Odhalování skrytých odposlechových prostředků pro hlasovou komunikaci

Detection of hidden tapping devices for voice communication

Bc. Marián Sehnálek

Diplomová práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2008/2009

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Marián SEHNÁLEK**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Odhalování skrytých odposlechových prostředků pro hlasovou komunikaci**

Zásady pro vypracování:

1. **Popište technické řešení používaných prostředků pro hlasový odposlech.**
2. **Podrobně rozeberte právní otázky týkající se odposlechu hlasové komunikace**
3. **Navrhněte ucelený postup jakým provádět radiotechnickou prohlídku objektu pomocí dostupné techniky proti odposlechu (přehledový přijímač, detektor pole, vyhledávání pomocí směrových antén).**
4. **Proveďte měření šíření signálů v pásmu VHF a UHF po budově pro nejběžnější situace, které v praxi nastávají. Pro vybrané situace vytvořte jednoduchý analytický nebo numerický model, kterým bude možné předpovědět úroveň signálu produkovaného radiomikrofony.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Radiomonitoring and Radiolocation – Katalog 2007/08. Munich. Rohde-Schwarz. pg. 60-83. 2007.**
2. **KOIEN, G.N.: An introduction to access security in UMTS. Wireless communications. 11 (1):8--18, Feb 2004.**
3. **Přehledový přijímač MRA-3. Uživatelský manuál. Elbi Praha. Dostupné z www.elbi.cz.**
4. **Problematika odposlechů všeobecně. Security magazín. Vydává FAMily media,spol.s.r.o. listopad – prosinec 2002. roč.9. ISSN 1210-8723.**
5. **BRABEC, F.: Ochrana bezpečnosti podniku. Brandýs nad Labem. ČTK REPRO. 1996. 203str. ISBN 80-85858-29-0.**

Vedoucí diplomové práce: **Ing. Stanislav Goňa, Ph.D.**
Ústav elektrotechniky a měření

Datum zadání diplomové práce: **20. února 2009**

Termín odevzdání diplomové práce: **22. května 2009**

Ve Zlíně dne 20. února 2009

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

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Moje diplomová práce popisuje a seznamuje s odposlechovou a špionážní technikou používanou k zachycení hlasové komunikace. Kromě odposlechového vybavení jsou zmíněna i zařízení pro detekci špionáže.

Další část práce popisuje zásady provádění obranně technické prohlídky. V samostatné části se práce stručně věnuje šíření elektromagnetických vln v UHF pásmu v budovách, která je doplněna o měření útlumu cihlové zdi.

Klíčová slova: Konkurenční zpravodajství, odposlechový prostředek, ochrana proti odposlechu, elektromagnetické vlny, obranně technická prohlídka

ABSTRACT

The thesis describes and introduces tapping and spying equipment which is being used for gathering of voice information. Besides of spying equipment the technical equipment for detection of spying are mentioned.

Another part of the thesis describes fundamentals of the defense technical inspection.

In the separate chapter, propagation of EM waves in UHF band in buildings is briefly described. This chapter is supplemented with measurements of an insertion loss of the brick wall.

Keywords: competitive inteligence, eavesdropping device, defence against tapping, electromagnetic waves, defense technical inspection

Úvodem bych chtěl poděkovat vedoucímu mé diplomové práce panu Ing. Stanislavu Goňovi, Ph.D. za cenné rady a připomínky při tvorbě mé práce.

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

Prohlašuji, že jsem na diplomové 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 …….

Podpis diplomanta

OBSAH

ÚVOD

V dnešní době si velmi málo firem uvědomuje, že by se jich mohl týkat určitý, těžko dokazatelný a nebezpečný druh kriminální činnosti. Jedná se o krádeže informací, jako je například firemní know-how, databáze firemní klientely a podobně. Začínají se objevovat případy odposlechů důležitých porad, telefonních hovorů, faxových zpráv nebo datových přenosů. Rozvoj těchto technologií je velmi rychlý, odposlechové prostředky jsou stále levnější a dostupnější, proto by firmy měly vzít na vědomí, že tahle činnost je velmi nebezpečná a je potřeba se proti ní chránit.

Prostřednictvím této práce bych chtěl upozornit na tuto problematiku. Na začátku se práce zabývá s problematikou konkurenčního zpravodajství a možných způsobech úniku informací. Dále práce poskytuje přehled o prostředcích pro hlasový odposlech a dále o prostředcích na účinnou obranu proti nim, je také popsána obranně technická prohlídka prostředky pro radiovou analýzu. Byla provedena měření, podle kterých můžeme předpovědět úroveň signálu radiomikrofonu v budově. Poslední kapitola rozebírá právní aspekty používání odposlechu v České republice.

1 HLASOVÝ ODPOSLECH

1.1 Speciální bezpečnostní prostředky

Pod pojmem speciální bezpečnostní prostředky v soukromých bezpečnostních službách rozumíme zejména komerčně využitelná technická zařízení sloužící ke zjišťování informací ze zájmového prostoru nebo techniku, která slouží z hlediska zákona k získávání informací v boji kriminalitě, nebo také techniku, která byla k tomuto účelu instalována nezákonně. Odposlechovým prostředkem rozumíme různé technologie k tichému získávání informací ze zájmového prostoru, které mohou mít různou podobu, a to mluvené slovo, obraz, data.

Ve státní správě se odposlechové prostředky používají zejména proto, že jsou schopny zajistit důkazy o trestné činnosti. Využívají toho, že pachatelé se cítí bezpečně a komunikují spolu naprosto otevřeně. Dále se používají za účelem špionáže, kdy mohou zajistit důvěrné informace z různých oblastí, například v domácí a zahraniční ekonomice, ale také v oblasti terorismu.

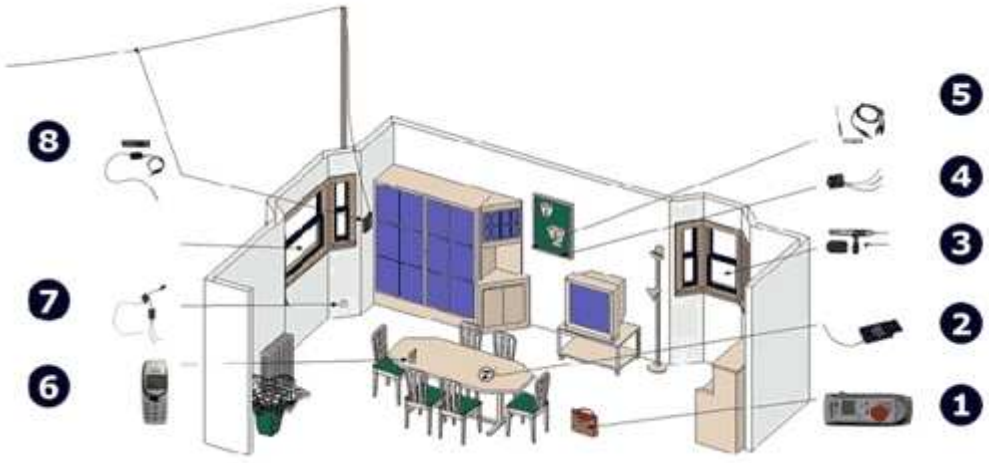
V komerčním sektoru se odposlechové prostředky používají zejména k zjišťování důkazů o vnitropodnikové kriminalitě, kdy je použití běžných bezpečnostních technologií neúčinné. Dále se používají v konkurenčním boji za účelem zajištění konkurenční výhody. Pak také jako preventivní prostředek pro zjištění chování obchodních zástupců a manažerů a podobně

1.2 Způsoby úniku informací

Nečastěji mohou informace unikat velmi jednoduchou a těžko zjistitelnou formou, kterou je vyzrazení některými zaměstnanci firmy, kteří šíří informace buď z neopatrnosti nebo za finanční odměnu od konkurenční firmy. Jiný způsob získávání informací, technicky složitější, je odposlech prostor firmy, například různé zasedací místnosti, ve kterým probíhají porady, kanceláře ředitelů a jeho asistentů a jiných osob z vedení společnosti, ale také kanceláře obchodníků, kteří komunikují se zákazníky a další různá pracoviště, kde se pracuje s informacemi, které by měly zůstat pouze uvnitř podniku. Pro takovýto způsob odposlechu slouží radiové mikrofony, které se umisťují do zájmové místnosti nebo do její blízkosti. Radiové mikrofony snímají hlasy ze zájmového prostoru a jeho okolí a ty pak

přenáší pomocí elektromagnetických vln na místa příjmu, umístěná v různých vzdálenostech od odposlouchávaného prostoru. Jako přenosové medium může sloužit i jakékoliv vedení v budově, například elektrická instalace, rozvody pro EZS a EPS, telefonní linka, elektrický vrátný a podobně. Tyto mikrofony jsou většinou napájeny z baterií, ale mohou být připojeny i k trvalému zdroji elektrické energie, například telefonní linka nebo EZS. U nás není problém tyto mikrofony koupit, na internetu je spousta firem, které nabízí tyto produkty a velmi dostupné ceny. Dalším způsobem získávání důležitých informací je odposlech telefonní linky, po níž probíhá spousta důležitých hovorů formou mluveného slova, faxových zpráv nebo datovým přenosů bez jakékoliv ochrany. Dnes ovšem používání klasické pevné linky opadá, ve velké míře se používají mobilní telefony. Odposlech mobilní telefonů v radiotelefonní síti NMT450 pracující na frekvenci 450-485MHz byl velmi snadný, což je jeden z důvodů, proč se tato síť u nás již nepoužívá. Dnes je velmi rozšířený standard GSM pracující na frekvencích 900 a 1800MHz, u něhož se odposlech velmi složitý a nákladný ale reálný. V dnešní době se u nás začíná používat i standard UMTS. Mobilní telefon s sebou nenese jen informace o kontaktech, hovorech a SMS zprávách, ale také o pohybu uživatele, tedy o poloze telefonu. Proti všem druhům odposlechu je možné se určitým způsobem bránit.

1.2.1 Místa instalací odposlechové techniky



Obr. 1 Místa instalací odposlechové techniky [3]

1. Diktafon (s odposlechem)

2. Miniaturní rádiomikrofon (dálkový odposlech)

3. Laserový odposlech

4. Miniaturní sledovací kamera (s odposlechem)

5. Miniaturní mikrofon (s nahráváním odposlechu)

6. Speciálně upravený mobilní telefon doplněný odposlechem

7. Rádiomikrofon 220V (dosah odposlechu 5km)

8. Rádiomikrofon na telefonní lince (dosah odposlechu do 50m) [3]

1.3 Způsoby ochrany informací

Osoba, která se snaží získat informace, často investovala nemalé částky do odposlechového zařízení, je velmi vynalézavá a používá často velmi sofistikované metody a prostředky, proto je téměř nemožné odhalení odposlouchávacího zařízení zaměstnanci firmy, kteří nemají technické vybavení a znalosti. Na tuhle činnosti se specializují některé profesionální firmy, které nabízejí různé služby, jako jsou vyhledávání odposlechových prostředků nebo zpracování komplexního projektu na ochranu informací firmy ve formě organizačních a technických opatření. Jde o rozbor pohybu zaměstnanců a jejich styku s důvěrnými informacemi, rozbor pracovního režimu firmy a podobně, jehož závěrem jsou organizační a opatření zabraňující úniku informací vlastními zaměstnanci a technická opatření, která svou instalací a uvedením do provozu detekuje odposlechové zařízení nebo znemožní jeho funkci. Pro zjištění radiových mikrofonu se používají různé širokopásmové spektrální analyzátory nebo přijímače se signalizací silného vysílače. Jsou ovšem pouze orientační, nedokážou skrytý vysílač zachytit na větší vzdálenosti. K zjišťování mikrofonů vysílajících na kabelovém vedení slouží různé druhy telefonních analyzátorů a přístrojů na kontrolu kabelových vedení. Problematické může být zjišťování přítomnosti mikrofonů zapínaných na dálku, kdy jejich funkce může být během měření vypnuta. Pak přichází na řadu detektor nelineárních přechodů, který dokáže odhalit skryté polovodičové součástky. Tento detektor vysílá pomocí antény harmonické kmitočty, které se od polovodičových součástek odráží a ty pak detektor porovnává. Uvedené zařízení vyžaduje nemalé investiční náklady do technického vybavení a také bohaté zkušenosti osoby vyhledávající skryté zařízení. Proto různé společnosti nabízejí profesionální služby, ve kterých kontrolují radiová spektra a zájmových prostorech, kontrola vedení a podobně. Závěrem takové služby je osvědčení o jejím výsledku, zda byl nebo nebyl nalezený odposlechový

prostředek a případné naložení s ním. Tyto kontroly je potřeba provádět pravidelně, zejména před důležitými poradami. Dalším prostředkem, jak vyrušit funkci odposlechových mikrofonů, je umístění šumového generátoru v zájmovém prostoru. Ten generuje šum, který zahltí mikrofony tak, že není možné zachytit hlasovou komunikaci. Odposlouchávání telefonních linek je hůře odhalitelné, takže je optimální přenášet data po této lince v šifrované podobě. K tomuto účelu slouží různé scramblery a složité šifrátory. Scramblery pracují tak, že rozdělí mluvené slovo do určitých frekvenčních pásem a vzájemně je přehází tak, že během přenosu je hovor nesrozumitelný. K přeměně do srozumitelné podoby dochází u přijímače, který je vybaven stejným scramblerem nastaveným na stejný číselný kód jako u vysílacího scrambleru. Šifrátory jsou složitější ale také bezpečnější zařízení, které šifrují přenosy hlasové komunikace, faxových zpráv a počítačových dat. Používají se pouze v páru, kdy na vysílacím i přijímacím zařízení je nastavena stejná šifra.

Cena odposlechových prostředků je v porovnání s cenou zcizených informací velmi malá, proto se odposlech stává účinným nástrojem konkurenčního boje. Také díky nízké ceně není jejich pořízení a použití žádný velký problém, proto by každá firma měla začít zabývat možnostmi ochrany proti konkurenčnímu boji a konkurenčnímu zpravodajství a ochrany svých důvěrných informací, neboť investice vložené do zařízení na ochranu informací může být minimální s porovnáním ceny ztracené informace.

1.4 Konkurenční zpravodajství

Zpravodajství bylo po dlouhou dobu používáno zejména u státních tajných služeb, ale v současnosti se stává hlavní aktivitou v soukromém sektoru, která je zaměřena na ekonomické a obchodní zájmy. Pro vyspělé podniky je nezbytnou součástí pro strategické a operativní rozhodování, optimalizaci procesů, řízení změn a hlavně pro zajištění a růst konkurenceschopnosti.

Cílem je získat potřebné informace o aktivitách konkurence – ofenzivní konkurenční zpravodajství, zabránit úniku vlastních informací, znemožnit průniku dezinformací do vlastní firmy - obranné konkurenční zpravodajství, vhodně využít získané informace pro lobbying a korekci úniků v tržním prostředí.

Zpravodajství je třeba chápat jako cestu k dosažení znalosti. Podnikatelské či komerční zpravodajství je tedy cestou k dosažení managementu znalostí. Základem dosažení jakéhokoliv cíle je umění získat, zpracovat a využít informace – znalost. Zpravodajství musí dávat odpovědi – znalosti jak pro rozhodnutí operativního, taktického tak i strategického rázu. Zpravodajství je třeba chápat jako nástroj řízení. Jde o schopnost vyhledat, filtrovat a interpretovat informace ve smysluplných souvislostech.

V dnešní době globalizace, v době finanční krize a v době stále ostřejších konkurenčních bojů má konkurenční zpravodajství stále větší význam. Informace jsou velmi cenné a drahé zboží a jsou stavebním materiálem managementu znalostí a jeho rozhodovacích procesů.[6]

1.4.1 Ofenzivní konkurenční zpravodajství

Podstatou ofenzivního konkurenčního zpravodajství jsou postupy:

- jimiž je možno odhalit strategii konkurence a využít ji ve prospěch vlastní organizace (podniku společnosti, firmy, instituce, organizace apod.)
- zajistit informace marketingového charakteru a další informace potřebné pro podnikání
- Informace marketingové
- Informace o technologiích
- Informace o konkurenci
- Ostatní informace.

Informace je ale prvým stupněm činnosti, cílem je znalost. [6]

1.4.2 Obranné konkurenční zpravodajství

Obranné konkurenční zpravodajství zahrnuje a zajišťuje:

- Personální bezpečnost
- Režimovou bezpečnost
- Bezpečnost technických prostředků
- Bezpečnost programových (softwarových) prostředků

- Bezpečnost dat informací, znalostí a KNOW HOW, ochranu technologických procesů
- Bezpečnost komunikačních systémů a cest
- Fyzickou bezpečnost
- Aktivní ochranu proti úniku informací a dat
- Ochranu obchodních aktivit
- Aktivní ochranu proti dezinformacím a působení vlivového 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.). [6]

1.4.3 Vlivové konkurenční zpravodajství

Nejčastějšími metodami vlivových opatření jsou:

- Metoda veřejné či cílené argumentace a odborně věcného přesvědčování
- Asertivní metody
- Demonstrativní metody
- Metody veřejné či cílené dezinformace [6]

2 PROSTŘEDKY PRO HLASOVÝ ODPOSLECH

2.1 Mikrofony

Slouží k utajenému snímání rozhovorů a následnému zpracování. Mikrofony se používají v ucelených audiosystémech, které mění zvuk na elektrické signály, které se vysílají pomocí drátového vedení nebo bezdrátově k přijímači a následné ukládaní dat pomocí záznamového zařízení a poslech rozhovoru na vzdáleném místě.

Nové technologie umožnily vývoj velmi malých mikrofonů, které jsou nenápadné a téměř neidentifikovatelné. Ke své funkci ovšem potřebují různá přídavná zařízení připojená drátem, například napájení, vysílač či záznamové zařízení. Poměrně složitá je montáž zařízení do zájmového prostoru, protože vyžaduje určité technické znalosti, zajištění přístupu do zájmového prostoru, čas pro jeho montáž, ale také nalezení správného místa na instalaci. Kvalitní odposlech je velmi závislý na umístění, převážně platí, že čím je mikrofon blíž k mluvící osobě, tím je kvalita odposlechu vyšší. Pozor si musíme dát i na akustiku místnosti. Mikrofony můžeme použít i jako doplněk pro umístění na tělo, do oděvu či do kufříku pro monitorování vlastního rozhovoru.

