Specialní bezpečnostní technika a její použití

Special safety eguipment and its use

Karel Kostrbel

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Karel KOSTRBEL**
Osobní číslo:	**A06283**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Speciální bezpečnostní technika a její použití**

Zásady pro vypracování:

Zpracujte problém ve dvou dimenzích.

1. **Technická dimenze, zde shromážděte nejnovější poznatky o tomto typu technologií na současném trhu, včetně cenových relací.**
2. **Uveďte nové technologie, jejich klady a zápory. Tyto zanalyzujte.**
3. **Předpokládaný vývoj v budoucnu, směry vývoje.**
4. **Právní dimenze. Zákonnost nasazování technických prostředků, uveďte legislativní ošetření problému.**
5. **Technické odhalování speciálních bezpečnostních prostředků fyzikální cestou.**
6. **Druhy právního postihu za nezákonné nasazování technických prostředků.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KAMENÍK J., BRABEC F. a kolektiv Komerční bezpečnost. 1. vyd. Praha: ASPI, a.s., 2007. ISBN 978-80-7357-309-6.**
2. **LUKÁŠ L. Bezpečnostní technologie, systémy a management. 1. vyd. Univerzita Tomáše Bati ve Zlíně, 2008. ISBN 978-80-7318-605-0.**
3. **LAUCKÝ V. Technologie komerční bezpečnosti II. 2. vyd. Univerzita Tomáše Bati ve Zlíně, 2007. ISBN 978-80-7318-631-9.**
4. **LAUCKÝ V. Speciální bezpečnostní technologie. 1. vyd. Univerzita Tomáše Bati ve Zlíně, 2008. ISBN 978-80-7318-762-0.**
5. **Listina základních práv a svobod.**

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

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

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

Ve Zlíně dne 19. února 2010

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

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Tato bakalářská práce je zaměřena na speciální bezpečnostní techniku a její použití z technického i právního hlediska.

V technické dimenzi je rozebrána problematika spojená se získáváním pravdivých informací z odposlechových a obrazových zařízení. Dále jsou zde shromážděny nejnovější poznatky o speciálních bezpečnostních prostředcích, které se prodávají hlavně na českém trhu, včetně cen za konkrétní prostředky. Práce popisuje nejnovější používané technologie a jejich předpokládaný budoucí vývoj. Také je zde popsán postup provádění obranně technické prohlídky prostorů, ve kterých se nacházejí legálně či nelegálně nasazené prostředky k získávání pravdivých informací.

Právní dimenze je zaměřena na zákonitosti spojené s nasazováním speciálních bezpečnostních prostředků včetně právních postihů při jejich nezákonném nasazení.

Klíčová slova: prostředky speciální bezpečnostní techniky, odposlech, mikrofon, minikamera, obranně technická prohlídka, právní normy, právní postihy.

ABSTRACT

The work is focused on special safety equipment and its utilization in light of technique and law.

In the dimension of technique, there are described problems of obtaining data from monitoring and screening machines. There are also collected the newest pieces of knowledge on special safety equipment, which are to be bought mainly on the Czech trade, concluding the prices. The work gives an account of the newly used technologies and their supposed development. There are also described procedures of defensive technical inspection of the space, where are legally or illegally used obtaining data machines situated.

The law dimension is focused on patterns connected with putting on the special trade equipment, concluding the legal sanction within their illegal putting on.

Keywords: special trade equipment, monitoring, microphone, minicamera, defensive technical inspection, rule of law, legal sanction.

Děkuji svému vedoucímu práce panu JUDr. Vladimíru Lauckému za cenné rady a připomínky při tvorbě této bakalářské práce.

Všem ostatním děkuji za pochopení a podporu, kterou mi projevovali v průběhu zpracování této bakalářské práce.

Prohlašuji, že

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

Prohlašuji,

že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

V dnešní době plné kriminality, rychlých změn na trhu práce a z důvodu ekonomické krize, je nedílnou součástí soukromého podnikání ochrana informací a chránění vlastního know-how, které je součástí každého podniku. Mnoho nezačleněných lidí do této problematiky si myslí, že právě jim žádné nebezpečí nehrozí. Kdyby však věděli, jak lehce a zároveň levně (v poměru s odcizenými informacemi) mohou přijít o své tajné informace, věnovali by se této problematice podrobněji a důsledněji. Také objasňování trestných činů by se v některých případech neobešlo bez nasazení speciální bezpečnostní techniky. Špionáž jakožto zpracovávání informací, které byly získány za použití určité techniky, je známa už několik desítek či stovek let.

Cílem této bakalářské práce je objasnit, jaké druhy speciální bezpečnostní techniky jsou v dnešní době dostupné na trhu včetně jejich cenové relace, a nastínění možností nasazení a vzhledu speciální bezpečnostní techniky. Dále budou analyzovány právní normy a nezákonné nasazování prvků speciální bezpečnostní techniky.

Bakalářská práce se skládá ze dvou hlavních částí. První část bude zaměřena na speciální bezpečnostní techniku z technického hlediska. Taktéž zde budou nastíněny možnosti nových technologií používaných ve speciálně bezpečnostní technice. V druhé části bude proveden rozbor právních norem vztahujících se k zákonnému či nezákonnému nasazování prostředků speciální bezpečnostní techniky.

V závěru práce budou uvedeny druhy právních postihů, kterými může být potrestána osoba, při nezákonném nasazení prostředků speciální bezpečnostní techniky.

I. TECHNICKÁ DIMENZE

1 SPECIÁLNÍ BEZPEČNOSTNÍ TECHNIKA

Na českém i zahraničním trhu působí řada společností, které se zaměřují na dodávky špičkové bezpečností techniky. Mnoho firem se specializuje na technické vybavení určené pro policii, bezpečností agentury, soukromé detektivní kanceláře, ale i běžnou veřejnost. Prostředky speciální bezpečností techniky jsou prodávány koncovým zákazníkům přímým prodejem v kamenné prodejně nebo přes internetový obchod.

1.1 Definice a dělení speciální bezpečnostní techniky

Pod pojmem speciální bezpečnostní technika se v sektoru soukromých bezpečnostních služeb rozumí, souhrn všech možných komerčně využitelných prostředků, které slouží k získávání určitých informací od zadavatele. Do kategorie speciálních bezpečnostních prostředků patří nejen prostředky pro získávání kriminálních podtextů nebo technika, která je nainstalována legálně či nelegálně pro získávání informací.

Technické prostředky můžeme rozdělit z několika hledisek:

a) Podle informačního průniku

- Invazivní – s nutností fyzického průniku do prostoru.
- Neinvazivní – bez nutnosti průniku do prostoru.

b) Podle typu přenosu informace z cílového prostoru k záznamu

- Drátové.
- Bezdrátové.

c) Podle druhu přenášené informace

- Audio.
- Video.
- Kombinace audio/video. [12]

1.2 Prvky speciální bezpečnostní techniky na současném trhu

Vlivem rychle se měnícího ekonomického prostředí, přibývající konkurence v odvětví je velmi důležité neustálé sledování vývoje nových technologií. Jen tak může firma poskytnout svým klientům to nejlepší zboží včetně kompletního servisu a maximální technické podpory, a tak obstát v široké konkurenci na trhu.

Základ odposlechového zařízení

Základem klasického odposlechového zařízení, které přenáší signál, jak po vedení, tak i vzduchem, je mikrofon. Uvedená odposlechová zařízení se zejména opatřují elektretovými mikrofony. Takové mikrofony mají velkou citlivost a dokážou zachytit i šepot z místnosti (10 x 10) metrů. Při výběru mikrofonu je třeba brát ohled na způsob použití a podle toho volit i technické vlastnosti mikrofonu.

Základní parametry, které je třeba brát v úvahu:

- Konstrukce mikrofonu,
- přenášené frekvenční pásmo,
- směrovost,
- citlivost,
- a impedance. [2]

1.2.1 Odposlechové zařízení s přenášeným signálem po vedení

Pro instalaci odposlechového zařízení s přenášeným signálem po vedení je nutností pečlivé ukrytí vedení sloužícího pro přenos získaného signálu, fyzický přístup do zájmového prostoru na dobu od několika minut až po několik desítek hodin. Dále je zapotřebí, aby se v místnosti nacházelo zejména drátové propojení s předzesilovačem a dalšími potřebnými elektrickými zařízeními pro správnou funkčnost snímání zvuku. K dosažení kvalitního odposlechu je potřeba umístit mikrofon na správné místo. Čím blíže se mikrofon nachází u hovořící osoby, tím je odposlech kvalitnější. Také musíme brát v úvahu akustiku místnosti, abychom vyloučili nežádoucí brum.

Při přenosu informace z mikrofonu se zejména používají metalická vedení. Po modulaci a zesílení přeneseného výsledného signálu můžeme na vedení přímo připojit reproduktory,

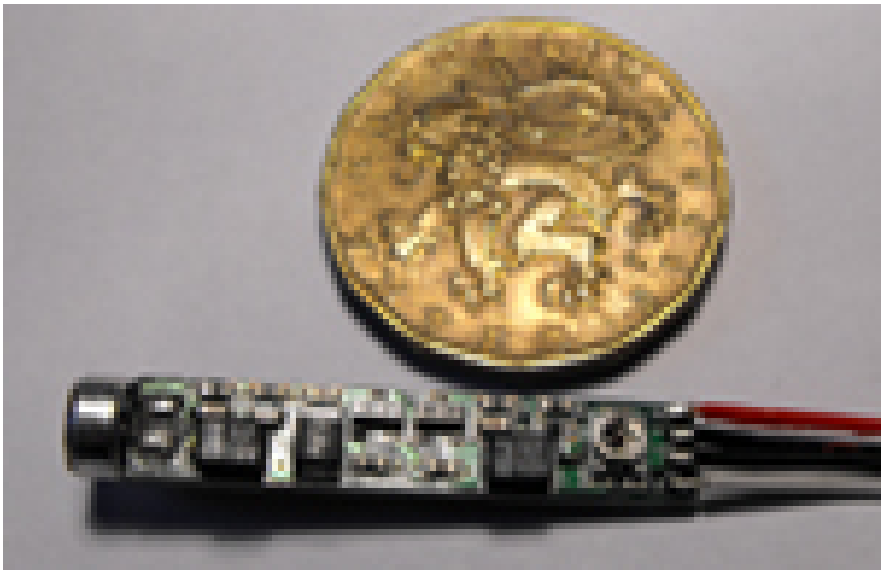
sluchátka nebo záznamové zařízení. Dalším typem vedení získaného signálu je po světlovodném kabelu. Pro přenos signálu z mikrofonu po světlovodném kabelu potřebujeme nejprve elektrický signál z mikrofonu převést pomocí elektricky-optického převodníku (konvertoru) na světelný signál. Na druhém konci světlovodného kabelu musíme zase světelný signál převést zpět na elektrický a to za pomoci opticko-elektrického převodníku (konvertoru). Při použití světlovodného kabelu, můžeme po jednom kabelu vést signál i z několika mikrofonů najednou. Pro přenos signálu získaného z mikrofonu můžeme také použít zařízení pracující na principu radiového vysílače, který pracuje na frekvenci 50 kHz–400 kHz. Signál není veden vzduchem, ale po stávajícím alternativním vedení, např. vodovodní potrubí, přívody topení, telefonní linky, datové linky, klasické elektrické vedení 230 V, PZTS, EPS apod. Na druhém konci od mikrofonu nám stačí upravený přijímač, který odfiltruje nepožadovanou frekvenci od požadované na vzdálenost až 200 m.

Hlavní výhodou odposlechového zařízení s vedením signálu po vedení je přenos signálu na velké vzdálenosti dokonce až několika kilometrů. [2]

1.2.1.1 Příklady odposlechových zařízení s přenosem signálu po vedení

Předzesilovač s elektretovým mikrofonem PRZES

Předzesilovač s elektretovým mikrofonem PRZES je díky svým miniaturním rozměrům určen pro skrytou povrchovou montáž a vedení signálu z odposlouchávané místnosti za pomoci drátového vedení. Jeho napájení je v rozmezí 9–12 V DC. Cena tohoto předzesilovače s elektretovým mikrofonem je cca 400 Kč včetně DPH. [32]



Obr. 1 Předzesilovač s elektretovým mikrofonem PRZES [32]

Odposlechová souprava F-555 EX

Odposlechová souprava F-555 EX je souprava, která obsahuje kontaktní, jehlový a drátový mikrofon s příslušným zesilovačem. Rozměry zesilovače jsou (21 x 55 x 70) mm, rozměry snímače jsou (32 x 27 x 30) mm, délka kabelu je 970 mm, jehlový mikrofon má rozměry (8 x 28) mm, kabel je 1 050 mm dlouhý, mikrofon má velikost (7 x 12) mm. K napájení slouží klasická 9V baterie. Kompletní hmotnost je 440 g. Doba provozu je 50–60 hodin. Výstup je na sluchátko nebo k nahrávacímu zařízení. Cena soupravy je kolem 12.000 Kč včetně DPH. [32]

Obr. 2 Odposlechová souprava F-555EX [32]

Odposlechová souprava MC-06

Souprava obsahující šestikanálový dlouhovlnný přijímač a 6 vysílačů pracujících v pásmu 60 kHz–200 kHz. Jako přenosovou cestu získaného signálu, využívá klasické elektrické vedení s napětím 230 V. Přijímač je určen pro příjem až šesti vysílačů MCX-06. Jeho velikost je (190 x 140 x 50) mm. Napájení vysílačů je ze sítě s napětím 230 V AC. Cena se pohybuje kolem cca 10.000 Kč včetně DPH. [2]

Obr. 3 Odposlech po vedení MC-06 [2]

1.2.2 Odposlechové zařízení s bezdrátovým přenosem signálu

Výhodnější pro instalaci jsou zařízení pracující na bezdrátovém přenosu informací ze zájmové nebo vedlejší místnosti. V dnešní době jsou již tyto prostředky značně miniaturizované a obsahují i vlastní vysílač, který nám umožňuje přenos informací na stovky až tisíce metrů. Přenos informací je veden pomocí radiových vln a infračerveného záření, které každý známe např. dálkového ovládání televizoru. Vysílací signál pomocí radiových vln bývá buď stabilizovaný nebo nestabilizovaný, a dále může být šifrovaný nebo otevřený. Stabilizovaný signál je výhodnější v tom, že se nemusíme starat o to, jestli se nám nezměnila vysílací frekvence třeba jen o desetinu frekvence např. vlivem stárnutí zdroje. Kolísání může dělat problém při bezobslužném nahrávání. Velkou roli při vysílání signálu z odposlechového zařízení pomocí radiových frekvencí, hraje vysílací pásmo. Vysílací pásmo se pohybuje v rozmezí 60 Hz–450 MHz. Tyto frekvence jsou ověřeny praxí, že dobře procházejí přes různé překážky a zdi. Frekvence 88 MHz–108 MHz jsou využívány pro komerčně rozhlasové vysílání, ale dají se použít i pro dálkový odposlech. U těchto frekvencí je výhodou, že nám stačí k poslechu záznamu z odposlechu obyčejný

radiopřijímač. Avšak velkou nevýhodou je, že se nám může někdo cizí napíchnout na naši frekvenci. Další důležitou vlastností odposlechu je výkon. Asi na 10 metrovou vzdálenost nám postačí vysílač o výkonu 1 mW. Čím vyšší je výkon, tím větší je vzdálenost, na kterou nám vysílač vysílá signál, ale také spotřeba elektrické energie. Na tyto parametry si musíme dávat pozor při bateriovém napájení. V praxi se používají výkony 20 mW–100 mW, kdy na 9 V baterii při výkonu 20 mW dokáže odposlech pracovat až 10 hodin, a to na vzdálenost 200 m–300 m. Výkon by měl být úměrný vzdálenosti odposlechu od přijímače. Zbytečně velká vysílací vzdálenost je nebezpečná pro odhalení, a proto se používají takové výkony, které budou stačit na 150 m–200 m. Podle způsobu použití se dělí na jednoúčelové a trvalé. [2]

