Personální bezpečnost ve veřejné správě

Personnel security in public administration

Jakub Beneš

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jakub BENEŠ**
Osobní číslo:	**A08855**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Personální bezpečnost ve veřejné správě**

Zásady pro vypracování:

1. **Popište současný stav vybavenosti fyzických osob ve veřejné správě.**
2. **Vysvětlete rozdíl v personální bezpečnosti v oblasti veřejné správy a soukromého sektoru.**
3. **Definujte ideální stav zabezpečení.**
4. **Vyjmenujte rozdíly v personální bezpečnosti EU a v ČR.**
5. **Uveďte způsoby právního zabezpečení osobní ochrany.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Bartík, Václav. Ochrana osobních údajů v aplikační praxi: vybrané otázky. Vyd. 1 Praha: Linde 2010. ISBN 978-80-7201-817-8**
2. **Brabec, František. Ochrana bezpečnosti podniku. Vyd. 1 Praha: Eurounion 1996, ISBN 80-85858-29-0**
3. **Ivanka, Ján. Mechanické zábranné systémy. Vyd. 1 Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, ISBN 978-80-7318-910-5**
4. **Laucký, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, ISBN 978-80-7318-889-4**
5. **Morávek, Jakub. Ochrana osobních údajů v pracovněprávní agendě Praha: BMSS-Start, 2010, ISBN 978-80-86140-64-3**
6. **Říha, Milan. Bezpečnostní systémy (1. a 2. díl) Vyd.1 Praha: Námořní akademie České republiky, 2007 ISBN 978-80-87103-03-6 a 978-80-87103-13-5**

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

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

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

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Bakalářská práce se zabývá současným stavem personální bezpečnosti fyzických osob ve veřejné správě a personální bezpečností celkově.

V práci se snažím postihnout i rozdíly mezi personální bezpečností ve veřejném sektoru a soukromém sektoru v ČR i v zahraničí.

Také se v této práci zabývám ideálním stavem zabezpečení či způsoby právního zabezpečení osobní ochrany v této problémové oblasti.

Klíčová slova: personální bezpečnost, veřejná správa, zabezpečení, soukromý sektor

ABSTRACT

The bachelor thesis deals with the current state of personnel security of individuals in public administration and personal security of personnel in general..

In this thesis I try to capture the differences between personnel security in public sector and in private sector in the Czech Republic as well as abroad.

In this thesis I also deal with the ideal state of personnel security and legal data protecting safety measures, regulations in this komplex area.

Keywords : personal security and safety, public administration, security, private sector

Rád bych poděkoval vedoucímu mojí bakalářské práce, panu JUDr. Františku Brabcovi, za mnoho cenných rad a trpělivé odborné vedení mé práce.

Dále bych chtěl poděkovat tajemníkům, vedoucím personálních a bezpečnostních odborů mnou oslovených městských úřadů a vedoucím personálních oddělení oslovených firem za poskytnutí cenných informací.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Personální bezpečnost je typem zajištění ochrany utajovaných informací. Na ochranu informací se můžeme dívat v širším spektru z hlediska informační bezpečnosti, která zahrnuje optimálně fungující informační systém, zajištěný zpravodajským servisem či komerčním nebo konkurenčním zpravodajstvím. Obranné nestátní zpravodajství komplexně zajišťuje ochranu nejen utajovaných informací, ale i ochranu obchodního tajemství, osobních údajů a zvláštních skutečností.

Personální bezpečnost zajišťuje i výchovu fyzických osob, kterým je umožněn přístup k utajované informaci, a to zejména jejich proškolením a ověřením podmínek stanovených zákonem. Podle stupně utajení se liší i způsob a rozsah ověřování podmínek, které musí fyzická osoba splnit, aby jí byl umožněn přístup k dané informaci.

Uvědomme si, že personální bezpečnost je systémem opatření, která vytvářejí možnost, aby se s utajovanými informacemi seznamovala pouze příslušná fyzická osoba a zároveň také, aby byla vytvořena opatření zajišťující ochranu této osoby.

Předkládaná práce proto nemůže obsáhnout vyčerpávajícím způsobem veškerou problematiku týkající se personální bezpečnosti ve veřejné správě.

Můžeme předpokládat, že velkou část problémů ve veřejnosprávních organizacích bychom odstranili lepším bezpečnostním zajištěním chodu těchto úřadů a samospráv.

Základním pilířem této práce bylo zjistit stav personální bezpečnosti ve veřejné správě u nás a porovnat tento stav se zabezpečením v dalších státech Evropské unie.

Vzhledem k tomu, že se v oblasti veřejné správy vyskytuje jak státní správa, která zahrnuje zejména ústřední orgány na úrovni působnosti pro celý stát (ministerstva, úřad vlády apod.), tak samospráva, která působí v rámci obcí či krajů, je možné pozorovat rozdíl v personální bezpečnosti i v oblastech veřejné správy.

Pokud zjišťujeme rozdíl v personální bezpečnosti v oblasti veřejné správy a v oblasti soukromého sektoru, vidíme i další odlišnosti zejména v působení různých norem i v materiálním zabezpečení osob vzhledem k jejich ochraně.

Součástí úkolu bylo uvést způsoby právního zabezpečení osobní ochrany, případně i uvést změny týkající se právních norem pro ochranu osob a osobních dat.

Dnes při zajišťování personální bezpečnosti můžeme narazit na několik úskalí, která znemožňují účinně využít všechny dostupné prostředky. Proto jsem se také zaměřil na ideální stav zabezpečení objektů ve veřejné správě, neboť tím by se dalo předejít mnohým komplikacím, které se týkají ochrany osob, dat i majetku.

Ve své práci se zabývám uvedenou problematikou, jak obecně, tak i vnější ochranou fyzickou i technickou a následně i ochranou vnitřní.

Vzhledem ke statistickému vyhodnocení, které jsem zpracoval, věřím, že tato práce bude přínosem a přispěje k účinnější personální bezpečnosti.

I. TEORETICKÁ ČÁST

1 OBECNÁ CHARAKTERISTIKA OCHRANY INFORMACÍ

1.1 Význam ochrany informací

Informace představují základní výhodu v tržním hospodářství. Stárnou rychle, a pokud mají být upotřebitelné, musí se aktualizovat. Jsou prostředkem rychlého obohacení, a proto je nutné je co nejvíce chránit a zároveň dobře využívat.

Informace podle své váhy obklopujeme určitým utajením, aby k nim měla přístup jen oprávněná osoba. Každá informace proto musí doznat vlastní systém ochrany – chráníme místo, kde se s informacemi pracuje, chráníme osoby, které s těmito informacemi pracují. Zároveň tyto osoby musí být pečlivě vybírány. Informační bezpečnost představuje optimální ochranu informací před jejich zcizením, zneužitím, poškozením, zkreslením a únikem k neoprávněným osobám.

Vždy docházelo k ochraně utajovaných informací a bylo to ošetřeno i právně. Není důležité tajit každou informaci, ale nejdůležitější informace utajit co nejkvalitněji, a proto nesmí selhat zejména lidský faktor.

Ochrana utajovaných informací je zajišťována prostředky komplexní ochrany, které vyžadují nejrůznější opatření. Patří k nim personální, administrativní, objektová a technická bezpečnost, dále pak je nutná bezpečnost informačních systémů a kryptografická ochrana.

Základním opatřením z hlediska administrativní bezpečnosti organizace je vypracování Spisového a skartačního řádu, ve kterém jsou určeny veškeré manipulace s utajovanými písemnostmi v organizaci.

Objektová bezpečnost si klade za cíl zabránit proniknutí nepovolané osoby do objektu, minimalizovat následky proniknutí, včasně proniknutí nepovolané osoby do objektu zjistit, a tak předcházet úniku nebo znehodnocení utajovaných informací.

Technické prostředky, které mohou být používány k ochraně utajených informací, musí být certifikované a jejich seznam je uveden ve věstníku Národního bezpečnostního úřadu. Úřad také stanoví způsob použití těchto prostředků k technickému zabezpečení utajovaných informací.

Informační systémy používané k nakládání s utajovanými informacemi jsou certifikovány NBÚ nebo jím pověřenou organizací.

Při zpracování, přenosu, ukládání a archivaci utajovaných informací je zajišťována kryptografická ochrana odborně způsobilými pracovníky a kryptografickými prostředky certifikovanými NBÚ. Úřad stanoví právním předpisem způsoby použití, nasazování a evidence kryptografických prostředků.

1.2 Systém ochrany informací

Základem informační bezpečnosti je samozřejmě prevence, ale pokud dojde ke zjištění úniku informací, mělo by dojít následně k represi a zároveň k aktualizaci a zkvalitnění informační prevence. Informační bezpečnost představuje ochranu fyzickou, technickou a softwarovou, režimovou i detektivní a zpravodajskou. Z toho důvodu ochrana informací vyžaduje zajištění fyzické ochrany objektu a osobní ochrany osob pracujících s informacemi. Nesmíme samozřejmě opomenout v této souvislosti technickou a softwarovou ochranu informačních systémů, proto dodavatelé ICT, hardware a zabezpečovacích systémů by měli projít prověřením. Dále musí být zabezpečena ochrana proti vlivu konkurence a získávání informací konkurencí pomocí organizačních a režimových opatření k ochraně informací.

Personální bezpečnost je součástí systému ochrany informací a dat. Je důležité správně ocenit bezpečnostní rizika, vést odpovídající bezpečnostní politiku a vytvořit bezpečnostní projekt, který bude zahrnovat bezpečnost personální, administrativní, technickou i objektovou.

„Bezpečnostní analýza by měla předcházet všem bezpečnostním opatřením a jejich krokům. Bezpečnostní analýza není ani jednorázovou záležitostí, ale musí se opakovat periodicky (po jisté době), a při všech změnách bezpečnostní situace.

Bezpečnostní analýza je nezbytným východiskem pro proces syntézy získaných poznatků a vypracování bezpečnostního projektu, jehož úkolem je stanovit naprosto konkrétní opatření, kterými bude dosaženo cíle definovaného bezpečnostní politikou. Přitom bezpečnost nelze chápat jen jako prostý souhrn použitých prostředků, opatření a postupů, ale jako určitý celek – systém, který je vytvořen za účelem dosažení konkrétního cíle.“[1]

Prvky bezpečnostního systému musí být logicky provázány tak, aby reagovaly na změny vnějších i vnitřních podmínek kdykoliv v budoucnu. Bezpečnostní projekty řeší fyzickou ostrahu objektu, jeho elektronickou ochranu, případně detektivní ochranu a zaměřují se i na mechanické zábranné prostředky a systémy. Těmito opatřeními se zabývají poradenské firmy a kombinují běžně používané techniky s vlastními postupy, ale vždy musí dodržet opatření vycházející ze zákona. Kvalita bezpečnostních opatření je oceňována bezpečnostním auditem, který by měl potvrdit, že stupeň účinnosti zabezpečení je odpovídající.

Speciální objekty vyžadující zajištění podle zákona 412/2005 Sb. ve znění pozdějších předpisů o ochraně utajovaných informací musí být z hlediska mechanických zábranných systémů zajištěny podle požadavků NBÚ a technické prostředky smí být pouze certifikované Národním bezpečnostním úřadem nebo jím pověřenou organizací. Ostatní technické prostředky lze použít pouze doplňkově tak, že jejich použitím nedojde ke snížení úrovně ochrany požadované pro daný stupeň utajení. Seznam certifikovaných technických prostředků je uveřejněn ve věstníku, který NBÚ vydává. Národní bezpečnostní úřad určuje právním předpisem systém opatření, technické prostředky a způsob jejich použití při ochraně utajovaných informací.

Vnější ochranu úřadu státní správy můžeme rozdělit na ochranu fyzickou a technickou.

Technická ochrana slouží ke zvýšení účinnosti fyzické ochrany objektu, ale pokud na fyzickou ochranu není vázána, je pouze otázkou času, kdy dojde k jejímu překonání.

K prostředkům technické ochrany patří mechanická zařízení, elektronická zařízení a technické prostředky režimových opatření.

Mechanickou obranou rozumíme prvky, prostředky nebo celé systémy, které znesnadňují proniknutí do chráněného objektu či k chráněné osobě.

Do mechanické obrany řadíme :

- mechanické zábranné systémy obvodové – oplocení, brány, závory, zastavovací pásy, retardéry, turnikety,
- mechanické zábranné systémy plášťové ochrany – mříže, rolety, ochranné folie, bezpečnostní skla a dveře s příslušným kováním, bezpečnostní zámky s cylindrickými

vložkami a celými bezpečnostními uzamykacími systémy.

