POUŽITÍ SPECIÁLNÍCH BEZPEČNOSTNÍCH PROSTŘEDKŮ V PRAXI PODNIKŮ KOMERČNÍ BEZPEČNOSTI, PROSTŘEDKY SPECIÁLNÍ, ODPOSLECHOVÉ TECHNIKY A JEJICH ODHALOVÁNÍ A OBRANA PROTI NIM

USING SPECIAL SECURITY DEVICES IN PROFESSION COMMERCIAL SECUTITY COMPANIES, SPECIAL DEVICES, EAVESDROPPING TECHNICS AND THEIR

Marián Sehnálek

Bakalářská práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Marián SEHNÁLEK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Použití speciálních bezpečnostních prostředků v praxi podniků komerční bezpečnosti, prostředky speciální, odposlechové techniky a jejich odhalování a obrana proti nim**

Zásady pro vypracování:

Zpracovat jako právně bezpečnostní příručku pro PKB
1. Definice speciálních bezpečnostních prostředků
2. Prostředky speciální odposlechové a jiné dokumentační techniky
-seznámení s technologiemi získávání citlivých informací
-odposlechové štěnice, telefonní odposlech, mikrofonní sonda, minikamery pro skrytou montáž
3. Odhalování a obrana proti použití speciálních bezpečnostních prostředků (formy a metody)
-zařízení pro detekci, vyhledání a trvalou ochranu proti odposlechu
-fyzická prohlídka, rádiová prohlídka, kontrola nelinearit
4. Zákonnost použití speciálních bezpečnostních prostředků v praxi průmyslu komerční bezpečnosti

Rozsah práce:

Rozsah přiloh:

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

Seznam odborné literatury:

[1] Listina základních práv a svobod
[2]Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
[3]Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti
[4] Magazín Security
[5] Vnitropodniková literatura – Probin, Safecom
[6] Poznámky ze studia předmětu Speciální bezpečnostní technologie

Vedoucí bakalářské práce: **JUDr. Vladimír Laucký**

Datum zadání bakalářské práce: **13. února 2007**

Termín odevzdání bakalářské práce: **29. května 2007**

Ve Zlíně dne 13. února 2007

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Má bakalářská práce seznamuje s problematikou speciálních bezpečnostních prostředků, používaných k získávání informací a s prostředky sloužící k jejich odhalovaní a ochraně informací.

Klíčová slova: Odposlechové zařízení, obrana proti odposlechu, ochrana informací, konkurenční zpravodajství

ABSTRACT

My bachelor thesis get acquainted wiht questions of special security devices used for data acquisition and with devices for their detection and protection of data..

Keywords: Eavesdropping device, defence against tapping, protection of data, competitive intelligence

Úvodem bych chtěl poděkovat vedoucímu mé bakalářské práce panu JUDr. Vladimíru Lauckému za cenné rady a připomínky při tvorbě mé práce.

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

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně dne 24.května 2007 ……

Marián Sehnálek

OBSAH

ÚVOD

Velmi málo se mluví o jiném obtížně zjistitelném a těžko dokazovatelném, ale o to nebezpečnějším druhu kriminální činnosti. Jde se o krádeže informací. S postupným začleňováním České republiky do tržního prostředí, se vstupem do Evropské unie a s rozvojem soukromého podnikání, se objevují již i u nás první případy odposlechu důležitých porad, telefonních hovorů, faxových zpráv nebo datových přenosů. Mnoho firem si neuvědomuje nebezpečnost této činnosti a podceňují ochranu svých informací a know-how.

Cílem mé práce je vytvoření souhrnného celku obsahujícího různé způsoby narušení soukromí speciálními bezpečnostními prostředky, různé druhy odposlouchávacích technologií a prostředků na ochranu proti nim.

1 DEFINICE SPECIÁLNÍCH BEZPEČNOSTNÍCH PROSTŘEDKŮ

V soukromých bezpečnostních službách pod pojmem speciální bezpečnostní prostředky rozumíme zejména komerčně využitelná technická zařízení sloužící ke zjišťování informací ze zájmového prostředí zadavatele nebo techniku, která slouží z hlediska zákona k získávání informací v boji proti kriminalitě a nebo též techniku, která byla pro tento účel instalována protizákonně.

Používání odposlechových prostředků se rozvíjí mimo jiné proto, že jsou tyto prostředky jsou schopny zajistit „důkazy“ trestné činnosti. K tomuto účelu se používají zejména ve státní správě, kde se využívá skutečnosti, že se pachatelé cítí bezpečně a komunikují naprosto otevřeně. Ve státní správě se pak dále používají za účelem špionáže, kdy pomáhají zajišťovat důvěrné informace z různých zájmových oblastí jednak v domácí ekonomice ale také v zahraničí.

V komerční oblasti se odposlechová technika používá v těchto případech:

- zjišťování důkazů o vnitropodnikové kriminalitě, protože v mnoha případech je použití klasických bezpečnostních technologií neúčinné,
- v konkurenčním boji za účelem zajištění si konkurenční výhody
- jako preventivní prostředek pro zjištění chování obchodních zástupců, manažerů, …

V současnosti rozumíme odposlechovým prostředkem technické prostředky sloužící k „tichému“ získávání informací. Tyto informace mohou mít podobu jednak pouze mluveného slova (záznam rozhovoru několika osob) nebo obrazovou a zvukovou podobu (záznam obrazu a zvuku určité scény), ale také datovou podobu (emaily nebo jiná data uložená v počítačích). [3]

1.1 Jak mohou citlivé informace unikat?

Nejjednodušším a technickými prostředky nezjistitelným kanálem úniku informací je jejich vyzrazení některými ze zaměstnanců firmy. To se děje buď z neopatrnosti a neznalosti nebo za finanční odměnu od některé z konkurenčních firem. Dalším způsobem získávání důležitých informací je odposlech klíčových prostor firmy, jako jsou např.místnosti ředitele nebo jeho sekretářky, náměstků nebo jednací místnost. Pro tento způsob odposlechu slouží radiové mikrofony umístěné přímo v zájmové místnosti nebo v jejím sousedství. Tyto mikrofony

snímají hlasy ve svém okolí a vysílají je buď pomocí radiových vln nebo infrazáření na různé zdálenosti, nebo po jakémkoliv vedení (např. elektrická instalace, EZS, telefonní linka, elektrický vrátný apod.) mimo prostory odposlouchávané firmy. Tam se již rozhovor z vedení bez problémů snímá. Tyto radiové mikrofony jsou napájeny pomocí malé baterie, nebo je lze připojit k trvalému zdroji elektrické energie, jako je telefonní linka, zabezpečovací zařízení apod. Není žádným tajemstvím, že zmíněné štěnice jsou již dostupné i u nás a za dostupné ceny.

Poměrně jednoduchý způsob získání důležitých informací je odposlech telefonních linek.

Pomocí telefonní sítě křižují naši republiku velmi důležité informace ve formě mluveného slova, faxových zpráv nebo počítačových datových přenosů bez jakékoliv ochrany. Je až zarážející, jak bezstarostně se naši podnikatelé svěřují tomuto druhu přenosu informací. Zjištění odposlechu na telefonní lince v naší telefonní síti plné šumů a přeslechů je velmi obtížné. Existují však technické prostředky, kterými se lze tomuto úniku informací účinně bránit.

Zvláštní kapitolou odposlechu telefonních hovorů je odposlech mobilních telefonů NMT.

Radiotelefonní síť v České republice používá systém NMT 450, pracující na frekvencích 450-485 Mhz a systém GSM, pracující na frekvencích 900Mhz a 1800Mhz a nově také sítě „třetí generace“, například UMTS. Velice snadné je odposlouchávat síť NMT 450, která je provozována analogově bez jakékoli ochrany. Je to jeden z důvodů., proč se tato síť již téměř nepoužívá. Odposlech digitálního systému GSM je již poněkud komplikovanější, ale ne nemožný. [2]

1.2 Jak se úniku informací bránit?

Je nutné si uvědomit, že náš konkurent, zloděj informací, vložil do zařízení na získání našich důvěrných informací mnohdy nemalé prostředky a velkou dávku vynalézavosti. Proto bychom si měli uvědomit, že je málo pravděpodobné, že by odposlouchávací zařízení odhalili zaměstnanci firmy sami bez jakéhokoli technického vybavení a znalostí.

Některé profesionální společnosti nabízí svým klientům mimo jiné i zpracování komplexního projektu zajištění ochrany informací firmy. Jedná se o rozbor pohybu zaměstnanců a jejich styku s důvěrnými informacemi, rozbor pracovního režimu firmy, atd. Projekt vyústí v návrh

technicko - organizačních opatření a doporučení, jak únik informací eliminovat. Navržená organizační opatření zabraňují již zmíněnému vynášení informací vlastními zaměstnanci, mezi technická opatření zahrnujeme vybavení prostor firmy zařízením, které buď zjistí nainstalované odposlechové zařízení nebo znemožní jeho funkci.

Pro zjištění radiových mikrofonů se používají širokopásmové plynule přeladitelné přijímače ve spojení se spektrálními analyzátory nebo jednoduché ruční přijímače se signalizací silného vysílače. Ty jsou však pouze orientačním pomocníkem a nedokáží skrytý přijímač zachytit na větší vzdálenost. K zjišťování „štěnic" vysílajících po kabelovém vedení slouží různé typy telefonních analyzátorů a přístrojů na kontrolu kabelových vedení.

Zvláštní kapitolou jsou radiové mikrofony zapínané na dálku. Zjistit jejich přítomnost kontrolou radiového spektra je problematické, neboť jejich funkce může být v době provádění měření přerušena. V tomto případě lze použít detektor nelineárních přechodů, který odhalí všechny skryté polovodičové prvky, a to porovnáním odražených harmonických kmitočtů vlnění vysílaného anténou přístroje od tohoto skrytého polovodiče. Používání většiny uvedených přístrojů vyžaduje poměrně značnou zkušenost operátora a nemalé investice do technického vybavení. Z tohoto důvodu nabízejí specializované společnosti služby, spočívající v kontrole radiového spektra v zájmových prostorách, včetně kontroly kabelových vedení a vnitřních prostor automobilu. Po ukončení kontroly většinou dostane zákazník osvědčení o jejím výsledku, zda bylo nebo nebylo zjištěno aktivní odposlouchávací zařízení. Tyto kontroly se doporučuje provádět pravidelně, obzvlášť před důležitými poradami.

Poměrně jednoduchým prostředkem, jak eliminovat funkci skrytých mikrofonů, je umístit v zájmovém prostoru šumový generátor. Ten dokáže generovaným šumem zahltit aktivní mikrofony tak, že není možno zachytit mluvené slovo. Obtížněji odhalitelné je odposlouchávání telefonních linek. Z tohoto důvodu se jeví jako optimální přenášet důležité zprávy po telefonních linkách v šifrované podobě. K tomu slouží celá řada zařízení od nejjednodušších scramblerů až po složité šifrátory.

Scramblery pracují na principu rozdělení mluveného slova do určitých frekvenčních pásem a jejich vzájemného přeházení tak, že během přenosu po telefonních linkách je hovor nesrozumitelný. Ke složení hovoru do srozumitelné podoby dochází až u přijímací stanice, která je vybavena stejným scramblerem nastaveným na stejný číselný kód jako u stanice vy-

sílající. Složitějším, ale také bezpečnějším pro ochranu telefonního přenosu jsou šifrátory. Šifrovat lze přenosy mluveného slova, faxových zpráv, ale i počítačových dat. Šifrátory jsou vybaveny vnitřním generátorem náhodných čísel a šifrovací klíč se může během přenosu několikrát změnit. Šifrátory musí pracovat v páru, tj. na straně vysílací i přijímací.

Odposlech a získávání důležitých informací není žádným velkým problémem. Díky relativně nízké ceně odposlechových prostředků v porovnání s cenou zcizených informací, se odposlech i u nás stává velice účinným nástrojem konkurenčního boje. Proto by se každá firma měla začít vážně zabývat možností ochrany svých důvěrných informací, neboť investice vložené do této ochrany mohou být pouze zlomkem hodnot ztracených jejich únikem. [2]

1.3 Důvod použití speciálních bezpečnostních prostředků

1.3.1 Konkurenční zpravodajství

Je nezvratným faktem, že žijeme v prostředí neustále se prohlubující globalizace tržní ekonomiky, charakterizovaném neustále se prohlubujícími změnami s ostrými konkurenčními střety. S obchodem a podnikáním je konkurence spojena odedávna. Díky fenoménu globalizace se konkurence neustále vyostřuje. Objevují se stále nové hrozby, kterým je nutno čelit. Informace jsou velmi ceněným a drahým zbožím. Informace jsou stavebním materiálem managementu znalostí a jeho rozhodovacích procesů. „…Úspěšnou firmu odlišuje od šedi průměru, jak dobře využívá informace…“ (Bill Gates). Prostředkem k dosažení managementu znalostí je konkurenční zpravodajství. Konkurenční zpravodajství není pouze bezpečnostní – detektivní záležitost, ale představuje celý komplex. Jde o to:

- Legálním a etickým postupem shromažďovat informace

- Objektivní analýzu informací, která se nevyhýbá nepříjemným závěrům

- Zajistit řízený tok (distribuci) informací k těm kdo rozhodují (management znalostí).

Ochrana ekonomických zájmů však vyžaduje komplexní přístup, ale především je daleko širší než technická či fyzická ochrana objektů. Významným faktorem ovlivňujícím prosperitu , konkurence schopnost, exportní schopnost (efektivnost podnikání), každé firmy (společnosti, podniku, instituce, organizace apod.) je nesporně schopnost předvídat a řešit krizové situace, schopnost odolávat nejrůznějším ohrožením, rizikům a nástrahám a to jak vnějšího tak vnitřního charakteru.

1.3.1.1 Obranné konkurenční zpravodajství

Úkolem obranného konkurenčního zpravodajství je převážně:

- Zajišťování personální bezpečnosti,režimové bezpečnosti, bezpečnosti technických prostředků, bezpečnosti softwarových prostředků

- Zajišťování informační bezpečnosti

- Zajišťování bezpečnosti KNOW HOW, ochranu technologických procesů

- Zajišťování provozní bezpečnosti

- Zajišťování bezpečnosti v obchodních vztazích

- Aktivní ochranu proti dezinformacím a působení vlivového zpravodajství konkurence.

- Obrana proti ofenzivnímu konkurenčnímu zpravodajství konkurence; Prvotním úkolem, k tomu,aby podnikatelský subjekt mohl úspěšně fungovat, je ochránit sám sebe (ochránit vlastní podnikatelský subjekt jeho hmotný i nehmotný majetek, Know How apod.).

1.3.1.2 Ofenzivní konkurenční zpravodajství

Úkolem ofenzivního konkurenčního zpravodajství je převážně:

- Zajišťování informací potřebných pro podnikání – pro naplnění managementu znalostí;

- Zajišťování informací marketingového charakteru;

- Zjišťování informací o konkurenci;

- Zjišťování informací o technologiích;

- Zjišťování informací jimiž je možno odhalit strategii konkurence a využít ji ve prospěch vlastní organizace (podniku společnosti, firmy, instituce, organizace apod.).

1.3.2 Bezpečnostní složky státu

Bezpečnostní složky státu musí mít moderní monitorovací techniku, neboť v bezpečném a moderním státě je nepostradatelná pro účinnou a efektivní práci vojenské i civilní kontrašpionáže. Její nezbytnost potvrzují i zvyšující se aktivity teroristických organizací a

mafiánských skupin operujících na území našeho státu. Kdo o nezbytnosti této speciální techniky dlouho pochyboval nebo ještě stále pochybuje, ať si vzpomene, jaké důsledky měla nekvalitní práce amerických tajných služeb 11. září 2001.

2 PROSTŘEDKY SPECIÁLNÍ ODPOSLECHOVÉ A JINÉ DOKUMENTAČNÍ TECHNIKY

2.1 Dělení odposlechových prostředků

2.1.1 Podle umístění v zájmovém prostoru

a) s nutností průniku do prostoru

b) bez nutnosti průniku do prostoru

2.1.2 Podle typu přenášené informace

a) audio prostředky

b) video prostředky

c) kombinované prostředky audio/video

2.1.3 Podle typu přenosu informace ze zájmové oblasti k záznamu

a) drátově

b) bezdrátově

2.2 Drátové mikrofony

Nejedná se o běžné mikrofony, jak je známe z audio-vizuální techniky, ale o supercitlivé elektretové mikrofony, které umí bez problému monitorovat šepot v místnosti 6x6 metrů. Tyto mikrofony lze připojit k nahrávači a potom si již jenom chodit pro získané nahrávky.

Jsou vhodné spíše jako doplněk pro různá digitální i analogová záznamová zařízení nahrávající zvuk z daného prostoru, nebo jako doplněk pro umístění na tělo, do oděvu, do kufříku, pro vlastní monitoring rozhovoru, jednání a pod. Čím blíže je mikrofon u

hovořící osoby, tím je poslech kvalitnější. V úvahu je třeba vzít i akustiku místnosti, a k vyloučení brumu i umístění zdrojů síťového napětí.

Pro přenos informace se používají metalická vedení, které pracují na principu zesílení výsledného signálu a jeho modulace na vedení, přičemž na opačném konci mohou být přímo reproduktory nebo záznamová jednotka. V současné době mohou kvalitní drátové mikrofo-

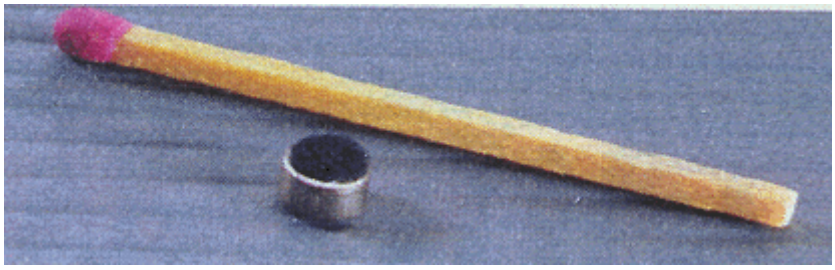
ny přenášet informace až do vzdálenosti 2 km. Dalším typem vedení jsou optické kabely. Princip jejich činnosti je stejný jako u drátového provedení, modulace na optický kabel však vyžaduje minimum elektronických součástek, čímž je velmi znesnadněno jejich vyhledávání a odhalování. Základní komponenty, použitelné pro kvalitní odposlech, tj. mikrofony, vedení, magnetofon a sluchátka se dají pořídit běžně na trhu za poměrně nízkou cenu. Pomocí soustavy vhodně umístěných mikrofonů můžeme monitorovat i několik důležitých míst najednou.

Při koupi mikrofonu je třeba brát ohled na způsob použití mikrofonu a podle toho volit i technické vlastnosti mikrofonu. Základní parametry, které je třeba brát v úvahu je konstrukce mikrofonu, přenášené frekvenční pásmo, směrovost, citlivost a impedance. [6]

2.2.1 Příklady mikrofonů

2.2.1.1 TECT

Příklad elektretového mikrofonu je mikrofon s označením TECT. Jeho průměr je 5mm a délka 4mm, vhodný pro odposlechy místností a s možností napojení na diktafon s napájeným mikrofonním vstupem.



Obr. 1 Elektretový mikrofon TECT

2.2.1.2 MAS

Mnoho firem nabízí již hotové odposlechové soupravy, které obsahují jak mikrofon, tak zesilovač i nahrávací zařízení. Souprava drátového mikrofonu a citlivého zesilovače s označením MAS je určena k poslechu místností pomocí drátového vedení. K zesilovači je připojeno ušní naslouchátko a lze též připojit magnetofon.

Obr. 2 Odposlechová souprava MAS

2.2.1.3 BW80

Souprava drátového mikrofonu a citlivého předzesilovače BW80 je určena k poslechu místností pomocí drátového vedení. K předzesilovači je připojen magnetofon.