Obr. 2 Malé digitální odposlechové zařízení - hlasový záznamník EDIC MINI B21 [11]

Převážně se používají supercitlivé elektretové mikrofony, které umí bez problému monitorovat hlasovou komunikaci v místnosti velkém 6x6 metrů. Mezi výhody mikrofonního odposlechu patří možnost vedení signálu do velkých vzdáleností až několik kilometrů. Napájení mikrofonu je buď bateriové, nebo může být napájeno přímo v místě odposlechu z vedení od EZS, EPS, elektrický vrátný a podobně, kdy nemusíme měnit baterie. Pro výběr vhodného mikrofonu musíme brát ohled na způsob použití a podle toho

volit technické vlastnosti. Základními parametry mikrofonu jsou přenášené frekvenční pásmo, směrovost, citlivost a impedance. Přenášené frekvenční pásmo u miniaturních elektretových mikrofonů se pohybuje od 300Hz do 6kHz, což je ideální na přenos řeči. Směrovost udává citlivost na akustický tlak podle směru dopadu na jeho membránu. Pro odposlech jsou nejvhodnější směrové mikrofony s ledvinovou nebo kardiodní směrovou charakteristikou. Citlivost mikrofonu udává velikost výstupního napětí mikrofonu při určitém akustickém tlaku, tedy jak slabý zvuk je mikrofon ještě schopen zaznamenat. Při použití určitého typu mikrofonu musíme vhodně vybrat typ zesilovače a záznamové zařízení, aby spolu dokázali pracovat. Je možné také zakoupit již kompletní akustický systém obsahující mikrofony, zesilovače, sluchátka či záznamové zařízení a tenké drátové vedení. [4]

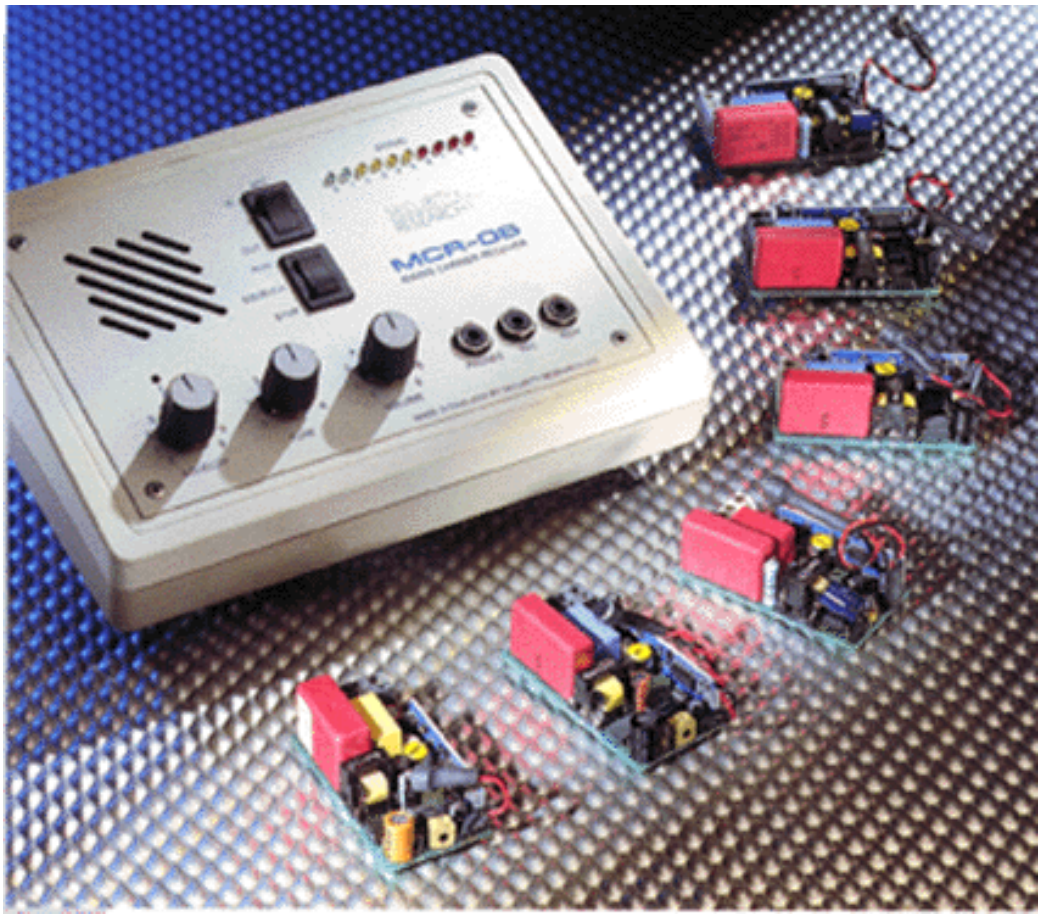
Obr. 3 Elektretový mikrofon[5]

2.1.1 Drátové mikrofony

Velká nevýhoda těchto mikrofonů je nesnadné ukrytí kabelů vedoucích od mikrofonů k záznamovému zařízení. Proto je možno použít alternativních způsobů vedení, kterými mohou být trubky od topení, vodovodního potrubí, klimatizace, nebo využít elektrické vedení od EZS, EPS, elektronického vrátného, telefonní liny, interimu, vedení 220V a podobně. Pro přenos signálů se využívají velmi dlouhé vlny a frekvenčně modulovaný signál v pásmu 50 kHz až 400 kHz, který se šíří po zmiňovaných vodičích. Takový vysílač není o moc větší než samotný mikrofon, není detekovatelný zesilovačem, protože pracuje v nadhovorovém pásmu. Na přijímacím pracovišti je zapojen dekodér, přijímač velmi dlouhých vln a záznamové zařízení.

Nejvýhodnější a nejpoužívanější je přenos akustického signálu po síťovém vedení 220V. Proto se vysílače připojují přímo do zařízení, které jsou trvale připojeny do sítě 220V, jako

jsou například televizory, radiopřijímače, počítače, stolní lampy, ale také různé prodlužovaly nebo zabudování přímo do zásuvkové krabice. Omezením může být použití oddělovacích transformátorů použitých u rozvodů. V takovém případě musíme vysílač zapojit až za transformátor nebo použít jiný způsob přenosu signálu. Jiný způsob může být použití bezdrátového vysílače. [4]



Obr. 4 Souprava pro odposlech využívající vedení 230V jako přenosové cesty [5]

2.1.2 Bezdrátové mikrofony

Abychom odstranili nutnost použití různých druhů vedení, můžeme k mikrofonu připojit bezdrátový VKV vysílač. Použití ovšem vyžaduje pečlivou přípravu a nalezení správného místa na umístění mikrofonu. Pro krátkodobé odposlouchávání prostoru se používají miniaturní rádiové vysílače, tzv. štěnice. Ty mají v dnešní době miniaturní rozměry a dají se pořídit za nízké ceny, jejich instalace je rychlá a snadná. Odposlouchávaný hovor lze zachytit na běžných radiopřijímačích do vzdálenosti asi 100m, proto se doporučuje naladění mimo rozsah VKV. Zpravidla se používají pásma 200MHz až 400Mhz a poslech

je možný běžným širokopásmovým přijímačem, ke kterému můžeme připojit sluchátka nebo záznamové zařízení. [4]

Obr. 5 Odposlechový vysílač UHF – CR2 [15]

2.1.2.1 Frekvenční pásma

Výborné a nenápadné řešení je použití pásma 110MHz až 130MHz, tedy těsně nad kmitočtovým rozsahem VKV. Jako přijímač použijeme kapesní radiopřijímač se sluchátky s upraveným přijímacím rozsahem. Vhodné je použít MP3 přehrávače a radiopřijímačem, které do své vnitřní paměti dokážou nahrávat hovor z vysílání. Toto řešení je skvělé v tom, že se sluchátky na uších a MP3 přehrávačem daná osoba nebudí pozornost a vypadá nenápadně.

Přenosové vlastnosti rádiových vln jsou různé při různých frekvencích vysílače. Praxí ověřené a nejvhodnější kmitočty jsou v pásmu od 60MHz do 450MHZ, které zaručují dobrou kvalitu přenosu signálu a snadno pronikají zdmi budov. Nižší kmitočty vyžadují delší antény, které však jsou pro toto využití velmi nepraktické. Kmitočty v pásmu nad 300MHz velmi špatně pronikají stěnami budov, protože dochází k jejich absorbci a odrazu. Toto pásmo je ale děleno na další pásma rozdělená mezi další uživatele. Frekvenční pásmo 60MHz až 73MHz a 88Mhz až 108MHz jsou využívány pro komerční rozhlasové vysílání, pásmo od 77MHz do 88MHz je určeno pro záchrannou službu. Velké rušení je v pásmu 433MHz od různých dálkových ovladačů a datových spojů. [4]

2.1.2.2 Modulace

Přenos signálu a jeho kvalita je ovlivněna i způsobem modulace. Základní jsou amplitudová modulace (AM) a frekvenční modulace (FM). Amplitudová modulace se používá v pásmech dlouhých, středních a krátkých vln, frekvenční modulace se používá v pásmech velmi krátkých vln a v amatérských pásmech pro občanské radiostanice. U miniaturních odposlechových vysílačů se používá převážně frekvenční modulace se zúženým přenosovým pásmem na 12,5MHz a 25MHz, tedy úzkopásmová frekvenční modulace (FMN, písmeno N z anglického slova narrow). Zaručuje dobrou srozumitelnost odposlouchávaného hovoru a zvuk. [4]

2.1.2.3 Dosah vysílače a výkon

Dosah vysílače je různý a je závislý na výkonu vysílače a jeho napájení. Vysílací výkon také ovlivňuje výdrž napájecího zdroje – baterií. Odposlechové vysílače pracují s různými vysílacími výkony. Ty mohou být od 1mW až do 250mW, kdy 1mW má dosah asi 10metrů. Čím vyšší je výkon, tím lepší je dosah, ale také hrozí větší nebezpečí odhalení odposlechu. Nejpoužívanější výkony jsou mezi 20mW a 100mW. Například 20mW s 9V baterií dokáže pracovat až 10hodin na vzdálenost 200 až 300 metrů. [4]

2.1.2.4 Umístění bezdrátových mikrofonů

Velmi důležitou kapitolou je umístění a způsob použití bezdrátových mikrofonů. Možnosti umístění jsou téměř neomezené, mikrofony se instalují do elektrických zařízení, obrazů, zdí a nábytku, ale také mohou být umístěny skoro do každého předmětu umístěného v zájmovém prostoru, jako je např. váza, popelník, kalkulačka, plnící pero, cigarety a podobně. Bezdrátové mikrofony, které mohou být skrytě umístěny na těle osoby nebo v šatech, se nazývají osobní vysílače. Příkladem umístění mohou být hodiny, kde může být odposlech napájen bateriově nebo přímo z elektrické sítě, v květináči, v odpadkovém koši, velmi skryté je umístění v kouřovém detektoru s napájením přímo ze systému EPS nebo také síťově napájený odposlech v zásuvce, rozdvojce či v prodlužovací šňůře, kdy životnost takového odposlechu je prakticky neomezená. [4]

Obr. 6 Rádiový vysílač s mikrofonem v krytu zásuvky 230V [5]

2.1.2.5 Systém VOX

Malé odposlechové mikrofony mají i nevýhody, protože vysílají trvale. To vede nejen k vybíjení zdroje energie, ale signál je možné zachytit na širokopásmovém komunikačním přijímači. To lze vyřešit několika způsoby, a to použitím zvláštního druhu modulace, snížením výkonu vysílače, omezení doby vysílání nebo použití dálkového ovládání. Dražší bezdrátové mikrofony jsou vybaveny systémem VOX, který automaticky spustí vysílač při dosažení stanovené hladiny akustického tlaku v zájmovém prostoru. Tento systém je výhodný pro dlouhodobé monitorování, nepotřebuje trvalou obsluhu, snižuje možnost náhodného zachycení rádiovysílaní, ale také prodlužuje životnost baterií.

2.2 Speciální odposlechová zařízení

Kromě klasických druhů mikrofonů se k odposlouchávání místností používají i upravené či zkonstruované mikrofony. Mezi nejznámější patří kontaktní mikrofony, elektronické stetoskopy, jehlové mikrofony ale také laserový odposlech.

2.2.1 Kontaktní mikrofony

Princip funkce těchto mikrofonů je takový, že akustický tlak vznikající při rozhovoru v místnosti rozechvěje zdi, dveře a okenní tabule, na které se přiloží kontaktní mikrofon – piezoelektrický krystal, který dokáže toto chvění sejmout. Kvalitní kontaktní mikrofony dokážou snímat vibrace i ze zdí tlustých několik centimetrů. Přenosové vlastnosti pevných materiálů jsou nevypočitatelné, je tedy potřeba vyzkoušet a najít na zdi vhodné místo, kde je slyšitelnost a srozumitelnost hovoru největší. Je výhodné použít vhodný gel na zvýšení přilnavosti mikrofonu ke stěně (např. gel, který se používá v lékařství při sonografii). Ke snímání není potřeba využívat jen stěny, je možné využít i stoupačky ústředního vytápění nebo potrubí vzduchotechniky a klimatizace.

Obr. 7 Kontaktní mikrofon se zesilovačem [5]

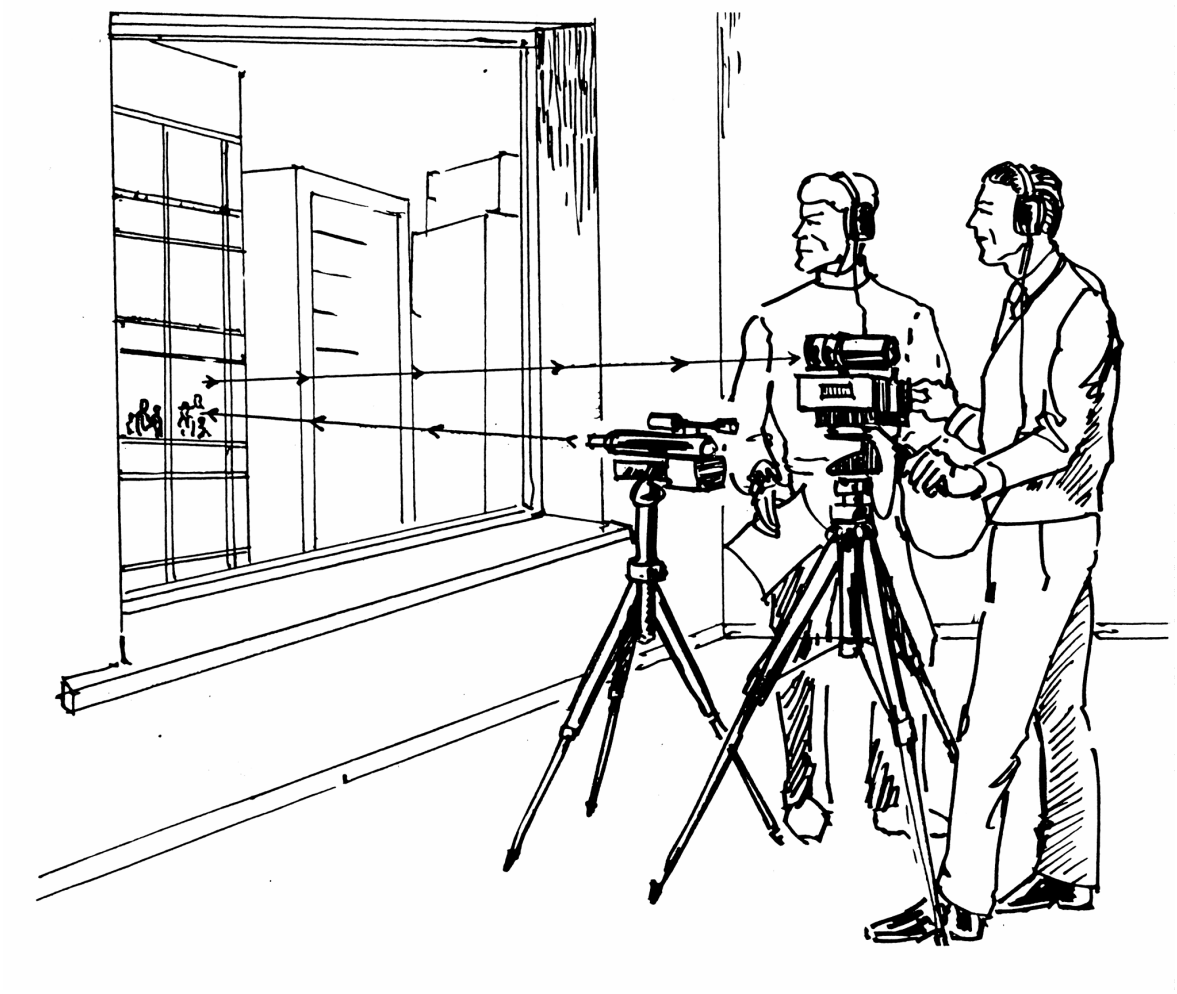
2.2.2 Stetoskopické mikrofony

Stetoskopické mikrofony jsou další druhem speciálních odposlechových mikrofonů. Jsou založené na principu přiloženého hrníčku přiloženého na zeď. Nazývají se také dutinové mikrofony. Dnes jsou vypěny a používány mikrofony obsahující oba druhy dohromady, tedy kontaktní a stetoskopický mikrofon, pro zvýšení kvality snímaného hovoru.

Hovor získaný těmito metodami se musí ještě dále zpracovávat, protože ne vždy je nahrávka srozumitelná. Platí, že čím je mikrofon blíže hovořící osobě, tím je nahrávka srozumitelnější.

