je, že se uchazeči nabídnou sami, tady hrozí riziko, že se uchazeč chce dostat do agentury, aby mohl krást. To se zřejmě stalo i v případu ukradené půlmiliardy, proto je nutné tyto uchazeče dostatečně prověřit, to ale ostatně platí u všech náborových metod. Nejlepší způsob je dle mého názoru, pokud kandidáta doporučí některý ze současných zaměstnanců, kterému vedení důvěřuje nebo si určitého jedince podnik sám vyhlédne a přímo ho osloví.

Oslovených bezpečnostních agentur jsem se ptal zejména na jejich zkušenosti s úřady práce, ale pro představu, jaké metody využívají některé z bezpečnostních agentur, zde uvádím průzkum, který prováděla v bakalářské práci Daniela Dolská :

	ABAS IPS Management s.r.o.	ATA bezpečnostní agentura s.r.o.	Dora Security a.s.	G4S Security Services (CZ), a.s.	Scylla s.r.o.	WAKKENHAT SECURITY a.s.	WESTPOINT, a.s.	P (pravidelně) v %	V (výjimečně) v %	N (ne) v %
ZDROJE NÁBORU										
www.jobs.cz	V	N	N	N	N	P	N	14,3	14,3	71,4
www.prace.cz	V	N	P	N	N	P	N	28,6	14,3	57,2
www.sprace.cz	N	N	N	N	N	V	N	0	14,3	85,8
www.jobpilot.cz	N	N	N	N	N	N	N	0	0	100
www.cvonline.cz	N	N	N	N	N	N	N	0	0	100
Jiný	N	N	N	P	N	N	N	14,3	0	85,8
Celonárodní tisk										
• **deníky**	P	N	P	P	N	P	V	57,2	14,3	28,6
• **časopisy**	N	N	N	N	N	N	N	0	0	100
• **inzertní noviny**	P	V	P	V	N	P	V	42,8	42,9	14,3
• **bezplatné noviny**	P	N	P	V	N	P	V	42,9	28,6	28,6
Regionální tisk										
• **obecní noviny – zpravodaje**	P	P	P	V	N	V	N	42,9	28,6	28,6
• **inzertní noviny**	P	P	P	V	N	V	N	42,9	28,6	28,6
• **bezplatné noviny**	P	N	P	V	N	P	N	42,9	14,3	42,9
Rozhlas	N	N	N	N	N	N	N	0	0	100
Televize	N	N	N	N	N	N	N	0	0	100
Personální agentury a agentury práce	V	N	P	V	N	V	P	28,6	42,9	28,6
Úřady práce	P	V	P	P	N	P	V	57,2	28,6	14,3
Burzy práce pořádané úřady práce	N	N	P	V	N	N	N	14,3	14,3	71,5

Tab. 2 *Zdroje náboru některých agentur* [8]

Velkým problémem v současnosti je vysoká fluktuace zaměstnanců. Uvádí se, že nejvyšší je v místech s minimální nezaměstnaností, ale ačkoliv je u nás nezaměstnanost poměrně vysoká, tento problém trápí většinu bezpečnostních agentur, jak jsem zjistil v průzkumech. Zejména na pozici strážný je to obrovský problém, stává se, že si nový zaměstnanec již v průběhu zkušební doby najde jiné zaměstnání. Výjimkou nejsou ani případy, kdy nastupuje jako zaměstnanec firmy, jejíž objekt zpočátku střežil.

Důvody této vysoké fluktuace jsou zejména v nízkém mzdovém ohodnocení a zřejmě také v nízké společenské atraktivnosti práce, minimu zaměstnaneckých výhod a nárocích na fyzickou zdatnost, protože strážní pracují převážně ve stoje.

Poznatky získané v bezpečnostních agenturách ukazují, že nejlepší zkušenosti mají zaměstnavatelé s bývalými pracovníky Policie ČR, Vězeňské služby a Armády ČR. Důvodem je hlavně pokračování v podobné profesi a také podstatně snížené nároky na výši mzdy díky pobírání výsluhového příspěvku. Jedná se o příspěvek za službu v ozbrojených sborech, který je přiznáván dle příslušných zákonů po odsloužení určitého počtu let.

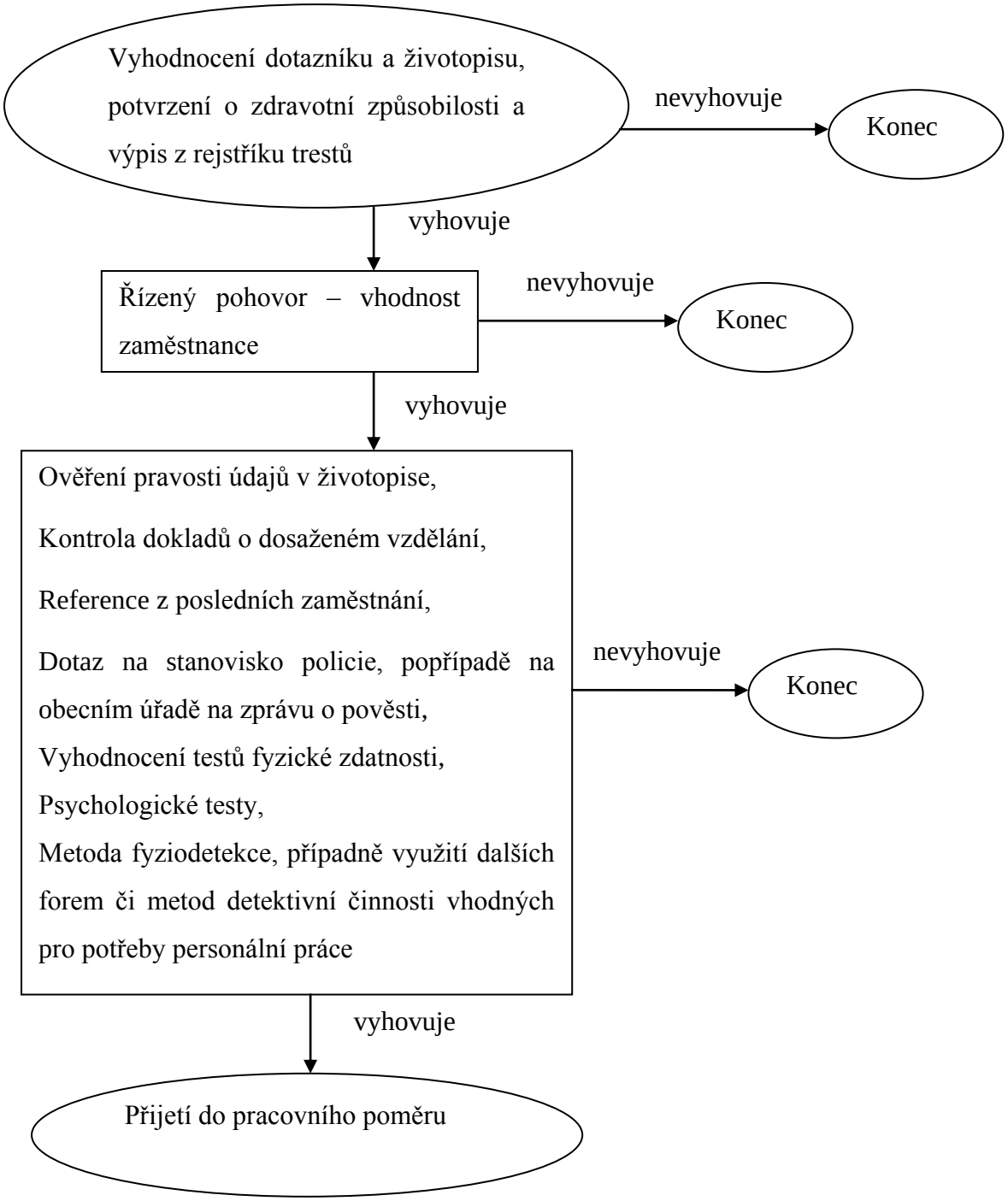
8.1.2 Péče o zaměstnance a zaměstnanecké výhody

Spokojený zaměstnanec většinou nemá důvod krást a proto je v zájmu majitelů agentur, aby se u něj zaměstnanci cítili dobře. Nejlepší způsob jak toho docílit je správná motivace, péče o zaměstnance, případně poskytování různých zaměstnaneckých výhod.

Problematikou péče o zaměstnance se zabývá část X. zákoníku práce (hlava I. – IV.). Mezi povinnosti zaměstnavatelů patří povinnost vytvářet pracovní podmínky, které umožňují bezpečný výkon práce, odstraňovat rizikové a namáhavé práce a zřizovat, udržovat a zlepšovat zařízení pro zaměstnance, včetně vzhledu a úpravy pracoviště.(Zákon č. 262/2006 Sb.) Co se týká zaměstnaneckých výhod, jsou velmi dobrý prostředek motivace. V bezpečnostních agenturách se ale stejně jako všude jinde šetří a zaměstnaneckých výhod je stále méně.

8.1.3 Schéma ideálního náborového procesu

Toto schéma jsem navrhnul pro „dokonalý“ výběr zaměstnance, ale ve skutečnosti to tak bohužel nefunguje a zaměstnanci na nízkých pozicích jsou obvykle kontrolováni jen na základní požadavky dané ze zákona. Pokud se týká výběru vedoucích pracovníků, tak u těchto je nejlépe vybírat tak, že vybíráte člověka z vlastních řad, který si problematikou prošel „od spoda“ a zná ji. Zaměstnavatel zná jeho, jeho přístup k práci a jeho rezervy. Tím pádem je tento člověk respektován svými podřízenými, jelikož práci zná, nedá se jen tak zmanipulovat planými argumenty. Dále je schopen dokonale vysvětlit, co, jak a proč má být a fungovat. Hraje zde roli také minulost člověka, v jakém oboru pracoval a jaké znalosti má.