- mechanické zábranné systémy předmětové ochrany - trezory, ohnivzdorné a kartotéční skříně, manipulační schránky a příruční pokladničky
- ostatní prostředky ochrany - speciální ochrana chemická a fyzikální předmětů a dokumentů (plomby, pečetě, vodoznaky, hologramy, kolky, horká ražba fólií). Tato technika slouží především k ochraně proti napodobeninám a padělkům písemností a dokumentů.

Elektronickou ochranou rozumíme ochranu pomocí elektrických prvků, zejména pomocí zabezpečovací a požární signalizace, střežících televizních okruhů, přístupových a biometrických identifikačních systémů.

Fyzická ochrana patří mezi nejstarší formy ochrany. Je prováděna zaměstnanci státní správy nebo na základě smluvního vztahu mezi úřadem a soukromou bezpečnostní agenturou v závislosti na tom, s jakými materiály se na daném místě pracuje. Podle toho může být fyzická ochrana ozbrojena či neozbrojena, případně uniformovaná či skrytá. Jejím úkolem je provádět ochranu dohledovou, doprovodnou, víceúčelovou nebo jen stacionární ať už v době pracovní doby úřadu či nepřetržitě či nárazově podle potřeby. Podmínky nasazení fyzické ochrany v rámci bezpečnosti objektu jsou stanoveny právním předpisem. Stanoviště stálého výkonu fyzické ostrahy objektu je určeno ve výstupu hlášení technických prostředků ochrany. Povinnosti těchto pracovníků jsou popsány v Pravidlech pro výkon fyzické ostrahy objektu a jsou součástí Provozního řádu objektu, ve kterém jsou popsána i režimová opatření.

Režimová ochrana je sjednocujícím a řídícím prvkem zabezpečovacího systému objektu. Režimová opatření tvoří soubor procesů, které obsahují režim vstupu, výstupu a pohybu osob, vjezdu, výjezdu a pohybu dopravních prostředků. Tato opatření se týkají i pohybu utajovaných informací v objektu, manipulace s identifikačními prostředky, médii i klíči, které se používají k zabezpečení vstupů a manipulaci s technickými prostředky.

K ochraně bezpečnosti objektu je stanovena příslušná dokumentace, která musí být vedena. Jedná se o Provozní řád a Krizový plán ochrany objektu.

Provozní řád objektu zavazuje všechny osoby, které jsou oprávněny do objektu vstupovat, k pohybu podle určitých pravidel, stejně tak i návštěvy v objektu. Písemnou podobu mají i Pravidla pro režim pohybu utajovaných předmětů a materiálů v objektu. Provozní řád zpracovává i provozní dokumentaci k technickým prostředkům a pokyny pro užívání těchto prostředků (provozní kniha, návod k obsluze elektronických zabezpečovacích systémů), stanovuje pravidelné kontroly funkčnosti technických prostředků apod. Provozní řád popisuje také režimová opatření pro ochranu oblastí Tajné a Přísně tajné, v nichž jsou pravidelně projednávány utajované informace. Do provozního řádu patří i Pravidla pro manipulaci s klíči, popřípadě s identifikačními prvky elektronické kontroly vstupu, od vstupů do objektu a zabezpečených oblastí a s klíči od úschovných objektů. Popis způsobu kontroly osob a dopravních prostředků, způsob provádění namátkových vstupních a výstupních prohlídek, způsob reakce ostrahy na poplachové hlášení technických prostředků i způsob provádění obchůzek je dán Pravidly pro výkon fyzické ostrahy.

Pokyny k ochraně utajovaných informací v případě vzniku mimořádné situace jsou popsány Krizovým plánem ochrany objektu. Tyto pokyny určují sled činností v případě vzniku požáru, havárie rozvodu vody nebo plynu, v případě napadení objektu nebo v případě sabotáže či při teroristickém vyhrožování.

Veřejná správa vzhledem k ochraně utajovaných informací je povinna vypracovat kromě Provozního řádu objektu, Krizového plánu ochrany, Pravidel pro výkon ostrahy objektu, Technické dokumentace objektové bezpečnosti, Bezpečnostního projektu ochrany objektu. Spisového a skartačního řádu ještě Dokumentaci o zajištění bezpečnosti informačních systémů nakládajících s utajovanými informacemi o provádění jejich certifikace a náležitostech certifikátu.

Je tedy tím zřejmé, že nesmíme zapomenout na ochranu informačních systémů. Kromě informačních systémů se certifikují NBÚ nebo jimi pověřenou organizací i kryptografické prostředky užívané k ochraně utajovaných informací. Při certifikaci musí dojít ke shodě technických i kryptografických prostředků i informačních systémů s bezpečnostními parametry.

Informační systémy mohou mít formu písemnou, počítačovou i kombinovanou. Informace v nich mohou být textové, grafické i různě strukturované. Tyto systémy mohou

být určeny pro jedince i celá pracoviště, ale Úřad národní bezpečnosti vždy stanoví minimální požadavky v oblasti počítačové bezpečnosti. Bezpečnost softwarových prostředků musí být kontrolována tak, aby vždy bylo možno identifikovat uživatele. Je důležité chránit programové prostředky proti virům, proti zneužití softwaru i proti poškození či zničení programového vybavení. Mezi jednotlivými částmi komunikačních systémů musí být dodržena jejich bezpečnost, ať už fyzickou ochranou, tzn. zajištěním oprávněnosti přístupu k informacím, nebo ochranou aktivní správným výběrem zaměstnanců.

Kryptografická ochrana souvisí s bezpečností informačních systémů. Při zpracování, přenosu, ukládání a archivování utajovaných informací je možno použít kryptografické metody v informačních systémech. Úřad národní bezpečnosti ověřuje odbornou způsobilost pracovníků kryptografické ochrany utajovaných informací. Zároveň NBÚ stanoví právním předpisem, jaké kryptografické prostředky mohou být používány, a eviduje je stejně jako používání klíčových materiálů.

Velice důležitým dokumentem ve státní správě, který slouží k ochraně informací, je Spisový a skartační řád. Spisový a skartační řád tvoří souhrn předpisů pro vedení spisové služby. Cílem řádu je sjednotit manipulaci s dokumenty. Spisový řád stanoví zásady oběhu dokumentů, systém jejich posuzování a schvalování a zejména jejich způsob předávání, tzn. kopírování, ukládání a postupy v případě ztráty.

Nedílnou součástí spisového a skartačního řádu je spisový a skartační plán. Podle důležitosti agendy je dokument označen skartačním znakem A, S nebo V, a tím je zařazen k uložení do archivu nebo navržen k likvidaci po uplynutí skartační lhůty. Skartační lhůtu – dobu, po kterou zůstává dokument uložen, nelze zkracovat, neboť je závazná.

Ve spisovém řádu je uvedeno i jak manipulovat s dalšími administrativními pomůckami jako jsou razítka, kopírovací papíry, barvící pásky, magnetická média apod.

Spisový a skartační řád je součástí administrativní bezpečnosti ve veřejné správě. Administrativní ochrana je tvořena celým systémem opatření za účelem ochránit utajované informace. Úřad proto stanoví požadavky k manipulaci s utajovanou písemností – její příjem, evidenci, čísla jednací, předávání, odesílání a přepravu stejně jako její ukládání, výpůjčky, zabezpečení a vyřazování. V souvislosti s administrativní ochranou se k manipulaci s utajovanými písemnostmi vytvořili administrativní pomůcky, které zajišťují

informace o tvorbě a pohybu písemností, kam můžeme zařadit jednací protokoly, manipulační a zápůjční knihy apod. Pro přenášení a ukládání utajované informace slouží přenosné schránky a úschovné objekty. Písemnost poskytovaná do zahraničí a ze zahraničí musí mít příslušné náležitosti.

Režimová ochrana v sobě zahrnuje organizační, administrativní a věcná opatření, která směřují k zajištění fungování celého zabezpečovacího systému objektu.

Vnitřní ochraně úřadu je často věnována pozornost menší, přestože se zabývá ochranou vnitřních, ale i vnějších vztahů. Soustřeďuje se zejména proti nedovolenému podnikání zaměstnanců. Zaměřuje se na informační činnost pro potřeby personalistiky a také na ochranu vnějších vztahů proti úniku informací.

1.3 Charakteristika personální bezpečnosti

„Personální bezpečnost je základním druhem zajištění ochrany utajovaných informací. Kromě ověřování podmínek, které musí fyzická osoba splnit, aby jí byl umožněn přístup k utajované informaci, zahrnuje personální bezpečnost i výchovu těchto osob. Za zajištění proškolení fyzických osob, které mají přístup k utajované informaci, ručí odpovědná osoba. Ta je povinna jednou ročně zajistit u osob, které mají přístup k utajované informaci, proškolení z právních předpisů v oblasti ochrany utajovaných informací.

Způsob a rozsah ověřování podmínek, které musí fyzická osoba splnit, aby jí byl umožněn přístup k utajované informaci, se liší podle stupňů utajení, k nimž má mít fyzická osoba přístup.“[2]

U personální bezpečnosti nejde o nic jiného než o vhodně prováděný výběr zaměstnanců a smluvních partnerů včetně následného uplatnění zásad, které mají co nejvíce snížit pravděpodobnost, že se setkáme s tzv.“vnitřním nepřítelem“ tváří v tvář. Zní to vcelku jednoduše, ale realita je v tomto případě od teorie velmi odlišná.

Přitom je to jednoduché. Musí dostatečně záležet na výběru osob pracujících s informacemi. Člověk uvnitř má informace o systému, které externí útočník nemůže nikdy získat. „Insider“ se podílí na vytváření systému a denně s ním pracuje. Ví, kde jsou jeho slabiny i silné stránky. Ví, jak má bezpečnost fungovat a jak ve skutečnosti funguje. Kromě znalostí může mít ovšem vnitřní nepřítel i silnou motivaci. Pokud se na pracovišti vyskytnou spory s nadřízenými či kolegy, zneuznání, ukončení pracovního poměru, potom

se každý člověk snaží zvýšit svoji cenu na trhu práce a stát se tak důležitým. Externí útočník je naproti tomu zpravidla veden jen zvědavostí nebo zejména je finančně motivován.

Nejde přitom o nikterak nový problém. Už v 80. letech minulého století americká FBI upozorňovala na to, že osm z deseti incidentů vzniká uvnitř systému. Stojí za nimi lidé, kteří s tímto informačním systémem přímo pracují. Současné průzkumy stavu bezpečnosti ukazují v podstatě totéž.

Prvním pravidlem při přidělování přístupu uživatelům i při samotném výběru zaměstnanců, kteří budou informační systém používat, je jejich prověření. Prověřování nově přijímaného pracovníka závisí na tom, jakou činnost bude vykonávat. Někdy stačí reference z bývalého zaměstnání, výpis z trestního rejstříku, psychologický posudek. Tyto požadavky mohou ještě pak rozvíjet dodatky k pracovní smlouvě o odpovědnosti a povinnostech zaměstnance. Speciální požadavky jsou pak definovány pro práci s utajovanými informacemi zákonem 412/2005 Sb. o ochraně utajovaných informací a

o bezpečnostní způsobilosti.

Podmínky pro jednotlivé stupně utajení, které musí fyzická osoba splňovat, jsou závislé na tom, zda se jedná o stupeň utajení Vyhrazené, Důvěrné, Tajné nebo Přísně tajné.

Pro všechny stupně utajení musí osoba splňovat věkovou hranici minimálně 18 let, být bezúhonná a být způsobilá k právním úkonům. Osvědčení pro stupně Důvěrné, Tajné nebo Přísně tajné může získat osoba, která má státní občanství České republiky, země EU, NATO a musí být osobnostně způsobilá a bezpečnostně spolehlivá.

Splnění těchto podmínek je kontrolováno příslušným bezpečnostním zařízením podle toho, kam se uchazeč hlásí o přijetí (například Ministerstvem vnitra u příslušníků policie).

Zjišťování osobní způsobilosti žádající osoby k nakládání s utajovanými informacemi obsahuje zpracování posudku žádajících osob na základě psychologického vyšetření, bezpečnostního dotazníku a dalších podkladů. Zákon specifikuje také akreditovaná odborná pracoviště, která mohou vykonávat příslušná vyšetření. Při psychologickém vyšetření sleduje vyšetřující psycholog jednotlivé faktory ovlivňující chování lidí jako je intelekt, motivace, hodnoty a postoje posuzované osoby.