Jednoúčelové odposlechové zařízení

Jednoúčelové odposlechové zařízení je napájeno z baterie, a proto je vhodné pro rychlou a snadnou instalaci, kterou zvládne i technický laik. Právě baterie nám určuje velikost odposlechového zařízení a také na jak dlouho a na jak velkou vzdálenost nám bude fungovat. Čím menší je odposlechové zařízení, tím menší je vysílací vzdálenost nebo doba, po kterou bude odposlechové zařízení vysílat. Pokud budeme potřebovat, aby nám odposlechové zařízení fungovalo déle než měsíc, musíme zajistit výměnu baterie, nebo můžeme k odposlechovému zařízení připojit navíc fotovoltaický článek, který nám při dostatečném osvětlení bude baterii dobíjet. V praxi se častěji setkáváme s trvalým napájením z elektrické sítě než s fotovoltaickým dobíjením. Pro snížení odhalitelnosti a zároveň prodloužení doby provozu odposlechového zařízení napájeného baterií se vybavuje takové zařízení dálkovým spínáním nebo aktivací hlasem (VOX). Takové odposlechové zařízení vysílá signál jen tehdy, když je dálkově zapnuto nebo když se v místnosti začne mluvit. Takové jednoúčelové odposlechové zařízení najdeme v nejrůznějších předmětech denní i osobní potřeby, např. váza, socha, popelník, kalkulačka, zápisník, propisovací tužka, cigaretový obal, zapalovač, hodinky, kreditní karta, mobilní telefon apod. [2]

Trvalé odposlechové zařízení

Základní faktor, který nám určuje na jakou vzdálenost a po jakou dobu nám bude odposlechové zařízení vysílat signál, je dostatek elektrické energie. Není možné, aby odposlechové zařízení o velikosti knoflíku, vysílalo signál na jeden kilometr po dobu

jednoho měsíce. Trvalé odposlechové zařízení se proto instalují do míst, kde je zaručen relativně nevyčerpatelný zdroj elektrické energie. Takovými místy jsou např. zásuvky, rozdvojky, prodlužovací šňůry, lampičky a většina elektrických spotřebičů pracujících na napětí 230 V. Další možností umístění jsou také telefonní linky, prvky zabezpečovacího zařízení, ale i prvky požárního zařízení mohou obsahovat skrytě umístěné trvalé odposlechové zařízení. Nejen jednoúčelové, ale také trvalé odposlechové zařízení můžeme nalézt v oděvu, obuvi apod. Aby toto odposlechové zařízení mohlo být umístěno po delší dobu na určeném místě, musíme k němu zajistit přístup pro výměnu baterií. [2]

1.2.2.1 Příklady odposlechových zařízení s bezdrátovým přenosem signálu

Odposlechové zařízení OPTIMUM 600

Odposlechové zařízení pro bezdrátový přenos získaného signálu Optimum 600 je výkonný vysílač v pásmu FM s nastavitelnou frekvencí 80 MHz–110 MHz a také s nastavitelnou citlivostí, které dosáhneme pomocí malého šroubováčku. Dosah signálu je ve volném prostředí 600 m a v zástavbě zhruba polovinu. Rozměry jsou (5 x 2 x 1) cm. Napájení je zajišťováno klasickou 9V baterií. Při použití kvalitní baterie je doba provozu asi 1 týden. Pro příjem signálu postačí běžné FM rádio, autorádio. Cena včetně DPH je kolem 1.200 Kč. Podobný vysílač, ale za cenu 120 Kč se dá koupit na různých internetových aukcích. V podstatě má i stejné rozměry a dosah vysílaného signálu je jen 5 m–20 m, napájení i frekvenční pásmo jsou stejné. [23]

Obr. 4 Odposlechové zařízení OPTIMUM 600 [23]

Odposlechové zařízení R250

Odposlechové zařízení R250 je vybaveno miniaturním mikrofonem s bezdrátovým vysílačem. Díky výrobě technologií SMT nám dosahuje miniaturních rozměrů. Odposlechové zařízení vysílá signál na frekvencích mimo veřejné pásmo, a tudíž nám zajišťuje nerušený přenos. Frekvence je stabilizovaná a volitelná v rozmezí AIR pásma 110 MHz–135 MHz. Rozměry bez baterie jsou (28 x 12 x 6) mm, dosah při zastavěném prostoru je 100 m–300 m a volném prostoru až 500 m. Při použití kvalitní 9V alkalické baterie s kapacitou 1 200 mAh je doba nepřetržitého provozu až 180 hodin. Pro příjem signálu od odposlechového zařízení potřebujeme speciální přijímač AIR M9, obyčejný radiový přijímač nám stačit bohužel nebude. Cena bez přijímače je včetně DPH cca 4.300 Kč, přijímač se dá pořídit za 1.800 Kč včetně DPH. [18]

Obr. 5 Bezdrátové odposlechové zařízení R250 [18]

Odposlechové zařízení MUD-R

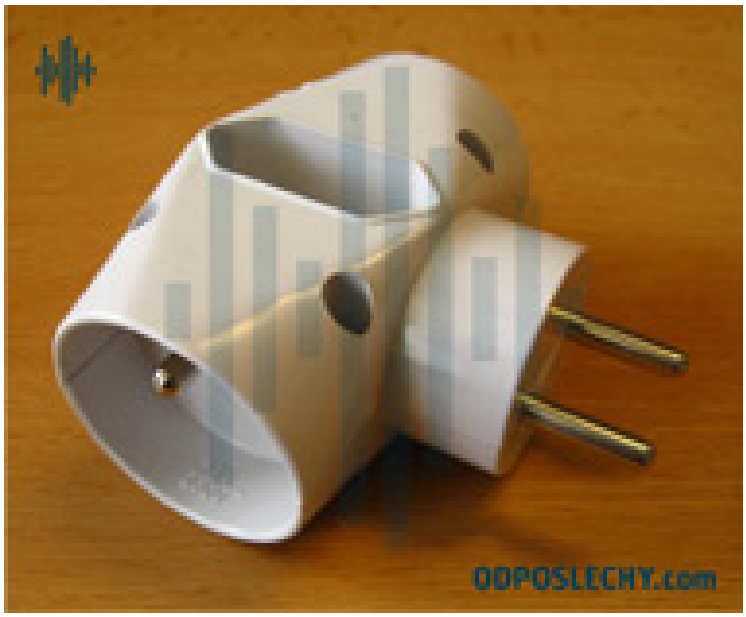
Odposlechové zařízení MUD-R se stabilizovaným radiovým vysílačem a mikrofonem o výkonu 5 mW je napájen 3V knoflíkovou baterií o kapacitě 1 000 mAh. Frekvence je stabilizovaná SAW rezonátorem na frekvenčním pásmu 430 MHz. Doba provozu je až 100 hodin na vzdálenost 100 m–150 m. Průměr vysílače je 30 mm a tloušťka 16 mm. Cena včetně DPH je kolem 9.500 Kč. [8]

Obr. 6 Odposlechové zařízení MUD-R [8]

Odposlechové zařízení R200 AC

Odposlechové zařízení R200 AC je vybaveno bezdrátovým miniaturním mikrofonem a vysílačem zabudovaným v plně funkční klasické elektrické rozdvojce. Díky svému vzhledu je vhodný pro rychlou i laikem zvládnutelnou instalaci. Díky použití kvalitního mikrofonu může být rozdvojka umístěna klidně i za skříní, stolem apod. Dosah vysílaného signálu je 50 m–400 m podle druhu prostředí. Vysílací frekvence je stabilizovaná a pevně nastavená v neveřejném AIR pásmu 110 MHz–135 MHz. Doba provozu je nevyčíslitelná z důvodu napájení z klasické elektrické sítě na 230 V. Pro příjem signálu je zapotřebí speciálního přijímače, např. AIR M9. Cena včetně DPH je 4.200 Kč.

Na internetu v různých aukcích se dá pořídit skoro stejné zařízení za čtvrtinovou cenu. Zařízení se liší jen vysílací frekvencí, která je ve veřejném pásmu, a tudíž nám pro poslech postačí klasický radiopřijímač, který určitě budeme vlastnit, nebo si ho můžeme pořídit za několik desítek korun. [20]



Obr. 7 Odposlechové zařízení R200 AC [20]

Odposlechové zařízení R500 AC2

Odposlechové zařízení R500 AC2 je vybaveno bezdrátovým miniaturním mikrofonem a vysílačem, který vysílá v pásmu ultra vysoké frekvence, a to na frekvencích 350 MHz-450 MHz se SAW rezonátorem. To vše je zabudováno v plnohodnotné prodlužovací šňůře na 230 V. Díky svému důkladnému zamaskování se dá použít takřka

kdekoliv, kde je přívod elektrické energie na 230 V, napájení je přímo ze sítě. Díky použití nízkošumového zvukovodního mikrofonu Knowles a obvodu automatického řízení citlivosti mikrofonu a také automatické šumové bráně, je odposlechové zařízení R500 AC2 vhodné pro použití v prostorách s rozdílnou intenzitou okolních zvuků. Prodlužovací šňůra je vysoce odolná vůčí EMC a také ochrannou proti detekci nelinearit. Signál je vysílán na předem určené frekvenci na vzdálenost až 400 m v zástavbě a 700 m ve volném prostředí. Pro příjem potřebujeme speciální přijímač, např. Alinco MK. Cena bez přijímače včetně DPH je kolem 17.500 Kč. Cena přijímače Alinco MK je asi 13.700 Kč včetně DPH.

Tento druh mikrofonu s vysílačem se dá použít i u jiných prostředků napájených přímo ze sítě na 230 V, např. rozdvojka, kryt zásuvky, lampička, nabíječka mobilu apod. [21]

Obr. 8 Odposlechové zařízení R500 AC2 [21]

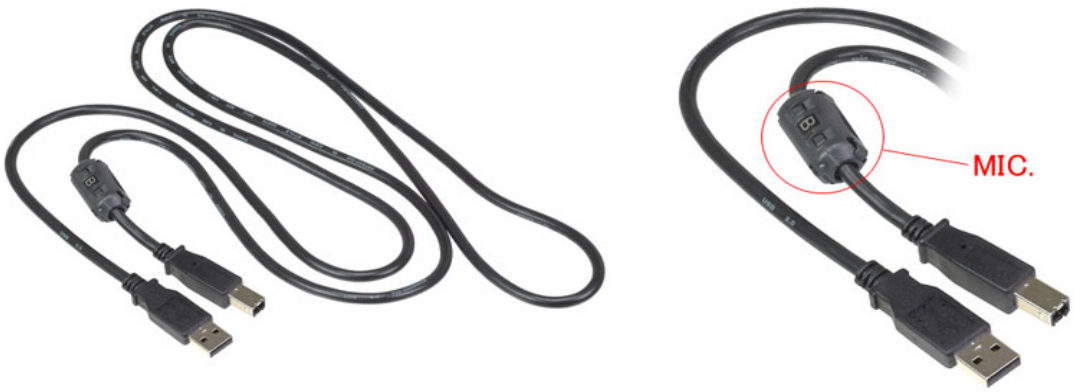
Odposlechové zařízení CD-VOXER

Odposlechové zařízení CD-VOXER je vysílač o velikosti kreditní karty. Rozměry jsou (54 x 85 x 6) mm, hmotnost s baterií je 27 g, napájení je pomocí knoflíkové baterie CR-2430 (3 V), dosah vysílaného signálu je cca 30 m v UKV (Ultra krátké vlny 350 MHz-450 MHz) a doba provozu je asi 50 hodin. Pro příjem signálu je potřeba speciální přijímač, např. Alinco MK. Cena bez přijímače včetně DPH je okolo 9.200 Kč. [33]

Obr. 9 Odposlechové zařízení CD-VOXER [33]

Odposlechové zařízení UB-40

Odposlechové zařízení UB-40 obsahuje vysílač s mikrofonem maskovaný v USB kabelu. Délka kabelu je 1,5 m, hmotnost 77 g, napájení je na 5 V přímo z USB zásuvky v PC. Dosah vysílacího signálu je cca 30 m v UKV pásmu, pro příjem signálu je zapotřebí speciální přijímač. Cena bez přijímače včetně DPH je 6.400 Kč. [33]



Obr. 10 Odposlechové zařízení UB-40 [33]

Odposlechové zařízení R3000

Odposlechové zařízení R3000 obsahuje vysílač a přijímač, který zajišťuje vysoce sofistikovaný přenos zvuku z monitorovaného prostoru. Na tento vysílač, při vzdálenosti větší než několik centimetrů, nereagují žádné detektory odposlechů. Paměťové analyzátory RF spektra dokonce nereagují ani tehdy, když je tento odposlech přímo u antény. Zařízení se vyznačuje nejvyšší kvalitou přenosu, malými rozměry cca (37 x 25 x 8) mm a při přímé viditelnosti s dosahem až 1 km. V zástavbě je dle podmínek šíření dosah limitován hustotou objektů na dosah 50 m až 500 m. Vysílač se dá ukrýt např. do běžné spotřební elektroniky vyskytující se v domácnosti nebo kanceláři. Vysílač vysílá signál mimo veškerá používaná a skenovaná frekvenční pásma. Aktivace pomocí VOX spouštěče. Parametry vysílače: napájecí napětí 7 V DC–13 V DC, odebíraný proud 80 mAh–120 mAh, provozní teplota -20 až +50°C, rozměry bez antény (27 x 37 x 10) mm. Parametry přijímače: napájecí napětí 10 V DC–14 V DC, napájecí proud 80 mAh–120 mAh, provozní teplota -20 °C až +50 °C, rozměry bez antény (90 x 75 x 35) mm, rozměry antény (80 x 65 x 30) mm. Pro nahrávání můžeme použít diktafon. Cena bez diktafonu včetně DPH je kolem 65.400 Kč. [22]

Obr. 11 Odposlechové zařízení R3000 [22]

V kapitole „Příklady odposlechových zařízení s bezdrátovým přenosem signálu“ jsem si vybral a stručně charakterizoval jen některé typy těchto prvků z širokého sortimentu, které firmy nabízí svým zákazníkům. Na základě našich konkrétních potřeb, např. na jakou vzdálenost potřebujeme dosah vysílaného signálu, v jakém frekvenčním pásmu budeme

vysílat, jak často můžeme chodit měnit baterie, jak velké rozměry vysílač může mít apod., si vybereme vysílač, který bude splňovat naše požadavky. Velkou výhodou při použití bateriového vysílače je dálkové spouštění nebo také VOX spouštění hlasem, protože tyto spouštěče nám hodně šetří baterie.

1.2.3 Speciální mikrofony

Kromě klasických výše popsaných druhů zařízení k odposlechu místností, se používají speciálně upravené či zkonstruované mikrofony. Nejznámější jsou stetoskopy, laserové odposlechové zařízení apod.