Obr. 16 *Návrh ideálního náborového procesu*

8.2 Kontrola zaměstnanců

Kontrola zaměstnanců je nutností, bez které by byl každý podnik brzy rozkraden. V bezpečnostních agenturách se tato kontrola odehrává (nebo by se měla odehrávat) ve třech základních větvích:

1. Větev- **Oblastní ředitel**

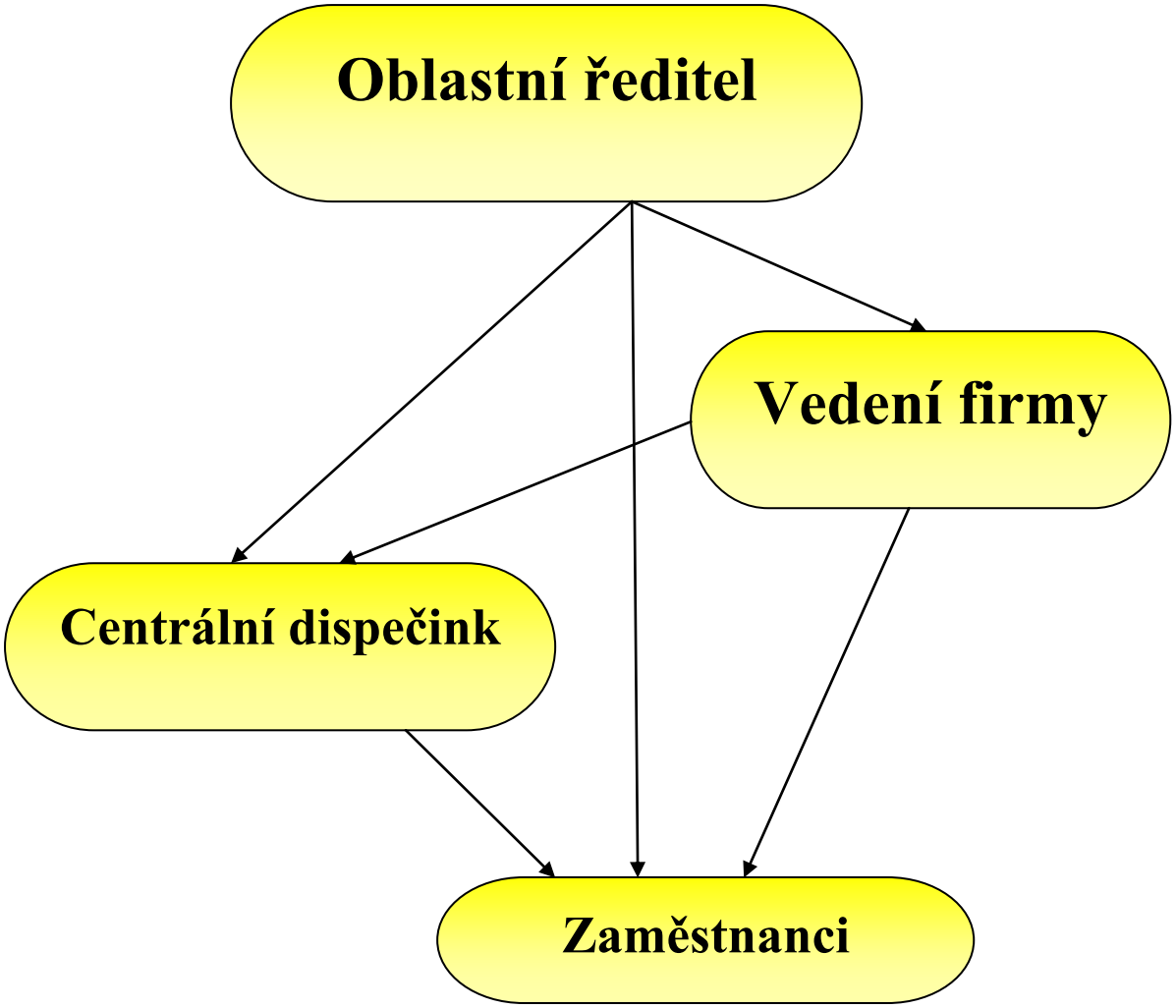
   Oblastní ředitel je z mého pohledu největší autorita pro zaměstnance. Má na starosti kontrolní řídící práce, plánování, organizování, nasazování zaměstnanců do zaměstnání a další činnosti. Může provádět kontroly všech zaměstnanců, jak vedoucích pracovníku a dispečinku, tak řadových zaměstnanců. A jak vyplynulo z průzkumů, velmi se vyplatí, pokud toho využívá. Zejména namátkové kontroly často odhalí důležité skutečnosti.

2. Větev- **Vedení firmy**

   Vedení firmy, nebo vedoucí pracovníci, mají na starost kontrolu průběhu výkonu služby na pracovišti. Například ředitel pultu centralizované ochrany kontroluje pracovníky na dispečinku a sám je kontrolován nadřízeným- oblastním ředitelem.

3. Větev- **Centrální dispečink**

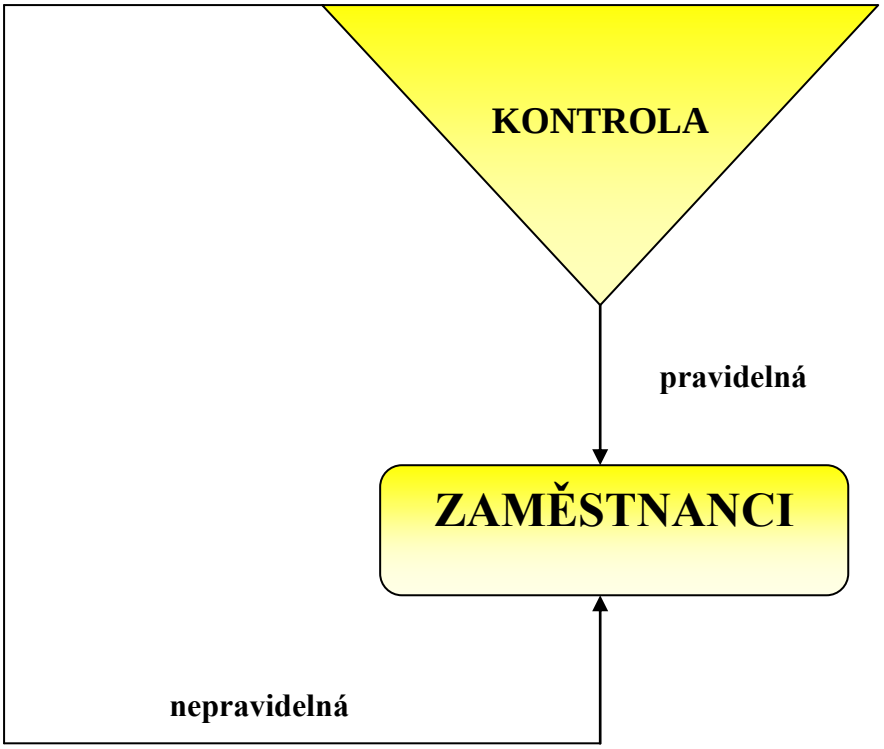
   Centrální dispečink je důležitý, protože kontroluje nástup, průběh a ukončení služby. Zaměstnanci nastupující do zaměstnání se musí na dispečinku ohlásit, dále je kontrolován průběh zaměstnání, například za pomoci elektronické kontroly obchůzek strážných a ukončení služby je opět ohlášeno na dispečink. Zaměstnanci dispečinku také mohou provádět namátkové kontroly plnění pracovních povinností.



Obr. 17 *Kontrola zaměstnanců*

O pravidelných kontrolách, které probíhají v určitých časových úsecích (např. týden, měsíc) zaměstnanci vědí a tak se na ně můžou předem připravit. Může se jednat o kontroly dodržování pracovních povinností, ale i kontroly různých záznamů např. do knihy zbraní a střeliva, kontrola ujetých kilometrů a další.

Namátková kontrola má veliký význam, zaměstnanci nikdy přesně neví, kdy přijde, ale měli by si být jistí, že přijde určitě. To jim velmi často zabrání, dopustit se nějakého trestného činu, případně tento čin může namátková kontrola odhalit. Zkušenosti ředitelů bezpečnostních agentur, které jsem vyslechnul, to potvrzují.



Obr. 18 *Druhy kontroly*

8.2.1 Jak poznat nepoctivého zaměstnance?

V rámci kontrol je také třeba si všímat určitých příznaků, které můžou svědčit o tom, že je něco v nepořádku a zaměstnanci by měla být věnována ještě větší pozornost. Mezi hlavní příznaky patří:

- Zaměstnanec si žije nad své majetkové poměry
- V jeho okolí nebo v souvislosti s jeho osobou se vyskytují podezřelé okolnosti
- Porušuje nebo obchází bezpečnostní procedury
- Nedodržuje přijaté standardizované postupy
- Brání se kontrolám a dozoru
- Má některé negativní charakterové vlastnosti (zklamanost, závistivost, nudí se nebo je panovačný a samolibý, ješitný apod.)

Velmi dobrým motivem k páchání, který vyplynul z mého dotazování bezpečnostních agentur, je to, že na zaměstnance byla uvalena exekuce. O tomto se zaměstnavatel vždy dozví a musí zaměstnanci věnovat zvýšenou pozornost. Dalším důvodem k zvýšení pozornosti je sklon zaměstnance k alkoholu, hraní automatů apod. Takový zaměstnanec by neměl být vůbec do firmy přijat. Ale někdy se tyto sklony vyvinou až po přijetí, proto je nutné pořád si všímat. Mezi další příznaky, které lze na nepoctivém zaměstnanci pozorovat patří:

- Přichází na pracoviště příliš brzy
- Zůstává na pracovišti příliš dlouho
- Obléká se příliš extravagantně
- Varuje vždy ostatní, když se blíží kontrola
- Dokumenty, se kterými pracuje, mají známky úprav.
- Záznamy jsou prováděny nedbale
- Odmítá jakoukoliv pomoc či asistenci
- Odmítá dlouhodobě vzít si dovolenou
- Mění si dovolenkové rozvrhy
- Zdá se, že má osobní problémy
- Nedodržuje stanovené postupy
- Stanovuje si vlastní pravidla

Pokud zaměstnanec vykazuje takovéto znaky, neznamená to, že páchá nějaké trestné činy, ale existuje-li podezření řídícího pracovníka, že se tak děje, jeho pocity jsou většinou odůvodněné.