2.2.3 Laserový mikrofon

Laser patří mezi mladší vynálezy 20. století a velmi rychle se rozšířil v technice, v našich životech, ve vojenství k navádění střel, ale také v oblasti špionážní techniky. Laserový mikron je dálkový způsob snímání hlasu. Využívá snímání vibrací z okenních tabulek v zájmovém prostoru pomocí laserového paprsku. Paprsek se zaměří na dané okno a podle zákonů optiky se pod stejným uhlem odrazí zpět. Nyní je už však modulován vibracemi okenní tabule, tedy hovorem, který potřebujeme sejmout. Provádění takového odposlechu je velmi náročné, protože musíme najít vhodné místo pro vysílač laserového paprsku, který musíme umístit pevně na stativ a do míst odraženého paprsku umístit přijímač. To ovšem vyžaduje trpělivost při zaměřování. Okenní tabule jsou rozechvívány všemi zvuky dopadajícími na okno, velmi záleží na poměru jejich akustických tlaků. Snímáme tak tedy i různé nepotřebné zvuky, například z ulice. Dosah takového mikrofonu je kolem 200metrů. Velkou nevýhodou jsou vysoké pořizovací náklady. [2]



Obr. 8 Použití laserového mikrofonu [2]

2.2.4 Pasivní rezonátory

Rezonátory jsou typem odposlechového zařízení, které pracuje bez napájení libovolnou dobu a jak název napovídá, je zcela pasivní. Základem systému je malý kovový váleček (dutinový rezonátor) o délce asi 2 cm, ukončen 20cm anténou, která může sloužit jako mechanické zavěšení systému. Druhý konec rezonátoru je uzavřen pružnou kovovou membránou. Celé zařízení se volně umístí v místnosti nebo zabuduje do lustru, plastiky, zdi, nábytku apod. Radiovým vysílačem o velkém výkonu je kovový váleček dálkově ozařován rezonančním kmitočtem. Část vysílané radiové energie je rezonátorem vyzářena zpět do prostoru, modulována hovorem v místnosti. Modulace je umožněna pohybem kovové membrány rozechvívané akustickým tlakem hovoru. Podobné zařízení, využívající k přenosu radiové energie koaxiálního kabelu je možno zabudovat do zdi místnosti. Princip

činnosti je stejný, rezonátor však není ozařován vzduchem, ale po vedení koaxiálního kabelu. [2]

2.2.5 Parabolický mikrofon

Parabolické mikrofony jsou hlavním představitelem dálkových mikrofonů. Mají parabolickou odraznou plochu a pracují na principu odrazu akustické energie do ohniska paraboly, kde je umístěn velmi kvalitní mikrofon. Tvarově i velikostně se velmi podobá klasické satelitní anténě, běžná velikost je kolem 70cm. Dá se poslouchat rozhovor až do vzdálenosti 100metrů. Velkou nevýhodou je, že mikrofon snímá veškerý hluk mezi mikrofonem a odposlouchávaným prostorem. Ideální je proto použití na otevřeném prostranství, například na louce nebo v parku, nebo v noci, kdy je nižší okolní hluk. Téměř nemožné je použití parabolického mikrofonu v městských ulicích, protože tam je velmi vysoká hladina nežádoucího hluku. [4]

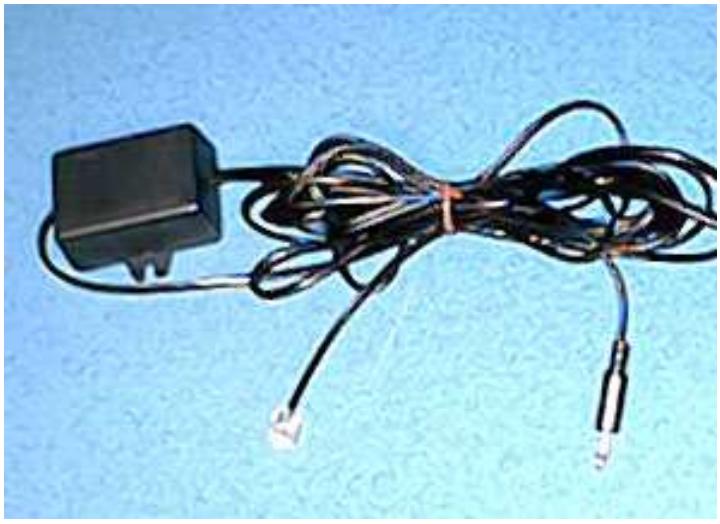
Obr. 9 Použití parabolického mikrofonu

2.3 Telefonní odposlech

Častým místem, kde můžeme nalézt odposlechové zařízení, je telefonní přístroj. Ten je umístěn téměř v každé kanceláři či domácnosti, použití telefonu k odposlechu je ideální řešení. Telefon je nejčastěji připojený do sítě čtyř vodičovým vedením. Existují dva způsoby odposlechu, tedy možnost přímo odposlouchávat telefonní hovor nebo využít telefonu k monitorování místnosti.

2.3.1 Drátový odposlech telefonní linky

Hlavní možností odposlechu telefonního hovoru je napojení citlivého zesilovače nebo záznamového zařízení na přívodní linku na hnědý a bílý vodič. Není důležité, na kterém místě telefonní linky se připojíme, záleží pouze na našich možnostech přístupu k vedení. Jestliže zvolíme tento způsob odposlechu, je vhodné použít záznamové zařízení s automatickým spuštěním záznamu při zvednutí sluchátka telefonu, nebo použít systém VOX, který sám spustí záznamové zařízení při detekci zvuku. Lze také použít zařízení, které hlídá napětí na telefonní lince a spíná záznam v okamžiku zvednutí sluchátka. Pak není nahrán pouze hovor, ale také impulzy tónové volby, z které lze poznat, jaké číslo bylo vytočeno.



Obr. 10 interface pro nahrávání telefonních hovorů na HDD počítače[5]

2.3.2 Rádiový odposlech telefonní linky

Když nemáme možnost připojit drátový odposlech mimo zájmový prostor, pak se musíme připojit na telefonní linku buď v zásuvce telefonní linky nebo přímo v telefonním přístroji.

Zde je ovšem problém s pravidelným vyzvedáváním nahrávky ze zájmového prostoru, kdy můžeme mít problém se dostat k záznamu. Proto je vhodnější použít malé radiovysílače, které přenáší hovor vzduchem po rádiových vlnách. Radiomikrofony byly popsány v předchozích kapitolách. Napájení se provádí buď z baterií nebo přímo z 60V napájené přímo z telefonní sítě. Některé dražší radiovysílače jsou dvoukanálové, kdy jeden kanál snímá a vysílá telefonní hovor, druhý zvuky v místnosti.

Obr. 11 Radiovysílač ukrytý v telefonní rozdvojce s dosahem až 200m [5]

Existují dva způsoby připojení k telefonní lince a to paralelně, kdy je telefonní linka radiovysílačem přemostěna a sériově, kdy je přerušen přívodní vodič telefonní linky. Paralelní je tedy přemostění dvou aktivních vodičů, radiovysílač se tedy připojí na hnědý a bílý vodič. Paralelní zapojení má tu výhodu, že má menší spotřebu proudu a tedy i menší možnost odhalení a možnost připojení kdekoliv na trase telefonní linky. U seriového způsobu se přeruší bílý vodič telefonní linky a propojí se s radiovysílačem. Nelze použít jeden radiovysílač pro oba způsoby, vždy je vyroben pro jeden konkrétní způsob připojení. Na ukrytí radiovysílače máme několik možností, a to buď přímo ve sluchátku nebo v telefonním přístroji, v účastnické zásuvce, v rozdvojce či propojce nebo v pobočkové ústředně.

2.4 Odposlech mobilního telefonu

Mobilní telefony pracující v sítích GSM jsou proti odposlechu na první pohled dostatečně chráněny. Veškerá přenášená data (hovory, SMS zprávy, GPRS přenosy a podobně) jsou totiž šifrována. Pokud už se tedy útočníkovi podaří odposlechnout komunikaci vašeho telefonu s příslušnou BTS stanicí (do jisté míry obdoba ústředny v pevných telefonních sítích), což není zase tak jednoduché, musí ještě rozlomit šifru.

Samozřejmě, nic není ponecháno náhodě. Mobilní telefon je totiž zařízení inteligentní, při své komunikaci v síti přechází víceméně nepředvídatelně mezi různými BTS stanicemi, podle toho, která má zrovna nejkvalitnější signál, největší volnou kapacitu a podobně. K přecházení dochází i v průběhu hovoru. Aby toho nebylo málo, používá se technologie nazvaná frequence hopping. Telefon přenáší data postupně na různých frekvencích, opět podle toho, na které frekvenci se mu to daří nejkvalitněji. I k tomuto poskakování po frekvencích se nijak nerozpakuje – klidně si přeskočí několikrát během jednoho hovoru.

Je samozřejmé, že výše popsané vlastnosti byly použity především kvůli příznivému vlivu na kvalitu GSM přenosů. Ztížení odposlechu a z toho vyplývající zvýšení bezpečnosti je jen příjemným vedlejším produktem. Pokud totiž chcete odposlechnout probíhající spojení, musíte se připravit nejen na to, že spojení probíhá postupně na řadě frekvencí, ale je prováděno s více různými BTS stanicemi.

2.4.1 Co se stane, když zapnu telefon

Karta SIM mimo jiné tajný šifrovací klíč Ki. Tento klíč využívá algoritmus nazvaný A38 (spíš dvojice algoritmů A3 a A8), ve většině případů je ekvivalentní s algoritmem OMP128 či jeho vylepšenou verzí COMP128/2.

Když zapnete telefon, ten se pokusí přihlásit do sítě. Vybere si vhodnou BTS stanici a odešle jí identifikační číslo své SIM karty (IMSI). GSM síť si následně vymyslí náhodné číslo, které pošle telefonu zpět. Telefon pomocí svého tajného klíče a algoritmu A3 toto číslo zašifruje a pošle zpět na BTS. Ta si ovšem stejný výpočet udělala také a získané číslo teď porovná se svým výsledkem. Pokud čísla souhlasí, považuje se SIM karta za autentizovanou.

Nyní přichází ke slovu druhá část šifry A38 - algoritmus A8. Obě strany (karta i BTS) vypočítají z daného náhodného čísla pomocí další šifrovací klíč. Ten bude od nynějška

používán pro šifrování veškeré komunikace mezi telefonem a sítí. No, abychom byli přesní, po nějaké době si telefon a síť ustanoví z bezpečnostních důvodů nový klíč. Postup je ale stejný a odstup mezi ustavením jednotlivých klíčů dostatečně dlouhý na to, abychom mohli tuto skutečnost velkoryse přehlédnout. K šifrování se používá šifra A5. [9]

2.4.2 Šifra A5

Algoritmus A38 se tedy skládá z algoritmů A3, který slouží k autentizaci SIM karty vůči síti a algoritmu A8, který umí vygenerovat takzvaný relační klíč. Relační klíč používá šifra A5, která se stará o veškeré další šifrování.

Tato šifra byla vyvinuta ve třech modifikacích, přičemž všechny mobilní telefony by měly podporovat všechny tyto varianty. Nejméně používanou verzí je A5/0, která prostě nešifruje. Určena je pro problematické země, například Irák. Naopak nejkvalitnější šifrování nabízí verze A5/1, se kterou se běžně setkáte například v České republice. Poslední verze, A5/2 je docela oslabená varianta A5/1 – některé bity klíče jsou záměrně ignorovány, čímž se snižuje jeho efektivní délka. Tato verze byla v době vzniku standardu GSM určena původně pro země bývalého východního bloku.

Šifra A5 patřila dlouho mezi přísně utajované algoritmy. Každý smrtelník, který se s touto šifrou měl seznámit, musel předem podepsat smlouvu o doživotní mlčenlivosti. Jednalo se mimo jiné o vývojáře mobilních telefonů, vědce, inženýry, a tak dále. Na veřejnost se dostala, jak jinak, lidským lajdáctvím. V roce 1994 totiž britská společnost BTT zapomněla dát podepsat tuto smlouvu doktoru Shepherdovi. Ten toho okamžitě využil a algoritmus představil na své přednášce. Než stačila britská tajná služba uvalit na přednášku informační embargo, objevil se popis algoritmu na internetu.

Verze A5/0 je samozřejmě čitelná přímo, bez jakéhokoliv lámání. To bylo ovšem jejím účelem a proto se tomu nemůžeme divit. Pokročilejší A5/2 je čitelná víceméně online, A5/1 s mírným zpožděním také, rozhodně však bez problémů ze záznamu.

Šifra A5 byla pokořena odborníky z Weizmannova institutu v Izraeli, kteří k tomu použili běžné PC se 128 MB paměti a dvěma pevnými disky, každý s kapacitou 73 GB. Základem je získání dvouminutového záznamu stejných dat v zašifrované i nezašifrované podobě. Počítač pak v době kratší než jedna sekunda (údaj z roku 2001, nyní to bude pravděpodobně mnohem méně) najde útokem hrubou silou klíč, který používá algoritmus

A5. To samozřejmě umožní automatické dešifrování všech následně přenášených dat – hovorů, SMS, datových přenosů a podobně. [9]

2.4.3 Odposlech mobilního telefonu

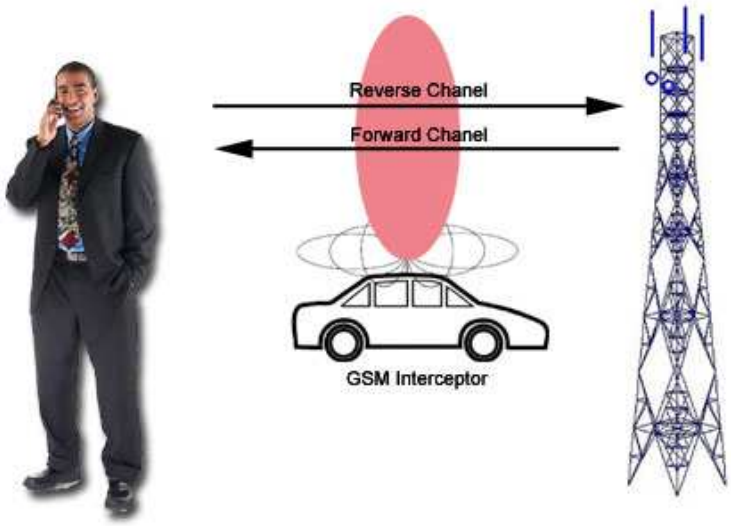
K získání relačního šifrovacího klíče tedy potřebujeme patřičně vybavený počítač a dvě minuty dat. Data v nezašifrované podobě nejsou zase takový problém. Pokud se nám podaří donutit potenciální oběť, aby si stáhla náš javový program, máme otázku nezašifrovaných dat vyřešenu. Pokud se nám toto nepodaří, neměl by být problém nahrávat s dotyčným člověkem běžný hlasový hovor. Stačí zavolat a zkusit fintu typu „děláme průzkum“, „vyhrál jste“, „tady je politik X.Y.“ a podobně. Udržet pak člověka na lince alespoň dvě minuty, to snad zvládne každý.

Větší problém je ale se získáním zašifrovaných dat – tedy odposlechnutí komunikace mezi telefonem a BTS stanicí. Odposlech je sice proveden nenápadně – nikde se nic nepřipojuje, nemusíme se k telefonu přiblížit na příliš nízkou vzdálenost. Oproti tomu se ale musíme vyrovnat s přeskakováním mezi různými frekvencemi a BTS stanicemi. Na trhu se ovšem objevily speciální GSM scannery, které se o všechny tyto záležitosti postarají za nás a na svém výstupu produkují čistá data.

Vybavení pro tento druh odposlechu je docela nákladné, navíc jsou vyžadovány relativně hluboké znalosti dané problematiky. Většina uživatelů se proto nemusí odposlechu bát, hovory běžného člověka nemají takovou cenu, aby se někomu vyplatilo takovými věcmi zabývat.Kromě toho, existují mnohem jednodušší metody, jak odposlechnout mobilní hovory. [9]

GSM Interceptor je zařízení o velkosti videorekordéru připojený přes USB do počítače, nejlépe notebooku se speciálním software a několika GSM anténami. Toto zařízení je schopno odposlouchávat až 8 mobilních telefonu současné v okruhu až několika kilometrů.

Obr. 12 GSM Interceptor



Obr. 13 Funkce GSM Interceptoru

3 ODHALOVÁNÍ PROSTŘEDKŮ PRO HLASOVÝ ODPOSLECH

Existuje celá řada prostředků a zařízení, pomocí nichž se můžeme bránit proti výše uvedeným prostředkům. Jen je potřeba se seznámit s možnostmi odposlechu a případné ochrany proti němu, ale také s úrovní ohrožení. Nezkušený člověk se ovšem nedokáže účinně bránit a potřebuje pomoc odborníka. Na trhu je mnoho firem, zabývajících se touto problematikou, které mají zkušenosti a potřebné technické vybavení na kontrolu místností proti odposlechu i na aktivní ochranu proti němu.

3.1 Zásady proti úniku citlivých informací

- nepoužívejte soukromý nebo firemní telefonní přístroj k projednávání citlivých informací
- pro citlivé telefonní hovory využívejte náhodně volenou telefonní budku
- nechte si nainstalovat kvalitní šifrátor telefonních hovorů
- dodržujte základní zásady při zpracování citlivých informací na počítačích
- objednejte si konzultační služby seriozní firmy [2]

3.2 Technika na vyhledávání prostředků pro hlasový odposlech

3.2.1 Kontrola a kontrola rádiového spektra

Měření radiového spektra, tedy radiová analýza, je nezbytnou součástí obranně technické prohlídky, neboť odposlech bývá nejčastěji prováděn pomocí miniaturních rádiových vysílačů. K tomuto účelu využíváme rádiové analyzátory, které kontrolují a vyhodnocují rádiové spektrum. Ty samotnému odposlechu nezabrání, jen jej spolehlivě odhalí a lokalizují. Nejprve proškolený pracovník provádí vyhledávání aktivních rádiových frekvencí, následně vyhodnotí tyto signály a ty zapíše do paměti přístroje. Následuje zapnutí přístroje do polohy SCAN, kdy zařízení neustále kontroluje radiové spektrum a porovnává s údaji uloženými v paměti. Jestliže je objevena frekvence, která není v paměti přístroje, je uživatel vizuálně nebo i akusticky upozorněn. Tento stav se nazývá předpoplach. Jestliže délka vysílání přesahuje 10 minut, dochází k přepnutí do stavu poplach a uživatel by měl tuto situaci řešit.