1.2.3.1 Kontaktní mikrofony

Akustický tlak vznikající při hovoru v místnosti rozechvívá zdi, dveře, okenní tabule apod. Přiložením kontaktního mikrofonu je možno toto chvění sejmout i ze zdí, které jsou několik desítek centimetrů tlusté. Přenosové vlastnosti pevných materiálů jsou nevypočitatelné, proto je potřeba najít na zdi vhodné místo, kde je slyšitelnost a srozumitelnost největší. Snímací kvality kontaktního mikrofonu se dají zvýšit předvrtáním otvoru do zdi na poslechové straně a k mikrofonu připevnit hřebík a pomocí vhodného gelu (gel, který se používá, např. při vyšetření na sonografii) zafixovat do připravené dírky. [3]

Stetoskop SINGLE

Jednostranný stetoskop SINGLE je jednoduchý základní prostředek pro poslech srdce, plic a orgánů lidského těla. Dá se také použít jako speciální kontaktní odposlech díky své dobré akustické odezvě. Cena stetoskopu včetně DPH je okolo 150 Kč. [11]

Obr. 12 Stetoskop SINGLE [11]

1.2.3.2 Elektronické stetoskopy

Elektronické stetoskopy jsou v podstatě mikrofony, které jsou založeny na principu přiloženého hrnečku na zeď. Pro zvýšení kvality odposlouchávané místnosti se skládají ze dvou částí, a to z mikrofonu a citlivého zesilovače. Umožňují nám získávat informace nejen ze zdí, ale také např. ze stoupaček inženýrských sítí. Tento druh mikrofonů používá např. zásahová jednotka a armáda. [2]

Elektrický stetoskop

Elektrický stetoskop je malý valeček o průměru 36 mm a délky 43 mm. Váha i se zabudovanou baterií je 200 g. Na čele stetoskopu najdeme zásuvku 3,5 mm pro sluchátka, USB zásuvku pro nabíjení, knoflík pro seřizování optimální citlivosti, který nám současně slouží i pro zapnutí stetoskopu. Prostupnost přes zeď, panel, sklo i dřevo je až 60 cm. Balení obsahuje sluchátka, nabíječku do sítě a USB kabel. K zařízení můžeme přímo připojit sluchátka nebo diktafon pro nahrávání. Cena včetně DPH činí kolem 2.500 Kč. [24]

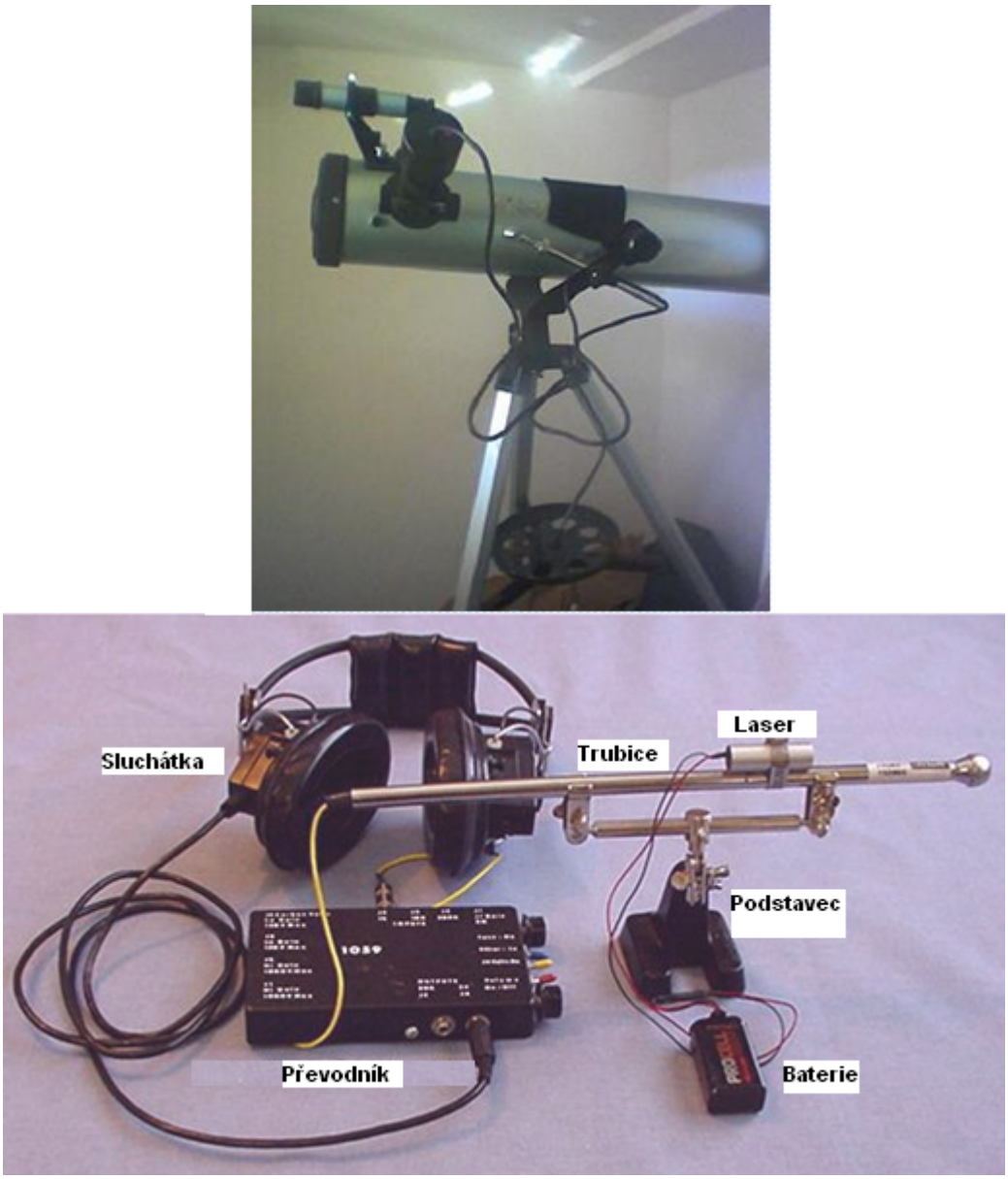
Obr. 13 Elektrický stetoskop [24]

1.2.3.3 Laserové odposlechové zařízení

Při laserovém odposlechu se využívá jako nosného prvku laserového paprsku. Laser vznikl v druhé polovině 20. století a našel využití ve vojenské, špionážní i průmyslové oblasti. Laser je elektromagnetické záření, které využívá toho, že laserové paprsky o stejné vlnové délce směřující stejným směrem a pomocí stimulované emise jsou zesilovány. Toto dává paprsku ostré svazkování a typickou barvu. Laserové odposlechové zařízení se řadí do speciálních optoelektronických odposlechových zařízení.

Souprava laserového odposlechu se skládá z vysílací jednotky s optickým zaměřovačem a příslušným přijímačem. Laserový paprsek se pomocí vysílače namíří přes okno na rezonanční stěnu v odposlouchávané místnosti. Zvukové vlny, které uvnitř místnosti vznikají hovorem, rozechvívají (rozvibrují) rezonanční stěnu, z které se odráží modulovaný paprsek. Přijímačem je zachycen modulovaný paprsek, který je následně demodulován do srozumitelné řeči. Tento typ odposlechu je velmi náchylný na fyzikální zákony, neboť je obtížné najít optimálně kolmý přístup k okenním tabulkám v odposlouchávané místnosti. V odposlouchávané místnosti mohou být použita jen čirá skla bez žaluzií a podobných doplňků. Když jsou splněny výše uvedené podmínky, pak je laserový odposlech velmi nebezpečný. Laserové odposlechy z důvodu náročného nastavení využívají většinou odposlechoví experti, kteří mají vysílače opatřeny puškohledem. Laserový odposlech je nejpřesnější, nejlépe nahraný, nejčistší a nejkvalitnější. Oproti jiným druhům odposlechů

není laserový odposlech ovlivňován povětrnostními podmínkami, proto dosah bývá až několik set metrů. Profesionální laserové odposlechové přístroje obsahují laserové nebo ultrafialové zdroje. Při dosahování kvalitních odposlechů na velké vzdálenosti pracujeme s 35mW zářivým zdrojem. Z důvodu poranění očí, by se neměl paprsek v žádném případě dostat do oka. Podle kvality se dá laserový odposlech pořídit za ceny od 5.000 Kč do cca 500.000 Kč. [2]



Obr. 14 Příklady laserového zařízení k odposlechu [34]

1.2.4 Zařízení pro odposlech telefonní linky

Telefonní přístroj, který se i v dnešní době určitě ještě najde v každé kanceláři, je dokonalým místem pro úkryt odposlechového zařízení. Telefonní přístroj je vhodný pro odposlech z důvodu jeho umístění (stůl v kanceláři) a spojení s okolním světem čtyřžilovým drátovým vedením. Telefonní přístroj je použitelný k odposlechu dvěma způsoby, a to přímo k odposlechu telefonního hovoru nebo k monitorování místnosti. [2]

1.2.4.1 Drátový odposlech telefonní linky

Drátový odposlech telefonní linky se provádí přímým napojením zesilovače nebo magnetofonu na přívodní telefonní linku. Umístění záleží na přístupu k uzlům kabelové trasy. Musí se vždy jednat o vedení sledované linky, ve které je signál ještě v analogové podobě a ne až za koncentrátorem, kde dochází k digitalizaci a kde se slučují i ostatní telefonní linky. Pokud použijeme přímé napojení na telefonní linku, doporučuje se použít odposlech, který je vybaven funkcí VOX (automatické spuštění hlasem) nebo aktivace při zvednutí sluchátka.

Zařízení pro odposlech vedení telefonní linky TO LINE 1

Souprava zařízení pro odposlech telefonního vedení je vybavena propichovacími svorkami, které připojíme paralelně na vedení telefonní linky. Dále záznamovým zařízením, které se spustí při zvednutí sluchátka nebo v okamžiku zvonění telefonu, dočasně se přeruší při odmlčení a automaticky aktivuje po promluvení. Napájení je přímo z telefonní linky. Délka výstupního kabelu je 50 cm a jeho ukončení tvoří klasický 3,5 mm jack, na který můžeme připojit velkou škálu diktafonů, sluchátek, reproduktorů apod. Cena se záznamovým zařízením je kolem 9.200 Kč včetně DPH. [19]

Obr. 15 Zařízení pro odposlech telefonní linky TO LINE 1 [19]

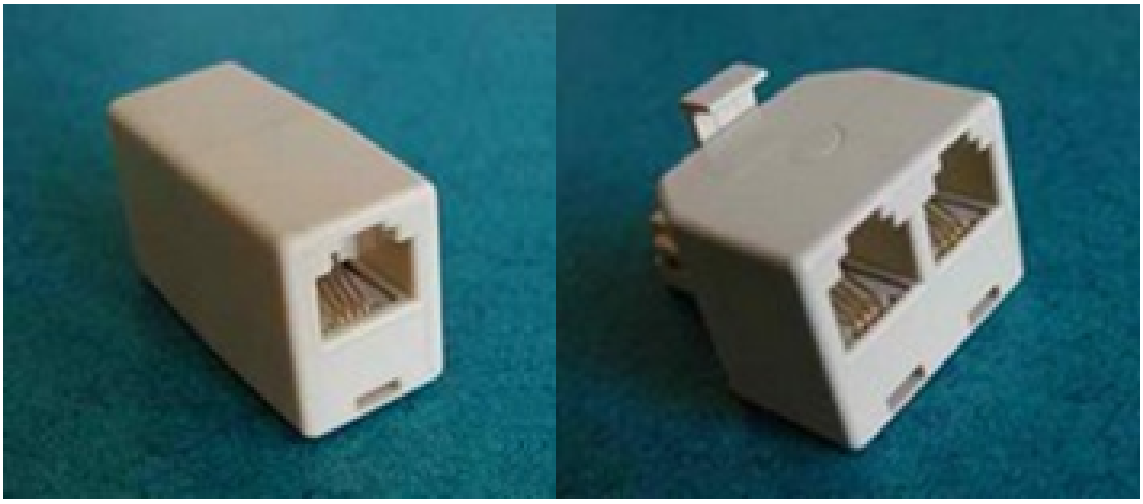
1.2.4.2 Odposlech telefonní linky pomocí radiových vln

Z technických důvodů není vždy možné se napojit na telefonní linku mimo odposlouchávaný prostor. Proto existují taková zařízení pro odposlech telefonní linky, která přenáší hovor na záznamové zařízení pomocí radiových vln. Také četnost pohybu a pravidelná kontrola v blízkosti zařízení není žádoucí. Miniaturní telefonní vysílač se připojí přímo do zásuvky telefonní linky. Telefonní síť nám zajišťuje zdroj napájení 60 V, anténu a zdroj odposlouchávaného signálu. Kvalitní radiopřijímače jsou dvoukanálové, přičemž jeden kanál vysílá telefonní hovor a druhý zvuky z okolního prostředí, kde se vysílač nachází.

Radiový odposlech telefonní linky MUD-TLF- Spojka

Radiový odposlech telefonní linky – MUD-TLF-Spojka je miniaturní telefonní vysílač o výkonu 10 mW pracující na frekvenci 430 MHz zabudovaný do telefonní spojky. Po zvednutí sluchátka automaticky vysílá obě strany telefonního hovoru, který přes spojku prochází. Napájení je z telefonní sítě, dosah vysílače je 100 m–200 m v závislosti na okolním terénu. Rozměry (12 x 12 x 21) mm a cena je cca 13.200 Kč včetně DPH. Jako přijímač musíme použít příslušné zařízení, které přijímá frekvenci 430 MHz. Instalaci

zvládne i úplný technický laik. Za stejnou cenu můžeme pořídit vysílač v provedení rozdvojky telefonní linky. Parametry jsou stejné jako u spojky, ale rozměry jsou větší, a to jako klasická telefonní rozdvojka. [31]



Obr. 16 Radiový odposlech telefonní linky MUD-TLF spojka a rozdvojka [31]

1.2.5 Odposlech mobilního telefonu

Odposlech mobilního telefonu je v poslední době celkem rozebíranou věcí, jak médii, tak i politiky apod. Většina nezačleněných lidí v této problematice si myslí, že operátor je jediný, kdo může mobilní telefon odposlouchávat a zaznamenávat jeho polohu, ale pravda je úplně jiná. Odposlech mobilního telefonu se zdá být velmi lákavý, a to z důvodu přenosu informací na velkou vzdálenost, ale také proto, že většina lidí má mobilní telefon stále u sebe.

1.2.5.1 Odposlech za doprovodu operátora

Odposlech za doprovodu operátora využívá především Policie ČR, neboť operátor musí ze zákona poskytnout policii přístup ke konkrétním uživatelům nebo jen číslům. Možnost nelegálního odposlechu pomocí operátora, neboli spíše zaměstnance operátora, je zcela vyloučený. Každý zaměstnanec, který má přístup k odposlouchávání hovorů, musí mít za sebou bezpečnostní prověrky u NBÚ. Místa, kde se dají hovory odposlouchávat, jsou pod neustálým přísným dohledem. Kdyby zaměstnanec chtěl nelegálně odposlouchávat hovor, byl by rychle odhalen a následně potrestán.

1.2.5.2 Odposlech v GSM síti

Bezpečnější než odposlech s pomocí operátora, pro běžného špiona, je odposlech mobilního telefonu přímo ze vzduchu s následným dešifrováním signálu. V Evropě však existuje asi jedna firma, která prodává mobilní zařízení, které je schopné ze vzduchu precizně monitorovat a dešifrovat hovor vedený v síti libovolného operátora. Cena takového zařízení se pohybuje kolem 15 milionů Kč, což je i pro náročného špiona příliš velká finanční částka. Z důvodu cenového a technického zatížení se o tomto zařízení nebudu ve své práci více rozepisovat, protože u většiny špionů jej nenajdeme. [2]

Podobný systém, jež je popsán výše pro odposlech mobilního telefonu v GSM síti, využívá i Policie ČR pod krycím názvem „Agáta“. Jak „Agáta“ vypadá? Je to nenápadná, bíle zbarvená, někdy i potisknutá smyšlenými nápisy dodávka většinou značky Wolsvagen Transportér nebo Ford Transit. Na vozidle je skrytě zabudovaná parabolická anténa a vně vozidla se nachází spleť různě využitelných počítačů. Cena takové dodávky se pohybuje kolem 15 milionů Kč.

Na obsluhu „Agáty“ má Policie ČR školené specialisty. „Agáta“ sama o sobě mobilní telefony neodposlouchává, ale je jednou z důležitých součástí celého odposlechového systému. „Agáta“ slouží k zjišťování telefonního čísla u předplacených SIM karet jednotlivých operátorů. Většina zločinců používá právě předplacené SIM karty. Z důvodu zdánlivé anonymity jsou právě předplacené SIM karty využívány pachateli trestných činů. Policie ČR vyjede s „Agátou“ do míst předem určených, kde se zrovna nachází podezřelá osoba. Podle síly signálu zjistí, jaký mobilní telefon pachatel momentálně při hovoru užívá včetně určení jeho telefonního čísla. Takto policie získá telefonní číslo podezřelé osoby a může spustit odposlech za pomoci operátora.

Hlavně před několika lety si Policie ČR pomocí „Agáty“ zjišťovala i přesnou polohu vytipovaného mobilního telefonu. K tomu Policii ČR stačilo znát jen telefonní číslo vytipované osoby. Průběh hledání polohy mobilního telefonu probíhal následovně. Policie ČR jezdila s „Agátou“ po určeném kraji a natahovala na sebe vysílané signály z mobilních telefonů místo toho, aby signál šel až na BTS stanici. Tímto postupem zjistila celkem přesně, kde se nachází vytipovaný mobilní telefon. V dnešní době může také Policie ČR pomocí systému „Agáta“ zjišťovat, kde se právě nachází vytipovaný mobilní telefon, ale

mnohem jednoduší je zjistit polohu pomocí mobilního operátora. Bližší informace o „Agátě“ nejsou známy, protože si je Policie ČR velmi pečlivě chrání. [4]

1.2.5.3 Odposlech za použití upraveného mobilního telefonu

Odposlech upraveného mobilního telefonu není také možnou variantou pro každého špiona. Zde nám přibývá starost, jak upravený mobilní telefon dostat do rukou odposlouchávané osoby, a ještě k tomu, aby ho vůbec odposlouchávaná osoba používala a neměla ho jen do náhrady. Viz kapitola 2.