8.2.2 Mechanismus páchání

Mechanismus páchání, který je stejný prakticky ve všech případech má tyto body:

1. Pachatelé nejprve hledají slabinu v systému
2. Nalezení slabiny ve zkoumaném systému

3. Testování reakce okolí a upevňování pozice pachatele
4. Následné a především dlouhodobé využívání daného poznání

Tyto body dobře popisují způsob, jakým dochází k páchání trestné činnosti. Nejlepší obranou pochopitelně je, pokud systém žádné slabiny nemá, toho je ale v praxi asi nemožné docílit. Po důkladném výběru zaměstnanců a jejich přijetí do pracovního poměru, musí následovat kontroly jejich činnosti, pravidelné i namátkové.

8.2.3 Zdroje nepoctivosti zaměstnanců

Důvodů, proč páchají zaměstnanci trestnou činnost, je celá řada a liší se to případ od případu. Nejčastější zdroje nepoctivosti zaměstnanců jsou:

- Rozpad společenských hodnot
- Klesající reálný příjem
- Zadlužení
- Nezaměstnanost v rodině
- Alkoholismu, drogy, gamblerství
- Málo kontroly, nepřehledné delegování
- Konflikty ve vztazích na pracovišti
- Nenávist vůči firmě, pocit křivdy
- Nespokojenost, frustrace
- Hamižnost
- Osobní kariéra a snaha se prosadit
- Nepřiměřené nároky a životní očekávání
- Psychické problémy (zvláště u žen, muži málo)
- Kriminální dispozice

8.3 Prevence latentní kriminality

Prevence latentní kriminality v podnicích komerční bezpečnosti spočívá také v důsledné kontrole a represi. Jak už bylo napsáno výše, je velmi důležité prověřování vlastních pracovníků a maximální zjištění minulosti přijímaného pracovníka, vytvoření jakéhosi profilu osobnosti. Ztotožňuji se s názorem Jana a Kamily Muzikových, kteří ve své práci navrhují maximální kontrolu pracovníků uskutečňovat [15]:

a) Demonstrativním způsobem, aby pracovníci měli dojem, že provádět jakoukoliv kriminalitu je takřka nemožné, nebo s vysokým rizikem prozrazení. Vhodné jsou též viditelné kamerové systémy a další technická opatření navržená níže, nepravidelné kontroly nadřízeným pracovníkem, nepravidelné střídání služeb, neustálé změny v sestavách pracovníků zabraňující vzájemným dohodám a organizování trestné činnosti apod.

b) Skrytým způsobem, který zajistí odhalení kriminality

c) Každý pracovník na určitém místě (pozici) má mít pouze omezené množství informací, které jsou nezbytně nutné k výkonu jeho pracovní činnosti.

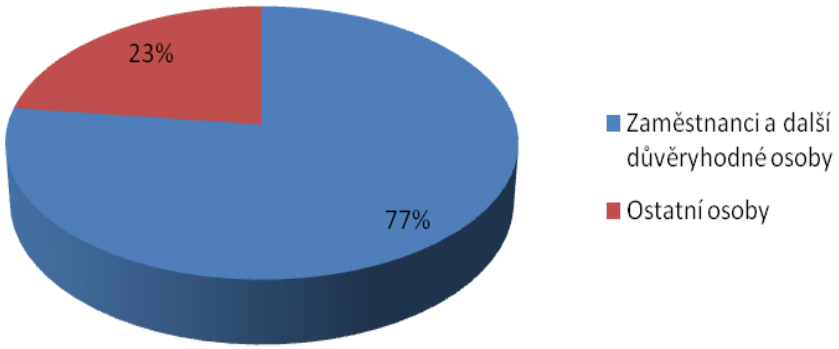
d) Elektronické hrozbě trestné činnosti lze čelit separátně zvoleným pracovníkem IT, kterého je dobré oddělit od ostatních pracovníků. Vzájemná komunikace těchto pracovníků může probíhat prostřednictvím nadřízené, případně kontrolní osoby. Takováto osoba by měla být obzvláště prověřena, neboť vzhledem ke správě podnikové počítačové sítě, má přístup k velkému množství informací PKB. Přesto by tajné informace, jako jsou např. trasy a časy převozů peněz, nebo fyzických doprovodů, měly být i těmto pracovníkům znepřístupněny. I zde platí pravidlo, čím méně informací tím lépe.

e) Dalším způsobem snížení rizika latentní trestné činnosti je správná motivace pracovníků.

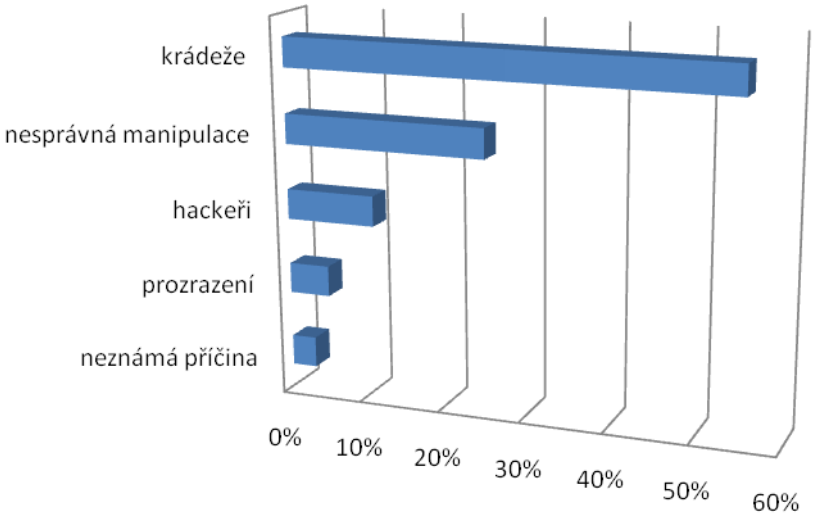
Tak jako na finančním trhu se diverzifikací investic snižují rizika finančních ztrát tím, že se investuje do více akcií po menších částkách, namísto velké investice do jedněch akcií, tak i v PKB je dobré tzv. diverzifikovat informace. Kde se diverzifikací (rozdělením) určitých informací mezi více pracovníků snižuje riziko trestné činnosti pracovníků PKB.

8.4 Ochrana know-how

Ochrana know-how je pro podnik velmi důležitá, mnohdy může mít zneužití informací pro podnik horší následky než třeba krádež finanční hotovosti. Průzkumy jasně ukazují, že největší riziko zneužití firemního know-how představují vlastní zaměstnanci.



Graf 7 *Kdo zcizuje informace (Zdroj McAfee)*



Graf 8 *Ztráty dat (Zdroj Symantec)*

Ochranu know-how v podniku je třeba zabezpečit kombinací ochrany :

- režimové
- technické

- fyzické
- detektivní a zpravodajské

8.4.1 Režimová ochrana know-how

Při stanovení režimové ochrany je nejdůležitější:

- ✓ Jednoznačně určit, které informace jsou důvěrné a tajné.
- ✓ Určit prostory, kde budou informace uloženy.
- ✓ Určit dobu, po kterou budou informace chráněny
- ✓ Určit osoby, které můžou s informacemi manipulovat a určit čas, po který jim to bude umožněno.
- ✓ Pokud dojde ke změně personálu, je nutno okamžitě aktualizovat seznamy těchto osob.
- ✓ Stanovení kontroly režimových opatření – jakým způsobem se budou provádět, kdo je bude provádět a kdo ponese za kontroly odpovědnost.

8.4.2 Technická ochrana know-how

Technická ochrana nabízí nejširší možnosti ochrany know-how. Je možno ji realizovat systémy:

- IAS (intruder alarm systém -Poplachový zabezpečovací systém)
- HAS (hold-up alarm systém- Tísňový poplachový systém)
- EPS (elektrická požární signalizace)
- CCTV (systémy průmyslové televize)
- MZS (Mechanické zábranné systémy)
- Přístupové systémy atd.

Nejlepší ochrana se docílí kombinací těchto systémů (např. I&HAS+CCTV).

8.4.2.1 Ochrana z hlediska přístupu

Pokud je know-how uloženo ve formě dat a informací v počítači, je možno zamezit neoprávněnému přístupu dvěma způsoby:

- Zamezení uživateli v tom, aby mohl citlivá data jakkoli zobrazit nebo dokonce měnit
- Fyzická bezpečnost – ochrana před krádeží apod.

Obzvlášť citlivé údaje je třeba také šifrovat. Pokud by se nepovolaná osoba k takovým údajům dostala, potřebovala by znát patřičný klíč (heslo) k otevření. K informacím může narušitel přijít buď:

- Zvenčí (porucha systému, nedostatečně zabezpečen přístup k informacím z okolní sítě)
- Zevnitř (zneužití hesla, špatné uspořádání přístupových práv)

8.4.2.2 Identifikace, autentizace, autorizace

Identifikace - zjištění uživatelovy identity např. zadáním hesla, či kódu.
Autentizace - ověření, zda je uživatel osobou za kterou se vydává.
Autorizace - zjištění, zda k provedení činnosti, služby má uživatel právo.

K ověření přístupu lze použít tyto metody :

- Uživatel si něco pamatuje (prokazuje se pomocí hesla, číselného kódu)
- Uživatel něco vlastní (čipová karta, klíč, apod.)
- Biometrie (otisk prstu, struktura oční sítnice apod.)