Ústřední úřady státní správy zpracovávají každý rok do 31. října podle §72 zákona 412/2005 Sb. personální projekt, který zasílají Národnímu bezpečnostnímu úřadu a hodnotí v něm stav personální bezpečnosti za předchozí období. V tomto projektu také navrhují počet osob, které by měly projít v nadcházejícím roce bezpečnostními prověrkami.

Vláda ČR schválila svým usnesením ze dne 16. února 2011 změnu termínu zasílání personálního projektu vždy do 31. července příslušného kalendářního roku a tento dokument postoupila k projednání Poslanecké sněmovně Parlamentu ČR. Důvodem této úpravy je, že projekty jsou pak předkládány NBÚ s jeho vyjádřením vládě ke schválení vždy do 30. listopadu kalendářního roku.

1.4 Základní pojmy v personální bezpečnosti

Utajovaná informace

Manipulací s utajovanými informacemi by mohlo dojít k újmě zájmů ČR nebo k újmě zájmů, k jejichž ochraně se Česká republika zavázala. Pokud by došlo k nesprávnému stanovení stupně utajení, považujeme i toto za neoprávněné nakládání s utajovanou informací. Seznam utajovaných informací je vydáván jako nařízení vlády ČR a na návrh ústředních orgánů státní správy ho zpracovává Národní bezpečnostní úřad.

Národní bezpečnostní úřad je orgánem státní správy a zajišťuje jednotné provádění ochrany utajovaných informací v České republice a nad touto ochranou vykonává nejen státní dozor, ale vydává i metodické pokyny k provádění např. bezpečnostních prověrek fyzických osob i organizaci a posléze vydává příslušná potvrzení a osvědčení.

NBÚ provádí i další činnosti stanovené zákonem jako například vydávání vyhlášek nebo vedení spisů k bezpečnostním prověrkám. Vzhledem k tomu, že NBÚ je ústředním správním úřadem, je oprávněn získat i potřebné informace u státních orgánů, které jsou nezbytné pro plnění povinností a úkolů NBÚ.

Předmětem ochrany utajovaných informací bývají informace z mezinárodních jednání, krizové plánování, stav zabezpečení ochrany utajovaných informací a elektrotechnický systém ochrany objektů, ve kterých se informace nalézají. V jednotlivých rezortech se navíc můžou vyskytovat další utajované informace.

Poučení

Před prvním seznámením s utajovanou informací podepisuje fyzická osoba písemný záznam o seznámení s jejími právy a povinnostmi v oblasti ochrany utajovaných informací a s následky jejich porušení. Dokument - poučení podepisuje zároveň i odpovědná osoba, která poučení provedla.

Osvědčení fyzické osoby

Pokud fyzická osoba splnila podmínky přístupu k utajované informaci, získává osvědčení a poté může vykonávat určitou činnost. Vzhledem k tomu, že tento dokument se vydává jako trojjazyčný, je možno ho použít ve všech orgánech EU. Platnost osvědčení je 9 let (Důvěrné), 7 let (Tajné), 5 let (Přísně tajné) - podle §54, §55, §56 zákona.

Bezpečnostní řízení

Národní bezpečnostní úřad zajišťuje tento proces k ověření, zda osoba – účastník bezpečnostního řízení splňuje podmínky pro vydání osvědčení fyzické osoby. Specifické úkony v tomto řízení jsou dány §107 zákona 412/2005 Sb.

Odpovědná osoba

Odpovědná osoba za výkon určitých opatření v oblasti utajovaných informací splňuje zákonem daná ustanovení. Tomuto subjektu je podřízen i bezpečnostní ředitel, jehož funkce je nezbytně nutná u orgánu státu, u něhož vzniká utajovaná informace nebo kterému je poskytnuta, dále u právnických nebo fyzických osob, které mohou přijít do styku s utajovanou informací. Do 15 dnů od vstupu do funkce bezpečnostního ředitele musí být písemně informován i NBÚ o konkrétní osobě, kterou může být i sama odpovědná osoba.

Odpovědnou osobou rozumíme např. ministra u ministerstev, guvernéra České národní banky, ředitele Bezpečnostní informační služby, ředitele krajského úřadu, ředitele magistrátu hlavního města Prahy, tajemníka magistrátu statutárního města, tajemníka nebo starostu dalších měst a obcí.

Rozklad

Pokud účastník bezpečnostního řízení nesouhlasí s rozhodnutím a v závěru příslušného rozhodnutí je uvedena možnost podání rozkladu, může prostředku využít a domoci se opravného prostředku.

Určené osoby ze zákona

Mezi určené osoby pro všechny stupně utajení se stávají dnem svého zvolení nebo jmenováním do funkce prezident republiky, předseda Poslanecké sněmovny, předseda Senátu, členové vlády, prezident, viceprezident a členové Nejvyššího kontrolního úřadu. Soudci, Veřejný ochránce práv a zástupce Veřejného ochránce práv.

Určenými osobami jsou pouze po dobu výkonu funkce a pro účely jejího výkonu.

2 IDEÁLNÍ STAV ZABEZPEČENÍ OBJEKTŮ VEŘEJNÉ SPRÁVY

2.1 Úvod

Vzhledem k tomu, že personální bezpečnost má zajišťovat i ochranu fyzických osob, které mají umožněn přístup k utajovaným informacím, zaměřil jsem se v této části na zabezpečení objektů. Bezpečností objektů je zajištěna z velké části i bezpečnost osob, které se v nich nacházejí a samozřejmě je bezpečností objektu zajištěna i bezpečnost dat vůči vnějšímu napadení.

Zabezpečení objektu vždy záviselo a záviset bude na objemu financí, které můžeme tomuto úkolu věnovat. Čím menší oblast daný úřad spravuje, tím méně prostředků může na zabezpečení vynaložit. Proto se setkáváme s budovami místních a městských úřadů, které nejsou dostatečně zabezpečeny.

V této části práce bych se chtěl věnovat ideálnímu stavu zabezpečení objektů veřejné správy.

Bezpečnostní systém by měl být kombinací mechanických zábranných systémů a elektronických zabezpečovacích systémů, ve kterém by hrála svou roli i fyzická ochrana objektu sladěním všech bezpečnostních pravidel pomocí nastavení režimu ochrany. Aby byla preventivní bezpečnost účinná, musí být založená na komplexnosti, odbornosti, rychlosti a součinnosti veškerých bezpečnostních opatření. Základem každého zabezpečení objektu jsou mechanické zábrany jako bezpečnostní dveře, zámky, fólie, trezory, mříže, ale i kvalitní mechanický zábranný systém musí být doplněn elektrickou bezpečnostní signalizací a televizními střežícími systémy.

„Každá elektronická zabezpečovací signalizace neobstojí pouze se signalizací lokální (siréna, maják), ale je třeba signál vyvést na pult centralizované ochrany objektu a to buď Policie ČR, obecní policie, ale zejména soukromých bezpečnostních služeb (SBS).“[3]

Samozřejmě je důležité po instalaci všech bezpečnostních součástí řádně proškolit obsluhu bezpečnostního zařízení, aby dokázala včas a správně zareagovat na daný signál.

2.2 Mechanické zábranné systémy

Mechanické zábranné systémy jsou založeny na mechanických prvcích, které oddálí proniknutí neoprávněné osoby do objektu. Každý takový systém je překonatelný v určitém čase, ale důležitá je doba překonání. Doba pro překonání mechanického zábranného systému je určena nejen kvalitou tohoto systému, ale i znalostmi osoby, která se snaží systém překonat a také tím, jaké má narušitel možnosti použití techniky k překonání zábranného systému. Každý MZS má svou průlomovou odolnost, tj. minimální čas, který musí člověk vynaložit k překonání systému. Tento čas by měl být dostatečný k tomu, aby bylo možno mobilizovat další zábranný systém např. fyzickou kontrolu.

Vhledem k tomu, že úřady samospráv veřejné správy většinou nevyužívají obvodové mechanické zábranné systémy (oplocení, brány, závory, zastavovací pásy, retardéry, turnikety), zaměřil jsem se na mechanické zábranné systémy plášťové ochrany objektů.

Základním mechanickým prvkem plášťové ochrany jsou dveře a bezpečnostní úpravy dveřního prostoru. Zárubeň dveří se v rámci bezpečnosti zhotovuje z ocelových profilů a důležité je ji správně usadit do ostění, tak aby se dveře staly odolnými proti vyražení či prořízнutí nebo páčení. Ke zvýšení bezpečnosti dveří se používají bezpečnostní zámky s cylindrickými vložkami, ale můžeme rozšířit počet odolných zámků po celém obvodu, případně užít celé bezpečnostní uzamykací systémy.

Často překonávaným prvkem vstupu do objektů jsou okna. Pokud mají okna bezpečnostní mříže správně ukotvené a se správnou velikostí ok a současně mříže se v konstrukci neprohýbají, jsou vhodně zabezpečena. Jsou-li bezpečnostní mříže zkombinovány s bezpečnostními skly nebo alespoň s bezpečnostními foliemi, průlomová odolnost oken se navýší.

Jako ochrana proti vniknutí mohou sloužit tvrzená skla, případně skla s bezpečnostní fólií, která zvýší odolnost proti nárazu až třikrát. K ochraně proti násilným vniknutím se spíše užívají vrstvená bezpečnostní skla, která se vyrábějí plošným spojením několika vrstev skla s jednou nebo více vrstvami fólie. Je jasné, že čím sklo bude mít větší tloušťku, tím je odolnější, a tím může sloužit i proti prostřelení či výbuchu.

Hlavní výhodou bezpečnostní fólie je možnost dodatečného umístění na sklo a dále její nenápadnost. Fólie můžeme instalovat na skla minimální tloušťky 3 mm. Přestože tloušťky bezpečnostních fólií bývají desetiny milimetru, mohou zamezit prohození cizích předmětů

do vnitřní části objektu. Pokud se tlakovou vlnou sklo rozbije, nehrozí vysypání střepů a sklo nadále zůstane neprostupnou překážkou pro útočníka.

Důležité materiály lze chránit v trezorech, které jsou vyrobeny ze speciálního materiálu odolného proti vloupání. Jedná se většinou o dvouplášťovou konstrukci ze speciálních slitin silnou 80–150 mm. Skříňové trezory mají v uzavřeném stavu délku alespoň jedné vnitřní strany větší než 1 m. Naproti tomu komorové trezory jsou pevné celky uvnitř objektů a jsou osazeny speciálními vstupními dveřmi o tloušťce 20-50 cm, jejichž průlomová odolnost je shodná s průlomovou odolností stěn. Bezpečnost při otvírání komorového trezoru může být zvýšena přítomností více osob kvůli vzájemné kontrole, kdy každá osoba vlastní jiný klíč potřebný k otevření.

Trezory jsou ideálně zabezpečeny ještě kombinací s elektronickými zabezpečovacími systémy, časovými spínači, trezorovými detektory a případně jsou snímány kamerovými přístupovými a záznamovými systémy.

K ochraně papírových materiálů, datových médií jsou vyrobeny z ocelových nehořlavých materiálů ohnivzdorné skříně. Tyto skříně jsou dvouplášťové s prostřední vrstvou, kterou tvoří popel nebo písek. Mezi nejnovější ohnivzdorné skříně kombinované s bezpečnostní třídou patří takové, které mají zabezpečení pro datová média a jsou chráněny zároveň čtyřstranným zavíráním, které se užívá pro bezpečnostní třídu 1. Při zkoušce požární odolnosti po dobu 1 hodiny byla okolní teplota 1090° C, a přesto vnitřní teplota nepřesáhla maximální přípustnou hranici 30° C. Této vlastnosti je dosaženo nejen výběrem materiálu, ale zejména tím, že centrální dveře i kompletní tělo trezoru jsou třístěnné. [1]

2.3 Elektronické zabezpečovací systémy

Úlohou elektronických zabezpečovacích systémů je zvyšovat efektivnost fyzické ochrany a přenášet poplachový signál do místa se stálou obsluhou. Jejich úkolem je dodat včas informaci o porušení bezpečnostních prvků a umožnit rychle fyzické ochraně zasáhnout.

První centrály elektrické ochrany uvedla do provozu firma Hinds&Williams v roce 1853. Ve 20. století se začala využívat elektromechanická čidla založená na principu setrvačnosti. Zpočátku se jednalo o releovou záležitost, později se přešlo k elektronickým čidlům. V druhé polovině 20. století se uplatňovala VKV prostorová čidla, která snímala signál o frekvenci stovek MHz. Pasivní infračervené čidlo se stalo nejúspěšnějším zabezpečovacím

prvkem v 2. polovině 70. let. Nyní jsou využívány biometrické systémy, které jsou založeny na anatomických a fyziologických vlastnostech člověka a slouží k jeho identifikaci, a to zejména v přístupových systémech ACCESS.