1.2.6 Optické systémy

K průniku do sledované oblasti či místnosti je mnoho jednoduchých i složitějších metod optického pronikání. Jednou z metod optického sledování je, např. z kanceláře protějšího domu můžeme dalekohledem nebo za pomoci fotoaparátu sledovat lidi, které k vám do kanceláře vstupují, zdržují se tam apod. Tímto způsobem je možné zjistit, s kým máte pracovní schůzky, chování zaměstnanců apod. Tato metoda sledování byla závislá na lidské obsluze, a proto byla málo účinná a efektivní. Lidské oko, jakož nedokonalý lidský orgán, byl nahrazen fotoaparátem a později videotechnikou. Pro velké rozměry videotechniky bylo její nasazování k pronikání do sledované oblasti těžkopádné a komplikované. Velkou změnu přinesl vynález CCD čipu a malých velkokapacitních pamětí. Tyto věci zmenšily rozměry videotechniky až několikanásobně. [2]

1.2.6.1 Minikamery s CCD čipem

Minikamery s CCD čipem se vyznačují zejména malými rozměry, dobrými rozlišovacími vlastnostmi, pevným objektivem, velkou citlivostí, zpravidla automatickou clonou a kompenzací protisvětla. Díky CCD čipu, kterým jsou minikamery vybaveny, se jejich využití našlo v průmyslu, u policie, ale také u špionážní techniky. Kamery jsou malých rozměrů v řádu milimetrů až centimetrů (pro představu, např. ve velikosti kostky cukru). Pro ukrytí objektivu nám postačí otvory o velikosti 5 mm, u dírkových objektivů nám postačí i otvor o velikosti jen 1 mm. Pro své malé rozměry jsou vhodné pro zabudování do různých předmětů nejen denní potřeby např. do nábytku, televizoru, radiopřijímače, knihy, hodin, psacího pera, hraček, umělých květin, telefonů, tiskáren, počítačů apod. Vhodným umístěním jsou i osvětlovací zařízení, prvky požární techniky, prvky zabezpečovacího

zařízení, krabice elektrických rozvodů na 230 V nebo telefonních rozvodů apod. Pro jednotlivé umístění je důležitá velikost přístroje a velikost otvoru pro objektiv. Při použití jehlového objektivu je úhel záběru asi 60º v horizontální rovině, při větším záběru musí být použit objektiv s běžnou čočkou. Protože minikamery se vyznačují celkem velkou spotřebou elektrické energie, je jejich umístění většinou na místech, kde je zajištěno trvalé připojení k síti. [2]

Použitím světlovodných kabelů můžeme prodloužit objektiv až o několik centimetrů. Kabely mohou být pevné nebo ohebné, proto se dají protáhnout nejen otvorem ve zdi. Jejich použití je bez ztráty kvality obrazu, ale ztrácí se světelnost. Při použití světlovodného kabelu pro prodloužení objektivu můžeme využít jednoho kabelu pro přenos optického i akustického signálu. Některé minikamery jsou totiž vybaveny už i elektretovými mikrofony pro přenos nejen obrazu ale i zvuku. [2]

1.2.6.2 Příklady minikamer s CCD čipem včetně příslušenství

Minikamera 281-TIC 725

Barevná minikamera 281-TIC 725 s pinhole objektivem o průměru 3,9 mm, má díky svým malým rozměrům využití zejména při skryté montáži. Minikamera je vybavena 1/3“ CCD čipem. Počet pixelů je 500 na 582 s rozlišení 380 TV řádků. Citlivost je 1 Lux a výstupní signál je v PAL normě. Napájení je na 12 V DC a rozměry jsou (30 x 30 x 18) mm. Cena včetně DPH je okolo 2.000 Kč. [7]

Obr. 17 Minikamera 281-TIC 725 [7]

Minikamera MO-S1616P

Barevná ultra miniaturní kamera MO-S1616P s rozměry (16 x 16 x 11) mm je vybavena senzorem CMOS 1/3" s technologií CCIQ. Minikamera má rozlišení 380 TV řádků s vysokou citlivostí 1 Lux. Kamera je vhodná ke skryté montáži, má širokoúhlý tenký pinhole objektiv o průměru 3,1 mm. Napájení může být bateriové nebo ze sítě v rozmezí 5–12 V DC. Cena včetně DPH je kolem 5.300 Kč. [31]

Obr. *18 Minikamera MO-S1616P [31]*

Minikamera HI-RES

Barevná minikamera HI-RES s dírkovým objektivem, kterému stačí otvor o průměru 1,2 mm a je vybavena 1/4“ CCD čipem. Objektiv zabírá až 78° záběru s rozlišením 380 TV řádků s citlivostí 0,2 Lux. Minikamera má rozměry (11 x 11 x 18) mm, váhu jen 8 g a je určena k 12 V DC napájení. Cena včetně DPH je okolo 9.000 Kč. [7]

Obr. 19 Minikamera HI-RES [7]

HI-RES minikamera je díky svým miniaturním rozměrům vhodná pro různé instalace. Pro inspiraci uvádím některé skryté instalace v různých předmětech. Podobná minikamera ukrytá v propisovací tužce se dá na internetových aukcích pořídit už za cenu kolem 1.500 Kč.

Obr. 20 Umístění minikamery HI-RES [7]

1.2.6.3 Uchování videosignálu

Některé kamery jsou už od výrobce vybaveny paměťovou kartou pro ukládání nahrávky. Jejich použití je určeno jen tam, kde po určitém čase můžeme zajistit výměnu paměťové karty. Doba uložené nahrávky je závislá na kapacitě paměťové karty, zpravidla je to několik hodin. Při ukládání většího množství dat z kamer se používají pomalu nahrávací

videorekordéry, DVD-rekordéry, PC apod. Na jednu videokazetu se dá pořídit až 960 hodin záznamu. Při použití DVD-rekordéru nebo PC je délka záznamu závislá na kapacitě paměti. V dnešní době je velký pokrok v kapacitách a rozměrech pamětí, proto se i v kapse dají přenášet záznamy o délce stovek hodin. Možností jak ušetřit čas na paměti je v době klidu nic nenahrávat. Spustit nahrávání můžeme ručně nebo pomocí PIR detektoru, dveřního kontaktu, nastavením časových intervalů apod. Tohoto se využívá při šetření místa na paměťových mediích. [2]

1.2.6.4 Přenos videosignálu

Výstupní signály z kamer jsou normovány, tudíž je můžeme přímo připojit do audio-video vstupů na videorekordérech, DVD-rekordérech, televizorech, monitorech apod. Při přenosu signálu na klidné místo a následném připojení k monitoru využíváme různých přenosových cest. Jednou z nich je kroucená dvojlinka, u níž potřebujeme na straně kamery umístit vysílač a na druhém konci přijímač signálu. Další možností je použití tenkého stíněného kabelu. Z důvodů velkých ztrát signálu jsou tyto varianty připojení jen na vzdálenosti cca 50 m. Nejčastěji se používá koaxiální kabel, který je stíněný. Signál můžeme vést na velké vzdálenosti jen s malými ztrátami. Nevýhodou je však jeho velký průměr a také to, že se nesmí příliš ohýbat. Jednou z možností je také použití světlovodného kabelu. Na začátku i konci kabelu musí být použity optické převodníky (konvertory). Výhodou je, že není náchylný na žádné rušení a může být veden souběžně i s rozvody síťového napětí na velké vzdálenosti. V některých případech pro přenos signálu z kamery se dá použít i telefonní nebo ISDN linka, přičemž musíme použít patřičný převodník.

Přenos videosignálu může být i bezdrátový pomocí mobilní sítě GSM, UMTS, frekvenčního pásma 2,4 GHz apod. Speciální aplikace využívají vysílací frekvence 900 MHz a výše. Modulace bývá zpravidla kmitočtová, šířka pásma 5 MHz a výkon vysílače od 100 mW do 2 W. Pro znemožnění náhodného zachycení signálu nechtěnou osobou, bývá signál zašifrován. [2]

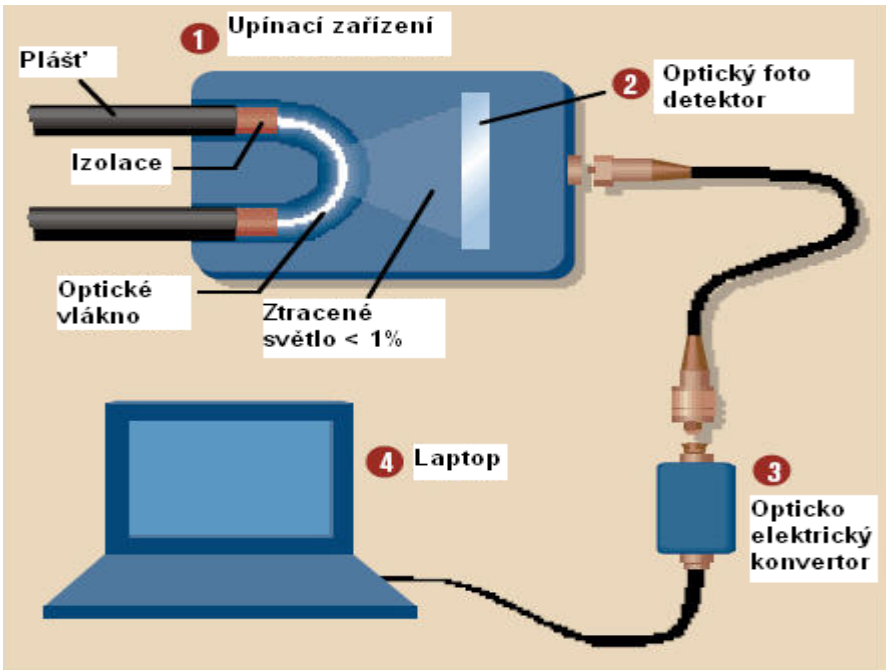
1.2.7 Odposlech signálu vedeného za použití světlovodného kabelu

Světlovodný neboli optický kabel je jedním z novějších druhů přenosových cest pro přenos signálu. Jeho využití se uplatňuje především v telekomunikačních sítích, kde bývá přenášeno velké množství dat. Jeho využití najdeme i pro přenos signálu, např.

z kamerového systému. Přenášený signál je přenášen ve formě světelného paprsku. Pro přenos po světlovodném kabelu je zapotřebí přenášený signál přeměnit na světelný, a to pomocí optických převodníků (konvertorů). Výhodou světlovodných kabelů je, že nepodléhají žádným rušivým vlivům a že je po nich možnost převést velké množství dat na velké vzdálenosti. Protože světlovodné kabely nevytváří žádná elektrická rušení, proto je můžeme vést v jednom kabelovém tunelu společně s kabely s vysokým napětím. Oproti ostatním kabelům je nevýhodou precizní a nákladné spojování světlovodných kabelů a nemožnost vedení napájení.

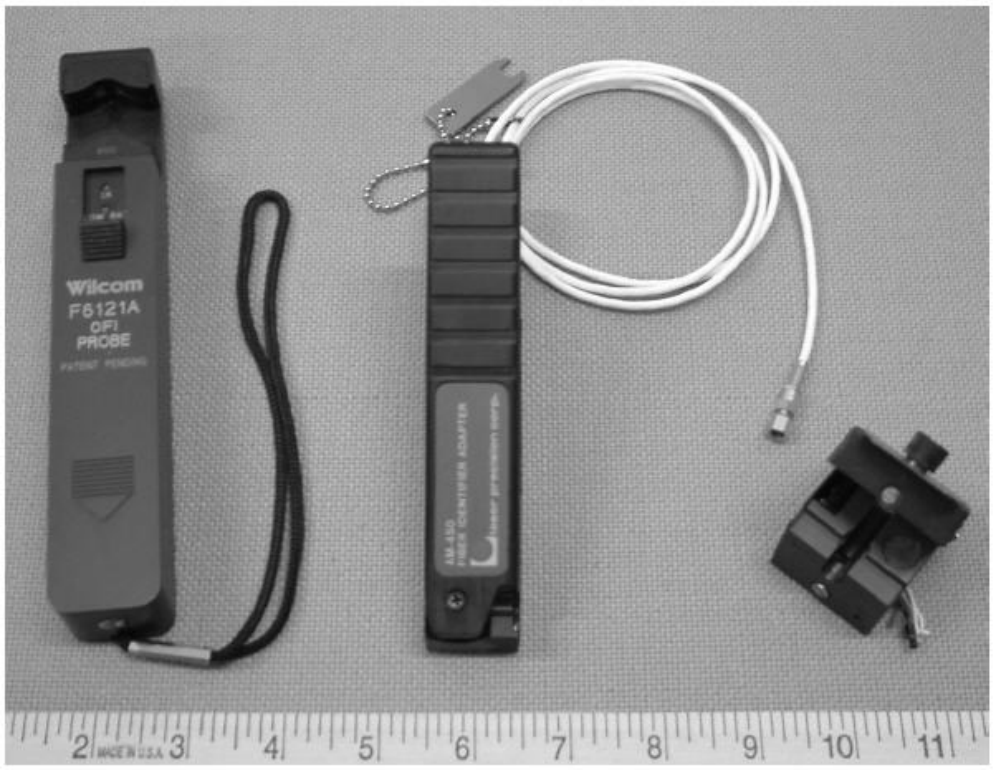
Většina výrobců a také prodejců uvádí na svých internetových stránkách či jiných upoutávacích prostředcích, že světlovodné kabely jsou zabezpečeny proti odposlechu a jinému druhu nelegálního získávání dat. Bohužel tomu tak ve skutečnosti není.

Pro odposlech světlovodného kabelu nám postačí sada k tomu určená, která se dá pořídit za částku kolem 20.000 Kč. Při odposlechu světlovodného kabelu je nezbytný fyzický přístup ke kabelu, dále pak nám postačí si zakoupit odposlechovou sadu určenou k tomuto druhu odposlechu a laptop se speciálním softwarem. [5]



Obr. 21 Zapojení odposlechu světlovodného kabelu [5]

Z obrázku 21 vidíme, že je nejprve třeba najít ten správný světlovodný kabel, který chceme odposlouchávat. Následně jej musíme patřičně ohnout a upevnit do upínacího zařízení. Část ohybu musíme zbavit izolace, aby světlo mohlo být zachyceno optickým fotodetektorem. Pak stačí přenést získaný optický signál do opticko-elektrického konvertoru, kde se přemění optický signál na požadovaný elektrický. Získaný elektrický signál zpracujeme pomocí speciálního softwaru na laptopu.



Obr. 22 Zařízení pro odposlech světlovodného kabelu [5]

Nejběžnější způsob, jak chránit světlovodné kabely proti tomuto typu odposlechu je, aby se ke světlovodným kabelům zamezil fyzický přístup. Při nadměrném ohnutí kabelu je možnost odhalení, a to z důvodu velkého útlumu přenášeného signálu. Pro větší bezpečnost přenášených dat se doporučuje všechna důvěrná data bezpečně zašifrovat.

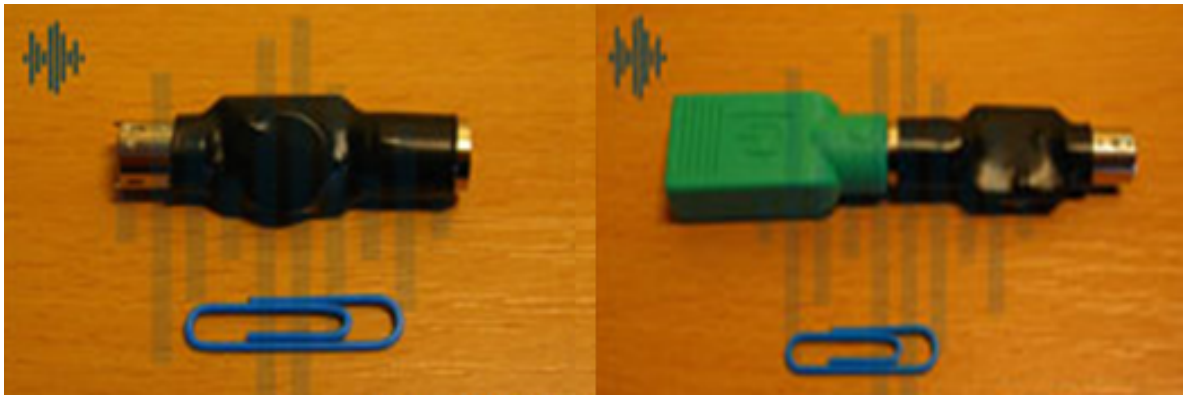
1.2.8 Záznamové zařízení pro činnost na PC

V dnešní době, kdy je velký vývoj výpočetní techniky, se většinou všechny informace získané v různých odvětvích podnikání i státní sféře, ukládají na pevné disky v počítačích. Počítač je výborný prostředek pro skryté naistalování speciální techniky, kterou jsem uvedl

už výše. Většina z nás při koupi nebo po provedení opravy počítače nezjišťuje, jestli se v PC nenachází nějaká součástka navíc. Proto je počítač dobrou volbou pro skrytí speciální techniky. V některých případech může být počítač ukraden nebo jeho informace z něj zkopírovány apod. Tyto druhy odcizení dat v mé bakalářské práci rozebírat nebudu. Na dnešním trhu se nachází různé prvky a softwary pro zjišťování činnosti na počítači. Konkrétním softwarem se budu zabývat v kapitole 2.