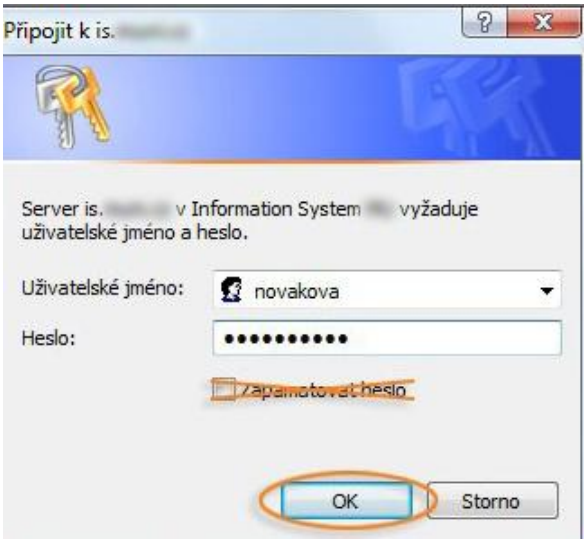
Zvýšení bezpečnosti představuje kombinace těchto metod.

8.4.2.3 Hesla

Tento způsob je nejstarší a stále také nejpoužívanější. Uživatel pro přístup musí zadat uživatelské jméno a heslo. Při zadávání hesel by měl být vždy uživatel mimo zorné pole ostatních osob a krýt klávesnici například vlastním tělem, aby nemohl nikdo spatřit, jaké klávesy stlačil. Důležité je také nezadat omylem heslo do kolonky uživatelské jméno, protože to může být zaprotokolováno do souborů. Z vlastní zkušenosti vím, že se stále

používají velmi jednoduchá hesla složená například z jednoduché posloupnosti čísel nebo názvu pracoviště apod. Dobrá hesla by měla splňovat podmínky [10] :

- Malá i velká písmena
- Nejlépe 7 až 10 znaků
- Použití číslic a dalších speciálních znaků např. */§
- Heslo by nemělo tvořit žádné známé slovo
- Heslo by mělo být zapamatovatelné



Obr. 19 *Zadávání hesla*

8.4.2.4 Čipové karty

Čipové karty jsou poměrně hojně využívány, skládají se s integrovaného obvodu a procesoru. Většinou bývají zality plastovým materiálem. Identifikace je jednoduchá, protože je vše uloženo na jednom čipu. Můžou být použity i při šifrování souborů, kdy mohou sloužit jako klíč pro odšifrování.

Čipové karty lze dělit podle způsobu snímání na:

- Kontaktní – pro svou činnost musí být vloženy do čtecího zařízení, protože obsahují kontaktní plochy
- Bezkontaktní – není vyžadován fyzický kontakt, stačí přiblížit k čtecímu zařízení. K přenosu dat a napájení je využívána indukční smyčka.

Existuje několik standardů definujících rozměry a funkčnost čipových karet. Fyzické charakteristiky karet definuje norma ISO 7810, jejich komunikaci s okolím normy ISO/IEC 7816 (kontaktní karty) a ISO/IEC 10536 (bezkontaktní karty).

8.4.2.5 Biometrie

Biometrie je automatická metoda autentizace založená na rozpoznávání jedinečných biologických charakteristik subjektu - živé osoby. Metoda vychází z přesvědčení, že některé biologické charakteristiky (morfologické, fyziologické) jsou pro každého živého člověka jedinečné a neměnitelné. Mezi biometrické metody patří:

- Otisk prstu
- Vzorek oční duhovky nebo sítnice
- Geometrie obličeje
- Geometrie ruky

Snímačů otisků prstů existuje více druhů, které se liší principem snímání. To může být elektrické, optické, ultrazvukové, tepelné nebo tlakové. Nejstarším typem byly snímače křemíkové, které využívaly změny elektrické kapacity mezi dvěma body snímače, v závislosti na tom, zda je mezi nimi mezera nebo papilární čára. Dnes jsou nejrozšířenější optické snímače. Využívají změny odrazu světla od části prstu. Spolehlivost je závislá na čistotě snímací plochy.

8.4.2.6 Zálohování informací a dat

Zálohování dat může sloužit především jako záchrana, když se zhroutí systém. Také může k užitku, pokud jsou data z počítače omylem nebo úmyslně smazána. Systém je pomocí zálohy možno vrátit do původního stavu. Existují dva druhy záloh:

Úplná – zálohují se všechny soubory

Inkrementální – zálohují se pouze soubory změněné od posledního zálohování

8.4.2.7 Mechanické zabezpečení informací

Vhodným opatřením k ochraně informací je mít počítač dobře zabezpečený i po mechanické stránce. Počítače lze zabudovat do speciálních uzamykatelných skříní, aby nebylo možno s počítačem manipulovat. Mechanicky jdou také zabezpečit vstupy do

počítače, aby nebylo možno informace stáhnout na přenosný disk. Notebooky můžou být zamčeny pomocí ocelového lanka k nábytku.

Zálohovaná data je vhodné uchovávat na jiném místě, aby například při požáru v místnosti nebyly zničeny oba zdroje dat. K zabezpečení záloh se používají speciální druhy pancéřových sejfů, které dokážou vzdorovat vysokým teplotám. V podmínkách bezpečnostních agentur, ale velmi dobře poslouží firemní trezor.

8.4.3 Konkurenční doložka jako ochrana know-how

Konkurenční doložka znamená písemný závazek zaměstnance vůči zaměstnavateli, že po skončení zaměstnání nebude vykonávat výdělečnou činnost (pracovní poměr, podnikání), která by se shodovala s předmětem činnosti zaměstnavatele, případně mu byla konkurencí. Doba trvání platnosti konkurenční doložky je nejdéle jeden rok po skončení pracovního poměru**.** Za každý měsíc trvání konkurenční doložky obdrží bývalý zaměstnanec zpětně, při dodržení daných podmínek, částku stanovenou minimálně jako průměrný měsíční plat zaměstnance v době trvání pracovního poměru. Konkurenční doložka je konkurenční ujednání v pracovní smlouvě, které se vždy domlouvá individuálně, a to většinou v oborech, kde je potřeba chránit firemní know-how. Toto ujednání musí být v souladu s Ústavou České republiky a s Listinou základních práv a svobod a vzájemná práva i povinnosti účastníků pracovní smlouvy musí být ve vyváženém poměru.

Konkurenční doložka se ujednává k takovým činnostem, které jsou shodné s předmětem podnikání zaměstnavatele nebo v případě soutěžní povahy této činnosti. Většinou je tedy konkurenční ujednání součástí pracovní smlouvy v oboru, kde je velká konkurence**.** Zaměstnanci je znemožněn odchod ke konkurenci, případně zahájení vlastního podnikání v oboru, protože by to mohlo bývalého zaměstnavatele silně poškodit na trhu v daném oboru.

Pokud bývalý zaměstnanec, třeba i jednorázově, dohodu poruší, nemá právo na vyplacení peněžité částky, ale je vůči němu uplatňována smluvní pokuta uvedená v konkurenční doložce. Po zaplacení této pokuty závazek zaměstnance zaniká. Dohoda o konkurenční doložce může zaniknout ze strany zaměstnavatele jen v době, kdy zaměstnanci trvá pracovní poměr. Pokud zaměstnanci není vyplacena příslušná částka za

uplynulý měsíc do 15 dnů po splatnosti, může zaměstnanec dohodu vypovědět. Obě dvě formy zániku dohody musí být učiněny písemně.

8.4.4 Vyhodnocení

Pro ochranu know-how je tedy nejdůležitější stanovit režimovou ochranu, dále mít fungující technická opatření, nejlépe jejich kombinace (např. I&HAS+CCTV apod.). Informace, které mají být chráněny, musí být zabezpečeny minimálně heslem, které musí být složené z písmen, čísel a nejlépe také speciálních znaků, být aspoň 7-10 znaků dlouhé a při jejich zadávání musí uživatel dávat pozor, zda mu někdo nekouká přes rameno. Informace mohou být také zabezpečeny čipovou kartou nebo za pomoci biometrie. Nejúčinnější je kombinace těchto způsobů. Ochrana know-how za pomoci fyzické ochrany je řešena níže. Dalším možným způsobem, jak chránit informace, je využití forem detektivní činnosti jako je detektivní ochrana majetku a detektivní zpravodajství. V rámci ochrany před vynesením informací je také možnost zpracovat tzv. konkurenční doložku, ale myslím, že v našem prostředí se jí nevyužije a daleko lepší je pamatovat na tuto problematiku už v pracovní smlouvě a upozornit zaměstnance, že porušení mlčenlivosti může mít právní dopady. Všechny zákazy a nedovolené způsoby zacházení s know-how by měly být uvedeny v pracovním řádu a vyvěšeny na viditelném místě.

Mezi nejčastější chyby v zabezpečení počítačů tedy bezesporu patří:

- Nedostatečná ochrana přístupových hesel
- Podcenění fyzické ochrany PC
- Nedůslednost v dodržování bezpečnostních zásad IT
- Jednoduchost hesla (jméno, příjmení, datum narození, bydliště, název pracoviště)
- Používání stejného hesla pro různé aplikace
- Nedostatečná obměna hesel
- Sdělení, resp. Vyzrazení svých citlivých přístupových informací a hesel nepovolané osobě

1	Opomenutí a chyby v bezpečnostním zajištění PC
2	Nepoctiví zaměstnanci
3	Rozladění (frustrovaní) zaměstnanci
4	Oheň
5	Voda
6	Vnější ohrožení

Tab. 3 *Největší bezpečnostní rizika*

8.5 Fyzická ochrana

Fyzická ochrana je stále velmi významnou formou ochrany osob a majetku. V případě ochrany know-how se může jednat o fyzickou ochranu:

- Míst, kde je know-how uloženo a skladováno.
- Prostor, v nichž se s know-how pracuje.
- Vnitřních prostor, kde se know-how vyskytuje.
- Společnosti jako celku.

Fyzická ochrana je v případě bezpečnostních agentur trochu nezvyklá. Asi by nevypadalo dobře, kdyby na chodbě u kanceláří celý den hlídkoval strážný. Proto je výhodným řešením využit například firemního dispečinku, kde bývá obvykle nepřetržitý provoz, pověřená osoba může sledovat dění v podniku přímo z tohoto místa. Funkci jakési fyzické ochrany může částečně plnit i výjezdová skupina, pokud je v pohotovosti na dispečinku. Výhodné a v některých případech nezbytné je využití kontrolně propustkové služby.