Obr. 3 Souprava drátového mikrofonu a citlivého předzesilovače BW80

2.2.2 Odposlech po vedení

Do této skupiny můžeme zařadit odposlechová zařízení, která nejsou tak často používaná, cenově jsou dražší a jejich odhalení je náročnější. Především sem patří staré známé štěnice, které pro svou činnost využívají stávající metalická vedení – telefonní linky, elektrické vedení 230 V, vedení systémů EPS, EZS, elektrický vrátný apod. Na druhém konci je upravený přijímač, který odfiltruje frekvenci 50 Hz a nosnou frekvenci a nic nebrání tomu, abychom slyšeli, co se děje v místnosti vzdálené třeba 200 m. Toto zařízení nelze odhalit scannerem, neboť nosná frekvence je většinou dost nízká (řádově v KHz). Tyto systémy jsou omezeny buďto telefonní ústřednou nebo oddělovací transformátorem při síťovém provedení. Jako ochrana před touto štěnicí se dá použít filtr umístěný na síťový rozvod, který nepropustí vyšší frekvence. Při podezření, že jste odposloucháváni, a váš scanner nic neodhalil, je dobré nechat byt prověřit odborníkem v oboru. [24]

2.2.2.1 Příklad - MC - 06

Souprava obsahující šestikanálový dlouhovlnný přijímač a 6 vysílačů pracujících v pásmu 60-200kHz a využívajících jako přenosové cesty vedení 220V. Přijímač je určen pro příjem až šesti vysílačů MCX-06. Velikost 190x140x50 mm. Napájení ze sítě 220V.

Obr. 4 Odposlech po vedení – MC - 06

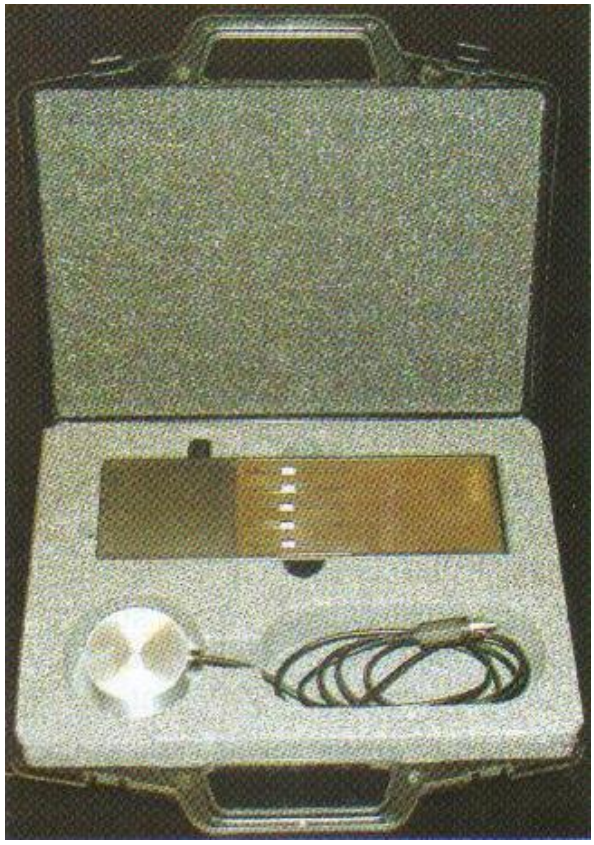
2.2.3 Speciální mikrofony

Mimo klasické, výše popsané druhy mikrofonů, které jsou běžně k dostání v obchodní síti, se k monitorování místností používá speciálně upravených či zkonstruovaných mikrofonů.

Nejznámější jsou kontaktní mikrofony. Princip činnosti je jednoduchý - akustický tlak, vznikající při hovoru v místnosti rozechvívá zdi, dveře a okenní tabulky a přiložený mikrofon (vlastně piezoelektrický krystal) je schopen toto chvění sejmout. Kvalitní kontaktní mikrofony snímají vibrace zdí i několik desítek centimetrů silných. Přenosové vlastnosti pevných materiálů jsou nevypočitatelné, je třeba zkusmo najít na zdi vhodné místo, kde je slyšitelnost a srozumitelnost hovoru největší. Snímací kvality kontaktního mikrofonu je možno vylepšit předvrtáním malé dírky do zdi na straně poslechu, k mikrofonu přilepit kousek šroubku nebo hřebíku a takto upravený kontaktní mikrofon těsně fixovat do otvoru ve zdi. Přilnavost mikrofonu na zeď je možno zvýšit použitím vhodného gelu. (např. gel, který se používá v lékařství při sonografii).

Dalším speciálním druhem mikrofonu jsou tzv. elektronické stetoskopy, mikrofony založené na principu přiloženého hrníčku na zeď. Nazývají se také dutinové mikrofony.

Jsou vyráběny a používány i mikrofony, které pro zvýšení kvality snímání obsahují oba systémy v jednom tělese. [1]



Obr. 5 Kontaktní mikrofon se zesilovačem

2.3 Bezdrátové mikrofony

Složitějším zařízením jsou tzv. radiové mikrofony umístěné přímo v zájmové místnosti nebo v jejím sousedství. Dnes už jsou tyto přístroje značně miniaturizované s vlastním vysílačem, které snímají hlasy ve svém okolí a přenáší do vzdálenosti několika kilometrů na přijímací a monitorovací pracoviště. Přenos zachycených zvuků je možný pomocí radiových vln, infračerveného záření tak, jak to známe z dálkových ovladačů spotřební elektroniky, nebo laserové odposlechové prostředky a prostředky, které pro svou činnost využívají světlo.Z hlediska vlastního přenosu je lze rozdělit do dvou základních kategorií, a to na prostředky analogové a digitální. Každá z těchto kategorií může ještě pracovat se signálem šifrovaným a nebo otevřeným. [6]

Prostředky pracující v infraspektru jsou omezeny krátkou vzdáleností a za nepříznivých podmínek dochází k jejich neúčinnosti. Výhoda spočívá v těžké odhalitelnosti, protože dnes je možné v každé kanceláři najít nějaké další (i když pouze občasně používané) vysílače v infraspektru (dálková ovládání HiFi věží, klimatizací, televizorů, videa, …).

Laserové odposlechové prostředky se vyznačují tím, že pro jejich činnost není nutný průnik do zájmového prostoru, přičemž vzdálenost mezi prostorem a místem pro vyhodnocení může být poměrně značná (stovky metrů). Základní nevýhoda pak spočívá v tom, že pro svou správnou činnost vyžadují naprostou kolmici k oknům zájmového prostoru.

Vysílací frekvence radiových mikrofonů může být stabilizována nebo nestabilizována. Stabilizované prostředky jsou výhodnější, neboť jejich vysílací frekvence má stálou a neměnnou hodnotu. U nestabilizovaných může mírně kolísat např. vlivem slábnutí zdroje. Pro bezobslužné nasazení je výhodnější použít prostředek stabilizovaný.

Podle způsobu použití se dělí na jednoúčelové a trvalé. Jednoúčelové štěnice jsou napájeny z baterie a jejich velkou výhodou je snadná instalace, kterou zvládne i technický antitalent. Pro rychlou instalaci a krátkou dobu provozu postačí napájení z vestavěné baterie. Právě baterie je základním prvkem určujícím dosah a rozměr odposlechového prostředku. Za požadavek minimálního rozměru se musí zaplatit malým dosahem a krátkou dobou provozu. Pokud je žádoucí, aby odposlechový prostředek pracoval po dobu alespoň jeden měsíc či déle a nelze u něho pravidelně měnit baterii, musí být zajištěn trvalý přívod elektrické energie. Pro maximální prodloužení doby provozu odposlechových prostředků s baterií a také pro snížení možnosti jejich odhalení, vybavují se dálkovým spínáním nebo aktivací hlasem (VOX). Takový prostředek vysílá pouze v době, kdy je dálkově zapnut, nebo když se v místnosti mluví.Taková jednoúčelová štěnice může být dokonce i v kalkulačkách, propiskách anebo kreditních kartách. [6]

2.3.1 Trvalé štěnice

Štěnice, aby pracovala, musí mít nějaký zdroj energie - a to poměrně silný. To je důležitý fakt. Nelze si představovat, že štěnice velikosti knoflíku bude vysílat signál na vzdálenost jednoho kilometru třeba měsíc. Proto, máme-li podezření na odposlech, je třeba zkontrolovat místa, kde by štěnice mohla mít trvalý zdroj energie (zásuvky, rozdvojky, prodlužovačky, lampičky, telefonní linky). To se provádí širokopásmovým scannerem, který dokáže najít zdroj elektromagnetického záření. Trvalé štěnice mají na rozdíl od krátkodobých jedno veliké kouzlo. Jsou napájeny ze zdroje, který je relativně nevyčerpatelný, takže taková štěnice pracuje, dokud se nepoláme nebo není odhalena když splnila účel a je z bezpečnostních důvodů odstraněna. Optimální je napojení na síť 220V nebo na jiný trvalý zdroj, jako je např. telefonní linka, zabezpečovací zařízení apod. Tato zařízení jsou schopná pracovat celé roky.

2.3.2 Místa umístění radiových mikrofonů

- V hodinách - podle typu hodin může být odposlech napájen buď z baterií, nebo z elektrické sítě. Jeho životnost je velmi vysoká.

- V kouřovém detektoru - do zařízení tohoto typu se obvykle instalují síťově napájené prostředky s radiovým přenosem informací.

- Přes klimatizační potrubí - do těchto míst se obvykle umísťují bateriově napájené prostředky s dobou životnosti až 75 dnů.

- Stetoskopický odposlech přes zeď - tento odposlech je možno provádět hlavně přes obvodové zdivo. Tento trvalý odposlech má pro pachatele minimální riziko.

- Vnesený radiový odposlech v květináči - nejjednodušší možnost o získání informací pomocí zpravodajské techniky, kterou zvládne i naprostý laik. Jedná se o odposlechy napájené bateriově s dobou provozu až 75 dnů.

- Odposlech telefonní linky - může být napájen jak z telefonní linky s neomezenou dobou životnosti, tak i bateriově, přenos informací může být jak po vedení, tak i radiovým spojením s dosahem opět okolo 50 m. Vyžaduje profesionální znalosti. Pokud není proveden přímo v telefonním aparátu popřípadě v zásuvce, pak je to takřka neodhalitelný odposlech.

- Radiový odposlech v odpadkovém koši - nejjednodušší možnost o získání informací pomocí zpravodajské techniky, kterou zvládne i naprostý laik. Jsou to radiově napájené odposlechy s dobou provozu až 75 dnů, přenos informace je radiovým spojením.

- Odposlech PC monitoru pomoci parazitního vyzařování - informace je možno získávat i zachycováním parazitního vyzařování počítače. Nejedná se o běžně dostupné prostředky, častější jsou krádeže celých počítačů.

- Radiový odposlech přilepený pod stůl - nejjednodušší možnost o získání informací pomocí zpravodajské techniky, kterou zvládne i naprostý laik. Jedná se o odposlechy napájené bateriově s dobou provozu 3-75 dnů, přenos informace je radiovým spojením.

- Síťově napájený odposlech v zásuvce - tento styl odposlechového prostředku je možno instalovat do elektrické zásuvky, rozdvojky nebo prodlužovací šňůry, jeho životnost je prakticky neomezená, obvykle pracuje na principu radiového vysílače s dosahem do 50 m. [9]

2.3.3 Příklady radiových mikrofonů

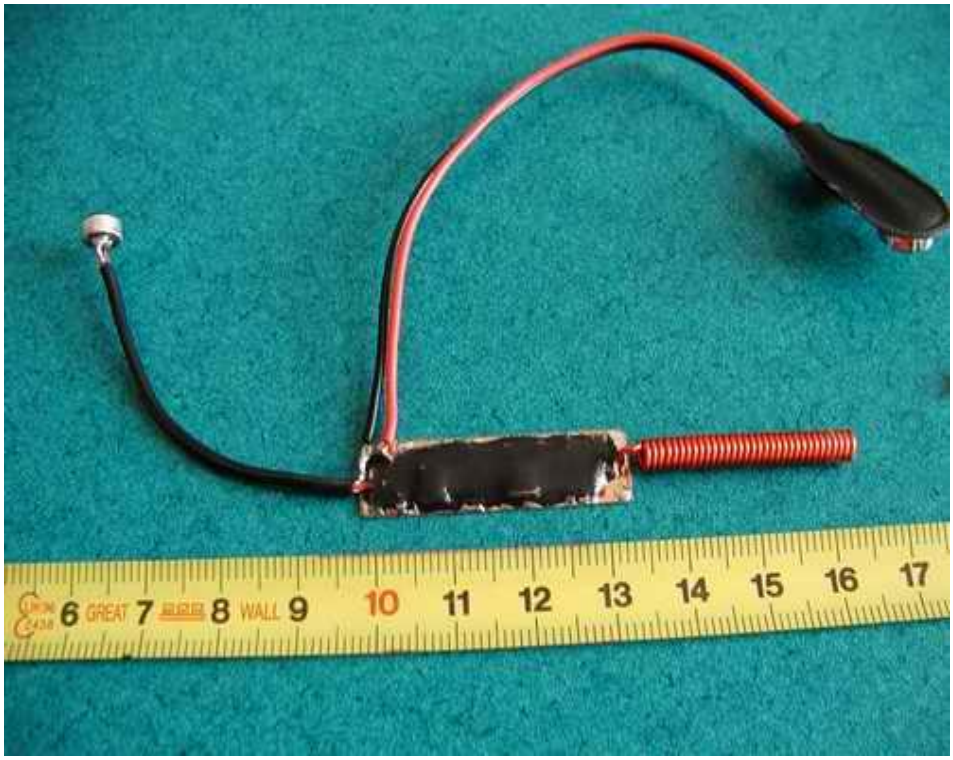
2.3.3.1 Vysílač - MUD-R

Rádiový vysílač s mikrofonem o výkonu 5mW. Napájení 3V knoflíkovou baterií 1000 mAh. Doba provozu až 100 hod. Frekvence v pásmu 430 MHz je stabilizována SAW rezonátorem. Rozměry: průměr 30 mm, tloušťka 16 mm. Dosah 100 až 150 m.

Obr. 6 Vysílač - MUD-R

2.3.3.2 Vysílač TX OEM mini

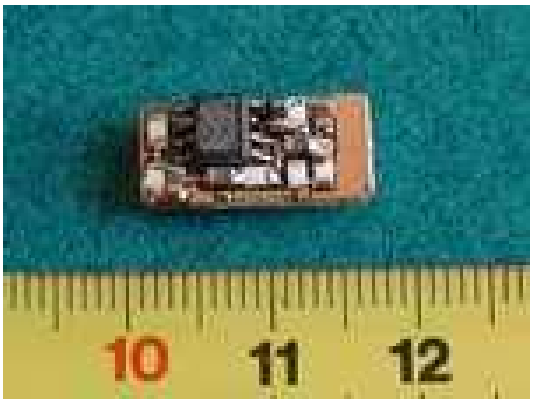
Rádiový vysílač s mikrofonem o výkonu 10 mW. Napájení 3 až 12V. Frekvence v pásmu 430 MHz je stabilizována SAW rezonátorem. Vysílač je určen k zabudování do vhodných predmětů. K vysílači je dodáván upravený přijímač ALINCO. Rozměry 36x11x3 mm bez anteny a zdroje. Přibližný dosah je 100 až 300 m v závislosti na napájecím napětí a okolním terénu..



Obr. 7 Vysílač TX OEM mini

2.3.3.3 Vysílač TX OEM mili

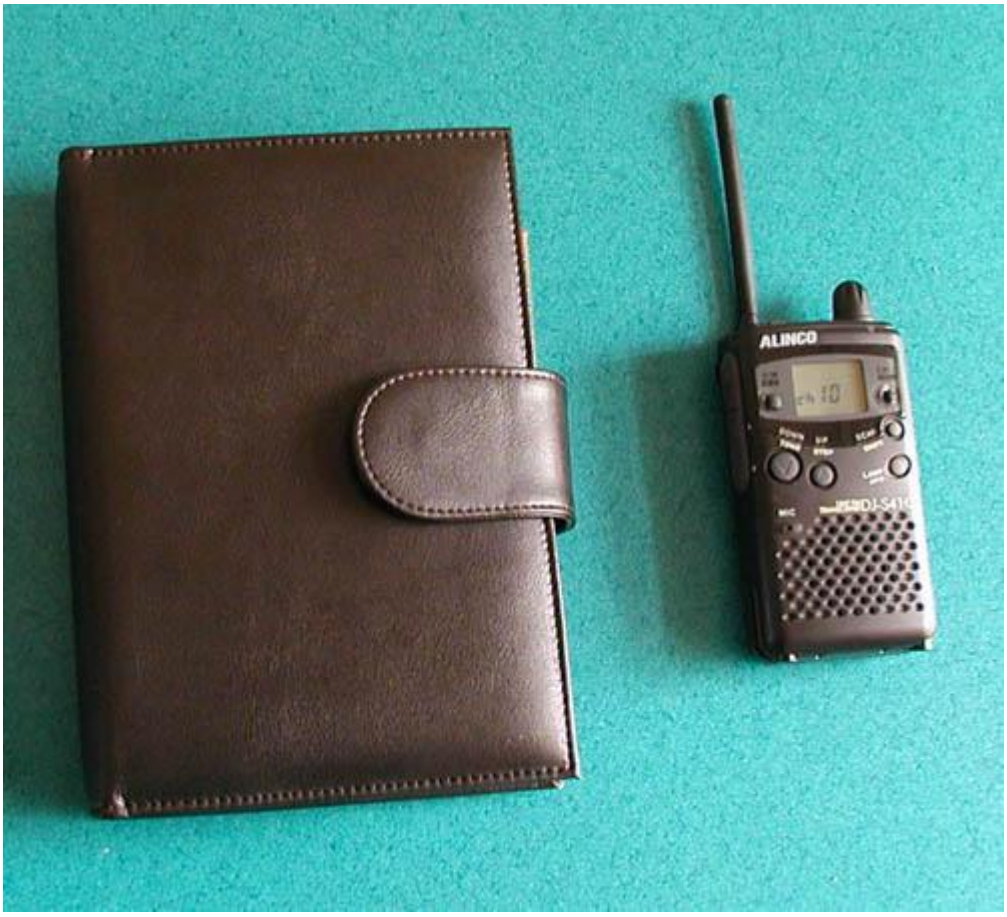
Rádiový vysílač s mikrofonem o výkonu 10mW. Napájení 3 až 12V. Frekvence v pásmu 430 MHz je stabilizována SAW rezonátorem. Vysílač je určen k zabudování do vhodných predmětů. K vysílači je dodáván upravený přijímač ALINCO. Rozměry 7x12x8 mm bez anteny a zdroje. Přibližný dosah je 100 až 300 m v závislosti na napájecím napětí a okolním terénu..



Obr. 8 Vysílač TX OEM mili

2.3.3.4 Maskovaný vysílač MUD-ORG

Rádiový vysílač s mikrofonem o výkonu 5mW zabudovaný v koženém diáři. Napájení 2 knoflíkovými bateriemi 3V. Doba provozu cca 5 hod. Frekvence v pásmu 430 MHz je stabilizována SAW rezonátorem. Vysílač je vybavenen automatickou regulací citlivosti mikrofonu (AVC). Vypínání a zapínání vysílače je vyndáním nebo zasunutím kuličkového pera do poutka diáře. K vysílači je dodáván upravený přijímač ALINCO. Rozměry: 170 x 120 mm. Dosah 100 až 300 m.



Obr. 9 Maskovaný vysílač MUD-ORG

2.3.3.5 Maskovaný vysílač TX Rozdvojka

Rádiový vysílač s mikrofonem o výkonu 10 mW v zabudovaný do rozdvojky na 230V. Vysílač je napájen z 230V v zásuvce. Frekvence v pásmu 430 MHz je stabilizována SAW rezonátorem. Přibližný dosah je 100 až 300 m v závislosti na okolním terénu.