Zařízení pro zaznamenání činnosti klávesnice připojené k PC KEYLOG TIME

Zařízení pro zjištění činnosti na klávesnici připojené k PC KEYLOG TIME je ideální nástroj, který nám umožní mít kompletní přehled o dění na počítači. KEYLOG TIME je malá „redukce“ mezi konektorem klávesnice a počítačem, která zaznamenává veškerá data (všechny stisky kláves) a ukládá je do své vlastní pevné paměti (přes 75 stránek A4 psaného textu), funguje na všech počítačích s PS2 kompatibilní klávesnicí, pomocí redukce funguje také na USB klávesnicích. Pro získávání dat z klávesnice není nutná žádná softwarová instalace. KEYLOG TIME nelze vystopovat žádným antivirovým nebo spywarovým programem. Instalace a odinstalace se provádí pouhým vyjmutím a zasunutím konektoru klávesnice při vypnutém počítači. Uložená data lze velmi snadno číst a celé zařízení se ovládá pomocí textového editoru, např. poznámkového bloku. Při procházení uložených dat se po 25 sekundách následné nečinnosti poznámkový blok vypne, a to z důvodu nebezpečí odhalení. Díky své vestavěné baterii se nám zaznamenaná data ukládají přehledně podle přesného data a času, které lze různě vyhledávat i tisknout. Využití zařízení KEYLOG TIME je možností, jak zjistit hesla, která jsou do počítače zadávána ještě před startem operačního systému. Například přihlašovací hesla do Windows, hesla do Biosu, „hardwarová“ hesla pro start počítače apod. Integrovaná 3V lithiová baterie v případě delšího nepoužívání počítače vydrží bez dobíjení cca 6 měsíců a její následné úplné nabití z počítače trvá cca 12 hodin. Integrovaná paměť má kapacitu 128 kB což nám postačí na cca 130 000 stisků klávesnice. Rozměry jsou (47 x 14,5 x 10) mm. Cena včetně DPH je kolem 4.700 Kč. Nevýhodou použití KEYLOG TIMU je fyzická přístupnost ke sledovanému počítači, a to z důvodu nainstalování, odistalování redukce. Nevýhodou v některých případech může být také fyzický přístup ke sledovanému počítači při získávání zaznamenaných dat. KEYLOG TIME můžeme nechat skrytě namontovat přímo do určené klávesnice. [16]



Obr. 23 Záznamové zařízení pro zjištění činnosti na klávesnici připojené k PC KEYLOG TIME, vpravo i KEYLOG TIME s USB redukcí [16]

2 NOVÉ TECHNOLOGIE VE SPECIÁLNÍ BEZPEČNOSTNÍ TECHNICE

Nové technologie jsou zaměřeny na sledování s přenosem signálu na velké vzdálenosti a také s určením aktuální polohy, kde se právě nachází sledovaná osoba či věc nebo také právě to, co se s ní děje.

2.1 Monitorování mobilního telefonu pomocí speciální úpravy operačního systému

Odposlech upraveného mobilního telefonu je zajímavou věcí, při které můžeme zjistit, kde se zrovna sledovaná osoba nachází a co se děje v jejím okolí apod. Odposlech upraveného mobilního telefonu není možnou variantou pro každého špiona. Přibývá starost, jak upravený mobilní telefon dostat do rukou odposlouchávané osoby a ještě, aby ho vytyčená osoba vůbec náležitě používala a neměla ho jen do náhrady.

Mobilní telefony, které jsou vhodné pro úpravu, musí pracovat na jednom ze tří následujících operačních systémů.

- Windows Mobile.
- Black Berry.
- Symbian.

Pro úpravu je zapotřebí mít k dispozici mobilní telefon na dobu potřebnou pro přeinstalování operačního systému. Doba přeinstalování se pohybuje v jednotkách až desítkách minut podle typu telefonu. Další možností je koupit si už upravený mobilní telefon.

Některé druhy mobilních telefonů, které jsou vhodné pro úpravu operačního systému: **Nokia –** 3250, 5320, 5500, 5800, 6120, 6124, 6210, 6630, E51, E60, E65, E66, N70, N71, N72, N73, N80, N81, N85, N91, N92, N95, N97 a mnoho dalších nokií.

Samsung – SGH-i400 SGH-i520, SGH-i550, SGH-i560, SGH-G810, SGH-L870, I7110, INNOV8, apod.

LG – KT610, KT615, KS10 apod. [14]

Funkce, které nám může upravený telefon nabídnout, jsou následující:

- **Dálkový odposlech** – umožňuje při zavolání z nastaveného čísla skrytě slyšet okolní prostor cílového telefonu a to díky svému vestavěnému mikrofonu. Cílový telefon tento hovor nijak neindikuje. Pozn.: tato funkce neumožňuje poslouchat právě probíhající hovor.
- **Dálkové SMS nastavení** – uživatel nepotřebuje mít fyzický přístup k cílovému telefonu pro různá nastavení aplikace, vše se dá jednoduše nastavit pomocí SMS zpráv. Každý klient má své unikátní nastavovací tvary SMS zpráv.
- **Archivace SMS zpráv a e-mailu** – zaznamenány jsou všechny odeslané i přijaté SMS zprávy, mobilní e-mail a jejich obsah je zaslán na klientův webový účet. Podporovány jsou všechny světové jazyky včetně českých znaků.
- **Archivace informací o hovorech** – na klientův webový účet jsou zaslány všechny informace o hovorech (čas, délka trvání a počet). Pokud je telefonní číslo v adresáři cílového telefonu, pak se jeho název (jméno) také zobrazuje.
- **GPS sledování polohy** – pravidelné zjišťování aktuální polohy pomocí vestavěného GPS přijímače v cílovém telefonu je zasíláno do webového účtu zákazníka. Přesnost lokalizace GPS se pohybuje okolo 3 m až 5 m v dosahu viditelnosti družice. Systém GPS potřebuje „vidět“ na satelity, tudíž není podle něj možné lokalizovat telefon např. v budovách nebo podzemních garážích.
- **Odposlech probíhajícího hovoru** – umožňuje při zavolání z nastaveného čísla slyšet právě probíhající komunikaci na cílovém telefonu a to díky skrytému konferenčnímu hovoru. Cílový telefon konferenční hovor na displeji nezobrazuje.
- **SMS o probíhajícím hovoru** – pomocí dálkových SMS zpráv uživatel nastaví zájmová čísla, o kterých chce být informován v případě volání. Jakmile proběhne odchozí nebo příchozí hovor, cílový telefon pošle SMS zprávu na mobilní telefon klienta.
- **Zabezpečený webový účet** – webový účet, kde se zákazníkovi přehledně zobrazují všechny záznamy, je chráněn pomocí speciální technologie. Server, kde jsou uložena získaná data, je mimo prostor Evropské unie. Heslo pro vstup do systému si klient může libovolně měnit.

- **Pokročilé vyhledávání v záznamech** – na webovém účtu má uživatel možnost přehledně v záznamech vyhledávat podle jednotlivých kritérií např. vyhledávání klíčových slov v e-mailu nebo SMS zprávách, telefonního čísla a kontaktního jména podle času apod.
- **Stažení záznamů z účtu** – pokud je potřeba zálohovat uložené záznamy ze zabezpečeného účtu např. před kompletním smazáním účtu, nebo když chce klient analyzovat data bez připojení k internetu, lze kompletní nebo vybrané záznamy stáhnout do souborů ve formátech PDF apod.
- **SMS při změně SIM karty** – pokud je SIM karta v cílovém telefonu vyměněna za jinou, aplikace okamžitě pošle na zákazníkovo číslo SMS zprávu s novým telefonním číslem. Tato funkce slouží k tomu, aby zákazník věděl, kam uskutečnit dálkový odposlech, nastavovací SMS apod. Tato funkce se hodí zejména při odcizení telefonu.
- **Záznam a poslech hovorů** – cílový telefon ukládá obsah hovorů jako zvukovou nahrávku a odesílá ji na server. Zákazník má potom ze svého webového účtu možnost záznamy poslechnout a uložit si je. Díky této funkci má klient např. maximální přehled o svých hovorech.
- **Výběr aktivních funkcí** – zákazník pomoci nastavovacích SMS si může kdykoliv zapnout či vypnout jakoukoliv výše uvedenou funkci. [13]

Výhody upraveného mobilního telefonu jsou zřejmé z výše uvedených funkcí.

Nevýhody upraveného mobilního telefonu jsou následující:

- Bliknutí nebo rozsvícení displeje při provádění dálkového odposlechu.
- Při dlouhém dálkovém odposlechu, když se odposlouchávaný mobilní telefon nachází v blízkosti např. radiopřehrávače, může vyvolávat dlouhé vrnění v reproduktoru, jako když se mobilní telefon připojuje k BTS stanici při ztrátě signálu, ale mnohem delší. Toto dlouhé vrnění se může stát velmi nápadným.
- Nutnost zpřístupnění k mobilnímu internetu a následného používání, protože data jsou na zabezpečený server odesílána pomocí mobilního internetu.

- Při dlouhém nebo častém provádění dálkového odposlechu se v cílovém telefonu výrazně vybijí baterie.
- Při provádění dálkového odposlechu je lepší vlastnit takový mobilní telefon, který je vybaven funkcí vypnutí mikrofonu, a to z důvodu, abychom neslyšeli např. kýchnutí, dýchání na cílovém telefonu.
- Nutnost použití alespoň jedenkrát GPS navigaci.
- Nutnost přístupu k internetu pro získávání dat ze zabezpečeného serveru.
- Při nepoužívání GPS navigace a mobilního internetu na sledovaném mobilním telefonu se může sledovaná osoba pozastavit nad výpisem od operátora, proč musí platit za to, co nepoužívá. Všechny informace jsou totiž na zabezpečený server posílána jako data a jsou zpoplatněna dle příslušného tarifu.

Využití takto upraveného mobilního telefonu, kromě skryté špionáže, může být

- Pro starostlivé rodiče, kteří chtějí mít ochranu svých dětí před vlivy dnešního světa (drogy, šikana, kriminalita, únosy atd.).
- Pro osoby pečující o své blízké se sníženými mentálními schopnostmi nebo fyzickým handicapem.
- Pro lidi, kteří potřebují chránit a zabezpečit svůj majetek.
- Pro majitele a ředitele firem střežící své know-how, obchodní tajemství a objednávky.

Cena výše popsané úpravy mobilního telefonu se pohybuje okolo 27.000 Kč včetně DPH. Doba použitelnosti výše uvedených funkcí, po kterou je můžeme využívat, bývá zpravidla omezena na jeden rok. Po uplynutí doby jednoho roku je možnost dalšího prodloužení služby za snížené ceny, dle společnosti, která úpravu provádí. Pro prodloužení výše uvedené služby nám postačí na sledovaný mobilní telefon poslat jen určitý kód a funkce nám budou znovu fungovat po dobu jednoho roku. Většinou nám pro zjištění informací, které jsme chtěli, postačí i kratší doba než je jeden rok. [15]

2.2 Monitorování počítače pomocí speciálního softwaru

Osobní, firemní stolní počítač nebo laptop (dále jen počítač) nás každodenně spojuje s okolním světem. Komunikace se svými důležitými obchodními partnery, kolegy, známými apod. se stále z větší míry uskutečňuje pomocí počítače např. práce projektantů je z velké části prováděna na počítači, kde si uchovávají a propracovávají své nápady a projekty. Proto bychom pro ochranu svého počítače měli udělat určitá opatření, aby se nemohl jen tak někdo dostat k datům, které jsou v něm uloženy apod. Při nasazení softwarového monitorování počítače a následného vyhodnocení získaných dat, nás mohou takto získaná data tzv. oddělat nebo také podle místa nasazení, mohou posílit mezilidské vztahy.

Software, který byl speciálně vyvinut pro skryté monitorování počítače, odposlech komunikace a získávání přihlašovacích údajů a hesel, je poskytován v profesionální české verzi a je kompatibilní se všemi běžnými operačními systémy včetně Windows Vista a Windows 7. Software bývá dodávaný na CD, flashdisku, e-mailem nebo také přímo za asistence technika určité firmy. CD nebo flashdisk stačí vložit do počítače, který chceme monitorovat, a poté dojde k automatickému skrytému instalování softwaru. Počítač, na který je software nainstalován, je znám jen tomu, kdo ho tam nainstaloval. Nastavení softwaru, jakož je rozsah monitorování, odesílání informací na e-mail apod. je většinou určen po předchozí domluvě. [17]

Funkce, které nám software pro monitorování počítače zajišťuje, jsou následující:

- Kompletní monitorování všech činností a komunikace na počítači.
- Získávání přihlašovacích údajů a hesel na počítači.
- Odposlech okolního prostoru počítače.
- Velmi vysoký stupeň utajení přítomnosti a činnosti programu v počítači.
- Česká verze s plnou podporou místního prostředí včetně české znakové sady.
- Inteligentní prohlížeč získaných informací z počítače.
- Dostupnost informací na dálku (email, FTP, síť, flashdisk).
- Přístup k nastavení a získaným datům z počítače má pouze určená osoba. [17]

Informace, které nám software pro monitorování počítače diskrétně zajistí, jsou následující:

- **Nahrávání obrazovky** – získáme videozáznam všeho, co se zobrazilo na monitoru. Snímek obrazovky je vytvořen po každé změně v obraze. Objem získaných dat dosahuje cca 100 MB za jeden den běžné práce na PC.
- **Sledování a záznam stisknutých kláves** – psaný text, webové adresy, e-mailové adresy, hesla a přihlašovací údaje.
- **Odposlech a záznam komunikace** – přehledné a relevantní ukládání textové a hlasové komunikace uskutečněné pomocí programů Skype, ICQ, QIP, Miranda, Windows Live Messenger, MSN Messenger, Google Talk a Yahoo Messenger.
- **Monitorování sociální sítě Facebook** – získáme kompletní přehled přátel, statusů, komentářů, fotografií, soukromých zpráv a chatu.
- **Sledování a záznam aktivity na internetu** – prohlížené stránky, navštívené odkazy, internetový chat, konverzace na seznamce atd.
- **Monitorování e-mailových zpráv** – kontrola e-mailových schránek přes webové rozhraní a pomocí poštovních programů, např. Outlook, Windows Mail, Thunderbird.
- **Odposlech a záznam prostoru okolo počítače** – ukládání všech rozhovorů, které zachytí mikrofon počítače.
- **Bezpečné ukládání získaných dat** – zaznamenané informace jsou ukládány v šifrovaném datovém souboru, který je uložen na pevném disku počítače.
- **Zasílání získaných dat** – automatické zasílání v pravidelných intervalech na libovolný e-mail, FTP nebo do síťové složky v rámci lokální sítě.
- **Inteligentní prohlížení záznamů** – získané informace jsou ukládány podle data a času a třídí se do jednotlivých kategorií. To nám urychlí vyhledávání informací, které se uložily před týdnem, měsícem, rokem apod.
- **Vyvolání menu** – nastavovací a prohlížecí menu se vyvolá pomocí unikátního přístupového hesla na klávesnici sledovaného počítače. [17]

Výhody softwarového monitorování počítače jsou zřejmé z výše uvedených funkcí.

Nevýhody softwarového monitorování počítače jsou následující:

- Pro odposlouchávání okolního prostředí počítače je nutností, aby v počítači byl přítomen mikrofon. Většina stolních počítačů nemá od výroby přímo zabudován mikrofon. Laptopy jsou už z velké části od výroby osazeny vestavěnými mikrofony.
- Při monitorování počítače, který nebývá připojen k internetu nebo jiné síti, je podmínkou fyzický přístup pro získání skrytě uložených dat.