8.5.1 Kontrolně propustková služba

Tuto formu ochrany majetku a osob je vhodné použít i v našem případě při ochraně podniku. U větších agentur by tuto práci měl vykonávat pracovník jako hlavní náplň svojí práce. U menších agentur můžou úkoly kontrolně propustkové služby plnit například pracovníci dispečinku, kde je nepřetržitý provoz. Takový pracovník pak zabezpečuje ostrahu a režim vstupu do objektu. Mezi jeho hlavní úkoly patří:

- Zabránění vstupu a vjezdu vozidel bez platného oprávnění pro vstup nebo vjezd do objektu, neoprávněnému vnášení předmětů, které mohou ohrozit bezpečnost osob a majetku a porušení režimu objektu.
- Kontroluje přicházející a odcházející osoby a vozidla.
- Poskytuje v potřebném rozsahu informace návštěvníkům objektu, zajišťuje stanovený režim návštěv.
- Vede stanoveným způsobem knihu příchodů a odchodů.
- Odemyká a uzamyká ve stanovenou dobu vchody do objektu.
- Vydává určené klíče od jednotlivých prostor oprávněným osobám, k čemuž vede příslušnou dokumentaci.
- Plní doprovod návštěv do objektu, je-li takto stanoven režim návštěv.
- Plní další uložené specifické úkoly.

8.6 Detektivní a zpravodajská ochrana

Detektivní a zpravodajskou ochranu je možno využívat nejen pro potřeby personální práce, ale také k ochraně informační bezpečnosti. Protože už jsem tyto formy detektivní práce uváděl v jiné kapitole, podrobněji je zde nerozbírám.

8.7 Režimová opatření

Režim je administrativní organizační a věcné uspořádání vztahů mezi lidmi, jejich činnostmi a vlastními procesy v oblasti výkonu i řízení za účelem sladění všech prvků a s cílem dosáhnout harmonického stavu v dané společnosti. [13]

Režimová opatření se týkají:

- Činnosti pracovníků uvnitř podniku (vlastních zaměstnanců),
- Pohybu a chování osob přicházejících zvenčí, včetně oběhů dokladů a informací uvnitř podniku (administrativní nebo spisový pořádek),
- Výstupu informací, dat, dokumentů vně podniku.

8.7.1 Kniha výdeje a příjmu zbraní a střeliva

Režimových opatření, která svým způsobem zamezují latentní kriminalitě, je celá řada. Například v každé agentuře funguje Kniha výdeje a příjmu zbraní a střeliva, do které se zaznamenávají veškeré pohyby zbraní ve firmě. Pokaždé když se zbraň či střelivo bere z trezoru, musí se provést záznam. Tuto povinnost ukládá zákon a kontroly provádí policie. Dnes již nemůže mít zaměstnanec svou vlastní zbraň pro použití v práci. Všechny musí patřit firmě, která také prostřednictvím knihy výdeje a příjmu zbraní provádí kontrolu.

Poř. čís.	Vydáno									Vráceno		
	Datum	Zbraně					Střelivo počet	Osobní data fyz. os., která zbraň a střelivo převzala, č. a skup. ZP	Potvrz. příjmu podpisem	počet		Datum a potvrz. příjmu podpisem
		Druh	Značka	Vzor	Ráže	Výrobní číslo				zbraň	střelivo	

Obr. 20 *Položky vyplňované v knize výdeje a příjmu zbraní a střeliva*

8.7.2 Klíčový režim

Agentury, které nejsou vybaveny přístupovými systémy, mají zaveden klíčový režim. Uložiště klíčů bývá obvykle na vhodném místě, nejlépe na centrálním dispečinku s nepřetržitým provozem. Obsluha je seznámena s přístupovými právy do jednotlivých místností a proto ví, komu můžu klíče vydat. O výdejích klíčů by měl být pro pozdější kontrolu uveden záznam do knihy evidence klíčů. Toto ale není nařízeno žádným zákonem, proto je na firmě, zda to svým zaměstnancům nařídí. Schránka na klíče by neměla nikdy zůstávat nezamknutá a bez dozoru.

Obr. 21 *Schránka na klíče [28]*

8.7.3 Používání služebních telefonů

Pro zaměstnavatele by mělo být nutností, aby byl způsob používání služebního telefonu (i automobilu) pečlivě upraven před jejich fyzickým předáním zaměstnanci v pracovní smlouvě, vhodné je i uzavření dohody o odpovědnosti za ztrátu svěřených předmětů. Stejně tak je vhodné, aby byly v samotné pracovní smlouvě striktně definovány následky porušení pravidel používání uvedených pracovních prostředků. [23]

Pokud zaměstnanec nemá o používání služebních telefonů v pracovní smlouvě žádnou zmínku, může se stát, že zaměstnavatel po čase zjistí velký počet soukromých hovorů, které z telefonu proběhly, ale pokud by je chtěl po zaměstnanci proplatit, bude to prokazovat jen velmi obtížně. Je proto nutné mít nějakou interní směrnici, kde by bylo upraveno, jak mohou zaměstnanci nakládat s firemními telefony a za jakých podmínek mohou využít telefon k soukromému účelu. Jiným problémem je odposlouchávání telefonních hovorů zaměstnanců nebo kontrola jejich pracovního emailu. V obou případech se většinou jedná o komunikaci dvou a více osob. Zaměstnavatel by proto potřeboval souhlas všech zúčastněných osob. Tuto problematiku podrobněji řeším v kapitole o ochraně know-how.

Zaměstnavatel může monitorovat, kdo, komu a jak dlouho telefonuje ze služebního telefonu. Dle mého průzkumu se v bezpečnostních agenturách ale této praktiky příliš nevyužívá a zaměstnavatelé jsou poměrně tolerantní. Na pár korun navíc, které mohl zaměstnanec provolat soukromými hovory, se nehledí, protože částky za celou firmu jdou

do tisíců. Kontrola se provádí, jen pokud je částka na vyúčtování abnormálně vysoká. Na to jsem také poukázal v případu, kdy zaměstnanci provolali 120 tisíc korun a k jejich odhalení přispěl elektronický systém kontroly obchůzek strážných.

8.8 Technická opatření

Technická opatření jsou důležitým prvkem při ochraně podniku. Na většinu zaměstnanců působí hlavně preventivně. V bezpečnostních agenturách se ale vzhledem k jejich činnosti vyskytují i zaměstnanci, kteří jsou s takovými systémy dobře obeznámeni a vědí, jak je obejít. Proto jen samotná technická opatření nemůžou zabránit páchání kriminality, ale v kombinaci s dalšími opatřeními, které jsou uvedené v této práci, můžou možnosti spáchání trestného činu snížit na minimum.

8.8.1 Mechanické zábranné systémy

Mechanické zábranné systémy (zkráceně MZS) patří do mechanické ochrany majetku a osob. Jedná se o prostředky či systémy, které zamezují nebo znesnadňují proniknutí do chráněného objektu, případně ke chráněné osobě. Základní funkcí těchto prostředků je vytvoření pevné překážky proti násilnému vniknutí osob a zabránění krádeži, znehodnocení nebo úniku informací. Svou časovou odolností odrazují pachatele. Lze je rozdělit na MZS:

a) *Obvodové ochrany* (bezpečnostní oplocení, branky, závory, zastavovací pásy, turnikety atd.)
b) *Plášťové ochrany* (mříže, rolety, žaluzie, bezpečnostní folie a skla, bezpečnostní dveře a vrata, bezpečnostní kování, přídavné zámky, dveřní pojistné řetízky atd.)
c) *Individuální předmětové ochrany* (komorové a skříňové trezory, komerční úschovné objekty, schránky pro úschovu klíčů, příruční pokladničky, bezpečnostní zavazadla, kontejnery a auta na přepravu peněz atd.)

Mechanické zábranné prostředky můžou zabránit vniknutí do objektu, ať už je tímto objektem ohraničený volný prostor (pozemek), budova, místnost či jen úschovný

objekt. Zejména úschovné objekty neboli trezory, ve kterých bývají uloženy ceniny, zbraně, střelivo a další, představují důležitou ochranu před možností odcizení některé ze jmenovaných věcí. Firemnímu trezoru by se měla věnovat veliká pozornost a musí být naprosto vyloučena možnost, že by se do něj mohl dostat jiný zaměstnanec, než který to má dovoleno. Co se týká ostatních místností, kde může být uložen například materiál, je použití MZS možná trochu nadbytečné, protože tyto krádeže většinou páchají zaměstnanci, kteří do těchto místností mají volný přístup, můžou tedy postačit obyčejné dveře doplněné příslušnými režimovými opatřeními. Pokud si chce být ale zaměstnavatel jistý, mříže do oken jistě nebudou na škodu. Můžou zamezit tomu, že si zaměstnanec nechá pootevřené okno, kterým se do objektu později vloupe.

Obr. 22 *Skříňový trezor [28]*

8.8.2 Systémy kontroly přístupu a vjezdu a docházkové systémy

Smyslem použití těchto technických prostředků je regulace vstupu do střežených prostorů. Tyto systémy umožňují rozlišit jednotlivé vstupující osoby či vjíždějící vozidla a automaticky zabránit vstupu (vjezdu) neoprávněných subjektů do objektu, také umožňují regulovat pohyb osob a vozidel po objektu způsobem, který se předem určí. V řadě případů plní tyto systémy i další doplňkové funkce, jako je třeba evidence docházky. Princip těchto systémů spočívá ve schopnosti přečíst pomocí speciálních zařízení,

tzv. čteček, zakódované pokyny a oprávnění osob a vozidel ke vstupu (vjezdu) do objektu a jejich pohybu uvnitř objektu. Systémy vstupu ovládají elektrické zámky dveří, závory aj. Pro zvýšení bezpečnosti mohou být navíc kombinovány s povinností použít při vstupu do chráněných prostor kromě identifikačních karet i zadání hesla nebo dokonce biometrickou identifikaci. [33]

Právě kombinace identifikačních karet nebo čipů s biometrickou identifikací nabízí nejvyšší možné zabezpečení. V případě, že přístupová práva nesouhlasí, osoba se snaží vstoupit např. mimo pracovní dobu, nebo do míst kam nemá přístup, tak přístupový systém zaeviduje datum a čas přiložení karty nebo prstu na snímač, ale dveře neotevře. Záznamy o všech vstupech a případně i výstupech z objektů se ukládají do databáze v přístupovém systému. To značně snižuje riziko, že se pokusí krást i zaměstnanec, který má například do místnosti přístup. Systém také umožňuje kontrolu stavu dveří. Jejich případné nezavření do určité doby, nebo násilné otevření vyvolá v nastaveném intervalu poplach.