Radiové analyzátory připomínají tvarem i velikostí běžné radiostanice. Jsou širokopásmové a automaticky přeladitelné lokátory s detekcí nejsilnějšího signálu, mající výstupní měřící přístroj, který určuje sílu signálu v daném místě. Ten může být ručičkový nebo tvořen řadou LED diod. Dražší přístroje mohou být vybaveny i měřičem frekvence signálu, s jehož pomocí můžeme snadno rozlišovat užitečné a neužitečné signály. Při koupi takového přístroje je třeba dbát na co největší rozsah kmitočtů a největší citlivost. Detekční dosah těchto analyzátorů je velmi závislý na výstupním výkonu odposlechového přístroje, účinnosti jeho antény a na frekvenčním prostředí, které může být ovlivněno komerčním vysíláním rádia a televize. [3]

3.2.1.1 Průběh měření rádiového spektra

Pomocí radiového analyzátoru provedeme vyhledávání aktivních radiových frekvencí v celém spektru, tedy od f_{min} do f_{max}. Zvýšená úroveň signálu může být způsobena známými rádiovými a televizními vysílači, ale i skrytým odposlechovým vysílačem. Z naměřených signálů vyloučíme ty, které rozhodně nevyužívají odposlechové vysílače, tedy například pásmo VKV, které se používá na FM rádio, 420MHz používané mobilním operátorem UFON, analogová televize 470 až 860MHz a další, které jsou uvedeny v příloze. Vyloučené signály můžeme uložit do paměti frekvenčního analyzátoru, který nás již na ně nebude upozorňovat. Zbylé signály jsou pro nás podezřelé, je tedy nutno jim věnovat zvýšenou pozornost. Naladíme se na ně a změříme jejich amplitudu a výkon. Dále určíme, jestli je signál širokopásmový nebo úzkopásmový. U širokopásmového se pravděpodobně nejedná o odposlech, ale o datové přenosy. Může se ovšem jednat o odposlech, který v určitých časových intervalech vysílá paketově data. U úzkopásmového, kdy je šířka pásma kolem 50 až 100 kHz, se může jednat o odposlech a musíme se jim dále zabývat. Radiový analyzátor umístíme doprostřed místnosti a změříme výkon P a intenzitu pole E.

$$E_2 = \frac{\sqrt{30 \cdot P \cdot D}}{R} = \frac{\sqrt{30 \cdot 10 \cdot 10^{-3} \cdot 3{,}28}}{5} = 0{,}1984 V/m$$

E_2 – intenzita pole u přijímače

P=10÷50mW, dosadíme 10mW – výkon

D=3,28 – činitel směrovosti antény

R – vzdálenost vysílače a přijímače

$$P_2 = \frac{U_2^2}{R_a} = \frac{(U_{20} \cdot k)^2}{R_a} = \frac{(E_2 \cdot l_{ef} \cdot k)^2}{R_a} = \frac{(0{,}1984 \cdot 0{,}12 \cdot 0{,}5)^2}{37} = 3{,}8229 \cdot 10^{-6} W$$

P_2 – výkon u přijímače

k=0,5 – konstanta zahrnující převodní poměr děliče napětí tvořený vstupním odporem antény a přijímače

l_{ef}=0,12m – efektivní délka antény pro 420MHz

$$P_{2dB} = 10log\left(\frac{P_2}{0{,}001}\right) = 10log\left(\frac{3{,}8229 \cdot 10^{-6}}{0{,}001}\right) = -24{,}17dBm$$

Od této hodnoty musíme ještě odečíst 20dB z důvodu překážek po cestě a dalších 20dB vlivem umístění mikrofonu.

$$P_{2dB} = -64{,}17dBm$$

Minimální přepokládaná úroveň signálu v místnosti je tedy kolem -64dBm.

Kromě amplitudového spektra a je důležité změřit a zjistit, jaký typ modulace odposlech používá. Pomocí přístroje na analýzu modulace se naladíme na kmitočet a zobrazíme konstalační diagram. K analýze modulace můžeme použít širokopásmový monitorovací přijímač R&S ESMD.

Jestliže se budeme s radiovým analyzátorem přibližovat k vysílacímu zařízení, bude se nám zvyšovat úroveň signálu na stupnici. V místě, které má nejvyšší úroveň signálu, musíme věnovat pozornost při zjišťování přesné lokalizace skrytého odposlechu. Vyloučíme také signály přicházející z venku, tedy ty, které jsou u oken silnější, některé mohou být falešné, všechny ostatní vyhledáváme.

3.2.1.2 Měření pomocí přehledového přijímače MRA-3

Pro neustálou kontrolu radiového spektra je vhodné použít paměťový radiový analyzátor MRA-3, který umožňuje rychlé ladění a automatickou kontrolu kmitočtového spektra. Jednotlivé signály lze naladit, poslouchat a také měřit jejich intenzitu. Již zkontrolované radiové spektrum v místnosti je uloženo do paměti, která je neustále porovnávána s aktuálními signály v zájmovém prostoru, tedy neustále scanuje frekvenční spektrum 43 až

2700 MHz. Je-li nalezen nový neznámý signál, je signalizován poplach a událost zapsána do poplachové paměti. K omezení falešných poplachů je má přístroj 3 úrovně poplachových hlášení, tedy předpoplach, poplach, minulý poplach. [7]

Obr. 14 Rádiový analyzátor MRA-3 [7]

kmitočtový rozsah	43-2700 MHz
citlivost pro SN=10dB	50-1200 MHz 20-40 µV; 43-50 a 1200-2700 MHz 40-1000 µV
demodulace	WBFM, NBFM, AM
šířka pásma	400 kHz
LCD display	2x16 znaků alfanumerický
měření síly pole	40 úrovní LCD čárový indikátor
měření vzdálenosti vysílače	1mW 1 - 50 m
paměť spektra zálohovaná baterií	
512 multifrekvenčních kanálů záznamu spektra	
16 průběžně aktualizovaných poplachových kanálů	
identifikační kód proti neoprávněné manipulaci (65536 stavů)	
jemné doladění + - 1 multifrekvenční kanál	
automatické scannování 6 sekund/cykl	
Rozsah měření kmitočtů	43 - 4000 MHz, rozlišení 0.1MHz (přesnost měření lepší než 10^{-4})
optická a akustická poplachová signalizace	
předpoplach (upozornění na přítomnost nového signálu) po každém scannovacím cyklu	
poplach po 10 (1-20) min.přítomnosti trvalého signálu	
časová informace o minulém poplachu	max. 999 min
regulovatelný audio výstup s vypínatelným reproduktorem	
napájení	9V (vestavěná AKU nebo 6F22 baterie)
spotřeba	SCAN cca 44 mA, OFF pod 4 µA
indikace poklesu baterie pod 7V	
nabíjecí vstup a externí napájení 12-25V DC	
ochrana proti přepólování	
výsuvná teleskopická anténa	
rozměry	136x49x137 mm
váha	620 g (včetně baterie)

Tab. 1 Technická specifikace MRA-3

3.2.1.3 Měření pomocí širokopásmového monitorovacího přijímače R&S ESMD

Na vyhledávání odposlechu je možno také využít širokopásmové monitorovací přijímače a přijímače speciálně určené pro kontrolu radiového pásma, tzv. scanery. Přijímače jsou z technického hlediska kvalitnější než běžné lokátory. Mají větší citlivost, větší kmitočtový rozsah, jsou schopny dekódovat různé druhy modulací, mají digitální zobrazení přijímaného kmitočtu, zpravidla několik typů pamětí a vyhledávacích režimů. Vyrábí se v různých variantách a cenových relacích, nejkvalitnější typy jsou programovatelné počítačem.

Širokopásmový monitorovací přijímač R&S ESMD rychle vyhledává ve velkém kmitočtovém pásmu, slouží k analýze modulace a je schopen zjistit modulaci složitých

signálů, detekuje a měří rychle proměnné signály (číslicově modulované signály, kmitočtové skákání apod.) ve velké šířce pásma 20MHz a ve frekvenčním spektru 9kHz až 26,5GHz. Jedná se o vysoce profesionální zařízení.

Obr. 15 Širokopásmový monitorovací přijímač R&S ESMD [8]

Monitorování téměř všech typů signálů
Rychlé vyhledávání ve volitelném kmitočtovém rozsahu
Doplňkový modul pro zaměřování zdroje vysílání
Spolehlivé vyhledávání zdrojů rušení
Záznam signálu, interní i externí
Akustický výstup demodulovaného signálu
Analýza signálu (software pro PC)
Zobrazení spektra a diagramu typu „vodopád“
Výstup komplexních dat základního pásma
Displej 8,4 ", XGA (1024 × 768 bodu)
Šířka pásma zpracovávaného v reálném case 20 MHz
Demodulace s šířkou pásma až 20 MHz
31 mf filtru od 100 Hz do 20 MHz
Přehledové spektrum ve volitelném kmitočtovém rozsahu, rychlost skenování až 50 GHz/s
Mezifrekvenční spektrum, zobrazované rozpětí 10 kHz až 20 MHz
Spektrum videosignálu
Režimy skenování: skenování kmitočtového rozsahu; skenování kmitočtu uložených v paměti; skenování v přehledovém zobrazení
Dvě rozhraní LAN, každé 1 Gigabit,(SCPI)

Tab. 2 Funkce a specifikace přijímače R&S® ESMD

3.2.1.4 Průběh měření a vyhledání odposlechového prostředku pomocí přístroje RFD-5

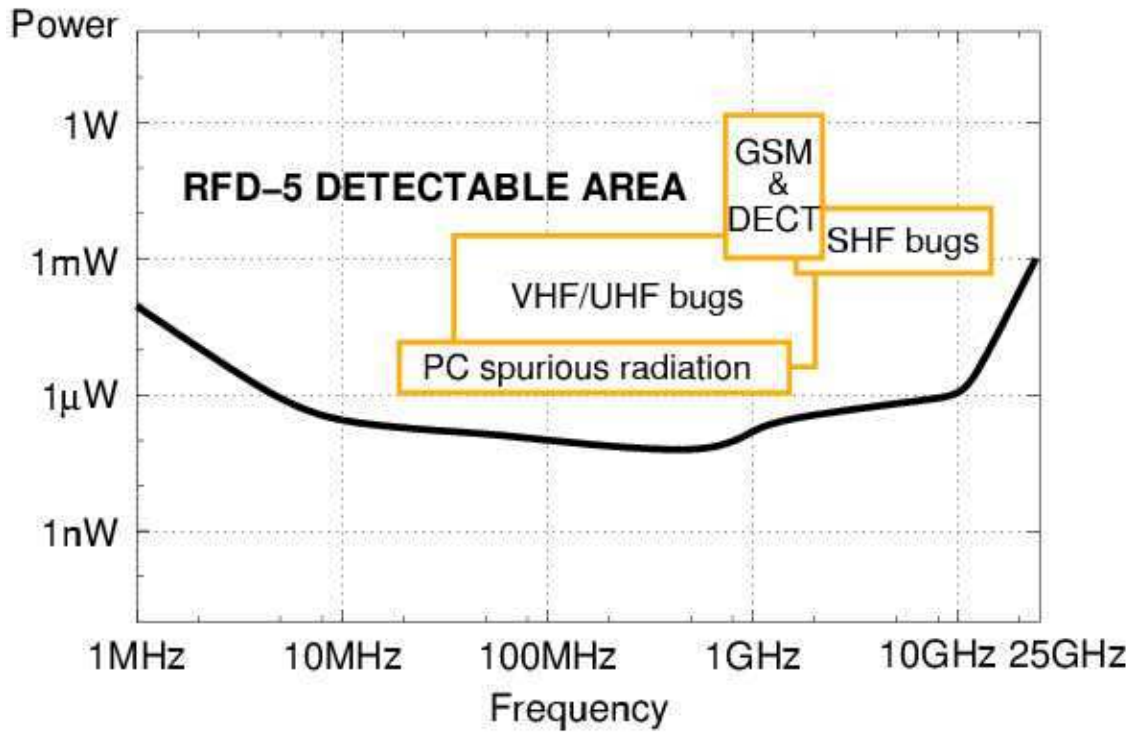
Pro měření frekvenčního spektra a vyhledání odposlechového prostředku je vhodné použít širokopásmový, vysoce citlivý detektor vysokofrekvenčního pole, například přístroj s označením RFD-5. Tento detektor je optimalizovaný pro vyhledávání rozmanitých radiových odposlechových prostředků, a to od základních až po ty nejzákeřnější využívající moderní metody (digitální kódování, spread spectrum, hopping, pulsní přenos, extrémně vysoké kmitočty až do 25 GHz atd.).

Pro měření přístroj zapneme, vysuneme teleskopickou anténu a nastavíme na mód MEASURE M:WIDE. Následně pomalou chůzí procházíme celou kontrolovanou místnost. Zvláštní pozornost dáváme místům, kde předpokládáme, že by mohl být ukryt odposlechový prostředek. Jestliže v některém místě nebo u nějakého předmětu zjišťujeme prudký nárůst VF pole, je nutné zjistit, zda se nejedná o odposlechový prostředek. Hledáme-li odposlechový prostředek, je vhodné k přístroji připojit sluchátka, které nám pomáhají odlišit rozhlasové, televizní a GSM signály a také zrychlující zvukové pulzy usnadňují hledání zdroje signálu. U televizního signálu slyšíme brum, který zesiluje zejména u oken, u rozhlasu slyšíme samotné vysílaní, tedy hlas nebo hudbu. U buňky GSM slyšíme tón kolem 2kHz a u mobilního telefonu přerušovanou sérii impulzů závislých na hovoru. Jestliže signál nespadá ani do jedné kategorie, je třeba zjistit, zda je jeho zdroj uvnitř nebo vně místnosti přicházející ze vzdálených zdrojů. V blízkosti zdroje signálu pro dohledání odposlechového prostředku je vhodné zkrátit teleskopickou anténu, tím umožníme podstatně přesnější lokalizaci vysílače. [7]

Obr. 16 Detektor vysokofrekvenčního pole RFD-5 [7]

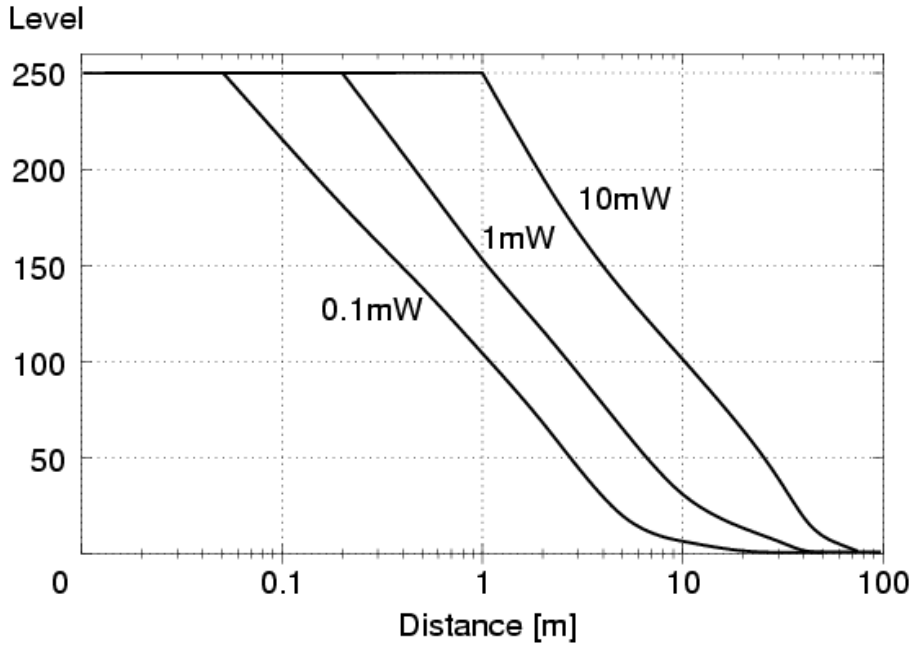
kmitočtový rozsah	0.5 MHz až 25 GHz
typická citlivost	0.06 µW ERP (400 MHz / 5 cm / 5 dílku)
LCD display	2 x 12 znaků
měřitelný impuls	nad 80 µs
okamžité vyhodnocení síly pole	čárkový indikátor 39 hodnot/numerické 251 hodnot
vyhodnocení špičkové hodnoty	zpožděná čárka maxima/zpožděný údaj PEAK 251 hodnot
zpoždění přepisu max. hodnoty	nahoru 1 ms, dolů 6 sec.
dynamický rozsah	43 dB základní, + 40 dB útlum LOCAL
útlum KV	filtr HF OFF 10 MHz - 26 dB
regulace hlasitosti příposlechu	36 dB
proměnný tón lokalizace vysílače	vypínatelný
čítač poplachů	99 událostí
paměť poplachů	16 událostí včetně času a síly signálu
zpoždění záznamu následujícího poplachu	70 sec.
vestavěná teleskopická anténa	nastavitelná 1 až 37 cm
sluchátka	provedení stereo 32 ohm
indikace poklesu napětí baterie	pod 7 V
externí napájení a dobíjení	12 až 20 V DC, nestabilizované
obvod dobíjení akumulátoru	optimalizován pro NiCd
baterie	9V (6F22) nebo 9V akumulátor
spotřeba	3.5 až 6 mA
rozměr	150 x 60 x 31 mm
váha	295 g

Tab. 3 Technická specifikace RFD-5



Obr. 17 Závislost schopnosti detekce RFD-5 pro vzdálenost 5cm a výchylku 5dílků [7]

Z grafu je patrné, že přístroj RFD-5 je velmi citlivý detektor s velkým kmitočtovým rozsahem pro detekci odposlechových prostředků až do frekvence 25GHz. Z grafu vyplývá, že přístroj je schopný detekovat na vzdálenost 5cm efektivní vyzářený výkon 1µW, což je hodnota mnohonásobně menší, než používají reálné odposlechové prostředky.



Obr. 18 Výchylka v závislosti na vzdálenosti u RFD-5 [7]

Graf zobrazuje výchylku v závislosti na vzdálenosti pro 3 různé hodnoty vyzářeného výkonu odposlechového prostředku. Při známé poloze odposlechu, tedy i známe vzdálenosti odposlechu a měřícího přístroje lze pomocí tohoto grafu odvodit efektivní vyzářený výkon a tedy i možný teoretický dosah odposlechu v reálném prostředí.

U každého měření může dojít k nečekaným situacím. Například naše měření nás několikrát přivede do rohu místnosti a žádný odposlechový prostředek tam nenalezneme. V tomto případě je nutné podívat se do vedlejší místnosti.

3.2.1.5 Průběh měření a vyhledání odposlechového prostředku spektrálního analyzátoru FSH3 a směrové antény HE200

R&S FSH 3 je bateriový spektrální analyzátor vhodný pro velmi přesné měření v terénu či laboratořích. Přístroj vybaven mnoha měřícími funkcemi, které jsou vhodné například pro instalaci či údržbu radiových aplikací. Výhodou je velká paměť na 100 měření a následná snadná záloha či práce s naměřenými daty na osobním počítači. Je možno k němu připojit mnoho příslušenství, pro nás je důležitá směrová anténa HE200. HE200 je příruční širokopásmová aktivní anténa, která je v kombinaci s FSH 3 vhodná pro lokalizaci vysílacích a rušících zdrojů, v našem případě pro vyhledávání odposlechových prostředků. Pomocí této antény jednoznačně vyhledáme směr, tedy směrový diagram s maximem příjmu směřujícím dopředu. Maximální hodnota výstupního signálu tedy slouží jako kritérium pro určení směru – vyhledávání směru podle maxima.