Pomocí elektrické zabezpečovací signalizace je zjištěn neoprávněný vstup do chráněného prostoru nebo neoprávněná manipulace s určitou věcí. Celý systém je řízen ústřednou EZS, která má potřebnou certifikaci a pro případ výpadku elektrické energie musí být připojena na náhradní zdroj. Ústředna by měla být bezpečnostně zajištěna proti nežádoucímu otevření. Signál je přenášen na pult centralizované ochrany využitím jednotné telekomunikační sítě radiového signálu nebo pomocí mobilních sítí či linky ISDN.

Ke zjištění narušení lze využít pasivních nebo aktivních detektorů případně detektorů ultrazvukových, akustických, mikrovlnných, detektorů PIR, duálních detektorů, piezoelektrických detektorů či jiných zařízení.

K cenově nejdostupnějším patří detektory pasivní pro vnitřní i venkovní použití a slouží ke zjištění nežádoucího otevírání vstupních otvorů. Jedná se zejména o magnetické kontakty, které vyžadují správně seřízenou citlivost, aby byl vyloučen falešný poplach. Piezoelektrické detektory tříštění skla se lepí přímo na skleněnou plochu pomocí speciálního dvousložkového lepidla, které musí být časově a teplotně stálé a nevytvoří se sklem pružící spoj. Výhodou tohoto detektoru je schopnost zjistit rozbití skla i v klidovém stavu elektrického zabezpečovacího systému.

K prvním prostorovým detektorům patří detektory, které pracovaly na kmitočtové řadě stovek MHz, potom vznikly mikrovlnné detektory pracující v rozsahu 3-12 GHz, ale vždy byly zkonstruovány na principu Dopplerova jevu. Přijímač přijal odražené elektromagnetické vlnění vysílače a kmitočet byl vyhodnocen. Pokud se vysílané vlnění odrazilo od nepohyblivého předmětu, byla odpověď stejná. Při odrazu vlnění došlo ke změně kmitočtu, pokud se objekt pohyboval. Nevýhodou těchto detektorů je průnik vlnění mimo chráněný prostor a při špatném umístění dochází k velkému počtu falešných poplachů. Vlivem digitalizace, lepšího anténního systému a přesunem vlnění do mikrovln 3-12 MHz se mikrovlnné detektory staly velice kvalitním systémem prostorové ochrany. Jejich nevýhodou ovšem zůstalo znečišťování životního prostředí elektromagnetickým zářením. Proto je nutné, aby tento typ detektorů, přestože jsou nejkvalitnější, byl v provozu pouze po dobu nutnou k zabezpečení objektu.

Ultrazvukové vlnění o frekvenci 25-45 KHz využívají detektory v prostoru 8-10 m. Ultrazvukové detektory se používají spíš v kombinaci s detektory PIR u duálních detektorů.

Detektory PIR reagují na vyzařování lidského těla. Signál však může být ovlivněn i pohybem zvířat, reaguje i na teplotní změny způsobené teplým vzduchem, topnými tělesy, ventilací. U detektorů pohybu byla zpočátku užívána pouze zrcadlová optika, ale v současnosti, aby se eliminovaly nežádoucí složky zařízení a bylo odráženo infračervené vlnění o požadované délce, se používá tzv. černé zrcadlo.

K zajištění bezpečnosti místností slouží stropní infradetektory, které jsou méně nápadné než detektory s antimaskingem. Stropním PIR detektorům nevadí různé konfigurace nábytku a tvar místnosti. Jeho poloha vůči snímacím lalokům se mění v závislosti na směru pohybu člověka v místnosti.

Detektory opatřené antimaskingem používáme v místech s vyšším rizikem napadení. Existuje více druhů antimaskingu, které jsou založeny na různých fyzikálních principech, ať už je to vysílání infračerveného záření diodou do prostoru a jeho následný příjem nebo vysílání mikrovlnného záření. Základem je, že pokud se odrazí záření od předmětu maskujícího výhled detektoru, detektor vyhlásí poplach.

Všechna signalizační, přenosová a zapisovací zařízení jsou ovládána z ústředen EZS, které napájejí zařízení elektrickou energií a vyhodnocují výstupní signály z těchto čidel. Kódově zámky nebo elektromagnetické ovládání umožňuje systém EZS uvést do stavu chodu nebo klidu.

Ústředny fungují na principu smyčkového vedení, které je tvořeno rozsáhlou kabelovou sítí se sériovým zapojením rozpínacích kontaktů čidel. Jiná ústředna může pracovat s přímou adresací čidel. Výhodou tohoto systému je, že při narušení konkrétní části objektu ihned víme, které konkrétní čidlo bylo aktivováno, a tím zjistíme, kde přesně k narušení došlo.

K nejmodernějším ústřednám v současné době zařazujeme ústředny pracující v pásmu 433 MHz. Jedná se o ústředny s bezdrátovým přenosem od čidel, jejichž dosah je ve volném prostředí 100 až 200 metrů.

2.4 Fyzická a režimová ochrana

Fyzická ochrana je klíčovou a základní ochranou. Výsledná účinnost všech ostatních druhů ochrany závisí na její úrovni. Základem je fyzická ostraha, která ať už pozorováním nebo kontrolou osob či vozidel zajišťuje bezpečnost objektu.

Vzhledem k tomu, že aspekty výběru fyzické ochrany ve veřejné správě jsem se zabýval již v části 1.2, uvádím pouze některé úkoly, které fyzická ochrana musí splňovat, a jak jsou tyto problémy provázány s elektronickou kontrolou vstupu a režimovou ochranou.

U vchodu by měla být kontrolní propustková služba, která zabezpečuje režim vstupu či vjezdu do objektu a jeho opouštění a tak zabrání vnášení a vynášení předmětů z objektu. Zároveň může působit jako informační služba návštěvníkům, může vést evidenci docházky a odchodů zaměstnanců a návštěv, doprovázet návštěvy v objektu a uzamykat a odemykat určené prostory.

Se vstupem do objektu může být spojena i kontrola osob, jejich evidence, kontrola dokladů či vstupních průkazek. Profesionálnější je určitě metoda přesvědčování a tím odvrácení protiprávního jednání, která působí uklidňujícím dojmem na objekt, než metoda fyzických zábran a bariér, ke které může fyzická ochrana přistoupit až v době nutné obrany nebo krajní nouze.

Kontrola vstupu osob do objektu může být zajišťována fyzickou ostrahou v kombinaci se systémem elektronické kontroly vstupu. Tyto systémy se opírají o různé fyzikální principy. Nejpoužívanějším je bezdotykový systém kontroly přístupu založený na radiofrekvenční identifikaci přenosu signálu. Nejčastěji nosičem bývá identifikační karta s textem a fotografií, do které je vložen 64 bitový kód. Když se ID karta dostane do aktivního pole antény, čtecí zařízení vyšle impuls transpondéru a ten vyšle identifikační kód zpět do snímací jednotky. Karty, které nejsou registrovány v paměti řídícího systému, nemají přiděleno oprávnění a je jim vstup odmítnut. Zároveň je tím vyvolán signál o pokus neoprávněného vstupu a vše další probíhá podle režimových opatření.

Základem celého fungování systému je programové vybavení, které ovládá přístup ke čtení dat. Změny nastavení systému týkající se povolení vstupu musejí odpovídat požadavkům zabezpečovacího systému. Software musí být zabezpečen proti neautorizovanému přístupu a systém vstupu nesmí být zdrojem planých poplachů. Volně přístupné nesmí být ani nastavovací prvky, blokovací zařízení, ani další důležité části

vstupního systému. Ke kopírování nebo rozklíčování informací nemůže dojít, pokud je v systému dostatečný počet kódových kombinací.

Identifikační karty umožňují uživateli vstupovat do prostor jemu zpřístupněných a zároveň kontrolují čas vstupu a výstupu z daného prostoru. Tím je poskytována informace o pohybu osob v objektu a zaznamenáno nejen místo pohybu, ale i čas.

Identifikační karty nebo jiné prvky mohou omezit přístup nepovolaných osob do určitých prostor objektu nebo omezit přístup do prostoru objektu v jiných časových úsecích než je dovoleno. Identifikační karty mohou fungovat jako elektronické hodiny, protože registrují dobu pobytu i polohu. Údaje jsou často zpracovávány pro ekonomické i personální oddělení, protože lze jimi zjistit i vytíženost zaměstnanců, využívání pracovní doby, využívání materiálů a dodržování bezpečnosti při práci s daty a utajovanými informacemi.

Kromě identifikačních karet se mohou využívat biometrické prvky jako např. otisk prstu, které jsou zpracovávány pomocí programového modulu do softwarových aplikací. Ke zpřístupnění prostoru či dat dochází až po ověření shody mezi uloženým vzorkem a nově sejmutou informací k ověření biometrického údaje.

Kromě toho, že fyzická ochrana se podílí na zajištění správného fungování elektronické kontroly vstupu, může plnit další specifické úkoly. Provádět kontrolu stavu signalizačních zařízení protipožární signalizace, zajišťovat ochranná opatření při evakuaci osob, majetku a předmětů obsahujících důležité informace a další úkoly sloužící k zabezpečení chodu objektu.

II. PRAKTICKÁ ČÁST

3 PERSONÁLNÍ BEZPEČNOST VE VEŘEJNÉ SPRÁVĚ A V SOUKROMÉM SEKTORU A JEJÍ POROVNÁNÍ S JINÝMI STÁTY

3.1 Porovnání personální bezpečnosti ve veřejné správě a v soukromém sektoru v ČR

3.1.1 Problematika výběrového řízení

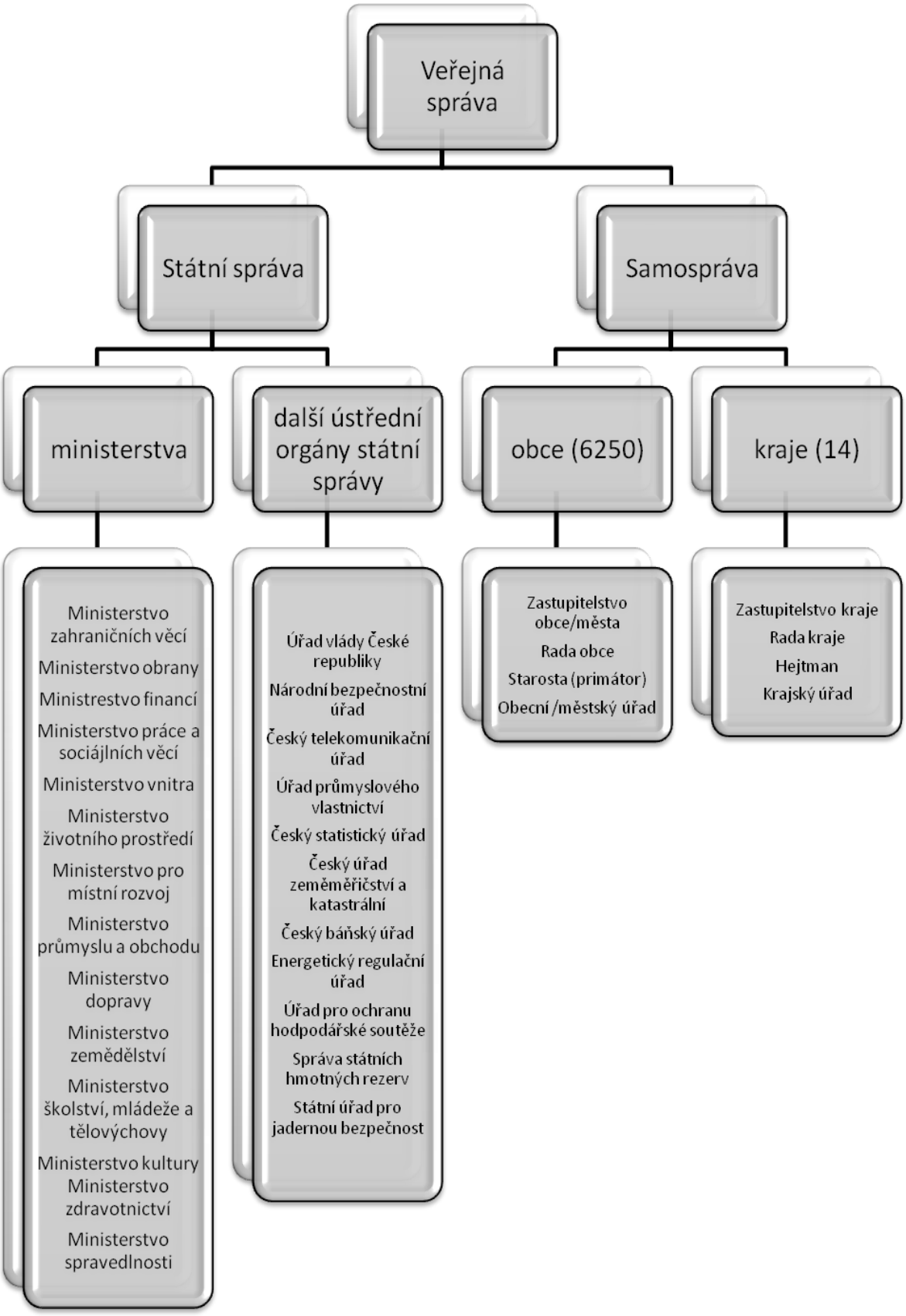
Podstatný rozdíl v personální bezpečnosti ve veřejné správě a v soukromém sektoru není možný. Vždy je personální bezpečnost založena na lidech, kteří jsou vybráni, aby pracovali s informacemi, které mohou poskytnout k zajištění zisku jiné osoby nebo organizace. Soukromé firmy často mohou vynaložit na zajištění fyzické a technické ochrany informací větší finanční částku než úřady veřejné správy, ale podstatnější je výběr osob.