Obr. 10 Maskovaný vysílač TX Rozdvojka

2.3.3.6 Maskovaný vysílač TX Kryt zásuvky

Rádiový vysílač s mikrofonem o výkonu 10 mW v zabudovany do krytu zásuvky na 230V. Po připevnění krytu na zásuvku je vysílač napájen z 230V v zásuvce. Frekvence v pásmu 430 MHz je stabilizována SAW rezonátorem. Přibližný dosah je 100 až 300 m v závislosti na okolním terénu.

Obr. 11 Maskovaný vysílač TX Kryt zásuvky

2.3.3.7 Maskovaný vysílač MUD-PERO

Rádiový vysílač zabudovaný do píšícího kuličkového pera. Frekvence v pásmu 430 MHz je stabilizována SAW rezonátorem. Přibližný dosah je 50 až 100 m v závislosti na okolním terénu. Napájení 6V baterie.

Obr. 12 Maskovaný vysílač MUD-PERO

2.3.3.8 Maskovaný vysílač UXC 1

Miniaturní, krystalem řízený vysílač v UHF pásmu zabudován do funkčního kapesního kalkulátoru, s dosahem min. 100 m, doba provozu dva týdny se dvěma monočlánky typu "AA".

Obr. 13 Maskovaný vysílač UXC 1

2.3.3.9 Vysílače s velkým dosahem S-AB, S-AH, S-AN

Krystalem řízený vysílač o rozměrech 59x30x13 mm pro monitorování místnosti. Hmotnost 20-25 g, dosah 1000 m, výkon 20 mW. Doba provozu 30 hod. Frekvence: S-AB 130-170 MHz, S-AH 380-410 MHz, S-AN 1,129-1,131 GHz.

Obr. 14 Vysílače s velkým dosahem S-AB, S-AH, S-AN

2.3.3.10 Vysílače s velkým dosahem S-AE, S-AK, S-AR

Krystalem řízený vysílač o rozměrech 50x30x25 mm pro monitorování místnosti, napájený ze síťového rozvodu 115-240V. Hmotnost 20-30 g, dosah 500 m, výkon 20 mW. Frekvence: S-AC 130-170 MHz, S-AJ 380-410 MHz, S-AU 1,129-1,131 GHz.

Obr. 15 Vysílače s velkým dosahem

S-AE, S-AK, S-AR

2.3.3.11 Vysílače s velkým dosahem S-AF, S-AL, S-AS

Krystalem řízený dálkově spínaný vysílač o rozměrech 65x45x17 mm pro monitorování místnosti. Hmotnost 50 g, dosah 500 m, výkon 20 mW. Doba provozu 40 hod, v pohotovostním režimu 800 hod. Frekvence: S-AF 130-170 MHz, S-AL 380-410 MHz, S-AS 1,129-1,131 GHz.

Obr. 16 Vysílače s velkým dosahem

S-AF, S-AL, S-AS

Z uvedených příkladů je vidět, že existuje mnoho kombinací vlastností daných vysílačů. Na základě zhodnocení našich potřeb vybereme ten nejlepší. Musíme uvážit, jak by měl být maximálně velký, jak daleký dosah potřebujeme, jak dlouho potřebujeme odposlouchávat či jak často můžeme chodit měnit baterie a podobně. Velmi užitečná je funkce VOX, která spíná zařízení při detekci hlasu a šetří nám tak baterie. Obdobně je na tom dálkově spínaný vysílač, kdy si sami určujeme, kdy budeme odposlouchávat.

2.3.4 Laserový mikrofon

Laser patří mezi mladší vynálezy 20. století. Přesto, že mu bude příští rok teprve 40 let, stal se nedílnou součástí našeho života. Laser si našel velmi rychle cestu i v oblasti vojenské techniky (navádění střel a bomb) a špionážní techniky (laserový mikrofon). Vedle štěnicových instalací existují také elegantnější cesty, jak odposlouchávat místnost. Laserové odposlechové zařízení se řadí do optoelektronických odposlechových zařízení. K odposlech na dálku je určen laserový vysílač, jehož laserový paprsek je zaměřen na okno odposlouchávané místnosti a okenním sklem odražený paprsek je zachycen laserovým přijímačem. Zvukové vlny vyvolané hovorem uvnitř místnosti rozechvějí okenní tabule ke slabé vibraci. Lase-

rový paprsek dopadající na tabuli skla je těmito vibracemi modulován a po zachycení v přijímači je opět demodulován do srozumitelné řeči. Normálně je tato technika nasazena jen High-Tech - odposlechovými experty.

Tento typ odposlechu má velmi problematické využití – z platnosti fyzikálních zákonů je obtížné najít optimálně kolmý přístup k okenním tabulkám a v zájmovém prostoru musí být použita čirá skla. Při splnění těchto podmínek je pak laserový odposlech velmi nebezpečný. Dosah zařízení je okolo 200 metrů. Nevýhodou jsou velmi vysoké pořizovací náklady.

Odposlechová laserová technika může být smontována také s heliovým - neonovým paprskem, nebo polovodičovým laserem a levným laserovým přijímačem. Systém může být pro náročné uživatele doplněn puškohledem pro monitorování a nahrávání pohybujících se objektů.

Komunikace pomocí modulovaných světelných paprsků není žádná nová myšlenka. Právě v 80. letech 19. století experimentoval Graham Bell s pokusným přístrojem s popisem ,,fotofonu". Tento přístroj se hodil k modulaci slunečního paprsku. K tomu má přístroj druh hubice s ozrcadlenou membránou. Při rozhovoru byl na membráně řízený sluneční paprsek vychýlen v rytmu řečové frekvence. Na místě příjmu reflektovaného paprsku může být udělán hlas pomocí solárního článku a citlivého sluchátka opět slyšitelným. Komerčnímu využití tohoto komunikačního způsobu bylo však zabráněno vzhledem k pohybu slunce a mračen.

Na základním principu Grahama Bella se i v moderní době nic nezměnilo. Úkol slunečního paprsku přebírá teď laserův paprsek s koherentním světlem.

Profesionální laserové odposlechové přístroje obsahují infračervené laserové zdroje. Infračervené světlo nemůže být vnímáno lidským okem. Aby se docílilo také na velké vzdálenosti ještě dobrých odposlechových výsledků, pracuje se s zářivým zdrojem o výkonu až 35mW. Kdo se náhodně podívá při tomto zářivém zdroji z odposlechového okna do paprsku, může si odnést těžké poškození zraku. Laserové světlo, ať viditelné nebo neviditelné, se značně odlišuje od normálního světla.

Světlo žárovky nebo zářivky obsahuje široké spektrum různých vlnových délek , přičemž vyzařování se koná spontánně a náhodně ve všech možných směrech. U laserového zdroje jde záření jen jedním směrem a obsahuje jen jedinou vlnovou délku.Toto dává paprsku ostré svazkování a typickou barvu. Když se setkají dva laserové paprsky stejné vlnové délky, mo-

hou buď zhasnout nebo zesílit. Tento vypínací nebo zesilovací efekt může být vyhodnocen při pohybu reflektujícího povrchu prostřednictvím interferometru.

Na polopropustném zrcadle (tzv. Beam- Splitter), je přeladěna část nastupujícího paprsku. V přijímači může být paprsek srovnán ze zdroje cílovým reflektorem přicházejícího paprsku fázově, popř. výchylkově. Hlavní problémy u tohoto interferenčního odposlechového postupu záleží na skutečnosti, že přes paprskovou štěpinu může být řízena na cíl jen část laserové energie. Toto vede k omezení dosahu. Dále reaguje interferometr nejen na okenní vibrace, ale i na vibrace zdroje laserového záření a samotného interferometru. Proto se u profesionálních přístrojů dává přednost přímé reflexi podle Graham Bellova fotofonního principu.

Nezávisle na funkčním principu je nutný v každém případě zdroj laserova paprsku. Kvůli jednoduchosti se používá v této aplikaci heliovo-neonový laser typu ETS 4200 firmy Heathkit (při našem vývoji požíváme jiný). Podobné lasery mohou být cenově výhodně obstarány u firmy ELV. Výchozí výkon obsahuje asi 0,9 mW. Ve vzdálenosti 70 m promítá laser světelnou skvrnu 35 mm průměru na cílový objekt.

Také při nepatrném paprskovém výkonu 0,9 mW by se neměl paprsek dostat do oka. Toto platí také pro provozování reflektujícího paprsku prostřednictvím zaměřovače, nebo dalekohledu. Jen když paprsek nastoupí na reflektující plochu, např.bílý list papíru, může být provozován bez nebezpečí.

Obr. 17 Laserový mikrofon

Obr. 18 Příklad použití laserového odposlechu

2.4 Telefonní odposlech

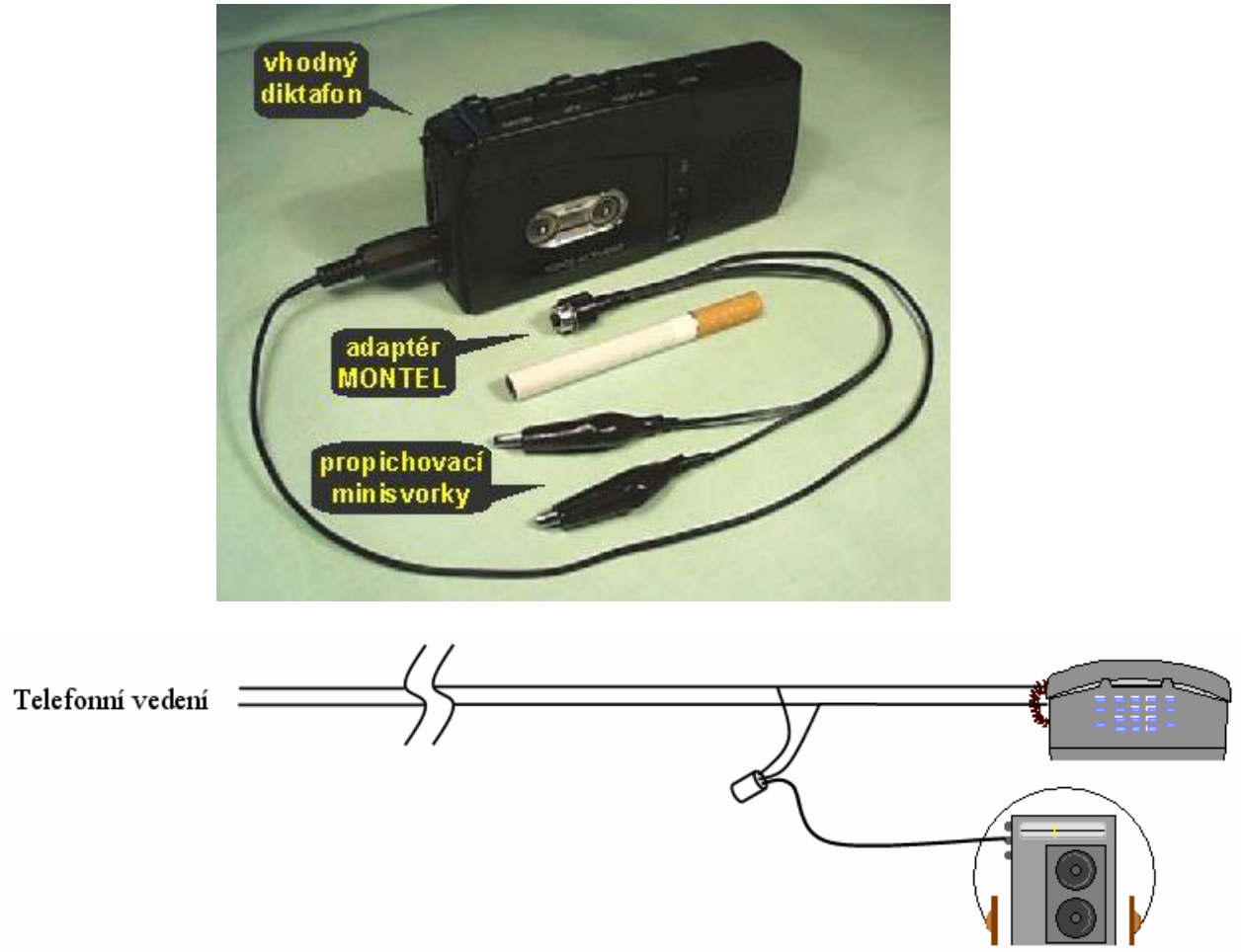
Telefonní přístroj je častým místem úkrytu odposlechových zařízení. Telefon je v téměř každé kanceláři a je zpravidla spojen s okolním světem čtyřžilovým drátovým vedením. Pro odposlech je výhodné i umístění telefonního přístroje blízko místa, kde se nejčastěji vedou rozhovory (stůl v kanceláři). Zkrátka použití telefonu k odposlechu je ideálním řešením. Telefonní přístroj je použitelný k odposlechu dvěma způsoby. Můžeme přímo odposlouchávat telefonní hovor nebo využít telefonního přístroje k monitorování místnosti. Používané telefonní přístroje prošly několika vývojovými etapami a tomu odpovídají i typy telefonních přístrojů. Postupnou modernizací byl nahrazen klasický zvonek tónovým a otočná číselnice byla nahrazena tlačítkovou. Princip přístroje byl ale zachován. Modernější telefony mají navíc elektronické obvody ke zlepšení komfortu obsluhy. Způsob odposlechu telefonního hovoru a možnosti napojení však zůstávají stejné. [2]

2.4.1 Drátový odposlech telefonní linky

Základní způsob odposlechu telefonního hovoru je přímé napojení citlivého zesilovače nebo magnetofonu na přívodní linku. Technicky není podstatné v kterém místě trasy telefonní linky se na vedení napojíte. Záleží pouze na možnostech přístupu k jednotlivým uzlům kabelové trasy. Pokud se rozhodnete pro přímé napojení na telefonní linku, je dobré, když připojený magnetofon je vybaven automatickým spouštěním záznamu při zvednutí sluchátka telefonního přístroje. Nejjednodušší je použití magnetofonu vybaveného systémem VOX (aktivace hlasem).[2]

2.4.1.1 MONTEL COMBI – telefonní záznamová souprava

Souprava se skládá z diktafonu a nahrávacího adaptéru Montel. Lze ji snadno napojit speciálními svorkami i přes izolaci vedení kdekoliv na trase telefonní linky bez nutnosti rozpojení vedení. Automaticky je nahráván každý odchozí hovor včetně vytáčeného čísla a každý příchozí hovor.



Obr. 19 MONTEL COMBI – telefonní záznamová souprava

2.4.2 Radiové systémy odposlechu telefonní linky

Ne vždy máme možnost se napojit na telefonní vedení mimo odposlechový prostor. Zbývá možnost napojení telefonní linky přímo v účastnické zásuvce nebo v telefonním přístroji a drátovým vedením propojit skrytý magnetofon. Pravidelná kontrola nahrávky a tím i četnost pohybu poblíž nebo přímo v odposlechovém prostoru není vhodná a proto se volí způsob, který přenáší telefonní hovor vzduchem po radiových vlnách. Používají se miniaturní radiovysílače, místo mikrofonu je zde adaptér pro napojení na telefonní linku. Napájení radiovysílače můžeme volit z baterie, nebo použít k napájení 60 V telefonní sítě. Klasická telefonní štěnice je krabička rozměru 2x2x1 cm se dvěma drátky na připojení. Telefonní vedení nahrazuje zdroj signálu - mikrofon, napájecí zdroj i anténu. Kvalitnější telefonní radiovysílače jsou dvoukanálové, jeden kanál snímá a vysílá telefonní hovor a druhý snímá zvuky z místnosti. [2]

Obr. 20 Druhy telefonních radiovysílačů

2.5 Odposlech mobilního telefonu

V poslední době se o možnosti odposlechu mobilních telefonů hovoří stále častěji. Jaká je skutečně reálná možnost odposlechu mobilního telefonu a jakými způsoby lze vlastně mobilní telefony odposlouchávat?

2.5.1 Odposlech za asistence operátora

Legální odposlechy realizuje Policie ČR v součinnosti s telekomunikačními operátory a pro jejich realizaci nepotřebuje vynaložit příliš velké úsilí, neboť operátoři jsou povinni poskytnout za tímto účelem policii přístup ke své síti. Problém nastává v případě těch, kteří se rozhodnou porušovat naše zákony a provádět odposlech mobilního telefonu v nesouladu s § 88 Trestního řádu, neboli odposlech nelegální. Možnost uplacení zaměstnance u mobilního operátora, který by prováděl na nelegální odposlechy stejným technickým postupem jako policie, je v podstatě vyloučena. Všichni zaměstnanci našich mobilních operátorů, kteří mají co do činění s aktivací odposlechů pro Policii ČR, mají za sebou bezpečnostní prověrky NBÚ. Všechna místa v mobilní síti, kde by šlo hovory odposlouchávat, jsou navíc pod neustálým přísným dohledem a je téměř na 100 % jisté, že pokud by se nějaký zaměstnanec pokusil o nelegální odposlech, byl by velmi rychle odhalen. [25]

2.5.2 Šifra pro GSM prolomena, máme se bát?

V médiích se nedávno objevily obrovské titulky, které říkaly, že šifra A5.1, kterou používají mobilní sítě pro šifrování hovorů byla prolomena a že dešifrovací program je volně přístupný na internetu. Lidé z toho pak logicky odvozovali, že pokud někdo má dešifrovací pro-

gram na A5.1, tak může kdykoliv kohokoliv odposlouchávat. Skutečnost je však odlišná. Je pravda, že existuje program na dešifrování A5.1, který je dokonce volně přístupný na Internetu. Pokud by tedy měl zájemce o odposlech vyhovující hardware, pak by skutečně byl schopen v relativně krátkém čase nějaký ten hovor dešifrovat. Problém je však v tom, jak onen hovor nalézt. [24]

2.5.3 Co vysílá telefon

Komunikace mobilního telefonu (MS) se základ-novou stanicí (BTS) v síti GSM probíhá na dvou frekvencích (přesněji kanálech): jedné pro příjem a druhé pro vysílání hovoru. Každá z těchto frekvencí je však rozdělena v čase na časové úseky o délce 0,577 ms (TDMA frame). Každý TDMA frame se skládá z 8 timeslotů, neboli časových rámců, kdy telefon vysílá. Tyto rámce jsou očíslovány od 0 do 7. Jeden timeslot je dlouhý cca 0,072 ms. Každý volající telefon má přidělen právě jeden timeslot. Mobilní telefony se ve vysílání na dané frekvenci pravidelně střídají v pořadí podle čísla timeslotu, který jim byl přidělen. Díky této technologii nazývané TDMA je možné, aby jednu frekvenci využívalo několik telefonů najednou.Ve skutečnosti tedy, i když si myslíte, že slyšíte hovor naprosto plynule a spojitě, tak z něj slyšíte vždy jen jeho osminu - díky nedokonalosti lidské-ho sluchu to nevadí. Z hlediska odposlouchávání hovoru to ovšem znamená, že se musí monitorovat dvě frekvence, na kterých se může nacházet klidně i osm hovorů; ty je nutné dešifrovat samostatně a následně je sestavit dohromady.To vše by bylo poměrně jednoduché, kdyby neexistovala technologie frekvenčních skoků (frequency hopping), která, zjednodušeně řečeno, slouží ke zlepšení kvality hovoru (respektive omezení možného rušení určitých frekvencí). Díky této technologii, kterou používají všichni naši operátoři, vysílá mobilní telefon pokaždé na jiné frekvenci, která se mění každých 0,577 ms podle jednoho ze 64 možných, pevně stanovených schémat.Ve skutečnosti by tedy kvůli odposlechu jednoho mobilního telefonu z komunikace mezi MS a BTS bylo nutné odposlouchávat všechny frekvence BTS najednou, odhalit číslo tzv. hoppovacího schématu každého z probíhajících hovorů, dešifrovat veškerý zachycený provoz, poskládat jednotlivé hovory k sobě, a následně najít ten správný hovor. To vše navíc za předpokladu, že jsme někde poblíž odposlouchávané osoby a v případě jejího pohybu takto odposloucháváme hned několik BTS v okolí najednou. Takovýto odposlech by byl velmi časově a finančně náročný, ale navíc by vyžadoval neustálé sledování odposlouchávané osoby.Odposlech na tomto principu by byl však mnohem snazší v případě, že bychom vlastnili identickou kopii odposlouchávané SIM karty. Pak by jen stačilo se pohybovat v okolí odpo-

slouchávané osoby a s patřičným vybavením "poslouchat" komunikaci mezi MS a BTS. Na rozdíl od předchozího případu bychom totiž měli k dispozici dešifrovací klíč přímo a věděli bychom také přesně, na jakých frekvencích máme hovor hledat. [25]

2.5.4 Jak poslouchat v síti

Mnohem snazší a reálnější je odposlech v další části mobilní sítě, tedy mezi BTS a řadičem základnových stanic (BSC - spravuje vždy několik BTS najednou) či mezi BSC a "mobilní telefonní ústřednou" (MSC - je k ní připojeno několik BSC a případně i další MSC). Mezi těmito prvky sítě totiž probíhá komunikace prostřednictvím bezdrátových či optických spojů, a to naprosto nešifrovaně. V okamžiku, kdy zjistíme, kudy daný spoj prochází, není v případě bezdrátového spoje příliš těžké se do něj napojit. Problém je v tom, že v takovém spoji probíhají desítky (u BTS - BSC) až stovky (u BSC - MSC) hovorů najednou navíc obohacených o řadu dalších informací, které si tyto prvky mobilní sítě mezi sebou vyměňují. Je tedy velmi náročné v takovéto změti dat identifikovat právě hovor, který hledáte. Výhoda je však v tom, že již není třeba přímo v okolí odposlouchávané osoby. Při odposlechu komunikace mezi BSC a MSC by stačilo být ve stejném okrese jako odposlouchávaná osoba (s tím, že bychom pak daný hovor museli umět "najít"). Menší problém je ovšem v tom, že pokud by odposlouchávaná osoba volala někomu ze stejné mobilní sítě, kdo by byl ve stejném okrese, pak by hovor přes spoj BSC - MSC vůbec neprocházel, neboť by jej spojilo přímo BSC samo.