Výhodou, ale také nevýhodou, může být přeinstalování operačního systému počítače s kompletním přemazáním pevného disku. Výhodou je to tehdy, kdy už nainstalovaný software ke sledování dění, co se na počítači děje nepoužíváme, např. z důvodu už odhalených chtěných činností nebo z nějakých neznámých důvodů, pro které může být software odhalen a následně řešen jeho postih. Nevýhodou to může být v době, kdy jsme do počítače nainstalovali software pro sledování prováděných činností na počítači, ale bohužel hned druhý den byl na daném počítači přeinstalován operační systém a kompletně vymazán pevný disk. Nevýhoda je v tom, že se musíme znovu fyzicky přiblížit ke sledovanému počítači a znovu do něho nainstalovat software pro sledování.

Na internetu je v dnešní době mnoho prodejců, kteří nabízejí různé sledovací programy, ale jejich skrytá funkčnost je v drtivé většině lehce odhalena mnohdy i začínajícími uživateli. U dalších nabízených programů je zase zapotřebí asistence IT specialisty. Pro výběr spolehlivého a ne příliš obtížného softwaru na obsluhu či instalaci je důležitý správný výběr prodávajícího.

Prodejce by nám měl zajistit:

- Úvodní konzultaci.
- Nastavení programu podle požadavků klienta.
- Zaškolení v obsluze programu.
- Licenci programu.
- Technickou podporu (po telefonu, e-mailem apod.).

Software, který je výše popsán, se dá pořídit za cenu okolo 6.000 Kč včetně DPH. [17]

3 ODHALOVÁNÍ TECHNICKÝCH BEZPEČNOSTNÍCH PRVKŮ POMOCÍ OBRANNĚ TECHNICKÉ PROHLÍDKY

V úvodu této kapitoly bych chtěl upozornit na to, že většina dnes používaných prostředků pro zjišťování legálně či nelegálně umístěných speciálních bezpečnostních prostředků v kontrolovaném prostředí je jen „drahou hračičkou“. Obranně technická prohlídka (dále jen OTP) by měla být nedílnou součástí prevence každého podniku. Při ztrátě nebo odcizení dat, vyzrazení know-how společnosti se může podnik dostat do velkých problémů nebo může být také přiveden i ke krachu. Smyslem provádění OTP je kompletní zjištění možných cest pro nelegální únik informací z kontrolovaného objektu. OTP se zaměřuje na zjišťování, zda se v objektu nachází či nenachází odposlechové nebo jiné nelegálně nainstalované zařízení pro přenos informací z klíčového objektu. Jedná se o kompletní posouzení objektu z technického hlediska, ale také dalších návrhů potřebných pro další opatření. OTP bude efektivní pouze tehdy, jen když po jejím vyhodnocení budou dodržována režimová, organizační a technická opatření, která budou cíleně navržena. [2]

3.1 Postup při provádění OTP

Výstupem provedené OTP je v mnoha případech volně psaný text, který v úvodu dokumentuje, kdy, kde a jakými prostředky byla OTP vykonána. Dále následuje vyjádření k jednotlivým postupům, ve smyslu, zda bylo nalezeno určité množství nelegálně či legálně umístěných prostředků pro získávání informací. Na závěr je uveden souhrn zjištěných nedostatků a následné doporučení, opatření vedoucí k dostatečnému zajištění informační bezpečnosti kontrolovaných prostor. [36]

3.1.1 Přípravná část

Při provádění OTP většinou zákazníci potřebují, aby byla vykonána rychle, diskrétně a také podle konkrétního případu i utajeně. Zjišťování dokumentace, ve které je určeno konkrétní umístění, kde vedou telefonní, elektrická, optická a jiná vedení, je v praxi z velké části nemožné. Je tomu tak z důvodu, že se mnohdy jedná o prostory, které mají jen pronajaty, a sídlí v nich zároveň třeba i několik firem. V mnoha případech je prakticky nemožné dát dohromady jakoukoliv skutečně validní dokumentaci. Dokumentace, která se po

zákazníkovi požaduje, je většinou prokázání vztahu k prostoru platným dokladem, např. nájemní smlouvou. [36]

3.1.2 Fyzická kontrola

V této části dochází k fyzické kontrole kontrolovaných prostor. Dále se provádí rozebírání a následné složení všech prostředků, ve kterých by se mohlo nacházet legálně či nelegálně umístěné zařízení, sloužící k vyzrazování informací z kontrolovaných prostor. Kontrolovanými prostředky jsou např. zásuvky, prodlužovací šňůry, rozdvojky, světla, ústředny, telefonní přístroje, různé druhy čidel a jiná elektronická vybavení. Rozdělávání nábytku a podobného vybavení není v mnoha případech možné, a to z důvodu, že se jedná např. o starožitné kusy nebo umělecká díla, u kterých je cizí zásah vyloučen a byl by vizuálně zcela zjevný. Proto si musíme dávat pozor např. na staré lampy, rádia a jiná elektrická zařízení, která slouží nejen jako dekorace. [36]

3.1.3 Kontrola vysílaných frekvencí

Kontrola vysílaných frekvencí se provádí pomocí triangulace spektra radiových frekvencí, (dále jen spektra RF), především za pomoci spektrálních analyzátorů a k nim příslušných přístrojů, které nám umožňují odhalit jakékoliv analogové, šifrované nebo jinak maskované přenosy odposlechových prostředků. Kontrola se z počátku provádí v dostatečné vzdálenosti mimo kontrolovaný prostor. Uvnitř prostoru se provádí až v další fázi kontroly. Těmito měřeními se do přístroje uloží celé prozkoumávané RF spektrum s vysokým rozlišením a dynamickou hloubkou. Především se kontrolují frekvenční pásma od akustických přes provoz KV, VKV, UKV až k mikrovlnným pásmům nad 3 GHz. To vše se provádí metodou spektrální analýzy a subanalýzy signálů. Těmito měřeními se zhotoví seznam všech vysílaných radiových frekvencí v kontrolovaných prostorech. Seznam vysílaných frekvencí může pak usnadnit periodické OTP. [36]

3.1.4 Kontrola nelinearit

Myslím si, že v dnešní době, kontrolu nelinearit využívají jen firmy, které se považují za velké odborníky v provádění OTP. Kontrola pomocí nelineárního detektoru je už minulostí. Nelineární detektor funguje na následujícím principu: nelineární detektor vysílá

elektromagnetické pole a signál, který se odrazí od polovodičového přechodu, se vyhodnocuje. [36]

Důvody, proč nepoužívat detektor nelinearit jsou následující:

- Detektory reagují nedefinovaně na jakýkoliv konvenční polovodič v „zorném poli“ detektoru.
- Použití detektorů nelinearit v praxi způsobuje především množství planých poplachů způsobených např. odrazy.
- Chytřejší osoba, která nelegálně nainstaluje prostředek k získávání informací ze zájmového prostoru, by zájmový prostor „prošpikovala polovodičovými nástrahami“.
- Je nezvratně prokázáno, že detektory nelinearit, jako je NR-900, Katran, Orion apod., jsou zcela překonatelné a na dnes běžně dostupné odposlechy mnohdy vůbec nereagují.
- Nikdo (ani sám výrobce) nedokáže se 100% zárukou deklarovat, že i ty nejmodernější detektory nelinearit budou vždy spolehlivě reagovat. [36]

3.1.5 Ostatní kontroly

Důvodem provádění ostatních kontrol je, že např. vysílač je umístěn úplně na jiném místě než mikrofon, někdy i v jiném patře kontrolovaného prostoru. Proto je hodně důležité, jakými přístroji budeme OTP provádět. Profesionální firmy, které provádí OTP na profesionální úrovni, si své používané speciální metody pro ostatní měření uchovávají v tajnosti. Je to z důvodu, aby neobohacovali konkurenci (pro ni) novými postupy a metodami. Jedná se o náhradní metodu za detekci nelinearit a postupy pro dohledání GSM/GPRS modulů upravených pro odposlech prostoru a přenosy dat. [36]

3.1.6 Příklad spektrálního analyzátoru používaného profesionálními společnostmi

Spektrální analyzátor řady FLS od firmy Rohde&Schwarz

Spektrální analyzátor je měřicí přístroj, který měří v kmitočtové doméně, graficky definovaně zobrazuje kmitočet [kHz, MHz, GHz] a výkonovou úroveň [dBm, dBmV, dBμV apod.] VF signálu (nosného signálu) s definovanou opakovatelnou přesností. Tyto přístroje patří do skupiny kalibrovaných měřidel. Z principu své funkce

jsou oproštěny od všech nedostatků, které se týkají kategorie přehledových přijímačů. Měřící rozsah v RF pásmu je od 9 kHz do 3 GHz. Díky svým malým rozměrům a možným napájením z baterie, je vhodný k rychlému přemístění. Jeho váha je cca 8 kg. Cena se pohybuje při rozsahu spektrálního analyzátoru do 3 GHz okolo částky 300.000 Kč, a při rozsahu do 18 GHz však cena strmě stoupá až do částek převyšujících 2.000.000 Kč. Spektrální analyzátory se většinou vyrábí až na základě zákazníkem stanovených požadavků, proto zde uvedené ceny musíme brát s patřičnou rezervou. [35]

Obr. 24 Spektrální analyzátor řady FLS [35]

4 PŘEDPOKLÁDANÝ VÝVOJ

Firmy zabývající se vývojem, výrobou, instalací a provozem speciální bezpečností techniky musely v posledních letech zcela zásadně změnit dříve zažité metody. Důvodem je rychlý vývoj různých komunikačních sítí, různých druhů radiových přenosů, rozvoj výpočetní techniky, rozmach zabezpečovacích systémů a mnoho dalších jiných podnětů. Před 10 lety málokdo vlastnil laptop nebo mobilní telefon. Vzdálený přenos informací se uskutečňoval od psacího stolu za pomocí stolního počítače a pevné telefonní linky. Dnešní mobilní telefony využívají operační systém, podobající se operačnímu systému, na kterém pracují stolní počítače či laptopy. Tyto prostředky, jakož jsou laptopy, mobilní telefony, které lidé využívají každodenně, slouží nejen ke komunikaci s okolním světem, ale také jsou vhodným místem pro uložení velkého objemu dat, a proto se staly nemalým terčem pro nelegální získávání dat. Možnost krádeže mobilního telefonu nebo laptopu je mnohem větší, než když jsme používali pouze stolní počítač a pevnou telefonní linku, které se nacházely, např. v chráněném prostoru firmy. Taková ztráta dat uložených v laptopu nebo mobilním telefonu může přinést velké komplikace nejen ve firemních a osobních záležitostech. Laptop či mobilní telefon můžeme z nedbalosti ztratit nebo nám také může být velmi rychle odcizen. Např. při večerním návratu ze zaměstnání, když si neseme veškeré důležité nápady a pracovní informace uložené na pevném disku v laptopu a všechny kontakty, důvěrné SMS a nafocené fotografie uložené v mobilním telefonu. Oba typy přístrojů máme v kufříku, který neseme v ruce. Náhle přiběhne zloděj, který nám rychlým a velmi šikovným tahem vytrhne kufřík z naší ruky a zmocní se veškerých našich důležitých dat. Než si uvědomíme, co se vůbec stalo, zloděj svým rychlým sprintem a s naším ukradeným kufříkem dobíhá k připravenému motorovému vozidlu, do kterého nasedá, a my jen vidíme, jak se nám rychle vzdaluje z dohledu. Takto lehce můžeme přijít o svá data, důležité kontakty či cenné informace.

Vývoj speciálních bezpečnostních prostředků bude v dalších letech spíše více zaměřen do úprav používaných softwarů, než do samotného vývoje nových typů speciálních bezpečnostních prostředků. Prostředky speciální bezpečnostní techniky, které známe v dnešní době, budou pomalu nahrazovány takovými prostředky, které nabývají miniaturních rozměrů, což je velmi praktické z důvodu ukrytí do předmětů nejen denní potřeby, ale také do věcí, které zřetelně vidíme za pomoci zvětšovacího zařízení. Miniaturizace prostředků je zapříčiněna velkým rozvojem nanotechnologií. Oblast vývoje

odposlechových zařízení, které nám zaznamenávají nebo přenáší jen zvuk, bude určitě klesat nebo bude úplně zastavena. Stane se tak z důvodu velkého rozmachu audio-video zařízení, které nám současně zaznamenávají nebo přenáší zvuk a obraz. Velikost audio-video zařízení bude v porovnání s nynějšími zvukovými zařízeními několikrát menších rozměrů, a to z důvodu už zmíněné nanotechnologie.

Vývoj speciální bezpečnostní techniky, se kterou nemusíme mít fyzický přístup do sledovaného objektu, nebude určitě zaostávat. Využívat se bude nejen infračerveného nebo mikrovlnného záření. Pro speciální úpravu softwaru v mobilním telefonu se určitě v blízké době nebude muset dávat mobilní telefon do rukou specialisty. Pro úpravu softwaru postačí poslat MMS zprávu na vytyčený mobilní telefon a po jejim otevření se na displeji mobilního telefonu zobrazí vtipný obrázek, který zaujme vytyčenou osobu, např. pro ženu květina, pro muže auto apod., po otevření této MMS zprávy se skrytě v mobilním telefonu bude software upravovat. Využití určitě najdou i záření, jakož jsou špionážní mouchy a jiná podobná zařízení, která jsou schopna nepozorovaně sledovat, např. co se děje v kanceláři v 9. patře. Taková zařízení jsou dnes sice teprve ve vývoji, ale např. americká armáda je začíná zkoušet zapojovat ke sledování různě znečištěných prostředí, přes která se musí dostat ke zdroji znečištění apod.

Důležitou roli bude mít vývoj přenosových bezdrátových cest, které už dnes jsou poměrně na vysoké úrovni. Také se budou muset řešit přenosy většího množství dat, a to z důvodu přenosu zvukové a obrazové nahrávky současně.

Prostředky, které slouží k odhalování nelegálně nainstalovaných speciálních prostředků, neměly by ve svém vývoji zaostávat, protože speciální bezpečnostní prostředky budou čím dál miniaturnějších rozměrů a jejich ukrytí bude čím dál tím více rafinovanější.

II. PRÁVNÍ DIMENZE

5 ZÁKONNOST NASAZOVÁNÍ TECHNICKÝCH PROSTŘEDKŮ

Technické prostředky nasazené pro získávání obrazové nebo zvukové nahrávky mohou být použity jen se souhlasem zaznamenávaných osob nebo za předpokladu zjišťování potřebných informací k rozjasnění vážných trestných činů daných zákonem.

5.1 Právní podmínky přístupu k informacím

Právní řád České republiky chrání svými předpisy osobnost člověka i jeho soukromí, což je v první řadě rozebráno v Listině základních práv a svobod. Základními podmínkami o užívání informací (údajů) se věnují články 7, 10, 13, 17 Listiny základních práv a svobod.

Článek 7 se zabývá nedotknutelností osoby a jejího soukromí, které mohou být omezeny v případech stanovených zákonem. [29]

Článek 10 se zabývá zachováním lidské důstojnosti, osobní cti, dobré pověsti a ochraně svého jména. Dále chrání před neoprávněným zasahováním do soukromého i rodinného života. Neoprávněné shromažďování, zveřejňování nebo jiné zneužívání informací (údajů) o osobě, je v uvedeném článku také chráněno. [29]

Další článek, který nesmí být porušen při nasazování např. audio-videotechniky, je **článek 13**, který se zabývá tím, že nesmí být porušeno listovní tajemství ani tajemství jiných písemností a záznamů, a to bez ohledu na to, v jaké formě a jakými prostředky jsou uchovány nebo pořízeny. Výjimkou jsou případy, které stanoví zákon. Tajemství zpráv podaných telefonem, e-mailem nebo jinou novou metodou předávání informací, je také chráněno. [29]

Z druhého oddílu, který se zabývá politickými právy, se věnuje **článek 17** o ochraně údajů. Listinou základních práv a svobod je zaručena svoboda projevu a práva na informace. To znamená, že každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu. Nepřípustná je cenzura v jakékoliv podobě. Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti. Státní orgány a orgány územní

samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon. [29]

5.2 Odposlech telefonního hovoru

Používání odposlechu telekomunikačního provozu bude s největší pravděpodobností trestným činem. Porušování tajemství dopravovaných zpráv, podle § 239, odst. 1, pís. b) Trestního zákona, a to bez ohledu na to, za jakým účelem byla takto dopravovaná zpráva zachycena a využití těchto zpráv, je také trestným činem zejména podle § 240, odst. 1.