Obr. 19: Spektrální analyzátor FSH3 a směrová anténa HE200 [8]

Zaměřování na maximum je klasický a nejstarší způsob zaměřování. Pomocí směrové antény a přijímače se sleduje úroveň. Maximální úroveň signálu znamená stav zaměření. Výhodou je jednoduchost, nevýhodou je menší azimutální přesnost. Tento způsob zaměření využívá pouze amplitudové informace a zaměření nastává, když je přijímací anténa zpolarizována stejně jako dopadající EM vlny. Pokud se v okolí nevyskytují překážky tak, nevznikají odrazy a na kruhovém zobrazovači se např. vynáší intenzita přijímaného signálu v závislosti na úhlu natočení směrové antény. Ideálně tedy dostaneme tvarově shodný obrazec, jako má charakteristika směrové antény. Hlavní nevýhodou je, že v místnosti mohou vznikat odrazy vln od stěn, takže můžeme maximum zaměřit na více místech. Zaměřování na maximum nám pro svoji jednoduchost při vyhledávání zpravidla dostačuje, vzniklé chyby v azimutálním zaměření nehrají roli, protože se jedná jenom o vzdálenosti jednotek metrů, tj. úhlová chyba např. 10 stupňů se na takto krátké vzdálenosti téměř neprojeví. Celé zaměření stejně několikrát opakujeme a korigujeme přijímaný směr, tak jak se postupně přibližujeme ke zdroji signálu (ukrytému odposlechovému prostředku).

Zpravidla se celý postup zaměření děje tak, že nejprve postupujme ze středu místnosti. Často se měření provádí z více směrů, abychom získali větší přehled o tom jak se EM vlny v místnosti šíří. Výše uvedené skutečnosti však neznamenají, že odhalení radiomikrofonu je vždy jednoduché. V některých případech je radiomikrofon rafinovaně ukryt, a navíc může být jeho drátová anténa částečně stočena a její vyzařování tak může být poměrně slabé.

3.2.2 Kontrola nelineárních přechodů

Protože existují vysílače, které mohou být spouštěny na dálku, hlasem, časovým spínačem nebo mohou pracovat s velmi malým vysílacím výkonem, které není možné odhalit ani profesionálními spektrálními analyzátory, musíme použít jiné vyhledávací metody. Důležitou součástí obranně technických prohlídek je kontrola nelineárních přechodů.

Detektor nelineárních přechodů se skládá z přijímací a vysílací antény a z vysílací a vyhodnocovací jednotky. Antény jsou umístěny na teleskopické tyči, vysílací a vyhodnocovací jednotka může být umístěna buď na druhém konci tyče nebo na popruhu na rameni. Tento přístroj využívá toho, že nelze vyrobit odposlechový prostředek bez polovodičové součástky. Vysílací anténa vysílá pulzní signál o frekvenci kolem 900MHz a přijímací anténa zachytává odražené signály. Polovodičové přechody odrážejí 2. harmonickou frekvenci a kovové předměty 3. harmonickou frekvenci. Vyhodnocovací jednotka pak vyhodnotí, zda se jedná o kov nebo polovodič a signalizuje tuto skutečnost vizuálně i akusticky do sluchátek. Takto je možno nalézt i dávno nefunkční odposlechová zařízení. Práce s tímto detektorem ovšem vyžaduje zkušenou obsluhu, neboť ne každá signalizace 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]

Obr. 20 Detektor nelineárních přechodů [16]

3.2.3 Kontrola vedení a linek

Kontrolujeme-li průběh neznámých kabelových a linkových vedení, můžeme použít tónový generátor připojený ke známému konci vodiče, který nám pak slouží jako anténa. Následně použijeme širokopásmový přijímač, pomocí kterého můžeme přesně sledovat průběh tohoto i pod omítkou. Je možno koupit celé soupravy obsahující detektor VF pole, externí sondy, sluchátka, širokopásmový generátoru, dvě drátové antény a linkový adapter, vše uložené v elegantním kufříku.

Obr. 21 Souprava RFDS-3 pro odhalování odposlechu [7]

Přímé napojení mikrofonu na telefonní nebo jinou sdělovací linku je možno odhalit citlivým zesilovačem s velkým vstupním odporem. Zesilovač je určen k poslechu podezřelých drátů, ke zjištění zda zde neuslyšíme hlasy nebo jiné signály. Umožňuje testovat telefony a telefonní linky na přítomnost různých zařízení jako jsou nekonečné a harmonické štěnice, které poslouchají místnost při zavěšeném telefonu. Vstup zesilovače musí být napěťově chráněn proti zničení. [2]

Během fyzické prohlídky můžete najít neznámé dráty a kabely. Citlivý zesilovač umožňuje takové linky kontrolovat a určit, zda vedou užitečný signál nebo jsou to vedení pro odposlech. Před připojením zesilovače na neznámé vedení nebo kabel se musíte ujistit, že toto vedení neobsahuje nebezpečné napětí.

3.3 Technika na ochranu informací

Pro zamezení úniku informací přes odposlechový prostředek, i po jeho případném nalezení, je nutno daný prostor chránit. V této kapitole budou popsány způsoby ochrany proti různým druhům odposlechových prostředků.

3.3.1 Ochrana proti rádiovému odposlechu

3.3.1.1 Rádiové analyzátory

Rádiové analyzátory pracují na kontrole a vyhodnocení rádiového spektra. Rádiovému odposlechu nezamezí, pouze jej velmi spolehlivě odhalí a lokalizují. Základní princip činnosti spočívá v zapsání aktivních rádiových signálů do paměti přístroje vyškoleným pracovníkem , vyhodnocení těchto signálu a zapnutím přístroje do polohy SCAN. V tomto režimu jednotka automaticky kontroluje rádiové spektrum a porovná aktuální rádiové signály se zaznamenanými. V případě, že je nalezena frekvence, která není v paměti přístroje, je uživatel upozorněn vizuálně, případně akusticky. Jednotlivé typy se liší zejména šířkou pásma, které dokážou kontrolovat a v rychlosti této kontroly. Tato problematika je podrobněji popsána v předchozích kapitolách, kde jsou také uvedeny příklady těchto zařízení. [3]

3.3.1.2 Jammery

Jammer je rušička určena pro zarušení všech mikrofonů v jejím dosahu, tedy znemožňuje pořízení jakéhokoliv zvukového záznamu přes mikrofon, diktafon, mikrofon kamery, radiomikrofon a další podobná zařízení. Existují různé druhy těchto rušiček pro různé frekvence, lze tedy rušit signály GSM, CDMA, WiFi a další.

Obr. 22 Kufříková rušička radiomikrofonů [11]

3.3.2 Ochrana proti snímání informací z oken nebo zdí

Jednou z možností provádění odposlechu je kontaktní či bezkontaktní snímání akustických informací ze zdí či oken subjektu. Tato forma odposlechu nevyžaduje přímý průnik do zájmového prostoru. Pro svou činnost využívá skutečnosti, že zvuk je mechanické vlnění, které je možné na dálku snímat a zpětně převádět na užitečnou informaci. Šumový generátor produkuje bílý šum, který dokáže hovor překrýt vlastním vlněním a zabrání tak zpětnému převodu vlnění na akustickou informaci. Minimální nevýhoda tohoto řešení spočívá v tom, že bílý šum je slyšitelný a uživateli se jeví jako zapnutá klimatizace. Největší nebezpečí pro nelegální získávání informací v sobě však dnes skrývající různé elektronické přístroje běžné spotřeby – mobilní telefony, PDA a podobně. Zamezit nahrávání na tyto prostředky se účinně daří pouze pomocí šumového. Nevýhodou je vysoká úroveň šumu nutná ke kvalitnímu překrytí. Obrovskou výhodou pak je to, že ani z nedůvěrnějších jednání si protistrana neodnese žádnou použitelnou nahrávku. [3]

Obr. 23 Inteligentní šumový generátor SNG [7]

SNG je inteligentní výkonový šumový generátor umožňující připojení až 100 piezokeramických akustických měničů, až 12 nízkoimpedančních reproduktorů, nebo jejich vzájemnou kombinaci. Účelem zašumění je zajistit ochranu prostoru proti odposlechu využívajícího všech forem snímání zvuku z oken, zdí, případně i z jiných předmětů pokud útočníkův systém využívá jako průnik do prostoru okna nebo zdi místností. Instalací piezoměničů na vnitřní stěny nábytku, stolů a dalších předmětů uvnitř kanceláře lze realizovat vhodnou doplňkovou ochranu proti operativně umístěným přenosným odposlechovým prostředkům. [3]

3.3.3 Faradayova klec

V některých speciálních případech, kdy klient není ochoten obsluhovat a kontrolovat výše zmiňované technické prostředky a má maximální nároky na ochranu proti odposlechu, může se prostor vybavit Faradayovou klecí. Jedná se o nejnáročnější a zároveň nejspolehlivější ochranu proti odposlechu. Obvykle se postupuje výběrem nejvhodnějšího prostoru v objektu, provede se úprava elektroinstalací (do prostoru se přivede pouze 1 napájecí kabel, jsou odstraněna všechna ostatní síťová připojení – telefony a PC). Na toto vedení je připojen síťový filtr. Poté je na stěny místnosti instalována síť piezoměničů pro zamezení kontaktního snímání informací z pláště místnosti, na ni je nalepena speciální měděná fólie (existují různé druhy v závislosti na požadovaném útlumu). Tato fólie je překryta omítkou. Do oken jsou instalovány speciální pokovená skla a je provedena úprava

dveří potažením samolepicí fólií, případně se instalují i speciální dveře a zárubně. Vše je uzemněno. Provede se měření, které určuje výsledný útlum. Tento výsledek je konfrontován s požadovaným útlumem. Pokud je potřeba, instaluje se další vrstva fólie. Následně se dokončí všechny ostatní interiérové úpravy a instalují se paměťový rádiový analyzátor a šumový generátor. Samozřejmostí pro tuto místnost je naprosté dodržování režimu vstupu a pobytu cizích osob v těchto prostorech. [3]

3.4 Obranně technická prohlídka

Cílem obranné technické prohlídky je odhalení skrytých odposlechových prostředků, a to aktivních i neaktivních v době provádění prohlídky. Je to komplexní prověrka bezpečnosti daného objektu z hlediska úniku informací, tedy celkové posouzení objektu, nalezení odposlechového prostředku a návrh potřebných opatření pro zamezení jeho následné instalace. Prohlídka by měla být prováděna podle zásad uvedených v této kapitole.

3.4.1 Určení místa provádění prohlídky

Ochrana proti nelegálnímu odposlechu se aplikuje především v místnostech, v nichž probíhají jednání a v kancelářích pracovníků vyššího managementu. Zjišťování interních informací o jednotlivých zakázkách, klientech, rozvojových plánech s využitím prostředků odposlechu umožňuje protivníkovi získat velmi rychle přehled o aktivitách společnosti, což může vést k poškození, případně i zničení celé společnosti. Údaje získané tímto způsobem mají mnohdy větší hodnotu, než podklady získávané sběrem veřejně dostupných informací po dobu několika let. Ochrana proti odposlechu spočívá v provádění obranně technických prohlídek s cílem vyhledat případné již aplikované nelegální odposlechové prostředky a instalací technických prostředků, které mají zabránit takovému získávání informací v budoucnosti. Při obranně technické prohlídce je nutné dodržet správný postup již při rozhodování toho, které prostory by měly být prověřeny, a která firma bude obranně technickou prohlídku provádět. [17]

3.4.2 Utajení prohlídky

Jednotlivé informace týkající se prohlídky by měl vědět jen velmi úzký okruh lidí a to až do chvíle, kdy má být vlastní prohlídka uskutečněna, pokud se jedná o více místností až do skončení prohlídky. Toto je nejdůležitější opatření před zahájením samotné prohlídky z

důvodu znemožnění demontáže případného odposlechového prostředku, který mohl být nainstalován vlastními zaměstnanci. [17]

3.4.3 Postup při odhalení odposlechového prostředku

Je-li odhalen odposlechový prostředek, je nejprve řádně zakresleno do situačního plánu místo odhalení odposlechového prostředku. Stejně tak je místo nálezu zadokumentováno i fotograficky. Poté je prostředek demontován a celý prostor ještě jednou řádně prověřen. Specialisté společnosti jsou do vysoké míry schopni určit druh a původ odposlechového prostředku. Z tohoto důvodu společnost doporučuje osobní asistence zodpovědného pracovníka zadavatele, čímž se předejde jakýmkoliv budoucím sporům a navíc je tato účast užitečná i pro případ, kdy se v konstrukci zachytí signál upozorňující na přítomnost polovodičového přechodu. Konečné rozhodnutí dalšího postupu však musí zůstat na zadavateli. Ten se může rozhodnout pro destruktivní metodu a vyjmutí případného zařízení, nebo využití této znalosti pro dezinformační účely apod. [17]

3.4.4 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. [17]

3.4.5 Druhy prohlídek

3.4.5.1 Fyzická prohlídka

Jedná se o podrobnou fyzickou prohlídku místností zaměřenou na odhalení odposlechových prostředků umístěných v síťových rozvodech, telefonních zásuvkách, telefonních aparátech, vypínačích, a dalším vybavením místností.

3.4.5.2 Rádiová kontrola

Rádiová kontrola je zaměřena na odhalení všech činných radiových prostředků a na vytvoření frekvenční mapy prostoru, což představuje zhotovení seznamu všech radiových

frekvencí, které se vyskytují v kontrolovaném prostoru a prověření všech elektrických rozvodů a kontrolu všech signálů vysílaných po metalických vedeních.

3.4.5.3 Kontrola nelinearit

Kontrola nelinearit je vyhledání všech polovodičových součástek pomocí detektoru nelineárních přechodů. Tento detektor využívá pro svou činnost tento základní předpoklad, že není možné vyrobit žádný zpravodajský prostředek, který by neobsahoval alespoň jednu polovodičovou součástku. Tato kontrola je důležitá z hlediska nalezení zpravodajských prostředků, které jsou dálkově ovládány nebo přenášejí informace paketově, to znamená, že informace uchovávají ve své paměti a po uplynutí periody je dokážou přenést ve velmi krátkém okamžiku (pasivní prostředky). Především ve starších budovách jsou tímto detektorem odhalovány i prostředky, které jsou napájené ze síťového rozvodu a jsou zazděné. [17]

3.4.6 Obecné zásady obranně technických prohlídek

Tyto zásady je nutno dodržovat bez ohledu na to, zda si prohlídku provádíte sami, nebo je vyhledávání odposlechu prováděno specializovanou firmou.

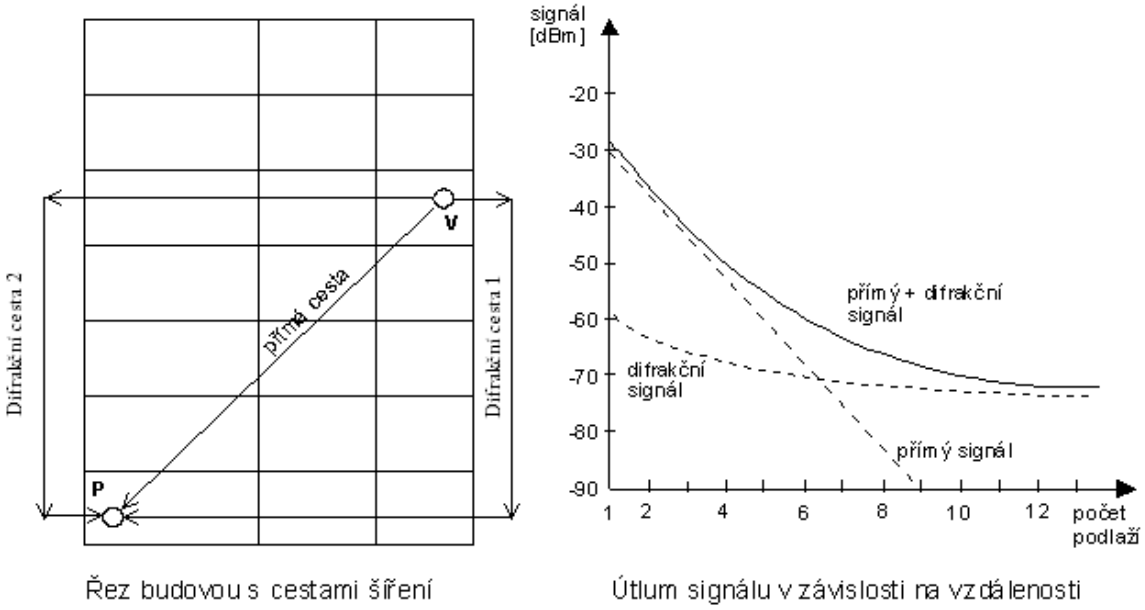
- Zahájení prohlídky by mělo být v čase, kdy se předpokládá aktivace odposlechových zařízení (v průběhu obchodních a jiných jednání)
- Některé odposlechy mohou být dálkově ovládány. Naplánované klamné, věrohodně vypadající obchodní, nebo jiné jednání může zabezpečit okamžitou aktivaci všech těchto odposlechů.
- Všechny následné prohlídky by měly být prováděny v náhodných intervalech.
- Vyhledávání musí být prováděno skrytým způsobem (před činností možného protivníka). Vaše porady s kolegy nebo zákazníky, zahájení prohlídky, nastavení přístrojů a lokalizace odposlechového zařízení nesmí dát tomu, kdo odposlech provádí, informaci o jeho odhalení.
- Úspěch při právě prováděné prohlídce je závislý na vybavení, odborných vědomostech a pečlivosti, která je vyhledávání věnována.