Nejrizikovějším faktorem je totiž vždy lidský faktor. Dojde-li k selhání režimových a administrativních opatření, je to selhání lidského faktoru. Dojde-li k selhání technických opatření, jde o selhání lidského faktoru v některém z článků řetězce projektování - výroba - instalace - servis - obsluha.

Základem je výběr zaměstnanců. Zatímco ve veřejné správě je přijímán zaměstnanec zejména na základě kvalifikace a případně po absolvování psychologických testů, v soukromém sektoru záleží především na kvalifikaci a referencích a teprve později v tomto sektoru probíhají prověrky loajality k podniku. Ovšem již při podpisu pracovní smlouvy je u většiny soukromých organizací uvedena klauzule, že nedodržení loajálnosti k podniku může být důvodem k rozvázání pracovního poměru.

Tyto uvedené skutečnosti jsem zjišťoval konkrétně u několika úřadů samospráv i u soukromých organizací. Několik soukromých firem mi sdělilo, že odpovědi na mnou připravené otázky jsou součástí jejich obchodního tajemství, a proto mi sdělit informace nemohou. U krajských úřadů jsem se setkal s odpovědí, že mi tyto informace nemohou sdělit vzhledem k zajištění bezpečnosti. Proto jsem získané informace mohl porovnávat jen mezi městskými úřady s různou působností a několika firmami.

Pro lepší orientaci v systému veřejné správy jsem vytvořil graf znázorňující systém orgánů veřejné správy.



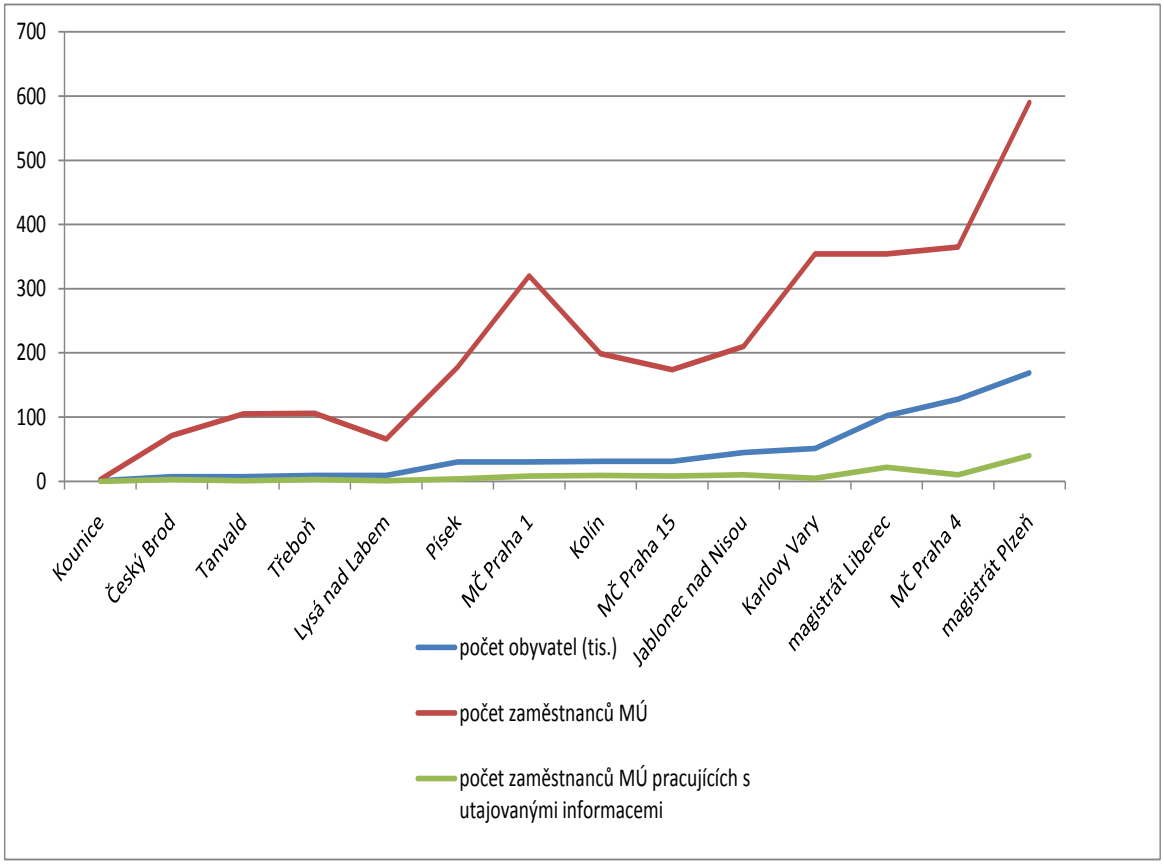
Graf 1. Systém veřejné správy v ČR

Ve veřejné správě jsem nejprve od jednotlivých subjektů zjišťoval počet zaměstnanců úřadu vzhledem k počtu obyvatel spádově patřících k dané správě. Stav obyvatel v dané lokalitě byl zjištěn k 31.12.2010 pomocí portálu veřejné správy ČR. [13]

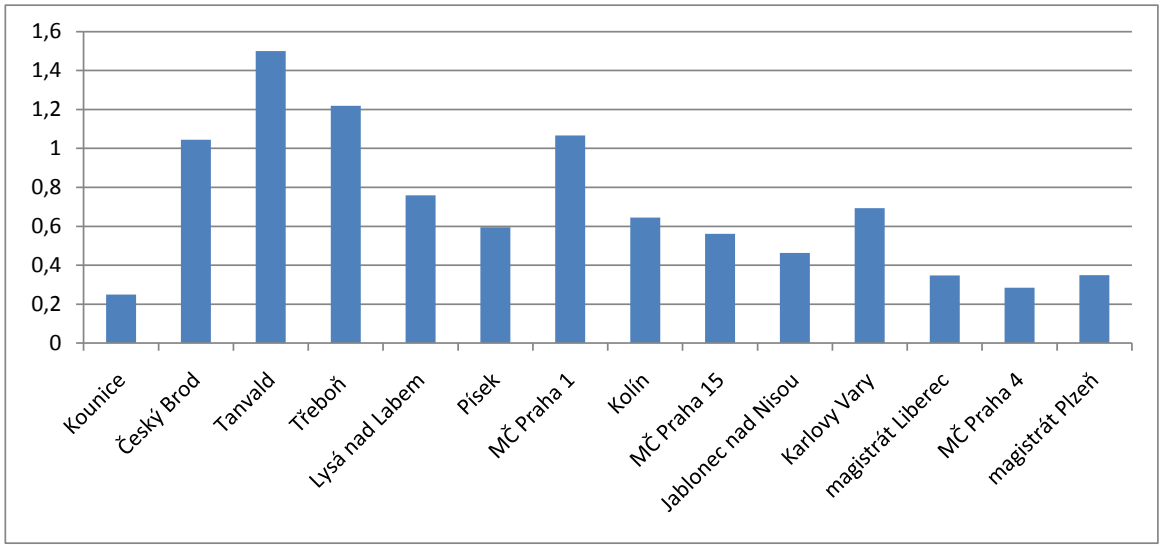
Tato zjištění jsem zapsal do tab. 1. a grafu 2. spolu s počtem zaměstnanců, kteří na daném úřadě pracují s utajovanými informacemi. Zároveň jsem vytvořil graf 3. vyjadřující procentuální závislost počtu zaměstnanců městského úřadu na počet obyvatel spravovaného území a graf 4. vyjadřující procentuální zastoupení zaměstnanců pracujících s utajovanými informacemi vzhledem k celkovému počtu zaměstnanců u jednotlivých městských úřadů.

samosprávní celek	počet obyvatel	počet zaměstnanců MÚ	osoby s osvědčením
Kounice	1 181	3	0
Český Brod	6 822	71	3
Tanvald	6 950	105	1
Třeboň	8 653	106	3
Lysá nad Labem	8 657	66	1
Písek	29 923	178	4
MČ Praha 1	30 002	320	8
Kolín	30 927	199	9
MČ Praha 15	31 015	174	8
Jablonec nad Nisou	45 356	210	10
Karlovy Vary	51 115	354	5
magistrát Liberec	101 865	354	22
MČ Praha 4	128 431	365	10
magistrát Plzeň	168 808	590	40

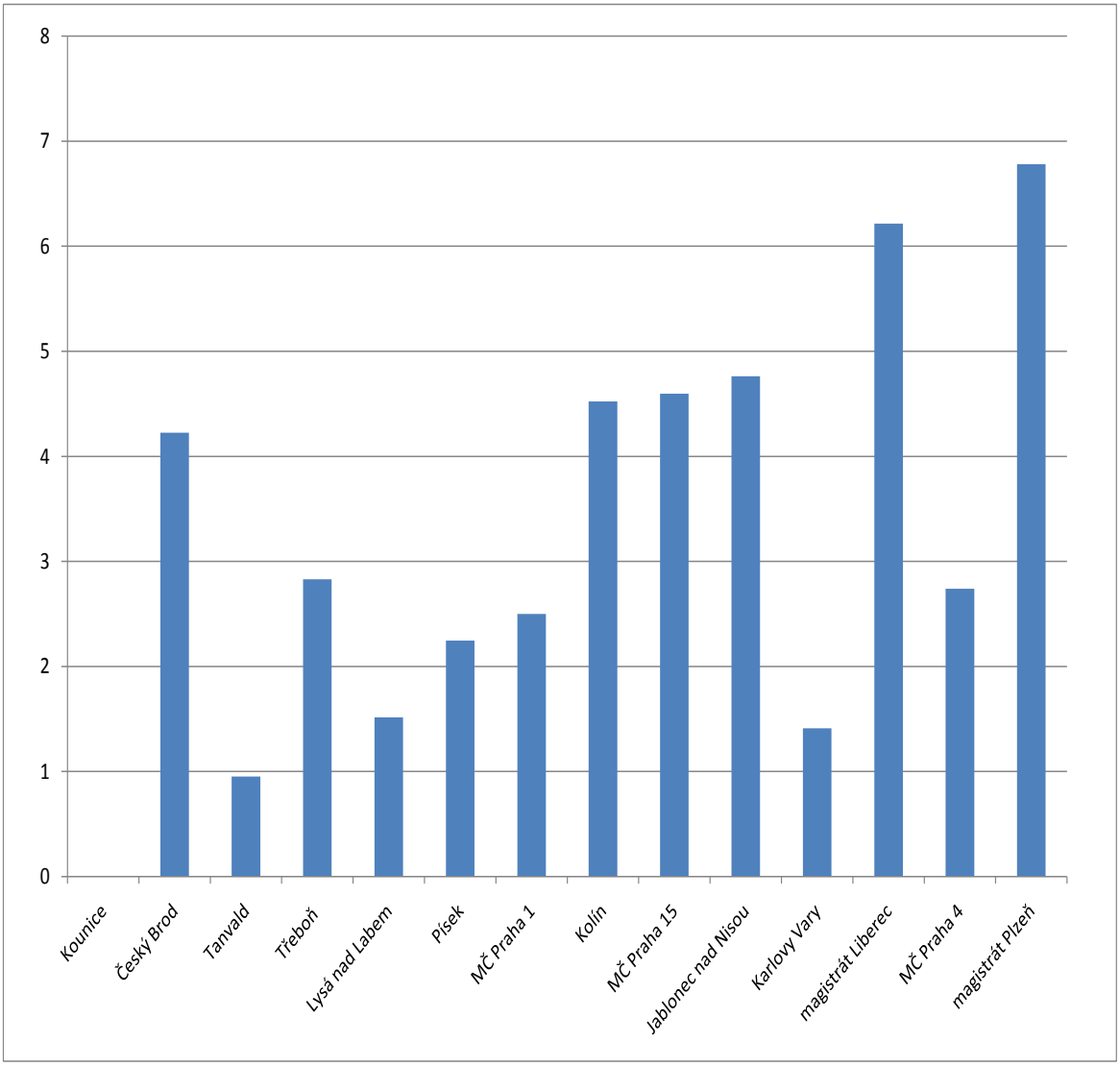
Tab. 1. Přehled zkoumaných samosprávních celků, úřadů samospráv a jejich zaměstnanců



Graf 2. Vyjádření závislosti počtu zaměstnanců MÚ na počtu obyvatel příslušných k danému MÚ



Graf 3. Vyjádření závislosti celkového počtu zaměstnanců samosprávy na počtu obyvatel dané oblasti v procentech



Graf 4. Vyjádření závislosti počtu zaměstnanců s osvědčením k celkovému počtu zaměstnanců samosprávního celku v procentech

Tyto tabulky a grafy nám ukazují, že počet zaměstnanců úřadů samosprávy nezávisí úplně na počtu obyvatel dané oblasti, ale na tom, zda se jedná o úřad s rozšířenou působností.