A co že z toho všeho vyplývá? Nelegální odposlech mobilních telefonů je technicky a finančně velmi náročná věc (pokud není "štěnice" přímo v telefonu). I když lze mobilní telefony odposlouchávat, tak v žádném případě není reálná představa, že lze odkudkoliv odposlouchávat kohokoliv. Téměř vždy se musí odposlouchávající nacházet ve větší či menší blízkosti odposlouchávaného.[25]

2.5.5 GSM Interceptor

Jednokanálová souprava pro odposlech jednoho mobilního telefonu GSM. Pracuje s jakýmkoli typem kódování, vč. A5.1 a A5.2. Nepotřebuje žádnou podporu ze strany operátora sítě. Zařízení je mobilní a je zabudované do kufříku. Telefon je identifikován podle IMSI, TMSI, IMEI, Classmark, MSISDN. Při první relaci si uloží všechny údaje o monitorovaném telefonu a pokud se některý z těchto identifikačních prvků objeví v relaci, začne monitoro-

vat. Proto systému nevadí ani změna SIM karty. Hovor je nahráván na HDD řídicího laptopu. Vytváří seznam volaných čísel a volajících (pokud jsou přístupná). [6]

2.6 Optické systémy

Je spousta jednoduchých i složitějších metod optického pronikání do osobních práv občanů. Nejjednodušší je pozorování vaší kanceláře dalekohledem. Je možno pozorovat vstup do budovy, okna kanceláře a pohyb v místnosti. Je možno zjistit vaše obchodní partnery, styky a chování zaměstnanců. Jednoduchá a levná metoda, málo účinná a efektivní. Pokud vaše kancelář sousedí s prostory jiného nájemníka, je možno předpokládat přímé pozorování místnosti skrz zeď. Lidské oko nedokonalý orgán, bylo nahrazeno fotoaparátem a později, při rozmachu video techniky téměř jednoznačně video kamerou. Ještě před několika lety byl tento způsob téměř jediný pozorovací systém. Velké snímací videokamery ani jiné použití neumožňovaly. Provrtávaly se stropy a pokud to nebylo možné, tak zdi. Metoda umožňovala kvalitní video i audio signál, byla to však metoda docela těžkopádná a komplikovaná. Změna nastala až s objevem čipu CCD. [2]

2.6.1 Mini kamery s čipem CCD

Současně používané malé kamery, od průmyslových po policejní a špionážní jsou osazeny

výhradně CCD čipy a tím i odpovídajícími vlastnostmi. Kamery jsou malé, s dobrou rozlišovací schopností, pevným objektivem, velkou citlivostí a zpravidla s automatickou clonou. Kvalitnější typy jsou vybaveny možností výměny objektivu. Kamery jsou velikosti krabičky zápalek nebo dokonce kostky cukru a mohou se zabudovat do různých předmětů, jejich použití není vázáno na otvory ve zdi. Na objektiv běžně používaných kamer stačí velikost otvoru asi 5 mm, u dírkových objektivů asi 1 mm. Kamery je možno zabudovat do nábytku, televizoru, radiopřijímače, obrazů, různých plastik a ozdobných předmětů, hodin, knih a hraček. Vhodným místem pro skrytou kameru jsou osvětlovací tělesa, požární a zabezpečovací čidla, krabice telefonních rozvodů a rozvodů 220V. Kamery se mohou ukrýt do umělých květin, telefonů, faxů a počítačů. Pro ukrytí kamery je limitujícím faktorem velikost přístroje a velikost otvoru objektivu. Zmenšení objektivu se provádí použitím jehlových objektivů, optickou soustavou, která zmenšuje vstupní otvor objektivu na velikost asi čtyř milimetrů. Jehlový objektiv má pevnou délku, od 10cm do 50cm, světelnost objektivu je asi 1,8 úhel záběru je od 40 do 80 stupňů. Jehlové objektivy mohou být zabudovány přímo v

tělese kamery,(což je výhodnější) nebo mohou být jako vnější přídavné zařízení. Nevýhodou je však poněkud větší energetická náročnost než je u vysílačů pouze na zvuk. Proto lze očekávat, že videoštěnice bude nainstalována v nějakém elektrickém spotřebiči trvale připojeném v síti.

Další možností prodloužení objektivu je použití světlovodného kabelu. Kabely mohou být pevné, nebo pružné, dají se prostrčit jakýmkoliv otvorem ve zdi, jsou ohebné bez ztráty kvality, mají nižší světelnost (asi 4). I u světlovodných kabelů platí, že pro speciální aplikace je možno do jedné trubice zabudovat optický i akustický systém. [2]

2.6.2 Přenos videosignálu

Signál je normovaný, uvedené způsoby platí pro jakoukoliv kameru. První způsob přenosu je kabelem. Můžeme použít koaxiální kabel. Je stíněný, signál je možno vést na velkou vzdálenost s relativně malými ztrátami. Kabel však vyžaduje slušné zacházení, je příliš silný a nesmí se příliš ohýbat. Tenký stíněný kabel má zase větší ztráty. Tím je možno vést videosignál na malou vzdálenost, asi do 50m. Další možností je optický kabel. Je tenký, neplatí na něho žádné rušení a je možno jej vést i rozvody síťového napětí. Jak napovídá název, vede jenom světlo. Na začátku i na konci kabelu musí být převodníky, optické konvertory. Firmy se zabezpečovací technikou používají pro automatizovaný přenos videosignálu bezpečnostních kamer převodník na telefonní linku. Podobné zařízení je možno přímo namontovat do video kamery a přenos signálu je možný po telefonní lince nebo jakémkoliv dvouvodičovém krouceném vedení. S troškou fantazie lze v takovém případě využít optický odposlech ve spojení s nekonečným vysílačem na telefonní lince, nebo vysílačem nosného proudu po síťovém vedení.

V poslední době se objevili též přenosy videosignálu po síti mobilních telefonů GSM s využitím datových přenosů GPRS a nově také v síti UMTS, která umožňuje kvalitní a rychlý přenos.

Je možno použít i video vysílač. Používají se legální vysílače původně určeny pro přenos signálu bezpečnostních videokamer. Speciální aplikace využívají speciální kamery i speciální videovysílače. [2]

2.6.3 Zpracování videosignálu

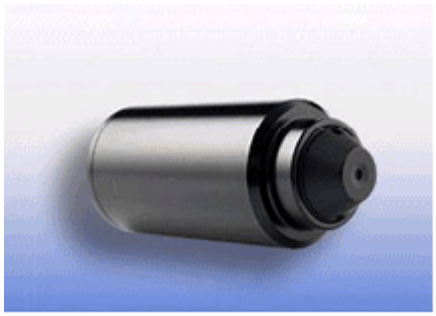
Můžeme použít běžný videorekordér, jsme-li na bezpečném místě a můžeme často vyměňovat kazetu, nebo použijeme pomalu běžné video dodávané k bezpečnostním systémům. Na jednu kazetu je možno nahrát zpravidla 720 hodin záznamu. Další možnost spouštění video systému je přímým pozorováním prostoru a zmáčknutím nahrávacího tlačítka. Je možno video aktivovat časově, pohybovým nebo PIR detektorem, dveřním kontaktem a pod. [2]

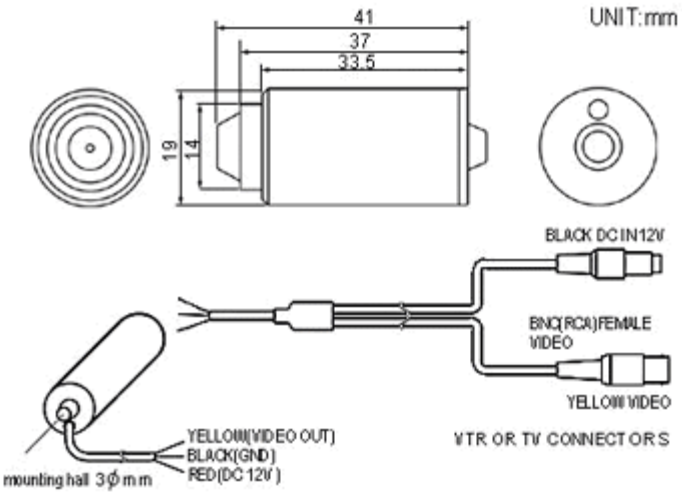
2.6.4 Příklady CCD kamer a jejich příslušenství

2.6.4.1 MK-S190SP1

MK-S190SP1 je miniaturní černobílá CCD kamera s pinole objektivem. Díky malým rozměrům je možné využít ke skryté montáži. Podle požadavku snímání prostoru lze zvolit ohniskovou vzdálenost objektivu. Kamera má odolný kovový plášť.

Formát signálu: 50Hz; ohnisková vzdálenost f: 3,7mm; rozlišení: 500(H)x582(V); horizontální rozlišení: 420 TV řádků; citlivost: 0,05Lux; napájení: 12V; rozsah pracovních teplot: -10°C až 50°C; rozměry: 41x19mm



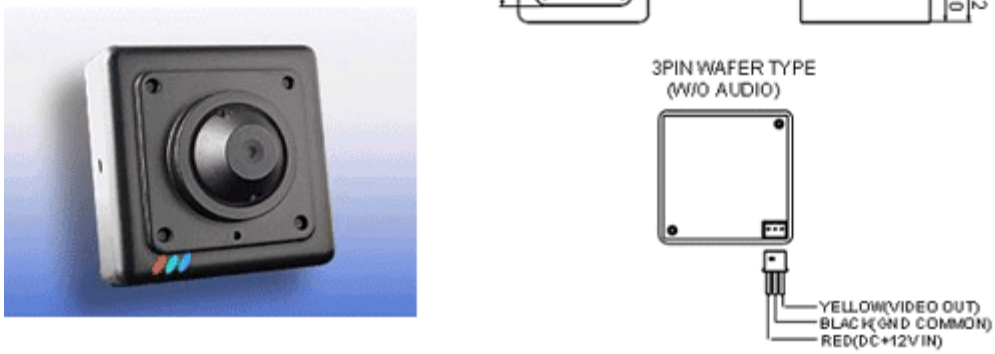


Obr. 21 CCD kamera MK-S190SP1

2.6.4.2 MK-S700CP1

MK-S700CP1 je miniaturní barevná CCD kamera s pinhole objektivem. Díky malým rozměrům je možné využít kameru ke skryté montáži. Podle požadavku snímání prostoru lze zvolit ohniskovou vzdálenost objektivu. Kamera má dobré světelné vlastnosti a odolný kovový plášť.

Formát signálu: PAL; ohnisková vzdálenost f: 3,7/4,3mm; rozlišení: 500(H)x582(V); horizontální rozlišení: 380 TV řádků; citlivost: 0,1Lux; napájení: 12V; rozsah pracovních teplot: -10°C až 50°C; rozměry: 30x30mm



Obr. 22 CCD kamera MK-S700CP1

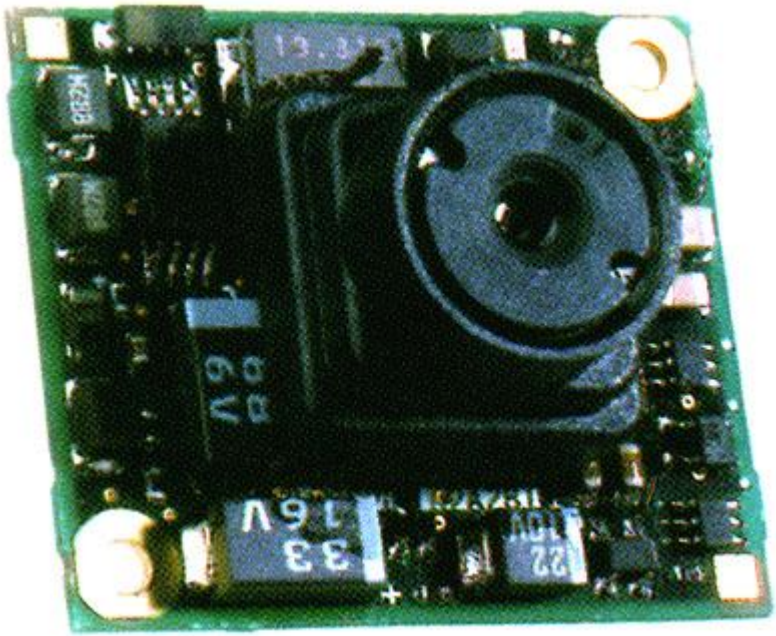
2.6.4.3 VCM 36

Desková kamera s CCD čipem 1/3", ČB provedení s objektivem f=3,8 mm, 0,2 Lux. Plná automatika, elektronická závěrka, 380 TV řádek, napájení 10 - 12,6 V DC. Vestavěný mikrofon pro snímání zvuku. Rozměry 32x32x30 mm.

Obr. 23 CCD kamera VCM 36

2.6.4.4 161/45E

Desková kamera s CCD čipem 1/4", barevné provedení PAL s dírkovým objektivem f=4,5 mm. Plná automatika, elektronická závěrka 1/60 až 1/96000 sec., 330 TV řádek, napájení 4,8 - 5,5 V DC, 10 LUX. Rozměr 26x22x13,5 mm (s objektivem).



Obr. 24 CCD kamera 161/45E

2.6.5 Příklady systémů pro bezdrátové audio-video přenosy

2.6.5.1 PROIV-T standardní vysílač ProfiLink

Obr. 25 PROIV-T standardní vysílač ProfiLink

Vysílač ProfiLink 2.4GHz / 25mW pro bezdrátový přenos video a audio (stereo) signálu a spínacího signálu (např.pro alarm), volba vysílacího kanálu, 5 volitelných kmitočtů, microstrip anténa, dosah do 700 metrů při přímé viditelnosti, napájení 12V DC

- frekvenční rozsah 2.4-2.4835GHz
- video vstup FBAS 1V š-š, 75 ohm, frekv.rozsah 30Hz-5MHz, CINCH konektor
- audio vstup (stereo) nastavitelný 0,1-10V š-š, frekv. 15Hz-15KHz, 2x CINCH
- spínací kanál Ton A 32kHz (otevřený kolektor GND, R>10kHz)
- kanálový volič s displejem pro nastavení 5ti volitelných kmitočtů
- modulace F3F (video / audio)
- napájení 10-30V DC (120mA/12VDC), DC konektor Jack 1.9/6.6mm
- anténa PCB Platinum
- rozměr 105x48x100mm
- krytí IP 30, provozní teploty -10 až +55 st.C
- hmotnost 400g

2.6.5.2 PROOUT-T venkovní vysílač ProfiLink

Obr. 26 PROOUT-T venkovní vysílač ProfiLink

Venkovní vysílač ProfiLink 2.4GHz / 25mW v plastovém krytu (ABS/IP54) pro bezdrátový přenos video a audio (stereo) signálu a spínacího signálu (např.pro alarm), volba vysílacího kanálu, 5 volitelných kmitočtů, microstrip anténa, dosah do 700 metrů při přímé viditelnosti, napájení 12V DC

- frekvenční rozsah 2.4-2.4835GHz
- video vstup FBAS 1V š-š, 75 ohm, frekv.rozsah 30Hz-5MHz, svorky
- audio vstup (stereo) nastavitelný 0,1-10V š-š, frekv. 15Hz-15KHz, svorky
- spínací kanál Ton A 32kHz (otevřený kolektor GND, R>10kHz)
- kanálový volič s DIP přepínačem pro nastavení 5ti volitelných kmitočtů
- modulace F3F (video / audio)
- možnost jednoduché ochrany proti odposlechu, inverze video signálu
- napájení 10-30V DC (160mA/12VDC), svorky
- integrovaná všesměrová anténa 0dB
- rozměr 180x120x70mm

- krytí IP 54, provozní teploty -20 až +60 st.C

- hmotnost 350g

2.6.5.3 PROKIT-T miniaturní vysílač do krytu a anténa

Obr. 27 PROKIT-T miniaturní vysílač do krytu a anténa

Souprava miniaturního vysílače ProfiLink 2.4GHz / 25mW pro zabudování (např. do venkovního kamerového krytu) pro bezdrátový přenos obrazu a zvuku (stereo), spínacího signálu (např.pro alarm), volba vysílacího kanálu, 5 volitelných kmitočtů, všesměrová anténa, dosah do 800 metrů při přímé viditelnosti, napájení 12V DC

- frekvenční rozsah 2.4-2.4835GHz

- video vstup FBAS 1V š-š, 75 ohm, frekv.rozsah 30Hz-5MHz

- audio vstup (stereo) 500mV, frekv. 15Hz-15KHz

- spínací kanál Ton A 32kHz (otevřený kolektor GND, R>10kHz)

- kanálový volič s DIP přepínačem pro nastavení 5ti volitelných kmitočtů

- modulace F3F (video / audio)

- napájení 130mA/12VDC

- integrovaná všesměrová anténa s propojovacím kabelem 40cm

- rozměr 75x68x28mm

- krytí IP 30, provozní teploty -20 až +60 st.C

- hmotnost 170g

2.6.5.4 PROIV-R přijímač, microstrip

Obr. 28PROIV-R přijímač

Přijímač ProfiLink 2.4GHz / 25mW pro bezdrátový přenos video a audio (stereo) signálu, spínacího signálu (např.pro alarm), volba vysílacího kanálu, 5 volitelných kmitočtů, microstrip anténa, dosah do 700 metrů při přímé viditelnosti, napájení 12V DC

- frekvenční rozsah 2.4-2.4835GHz

- video výstup FBAS 1V š-š, 75 ohm, frekv.rozsah 30Hz-5MHz, CINCH konektor

- nastavitelná amplitudová výstupní úroveň videosignálu 0,7-1,2V š-š

- audio výstup (stereo) nastavitelný 500mW

2.6.5.5 PROOUT-R venkovní přijímač

Obr. 29 PROOUT-R venkovní přijímač

Venkovní přijímač ProfiLink 2.4GHz / 25mW v plastovém krytu (ABS/IP54) pro bezdrátový přenos video a audio (stereo) signálu a spínacího signálu (např.pro alarm), volba vysílacího kanálu, 5 volitelných kmitočtů, vestavěná PCB anténa, dosah 600 m, napájení 12V DC (adaptér v cenně)

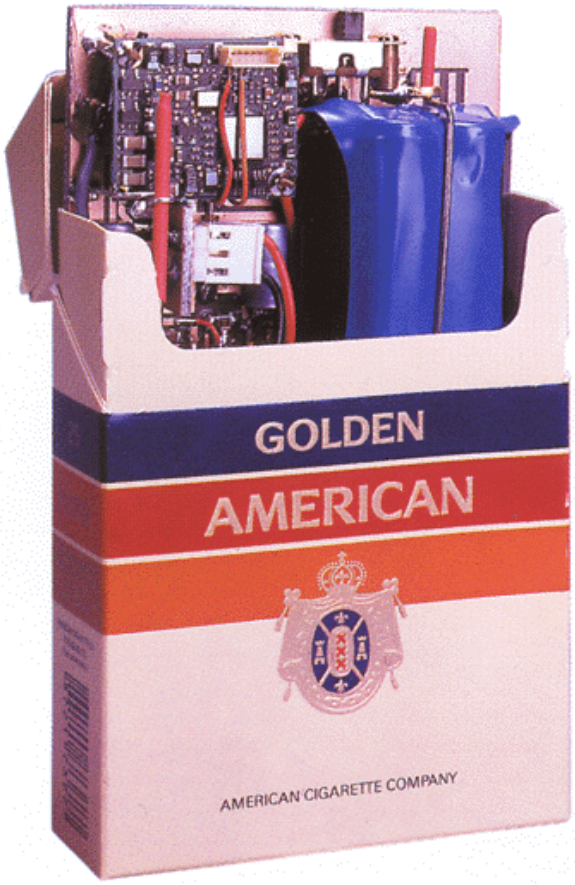
- frekvenční rozsah 2.4-2.4835GHz

- video výstup FBAS 1V š-š, 75 ohm, frekv.rozsah 30Hz-5MHz, svorky

- nastavitelná úroveň amplitudy videosignálu 0,7-1,2V š-š

- audio výstup (stereo) 500mV

2.6.5.6 ProfiLink Cigarette box - vysílač



Obr. 30ProfiLink Cigarette box - vysílač

Vysílač barevného video signálu a zvuku vč. kamery, umístěný v cigaretové krabičce. Vysílací frekvence 2,4 GHz, výkon 25 mW, dosah cca 400m. Napájení z vlastního akumulátoru 6 VDC, doba provozu na plně nabité akumulátory cca 2 hod. Hmotnost 120 g.