- Před vlastním zahájením vyhledávání se důkladně seznamte s jednotlivými detekčními metodami a možnostmi přístrojů. Tyto nácviky vyhledávání a procvičování detekčních metod provádějte zásadně na bezpečných místech.
- Největší pozornost věnujte oblasti, kde se běžně odehrávají důležité rozhovory (za psacím stolem, blízko telefonního přístroje). Největší množství odposlechových zařízení bude umístěno v okruhu do 7 metrů z důvodu dobrého hlasového příjmu.
- Vytvořte vhodné pokojové podmínky pro prohlídku. Zatáhněte všechny závěsy, abyste se vyhnuli sledování, zapněte všechna světla a některé další přístroje z důvodu vytvoření běžného pokojového prostředí. [2]

4 MĚŘENÍ ŠÍŘENÍ SIGNÁLŮ V PÁSMU UHF A VHF V BUDOVÁCH

4.1 Šíření elektromagnetických vln v budovách

Pro šíření radiových vln v budovách připadají v úvahu v zásadě dvě možné cesty mezi vysílačem a přijímačem. První cesta předpokládá více či méně přímočaré šíření mezi podlažími skrze zdi a stropy budovy. Druhá cesta spočívá v pronikání signálu okny vně budovy, jeho následném šíření difrakcí podél vnějšího pláště a opětném vniknutí okny do nitra budovy. Mimo tyto dvě cesty dochází v budovách samozřejmě k četným odrazům v místnostech, vybuzení a zpětnému vyzařování vodivých předmětů a stavebních prvků apod. Ovšem dominantní zůstávají dříve uvedené dvě cesty šíření. Která z obou cest v konkrétním případě převáží, závisí na přenosových ztrátách, ty jsou závislé na použitých konstrukčních systémech a materiálech. Protože pro stropní konstrukce je obvykle použito mohutnějších stavebních konstrukcí než pro stěny, lze ve vertikálním směru očekávat větší problémy se šířením radiových vln než ve směru horizontálním. Průchozí útlum je nejmenší u železobetonových stropů (cca 10 dB), u panelových stropů je potom kolem 13 dB a největší je u litých stropů na ocelových panelech (asi 26 dB; skutečnost je ale zřejmě ještě horší, protože uvedená hodnota je pravděpodobně ovlivněna difrakční cestou vně budovy). Přímý paprsek se při průchodu jednotlivými podlažími zeslabuje úměrně druhé mocnině koeficientu přenosu (tj. 10 dB i více). To má za následek prudký rovnoměrný pokles úrovně signálu při šíření od podlaží k podlaží. Při šíření difrakcí vně budovy přináší difrakční koeficient velký útlum při přechodu byť do sousedního podlaží, ovšem nárůst útlumu při delší vertikální trase (vzdálenější podlaží) je již nevýrazný a zvyšuje celkové ztráty jen mírně. Při šíření radiových vln mezi blízkými podlažími tedy převažuje signál šířící se přímou cestou, s přibývajícím počtem mezilehlých podlaží se rozdíl mezi přímým a difrakčním signálem snižuje, až převáží signál difrakční. Příklad útlumu při šíření přímou a difrakční cestou v pásmu 852 MHz je na obrázku. Převažující význam jednotlivých cest šíření velmi silně závisí na konstrukčním systému budovy. Obecně lze konstatovat výrazný vliv přímého signálu při malém počtu mezilehlých podlaží a narůstající vliv signálu difrakčního při narůstání jejich počtu. Při srovnání šíření do nadzemních a podzemních podlaží lze konstatovat nižší intenzitu signálu v podzemních podlažích z důvodu nepřítomnosti složky šířící se difrakční cestou. [18]



Obr. 24 Šíření radiových vln v budově [18]

Tloušťka materiálu 0,3m		**Frekvence signálu**				
		0,5GHz	**1GHz**	**2GHz**	**3GHz**	**4GHz**
Materiál	**Beton**	12,5 dB	15,3 dB	21,9 dB	22,1 dB	23,0 dB
	Cihla	6,0 dB	7,5 dB	10,7 dB	13,8 dB	16,6 dB
	Překližka	8,0 dB	12,6 dB	17,9 dB	21,6 dB	24,4 dB

Tab. 4 Příklady útlumu při průchodu stěnou z různých materiálů

K zjišťování šíření vln v budovách se v praxi používají 3 možné přístupy:

- zjednodušený přístup založený na ***semianalytických přístupech*** - vhodné pro orientační výpočet. Chyba často 20 dB.

- výpočet pomocí ***geometrické optiky a geometrické teorie difrakce*** *(ray tracing)* - rychlý a poměrně přesný způsob, chyba kolem 5 až 10 dB

- ***Fullwave elektromagnetická simulace*** *(FEM, FDTD)* – přesný způsob výpočtu pole, nutná pečlivá příprava geometrie modelu a přesná znalost permitivity a ztrátového činitele u dielektrickýh materiálů. U feromagnetických materiálů pak postačuje znalost reálné

části permeability. Velká přesnost – chyba 2 až 5 dB, velká výpočetní náročnost pro elektricky velké struktury

4.2 Frekvenční pásma

Zkratka	Název	Kmitočet	Délka vlny	Název pásma	Metrické zkratky
VLF	Velmi dlouhé	3 – 30 kHz	100 – 10 km	Myriametrické	Mam
LF	Dlouhé	30 – 300 kHz	10 – 1 km	Kilometrické	km
MF	Střední	300 – 3000 kHz	1000 – 100 m	Hektometrické	hm
HF	Krátké	3 – 30 MHz	100 – 10 m	Dekametrické	dam
VHF	Velmi krátké	30 – 300 MHz	10 – 1 m	Metrické	m
UHF	Ultra krátké	300 – 3000 MHz	10 – 1 dm	Decimetrické	dm
SHF	Centimetrové	3 – 30 GHz	10 – 1 cm	Centimetrické	cm
EHF	milimetrové	30 – 300 GHz	10 – 1 mm	Milimetrické	mm
-	-	300 – 3000 GHz	1 – 0,1 mm	Decimilimetrické	dmm

Tab. 5 Frekvenční pásma

4.2.1 UHF pásmo

Ultra vysoká frekvence (UHF) určuje rozsah (pásmo) elektromagnetických vln s frekvencí 300MHz a 3GHz (3000 MHz). Tyto jsou označovány také jako dekadické pásmo nebo dekadické vlny a to proto, že jejich vlnová délka je v rozmezí od deseti do jedné. Rádiové vlny přesahující tyto hodnoty jsou označovány jako SHF (super vysoká frekvence) a EHF (extrémně vysoká frekvence) pásma, které všechny spadají do mezi tzv. mikrovlnné frekvenční pásma. Naopak nízkofrekvenční signály spadají do tzv. VHF (velmi vysoká frekvence) nebo i nižších pásem. [19]

4.2.2 Charakteristika UHF

UHF a VHF jsou nejběžněji používaná frekvenční pásma pro přenos televizního signálu. Možná ne každý ví, že i moderní mobilní telefony také fungují v určitém typu UHF spektra.
UHF se hojně využívá ve veřejné službě a to jako běžná radiová komunikace, a to obvykle pomocí úzkopásmové frekvenční modulace. Moderní „digitální služby“, které jsou na razantním vzestupu této technologii trošku posunují do propadliště dějin.

Nemůžeme opomenout to nejdůležitější využití a to jako rozhlasové vysílání, které do určité míry přispělo ke globalizaci planety. Za zmínku stojí i to že například GPS technologie je postavena na využívání UHF pásem.

2,45 GHz pásma se dnes používají hlavně pro WiFi či Bluetooth. Pro radioamatérské operátory jsou určena teké určitá radiová pásma v pásmech UHF. Některé rádio identifikační štítky (tzv. RFID technologie) využívají UHF pásem a používají se k identifikaci zboží ve skladech.

Přenos rádiových vln je ovlivňován mnoha proměnnými. Atmosférická vlhkost, proud částic ze Slunce (tzv. sluneční vítr), a denní doba tato všechny aspekty mají vliv na přenos signálu.

Všechny rádiové vlny jsou částečně pohlcovány atmosférickou vlhkostí. Atmosférická absorpce snižuje nebo zeslabuje pevnost rádiových signálů na dlouhé vzdálenosti. Účinky útlum zvyšuje v závislosti na frekvenci. UHF signály jsou obecně více štěpeny vlhkostí než nižší pásma (VHF).

Ionosféra, vrstva zemské atmosféry, je plná nabitých částic, které mohou odrážet rádiové vlny. Odrazy rádiových vln mohou být užitečné při předávání radiového signálu na dlouhé vzdálenosti a to tak že rádiová vlna opakovaně „hopsá“ z nebe na zem.

Hlavní výhodou UHF přenosu je tvorba fyzicky krátkých vln, které se „vyrábí“ ve vysoké frekvenci. Velikost vysílacího a přijímacího zařízení (tedy antény), je závislé na velikosti dané rádiové vlny.

UHF je široce používán ve dvoupásmových radiových systémech a u bezdrátových telefonů. UHF signály mohou „cestovat“ přes dlouhé vzdálenosti. [19]

4.2.3 VHF pásmo

VHF (Velmi vysoká frekvence) je rádiová frekvence v rozsahu od 30 MHz do 300 MHz. Kmitočty těsně pod VHF jsou označeny vysoké frekvence (tzv. HF) a kmitočty vyšší než VHF jsou pak známé jako Ultra vysoká frekvence (UHF).

Využití VHF je především v oblasti FM rozhlasového vysílání, televizního vysílání, pozemních mobilních telefonů, radioamatérství, námořní komunikace, řízení letového provozu a letecké navigační systémy, apod. [19]

4.2.4 Charakteristika VHF

Díky vlastnostem VHF pásem, pak je jejich ideální použití pro krátké vzdálenosti (pozemní komunikace). Na rozdíl od vysokých frekvencí (HF) ionosféra neodráží VHF rádiové signály, tak jsou přenosy v pásmu VHF omezené na „místní“ oblast. VHF vlny jsou také méně rušeny atmosférickými šumy a rušením od elektrických zařízení.

VHF pásmo, resp. jeho přenos je ovlivněn značně výkonem vysílače, citlivostí přijímače a jejich vzdáleností. Vzdálenost je dána horizontem země (tedy obzorem či dohledovou vzdáleností).

Aproximace pro výpočet dosahu (na Zemi) je:

$$l = \sqrt{17 \cdot Am}\ [km]$$

l … vzdálenost [km]

Am … výška antény [m]

Tyto odhady jsou platné pouze pro antény v nízkých výškách (ve srovnání s poloměrem Země). Při budování komunikačních systémů se však v praxi používají mnohem složitější modely a vzorce. [19]

4.3 Anténa, vlastnosti

Anténa je zařízení sloužící k příjmu nebo k vysílaní signálů. Je to část vysokofrekvenčního vedení upravená tak, aby účinně vyzařovala energii do prostoru. Antény mohou být přijímací a vysílací, každá anténa ale může vysílat i přijímat. Vysílací anténa přeměňuje elektrickou energii na energii elektromagnetických vln, přijímací anténa k přeměně

elektromagnetických vln na elektrickou energii. Elektromagnetické vlny vyzařuje každý vodič, kterým prochází střídavý elektrický proud. Anténa je upravený vodič tak, aby vysílal maximální množství elektrické energie. Nejjednodušší anténa je syntetický zářič, takzvaný dipól. Ten vychází z úseku vedení o délce poloviny vlnové délky vysílaného/přijímaného signálu.

Vlastnosti antén popisujeme následujícími parametry:

- směrovost antény – jedná se o schopnost antény vyzařovat/přijímat elektromagnetické vlny v požadovaném směru, tuto směrovost vyjadřují takzvané vyzařovací charakteristiky

- vyzařovací úhel antény – tento úhel je dán tzv. směrovým diagramem a vypočítavá se jako rozdíl úhlů bodů, kde je pokles signálu o 3dB.

- impedance antény Z [Ω] – je vlastní impedance, která by měla být reálná (bez imaginární složky); Impedance antény musí být alespoň přibližně stejná, jako impedance přívodního kabelu, aby nedocházelo k odrazům a k nárůstu odraženého výkonu. V TV technice mají takřka všechny antény impedanci 300 ohmů, ta se přímo u svorek antény transformuje na impedanci kabelu - ta je obvykle 75Ω.

- zisk antény – udává, kolikrát větší výkon musíme dodat do půlvlnného dipólu, aby v místě příjmu byla stejná energie jako u směrové antény, jednotkou je decibel. Anténa, která přijímá signál stejně, jako dipól, má zisk 0 dB.

- efektivní délka antény – je taková délka, kterou prochází rovnoměrně rozložený vysílací (přijímací) proud.

- šířka přenášeného pásma – udává šířku přenášeného frekvenčního pásma

- činitel zpětného příjmu – vyjadřuje základní směrovost antény

- součinitel směrovosti – D - udává, kolikrát musíme zvýšit výkon vysílače při přechodu z měřené antény (např. směrové) na referenční (všesměrovo), abychom dosáhli v libovolném místě příjmu stejné intenzity EMG jako s anténou měřenou.

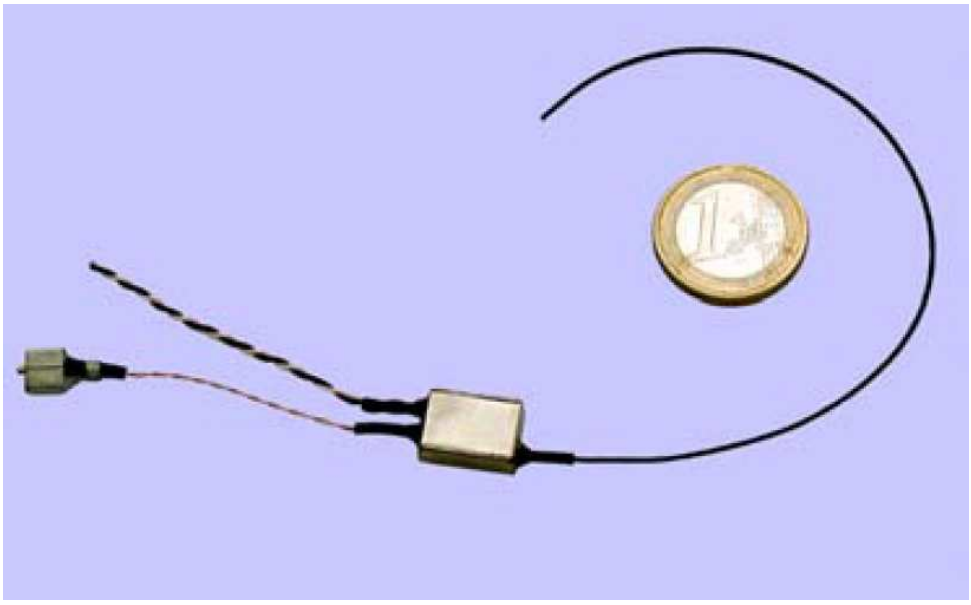
- polarizace antény - říká v jakém směru vzhledem v povrchu země jeorientován vektor elektrické intenzity, tj. může být vodorovná (horizontální) nebo svislá (vertikální).

4.4 Pokusná měření

4.4.1 Měření frekvence odposlechového prostředku RM-M3

K měření frekvence signálu byl použit spektrální analyzátor FSH 3 v kombinaci se směrovou anténou HE 200 a jako vysílač byl použit radiomikrofon MR-M3. RM-M3 je víceúčelový analogový radiomikrofon určený k provádění audio monitoringu. Audio informace je u tohoto odposlechového prostředku vysílána anténou jako radiový kanál v rozsahu frekvence 417-432 MHz. Signál je možno přijímat pomocí „UNIVERSAL“ (detektor stejného výrobce) nebo také příslušným FM snímačem. Zařízení je vyrobeno z dielektrických materiálů s malým pohlcováním elektromagnetických vln, doporučuje se pro skryté použití. Mikrofon je napájen dvěma AA bateriemi (tužkové), tedy napájecí napětí je 3V. Na spektrálním analyzátoru byla zobrazena frekvenční charakteristika a změřená maximální frekvence pomoci indikátoru MARKER – MAX PEAK. Měřením bylo zjištěno, že vysílací frekvence radiomikrofonu byla 417,926MHz.

$$f = 417{,}926MHz$$

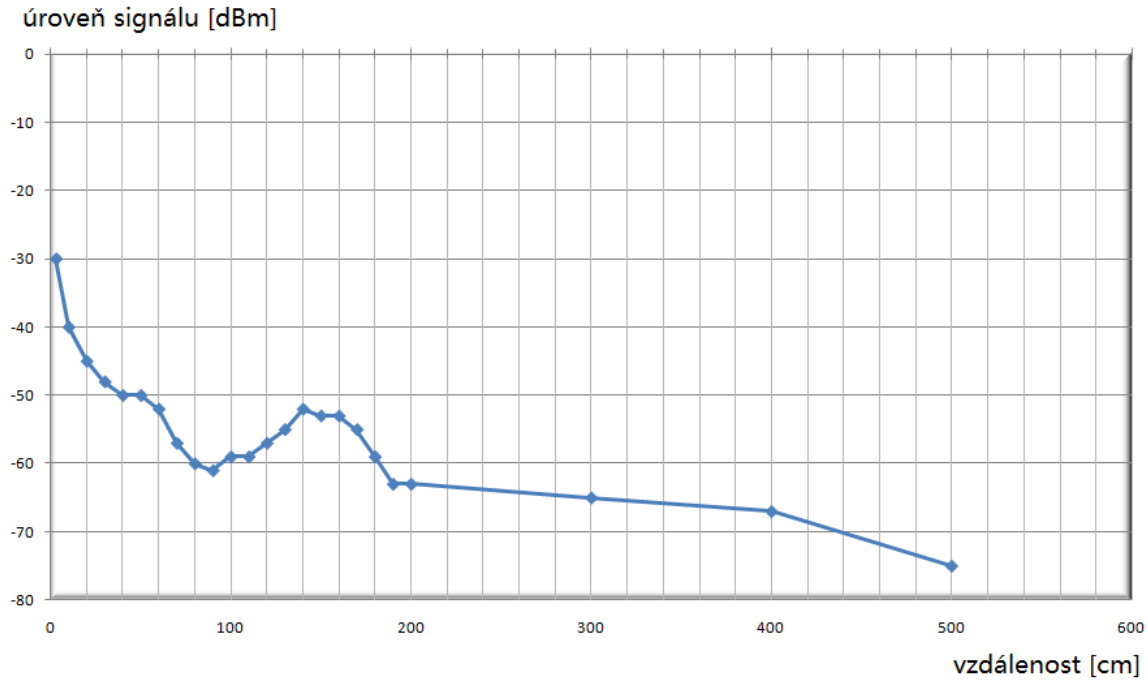


Obr. 25 Radiomikrofon MR-M3(bez baterií)

4.4.2 Měření úrovně signálu odposlechového prostředku MR-M3

Měření bylo prováděno za pomocí spektrálního analyzátoru R&S FS300 a všesměrového dipólu a bylo uskutečněno v tělocvičně v budově UTB na Jižních svazích ve Zlíně. Tělocvična byla zvolena proto, že se nejvíce podobá volnému prostranství – žádný nábytek a překážky. Měření nebylo prováděno na volném prostranství, protože jsme neměli k dispozici bateriový frekvenční analyzátor. Radiomikrofon MR-M3 byl umístěn ve vertikální polarizaci na stojanu ve výšce 1,5m, anténa byla umístěna taktéž na stojanu ve stejné výšce, vzdálenost se měnila po 10cm až do 2m, pak po 1m až do 5m, poté po 5m do 15m a byly zaznamenávány hodnoty úrovně signálu v jednotlivých vzdálenostech. Naměřené hodnoty jsou vyneseny do grafu. Teoreticky by měla úroveň klesat podle mocninné funkce, ovšem ne vždy se tak děje. To může být způsobeno různými odrazy elektromagnetických vln od různých ploch v místnosti a jejich následným skládáním a vznikem maxima a minima vysílaného signálu. Paradoxně tedy ne vždy menší vzdálenost vysílače a přijímače znamená silnější signál.