Porovnáme-li např. města s téměř shodným počtem obyvatel k 31.12.2010 Třeboň a Lysou nad Labem potom zjistíme, že počet zaměstnanců městského úřadu je odlišný, a tedy se liší i počet zaměstnanců těchto samospráv, kteří pracují s utajovanými informacemi. Tímto způsobem bychom mohli porovnávat i Městský úřad v Písku s Úřadem městské části

Praha 1. Při téměř shodném počtu obyvatel je počet zaměstnanců píseckého úřadu poloviční a stejně tak je i poloviční počet osob pracujících s utajovanými informacemi.

Procentuální vyjádření počtu zaměstnanců na počet obyvatel a zároveň procentuální vyjádření počtu zaměstnanců pro práci s utajovanými informacemi v poměru s celkovým počtem zaměstnanců by mohlo být zavádějící, protože ne každý samosprávní celek pracuje se stejnými informacemi. Např. Úřad městyse Kounice zpracovává pouze statistické údaje o obyvatelích obce a vykonává základní činnosti samosprávy, ale občanské průkazy obyvatel obce vydává jiný úřad, a to MÚ Český Brod, proto zaměstnanci Úřadu městyse Kounice nepotřebují ke své práci prověření stupně Vyhrazené.

Ve větších samosprávních celcích musí mít někteří zaměstnanci ke své práci už prověření stupně Důvěrné. Z uvedených úřadů v tabulce mi tuto skutečnost potvrdily úřady, které zároveň v této tabulce vykazují největší počet zaměstnanců s prověřením, tedy se jedná o úřad městské části Praha 4, liberecký a plzeňský magistrát. Tento stupeň utajení je nutný k tomu, aby nedošlo k prosté újmě zájmů ČR, a týká se např. opatření v odhalování celních a daňových podvodů a způsobu zajištění důležitých dokumentů a razítek proti padělání a pozměnění.

Na základě těchto poznatků bychom mohli usuzovat, že přijímání zaměstnanců do úřadů s vyšším počtem lidí, kteří zpracovávají velké množství informací, bude náročnější na vstupní výběrové řízení. Pomocí dotazníku a rozhovorů většinou s vedoucími personálního oddělení nebo tajemníky úřadů jsem zjistil, že přijímání zaměstnanců probíhá téměř všude stejně.

Obecní úřady, které jsou na nejnižším stupni hierarchie veřejné správy, zaměstnávají i osoby, které ani později žádnými testy nemusely procházet. Uvědomme si, že pokud má obec 1000 obyvatel bude stát v čele samosprávy volený starosta, který si ke spolupráci na úřadě zvolí dva zaměstnance, které „dostatečně zná“ ze svého okolí. V těchto malých samosprávních celcích se spíše příjem zaměstnanců blíží soukromému sektoru, protože se předem počítá s loajalitou zaměstnance, neboť v daném místě většinou žije.

Má-li úřad alespoň dva odbory, řídí práci zaměstnanců tajemník, a v tom případě jsou někteří zaměstnanci přijímáni nejen na základě kvalifikace, ale mohou procházet i psychologickými testy. Zároveň se v těchto úřadech může pracovat s utajovanými informacemi, kam patří např. dokumentace významných dopravních staveb, zabezpečení

řidičských průkazů, potvrzení o registraci vozidel a tabulek s registračními značkami vozidel, opatření v oblasti celních a daňových podvodů. V takovém případě musí zaměstnanci splňovat prověrku stupně Vyhrazené.

Tyto skutečnosti jsem zaznamenal do tabulky Tab. 2.

samosprávní celek	personální agentura	vlastní výběrové řízení	kvalifikace	kvalifikace a psychotesty
Kounice	ne	ano	ano	ne
Český Brod	ne	ano	ano	ne
Tanvald	ne	ano	ano	ne
Třeboň	ne	ano	ano	ne
Lysá nad Labem	rok 2005 - 1x jinak ne	ano	ano	ne
Písek	ne	ano	ano	ne
městská část Praha 1	ne	ano	ano	ne
Kolín	ne	ano	ano	ne
městská část Praha 15	ne	ano	ano	minimálně
Jablonec nad Nisou	ne	ano	ano	ne
Karlovy Vary	ne	ano	ano	ne
magistrát Liberec	ne	ano	ano	ne
městská část Praha 4	ne	ano	ano	ne
magistrát Plzeň	ne	ano	ano	ne

Tab. 2. Přehled metod přijímání zaměstnanců v samosprávě

Z tohoto přehledu je zřejmé, že úřady nepoužívají k předvýběru zaměstnanců personální agenturu na rozdíl od většiny soukromého sektoru. Pouze jednou k využití personální agentury došlo na MÚ Lysá nad Labem v roce 2005. Konečné výběrové řízení MÚ musel stejně provést, takže tato spolupráce s personální agenturou úřad neadekvátně finančně zatížila, a proto od ní ustoupili.

Výběr zaměstnanců na určitou pozici u samospráv probíhá vlastním výběrovým řízením. Standardně probíhá nejprve na základě životopisu, kde nejdůležitějším aspektem se stává kvalifikace. Dále se rozhoduje na základě řízeného rozhovoru a dalšího doporučení. Někdy se ještě může uplatňovat na základě uchazečem napsaného testu grafologická analýza. Ovšem zjištěná kriteriální validita je u referencí slabá. U rozhovorů závisí validita na druhu rozhovoru a u grafologické analýzy není validita žádná. [10]

V soukromém sektoru se často využívá předvýběru personální agenturou. Tím se výběr zaměstnanců může stát službou a následně obchodem mezi firmou a personální agenturou, ve kterém se uplatňují relativně vysoké finanční objemy. Jak jsem již dříve uvedl, veřejná správa si většinou tento předvýběr právě z hlediska finančního dovolit nemůže.

Vlastní výběr firmou probíhá většinou za přítomnosti manažera, který s přijatým zaměstnancem bude spolupracovat. Zástupce firmy vede se zájemcem vstupní rozhovor, a pokud užije v situačním rozhovoru Flanaganovu metodu kritických případů, může tím být nahrazena i práce psychologa, který tuto metodu také uplatňuje.

V podstatě vždy se jedná o základní otázky – umět práci, být ochoten se zdokonalovat a spolupracovat s týmem, tzn. koordinovat svůj postup podle požadavků celku a dát se řídit.

Větší firmy uplatňují na obsazení významných firemních pozic i různé psychologické testy.

Psychologické testy umožňují zkoumat a prakticky využít předpokladu, že lidské chování, myšlení a prožitek spolu vzájemně úzce souvisí. Psychologický test je objektivním měřením standardizovaného vzorku chování a není závislý na rozdíl od řízeného rozhovoru na osobě, která měření provádí. Ve státní správě i v soukromém sektoru se osobnostní testy provádí především formou dotazníků. Ovšem i při jejich užívání je důležité dbát zejména na ochranu osobnosti a ochranu osobních údajů.

„Používání psychologických testů umožňuje, aby psycholog nebo instituce získávali a shromažďovali citlivé údaje o jednotlivcích. Takové údaje se samozřejmě dají zneužít. Navíc se tyto údaje získávají způsobem, nad kterým nemá testovaná osoba kontrolu – když vyplníte test, sotva můžete tušit, co z vašich odpovědí může psycholog usoudit.“[4]

Morálně správné je požadovat informovaný souhlas testované osoby, aby věděla, že budou řešeny její povahové vlastnosti a poznávací schopnosti.

Vzhledem k tomu, že existují rozdíly v pojetí výběru u psychologů a personalistů, nejideálnější je užití Assessment Centre. Je to konfrontace několika postupů, které se mohou použít i k posuzování lidí, kteří již v organizaci pracují a výsledky této metody mají rozhodnout o jejich služebním postupu.

Assessment Centre je většinou několikadenní záležitost, kdy skupina nejlépe šesti uchazečů je posuzována dvěma až šesti hodnotiteli. Důvodem účasti skupiny je například užití simulované týmové práce.

Bezpečnostní opatření v personální oblasti se odvíjejí také od počtu zaměstnanců, které firma má. Firma s menším počtem zaměstnanců má tu výhodu, že lidé o sobě více vědí, jsou k sobě ohleduplnější, a málokdo si dovolí zklamat. Například firma Simpre s.r.o., která má jen tři stálé zaměstnance a další osoby zaměstnává jen dle potřeb zakázky, si tyto dočasné spolupracovníky vybírá pouze podle kvalifikace a finanční kalkulace. Provádění jakýchkoliv jiných prostředků výběrového řízení je totiž bezpředmětné, protože pokud jejich činnost se neztotožní s představou firmy, firma je k další spolupráci neosloví.

Další firma, která mi poskytla potřebné informace k jejich personální politice, byla firma Silvaco, a.s., pobočka v Praze. Tato pobočka má 35 zaměstnanců, u kterých v přijímacím řízení sehrála hlavní roli jejich kvalifikace a praxe. Při výběrovém řízení je někdy využívána práce personální agentury, jindy se koná pouze vlastní výběrové řízení firmou v závislosti na tom, o jakou pozici ve firmě se jedná. Nikdy prozatím nepoužili metodu Assessment Centre ani při výběru osob na postup ve firmě.

Při vyšším počtu zaměstnanců už musí být vedena dobrá personální politika, i když i ta může třeba při 100 zaměstnancích selhat. O to důkladnější musí být výběr uchazečů na pozici ve firmě.

Jednou z větších firem je Sipral, a.s., která zaměstnává 142 osob, ať už ve výrobě nebo v administrativě. Tím je také dán různý přístup k přijímacímu řízení. U zaměstnanců výroby se přihlíží zejména k jejich kvalifikaci a zkušenostem, u zájemců o práci, kteří mají přijít do styku přímo s obchodními a personálními informacemi se využívá i osobnostních testů. Většinou nábor probíhá přes personální agenturu a teprve potom dochází k vlastnímu výběru firmou. Zaměstnancům, u kterých se uvažuje o dalším profesionálním postupu, se umožňuje stálé vzdělávání a k výběru někdy volí i metodu Assessment Centre.

3.1.2 Problematika dalších aspektů personální bezpečnosti

Samozřejmě, že je nejdůležitější personální výběr zaměstnanců všech subjektů, ale existují i další prostředky, které snižují riziko úniku informací ze subjektu. Všechny subjekty mají snahu, aby jejich zabezpečení proti úniku informací o osobních údajích,

obchodním tajemství i o režimových opatřeních při zvláštních skutečnostech bylo optimální a blížilo se co nejvíce ideálnímu stavu. Stav zabezpečení ovšem nejvíce záleží, pomineme-li vlastní zaměstnance, na finančních možnostech subjektu a na předpisech, které je nutno dodržet.