2.6.6 Video systém na monitorování a střežení objektů - MRP-Video 4

MRP-Video je počítačový videosystém, který umožňuje přenášet obraz po telefonních sítích, sítích LAN a po Internetu. Tento osvědčený bezpečnostní systém ocení všichni majitelé firem, obchodů, rodinných domů a firmy zabezpečující ostrahu objektů. [22]

2.6.6.1 Monitorování

Pomocí Video serveru můžeme monitorovat jeden až šestnáct objektů(kamer) a snímky z daných objektů ukládat na pevný disk. Systém umožňuje analyzovat události až několik měsíců zpětně. [22]

2.6.6.2 Střežení

Na jednotlivých sledovaných objektech lze nastavit zóny střežení. Při narušení těchto zón Video-server událost zaznamená na pevný disk a dále se může bez zásahu obsluhy spojit se stanicí Video-klient ve vzdáleném objektu a odesílat jí snímky narušitele, umožňuje odeslat poplachové textové zprávy (SMS) se seznamem narušených kamer a poplachové multimediální zprávy (MMS) a e-maily se snímky narušené kamery. MRP-Video klient při přijetí hlášení o poplachu dokáže na Vás promluvit lidským hlasem. V provedeních disponujících vstupy a výstupy (Standard, Professional) může Video server při poplachu sepnout výstup a tím, např. spustit sirénu. [22]

2.6.6.3 Vzdálené monitorování a řízení

Z libovolného místa na světě, prostřednictvím Internetu nebo běžného telefonního připojení, můžete sledovat, co se právě děje ve vaší firmě, u vás doma, případně v odposlouchávané místnosti. Také můžete prohlížet archivní snímky, protokol událostí a nastavovat střežení Video serveru a parametry jednotlivých kamer. Video server můžete také ovládat prostřednictvím SMS zpráv a nechat si na vyžádání zaslat snímky z vybraných kamer prostřednictvím MMS zpráv. [22]

2.6.7 Utajovač bezdrátových videopřenosů - ViewLock

Zařízení pro utajení bezdrátového videopřenosu. Zařízení náhodně přerušuje a převrací řádky videosignálu. Původní řádkové impulsy však zůstávají zachovány. To umožňuje používat jak normu PAL, tak i NTSC. Je vybaven portem RS232 pro počítačovou konfiguraci. Je možno dodat s rozšířením o zvukový kanál. Krytí IP 65 umožňuje umístění ve venkovním prostředí. Napájení 8-32VDC. [6]

Obr. 31 Sada kodéru a dekodéru ViewLock

Obr. 32 Zachycený zakódovaný obraz a dekódovaný obraz

3 ODHALOVÁNÍ A OBRANA PROTI POUŽITÍ SPECIÁLNÍCH BEZPEČNOSTNÍCH PROSTŘEDKŮ

V souvislosti s růstem nabídky a s rostoucím počtem i v praxi používaných odposlechových prostředků vzrůstá přímo úměrně i počet kanceláří, které používají celou řadu technických prostředků na ochranu proti odposlechu.

Použití některých prostředků je povinné v prostorách, ve kterých dochází k seznamování se s utajovanými skutečnostmi v souladu se Zákonem na ochranu utajovaných informací a bezpečnostní způsobilosti.

3.1 Doporučené vybavení bezpečné kanceláře

3.1.1 Detektivní a bezpečnostní agentura

Každý subjekt, působící v oblasti bezpečnosti – společnosti montující zabezpečovací systémy, bezpečnostní a detektivní agentury – musí zajistit, aby veškeré informace získané od klienta v oblasti zabezpečení jeho majetku, osob, dat a informací zůstaly bezpečně v jejich držení. To se týká zejména plánů zabezpečení a přístupových kódů. U detektivní kanceláře jsou tyto nároky podstatně náročnější. Detektivní kancelář působí ve velice diskrétní oblasti – dostává k dispozici neveřejné informace o problémech v činnosti jejich klienta, včetně podezřelých osob, o případné nevěře, apod. Již tyto informace samotného mohou zadavatelům způsobit řadu obtíží (z praxe víme, že většina zejména průmyslových podniků, nemá nejmenší zájem na zveřejňování informací o vnitřní kriminalitě, ale i o vnějších bezpečnostních problémech – to platí především pro bankovní sektor). Zároveň při realizaci zakázky detektivní agentura zajišťuje pro klienta informace, které jeho podezření potvrzují nebo vyvracejí, případně pro něj zajišťují veřejné i neveřejné informace o jeho konkurentech.

Proto by měla zejména detektivní agentura zajistit jednak bezpečné uložení získaných informací a zpráv a také by měla zajistit, aby informace, které získá od klienta v ústní podobě nebo mu je v této podobě předává, by měly zůstat naprosto diskrétní.

Z hlediska prováděných opatření by se měly v jednacích prostorách provádět prohlídky proti odposlechu (v pravidelných intervalech, ale také náhodně před důležitým jednáním).

V těchto prostorách by měly být také nainstalovány technické prostředky, které zamezují nebo ztěžují provádění odposlechu – paměťový rádiový analyzátor a šumový generátor, pro

ochranu proti nežádoucímu provozu GSM telefonů by měl být v provozu identifikátor jejich provozu.

Veškeré písemné dokumenty by měly být uloženy v trezorech a informace v datové podobě by měly být šifrovány.

Vzhledem ke skutečnosti, že detektivní kanceláře mají většinou velmi málo zaměstnanců, jako dostačující další zabezpečení dostačuje systém elektronického zabezpečení napojené na pult centrální ochrany.

3.1.2 Manažerská kancelář

Co se týče zabezpečení manažerské kanceláře, mělo by být totožné jako u detektivní agentury. Toto zabezpečení by mělo být ale podstatně bohatší zejména v oblasti dodatečných bezpečnostních opatření – mimo funkční elektronický zabezpečovací systém by se mělo jednat o docházkový a přístupový terminál do vybraných prostor a případně i systém skrytých kamer (je však nutné dbát na zákonná omezení jejich použití).

Použití těchto systémů je nutné provádět z toho důvodu, že v praxi se ukazuje, že společnostem hrozí ve větší míře riziko z řad vlastních zaměstnanců než z jeho okolí (toho se využívá při některých detektivních postupech).

V případě, že si manažeři mezi sebou vyměňují citlivé informace a také komunikují s určitým okolím o důležitých záležitostech pomocí mobilních telefonů, doporučuje se v současnosti pro tyto účely používat kryptované GSM telefony.

3.1.3 Zásady k zamezení úniku citlivých informací

a) nepoužívejte soukromý nebo firemní telefonní přístroj k projednávání citlivých

informací

b) pro citlivé telefonní hovory využívejte náhodně volenou telefonní budku

c) nechte si nainstalovat kvalitní utajovač telefonních hovorů

d) dodržujte základní zásady při zpracování citlivých informací na počítačích

e) objednejte si konzultační služby seriozní firmy ke zhodnocení úrovně možného ohrožení a k provedení protiodposlechové prohlídky. [2]

3.2 Obranně technická prohlídka

Obranně technická prohlídka je nedílnou součástí systému speciální ochrany. Smyslem jejich provádění je komplexní prověrka bezpečnosti z hlediska úniku informací. To znamená zjištění, zda v dané době je nebo není v objektu umístěno odposlechové zařízení. Jedná se o celkové posouzení objektu a navržení dalších potřebných opatření. Prohlídka bude efektivní jen tehdy, pokud po jejím provedení budou dodržována organizační, režimová a technická opatření.

3.2.1 Postup při provádění obranně technické prohlídky

3.2.1.1 Přípravná část

Provádí se za velmi přísného utajení, její vyzrazení by mohlo degradovat účinek celé prohlídky. Pracovníci se musí seznámit s objektem, ve kterém se budou pohybovat, a to včetně jeho okolí, režimem údržby, úklidu, návštěv, konstrukčního a stavebního řešení a rozmístění nábytku. Sále musí být seznámeni s rozmístěním elektrických rozvodů, možnostni přístupu k elektrickým rozvaděčům, s rozmístěním telefonních rozvodů včetně pobočkových ústředen.

Odpovědná osoba daného objektu či firmy (zadavatele) provede vstupní analýzu zaměřenou na zjištění možného rizika, stanoví datum, čas a způsob provedení prohlídky. Ta může být provedena tak, že všem bude zřejmé, co se provádí nebo tajně mimo pracovní dobu bez vědomí ostatních pracovníků. Většina firem specializujících se na tuto činnost vyžaduje při provádění prohlídky trvalou přítomnost zodpovědné osoby zadavatele.. Ta mimo jiné určuje, co se provede s nalezeným odposlechovým zařízením.

Je tedy nutno stanovit:

- kdo bude seznámen s provedením obranně technické prohlídky
- zodpovědnou osobu zadavatele, která bude trvale přítomna
- časový harmonogram
- jak se bude postupovat při nalezení odposlechového zařízení

a) Fyzická kontrola

Jde o fyzickou prohlídkou místností. V této části dojde k rozebrání a následnému složení všech prostředků, ve kterých by se mohl nacházet odposlechový prostředek – zásuvky, rozdvojky, vypínače, prodlužovaní šňůry, telefonní aparáty, světla, detektory pohybu, kouře, atd.

b) Rádiová analýza

V této části se provádí spektrální analýza – vyhodnocují se frekvence, které jsou v daný okamžik v daném místě aktivní. Tato metoda odhalí pracující rádiové odposlechové prostředky. Vytvoří se frekvenční mapy prostor pomocí spektrálního analyzátoru, což představuje zhotovení seznamu všech radiových frekvencí, které se vyskytují v kontrolovaném prostoru (tj.aktivní prostředky). Tento soupis pak velmi usnadňuje další periodické prohlídky.

c) Detekce nelinearit

Jde o vyhledání všech polovodičových součástek pomocí detektoru nelineárních přechodů. Detekce nelinearit využívá následující princip – v praxi nebyl doposud vyroben odposlechový prostředek, který by neobsahoval polovodičové součástky. Detekce nelinearit tedy odhaluje všechny polovodičové součástky, které jsou zachyceny vyslaným elektromagnetickým polem a jsou diagnostikovány „harmonické“ odraženého signálu (v současnosti 2. a 3. harmonická – tato diagnostika oddělí od skutečných polovodičových přechodů přechody náhodně vzniklé např. dotykem 2 kovů).

Tato kontrola je důležitá z hlediska nalezení zpravodajských prostředků, takových, které jsou dálkově ovládány nebo přenášejí informace "paketově", to znamená, že informace uchovávají ve své paměti a po uplynutí periody je dokáží přenést ve velmi krátkém okamžiku (tj. pasivní prostředky) nebo přenášejí informace ze zájmového prostoru jiným způsobem. Především ve starších budovách jsou tímto detektorem odhalovány i prostředky, které jsou napájené ze síťového rozvodu a jsou zazděné. Tímto způsobem se kontrolují stěny objektu, stavební vybavení, kancelářské vybavení.

V současnosti se jedná o nejspolehlivější metodu odhalování odposlechových prostředků.

Obr. 33 Detektor nelineárních přechodů

SuperBroom

d) Ostatní měření

Do těchto měření patří kontroly telefonních vedení, kontroly v infraspektru, kontroly vedení v nadhovorovém pásmu, …

3.2.1.2 Nalezení odposlechového prostředku

Možnosti řešení:

- jeho likvidace
- přivolání Policie ČR
- využitá odposlechového prostředku pro dezinformaci předpokládaného pachatele

3.2.1.3 Ukončení obranně technické prohlídky

Zadavatel obdrží hned po ukončení prohlídky ústní zprávu o výsledku, poté je mu zaslána písemná zpráva s popsaným postupem a jeho výsledky. Ve zprávě je také provedeno zhodnocení ochrany objektu před únikem informací a navrhnuta nová organizační, režimová a technická opatření vedoucí ke snížení rizik.

3.2.2 Obecné zásady protiodposlechových prohlídek

Tyto zásady je nutno dodržovat bez ohledu na to, zda to provádíme sami nebo specializovaná firma.

a) Zahájení prohlídky v čase, kdy se předpokládá aktivace odposlechových zařízení (v průběhu jednání, některé odposlechy mohou být dálkově ovládání a předstírání jednání nám může zajisti aktivaci těchto prostředků).

b) Všechny následné prohlídky by měly být prováděny v náhodných intervalech.

c) Vyhledávání musí být prováděno skrytým způsobem. Porady s kolegy, nebo techniky, vlastní zahájení prohlídky, nastavení přístrojů, lokalizace zařízení nesmí dát tomu, kdo odposlech provádí informaci o provádění OTP nebo o jeho odhalení.

d) Úspěch při provádění prohlídky je závislý na vybavení, odborných vědomostech a pečlivosti, která je vyhledávání věnována.

e) Pokud si prohlídku provádíte sami je nutné se před vlastním zahájením vyhledávání důkladně seznámit s jednotlivými detekčními metodami a možnostmi přístrojů. Tyto nácviky vyhledávání je nutno provádět utajeně a zásadně na bezpečných místech.

f) Největší pozornost je potřeba věnovat oblasti, kde se odehrávají důležité rozhovory (za psacím stolem, blízko telefonního přístroje). Největší množství bude umístěno v okruhu

7 m z důvodu dobrého hlasového příjmu.

g) Je třeba vytvořit vhodné podmínky pro prohlídku, zatáhnout všechny závěsy – eliminace možnosti pozorování, zapnout všechna světla a některé další přístroje z důvodu vytvoření běžného pracovního prostředí. [2]

3.3 Speciální technika na ochranu informací

3.3.1 Ochrana proti kontaktnímu nebo bezkontaktnímu snímání informací z oken nebo zdí chráněného objektu

Generátor bílého šumu je prostředek, který generuje bílý (v některých případech růžový) šum. Šumová ochrana proti odposlechu spočívá v přímém mechanickém zašumění míst pomocí piezoelektrických nebo elektrodynamických měničů, kde lze zvuky snímat (zdi, okna) nebo zašumění částí nábytku kde lze operativní prostředky skrytě umístit. Jako doplněk

tohoto přístroje se může instalovat souprava reproduktorů, která dokáže překrýt nahrávku pořizovanou na diktafony. Bílý šum prochází všemi frekvencemi lidské řeči a vzhledem ke skutečnosti, že zvuk je mechanické vlnění se do užitečného signálu „přimíchá“ a nelze jej v současné době dostupnými prostředky odstranit.

Jedná se o efektivní zařízení, které dokáže velmi spolehlivě zabránit provádění odposlechu pomocí stetoskopických mikrofonů, laserových mikrofonů a při použití reproduktorů i nahrávání informací na diktafony.

Za nevýhodu můžeme považovat to, že bílý šum je ve slyšitelném spektru a tudíž šumový generátor působí jako novodobá náhrada tekoucích vodovodů. Při ochraně zdí chráněných prostorů je nutné počítat i se stavebními úpravami, proto je nutné na tento druh ochrany pamatovat již při výstavbě nebo rekonstrukci.