Obr. 26 Spektrální analyzátor R&S FS300



Obr. 27 Graf závislosti úrovně signálu na vzdálenosti

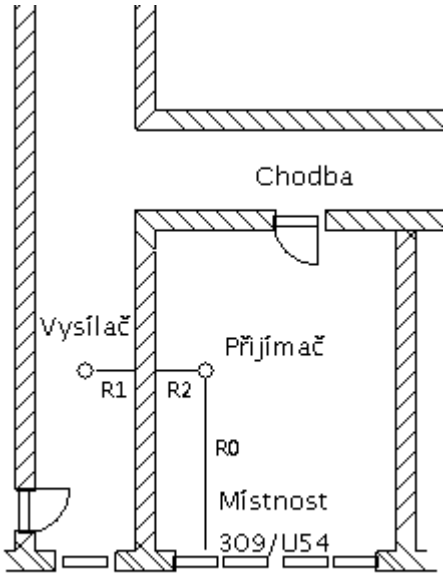
vzdálenost R [cm]	úroveň signálu [dBm]	vzdálenost R [cm]	úroveň signálu [dBm]
3	-30	130	-55
10	-40	140	-52
20	-45	150	-53
30	-48	160	-53
40	-50	170	-55
50	-50	180	-59
60	-52	190	-63
70	-57	200	-63
80	-60	300	-65
90	-61	400	-67
100	-59	500	-75
110	-59	1000	-79
120	-57	1500	-81

Tab. 6 Tabulka závislosti úrovně signálu na vzdálenosti

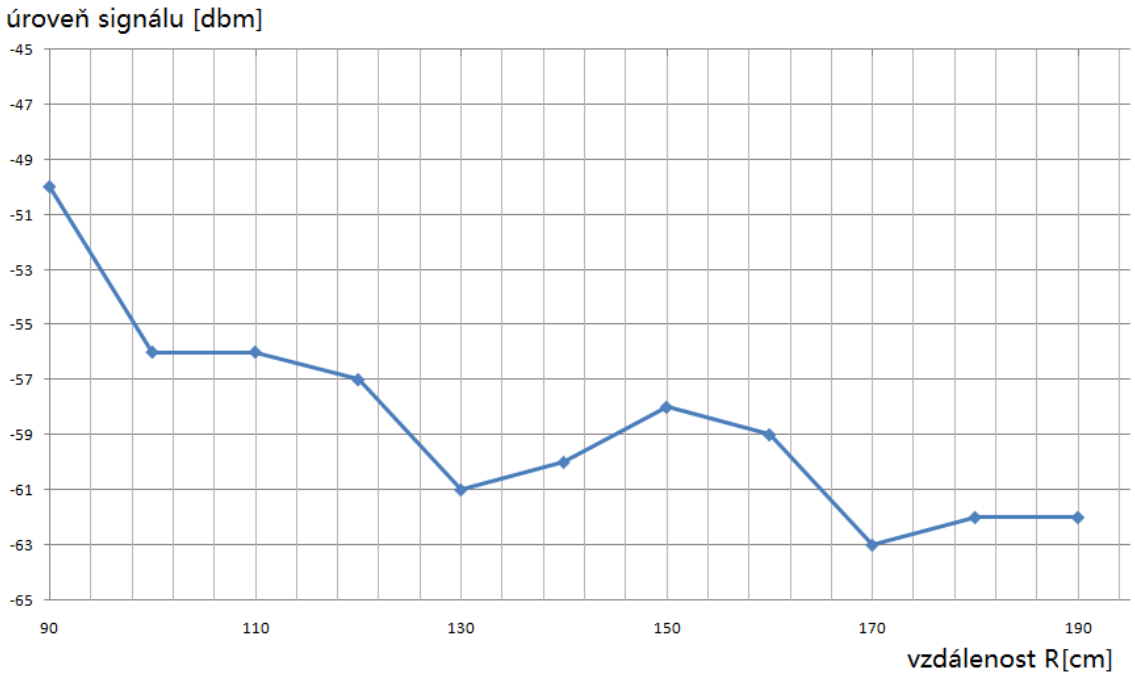
4.4.3 Měření šíření signálu přímou cestou s účinkem útlumu stěn

Měření bylo uskutečněno v místnosti 309/U54 v budově UTB na Jižních svazích ve Zlíně. V místnosti byl umístěn spektrální analyzátor R&S FS300 a všesměrový dipól, který byl umístěn na stojanu ve výšce 1,7m a ve vzdálenosti 0,5m od stěny a 3,3m od oken. Stěna byla zhruba 40cm silná a na druhé straně na chodbě byl na stojanu umístěn radiomikrofon

MR-M3, který byl umísťován do různých vzdáleností od stěny. Polarizace byla opět vertikální. Na spektrálním analyzátoru byla navolena frekvence radiomikrofonu, tedy 417MHz a měřena úroveň signálu při průniku zdí a různých vzdálenostech vysílače od zdi. Naměřené hodnoty jsou vyneseny do grafu. Pokusným měřením bylo vyloučeno šíření difrakční cestou, signál se tedy šířil přímo přes zeď.



Obr. 28 Nákres místnosti měření



Obr. 29 Graf závislosti úrovně signálu na vzdálenosti při průchodu zdí

vzdálenost R_1 [cm]	vzdálenost R [cm]	úroveň signálu[dBm]
0	90	-50
10	100	-56
20	110	-56
30	120	-57
40	130	-61
50	140	-60
60	150	-58
70	160	-59
80	170	-63
90	180	-62
100	190	-62

Tab. 7 Měření útlumu zdi

R – celková vzdálenost vysílače a přijímače

$$R = R_1 + R_s + R_2$$

R_1 – vzdálenost vysílače od stěny

R_s – tloušťka stěny, 40cm

R_2 – vzdálenost přijímače (antény) od stěny, 50cm

4.4.4 Porovnání výsledků předchozích měření – útlum zdi

vzdálenost R [cm]	úroveň signálu bez zdi[dBm]	úroveň signálu přes zeď[dBm]	útlum zdi [dB]
90	-61	-50	11
100	-59	-56	3
110	-59	-56	3
120	-57	-57	0
130	-55	-61	***-6***
140	-52	-60	***-8***
150	-53	-58	***-5***
160	-53	-59	***-6***
170	-55	-63	***-8***
180	-59	-62	***-3***
190	-63	-62	1

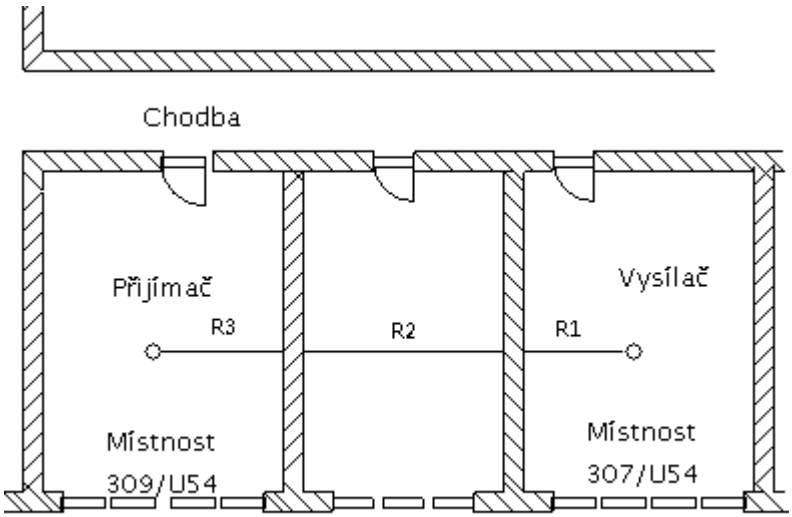
Tab. 8 Porovnání výsledků

Naměřené hodnoty úrovně signálu byly překvapující, zejména u vzdáleností 90 až 120cm, kdy se vysílač nacházel v blízkosti zdi, tedy od 0 do 20cm. Při těchto vzdálenostech zeď nevykazovala žádný útlum, ale dokonce zesílení. To je dáno pravděpodobně tím, že

radiomikrofon byl umístěn příliš blízko stěny a ta paradoxně fungovala jako plošný zářič - anténa. Při porovnání grafů z předchozíhoměření máme podobné křivky. Kolem hodnoty 150cm máme místní maxima, takže v jeho okolí určíme útlum stěny. Útlum stěny je rozdíl mezi úrovněmi signálu bez zdi a se zdí, průměrná hodnota je tedy kolem ***-6dB.***

4.4.5 Měření šíření signálu s účinkem útlumu dvou stěn

Měření bylo uskutečněno v místnostech 307/U54 a 309/U54 v budově UTB na Jižních svazích ve Zlíně. V místnosti 309/U54 byl umístěn spektrální analyzátor R&S FS300 a všesměrový dipól, který byl umístěn přibližně do středu místnosti, radiomikrofon MR-M3 byl umístěn taktéž přibližně do středu místnosti 307/U54. Vysílaný signál tedy musel buď projít oken, šířit se venkovním prostředím a pak opět oknem do místnosti přijímače, nebo přes 2 zdi 40cm silné.



Obr. 30 Nákres místností měření

Vzdálenosti R_1 a R_3 jsou přibližně 3,7m, R_2 je 8m.

Početní předpoklad:

$$E_2 = \frac{\sqrt{30 \cdot P \cdot D}}{R_1 + R_2 + R_3 + 2 \cdot R_s} = \frac{\sqrt{30 \cdot 10 \cdot 10^{-3} \cdot 3{,}28}}{3{,}7 + 8 + 3{,}7 + 2 \cdot 0{,}4} = 0{,}06 V/m$$

$$P_2 = \frac{(E_2 \cdot l_{ef} \cdot k)^2}{R_a} = \frac{(0{,}06 \cdot 0{,}12 \cdot 0{,}5)^2}{37} = 3{,}5 \cdot 10^{-7} W$$

$$P_{2dB} = 10log\left(\frac{P_2}{0{,}001}\right) = 10log\left(\frac{3{,}5 \cdot 10^{-7}}{0{,}001}\right) = -34dBm$$

Od této hodnoty musíme ještě odečíst 20dB z důvodu překážek po cestě a dalších 20dB vlivem umístění mikrofonu, pak ještě útlum 2 stěn zjištěný předchozím měřením, tedy 2x(-6)dB.

$$P_{2dB} = -34 - 40 - 12 = -86dBm$$

Předpoklad tedy je, že úroveň signálu se bude pohybovat kolem -86dBm, jestliže signál půjde přímou cestou, tedy projde 2 stěnami.

Předpoklad podle předchozích měření

V předchozím měření, bylo zjištěno, že úroveň signálu ve volném prostranství je ve vzdálenosti 15m -81dBm. Dále byl zjištěn útlum stěny, který je -6dB, musíme tedy odečíst útlum dvou stěn.

$$P_{2dB} = -81 - 12 = -93dBm$$

Měřením bylo zjištěno, že měřený signál je velmi slabý a téměř se ztrácí v šumu, jeho hodnota byla naměřena ***-95dBm***. Výkon vysílače byl tedy malý, dosah nestačil na překonání 2stěn a vzdálenosti přibližně 16m. Hodnota se velmi podobala předpovědi provedené podle předchozích měření, útlum stěny je tedy opravdu kolem ***-6dB***.

5 LEGISLATIVNÍ ROZBOR

5.1 Ochrana informací

Listina základních práv a svobod jako samostatný ústavní zákon je nejvyšší českou právní normou, v níž jsou zakotveny základní podmínky užívání informací.

Lidská důstojnost člověka, jeho osobní čest, dobrá pověst, jméno a soukromí jsou chráněna ustanoveními článku 10. 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.

Článek 13 je dalším článkem, který se zabývá informacemi, která říká, že „nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů“, které 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.

Informacemi se také zabývá článek 17 v druhém oddílu, který pojednává o politických právech. 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. [12]

5.2 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 případě, 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]

5.3 Zákony umožňující používání odposlechu

a) 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]

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

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

c) 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]

d) 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]

e) 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]

5.4 Zákony přikazující ochranu proti odposlechu

a) 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

5.5 Postup policie při vyžadování

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

Vývoj elektrotechniky v posledních letech, tedy i vývoj prostředků pro hlasový odposlech, umožňuje bezproblémový, snadný, stále rafinovanější a poměrně levný způsob, jak získat důležité informace. Dnešní odposlechová zařízení a radiomikrofony mají miniaturní velikost, mohou být tedy velmi dobře schovány v zájmovém prostoru a podle způsobu napájení i velmi dlouho fungovat bez objevení. Informace nemusí vždy unikat pouze technickými prostředky, ale také samotnými zaměstnanci. Firmy by se měly začít zabývat tím, jaké následky, zejména finanční, by mohla krádež informace a její zneužití mít.

V práci byly také popsány způsoby ochrany proti odposlechu a zásady provádění obranně technické prohlídky. Bylo zjištěno, že by měla být hlavně dodržována režimová opatření, aby byl zamezen přístup nepovolaných osob, zvláště do manažerských kanceláří a zasedacích místnosti, ve kterých se probíhají důležitá jednání. Takové místnosti by měly být vybaveny přehledovým přijímačem a pravidelně by v nich měla probíhat obranně technická prohlídka, jejíž zásady jsou v práci popsány. Důležitou součástí každé OTP je zejména radiová analýza, proto je v práci popsáno několik způsobů a zařízení pro její provádění. Zařízení na ochranu proti odposlechu mohou mít jen zlomkovou cenu v porovnání s cenou odcizené informace. Byla provedena také pokusná měření, která měla za úkol zjistit, jak se elektromagnetické vlny šíří při průchodu zdmi. Byl navržen způsob, jak předpovědět úroveň signálu radiomikrofonu v okolních místnostech. Některá měření ovšem prokázala, že šíření elektromagnetických vln je poměrně složitá problematika, některé naměřené hodnoty se hodně lišily od předpokladů. Měřením ovšem bylo zjištěno, že útlum cihlové stěny je při frekvenci 418MHz je -6dB, což je hodnota udávaná v literatuře.

Obranně technická prohlídka tedy je velmi odborná a složitá činnost, je tedy vhodné využít služeb firem zabývajících se touto problematikou.

ZÁVĚR V ANGLIČTINĚ

Electrotechnics development of late years, then also development of devices for vocal tapping, makes it possible to troublefree, easy, sophisticated and relatively cheap way, how obtain important information. Today's tapping devices and radiomicrophones have miniature size, then can be very well hidden in a room and according power supply can have the duration function without detection. Information doesn't run out only technical devices, but also by staff. Firms would have start speculate on aftermath and misuse, especially financial, would information theft have.

Types of protection against tapping were described in thesis and fundamentals of of the defense technical inspection. It was ascertained, it should had be adhere authoritarianism, prohibit an entry unauthorized persons, especially to the managerial office and boardroom, in which proceed important discussion. These rooms would have be equipped overview acceptor and the defense technical inspection would have be periodic, whose fundamentals were desscribed in this thesis. Important part of every defense technical inspection is especially a radium analysis, therefore some ways and devices were describe in the thesis. Devices for protection against tapping can be cheap as compared to price of information. Some experimental metering were made, how electromagnetic waves propagate through walls in buildings. A way was designed , how foretell signal level of radiomicrophone in surrounding rooms. Some metering proved, that the electromagnetic wave propagation is relatively complicated problems, some measured results differed from presumptions. It was ascertained by metering, that the electrical attenuation of brick wall stand by frequence 418MHz is -6dB, which is value from literature.

The defense technical inspection is very special and complicated activity, it is better to employ services of firms conversant by these problems.

SEZNAM POUŽITÉ LITERATURY

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

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

[5] SPY VPH, *Speciální technika a služby,* [online], [cit. 2009-03-15].

Dostupný z WWW: <http://spy.vph.cz/>

[6] Česká komora detektivních služeb, [online], [cit. 2009-02-05].

Dostupný z WWW: <http://www.ckds.cz/>

[7] Firemní materiály - ELBI Electronics, *Výrobce přístrojů proti odposlechu,* [online]. Dostupný z WWW: < http://www.elbi.cz/>

[8] Firemní materiály - ROHDE & SCHWARZ - Praha, s.r.o., *Výrobce elektronických testovacích a měřicích přístrojů,* [online].

Dostupný z WWW: < http://www.rohde-schwarz.cz/cz/>

[9] MobilMania. *Mobilní zločiny: jak odposlechnout mobil,* [online], [cit. 2009-03-20]. Dostupný z WWW:<http://www.mobilmania.cz/default.aspx?article=1104440>

[10] Odposlechy.com, *Speciální technika a služby,* [online], [cit. 2009-03-15].

Dostupný z WWW: < http://www.odposlechy.com/>

[11] Detekce.com, *Speciální technika a služby,* [online], [cit. 2009-03-15].