Zjištěné skutečnosti z úřadů samospráv jsem uvedl do tabulky tab. 3.

samosprávní celek	vzdálenost policie od MÚ	hlídací služba	vstupní karty	CCTV	čidla
Kounice	velká	ne	ne	ne	ne
Český Brod	malá	ne	ne	ano	ano
Tanvald	malá	ano	ne	ne	ano
Třeboň	v budově	ne	ne	ano	ano
Lysá nad Labem	v budově	ano	ne	ano	ano
Písek	malá	ne	ne	ano	ano
MČ Praha 1	velká	ano	neuvádí	ano	ano
Kolín	malá	ano	ne	ano	ano
MČ Praha 15	velká	ano	ne	ano	ne
Jablonec nad Nisou	malá	ano	ne	ano	ano
Karlovy Vary	malá	ne	ne	ano	ano
magistrát Liberec	malá	ne	ne	ano	ano
MČ Praha 4	v budově	ano	neuvádí	ano	ano
magistrát Plzeň	malá	ne	neuvádí	ano	ano

Tab. 3. Přehled některých bezpečnostních prvků používaných na úřadech

Zaměstnanci úřadů vstupují do objektů bez vstupních karet. Jedinou výjimku tvoří zaměstnanci MČ Praha 4. Tento stav je zřejmě dán větší finanční náročností vstupních karet než přístupových klíčů. V tom spatřuji velký rozdíl proti zabezpečení objektů soukromého sektoru. Většina moderních firem vstupní karty používá, aby zjistila skutečnou přítomnost zaměstnanců i jejich pohyb v objektu a zároveň, aby zabránila vstupu nepovolaným osobám. O to lépe musí být zajištěna fyzická ostraha úřadů.

Z těchto údajů je patrné, že hlídací služba, kterou mohou zajišťovat jak bezpečnostní agentury, tak proškolení zaměstnanci, není ve všech objektech. Důvodem je buď to, že úřad spravuje malou oblast (městys Kounice) nebo že služebna policie se nachází v blízkosti či přímo v budově úřadu.

Blízké umístění služebny policie ovlivňuje i další parametry zabezpečovacího systému. Tato skutečnost se zejména projevuje na užití prvků EZS, konkrétně se toto týká většího užití PIR detektorů a mikrovlnných detektorů (v tab. 3. uvedeno pod názvem čidla), které ohlašují vniknutí nepovolané osoby do objektu. Tyto detektory předávají zprávu rovnou PCO stejně jako kamerový systém. Přítomnost kamerového systému je v tab. 3. uvedena pod názvem CCTV a úřady nejčastěji využívají jen systém venkovní, pouze objekty magistrátů jsou zajišťovány také systémem vnitřním. MÚ Tanvald v současné době kamerovým systémem ochrany nedisponuje vzhledem k větší finanční nákladnosti systému, který by byl schopen odolávat zvýšeným teplotním výkyvům v této oblasti.

Pokud stav bezpečnostních prvků používaných na úřadech porovnám s užitím těchto prvků v soukromém sektoru, opět všechno závisí na finančních možnostech firmy. Objekt malé firmy bývá součástí domu, ve kterém majitel firmy žije. Jakým způsobem si chrání dům, stejně tak si ochraňuje obchodní tajemství a další informace. V domech nebývá fyzická ostraha, ale objekt střeží detektory, případně kamerový systém napojený na PCO (subjekt Simpre, s.r.o).

Větší firmy mají ve svých objektech alespoň recepci, která představuje určitý druh fyzické ochrany. Firma Silvaco, a.s. ke zvýšení bezpečnosti obchodního tajemství ještě užívá dalších bezpečnostních prvků např. detektorů a kamerových systémů napojených na PCO. Firma Sipral, a.s. používala k zajištění bezpečnosti i bezpečnostní agenturu, ale vzhledem k větší finanční zátěži a snižování počtu vlastních zaměstnanců je tato bezpečnostní agentura využívána pouze v nočních hodinách. K zajištění bezpečnosti ve firmě Sipral, a.s. jsou používány vstupní karty a elektronické číselné vstupní zámky do některých částí objektu. Kamery jsou samozřejmostí a na oknech a dveřích jsou magnetické kontakty, které se spínají v době nepřítomnosti ostrahy v objektu a reagují na otevření.

Veškeré tyto bezpečnostní prvky by vyšly jako liché, ať už ve veřejné správě nebo v soukromém sektoru, pokud by informace o obchodním tajemství, o osobních údajích či krizovém řízení, nebyly střeženy celkově.

Velké důležitosti nabývají v této kybernetické době počítačové informační systémy. Úřady i soukromé firmy mívají vlastního správce počítačové sítě k zajištění co nejvyšší bezpečnosti. Data, s kterými úřady pracují, mohou být ale chráněna i certifikovaným

počítačovým systémem dodaným a spravovaným soukromou firmou. Tak tomu je např. u MÚ Lysá nad Labem.

Správce sítě musí učinit taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně či ztrátě nebo k jejich jinému zneužití. Shodný přístup je i k ochraně obchodního tajemství, které zahrnuje informace o obchodních partnerech, smlouvy, zájmy organizace na trhu, marketingový plán, finanční kalkulace, výrobní programy apod. K zabezpečení místa uložení těchto dat slouží nejlépe pracoviště s jedním vstupem, které je zajištěno proti volnému pohybu nepovolaných osob.

Informační technologie se neustále rozvíjejí, takže zpracování dat a informací se stává stále dostupnější širokému spektru osob. Je proto důležité, aby zaměstnanec se věnoval své práci a byl si vědom toho, že když využije přístupu na internet, musí se vzhledem k bezpečnosti dat, které jsou v jeho počítači, chovat obezřetně. V rámci bezpečnosti je lepší přístup k některým složkám na internetu omezit vzhledem k možnosti narušení počítačového systému.

Jedním z největších nebezpečí současné doby v této oblasti jsou sociální sítě. Málokdo si uvědomí všechny aspekty užívání sociálních sítí. V podstatě nevědomě může dojít k přenosu dat, která v zaměstnání chráníme, protože málokterý člověk striktně odděluje práci od soukromí. Na domácím počítači často používáme podobná hesla jako v pracovní databázi, ale hlavně poskytujeme informace o sobě, o přátelích, o spolupracovnících, která se dají při vhodné kombinaci samozřejmě zneužít např. k vytvoření podvodných zpráv.

Zároveň operátoři mobilních sociálních sítí mají k dispozici data a polohy uživatelů. Někteří uživatelé svou polohu podle GPS sami zasílají do svého profilu. Sociální sítě tak otvírají cestu k obtěžování nejen uživatele, ale i dalších jím zmíněných subjektů různými zprávami se závadnou přílohou, šíří malware, spam a mohou být zneužívány v obchodní konkurenci.

Nejen v České republice, ale i shodně v celé EU a celkově ve světě je informační kriminalita problémem. Jde o to, co nejvíce ochránit počítačové systémy před hackingem. Skupiny hackerů často pracují ve prospěch konkurenční firmy, případně se dělí o zisk z útoku se zaměstnancem společnosti, proti které je útok veden. Hacker se dokáže nabourat do sítě, změnit data v databázi nebo ovládat vzdálený počítač. Někteří hackeři v narušení

sítě vidí možnost, jak se zviditelnit, aby jim byla nabídnuta spolupráce ve vývoji počítačových technologií. [12]

3.2 Personální bezpečnost v ČR a v EU

Chceme-li zajistit, co největší personální bezpečnost informací je nutné spoléhat na důkladný výběr zaměstnanců, kteří s nimi budou pracovat ať už v ČR, v EU nebo kdekoli jinde. Metody výběru zaměstnanců jsem popsal již v předcházejících částech.

V našich podmínkách se mohou stát významnou součástí výběru zkoušky jazykových znalostí, neboť další vývoj u nás je ovlivněn začleňováním České republiky do EU. Zaměstnanci budou stále častěji vybíráni pro pracovní místa v celé Evropě a ne pouze pro místa s pobočkami v Čechách, na Moravě nebo ve Slezsku. Zároveň se zřejmě rozšíří ověřování morální integrity zaměstnanců, které je u nás zatím na nízké úrovni.

V některých evropských organizacích se kromě základních metod výběru můžeme setkat s metodami dalšími, jako jsou grafologie, astrologie a polygrafie (tj. užití detektoru lži). Údaje o validitě těchto metod jsou však vzácné, přestože grafologie se ve velké rozsahu užívá při výběru zaměstnanců v Evropě. V USA ji používá více než 3000 firem. [10]

Všechny státy Evropské unie dodržují zákonné předpisy na ochranu osobních dat.

Před několika lety docházelo ve Slovenské republice k zvláštní interpretaci v tomto směru a žádná instituce nesměla získávat a uchovávat informace o osobách, které nebyly jejími zaměstnanci. Důsledkem toho bylo, že většina firem na Slovensku přestala provádět jakýkoliv výběr zaměstnanců. V jiných firmách postupovali tak, že všechny uchazeče ráno přijali, pak je podrobili přijímacímu řízení a ty, které nechtěli, tentýž den propustili. Teprve po třech letech vznikla legislativní úprava, kterou se ochrana osobních údajů na Slovensku změnila. [10]

Personální bezpečnost je vedena ve všech státech Evropské unie velice podobně a ovlivňují jí především nařízení Národního bezpečnostního úřadu (případně stanoveného bezpečnostního úřadu) v jednotlivých zemích. Vlivem spolupráce mezi státy dochází i k nutné výměně utajovaných informací, a to nejen mezi zeměmi Evropské unie, ale i mezi vládou USA a EU. V bezpečnostním označení utajovaných informací je rozdíl pouze v tom, že USA nemá odpovídající klasifikaci stupně Vyhrazené (Restreint UE).

Další stupně bezpečnosti se nazývají Důvěrné (Confidentiel UE, Confidental), Tajné (Secret UE, Secret) a Přísně tajné (Très secret UE, Top secret).

Seznamy utajovaných informací vydává vždy vláda země svým nařízením na návrh ústředních úřadů, který následně zpracuje Národní bezpečnostní úřad. Celkový stupeň utajení smlouvy mezi státy nesmí být nižší než nejvyšší stupeň utajení některého z jejich prvků. Naopak spojením stupňů utajení může celkový stupeň být vyšší.

Každá ze smluvních stran má bezpečnostní systém a opatření založená na zásadách a minimálních bezpečnostních normách stanovených ve svých právních předpisech. Tímto je zajištěna utajovaným informacím odpovídající úroveň ochrany, o jejíchž postupech a praxi musí jedna strana druhé na požádání poskytnout informace. Přístup k utajovaným informacím se poskytuje pouze osobám, jejichž přístup je pro výkon úředních povinností nezbytný a jsou držiteli osvědčení o bezpečnostní prověrce osob.

Mezinárodní předávání utajovaných materiálů EU se uskutečňuje v souladu s vnitrostátními postupy členských států – musí být zajištěna bezpečnost podle stupně ochrany a před pohybem materiálu musí být vypracován plán přenosu, který schvaluje příslušný NBÚ/DSA. Přenos utajovaných informací by měl být realizován z místa určení do místa určení nejlépe bez přerušení a co nejrychleji. Pokud je přenos realizován dopravní společností musí mít společnost i zaměstnanec bezpečnostní prověrku. Jestliže zásilka bude vést mimo území členských států EU potom je to možné pouze na základě povolení NBÚ / DSA státu, který zásilku vyslal i který ji má přijmout.

Za účelem ochrany utajovaných informací je možno po předchozí konzultaci vykonávat mezi státy vzájemné bezpečnostní návštěvy k ověření provádění bezpečnostních požadavků podle stupně utajení dané informace.

4 OPATŘENÍ K OCHRANĚ OSOB PRACUJÍCÍCH S INFORMACEMI

Součástí personální bezpečnosti jsou zároveň opatření k zajištění ochrany osob pracujících s utajovanými informacemi, jak to úřadům ukládá zákon 412/2005 Sb. Tato skutečnost je dána zákonem a musí být dodržena. Proto jsem se zaměřil spíše na osobní bezpečnost všech zaměstnanců, kteří na úřadě pracují.