Použití šumového generátoru je povinné v zabezpečených oblastech typu „T“ a „PT“ podle Zákona na ochranu utajovaných informací a bezpečnostní způsobilosti. [3]

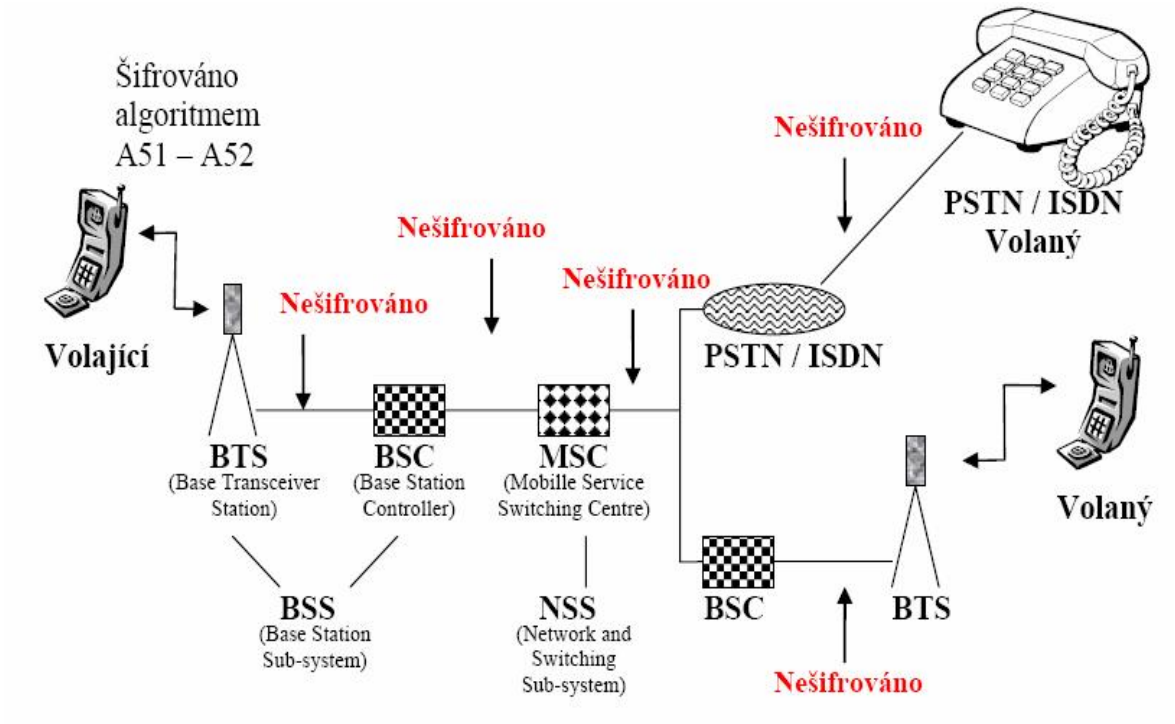
3.3.1.1 Příklad - Inteligentní šumový generátor SNG

SNG je inteligentní výkonový šumový generátor umožňující připojení až 100 piezokeramických akustických měničů, 2 - 12 nízkoimpedančních reproduktorů, nebo jejich vzájemnou kombinaci. Instalací piezoměničů na vnitřní stěny nábytku, stolů a dalších předmětů uvnitř kanceláře lze ralizovat vhodnou doplňkovou ochranu proti operativně umístěným přenosným odposlechovým prostředkům. Účinnost SNG optimalizuje vestavěný procesor, který v automatickém režimu analyzuje zvuky z místnosti a zajišťuje jen takovou úroveň zašumění, která je nutná v závislosti na hlasitosti konverzace. Pracovník není rušen šumem pokud je v místnosti klid, přístroj nevypíná, čímž je následně stoprocentně zajištěn automatický náběh šumu například při náhlé návštěvě, zahájení jednání, telefonním hovoru, atd. SNG je konstruován k zavěšení na zeď, nebo bok pracovního stolu, nejlépe v přímém dosahu uživatele. Z předního panelu lze pomocí tří ovládacích přepínačů zvolit buď "malý" nebo "velký" výkon a obě výkonové úrovně lze provozovat buď v manuálním nebo automatickém režimu. Pět barevných LED signalizuje nastavený režim včetně vnitřního testu činnosti procesoru. [20]

Obr. 34 Inteligentní šumový generátor SNG

3.3.2 Ochrana proti neoprávněnému užití GSM telefonů

Navzdory všeobecnému povědomí, komunikace přes síť GSM není dostatečně chráněna, může být jednoduše odposlouchávána. Poskytovatelé služeb GSM používají ochrany pomocí šifrovacího algoritmu. Algoritmus používaný pro vytvoření pseudonáhodných frekvencí je algoritmus A5. A5 je symetrický typ algoritmu, chránící přenos mezi poskytovatelem služby a předplatitelem. Tato ochrana je použita jen mezi základnovou stanicí BTS (první podsystém sítě GSM) a připojeným GSM zařízením. Nicméně ze základny je hlas přenášen přes GSM síť v nešifrovaném módu. [3]



Obr. 35 Schéma GSM a PSTN / ISDN sítě

Popis:

BTS základna vysílače s přijímačem

BSC základna dozorce

MSC mobilní služba spouštěcího centra

BSS základna podsystému

NSS síť a spínání podsystému

PSTN/ISDN Receiving number PSTN/ISDN číslo volaného

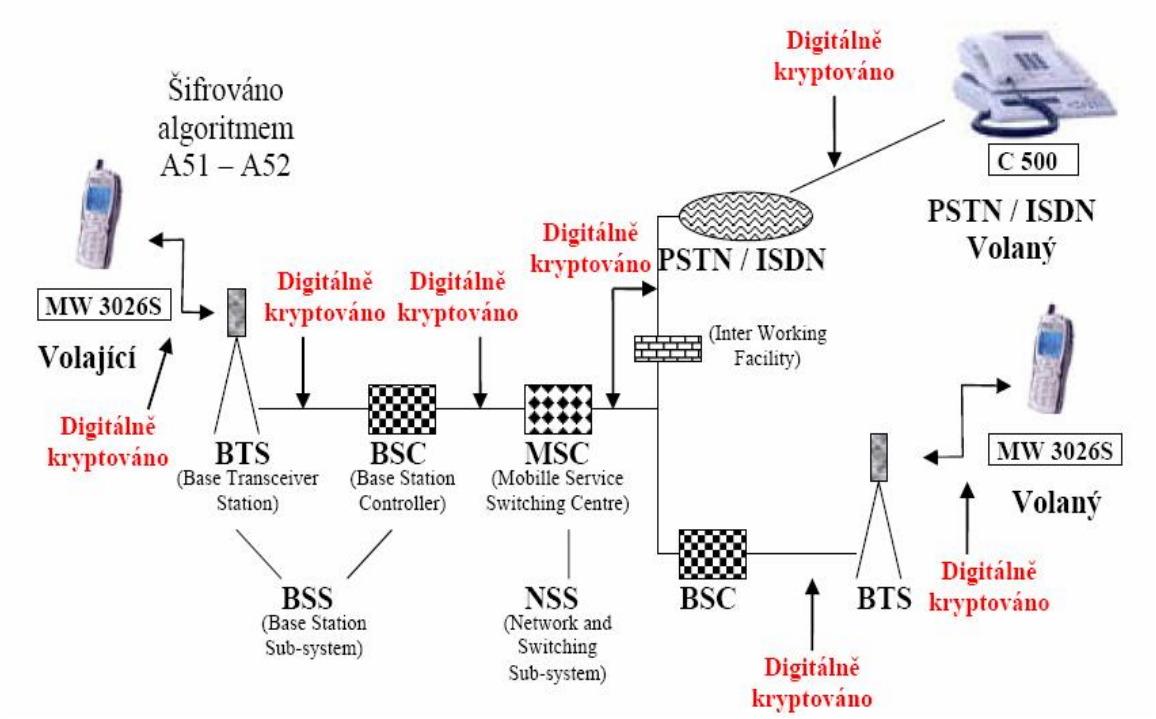
3.3.2.1 Šifrovaný mobilní telefon

Zachycení GSM komunikace je možné dokonce na vzdušné lince (mezi mobilním telefonem a BTS) nebo MSC (přepínač). Ve vzduchu je zachycení GSM komunikace provedeno náhradou nebo záměnou BTS. Z MSC je možné zachytit jakoukoli komunikaci z mobilního telefonu (GSM).

Proto někteří výrobci mobilních telefonů vyvinuli šifrované mobilní telefony.Například Sagem navrhl a vyvinul třetí generaci kompletně šifrovaného duálního (900 MHz a

1800 MHz) GSM mobilního terminálu: MW 3026 S, aby poskytl obranným složkám,

speciálním silám, policii, celním úřadům, stejně jako průmyslovým skupinám a společnostem atd. chráněnou komunikaci přes síť GSM.



Obr. 36 Schéma digitálně kryptované GSM a PSTN / ISDN sítě

Z obrázku 36 je patrné, že šifrovaný mobilní telefon nabízí uživateli skutečné, úplné kódování, nezávislé na síti a to jak přes sítě GSM/DCS tak přes sítě PSTN/ISDN a satelitní sítě.

Šifrovaný mobilní telefon nabízí následující služby vysokého stupně ochrany:

- utajenost (digitální kódování),

- ověření pravosti uživatele (zobrazuje identifikátor korespondentů během šifrované komunikace),

- kontrola přístupu (přístupový kód povolující šifrovací funkce).

Jak je vidět na obrázku, IWF (zařízení pracující uvnitř – Inter Working Facility) umožňuje digitální přenos mezi sítěmi GSM a PSTN nebo ISDN. Tak jako lze kryptovat hovor v

síti GSM, lze provést kompletní ochranu mezi GSM a PSTN nebo ISDN terminály stejně jako mezi dvěma PSTN nebo ISDN telefonními přístroji.

Obr. 37 MW 3026 S - přední strana mobilního telefonu a kryptovací modul.

Jako každý běžný mobilní telefon dovoluje komunikaci v jednoduchém módu a navíc pomocí kryptovacího modulu také dovoluje používat šifrovací technologii pro vytvoření kódované komunikace.

Použití MW 3026 S vyžaduje aktivaci dvou služeb, hlasové služby a datové služby společně se jim vyhrazenými čísly. To znamená, že čísla hlasového volání jsou používána pro jednoduchou komunikaci, zatímco čísla datového volání korespondují pouze s kódovanými hovory. Kódované komunikace jsou vytvářeny skrze datovou službu v asynchronním, transparentním módu, 4800 nebo 9600 b/s. Před tím než je hovor přenesen, se hlas nejprve digitalizuje, potom se zakóduje a nakonec se přenese datovým kanálem. Šifrované spojení může být navázáno mezi dvěma stejně vybavenými mobily.

Hlavní výhody řešení nabízené modelem šifrovaného mobilního telefonu:

- dvě hlavní funkce v jednom mobilním telefonu: běžné funkce mobilního telefonu (při nešifrovaných hovorech) a funkce pro šifrovanou komunikaci,
- velmi vysoký stupeň zabezpečení šifrované komunikace díky ověřenému vlastnímu symetrickému algoritmu používajícímu 128 bitových provozních klíčů,
- využívá současné infrastruktury sítě GSM,
- šifrovaná komunikace nezávislá na přenosové síti,
- funguje celosvětově na sítích GSM
- správa provozních klíčů umožňuje definovat strukturu hierarchických kryptovacích sítí,

- jednoduchá obsluha a použití jako u klasického GSM, uživatelsky příjemné rozhraní,

Kryptovací modul obsahuje následující technologii:

- Vocoder - zařízení převádějící hlas na signál schopný přenosu- digitalizuje hlas,

- Šifrovací jednotka - 128 bitový klíč symetrického algoritmu kóduje digitalizovaný hlas,

- Datové rozhraní - během odchozích hovorů je kódovaný digitální signál posílán do Mobilního telefonu a potom je přenášen do datové sítě. Během příchozích hovorů je kódovaný digitální signál přicházející z datové sítě přes mobilní telefon posílán do šifrovací jednotky a potom rozšifrován před zpětným vysláním do přijímače mobilního telefonu. [3]

3.3.2.2 Identifikace provozu GSM telefonů

Jsou to zařízení, která velmi citlivě detekují signály v oblasti GSM pásem a dokáží obsluhu informovat o nepovoleném vysílání vizuálně nebo akusticky. Jednotky mohou pracovat v autonomním nebo sběrnicovém režimu.

Nevýhoda jejich použití spočívá zejména v nutnosti pečlivého nastavení jejich citlivosti takovým způsobem, aby se minimalizovalo množství falešných poplachů způsobených signály zvenčí.

Tyto prostředky se nejčastěji používají ve vězeňské správě, ve finančních institucích. [3]

3.3.2.3 Příklad - DMC Detektor mobilní komunikace

Detektor mobilní komunikace DMC je určen pro selektivní zjištění činnosti GSM telefonních přístrojů v pásmech 900 i 1800 MHz. DMC plně respektuje specifikaci GSM komunikace ETSI a je schopen registrovat činnost mobilních telefonů i v extrémních podmínkách například v blízkosti základnových stanic GSM systému, kde je výkon mobilních telefonů automaticky snížen na minimální úroveň. V těchto podmínkách může vyzařovaný výkon telefonu klesnout i pod 1mW, přičemž výkon blízké základnové stanice je typicky více než 100 W.

DMC je odolný proti signálům lokálních TV a FM vysílačů, ale i proti často používané vnitřní komunikaci telefonními přístroji DECT. DMC je navíc schopen detekovat a zpracovat i analogové signály běžně používaných a rozířených komunikačních zařízení jako jsou

například mobilní telefony NMT 450 a kapesní radiostanice pracující v kmitočtovém rozsahu 20 až 600 MHz. Až 128 detektorů DMC může být zapojeno do systému s kontrolní jednotkou DMCC. DMCC. umožňuje účinně potlačit falešné poplachy vzniklé komunikací ve vlastní radiové síti objektu. DMCC uchovává informace o detekovaných událostech, jež mohou být též zazmenávány na připojené tiskárně nebo PC. [20]

Obr. 38 DMC Detektor mobilní komunikace

3.3.2.4 Příklad - DMCC Řídící jednotka pro detektory mobilní komunikace

DMCC je řídící jednotka pro detektory mobilní komunikace DMC. Až 128 detektorů DMC může být zapojeno do systému s jednotkou DMCC. DMCC umožňuje účinně potlačit falešné poplachy vzniklé komunikací ve vlastní radiové síti objektu. DMCC uchovává informace o detekovaných událostech, jež mohou být též zazmenávány na připojené tiskárně nebo PC. [20]

Obr. 39 DMCC Řídící jednotka pro detektory mobilní komunikace

3.3.2.5 GSM jammer

Jde se o prostředek, který pracuje v pásmu GSM telefonů a který zaruší přijímače v mobilních telefonech a ty se nedokáží přihlásit do sítě. V současné době existuje mnoho různých provedení jammerů, liší se však svou spolehlivostí. GSM jammer je určen pro rušení provozu mobilních telefonů zejména v menších prostorách, jako jsou kanceláře, byty apod.

Základní problém používání GSM jammerů je jejich nezákonnost (není povoleno rušit signál operátorů). Výjimka z tohoto ustanovení platí pouze pro část státní správy, která může používat nehomologovaná zařízení. Přesto se však ve světě i v ČR vyrábějí a používají. [3]

Příklady použití

- Zamezení odposlechu přes upravený mobilní telefon. Takové riziko je v současné době velmi reálné nejen při různých jednáních a poradách, ale prakticky v každodenním životě. Důvodem je velká rozšířenost mobilních telefonů, zejména pak jejich úprav a to i levných modelů. Přitom krása mobilního telefonu jako štěnice je v tom, že vypadá tak nevinně ...

- Ochrana před sledováním pomocí GPS. Rušička umístěná např. ve voze se zabudovanou jednotkou GPS zabrání dálkovému přenosu informací o poloze prostřednictvím sítě GSM.

- Nejčastější využití najde rušička všude tam, kde z různých příčin není vhodné nebo zakázané používat mobil - např. nemocnice, banky, kina, divadla, muzea, věznice apod.

Rušičky jsou ale také používány bezpečnostními složkami např. pro zamezení dálkové aktivace výbušniny apod.

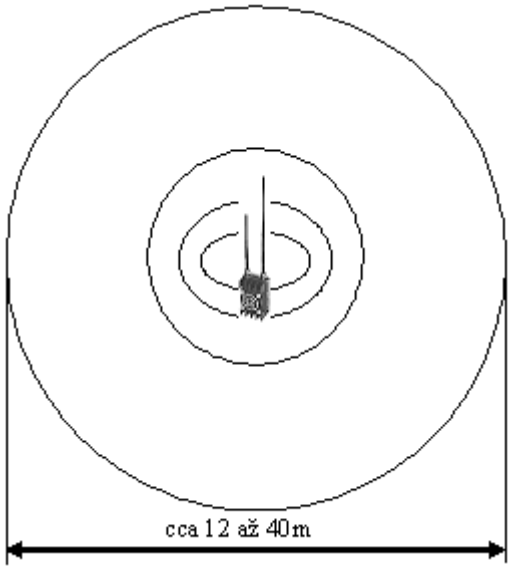
3.3.2.6 Přiklad - 2W duální rušička mobilních telefonů

Přenosná rušička je vybavena dvěmi laděnými anténami s kulovou vyzařovací charakteristikou. Rušící signál je tak vysílán všesměrově a ideálním umístěním je střed zájmového prostoru. Celkový vysílací výkon 2000 mW rovnoměrně pokrývá obě GSM pásma 900 i 1800 MHz. Systém je zabudován do malé kovové krabičky a vybaven aktivním chladičem.

Dosah rušičky v dané lokalitě je velmi závislý na intenzitě signálu od okolních základnových stanic mobilních operátorů (BTS). Průměr kruhové oblasti, která je účinně zarušena centrálně umístěným jammerem se pohybuje přibližně od cca 12 do 40 m (prostor bez překážek), což odpovídá kruhové ploše cca 100 až 1000 m2. V lokalitách s velmi slabým signálem BTS může být průměr zarušené oblasti až 80 m.

V zarušené zóně se mobilní telefon chová jakoby byl mimo dosah signálu. Je znemožněna jakákoliv komunikace a příjem / odesílání SMS nebo MMS. Na okraji zarušené oblasti telefon jen sporadicky navazuje spojení s BTS a hovor je nesrozumitelný, z převážné části poznamenán výpadky spojení. [21]

Obr. 40 2W duální rušička mobilních telefonů



Obr. 41 Rozsah 2Wrušičky

3.3.3 Ochrana proti rádiovému odposlechu

3.3.3.1 Rádiové analyzátory

Jedná se o prostředky, do jejichž paměti se zapíší všechny rádiové frekvence, které jsou v daném čase a v dané oblasti aktivní a jsou prohlášeny za bezpečné a v následném scannování rádiového spektra a porovnání skutečného stavu s pamětí. V případě nalezení neshody dokáží změřit frekvenci nového vysílače a umožňují obsluze poslechnout si nový signál, případně ukáží sílu pole (tzn. relativní vzdálenost vysílače od přijímače).

Jednotlivé typy se liší zejména šířkou pásma, které dokáží kontrolovat a v rychlosti této kontroly.

Nevýhoda spočívá v relativní náročnosti na obsluhu (některé pro správnou činnost potřebují pouze zaškolenou obsluhu a některé vyžadují práci specialisty). Základní problém je možné spatřovat v množství rádiových signálů aktivních zejména ve velkých městech (např. v Londýně je jich obvykle aktivních přes 600 a v Praze ve vybraných lokalitách přes 200). S tím opět souvisí citlivost nastavení a množství „falešných“ poplachů (ne všechny rušivé frekvence pochází z odposlechu – záchranné služby, taxislužba, messengeři, …). Toto nastavení je důležité pro správnou činnost a zabránění vzniku zbytečných obav.

Je možné koupit i rádiové analyzátory, které je možné propojit přes internet a zajistit jejich dálkovou správu. Tímto způsobem je možné „přivést“ specialistu v rychlém čase do kterékoliv kanceláře kdekoliv na světě.

Použití rádiových analyzátorů generátoru je povinné v zabezpečených oblastech typu „T“ a „PT“ dle Zákona na ochranu utajovaných informací bezpečnostní způsobilosti. [3]

3.3.3.2 Příklad - Radiový analyzátor MRA-3Q

MRA-3Q je systémová verze speciálního přijímače určeného k ochraně proti radiovému odposlechu v kmitočtovém pásmu 36 až 3600 MHz. „Štěnic prosté“ radiové spektrum je jednoduchou instrukcí uloženo do paměti přístroje a dále je automaticky porovnáváno s aktuálními signály v zabezpečeném prostoru. Jakýkoliv nový signál se okamžitě zapisuje do paměti nových signálů a uživatel je o jeho přítomnosti informován víceúrovňovou poplachovou signalizací. Přijímané signály lze vyladit, poslouchat a změřit jejich kmitočet. Statistické údaje o nových signálech zůstávají dlouhodobě uloženy v paměti (i po vypnutí), lze s nimi pracovat a zejména upravovat referenční radiové pozadí tak, aby se na základě dlouhodobého měření optimalizovala odolnost vůči falešným poplachům.

K samotnému MRA-3Q lze připojit audio nahrávač a zvolit vhodný režim automatického nahrávání vzorků signálů, které způsobují poplach. S pomocí audio nahrávek lze spolehlivě identifikovat zda a jak byl střežený objekt napaden radiovým odposlechem. [20]

Obr. 42 Radiový analyzátor MRA-3Q

3.3.3.3 Jammery

Tyto prostředky jsou funkčně obdobné jako jammer na GSM telefony. Proti jejich použití hovoří opět nezákonnost a neprozkoumaný vliv na zdraví člověka při jejich dlouhodobém používání. Pro jejich používání zase hovoří skutečnost, že neprodukují žádné falešné signály a tato funkce jim umožňuje nezávislost na práci specialisty. Jejich použití je velmi časté zejména v silových resortech. Speciální typy rádiových jammerů se nyní používají jako ochranný prostředek proti dálkově odpalovaným výbušninám, které mají roznětku iniciována rádiovým signálem. [3]

3.3.3.4 Bezpečnostní fólie a tapety

Jsou ti velmi specifické prostředky na ochranu proti rádiovému odposlechu.