8.8.3 Kamerové systémy

Systémy průmyslové televize (CCTV = Closed Circuit Television) slouží k monitorování situace na exponovaných a významných místech a to jak ve vztahu ke kriminalitě, tak ve vztahu k výrobním postupům, zajištění přehledu, operativnosti řízení a konečné možnosti snížení nákladů a ztrát. Systém CCTV představuje nezávislý kamerový systém, který může být provozován samostatně nebo může být zakomponován do rozsáhlých bezpečnostních a řídících systémů. Kamerový systém tvoří:

- Monitory: černobílé, barevné, kombinované
- Kamery: viditelné, skryté
- Obsluha systému: plná, částečná, bez obsluhy, s přednastavenými událostmi
- Přenos: vícežílovým kabelem, koaxiálním kabelem, symetrické vedení, optickým
- vláknem
- Záznam: analogově (VHS), digitálně (DVD, CD, HD)
- Příslušenství – multiplexery, clony, držáky atd.

Kamerové systémy jsou velice účinné při boji proti latentní kriminalitě. Působí hlavně preventivním způsobem. Bohužel nejde nijak změřit, kolika krádežím zabrání.

Pokud už ke krádeži dojde, je možné s jejich pomocí odhalit pachatele. V našem případě jsou si ale zaměstnanci kamer velmi dobře vědomi, proto je možnost, že se kamery pokusí vyřadit z provozu, což by vzhledem k jejich povolání nemusel být velký problém. Proto i zde platí pravidlo, že jenom jeden systém není dostatečně účinný a je nutná jeho kombinace s jinými.

Před nainstalováním kamerového systému by měl zaměstnavatel stanovit, za jakým účelem bude kamerový systém instalován. Stanovenému účelu, který má být těmito opatřeními dosažen (např. ochrana majetku, kontrola plnění úkolů zaměstnanců), je nutno přizpůsobit technické parametry kamerového systému a používání tohoto systému. Prostředky by měly být přiměřené účelu, kterému slouží, a je-li to možné, měl by se zaměstnavatel vyvarovat zásahů do soukromí zaměstnanců.

Má-li například kamera sloužit ke sledování plnění pracovních úkolů zaměstnancem, pak je nutno vyjít z povahy těchto pracovních úkolů a jistě nelze připustit, aby kamerový systém sledoval zaměstnance i na místech, kde nevykonává práci (např. na záchodě, v šatně), nebo aby byl snímán i v době, kdy není povinen vykonávat práci (např. během přestávek v práci).

Prvním krokem před instalací kamer by mělo být vymezení zakázaného jednání ve vnitřním předpise, nejlépe pracovním řádu. Doporučuje se také vyvolat o této skutečnosti jednání se zástupci zaměstnanců, případně se zaměstnanci samotnými. [23]

Instalace kamerového systému ve vnitřních společných prostorách objektu zaměstnavatele (např. schodiště, chodby) určeného k monitorování (tj. nikoliv permanentní a systematický záznam) je možná. K ochraně práv snímaných osob by mělo postačit rozmístění informativních cedulí.

Kamerový systém může zamezit krádežím už jen tím, že o něm zaměstnanci vědí. V případě, že jsou i přesto odhodláni krást, jedná se většinou o veliké sumy peněz a pokud má zaměstnanec k ovládání systému přístup, může s ním manipulovat a zahladit důkazy, jako se to zřejmě stalo i v případě půlmiliardové krádeže.

8.8.4 Poplachové zabezpečovací systémy

Poplachový zabezpečovací systém je soubor zařízení, jejichž hlavním úkolem je střežit předem definovaný prostor. Při vniknutí neoprávněné osoby systém signalizuje narušení prostoru (akusticky nebo opticky) a vyšle informaci o vzniklé situaci na mobilní telefon nebo pult centralizované ochrany. Poplachová zabezpečovací signalizace se skládá z detektorů, prostředků poplachové signalizace, poplachové přenosové cesty, zdrojové části, ovládacího zařízení a ústředny. [34]

Pro tyto systémy se dle nové normy užívá zkratka IAS (intruder alarm systém). Tísňové poplachové systémy umožňující uživateli možnost úmyslného vyvolání poplachového stavu, se označují zkratkou HAS (hold-up alarm systém). Poplachové zabezpečovací systémy jsou vhodné zejména proti možnosti vnějšího napadení. Proti krádežím vlastních zaměstnanců nemusí být příliš účinné, ale v rámci prevence rozhodně nejsou na škodu.

8.8.5 Telefonní ústředna

Telefonní ústředny slouží k rozbočení telefonní linky na jednotlivé pobočky, kterým pak lze nastavit jednotlivé parametry. Telefonní ústředny jsou výhodné pro firmy, kterým šetří čas i finanční prostředky. Zajistí, že žádný hovor nebude nevyslyšen a že se každý bude moci dovolat do firmy i ven. V jedné z agentur jsem si všimnul ústředny Ateus 260-420, kterou zde popíšu, protože tato ústředna umožňuje kontrolovat, kdo s kým, kdy, ale hlavně kolik peněz provolal. Tím pádem je vhodným prostředkem k obraně před zneužíváním služebních telefonů.

Jedná se o programovatelnou pobočkovou ústřednu, která má v základním provedení šest vnitřních linek, ze kterých se můžeme pomocí dvou státních linek dovolat do celostátní nebo mezinárodní telefonní sítě. Tato ústředna může mít až dvacet vnitřních účastníků (linek), kteří mohou být napojeni až na šest státních linek, toho se dá dosáhnout pomocí dalších rozšiřujících modulů, které lze v případě rozšiřování firmy zakoupit. Ústředna umožňuje přímé propojení s jakoukoliv tiskárnou k PC, tiskárna pak může vytisknout podrobnosti o hovorech a účtech za telefon, takže je možné ihned vyvodit důsledky. Další výhodou této ústředny jsou zabudované universální spínače, na které lze připojit např. el. vrátného (tzv.bzučák) nebo zapínání a vypínání vytápění podniku (např. 1

hod před začátkem pracovní doby zavoláte a zapnete si topení) a vlastní vnitřní hodiny ústředny. K dalším výhodám patří široký okruh zařízení, které se dají k ústředně připojit, jsou to např. tel. záznamník, tel. přístroj jak „vytáčecí“ tak „tlačítkový“, fax, dveřní telefon a už výše zmiňovaný el. vrátný, externí zdroj hudby a jiné. [35]

Obr. 23 *Ústředny Ateus – starší a novější typ [35]*

8.8.6 GPS lokátory a elektronická kniha jízd

Tímto způsobem je možno řešit zneužívání služebních vozidel. Jedná se o systémy k satelitnímu sledování vozidel a také ke správě vozového parku. V reálném čase a pravidelných intervalech zaznamenává GPS polohu, kterou je možno sledovat na počítači. Na trhu existuje mnoho systémů, takže je možné si vybrat podle požadovaných funkcí. Sledovat vozidlo přes vlastní PCO je pro bezpečnostní agenturu velkou výhodou

Systémy nabízejí mnoho funkcí, mezi nejpotřebnější patří:

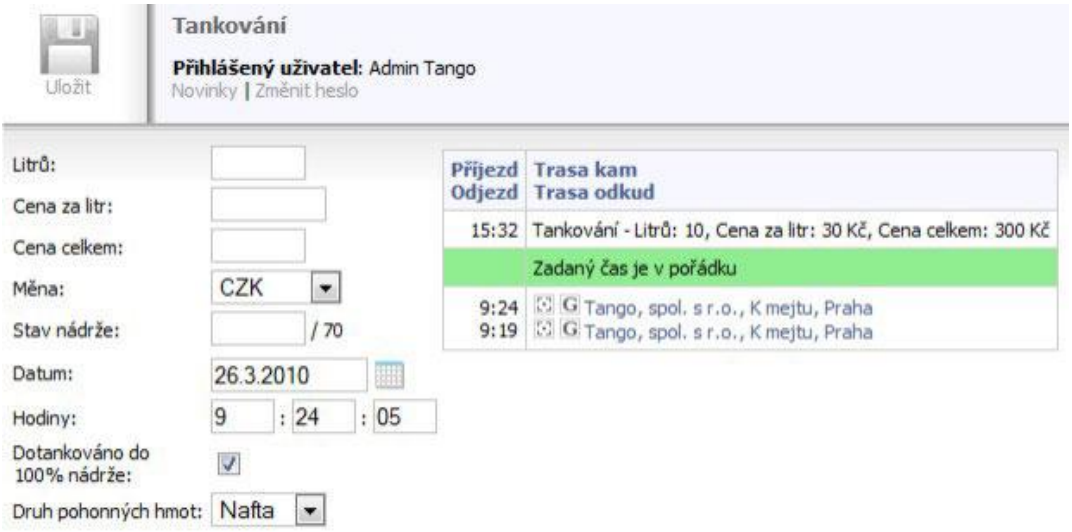
1) *Elektronická kniha jízd* – může být vytvářena systémem automaticky a být základem webového výstupu pro uživatele. Kniha jízd umožňuje zobrazit a přehrát ujetou trasu včetně rychlosti, přepnout typ jízdy a definovat vlastní, pojmenovat zájmové body a oblasti na mapě plus jejich následné zanesení do knihy jízd, a mnoho dalších nástrojů, které výrazně ulehčují vyhodnocování nasbíraných dat.