Jednou z mnou pokládaných otázek vedoucím personálních odborů na městských úřadech či tajemníkům městských úřadů byla otázka na osobní bezpečnost zaměstnanců. Jakým způsobem je zajištěna osobní bezpečnost zaměstnanců v areálu? Jakým způsobem je zajištěna osobní bezpečnost zaměstnanců na konkrétním pracovišti? Většinou na obě otázky zněla odpověď: „Soukromou bezpečnostní agenturou“ nebo „ U nás se nikdy nic nestalo“.

samosprávní celek	počet obyvatel	vzdálenost policie od MÚ	hlídací služba	telefon / tlačítka	ohrožení zaměstnance cizí osobou
Kounice	1 181	velká	ne	neuvádí	ne
Český Brod	6 822	malá	ne	telefon	ne
Tanvald	6 950	malá	ano	telefon	ne
Třeboň	8 653	v budově	ne	telefon	ne
Lysá nad Labem	8 657	v budově	ano	telefon	ne
Písek	29 923	malá	ne	telefon	ne
MČ Praha 1	30 002	velká	ano	telefon	ne
Kolín	30 927	malá	ano	telefon	ano
MČ Praha 15	31 015	velká	ano	telefon	ano
Jablonec nad Nisou	45 356	malá	ano	telefon	neuvádí
Karlovy Vary	51 115	malá	ne	telefon	ano
magistrát Liberec	101 865	malá	ne	telefon	ano
MČ Praha 4	128 431	v budově	ano	tlačítka	ano
magistrát Plzeň	168 808	malá	ne	tlačítka	ne

Tab. 4. Přehled některých prvků personální ochrany

Z tabulky tab. 4. můžeme zjistit, že ohrožení zaměstnance závisí ani ne tak na přítomnosti bezpečnostní agentury, blízkosti policie nebo na technických prostředcích, ale zejména na počtu obyvatel, kteří spádově do oblasti patří. Čím městský úřad spravuje větší

oblast, tím ho navštíví více lidí, a tím je větší pravděpodobnost vzniku konfliktů. Základem je, aby k nim docházelo co nejméně, a proto existují opatření k ochraně fyzických osob.

Pokud městský úřad působí v městě do 10 000 obyvatel, ostrahu mu zajišťuje hlídací služba nebo vzdálenost od služebny policie je malá, v tom případě je osobní bezpečnost zaměstnanců úřadu v pořádku. Pokud se ale jedná o oblast větší správy, obyvatelé měst se už tolik neznají, tam je třeba bezpečnostní opatření kombinovat.

Nejvíce konfliktů vzniká na sociálních odborech nebo na oddělení dávek hmotné nouze. Nejedná se o přímá napadení, ale spíš o agresivní chování, které bylo třeba řešit. Nicméně zaměstnanci těchto odborů úřadů větších měst se nikterak bezpečně necítí. To že má úřad u vchodu do budovy zaměstnance bezpečnostní agentury a sociální obor je „jenom“ ve 2.patře, člověka, který byl už jednou vystaven konfliktnímu jednání s klientem, neuklidňuje. O hodně bezpečněji a opodstatněně se cítí zaměstnanci úřadu, kteří v budově nebo v blízkosti mají služebnu policie, protože ta v případě konfliktu zaměstnance s cizí osobou může jednat efektivněji.

Pocitu bezpečí zaměstnanců správních celků by určitě napomohlo umístění bezpečnostního tlačítka v blízkosti místa, kde dochází k jednání s klientem, které by dávalo signál např. hlídací službě nebo jinému subjektu zajištujícímu bezpečnost. Zejména by tato tlačítka měla být umístěna tam, kde již k nějakému zásahu došlo. Ve skutečnosti k lepšímu zajištění bezpečnosti jsou tlačítka využívána jen na úřadech, které zajišťují správu více než 100 000 obyvatel.

Většina úřadů však používá pouze za tímto účelem telefony, jejichž použití je bohužel viditelnější než u tlačítek a je u nich větší riziko falešného poplachu. Na jednom z úřadů mi byl sdělen jiný postup při užití telefonu v tomto případě. Základem je, aby se služebna policie nacházela ve stejné budově jako úřad. Při vznikajícím konfliktu stačí, aby byl telefon na určitý čas vyvěšen, tím je dán signál na služebnu policie a může dojít k zásahu.

Uvědomme si, že vůbec není jednoduché pro zaměstnance úřadu konflikt řešit. Neustále musí mít na paměti, že nejlepší metodou je klienta uklidnit. Trestní zákoník sice každému v případě krajní nouze dovoluje použít nutnou obranu ke své ochraně při napadení podle § 28 a § 29 tohoto zákoníku, ale k takovému řešení by mělo dojít až po vyčerpání všech možných prostředků.

ZÁVĚR

Cílem bakalářské práce bylo vystihnout problematiku personální bezpečnosti ve veřejné správě ze základních hledisek a zjistit rozdíly mezi personální bezpečností ve veřejné správě a soukromým sektorem.

Vzhledem k tomu, že personální bezpečnost je založena na chování zaměstnanců, nemůže existovat žádný podstatný rozdíl ani mezi veřejnou správou a soukromým sektorem, ani tomu tak není v jiných státech.

Nejdůležitější bude výběr zaměstnanců, a pokud bude zajištěn optimálně, není třeba se obávat, že by docházelo k úniku informací. Soukromý sektor při tomto výběru není vázán předpisy jako veřejná správa ve smyslu, jak jednat musí, ale tím, kam až nesmí při svém jednání zajít. Právní rámec stanoví mantinely, ale nezavazuje, co smí a nesmí subjekt udělat při jednotlivých krocích na rozdíl od legislativních postupů veřejné správy.

Veřejná správa musí jednat podle přísně legislativně určených norem a má relativně úzký prostor pro změnu svých povinných úkolů, protože jsou legislativně určené, normativně vymezené a přísně kontrolované. Soukromý sektor má pravidla pro své jednání volnější.

K zajištění bezpečnosti ochrany osobních dat, obchodního tajemství a zvláštních skutečností disponuje soukromý sektor větším objemem financí než veřejná správa. Toto se projevuje zejména náročnějším a dokonalejším technickým zabezpečením objektů soukromého sektoru. Lepší technické zajištění objektu samospráv se vyskytuje zejména v místech, kde se nalézá samospráva a služebna policie ve stejné budově.

U obou sektorů je jistým nebezpečím zvyšující se závislost toku informací na počítačových sítích, které umožňují systémový a komplexní přístup k informacím. Všichni si uvědomují, že k úniku informací může dojít právě skrze tyto systémy.

Personální bezpečnost je vedena ve všech státech Evropské unie velice podobně a ovlivňují ji především nařízení stanovených bezpečnostních úřadů v jednotlivých zemích. Spoluprací mezi státy EU dochází k nutné výměně některých utajovaných informací, a proto musí být stanoveny příslušné postupy k předávání těchto informací.

Cílenými rozhovory se zaměstnanci veřejné správy jsem zjistil, že k úniku informací nedochází. Pouze někdy došlo na oddělení dávek hmotné nouze či na sociálním odboru k agresivnímu chování klientů, které bylo ihned řešeno. Nicméně zaměstnanci těchto

odborů úřadu se necítí nijak bezpečně, i když zásah byl proveden včas, a to by se mělo zlepšit.

ZÁVĚR V ANGLIČTINĚ

The main objective of this bachelor thesis was to describe issues, challenges concerning personnel security in public administration from the basic aspects and to specify the differences between personnel security in public administration and in private sector.

Due to the fact that personnel security is based on employees behavior, there cannot be any important difference between public administration and private sector in our country, the same situation being observed abroad.

The most important step, the crucial and the initial one, is the right choice of employees, and if it is mastered professionally, it will optimally guarantee that no information leak will occur. Private sector is legally less obliged in this area than public administration, the latter being strictly limited by particular regulations. Private sector is given a set of rules to act within certain limits which must be strictly observed. Legal framework provides barriers, but it does not impose each step of the procedure, unlike of the firmly established legislative steps of public administration.

Public administration must act in compliance with the strict legislation, rigorously defined standards and thus it has relatively little space for accommodating the approaches while dealing with its obligatory tasks, because they are legally determined, normatively defined and strictly supervised. Private sector enjoys less tough rules.

To secure protection of personal data, trade and professional secrets, confidential facts etc., private sector benefits from greater financial means than public administration. It mainly results in better and more sophisticated security systems of private sector premises. If public administration offices share the same building with the police, the security system proves to be better.

Both sectors are certainly concerned with the increasing danger due to the dependence of information flow via networks which allows systemic and complex seeking for information. These days everyone is conscious of the fact that information leak may occur through these systems.

Generally, personnel security is organized, managed and governed similarly within the European Union, each country modifying the measures and regulations by its own particular security authorities. The complex and comprehensive cooperation among the EU

member countries necessarily involves exchanging sensitive intelligence, confidential materials, classified information, thus uniform, clearly defined methods, guidelines for providing such information must be strictly established.

Based on my personal interviews with some employees of public administration I have found that there is no leak of information. Sometimes there were incidents of aggressive behaviour of clients at the departments of social, security, subsidiary benefits, which were immediately solved on the spot. However, the employees of these departments do not feel safe. Their safety and security should be improved.

SEZNAM POUŽITÉ LITERATURY

[1] IVANKA, Ján. *Mechanické zábranné systémy*, 1. vyd. Univerzita Tomáše Bati ve Zlíně, 2010, ISBN 978-80-7318-910-5

[2] BRABEC, František a kol.. *Bezpečnost pro firmu, úřad, občana,* 1. vyd. Public History, Praha 2001, ISBN 80-86445-04-06

[3] BRABEC, František. *Ochrana bezpečnosti podniku*. 1. vyd. Zlín, Praha : Eurounion 1996, ISBN 80-85858-29-0

[4] ČERNÝ, Josef. *Systemizace bezpečnostního průmyslu I , 2*. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2006, ISBN 80-7318-402-8

[5] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I* , 3. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010, ISBN 978-80-7318-889-4

[6] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II* , 2. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007, ISBN 978-80-7318-631-9

[7] BARTÍK, Václav. *Ochrana osobních údajů v aplikační praxi : vybrané otázky*. 1. vyd. Praha : Linde 2010, ISBN 978-80-7201-817-8

[8] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávní agendě,* Praha : BMSS-Start, 2010, ISBN 978-80-86140-64-3

[9] ŘÍHA, Milan. *Bezpečnostní systémy (1. a 2. díl),* 1. vyd. Praha : Námořní akademie České republiky, 2007, ISBN 978-80-87103 a 978-80-87103-13-5

[10] KOLMAN, L., CHÝLKOVÁ, H., MICHÁLEK, P., KOSÍKOVÁ, Z.. *Výběr zaměstnanců – Metody a postupy,* 1. vyd. Praha : Linde, 2010,

ISDN 978-80-7201-810-9

[11] ZUZÁK, R., KŘÍŽ, J., LENINSKÁ, R.. *Řízení administrativních procesů v organizaci,*1. vyd. Praha: Alfa Nakladatelství, s.r.o., 2009,

ISDN 978-0-87197-22-6

[12] *Security magazín*. Vydává Security Media, s.r.o.. roč. XVII., č. 97. 2010 – září/říjen, ISSN 1210-8723

[13] Portál veřejné správy ČR: *Na úřad přes internet* [online]. Dostupný z WWW :

<http://www.portal.gov.cz/wps/portal/_s.155/701/_s.155/6966/place>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

NBÚ	Národní bezpečnostní úřad.
ČR	Česká republika
EU	Evropská unie
NATO	Severoatlantická aliance (pakt)
ICT	Informační a komunikační technologie.
SBS	Soukromá bezpečnostní služba
MZS	Mechanické zábranné systémy
VKV	Velmi krátké vlny
ACCESS	Přístupový systém
EZS	Elektronický zabezpečovací systém
ISDN	Digitální komunikační síť s integrovanými službami
PIR	Pasivní infračervený detektor
ID	Identifikační
MÚ	Městský úřad
MČ	Městská část
DSA	Stanovený bezpečnostní úřad (Designated Security Authority)
GPS	Globální triangulační systém
USA	Spojené státy americké
FBI	Federální úřad pro vyšetřování

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM CITACÍ

[1] ČERNÝ, Josef a kol., *Systemizace bezpečnostního průmyslu I*,. Vyd. 2, Zlín : Univerzita Tomáše Bati ve Zlíně, 2006, ISBN - 80-7318-402-8; díl V. Soukromí bezpečnostní specialisté, Brabec, František, str. 8 11

[2] NBÚ: *Obecně k personální bezpečnosti* [online]. Dostupný z WWW: <http://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost/obecne-k-personalni-bezpecnosti/>..... 12

[3] LAUCKÝ, Vladimír, *Technologie komerční bezpečnosti* I, Vyd. 3, Zlín : Univerzita Tomáše Bati ve Zlíně, 2010, ISBN – 978-80-73-18-889-4, str. 11 22

[4] KOLMAN, L., CHÝLKOVÁ, H., MICHÁLEK, P., KOSÍKOVÁ, Z.. *Výběr zaměstnanců – Metody a postupy*, 1.Vyd, Praha : Linde, 2010, ISBN 978-80-7201-810-9 str.56 37