Pokud sledovaná osoba svolí pachateli, že u ní může být proveden odposlech a záznam telekomunikačního provozu, tak nedochází k jednání, které by mohlo být kvalifikováno jako úmyslné porušení „tajemství“, neboť poškozený svým předchozím projevem vůle, směřujícím k umožnění pachateli seznámit se s obsahem veškerých jím podávaných zpráv v telefonním provozu, dal pachateli na srozuměnou, že žádné tajemství v tomto telekomunikačním provozu nebude sdělovat. Tento souhlas však lze stěží získat od třetí osoby, pokud nebude před započetím telefonního hovoru výslovně upozorněna na to, že je její hovor zaznamenáván. Takže při neupozornění třetí osoby je takto pořízený záznam brán jako trestný čin. Legálně použít odposlech telekomunikačního provozu můžou jen instituce popsané níže. [28]

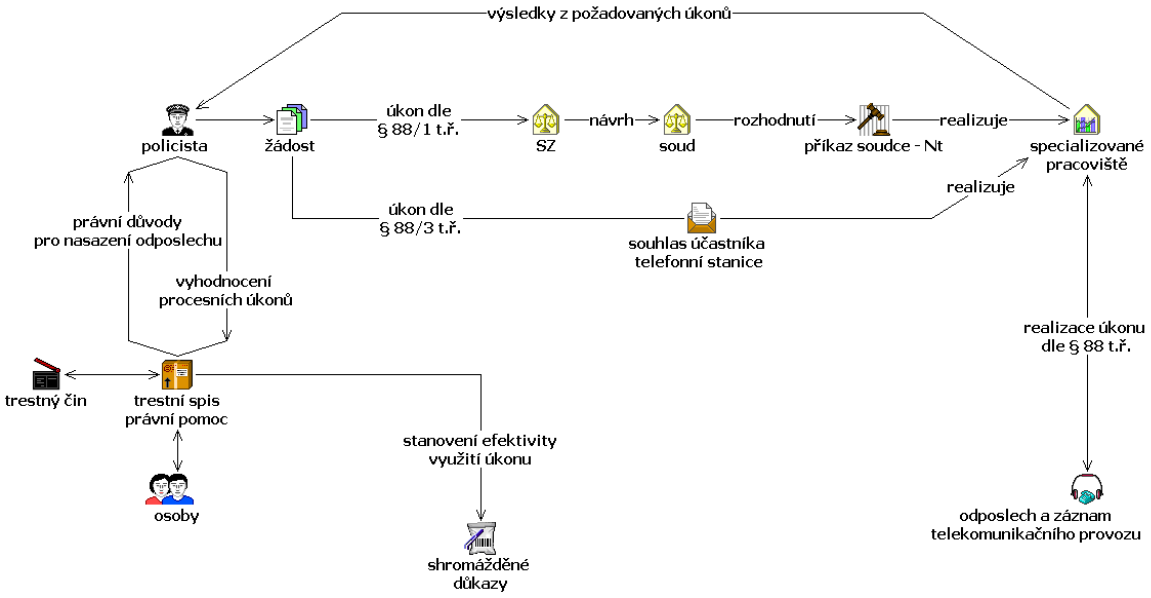
Odposlech telekomunikačního provozu za asistence policejního orgánu dle § 88 odst. 1, 3 Trestního řádu

Policejní orgán, při návrhu státnímu zástupci na odposlech a záznam telekomunikačního provozu, musí předpokládat, že jím budou zjištěny významné skutečnosti důležité pro objasnění trestného činu. Návrh musí mít písemnou podobu a musí v něm být obsaženo stručné zhodnocení skutkového stavu trestní věci a také odůvodnění provedení odposlechu.

Samozřejmostí návrhu je přínos informací pro trestní řízení, co se od odposlechu a záznamu telekomunikačního provozu očekává a dále také, po jakou dobu bude odposlech a záznam prováděn. Doba, po kterou odposlech a záznam telekomunikačního provozu je realizován, je maximálně 6 měsíců, ale na dalších 6 měsíců může být prodloužena.

Odposlech a záznam telekomunikačního provozu může policejní orgán nařídit i sám, ale jen v případě, kdy má písemný souhlas účastníka stanice, která má být odposlouchávána.

Vzhledem k tomu, že při odposlechu a záznamu telekomunikačního provozu dochází k velkému zásahu do základních práv a svobod občanů, je nezbytné dodržovat zásadu zdrženlivosti a přiměřenosti (§ 2 odst. 4 Trestního řádu). [1]



Obr. 25 Postup při odposlechu a záznamu telekomunikačního provozu orgány Policie ČR [1]

5.3 Právní normy upravující sledování zvukových, obrazových a jiných záznamů

Zákon č. 169/1999 Sb., o výkonu trestu odnětí svobody

Ustanovení § 18, odst. 4 zákona č. 169/1999 Sb. obsahuje oprávnění vězeňské služby seznamovat se formou odposlechu s obsahem telefonátů odsouzených. Podle § 25, odst. 4 prováděcí vyhlášky č. 345/1999 Sb., zjistí-li vězeňská služba při kontrole záznamu telefonátů nebo přímém odposlechu, že odsouzený komunikuje se svým advokátem, je povinna odposlech ihned zrušit, záznam o jeho obsahu zničit a informace, které se v této souvislosti dozvěděla, nesmí použít. [9]

Zákon č. 13/1993 Sb., Celní zákon

Ustanovení § 37 d, zákona č. 13/1993 Sb. umožňuje využívat operativní techniku celnímu úřadu, a to pouze tehdy, existuje-li důvodné podezření, že byl spáchán, např. trestný čin porušování povinnosti o oběhu zboží s cizinou (§ 124 Trestního zákona), porušování předpisů o nakládání s kontrolovaným zbožím (§ 124 a–124 c Trestního zákona), zkrácení daně, poplatku a podobné dávky (§ 148 Trestního zákona), nebo že se připravuje spáchání takového trestného činu. Operativní techniku lze používat pouze v případech, kdy odhalování takovýchto trestných činů je jiným způsobem neúčinné, nebo podstatně ztížené, a to pouze na dobu nezbytně nutnou, na povolení soudce v místě příslušného krajského soudu. Použití odposlechu zajišťuje Policie ČR. [25]

Zákon č. 154/1994 Sb., o Bezpečnostní informační službě

Ustanovení § 10 zákona č. 154/1994 Sb. umožňuje použití zpravodajských prostředků na základě žádosti a následného povolení soudcem v místně příslušného vrchní soudu. Žádost musí obsahovat druh zpravodajské techniky, která má být použita, dobu trvání jejího použití, základní identifikační údaje o osobě, vůči které má být zpravodajská technika použita, pokud jsou tyto údaje známy, číslo telefonní nebo jiné obdobné stanice, pokud z ní má být prováděn odposlech, popřípadě záznam, a je-li známo, i místo použití zpravodajské techniky; má-li být zpravodajská technika použita vůči ústavnímu činiteli nebo jejím použitím má být zasahováno do práva nedotknutelnosti obydlí, musí být tato informace součástí žádosti [26]

Zákon č. 283/1991 Sb., o Policii České republiky

Ustanovení § 36 zákona č. 283/1991 Sb. umožňuje využívat operativní techniku orgánům policie, a to pouze tehdy, kdy odhalování zvláště závažných trestných činů (tj. trestných činů uvedených v § 62 Trestního zákona nebo trestných činů, na něž je stanovena horní hranice trestní sazby nejméně osm let) je jiným způsobem neúčinné nebo podstatně ztížené, a to na nezbytně nutnou dobu. Nutností je povolení soudce v místě příslušného krajského soudu. [10]

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

Ustanovení § 158 d zákona č. 141/1961 Sb. umožňuje sledování osob a věcí (dále jen „sledování“). Tím se rozumí získávání poznatků o osobách a věcech prováděných

utajovaným způsobem technickými nebo jinými prostředky. Pokud policejní orgán při sledování zjistí, že obviněný komunikuje se svým obhájcem, je povinen záznam s obsahem této komunikace zničit a poznatky, které se v této souvislosti dozvěděl, nijak nepoužít. Sledování, při kterém mají být pořizovány zvukové, obrazové nebo jiné záznamy, lze uskutečnit pouze na základě písemného povolení státního zástupce. Pokud má být sledováním zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků, lze uskutečnit jen na základě předchozího povolení soudce. Při vstupu do obydlí nesmí být provedeny žádné jiné úkony než takové, které směřují k umístění technických prostředků. Povolení lze vydat jen na základě písemné žádosti. Žádost musí být odůvodněna podezřením na konkrétní trestnou činnost, a jsou-li známy, též údaji o osobách či věcech, které mají být sledovány. V povolení musí být stanovena doba, po kterou bude sledování prováděno a která nesmí být delší než šest měsíců. Tuto dobu může ten, kdo sledování povolil, na základě nové žádosti, písemně prodloužit vždy na dobu nejvýše šesti měsíců. Bez splnění výše uvedených podmínek lze sledování provést jen tehdy, pokud s tím výslovně souhlasí ten, do jehož práv a svobod má být sledováním zasahováno. Je-li takový souhlas dodatečně odvolán, sledování se neprodleně zastaví. [27]

6 DRUHY PRÁVNÍCH POSTIHŮ ZA NEZÁKONNÉ NASAZENÍ SPECIÁLNÍCH PROSTŘEDKŮ

Při používání prostředků speciální bezpečnostní techniky a následným využíváním informací prostřednictvím nich získaných, se musí řídit danými pravidly stanovenými zákonem. Jiné využívání je dle zákona trestáno.

6.1 Trestní následky

Provádění prostorového odposlechu není trestným činem. Informace získané tímto způsobem však mohou být snadno zneužity pro spáchání jiné trestné činnosti např. vydírání, útisk, apod. Zveřejnění odposlechů a obrazů pořízených ze skrytých kamer, odposlechu je bráno jako trestný čin. Trestněprávní následky jsou většinou posuzovány podle toho, jaká újma na zdraví, majetku či zisku vznikla, a také jestli osoba, která zmíněné informace vynesla, byla už někdy nějak trestána apod.

Trestní zákon § 178 Neoprávněné nakládání s osobními údaji

1. Kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiné osobě shromážděné v souvislosti s výkonem veřejné správy, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem.

2. Stejně bude potrestán, kdo osobní údaje o jiném získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, byť i z nedbalosti, sdělí nebo zpřístupní, a tím poruší právním předpisem stanovenou povinnost mlčenlivosti.

3. Odnětím svobody na jeden rok až pět let nebo zákazem činnosti nebo peněžitým trestem bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se údaj týká,

b) spáchá-li čin uvedený v odstavci 1 nebo 2 tiskem, filmem, rozhlasem, televizí nebo jiným obdobně účinným způsobem, nebo

c) spáchá-li čin uvedený v odstavci 1 nebo 2 porušením povinností vyplývajících z jeho povolání, zaměstnání nebo funkce. [30]

Trestní zákon § 180 Trestný čin obecně nebezpečný

1. Kdo z nedbalosti způsobí nebo zvýší obecné nebezpečí anebo ztíží jeho odvrácení nebo zmírnění, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

2. Odnětím svobody až na tři roky nebo zákazem činnosti bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 těžkou újmu na zdraví nebo smrt,

b) spáchá-li takový čin proto, že porušil důležitou povinnost vyplývající z jeho zaměstnání, povolání, postavení nebo funkce nebo uloženou mu podle zákona, nebo

c) způsobí-li takovým činem značnou škodu.

3. Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 2 písm. b)

a) škodu velkého rozsahu, nebo

b) těžkou újmu na zdraví nebo smrt.

4. Odnětím svobody na tři léta až deset let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 2 písm. b) těžkou újmu na zdraví nebo smrt více osob. [6]

Trestní zákon §181 Porušování povinnosti při hrozivé tísni

Kdo zmaří nebo ztíží odvrácení nebo zmírnění hrozivé tísně, která přímo postihuje větší skupinu osob, tím, že bez závažného důvodu

a) odepře pomoc, která je mu podle zákona uložena nebo k níž se zavázal, nebo

b) zmaří poskytnutí takové pomoci jinou osobou, bude potrestán odnětím svobody až na tři roky nebo zákazem činnosti nebo peněžitým trestem. [6]

Trestní zákon § 182

1. Kdo úmyslně ohrozí provoz

a) veřejného telekomunikačního zařízení, zařízení držitele poštovní licence nebo zařízení pro hromadnou veřejnou dopravu,

b) ochranného zařízení proti úniku znečisťujících látek,

c) zařízení energetického nebo vodárenského,

d) veřejného ochranného zařízení proti požáru, povodni nebo jiné živelné pohromě,

e) podmořského kabelu nebo podmořského potrubí,

f) ochranného nebo ochranného zařízení proti leteckým a jiným podobným útokům nebo jejich následkům, nebo

g) podobného obecně prospěšného zařízení, bude potrestán odnětím svobody na až tři léta nebo peněžitým trestem.

2. Odnětím svobody na jeden rok až šest let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 poruchu provozu obecně prospěšného zařízení, nebo

b) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu. [6]

ZÁVĚR

Speciální bezpečností technika se stále vyvíjí, její vzhled a umístění je rafinovanější. Prostředky pro získávání relevantních informací mohou zásadním způsobem urychlit práci bezpečnostních složek státu. Pomocí těchto prostředků dochází celkem velkým způsobem k zásahu do práva na ochranu soukromí. Na jedné straně tedy stojí snaha státu zajistit bezpečnost obyvatelstva, ale to pouze za podmínky omezení práv svých občanů, aby jim tuto bezpečnost mohl zajistit. Odhalování vážných trestných činů, přípravy na teroristický útok apod., by se určitě bez prostředků speciální bezpečností techniky neobešlo.

Používání speciální bezpečností techniky k zjišťování relevantních informací, mohou být konkurenční výhodou. Odposlech a záznam mobilního telefonu za asistence mobilního operátora není už jen záležitostí, kterou využívá pouze Policie ČR. Mobilní telefon s upraveným softwarem může sloužit k monitorování dění a polohy mobilního telefonu. Tato funkce mobilního telefonu může být do jisté míry velmi zajímavou.

Z bakalářské práce je patrné, že prostředky speciální bezpečností techniky určené pro získávání relevantních informací, jsou i za použití úplným technickým laikem velmi nebezpečnou zbraní v konkurenčním boji. Finanční částky, za které můžeme tyto prostředky pro získávání informací zakoupit, jsou mnohdy zanedbatelné, ve srovnání s odcizenými informacemi. Většina těchto prostředků se dá jednoduše zakoupit prostřednictvím internetového obchodu. Při vydírání a podobných praktikách, můžou prvky speciální bezpečností techniky zapříčinit nemalé zbytečné úniky např. finančních prostředků.

Každá firma, která chce v současné době uspět na trhu, musí dbát na ochranu vnitropodnikových dat a informací, aby společnosti jejich zneužitím nevznikly škody nemalého charakteru v porovnání s vynaloženými náklady na zajištění prostředků proti informačním únikům.

ZÁVĚR V ANGLIČTINĚ

Special safety equipment is being developed, its outlook and location is more and more artful. The means for gaining relevant information can essentially make the work of the safety related state organizations quicker. With a help of the means comes to an encroachment of the right to a privacy policy. On one hand the state tries to ensure the safeness of the people, on the other hand the state has to limit the rights to a privacy policy of the people, to be able to safe them. The uncloaking the crime could not be done without the special safety equipment. The special safety equipment application used to gain relevant information may be a competitive advantage. Not only Police of the Czech republic has been using the monitoring or recording of mobile telephones with an assistance of a mobile operator. The mobile telephones with special software can be used to location monitoring. This function of the mobile telephone can be interesting in some detail.

It is evidenced by this work, that the means of the special safety equipment designed for gaining relevant information are, even used by a very technical non-specialist, very dangerous weapon in a concurrent competition. The sum of money, the special safety equipment can be bought for, is not very high compared to information larceny. It is simply possible to buy these means in a web-based shop. Within the intimidation and other crimes like that may the special safety equipment means be the cause of a large information (or other) leak.

Every firm willing to be successful on the trade has to care of the intra-plant data and information safety, so that the plant could not have loss losing and abusing its data compared to the sum of money spent on the means against the information lose.

SEZNAM POUŽITÉ LITERATURY

[1] *Analýza úkonů dle § 88 odst. 1, 3 a § 158d odst. 2, 3, 6 trestního řádu za rok 2007.* Policejní prezidium České republiky úřad služby kriminální policie a vyšetřování. Květen 2008.

[2] LAUCKÝ V. *Speciální bezpečnostní technologie*. 1. vyd. Univerzita Tomáše Bati ve Zlíně, 2008. ISBN 978-80-7318-762-0.