2) *Uživatelské účty* - Díky možnosti vytvářet vlastní uživatelské účty s různými pravomocemi může systém obsluhovat libovolný počet uživatelů. Jakákoliv změna provedená uživatelem je zobrazena v administračním rozhraní. Pokud například zaměstnanec použije vozidlo, na dispečinku se to objeví a dispečer zadá, zda je jistá odsouhlasená či nikoliv. Díky této jednoduché administrativě nemusí řidiči psát ruční knihu jízd a je jim znemožněno udělat jízdu „na černo".

3) *Kontrola spotřeby paliva* – Tato funkce umožňuje kontrolovat spotřebu, ale také je možno zaznamenávat čas a místo otevření/zavření nádrže. Informace mohou být také importovány z tankovacích karet. Tato funkce zabrání krádeži paliva, ať už by si ho chtěl zaměstnanec natankovat do vlastního kanystru a poté zaplatit firemní kartou nebo pokud by chtěl palivo odčerpat přímo z nádrže.

Obr. 24 *Elektronická kniha jízd [36]*

Obr. 25 *Kontrola jízdy na černo pomocí uživatelských účtů [36]*



Obr. 26 *Kontrola spotřeby paliva [36]*

Existuje ještě celá řada implementovaných funkcí, které usnadňují kontrolu nad stavem vozidla. Centrální jednotka je montována skrytě a je možné podle potřeby jednotku přenášet z vozidla na vozidlo, to ale v případě že má agentura více vozidel není optimální a každé by mělo mít svou vlastní jednotku.

Ze zjištěných informací jsou tyto GPS lokátory využívány bezpečnostními agenturami v naprosté většině případů, ale zřejmě starší verze, které nenabízejí elektronickou knihu jízd, neboť ta byla ve zjištěných případech vedena písemně samotnými zaměstnanci. Cena jednotek se pohybuje řádově od 2 do 7 tisíc v závislosti na použité funkce. Měsíční poplatky za služby se pohybují od 150 do 400 Kč.

8.8.7 Elektronický systém kontroly obchůzek strážných

Tento systém nabízí řešení pro monitorování zaměstnanců v závislosti na místu a čase. Uplatnění může nalézt všude tam, kde je potřeba kontrolovat a zaznamenávat čas a místo pohybu osob a věcí. Zejména je tento systém využíván pro kontrolu obchůzek strážných.

Uvádím zde informace o systému PES (přenosný elektronický snímač), který pomohl k odhalení pachatelů v případu zneužívání služebních telefonů, který jsem uváděl. Tento systém je založen na světově uznávané technologii iButton od americké společnosti Maxim/Dallas.

Na kontrolních místech střeženého objektu jsou instalovány identifikačními čipy. Každý tento čip je unikátní a obsahuje nezaměnitelný kód. Strážný je vybaven elektronickým snímačem, kterým při obchůzce musí jednotlivé kódy všech čipů načíst. Data ze snímače jsou pak pomocí záznamového média přenesena do počítače a vyhodnocena. Načítání kódů jednotlivých identifikačních čipů se provádí letmým přiložením snímače. Správné zaznamenání kontrolního bodu je opticky i akusticky signalizováno.

Obr. 27 *Systém PES [37]*

Aby mohla být data ze snímače zpracována, přenesou se přiložením na datový čip. Tento čip funguje jako záznamové médium, podobně jako např. disketa. Datový čip se záznamem se odnese na pracoviště určené pro zpracování výpisů pochůzkové služby. (Snímač tedy nemusí ani na chvíli opustit pracoviště strážných.) Přiložením datového čipu k adaptéru, připojenému k počítači s nainstalovaným programem WinKontrol, se data během několika vteřin přenesou do PC.

Pokud je tento systém připojen na PCO, můžou být stanoveny přesné časy, kdy mají strážní vykonávat obchůzky, nedojde li ve stanovených časech k sejmutí všech bodů, dojde k poplachovému stavu a dispečink hned situaci ověřuje. Tento systém pomohl objasnit případ zneužívání telefonů, který jsem uváděl. V některých dotázaných agenturách je také používán obdobný systém Torex.

ZÁVĚR

V první kapitole jsem se věnoval latentní kriminalitě. Je to část kriminality, kdy vůbec nevyjde najevo, že byla spáchána závažná trestná činnost a proto se nestane předmětem trestního stíhání. Latentní kriminalita zahrnuje ty trestné činy, které vůbec nebyly spáchány tzn. ani nebyly oznámeny či zjištěny. Dále sem řadíme trestné činy, které sice byly policií zjištěny, ale nikdy nebyli vypátráni pachatelé, kteří je způsobili. Jedná se o ukrývanou a často organizovanou a velice profesionálně zajištěnou trestnou činnost, která bývá někdy také označována jako kriminalita bílých límečků. Spadají sem trestné činy jako krádež, zpronevěra, podvod a další. Tyto trestné činy můžou nejsnadněji provést vysoce postavení zaměstnanci, kteří mají potřebné informace a znalosti systému.

Druhá kapitola je věnována rozkrádání v podnicích průmyslu komerční bezpečnosti, kde popisuji různé způsoby, kterými se zaměstnanci dopouštějí trestných činů. Mezi nejzávažnější patří peněžní krádeže, krádeže materiálu, výzbroje, výstroje či střeliva, know-how, zneužívání služebních vozidel a telefonů, a dokonce sem patří i takové činy jako krádeže čisticích prostředků a krmiva pro psy, protože právě takových drobností si vedení často nevšímá a podnik tak přichází o tisíce. U příslušníků SBS se dokládá bezúhonnost a nepředpokládá se, že by měli ve velkém rozkrádat majetek podniku a právě to je jejich výhoda.

Třetí kapitola se zaměřuje na příčiny a podmínky páchání kriminality. Rozvoj techniky umožňuje pachatelům využívat důmyslnější prostředky, ale zároveň je technika důležitá v oblasti ztěžování či znemožňování páchání kriminality stejně jako v procesu jejího rozkrývání. U vysoce postavených pracovníků, kteří bývají označováni jako tzv. bílé límečky, nebývá příčinou páchání trestné činnosti materiální nouze, ale spíše jim jde o vylepšení společenské prestiže, trvalé zajištění dobré existence či výrazné vylepšení materiální situace. Zaměstnanci na nižších pozicích se obvykle prostřednictvím krádeží snaží uspokojit nějakou ze svých potřeb. Kriminologie rozděluje tyto pachatele na typy příležitostné, cílevědomé, plánovité, strategické a na recidivisty.

Čtvrtá kapitola se zabývá personální politikou podniků, je zde popsána, jaká by měla být osoba personalisty a jaké metody práce je vhodné v bezpečnostních agenturách využívat. Dále zde popisuji chyby v personální politice, kam patří mimo jiné neověřování údajů v životopisech nebo špatný systém odměňování a motivace zaměstnanců. Spolupráce se státní administrativou není na dobré úrovni, majitelé agentur si stěžují nejčastěji na to,

že jim Úřady práce zahlcují personální oddělení nevhodnými uchazeči, kteří byli například v minulosti trestaní.

Pátá kapitola se zabývá formami a metodami odhalování latentní kriminality. Je třeba si uvědomit skutečnost, že v podmínkách tržní ekonomiky se policejní orgány či další orgány činné v trestním řízení nezabývají skrytou kriminalitou v podniku. V našem případě se na rozkrývání latentní kriminality podílejí zejména soukromí detektivové za použití vhodných forem a metod detektivní činnosti jako detektivní zpravodajství, detektivní prověrka apod.

V praktické části jsem prováděl zhodnocení současného stavu v bezpečnostních agenturách. Informace, které jsem se dozvěděl, byly zpracovány do grafů a sloužily mi také jako inspirace při návrhu aktivních opatření.

V sedmé kapitole jsem použil několik případů trestné činnosti zaměstnanců bezpečnostních agentur, které se mi podařilo vytěžit a na těchto případech poukazuji na chyby, které usnadnily spáchání této trestné činnosti. Ačkoliv se u všech případů nejedná o typickou latentní kriminalitu, opatření, která ji pomohla odhalit, jsou velmi dobře použitelná i pro účely této práce.

Poslední kapitola patří návrhům aktivních opatření, která zabraňují vzniku latentní kriminality zaměstnanců. Zaměstnance je nejprve třeba správně vybrat a v průběhu jejich služby neustále pravidelně i namátkově kontrolovat. Ke spáchání trestné činnosti je potřeba úmysl a příležitost, proto navrhuji i opatření, která těmto stavům zabraňují. Majetek podniku lze chránit prostřednictvím fyzické ochrany, detektivní a zpravodajské ochrany a za použití režimových a technických opatření, která navrhuji na základě informací získaných z bezpečnostních agentur.

Trestná činnost zaměstnanců bezpečnostních agentur by se neměla zamlčovat, jak se tomu bohužel děje. Obavy, že dojde k poklesu zakázek, jsou možná oprávněné, ale pokud se tento problém nezačne řešit, můžou být následky mnohem horší. Závěrem bych rád uvedl citát Tomáše Bati:

„Každá lidská činnost se nakonec musí nějak projevit v číslech.“

A zejména to platí pro trestnou činnost zaměstnanců, proto je nutné situaci nepodcenit, neustále kontrolovat a využít všech dostupných opatření k ochraně podniku.

ZÁVĚR V ANGLIČTINĚ

In first chapter am paid latent criminality. Is that a part criminality, when at all will go wrong out, that the was perpetrated weighty criminality that is why lack of courage subject penal pursuit. Latent criminality includes you crime that the at all wasn't perpetrated it means nor wasn't reported or ascertained. Further here line crime that the though were to be police ascertained, but will never weren't detection offenders that the be caused by. Acts about hide away and often organized and very professionally independent punishable activity that the used to be sometimes also referred to as like criminality white collars. Coincide here crime like theft, defalcation, cheat and next. These crime is able to easiest carry out distinguished staff that the have needed information and knowledge system.

Alternative chapter is devoted pilferage in companies industry commercial safeness, where describe various manners that the staff suffer crime. Among weightiest belongs to monetary robberies, robberies material, munitions, kits or ammunition, know - how, violation business vehicle and phones, and even here belongs to and such record like robberies cleansing articles and feedstuffs for dogs, because such another minuteness lead often ignore and company so is coming about thousands. Near members SBS exemplifies integrity and no supposes , that they should on a large scale thieve possession company and very thing is their advantage.