Princip jejich činnosti spočívá ve vytvoření Farradayovy klece, která zamezí prostupu rádiových signálů z chráněného prostoru. Jedná se o technicky velmi náročnou aplikaci, která používá tapety s měděnou vrstvou. Tyto tapety musí být velmi pečlivě nalepeny po celé místnosti, je nutné dobře ošetřit každý kovový prostup do zdi, ochránit dveřní zárubně, dveře a okna (používá se na ně speciální sklo), instalovat síťové filtry na vedení 230 V. Celá sestava se musí velmi pečlivě uzemnit a poté se provádí měření.

Jediný zanedbaný detail má velký vliv na celkový výsledek.

Použití této technologie je vyjímečné, častěji se používají fólie na ochranu proti elektromagnetickému vyzařování počítačů. [3]

3.3.4 Ochrana proti neoprávněnému získávání informací jejich přímým nahráváním na záznamové jednotky.

S rozvojem digitální techniky se velmi ztížila ochrana proti přímému nahrávání akustických informací přímo na záznamová média. Do nedávné doby bylo možné specialistou vybaveným spektrálním analyzátorem zachytit vyzařování způsobené hlavou diktafonu. U digitálních zařízení však nic takového již nenalezneme a proto se způsob obrany musel radikálně změnit. Spolehlivou ochranu tvoří kombinace šumového generátoru se soupravou reproduktorů, které obvykle v okruhu do 1,5 m přehluší užitečnou informaci.

Druhá používaná metoda spočívá ve vytvoření silného elektromagnetického pole, které se „přimíchá“ do užitečného signálu. Tato metoda má výhodu v tichém provozu, nicméně se u

většiny těchto prostředků jedná o vysílací výkon minimálně 100 W s užitečným dosahem okolo 4 m – všichni lidé v okolí tohoto vysílače jsou tedy vystaveni tomuto záření. V praxi se také ukazuje, že spolehlivost těchto prostředků se pohybuje okolo 50%. [3]

3.3.5 Detektor nelineárních přechodů

U profesionální obranně technických prohlídek nevystačíme pouze s přístroji na kontrolu radiového spektra. Existují odposlechové vysílače aktivované na dálku, časovým spínačem, hlasem, mohou pracovat s malými výkony, v rozptýleném spektru s digitálním přenosem skrytým v silném rozhlasovém vysílači a podobně. Tyto prostředky mnohdy není možné odhalit ani profesionálními přijímači a spektrálními analyzátory. Proto se používají další detektor nelineárních přechodů. Přístroj se skládá z vysílací a přijímací antény a z vysílací a vyhodnocovací aparatury. Obě antény jsou umístěny na konci teleskopické tyče, vysílací a vyhodnocovací elektronika je ve skříňce umístěné na druhém konci této tyče, nebo se u jiných modelů se nosí pomocí popruhu na rameni. Napájení je z akumulátoru umístěného ve skříňce s elektronikou. Vysílací anténa vysílá většinou pulzní signál o frekvenco kolem 900 MHz. Přijímací anténa zachytává odražené signály od prověřovaných předmětů či stavebních konstrukcí. Polovodičové přechody odrážejí 2. harmonickou frekvenci základního signálu a kovové předměty 3. harmonickou frekvenci. Vyhodnocovací aparatura tak dokáže rozlišit, zda přístroj našel nějaký kovový předmět či polovodičovou součástku. V praxi nebyl doposud vyroben odposlechový prostředek, který by neobsahoval polovodičové součástky. Touto metodou se dají nalézt i vysílače nefunkční. Signalizace je umístěna většinou přímo na anténě, aby obsluha měla prohledávanou oblast, hlavici antény i signalizaci v jednom zorném poli. Kromě optické signalizace jsou přístroje ještě vybaveny i zvukovou signalizací do sluchátek. I práce s detektorem nelineárních přechodů však vyžaduje od obsluhy značné zkušenosti. Ne každá signalizace druhé harmonické frekvence znamená nalezení polovodičové součástky. Hrst drátěných sponek, lepený spoj dřevěných lišt v rámu obrazu, nedotažené šroubky na vodičích v elektrické zásuvce, zámky, kování skříní, pákové pořadače a mnoho jiných předmětu vykazuje nelineární přechod. Někdy stačí předmět poklepat gumovou paličkou nebo s ním zatřást a signalizace zmizí, jindy je třeba předmět rozebrat a podrobit podrobné fyzické prohlídce. [2]

3.3.5.1 Detektor nelineárních přechodů NR-900E

Přenosný pulsní detektor nelineárních přechodů představuje již čtvrtou generací v řadě NR-900. Přístroj umožňuje porovnávání úrovní druhé a třetí harmonické odraženého signálu od polovodičového přechodu. Operátor může ovládat celý detektor pomocí klávesnice s ergonomicky umístěnými ovládacími prvky. Na této klávesnici se nachází LCD display, který přehledně poskytuje množství velmi důležitých informací: zobrazení úrovně odraženého signálu druhé a třetí harmonické graficky (vyplňováním znaků) i číselně (bezrozměrně), rozdíl mezi druhou a třetí harmonickou, kde již podle znaménka a velikosti tohoto rozdílu lze identifikovat polovodičový přechod a množství pomocných údajů, jako je napětí baterie, vybraný vysílací výkon či úroveň zatlumení přijímací části. Detektor má výstup pro stereofonní sluchátka, do kterých jsou různými zvuky signalizovány tyto stavy: zvyšující se tón s rostoucí úrovní příslušné harmonické, překročení rozsahu vybrané harmonické, rozdíl harmonických vyšší než +20 dB a pokles napětí baterie.

- detekční vzdálenost: 0,5 - 2 m
- přesnost: 0,1 m
- vysílaná frekvence: 900 MHz
- vyzářený výkon pulsně - režim 300Hz: 150 W
- vyzářený výkon pulsně - režim 20 kHz: 20 W

Obr. 43 Detektor nelineárních přechodů NR-900E

Obr. 44 Použití detektoru nelineárních přechodů

4 ZÁKONNOST POUŽITÍ SPECIÁLNÍCH BEZPEČNOSTNÍCH PROSTŘEDKŮ V PRAXI PRŮMYSLU KOMERČNÍ BEZPEČNOSTI

4.1 Právní podmínky přístupu k informacím

Nejvyšší českou právní normou, v níž jsou zakotveny základní podmínky užívání informací, je Listina základních práv a svobod jako samostatný ústavní zákon. Informacemi se zabývají články 10, 13 a 17.

Ustanoveními článku 10 je chráněna lidská důstojnost člověka, jeho osobní čest, dobrá pověst, jméno a soukromí. I když se v tomto článku neužívá výrazu „informace“, ale výrazu „údaje o své osobě“, tak podle výkladu jsou informace vztahující se k určité osobě osobními údaji. Jedná se tedy o informace týkající se každého jedince, přičemž současně je vyjádřeno i právo na ochranu osobnosti před zneužíváním údajů o osobě.

Dalším článkem, který se zabývá informacemi, je článek 13, určující, že „nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů“, a to bez ohledu na to, zda jsou uschovány nebo přenášeny jakýmikoli prostředky. Zákaz porušování se týká osob fyzických, právnických i státu, a současně v souvislosti s předpokladem rozvoje technických prostředků pro přenos užívá i pojmu „jiná podobná zařízení“, jejichž uplatněním nesmí být narušeno tajemství přepravovaných zpráv.

K informacím se ještě váže článek 17 v druhém oddílu zabývajícím se politickými právy. Jedná se o to, že Listinou základních práv a svobod je zaručena „svoboda projevu a právo na informace“, „že každý má právo vyjadřovat své názory jakýmkoliv způsobem“, „svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu“. Ve čtvrtém odstavci tohoto článku je pak stanoveno, že onu svobodu „lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a spodob druhých, bezpečnosti státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti“. V odstavci pátém jsou pak stanoveny povinnosti státních orgánů a orgánů územní samosprávy „poskytovat informace o své činnosti“, přičemž podmínky a provedení stanoví zákon. [4]

4.2 Odposlech telefonních hovorů

V oblasti odposlechu telefonních hovoru i v oblasti odposlechu obecně, je významné publikované soudní rozhodnutí, které se výslovně týká použití záznamu telefonního hovoru jako důkazu v civilním soudním řízení. Jedná se o spor mezi zaměstnancem a zaměstnavatelem. Soud rozhodl takto: *"Navrhne-li účastník občanského soudního řízení k prokázání svých tvrzení důkaz, který byl pořízen nebo účastníkem opatřen v rozporu s obecně závaznými právními předpisy a jehož pořízením nebo opatřením došlo k porušení práv jiné fyzické nebo právnické osoby, soud takový důkaz jako nepřípustný neprovede. Nepřípustným důkazem je proto i záznam telefonického rozhovoru, který byl takto pořízen bez vědomí hovořících osob."*

Nepřípustnost důkazu spatřuje soud v porušení zejména Listiny základních práv a svobod (LZPS), zvláště článek 13. V odůvodnění svého rozhodnutí soud uvádí řadu velmi významných pravidel nejen z hlediska samotného užívání odposlechu telefonních hovorů, ale i z hlediska postavení zaměstnance a zaměstnavatele ve sporu o ochranu soukromí zaměstnance před zásahem provedeným prostřednictvím telefonního odposlechu.

Z toho vyplývá zákaz porušování tajemství dopravovaných zpráv (korespondence), včetně zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízení. Odposlech a záznam telekomunikačního provozu je možný jen v případech a způsobem stanovených zákonem. Takovým zákonem je v českém právním řádu např. trestní řád, který upravuje postup orgánů činných v trestním řízení (§ 88 trestního řádu). K tomu je nutno podotknout, že takovýmto zákonem je i občanský zákoník (§ 12, odst. 1 občanského zákoníku). Naproti tomu soud dále uvádí, že pracovněprávní předpisy záznam ani odposlech telekomunikačního provozu, jehož účastníky jsou zaměstnanci nebo zaměstnavatelé, neumožňují. Právní názor žalované (tj. zaměstnavatele), podle něhož jsou „obecná“ práva pracovníka na tajemství zpráv dopravovaných telefonem zaručená ústavou omezena „rámcem pracovní smlouvy a zákoníkem práce“, proto není správný.

Zprávami podávanými telefonem ve smyslu čl. 13 LZPS a korespondencí ve smyslu čl. 8 odst. 1 výše uvedené úmluvy mohou být i zprávy komunikované zaměstnancem v telefonickém hovoru jinému zaměstnanci prostřednictvím telekomunikačního zařízení jejich zaměstnavatele. Zaměstnavatel není oprávněn takové telefonické hovory bez souhlasu hovořících zaměstnanců či alespoň jejich předchozího upozornění o odposlouchávání, a to ani v přípa-

dě, že zprávy v těchto hovorech podávané se týkají jeho zájmů. Je technicky možné získat prokazatelně souhlas s odposlechem telefonických hovorů od zaměstnanců, ale je prakticky vyloučeno získat takovýto souhlas od třetích osoby, stejně tak, jako se vyhnout tomu, aby třetí osoby na odposlouchávanou linku zavolaly. [3]

4.3 Právní normy upravující používání odposlechu

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

Ustanovení § 18, odst. 4 tohoto zákona 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 nepoužít. [3]

- Zákon č. 13/1993 Sb., Celní zákon

Ustanovení § 37d tohoto zákona 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 TrZ), porušování předpisů o nakládání s kontrolovaným zbožím (§ 124a - 124c TrZ), zkrácení daně, poplatku a podobné dávky (§ 148 TrZ) anebo že se připravuje spáchání takového trestného činu. Operativní techniku lze používat jen v případech, kdy odhalování takovýchto trestných činů je jiným způsobem neúčinné anebo podstatně ztížené, a to pouze na dobu nezbytně nutnou, na povolení soudce místěn příslušného krajského soudu. Použití odposlechu zajišťuje Policie ČR. [3]

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

Ustanovení § 10 umožňuje použití zpravodajských prostředků na předchozí povolení soudce místně příslušného vrchní soudu. [3]

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

Ustanovení § 36 tohoto zákona umožňuje využívat operativní techniku orgánům policie, a to pouze tehdy, kdy odhalování zvláště závažných trestných činů (tj. trestných činů uvedených v § 62 TrZ a nebo trestných činů, na něž je stanovena hord¨ní hranice trestní sazby

nejméně osm let) je jiným způsobem neúčinné anebo podstatně ztížené, na dobu nezbytně nutnou, na povolení soudce místěn příslušného krajského soudu. [3]

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

Ustanovení § 88 tohoto zákona umožňuje předsedovi senátu příslušného soudu nařídit odposlech a záznam telekomunikačního provozu, pokud lze důvodně předpokládat, že jím budou sděleny významné skutečnosti pro trestní řízení o zvláště závažném trestném činu. Provádění odposlechu a záznamu telekomunikačního provozu mezi obhájcem a obviněným je nepřípustné. Zjistí-li policejní orgán při odposlechu a záznamu telekomunikačního provozu, že obviněný komunikuje se svým obhájcem, je povinen odposlech ihned přerušit, záznam o jeho obsahu zničit a informace, které se v této souvislosti dozvěděl, nesmí nepoužít. Bez příkazu může orgán činný v trestním řízení nařídit odposlech a záznam telekomunikačního provozu, nebo jej provést i sám, a to i tehdy, je-li vedeno trestní řízení pro trestný čin, který není zvláště závažným trestným činem, pokud s tím účastník odposlouchávané stanice souhlasí. [3]

4.4 Právní normy přikazující provádět ochranu proti odposlechu

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

§ 26 projednávání utajovaných informací

Odpovědná osoba je povinna zajistit, aby v jednací oblasti (ohraničený prostor v objektu, kde lze pravidelně projednávat utajované informace stupně tajné a přísně tajné) nedocházelo k ohrožení nebo úniku projednávaných informací. Osoba je povinna požádat Úřad o provedení kontroly, zda v jednací místnosti nedochází k nedovolenému použití technických prostředků určených k získávání informací. Tuto kontrolu Úřad zajistí v součinnosti se zpravodajskými službami a Policií České republiky. [3]

§30 Technickými prostředky jsou zejména:

- mechanické zábranné prostředky

- elektrická zámková zařízení a systémy kontroly vstupů

- zařízení elektrické zabezpečovací signalizace

- speciální televizní systémy

- tísňové systémy

- zařízení elektrické požární signalizace

- zařízení sloužící k vyhledávání nebezpečných lýtek nebo předmětů

- zařízení fyzického ničení nosičů informací

- zařízení proti pasivnímu a aktivnímu odposlechu utajované informace [11]

4.5 Postup policejního orgánu při vyžadování odposlechu a záznamu telekomunikačního provozu dle §88/1, 3 tr. ř.

Policejní orgán může navrhnout státnímu zástupci odposlech a záznam telekomunikačního provozu pouze v případě, že je vedeno trestní řízení pro zvlášť závažný úmyslný trestný čin nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje mezinárodní smlouva, pokud lze důvodně předpokládat, že jím budou zjištěny významné skutečnosti pro trestní řízení.

Návrh má písemnou podobu a je v něm obsaženo stručné zhodnocení skutkového stavu trestní věci a odůvodnění provedení odposlechu. Spolu s podnětem k podání návrhu předkládá policejní orgán státnímu zástupci i spisový materiál, ze kterého musí být zřejmé splnění výše uvedených podmínek stanovených trestním řádem, zejména zjištění jakých skutečností významných pro trestní řízení je očekáváno. Samozřejmostí návrhu jsou údaje nezbytné k identifikaci účastnické stanice a doba, po kterou má být odposlech a záznam prováděn.

Vzhledem k faktu, že v souvislosti s odposlechem a záznamem telekomunikačního provozu dochází k zásahu do základních práv a svobod občanů, je orgán činný v trestním řízení povinen uplatňovat zásadu zdrženlivosti a přiměřenosti (§ 2/4 tr. ř.) spočívající v tom, že má být použito takové opatření, které nejlépe povede k dosažení účelu trestního řízení, ale zároveň nebude nepřiměřeně zasahovat do základních práv a svobod osoby, vůči níž je uplatňováno, a bude šetřeno její osobnosti v mezích daných povahou příslušného omezení.

Odposlech a záznam telekomunikačního provozu může nařídit i sám policejní orgán, a to i v trestním řízení pro trestný čin výše neuvedený, avšak vždy jen se souhlasem účastníka stanice, která má být odposlouchávána. V tomto případě nařizuje odposlech vlastním písemným příkazem, který vydá jen na základě spolehlivě zjištěného skutkového stavu, a odůvodňuje

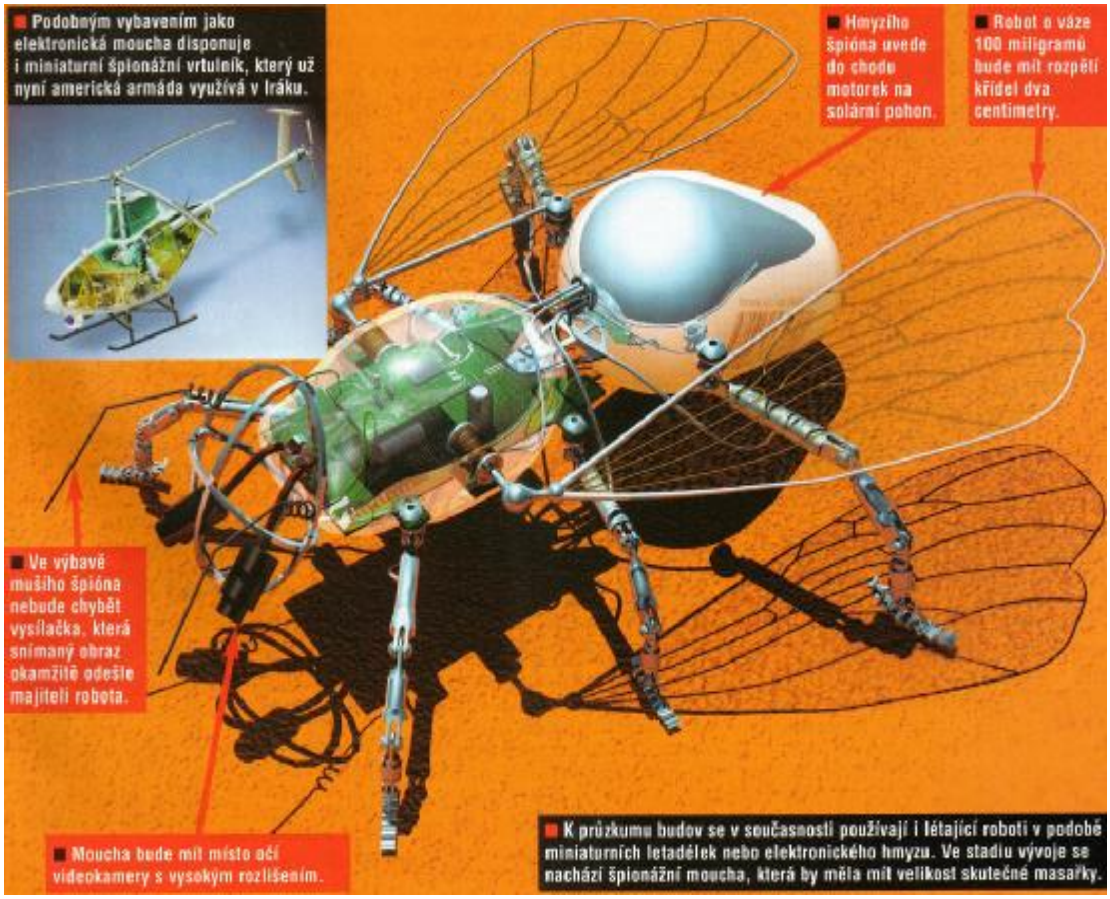
jej obdobně jako návrh na vydání rozhodnutí o odposlechu státnímu zástupci. Před vydáním příkazu policejní orgán musí zajistit písemný souhlas účastníka odposlouchávané stanice.