[3] *Magazín Security*. Vydává FAMily media, spol. s. r. o., ročník IX, vydání číslo 50, 6/2002 – listopad prosinec, 6x ročně, ISBN 1210-8723.

[4] *Bestpage.krasl.com* [online]. 2004 [cit. 2010-05-13]. Komunikace. Dostupné z WWW: <http://bestpage.krasl.com/komunikace.html>.

[5] *Blogs.techrepublic.com.com* [online]. 2007 [cit. 2010-05-13]. Odposlech světlovodného kabelu. Dostupné z WWW: <http://blogs.techrepublic.com.com/security/?p=222&tag=nl.e036>.

[6] *Business.center.cz* [online]. 2006, 2009 [cit. 2010-05-13]. Trestní zákon § 180 Trestný čin obecně nebezpečný. Dostupné z WWW: <http://business.center.cz/business/pravo/zakony/trestni_zakon/cast2h4.aspx>.

[7] *Detekce.eu* [online]. 2005 [cit. 2010-05-13]. Barevná minikamera. Dostupné z WWW: <http://www.detekce.eu/index.php?main_page=product_info&cPath=65_66_78&products_id=281>.

[8] *E-trade.cz* [online]. 2007 [cit. 2010-05-13]. Špionážní a odposlechová technika. Dostupné z WWW: <http://www.e-trade.cz/inshop/spionazni-a-odposlouchavaci-technika/odposlechova-zarizeni-mistnosti/vysilace-stabilizovane/%5Bid-MUD-R%5D-vysilac-stabilizovany-429-mhz-3v-knoflik-100-hod-100-200-m.html>.

[9] *Ley.cz* [online]. 2005, 2009 [cit. 2010-05-13]. Zákon č. 169 Sb., o výkonu trestu odnětí svobody. Dostupné z WWW: <http://ley.cz/?s103&q103=all>.

[10] *Ley.cz* [online]. 2005, 2009 [cit. 2010-05-13]. Zákon č. 283/1991 Sb., o Policii České republiky. Dostupné z WWW: <http://ley.cz/?s103&q103=all>.

[11] *Medi-shop.cz* [online]. 2002 [cit. 2010-05-13]. Stetoskop Single. Dostupné z WWW: <http://www.medi-shop.cz/product/stetoskop-single-233/>.

[12] *Mudrochlabs.sk* [online]. 2006 [cit. 2010-05-13]. Odposlechová technika, zpravodajská technika. Dostupné z WWW: <http://www.mudrochlabs.sk/cz/odposlechy.htm>.

[13] *Odposlechmobilu.cz* [online]. 2008 [cit. 2010-05-13]. Funkce softwaru. Dostupné z WWW: <http://www.odposlechmobilu.cz/funkce>.

[14] *Odposlechmobilu.cz* [online]. 2008 [cit. 2010-05-13]. Podporované telefony. Dostupné z WWW: <http://www.odposlechmobilu.cz/podporovane-telefony>.

[15] *Odposlechmobilu.cz* [online]. 2008 [cit. 2010-05-13]. Využití softwaru. Dostupné z WWW: <http://www.odposlechmobilu.cz/>.

[16] *Odposlechy.com* [online]. 2007 [cit. 2010-05-13]. Odposlech klávesnice. Dostupné z WWW: <http://www.odposlechy.com/odposlech-klavesnice-keylog-time/>.

[17] *Odposlechy.com* [online]. 2007 [cit. 2010-05-13]. Odposlech počítače. Dostupné z WWW: <http://www.odposlechy.com/odposlech-pocitace/>.

[18] *Odposlechy.com* [online]. 2007 [cit. 2010-05-13]. Odposlechová technika, zpravodajská technika. Dostupné z WWW: <http://www.odposlechy.com/odposlechova-stenice-r250/>.

[19] *Odposlechy.com* [online]. 2007 [cit. 2010-05-13]. Odposlech telefoní linky. Dostupné z WWW: <http://www.odposlechy.com/odposlech-pevne-linky-to-line-1/>.

[20] *Odposlechy.com* [online]. 2007 [cit. 2010-05-13]. Odposlechová štěnice. Dostupné z WWW: <http://www.odposlechy.com/odposlechova-stenice-r200ac/>.

[21] *Odposlechy.com* [online]. 2007 [cit. 2010-05-13]. Odposlechová štěnice. Dostupné z WWW: <http://www.odposlechy.com/odposlechova-stenice-r500-ac2/>.

[22] *Odposlechy.com* [online]. 2007 [cit. 2010-05-13]. Odposlechová štěnice. Dostupné z WWW: <http://www.odposlechy.com/r3000/>.

[23] *Odposlech-tech.cz* [online]. 2007 [cit. 2010-04-13]. Odposlechová technika, zpravodajská technika. Dostupné z WWW: <http://www.odposlech-tech.cz/product/odposlech-fm-stenice-optimum-600-vyprodej-5/>.

[24] *Odposlech-tech.cz* [online]. 2007 [cit. 2010-05-13]. Odposlech přes zeď. Dostupné z WWW: <http://www.odposlech-tech.cz/product/odposlech-pres-zed-45/>.

[25] *Portal.gov.cz* [online]. 2003, 2010 [cit. 2010-05-13]. Zákon č. 13/1993 Sb., Celní zákon. Dostupné z WWW: <http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=13/1993&PC_8411_l=13/1993&PC_8411_ps=10#10821>.

[26] *Portal.gov.cz* [online]. 2003, 2010 [cit. 2010-05-13]. Zákon č. 154/1994 Sb., o Bezpečnostní informační službě. Dostupné z WWW: <http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411?PC_8411_number1=154/1994&PC_8411_p=10&PC_8411_l=154/1994&PC_8411_ps=10#10821>.

[27] *Pravnik.cz* [online]. 2005, 2009 [cit. 2010-05-13]. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). Dostupné z WWW: <http://www.pravnik.cz/uplna-zneni/uz-217.html>.

[28] *Probin.cz* [online]. 2000 [cit. 2010-05-13]. Právní rozbor. Dostupné z WWW: <http://www.probin.cz/cz/pravni-rozbor>.

[29] *Psp.cz : Listina* [online]. 2000 [cit. 2010-05-13]. Listina základních práv a svobod. Dostupné z WWW: <psp.cz/docs/laws/listina.html>.

[30] *Skaloud.net* [online]. 2005, 2009 [cit. 2010-05-13]. Trestní zákon § 178 Neoprávněné nakládání s osobními údaji. Dostupné z WWW: <http://www.skaloud.net/clanky/novela-trestniho-radu-zakaz-zverejnovani-odposlechu-omezeni-svobody-slova-nebo-zbytecne-obavy-13-2-2008/>.

[31] *Odposlechy.com* [online]. 2007 [cit. 2010-05-13]. Odposlech telefoní linky. Dostupné z WWW: <http://www.odposlechy.com/odposlech-pevne-linky-to-line-1/>.

[32] *Spy.vph.cz* [online]. 2006, listopad 2009 [cit. 2010-05-13]. Speciální technika a služby. Dostupné z WWW: <http://spy.vph.cz/mikrofony.html>.

[33] *Spy.vph.cz* [online]. 2006, listopad 2009 [cit. 2010-05-13]. Vysílače stabilizované. Dostupné z WWW: <http://spy.vph.cz/vysilace_stab.html>.

[34] *Wiseeye.co.il* [online]. 2003 [cit. 2010-05-13]. Laserový odposlech. Dostupné z WWW: <www.wiseeye.co.il>.

[35] *2.rohde-schwarz.com* [online]. 2009 [cit. 2010-05-13]. Spektrální analyzátory řady FLS. Dostupné z WWW: <http://www2.rohde-schwarz.com/>.

[36] *Poznámky z odborných konzultací*

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

OTP Obranně technická prohlídka.

PIR Passive infra red – pasivní infra červený.

GSM Global system for mobile communications – globální systém pro mobilní komunikaci.

PZTS Poplachový systém pro detekci vniknutí a přepadení.

EPS Elektrická požární signalizace.

DC Direct current – stejnosměrný elektrický proud.

AC Alternating current – střídavý elektrický proud.

DPH Daň z přidané hodnoty.

V Volt – jednotka elektrického napětí.

A Ampér – jednotka elektrického proudu.

Hz Hertz – jednotka frekvence.

m Metr – jednotka délky.

Kč Koruna česká.

kg Kilogram – jednotka hmotnosti.

W Watt – jednotka výkonu.

VOX Hlasové spouštění.

SMT Surface mount technology – výrobní technologie.

AIR Frekvenční pásmo.

EMC Elektromagnetická kompatibilita.

PC Personal komputer – osobní počítač.

RF Radiofrekvenční (pásmo).

NBÚ Národní bezpečnostní úřad.

ČR Česká republika.

BTS Base transceiver station – vysílač a přijímač radiových signálů.

UMTS Universal mobile telecommunication system – systém standardu mobilních telefonů.

CCD Charge-coupled device – zařízení s vázanými náboji.

ISDN Integrated services digital network – digitální síť integrovaných služeb.

DVD Digital video disc – digitální video disk.

Lux Lux – jednotka osvětlenosti.

PAL Phase alternating line – signál barevné informace.

CMOS Complementary metal oxide semiconductor – výrobní technologie.

TV Televizor.

Apod. A podobně.

Např. Například.

SMS Short message service – krátká textová zpráva.

GPS Global positioning systém – vojenský polohový družicový systém.

SIM Subscriber identity module – identifikační karta v mobilní síti.

PDF Portable document format – přenosný formát informací.

CD Compact disc – kompaktní disk.

FTP File transfer protocol – protokol aplikační vrstvy.

ICQ Program pro internetovou komunikaci.

QIP Program pro internetovou komunikaci.

B Byte – bajt, jednotka množství dat.

IT Information technology – informační technologie.

GPRS General packet radio service – mobilní datová služba přístupná pro uživatele GSM mobilních telefonů.

MMS Multimedia messaging service – multimediální zpráva.

KV Krátké vlny.

VKV Velmi krátké vlny.

UKV Ultra krátké vlny.

dB Decibel – jednotka obecného měřítka podílu dvou hodnot.

FM Frekvenční modulace

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: CENÍK OBRANNĚ TECHNICKÉ PROHLÍDKY PROVEDENOU FIRMOU MUDROCH LABS, S. R. O.

Základní prověrka – analýza rádiového spektra

Prohlídka prováděna analýzou rádiového spektra je efektivní alternativou pro osoby, kterým se zdá být dočasná kontrola uživatelem-laikem za pomoci nespolehlivých detektorů a „paměťových analyzátorů spektra“ neúčinná. Analýzou a triangulací RF spektra poskytuje firma špičkovou ochranu za pomoci špičkové techniky, kterou obsluhuje odborník v tomto oboru.

Cena analýzy rádiového spektra

Spektrální analýza	Cena v Kč bez DPH
Prověření spektra jedné místnosti do 100m²	12.350
Příplatek za každou další místnost	4.225

Cena za dopravu je účtována v částce za pohonné hmoty.

Kompletní prověrka prostoru

Tato prověrka je vhodná pro klienty, u kterých je pravděpodobné použití profesionálních, sofistikovaných odposlechových prostředků, nebo jiných než rádiových metod odposlechu. Ceny uvedené v tabulce jsou pouze orientační, konkrétní ceny jsou vždy určeny podle konkrétních podmínek.

Cena kompletní prověrky prostoru proti odposlechu

Podlahová plocha v m²	Cena v Kč bez DPH
do 30m²	21.450
do 50m²	33.400
do 75m²	41.850
do 100m²	51.800
nad 100m²	dle konkrétní situace

Cena za dopravu je účtována v částce za pohonné hmoty, na opakované prohlídky poskytují výrazné **slevy.**

PŘÍLOHA P II: CENÍK OBRANNĚ TECHNICKÉ PROHLÍDKY PROVEDENOU FIRMOU PROBIN, S. R. O.

Základní prohlídka proti zpravodajským technikám

Je zaměřena na odhalení nelegálních odposlechových prostředků, které se dají v praxi velmi jednoduše zakoupit, instalovat a používat. Účinnost této prohlídky je přibližně 70-80 %.

Tento typ prohlídky je vhodný zejména pro klienty, u nichž je riziko použití sofistikovaných odposlechových prostředků zanedbatelné nebo mu nepřikládají velkou pravděpodobnost. Průměrná rychlost prováděných prací je cca 10 m^2 za hodinu práce dvou vyškolených techniků.

Kompletní prohlídka proti zpravodajským technikám

Kompletní prohlídka je určena pro klienty, u nichž je pravděpodobnost použití vysoce sofistikovaných odposlechových technologií, nebo kteří chtějí získat maximální jistotu. Technici společnosti používají oproti Základní prohlídce navíc „detektor nelineárních přechodů“, který umí odhalit i odposlechové prostředky, které nejsou v daný okamžik aktivní. Postupy, používané při tomto typu prohlídky se překrývají, aby se minimalizovalo riziko neodhalení odposlechových prostředků pracující na pomezí mezi 2 měřícími metodami. Průměrná rychlost prováděných prací je cca 10m^2 za hodinu práce 2 vyškolených techniků. Účinnost kompletní prohlídky činí až 99 %.

Bezpečná kancelář

Bezpečná kancelář je speciální balíček sestavený za účelem realizace pravidelných preventivních prohlídek proti odposlechům. S bezpečnou kanceláří výrazně ušetříte. Balíček totiž obsahuje čtyři odposlechové prohlídky (jednu kompletní + tři základní) v zajímavém cenovém zvýhodnění.

Bezpečná kancelář obsahuje:

- 1 x kompletní prohlídka proti odposlechu
- 3 x základní odposlechová prohlídka

Tento model je vhodný zejména pro ty klienty, kteří ve svých prostorách vedou desítky různých jednání a u kterých není z praktického hlediska možné dodržovat režimová opatření vstupu a pohybu v jednacích místnostech. U tohoto modelu se provádějí 4 prohlídky v roce. Začíná se vždy prohlídkou „kompletní“ a poté následují 3 prohlídky „základní“ (tato standardní varianta se dá dle konkrétního požadavku samozřejmě upravit a také v okamžiku, kdy dojde v prostorách k nestandardnímu chování, aplikuje se vždy mimořádná prohlídka „kompletní“). Tento model maximalizuje účinek z prováděných prohlídek při minimalizaci finančních nákladů se službou spojených (obvyklá úspora činí až několik desítek procent). Ceny jsou uvedeny bez DPH.

Podlahová plocha [m²]	**První prohlídka**		**Bezpečný kancelář – čtvrtletní náklady**	
	základní	**kompletní**	**I.–III. čtvrtletí**	**IV. čtvrtletí**
10	6.000 Kč	10.000 Kč	6.000 Kč	0 Kč
15	9.000 Kč	15.000 Kč	9.000 Kč	0 Kč
20	12.000 Kč	20.000 Kč	12.000 Kč	0 Kč
25	14.100 Kč	23.500 Kč	14.100 Kč	0 Kč
30	16.200 Kč	27.000 Kč	16.200 Kč	0 Kč
35	18.300 Kč	30.500 Kč	18.300 Kč	0 Kč
40	20.400 Kč	34.000 Kč	20.400 Kč	0 Kč
45	22.500 Kč	37.500 Kč	22.500 Kč	0 Kč
50	24.600 Kč	41.000 Kč	24.600 Kč	0 Kč
60	28.800 Kč	48.000 Kč	28.800 Kč	0 Kč
70	32.640 Kč	54.400 Kč	32.640 Kč	0 Kč
80	36.096 Kč	60.800 Kč	36.096 Kč	0 Kč
90	39.240 Kč	65.400 Kč	39.240 Kč	0 Kč
100	42.000 Kč	70.000 Kč	42.000 Kč	0 Kč
150	48.120 Kč	81.200 Kč	48.120 Kč	0 Kč
200	55.200 Kč	92.000 Kč	55.200 Kč	0 Kč
250	61.440 Kč	102.400 Kč	61.440 Kč	0 Kč
300	67.200 Kč	110.000 Kč	67.200 Kč	0 Kč
nad 300	dohodou	dohodou	dohodou	dohodou

Cena za dopravu v případě prostoru nad 40 m² při jednorázové kompletní prohlídce proti odposlechu se neúčtuje, platí po celé ČR. V ostatních případech je účtováno 8 Kč za 1 kilometr bez DPH. Příplatky jsou účtovány za svátky, víkendy, výšku stropu nad 3 m, práci mimo dobu 8:00–20:00 h apod. ve výši určené dohodou.