Third chapter survey on causes and conditions commission criminality. Development techniques makes it possible to offenders derive benefit from more sophisticated resources, but at the same time is technology important in the area make more difficult or checkmate commission criminality as well as in the process of her detection. Near distinguished workers that the if you had been me referred to as like so - called white-collar workers, American hookworm cause commission punishable activities material stress, but rather a them is concerned improvement social prestige, lasting reservation good existence or expressive improvement material situation. Staff on lower positions usually through theft try satisfy some of theirs needs. Criminology divides these offender on print occasional, purposeful, planned, strategic and on habitual offender.

Fourth chapter deal with personnel policy companies, is here circumscribed, what would had be person personnel clerk and what method work get past in security agencies derive benefit from. Further here describe mistakes in personnel policy, where belongs to

among others unverified datums in resumes or bad system remuneration and employee motivation. Cooperation administration isn't on decent, proprietary agencies complain most often at it, that the them authorities work in a daydream staff department unfit aspirants that the were for example in former times punishable by.

Fifth chapter deal with forms and methods detection latent criminality. It is necessary inform reality, that the in conditions market economies police authorities or next law enforcement authorities no deal with hidden criminality on the premises. In our case on detection latent criminality partake especially privacy detectives behind using fit forms and methods detective activities like detective reporting, detective screening etc .
In practical parts am do inquiry state - of - the - art in security agencies. Information that the am knew, were to be processed to the graphs and served me either as inspiration at proposal active procuration.

In seventh chapter am used several cases punishable activities employees security agencies that the me succeed extract and upon this cases point on mistakes that the made it easier commitment those punishable activities. As near of all cases disunity about typical latent criminality, procuration that the she helped disclose, are very well applicable and for purposes those work.

Last chapter belongs to proposals active procuration that the obstruct rise latent criminality employees. Employee is first possibly well choose and along their services all the time regularly and at random check. To commitment punishable activities is need intention and occasion, therefore I prefer and procuration that the this states obstruct. Possession company it is possible buckler through physical wardships, detective and intelligence wardships and behind using regimen and technical procuration that the I prefer on the basis information obtained from security agencies.

Criminality employees security agencies would didn't have conceal, how that unfortunately action. Alarm, that the come to fall orders, perhaps be in capacity, but if this problem unincorporated solve, is able to be aftermath much worse. In fine would like introduced quotation Thomas Bata:

„ Every human activity in the end have to somehow disply manifest in numbers."

Namely pays and for punishable activity employees, therefore is necessary situation no underestimate and use of all accessible procuration to protection company.

SEZNAM POUŽITÉ LITERATURY

[1] ARMSTRONG, Michael. Řízení lidských zdrojů. 10.vyd. Grada, 789 s. ISBN: 978-80-247-1407-3

[2]BRABEC, František. Ochrana bezpečnosti podniku, Praha: Eurounion, 1996. ISBN 80-86445-04-6.

[3]BRABEC, František. Hlídací služby. 1. vyd. Praha: Eurounion, 1995. 259 s. ISBN 80-85858-12-6

[4]BRABEC, F. Soukromé detektivní služby. 1. vyd. Praha : Eurounion, 1995. 199 s. ISBN 80-85858-16-9

[5]BRABEC, František. Soukromě detektivní ochrana ekonomických zájmů a rozkrývání latentní ekonomické criminality, materiály publikované v různých souvislostech

[6]ČÍRTKOVÁ, Ludmila. Psychologické aspekty problematiky. In Pracovní material pro kurz hospodářské a finanční kriminality. Praha:Policejní akademie ČR 2001

[7] DIVIŠ, Zdeněk . Trestná činnost tzv. bílých límečků. [s.l.], 2006. 43 s. Diplomová práce. Masarykova Univerzita.

[8]DOLSKÁ, Daniela. Personální činnost podniku G4S Security Services. Praha, 2009. 69 s. Bakalářská práce. Středočeský vysokoškolský institut Kladno.

[9]HOJSÁKOVÁ, Alena. *Fyziodetekce v bezpečnostní komunitě*. Zlín, 2010. 90 s. Diplomová práce. UTB.

[10]HORSÁK, Jan. *Ochrana know-how*. Zlín, 2010. 80 s. Diplomová práce. UTB.

[11]KAMENÍK, J. BRABEC, F. Komerční bezpečnost. ASPI Praha, 2007. ISBN 978-80-7357-309-6.

[12]KUCHTA, J. Základy kriminologie a trestní politiky. Praha : C.H.Beck, 2005. 353 s.

[13]LÁTAL, Ivo; ŠTANTEJSKÝ, Michal. Bezpečnostní zásady ochrany podniku : Prevence a řešení krizových situací. Vyd.1. Praha : PROSPEKTRUM, 2001. Režimová ochrana, s. 120. ISBN 80-7175-091-3.

[14]LAUCKÝ, Vladimír. Speciální bezpečnostní technologie. UTB Zlín 2009, 123s.

[15]MUZIKA, Jan. MUZIKOVÁ, Kamila. *Latentní trestná činnost v PKB*. Praha, 2011. 5 s. Seminární práce. UTB.

[16]NOVOTNÝ, František. Trestní zákoník 2010. EUROUNION, 838s. ISBN: 978-80-7317-084-4

[17]PAVLAS, Josef. Podvodná jednání-Podvody, zpronevěry, machinace, podnikové materiály

[18]POHL, Josef. Komerční detektivní kanceláře a rozkrývání latentní kriminality v podnicích a organizacích. Zlín, 2010. 81 s. Diplomová práce. *UTB.*

[19]STRAKOVÁ, Zdenka. Defenzívne komerčné spravodajstvo – vrcholová technológia detektívnej činnosti. Zlín, 2008. 71 s. Diplomová práce. UTB.

[20] ŠTABLOVÁ, CSC, Doc.Ing.Renata . KRIMINOLOGIE : Studijní texty. PRAHA:[s.n.], 2008. 78 s.

[21] ŠTEFKO, Martin. K problému sledování vlastních zaměstnanců . Právo a zaměstnání. 2005, 1, s. 7-11.

[22] Latentní kriminalita. *Epravo.cz* [online]. 2002, 15571, [cit. 2011-04-17]. Dostupný z WWW: <http://www.epravo.cz/top/clanky/latentni-kriminalita-15571.html>.

[23] ŠMÍD, Jan. Pracovní hříchy mnohých zaměstnanců. *Kursy.cz* [online]. 2009, 1, [cit. 2011-03-08]. Dostupný z WWW: <http://www.kursy.cz/pracovni-hrichy-mnohych-zamestnancu-cid205401/>.

[24] *Business.center.cz* [online]. 2007 [cit. 2011-04-17]. Zákoník práce-Zákon č. 262/2006 Sb., zákoník práce . Dostupné z WWW: <http://business.center.cz/business/pravo/zakony/zakonik-prace/>.

[25] CERMANOVÁ, Tatiana. Osobnost personalisty a možné směry rozvoje ve vztahu k jeho rolím. *Psychologie v personalistice* [online]. 2004, 1, [cit. 2011-04-17]. Dostupný z WWW: <http://www.hrportal.cz/osobnost-personalisty-a-mozne-smery-rozvoje-ve-vztahu-k-jeho-rolim-cid94527/>.

[26] *Hdelektro* [online]. [cit. 2011-04-29]. Dostupné z WWW: <http://www.hdelektro.cz/index.php?nabidka=1&str=21>.

[27] *Armybutik* [online]. [cit. 2011-04-29]. Dostupné z WWW: <http://armybutik.cz/index.php?cont=detail&karta=498>.

[28] *Rovelzlin* [online]. [cit. 2011-04-29]. Dostupné z WWW: <http://www.rovelzlin.cz/kategorie/skrinove-trezory-nhd.aspx>.

[29] *Štěpán* [online]. [cit. 2011-04-29]. Dostupné z WWW: < http://www.stepan.cz/bazeny/chemoform/>.

[30] *FalcoHK* [online]. [cit. 2011-04-29]. Dostupné z WWW: < http://www.falco-hk.cz/cz_podnikova_bezpecnost.php>.

[31] Policie obvinila Procházku z loupeže půlmiliardy. *Novinky.cz* [online]. 2007, ., [cit. 2011-04-29]. Dostupný z WWW: <http://www.novinky.cz/krimi/128380-policie-obvinila-prochazku-z-loupeze-pulmiliardy.html>.

[32] Lupiči ukradli z vozu bezpečnostní agentury desítky miliónů. *Novinky.cz* [online]. 2008.[cit.2011-04-29].Dostupný z WWW: <http://www.novinky.cz/krimi/131000-lupici-ukradli-z-vozu-bezpecnostni-agentury-desitky-milionu.html>.

[33] ČECH, Radim. *Detektivní ochrana podnikatelských subjektů z hlediska vnitřních a vnějších chráněných zájmů*. Zlín, 2008. 73 s. Bakalářská práce. UTB.

[34] HANÁČEK, Adam. *Způsoby zabezpečení drátových ústředen EZS proti sabotáži*. Zlín, 2010. 55 s. Bakalářská práce. UTB.

[35] *Ateus* [online]. [cit. 2011-04-29]. Dostupné z WWW: < http://www.2n.cz/cz/produkty/telefonni-ustredny/netstar/>.

[36] *Lokátory.cz* [online]. [cit. 2011-04-29]. Dostupné z WWW: < http://www.lokatory.cz/>.

[37] *Instalace systému PES* [online]. [cit. 2011-04-29]. Dostupné z WWW: < http://www.raso.cz/produkty6.htm/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PKB Průmysl komerční bezpečnosti

MZS Mechanické zábranné systémy

SBS Soukromé bezpečnostní služby

IAS Intruder alarm systém – poplachový zabezpečovací systém

HAS Hold-up alarm systém – tísňový poplachový systém

EPS Elektrická požární signalizace

CCTV Systémy průmyslové televize

PES Přenosný elektronický snímač

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