Příkaz soudce nebo vlastní příkaz spolu se souhlasem účastníka předává policejní orgán s žádostí o provedení příslušnému specializovanému pracovišti (Policii České republiky, Útvaru zvláštních činností služby kriminální policie a vyšetřování – dále jen ÚZČ).

Policejní orgán je povinen bezodkladně vyhodnocovat záznamy o provedeném odposlechu. Pokud má být některý záznam použit v trestním řízení jako důkaz, je třeba k němu připojit protokol, který zpracovává specializovaný útvar – ÚZČ, s uvedením údajů o místě, času, způsobu a obsahu provedeného záznamu a také o osobě, která záznam pořídila (nebo s údajem, že záznam byl pořízen automaticky bez účasti konkrétní osoby). Ostatní záznamy jsou označeny a spolehlivě uchovány, v protokolu musí být poznamenáno, kde jsou uloženy. Pokud při odposlechu nejsou zjištěny skutečnosti významné pro trestní řízení, má policejní orgán povinnost záznamy zničit předepsaným způsobem, a to tak, aby byla znemožněna rekonstrukce a identifikace skutečností, které záznam obsahoval (o zničení se provede záznam do spisového materiálu). [7]

ZÁVĚR

Speciální technika se stále vyvíjí a je stále rafinovanější. Vědci přišli na způsob, jak ukrýt zprávy mezi molekuly DNA. Dalším špionážním zařízením jsou satelity. Moderní satelit umí díky infračerveným paprskům zjistit teplotní rozdíly s přesností na desetiny stupě. Může tedy odhadnout, kde před hodinou tábořil vojenský tábor, nebo zda mají monitorované automobily nastartovaný motor. Dálkově ovládaná vážka o velikosti lidské dlaně se výborně hodí pro prozkoumání konkrétních objektů. Bez povšimnutí zkontroluje patra budov a jednotlivé místnosti. Přitom svému pánovi okamžitě odvysílá kvalitní obraz. Robot o váze 100 miligramů má rozpětí křídel 2 cm a do letu jej uvádí motorek na solární pohon. Obrovské možnosti pro špiony z celého světa dnes nabízí internet. Již dnes se hackeři a počítačový piráti nabourávají do počítačových síti firem zpracovávajících vojenské zakázky.



Obr. 45 Elektronická vážka

Drobná odposlouchávací zařízení dnes nejsou drahá, jsou miniaturní a nevyžadují být v blízkosti zařízení. Řada z nich má zabudovaný vysílač a dokáže hovor přenášet na vzdálenost až několika kilometrů. Nejmenší z nich se vlezou do propisky nebo na kreditní kartu. Největší hrozbou dnešní špionáže jsou mobilní telefony. Stačí, abyste mobilní telefon nastavený tak, aby bez vyzvánění automaticky přijal hovor, zapomněli v kapse u saka, v kanceláři, a odejdete třeba na toaletu. Pak už jen stač vytočit číslo z jiného mobilního telefonu a můžete v klidu poslouchat, co si o vás povídají za vašimi zády. Mobilní telefon také slouží jako dobrý prostředek pro lokalizaci hledané osoby.

Z mé práce je tedy patrné, že odposlech a získávání důležitých informací není žádný velký technický problém. Vzhledem k jeho malé finanční náročnosti v porovnání s cenou zcizených informací se stává i u nás velice účinným nástrojem konkurenčního boje. Každá firma by se tedy měla vážně začít zabývat možností ochrany důvěrných informací, protože investice do této ochrany mohou být jen zlomkem ceny odcizené informace.

ZÁVĚR V ANGLIČTINĚ

Special technics are developing and they are more crafty. Scientists developed, how to hide a messages among molecules DNA. Next spy device are satellites. Modern satellite can ascertain thermal differences with accuracy of decimals …desetiny stupně... with infrared beam. Satellite can judge, where the army camped an hour ago or if cars have a running motor. Remote controlled electronic dragonfly (size of human palm) can explore concrete object. Dragonfly control storeys and rooms. It's master gets a quality screen at the same time. Robot with a weight of 100 miligrams has a span of wings about 2 centimeters and energy from solar panels. Internet offers great potentialities for spy from all over the world. Nowadays, hackers and computer pirates attack computer nets of companies working with military order.

In these days, little tapping devices are not expensive, they are miniaturized and don`t demand near distance. They have transmitter and they can transfer voice to long distance. The smaller of them are in pens or in credit cards. The greatest menace of present spying is cellular phone. You just may have your cellular phone set, that it will automaticly and without ringing accept a call. Then you will forget it in the pocket of yout coat in the office and you will go to the toilet room. And then you just dial the number from other telephone and you can listen, what is told behind your back. Cellular phone is a great device to localization of wanted person.

So, from my work is evident, that tapping and getting important information is not big technical problem. Considering it's small financial costingness compared with a price of a stolen informations, it becomes (also in our country) very effectual instrument of the competitors fight. Therefore, each company should begin with the possibility of protection of the classified informations, because the investment to this protection may be just a fragment of the price of the stolen information.

SEZNAM POUŽITÉ LITERATURY

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

[2] Vnitropodniková literatura – SafeCom spol.s.r.o., *Jak se stát špionem snadno a rychle aneb jak se bránit odposlechu.* [online], Ing. Hofman, J.

Dostupný z WWW: <http://www.safecom.cz/>

[3] Vnitropodniková literatura – Probin s.r.o.., *Ochrana proti odposlechu, šifrované telefony, odposlechová zařízeni.* [online]. Ing. Schmidt, J.

Dostupný z WWW: <http://www.probin.cz/>

[4] JUDr. Brabec, F., *Bezpečnost pro firmu, úřad, občana.* Praha: Nakladatelství Public History, 2001, 400str., ISBN 80-86445-04-06

[5] JUDr. Brabec, F., *Ochrana bezpečnosti podniku.* Brandýs nad Labem: ČTK REPRO, 1996, 203str., ISBN 80-85858-29-0

[6] SPY VPH, *Speciální technika a služby,* [online], [cit. 2006-11-02].

Dostupný z WWW: <http://spy.vph.cz/>

[7] MVČR, *Analýza úkonů dle § 88/1,3 tr. ř. odposlech a záznam telekomunikačního provozu a § 158d/3,6 tr. ř. sledování osob a věcí.* [online], [cit. 2007-05-15].

Dostupný z WWW: <http://www.mvcr.cz/2003/aktualit/2005/odposlechy_zprava_info.html>

[8] Česká komora detektivních služeb, [online], [cit. 2006-12-02].

Dostupný z WWW: <http://www.ckds.cz/>

[9] *Specialista – military portal,* [online], [cit. 2006-11-20].

Dostupný z WWW: <http://www.specialista.info/>

[10] *Listina základních práv a svobod*

[11] *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti*

[12] *Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti*

[13] *Zákon č. 169/1999 Sb., o výkonu trestu odnětí svobody*

[14] *Zákon č. 13/1993 Sb., Celní zákon*

[15] *Zákon č. 154/1994 Sb., o Bezpečnostní informační službě*

[16] *Zákon č. 283/1991 Sb., o Policii České republiky*

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

[18] *§ 88 trestního řádu*

[19] *Časopis Epocha*. Vydává RF Hobby, s. r. o. rok 2006, číslo 12, 1x14dnů

[20] ELBI Electronics, *Výrobce přístrojů proti odposlechu.* [online], [cit. 2007-03-02]. Dostupný z WWW: < http://www.elbi.cz>

[21] Security Systems Odposlechy.com, *Elektronické systémy.* [online], [cit. 2007-03-02]. Dostupný z WWW: < http://www.odposlechy.com/>

[22] MRP-Informatics, spol. s r.o., *Video systém na monitorování a střežení objekt.* [online], [cit. 2007-03-09]. Dostupný z WWW: <http://www.mrp.cz/>

[23] ESCAD Trade s.r.o**.,** *Bezpečnostní kamery, kamerové systémy, CCTV.* [online], [cit. 2007-04-08]. Dostupný z WWW: <http://www.kamerove-systemy-cctv.cz/>

[24] 21. století, *Nesnesitelná lehkost špionáž,* [online], [cit. 2006-11-02] Dostupný z WWW: <http://www.21stoleti.cz/>

[25] Portal-x.cz, *Špionážní technika*. [online], [cit. 2006-11-17] Dostupný z WWW: < http://www.portal-x.cz/odposlechy/aktuality>

[26] *Poznámky ze studia předmětu Speciální bezpečnostní technologie*

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

[28] JUDr. Lacký, V., *Řízení technologických procesů v průmyslu komerční bezoečnosti.* Zlín: Univerzita Tomáše Bati, 2005, 101str., ISBN 80-7318-329-3

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

OTP	Obranně technická prohlídka
GSM	Global System for Mobile Communications
UMTS	Universal Mobile Telecommunications Systém
NMT	Nordic Mobile Telephone
EZS	Elektrická zabezpečovací signalizace
EPS	Elektrická požární signalizace
PC	Personal computer
AVC	Automatická regulace citlivosti mikrofonu
UHF	Ultra High Frequencies
PIR	Passive infra red

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

Příloha PI: Kalkulace obranně technické prohlídky – Probin s.r.o.

výměra podlahové plochy: 25metrů čtverečních

vzdálenost v km od Prahy: 20km

práce mimo pracovní dobu: ne

výška stropu: <3m (2,5m)

Datum zadání: 23.5.2007

Ceny služeb:

BEZPEČNÁ KANCELÁŘ opakované prohlídky:

Následující cyklus se opakuje každý rok ve stejném složení čímž je zajištěna maximální míra prevence a bezpečnosti.

První prohlídka			
Obsah:	Fyzická prohlídka, rádiová prohlídka, kontrola nelinearit		
Měsíc provedení:	květen	Cena:	10455 Kč

Druhá prohlídka			
Obsah:	Fyzická prohlídka, rádiová prohlídka		
Měsíc provedení:	srpen	Cena:	10455 Kč

Třetí prohlídka			
Obsah:	Fyzická prohlídka, rádiová prohlídka		
Měsíc provedení:	listopad	Cena:	10455 Kč

Čtvrtá prohlídka			
Obsah:	Fyzická prohlídka, rádiová prohlídka		
Měsíc provedení:	únor	Cena:	10455 Kč

KOMPLETNÍ PROHLÍDKA PROTI ODPOSLECHU jednorázová:

Obsah	Cena [Kč]
Fyzická prohlídka, Rádiová prohlídka, Kontrola nelinearit	23500
Příplatky	0
Dopravné	320
Cena prohlídky celkem	23820

ZÁKLADNÍ PROHLÍDKA PROTI ODPOSLECHU jednorázová:

Obsah	Cena [Kč]
Fyzická prohlídka, Rádiová prohlídka	14100
Příplatky	0
Dopravné	320
Cena prohlídky celkem	14420

DOPRAVNÉ

a) Dopravné není účtováno v případě Kompletní prohlídky proti odposlechu jednorázové, pokud se jedná o prohlídku o rozloze podlahové plochy nad 40m^2. V takovém případě je dopravné po celém území ČR zdarma
b) V ostatních případech je účtováno dopravné vždy ve výši 8,- Kč / 1 km bez DPH.

PŘÍPLATKY

Za práci mimo dobu 8.00-20.00 a za práci v sobotu, neděli a o svátcích je účtován příplatek ve výši 10%. Při výšce stropů nad 3 metry a při ztížených podmínkách je cena násobena koeficientem 1,1-1,4. Ceny mohou být také upraveny v závislosti na termínu realizace zakázky.

Příloha II: Kalkulace obranně technické prohlídky – SafeCom spol. s r.o.

výměra podlahové plochy: 25metrů čtverečních
vzdálenost v km od Prahy: 20km
práce mimo pracovní dobu: ne
výška stropu: <3m (2,5m)
Datum zadání: 23.5.2007

Kontrola RF spektra:

Místnost	Velikost [m^3]	Základní sazba 1[m^3]	Cena za m^3	Cena celkem
1	62.5	6000 Kč	60 Kč	9 750,00 Kč
Cena celkem:				9 750,00Kč

Kontrola nelineárních přechodů:

Místnost	Velikost [m^3]	Základní sazba 1[m^3]	Cena za m^3	Cena celkem
1	62.5	5000 Kč	90 Kč	10 625,00 Kč
Cena celkem:				10 625,00 Kč

Celková cena kalkulace: 20 375,00

Za další vedení (EPS, alarm, el. zámek atd) se účtuje 500,-Kč, za fyzickou prohlídku elektronických přístrojů (fax, kopírka,TV atd.) se účtuje také 500,-Kč.

Příloha PIII: Ceník bezpečnostních produktů - PROBIN s.r.o.

1.2.2006

Ochrana proti odposlechu

Obranně technické prostředky

Název	Popis produktu	*Cena v Kč
A-3 AD	Síťový adaptér 12V/0,3A, pro MRA - 3	349,-
SNG	Inteligentní šumový generátor	12 925,-
SNG AD	Síťový adaptér 12V/ 500 mA pro SNG	349,-
AP	Akustický piezoměnič	28,-
P30	Plastová krytka P30	8,-
OMS-2000	Soustava reproduktorů pro mobilní použití šumového generátoru	2 500,-
RVD	Osobní detektor VF pole s vibrátorem	18 200,-
TRN 2000	Elektrodynamický měnič	3 520,-
MD 200	Montážní deska elektromagnetického měniče	198,-
SafeLink	Ochrana proti odposlechu v telefonní lince	2 475,-
SH	sluchátka HAMA	275,-
MRA-3 v4.1	Paměťový radiový analyzátor	26 675,-

Prostředky na vyhledávání odposlechu

Název	Popis produktu	*Cena v Kč
NR-900-E	Detektor nelineárních přechodů, 2. a 3. harmonická	650 000,-
NR-M	Detektor nelineárních přechodů, 2. a 3. harmonická	595 000,-
Broom ECM	Detektor nelineárních přechodů	525 000,-
Super Broom ECM	Detektor nelineárních přechodů	798 000,-
Super Broom Plus	Detektor nelineárních přechodů	966 000,-
IPF-6	Přístroj pro operativní vyhledávání radiových vysílačů	55 700,-
TPU-5K	Zařízení pro kontrolu telefonních linek	58 000,-
RFDS-3	Detekční a vyhledávací souprava s LTA	35 953,-
RFD-2	Vyhledávací a sledovací přijímač	19 938,-
LTA	Linkový adaptér	2 750,-
PSC-5	Univerzální souprava pro vyhledávaní vysílačů pracujících v elektrických a telefonních rozvodech, s infračerveným přenosem akustické informace a stetoskopických mikrofonů	117 000,-
VIZIR	Zařízení pro kontrolu telefonních a síťových rozvodů	54 000,-

Speciální obranné prostředky

Název	Popis produktu	*Cena v Kč
SAGEM MW3026S	GSM telefon s kryptováním komunikace, dualband	85 000,-
SAGEM MW3026S-MR	GSM telefon s kryptovanou komunikací, modem na propojení s pevnou telefonní linkou nebo satelitním telefonem	121 000,-
SAGEM myX-8S	GSM telefon s kryptováním komunikace, triband	99 000,-
SAGEM AMADEUS	Software pro vytváření klíče	2 654 000,-
SAGEM obnova	Obnova klíče	5 000,-
SAGEM C500	Kryptovací jednotka pro pevnou telefonní linku (PSTN, ISDN nebo digitální), 1. a 2. kus	121 000,-
SAGEM C500	Kryptovací jednotka pro pevnou telefonní linku (PSTN, ISDN nebo digitální), každý další kus 113 000,-	
UAZI	Jammer	129 000,-
Voice Changer	Telefonní měnič hlasu (možná úprava na mikrofon x reproduktor)	22 000,-

Speciální technické prostředky

Vysílače

Název	Popis produktu	*Cena v Kč
RM-M3	Miniaturní radiomikrofon, 1-50mW	9 500,-
RM-M5	Miniaturní radiomikrofon, 7-20mW	9 500,-
RM-S2	Síťově napájený radiomikrofon, 5mW	15 200,-
RM-ST	Radiomikrofon se stetoskopem, 50mW	26 200,-
RM-Pero	Radiomikrofon v peru	26 200,-
PT-P	Telefonní vysílač napájený z telefonního rozvodu	9 500,-
KPL-S	Souprava vysílače napájeného ze síťového rozvodu a přijímače. Informace je předávána po síťovém rozvodu	40 000,-
KPL-SV	vysílač pro KPL-S, až 3 vysílače na 1 přijímač	20 000,-
KPL-T	Souprava vysílače napájeného z telefonní sítě a přijímače. Informace je předávána po telefonním rozvodu	40 000,-
KPL-TV	vysílač pro KPL-T, až 3 vysílače na 1 přijímač	20 000,-
ND-M-D	Radiomikrofon s digitálním kódováním a dálkovým ovládáním	44 000,-
ND-N5-D	Radiomikrofon se zvýšeným výkonem (až 500 mW), s digitálním kódováním a dálkovým ovládáním	51 000,-
ND-N2	Radiomikrofon s digitálním kódováním, určen pro nošení na těle	39 500,-
ND-T	Radiomikrofon s digitálním kódováním pro monitoring telefonní linky	28 400,-
ND-M2	Radiomikrofon s digitálním kódováním a dálkovým ovládáním	44 000,-
ND-V	Vysílač dálkového ovládání	17 400,-
ND-P	Přijímač dálkového ovládání	9 400,-
RM-N3	Radiový vysílač pro použití na těle, frekvence 417-419 MHz, výkon 250 mW, 8 hodin provozu	21 200,-

Přijímače

Název	Popis produktu	*Cena v Kč
UNIVERSAL	Přijímač pracující na frekvenci 417-419 MHz s demodulací	35 200,-
UNI-M3	Modul pro přijímač UNIVERSAL se záznamem po dobu 3 hodin	7 320,-
UNI-M6	Modul pro přijímač UNIVERSAL se záznamem po dobu 6 hodin	13 725,-
UNI-M9	Modul pro přijímač UNIVERSAL se záznamem po dobu 9 hodin	18 300,-
UNI-ANT	Automobilová anténa pro UNIVERSAL	3 200,-
UNI-AD	Adaptér 220 V pro UNIVERSAL	915,-
UNI-CAD	Automobilový adaptér pro UNIVERSAL	1 373,-

Mikrofony

Název	Popis produktu	*Cena v Kč
USAI	miniaturní mikrofon se zesilovačem, kabel až 2 km	5 000,-
TM-2	telefonní snímač	7 320,-

Rádiový přenos video signálu

Název	Popis produktu	*Cena v Kč
VF-A700	bezdrátový A/V přenos, výkon 700 mW, stereo zvuk	38 600,-
AN-2.5	Směrová anténa	11 300,-
AK-2.5	Anténa s kruhovou charakteristikou	8 200,-
AM-2.5	Automobilová anténa s magnetickou základnou	9 800,-
ATV-2.5S	Směrová anténa, pro nošení na těle	11 300,-
RTA	Přijímač pro bezdrátové A/V vysílače	24 900,-
battery pack		5 000,-

Digitální video záznam

Název	Popis produktu	*Cena v Kč

VRDR-4	Autonomní digitální jednotka pro záznam ze 4 CCD kamer, 4 alarmové vstupy, HDD 24 GB, záznam až 2 160 hod., konfigurace a práce se záznamem přes PC	61 000,-
GV-D800E	digitální videowalkman s barevným LCD displejem	37 000,-
GV-D200E	digitální videowalkman bez displeje	27 000,-
DC-V700	automobilový adaptér pro GV-D	5 600,-
NP-F950	baterie pro GV-D, až 5 hodin provozu	4 900,-
NP-F750	baterie pro GV-D, až 3 hodiny provozu	3 300,-
NP-F550	baterie pro GV-D, až 1,5 hodiny provozu	1 800,-

*Všechny uvedené ceny neobsahují DPH 19%
PROBIN s.r.o. si vyhrazuje právo změnit ceny bez předchozího upozornění.