Dostupný z WWW: < http://www.detekce.com/>

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

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

[14] *Poznámky ze studia předmětu Nadstandardní prvky objektové bezpečnosti*

[15] Infosafe.cz , *Ochrana proti odposlechu a úniku informací,* [online], [cit. 2009-15-03]. Dostupný z WWW: < http://infosafe.cz/>

[16] ELMES Praha s.r.o., *Bezpečnostní technika,* [online], [cit. 2009-03-15]. Dostupný z WWW: <http://www.elmes.cz/>

[17] COMEFLEX CONSULTING s.r.o., *Detektivní a bezpečnostní služby,* [online], [cit. 2009-01-04]. Dostupný z WWW: <http://www.comeflex.com/>

[28] Aleš Dudáček, *Komunikační systémy v PO.* Vysoká škola báňská – Technická univerzita Ostrava, 2000. [online], [cit. 2009-04-15]. Dostupný z WWW: http://homen.vsb.cz/~www547/WEB/TEXTY/KS/KomSyst.htm

[19] Uhf.cz, *Radiové vysílání,* [online], [cit. 2009-04-15]. Dostupný z WWW: < http://uhf.cz/>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

FM	Frekvenční modulace
AM	Amplitudová modulace
OTP	Obranně technická prohlídka
VF	Vysokofrekvenční
UHF	Ultra High Frequency
VHF	Very High Frequency
EZS	Elektrická zabezpečovací signalizace
EPS	Elektrická požární signalizace
GSM	Global System for Mobile Communications
NMT	Nordic Mobile Telephone
UMTS	Universal Mobile Telecommunications System
SMS	Short message services
EM	Elektromagnetický
PC	Personal computer

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: POUŽÍVANÁ KMITOČTOVÁ PÁSMA

3 - 30 kHz	VLF velmi dlouhé vlny
30 - 300 kHz	DV dlouhé vlny (LF)
150 - 420 kHz	rozhlasové vysílání dlouhých vln radionavigační námořní a letecké služby
262 - 282 kHz	český rozhlasový vysílač DV 272 kHz
300 - 3000 kHz	SV střední vlny (MF)
490 - 510 kHz	tísňový k. 500 kHz pro radiotelegraf
525 - 1605 kHz	rozhlasové vysílání - SV
1605 - 2170 kHz	telekomunikace
1750 - 1950 kHz	radioamatéři (pásmo 160m)
2170 - 2194 kHz	tísňový k. 2182 kHz pro radiotelegraf
2194 - 2498 kHz	telekomunikace
2498 - 2502 kHz	vysílání kmit. normálu 2500 kHz
2504 - 3125 kHz	civilní a vojenské letectvo
3,000 - 30,00 MHz	KV krátké vlny (HF)
3,000 - 3,500 MHz	civilní a vojenské letectvo
3,500 - 3,800 MHz	radioamatéři (pásmo 80m)
3,950 - 4,000 MHz	rozhlasové vysílání
4,000 - 4,700 MHz	vojáci a letectvo
4,750 - 4,995 MHz	rozhlasové vysílání (pásmo 49m)
4,995 - 5,005 MHz	vysílání kmitočtového normálu 5000 kHz
5,005 - 5,900 MHz	telekomunikace, vojáci a letectvo
5,950 - 6,200 MHz	rozhlasové vysílání (pásmo 41m)
6,200 - 7,000 MHz	telekomunikace, vojáci a letectvo
7,000 - 7,100 MHz	radioamatéři (pásmo 40m)
7,100 - 7,300 MHz	rozhlasové vysílání
7,300 - 9,500 MHz	telekomunikace, vojáci a letectvo
9,500 - 9,775 MHz	rozhlasové vysílání (pásmo 31m)
9,995 - 10,005 MHz	kmitočtový normál 10000 kHz
10,005 - 11,700 MHz	vojáci a letectvo
11,700 - 11,975 MHz	rozhlasové vysílání (pásmo 25m)
12,000 - 14,000 MHz	průmyslové, vědecké a lékařské využití
14,000 - 14,350 MHz	radioamatéři (pásmo 20m)

14,350 - 14,990 MHz	telekomunikace a vojáci
14,990 - 15,010 MHz	kmitočtový normál 15000 kHz
15,100 - 15,450 MHz	rozhlasové vysílání (pásmo 19m)
15,450 - 17,700 MHz	telekomunikace a vojáci
17,700 - 17,900 MHz	rozhlasové vysílání (pásmo 16m)
17,900 - 19,990 MHz	telekomunikace, vojáci a letectvo
19,990 - 20,010 MHz	kmitočtový normál 20000 kHz
20,004 - 20,010 MHz	tísňový kmitočet pro kosmické lodi
21,000 - 21,450 MHz	radioamatéři a amat. družice (pásmo 15m)
21,450 - 21,750 MHz	rozhlasové vysílání
24,990 - 25,010 MHz	kmitočtový normál 25000 kHz
25,600 - 26,100 MHz	rozhlasové vysílání
26,965 - 27,405 MHz	pásmo CB pro občanské radiostanice
28,000 - 29,700 MHz	radioamatéři (pásmo 10m)
30 - 300 MHz	VKV velmi krátké vlny (VHF)
30,0 - 33,0 MHz	kosmické spoje
33,0 - 48,0 MHz	vojáci a policie
46,0 - 49,0 MHz	bezšňůrové telefony
48,5 - 66,0 MHz	televize I. pásmo (1 a 2 kanál)
66,0 - 73,0 MHz	rozhlasové vysílání I. pásmo VKV
73,0 - 87,5 MHz	záchranná služba, policie
75,0 MHz	letecká navigace
76,0 - 100,0 MHz	televize II. pásmo (3,4,5, kanál)
88,0 - 104,0 MHz	rozhlasové vysílání II. pásmo VKV
104,0 - 144,0 MHz	vojáci a letectvo
108,0 - 112,0 MHz	civilní letectvo
118,0 - 136,9 MHz	civilní letectvo
144,0 - 146,0 MHz	radioamatéři a amat. družice (pásmo 2m), radiotelefony
146,0 - 174,0 MHz	telekomunikace, vojáci, říční plavba
174,0 - 230,0 MHz	televize III. pásmo (6-12 kanál)
230,0 - 420,0 MHz	radioreleové spoje
300 - 3000 MHz	UKV decimetrové vlny (UHF)
329,0 - 335,0 MHz	civilní letectvo
432,0 - 438,0 MHz	radioamatérské pásmo

450 – 485 MHz	radiotelefony
470,0 - 622,0 MHz	televize IV. pásmo (21-39 kanál)
622,0 - 790,0 MHz	televize V. pásmo (40-60 kanál)
790,0 - 958,0 MHz	televize (61-81 kanál)
900 MHz	bezšňůrové telefony
895 – 904 MHz	radiotelefony
960,0 - 1215,0 MHz	letecké radionavigace
1215,0 - 1300,0 MHz	radioamatéři (pásmo 24cm)
1300,0 - 1400,0 MHz	řízení letového provozu
2300,0 - 2450,0 MHz	radioamatéři (pásmo 12cm)
3 - 30 GHz	SHF centimetrové vlny

PŘÍLOHA P II: CENÍK SPECIÁLNÍ TECHNIKY

SafeCom s.r.o.

Kód výrobku	NABÍDKA PODLE KATEGORIÍ VÝROBKŮ	Cena Kč	Cena Kč s DPH
1. ODPOSLECHOVÁ ZAŘÍZENÍ MÍSTNOSTI			
Miniaturní drátové mikrofony			
TECT	Elektretový supercitlivý miniaturní mikrofon s kabelem	1 500	1 830
PRZES	Předzesilovač elektretového mikrofonu	500	595
MAS	Souprava drátového mikrofonu se zesilovačem	19 700	24 034
BW 80	Souprava drátového mikrofonu s předzesilovačem a magnetofonem	53 428	65 182
VOICE ACELER.	Souprava drátového mikrofonu a předzesilovače	13 432	16 387
Vysílače stabilizované			
MUD-R	Vysílač stabilizovaný, 429 MHz, 3V knoflík, 100 hod, 100-200 m	8 000	9 760
MUD-A	Vysílač stabilizovaný, 429 MHz, 9V destičková, 12 hod, 50-80 m	9 000	10 980
MUD-B	Vysílač stabilizovaný, 429 MHz, 9V destičková, 6 hod, 150-200 m	10 500	12 810
MUD-C	Vysílač stabilizovaný, 429 MHz, 9V destičková, 3 hod, 400-600 m	11 500	14 030
MUD-A/AVC	Vysílač MUD-A s kompresorem dynamiky	9 500	11 590
MUD-B/AVC	Vysílač MUD-B s kompresorem dynamiky	11 000	13 420
MUD-A/AVC	Vysílač MUD-C s kompresorem dynamiky	12 000	14 640
TX OEM mini	Vysílač TX OEM mini	12 000	14 640
TX OEM mili	Vysílač TX OEM mili	12 000	14 640
MUD-ORG	Vysílač stabilizovaný 429 MHz s AVC zabudovaný v koženém diáři	15 000	18 300
MUD-BAT	Vysílač stabilizovaný 429 MHz zabudovaný v akumulátoru NOKIA 6210	16 000	19 520
TX rozdvojka	Vysílač TX 10 mW a zdroj zabudovaný do rozdvojky	12 000	14 640
TX kryt zásuvky	Vysílač TX 10 mW a zdroj zabudovaný do krytu zásuvky	12 000	14 640
TX prodlužovačka	Vysílač TX 100 mW a zdroj zabudovaný do prodlužovačky	12 000	14 640
MUD-UT	Vysílač 20 mW s utajovačem a interface	12 000	14 640
MUD-PERO	Vysílač v kuličkovém peru	12 000	14 640
UXB	Radiový vysílač s baterií	24 953	30 443
UXB(S)	Radiový vysílač s baterií a scramblerem	33 131	40 420
UXP	Radiový vysílač v peru	38 922	47 485
UXC 1	Radiový vysílač v kapesní kalkulačce	38 444	46 902
UXC 1 (S)	Radiový vysílač v kapesní kalkulačce se scramblerem	47 757	58 263
UXC 2	Radiový vysílač ve stolní kalkulačce	38 444	46 902
UX-CARD	Radiový vysílač ve tvaru kreditní karty	39 877	48 650
UXM	Radiový vysílač s napájením z el. vedení	37 728	46 028
UXM(S)	Radiový vysílač s napájením z el. vedení se scramblerem	46 861	57 171
Laser 3V	Baterie pro UXB	418	510
Silver 2CR 6V	Baterie pro UXR1	358	437
RBC	Odposlechový kufřík s vysílačem a nahráváním (bez nahrávače)	58 502	71 373
S-AB	Krystalem řízený vysílač o rozměrech 59x30x13 mm	29 961	36 553
S-AH	Krystalem řízený vysílač o rozměrech 59x30x13 mm	33 069	40 344
S-AN	Krystalem řízený vysílač o rozměrech 59x30x13 mm	41 399	50 506
S-AC	Krystalem řízený vysílač o rozměrech 50x30x25 mm	30 003	36 603
S-AJ	Krystalem řízený vysílač o rozměrech 50x30x25 mm	33 069	40 344
S-AU	Krystalem řízený vysílač o rozměrech 50x30x25 mm	41 399	50 506
S-AE	Krystalem řízený vysílač o rozměrech 55x29x25 mm, VOX	37 482	45 729
S-AK	Krystalem řízený vysílač o rozměrech 55x29x25 mm, VOX	41 896	51 113
S-AR	Krystalem řízený vysílač o rozměrech 55x29x25 mm, VOX	52 049	63 499
S-AF	Krystalem řízený dálkově spínaný vysílač o roz. 65x45x17 mm	144 626	176 443
S-AL	Krystalem řízený dálkově spínaný vysílač o roz. 65x45x17 mm	149 039	181 828
S-AS	Krystalem řízený dálkově spínaný vysílač o roz. 65x45x17 mm	163 916	199 977

S-AG	Krystalem řízený dálkově spínaný vysílač o roz. 50x47x14 mm	144 626	176 443
S-AM	Krystalem řízený dálkově spínaný vysílač o roz. 50x47x14 mm	149 039	181 828
S-AY	Krystalem řízený dálkově spínaný vysílač o roz. 50x47x14 mm	157 700	192 394
S-AZ	Krystalem řízený vysílač pro monitorování tel. linky a místnosti	40 404	49 293
Soupravy digitálních vysílačů a přijímačů			
DHPS 11X	Digitální vysílač s dálkovou aktivací a frekvenčním hoppingem	60 000	73 200
DIG 1/4 Verz.3	Digitální vysílač s dálkovou aktivací, přijímač a opakovač	60 000	73 200
DIG-Tr	Samostaný další vysílač k soupravě DIG 1/4	20 000	24 400
TDK, RDK	Vysílač s digitální modulací a přijímač	40 000	48 800
Vysílače po vedení			
MC 06	Souprava přijímače a šesti vysílačů s přenosem po síti 220V	220 545	269 065
MCX-06	Vysílač k soupravě MC 06	32 448	39 587
MCR-06	Šestikanálový přijímač 60 kHz - 200 kHz	74 256	90 592
S-TUS	Vysílač využívající jako přenosové cesty telefonní linku	61 124	74 571
Odposlech pomocí GSM MT			
GSM PQ3/M5	Upravený mobilní telefon pro odposlech prostor	87 431	104 043
GSM PQ3/M6	Upravený mobilní telefon pro odposlech prostor s automatickou aktivací	97 146	115 604
Směrové mikrofony			
DSM-19	Souprava parabolického mikrofonu s nahráváním	51 811	61 655
Kontaktní mikrofony			
WCA-2	Zesilovač pro odposlech skrz zeď s citlivým mikrofonem a ekvalizerem	18 000	21 960
S-AD	Kontaktní mikrofon s vysílačem o rozměrech 59x30x13 mm	34 851	42 518
S-AI	Kontaktní mikrofon s vysílačem o rozměrech 59x30x13 mm	38 788	47 321
S-AO	Kontaktní mikrofon s vysílačem o rozměrech 59x30x13 mm	48 506	59 177
2. ODPOSLECHOVÁ ZAŘÍZENÍ TELEFONU			
Telefonní nahrávače			
MOHO	Interface pro připojení diktafonu k telefonní lince	1 800	2 196
MOHOS	Interface pro připojení diktafonu ke kabelu telefonního sluchátka	985	1 202
TCM-50DV	Kazetový diktafon na běžnou kazetu	3 300	4 026
DS-330	Digitální nahrávač na pevnou paměť 5hod,30min, USB rozhraní	7 010	8 552
DS-2000	Digitální nahrávač na kartu SmartMedia 64MB, USB rozhraní	11 464	13 986
DM-1	Digitální nahrávač na kartu SmartMedia 128MB, MP-3, USB	11 464	13 986
SMART SPY	Nahrávač telefonních hovorů na Flash karty	49 140	59 951
REM REC	SW pro nahrávání a archivaci audio vstupu do PC	1 500	1 830
FOX	Software pro převod nahrávky fax. přenosu z formátu WAV do TIFF	204 750	249 795
Telefonní odposlechové vysílače nestabilizované			
S-102 TR	Vysílač napájený z telefonní linky	16 058	19 591
RICEGRAIN	Subminiaturní vysílač telefonních hovorů	10 256	12 513
	Telefonní odposlechové vysílače stabilizované		
TX TLF rozdvojka	Radiový vysílač v tlf. rozdvojce	29 490	35 978
TX TLF spojka	Radiový vysílač ve spojce tlf. kabelu	29 490	35 978
UXT	Radiový vysílač napájen po tlf. lince	29 490	35 978
UX-AIT	Radiový vysílač napájen baterií, pro digit.telefony	50 742	61 905
S-AZ	Krystalem řízený vysílač pro monitorování místnosti a tel. linky	40 404	49 293
S-005	Krystalem řízený telefonní vysílač o rozměrech 30x20x10 mm	25 693	31 345
Telefonní odposlech po vedení			
ATRS	Přípravek k magnetofonu pro autom. přímé nahrávání tel. hovorů	13 133	16 022
ATRS(P)	Přípravek k magnetofonu pro autom. přímé nahrávání tel. hovorů	13 133	16 022
MITEL 02	Zařízení na monitorování tlf linky a místnosti	13 133	16 022
	Odposlech mobilních telefonů GSM		
GSM Interceptor	Zařízení na monitorování GSM mobilních telefonů	13 133	16 022
3. PŘIJÍMAČE			
Přijímače k vysílačům stabilizovaným			
DJ-496	Přijímač ALINCO 420-435 MHz, výstup na mgf	5 589	6 818
UXR 1	Dvoukanálový přijímač o rozměrech 48x66x19 mm	37 012	45 154
UXR 1(S)	Stejný jako UXR 1, signál je scramblován	47 757	58 263

UXR 3	Dvoukanálový citlivý přijímač	61 487	75 014
UXR 3(S)	Stejný jako UXR 3, signál je scramblován	70 441	85 938
SSV	Rozlišovač hovoru k UXR	45 667	55 714
UIR	Přijímač 2 vysílačů UX a 1 mikrofonem s telefonní komunikací	dotaz	dotaz
UIR-TS	Jako UIR, ale doplněno nahrávačem	277 586	338 655
Přijímače univerzální			
VOYAGER RY-630	Radiopřijímač pro příjem vysílačů v pásmu 535kHz - 218 MHz	5 397	6 584
AR 8200 MK3	Ruční scanner pro příjem vysílačů v pásmu 530 kHz - 3 GHz	22 188	27 069
AR8600 MK2	Stolní VHF/UHF komunikační přijímač 530kHz-2040MHz, RS232	38 028	46 394
AR 5000A	Stolní scanner pro příjem vysílačů v pásmu 10 kHz - 3 GHz	68 268	83 287
TRX-100	Ruční scanner pro příjem vysílačů v pásmu 100 kHz - 2,2 GHz	68 268	83 287
Příslušenství			
IEP	Skryté sluchátko s bezdrátovým přenosem	14 626	17 843
4. NAHRÁVACÍ TECHNIKA			
Kazetové magnetofony			
TCM-50DV	Kazetový magnetofon na běžnou kazetu, VOX, autoreverz	4 090	4 990
Digitální nahrávače			
DS-330	Digitální nahrávač na pevnou paměť 5hod,30min, USB rozhraní	7 010	8 552
DS-2000	Digitální nahrávač na kartu SmartMedia 64MB, USB rozhraní	11 464	13 986
DM-1	Digitální nahrávač na kartu SmartMedia 128MB, MP-3, USB	11 464	13 986
SmartMedia 128MB	Paměťová karta pro diktafon, kapacita 128MB	1 552	1 894
IO MONITOR	SW pro monitorování klávesnice PC	49 140	59 951
SMART SPY	Nahrávač na Flash karty	49 140	59 951
5. VIDEOTECHNIKA			
CCD Deskové kamery			
VCM36P	CCD1/3", ČB, f=3,7mm pinhole, napájení 1VDC, 380 TV řádek, zvuk	2 808	3 426
VCM36	CCD1/3", ČB, f=3,8mm, napájení 1VDC, 380 TV řádek, zvuk	2 808	3 426
217G	CMOS kamera 1/3", ČB, 380 řádků, f=3,6mm	3 338	4 072
217P	CMOS kamera 1/3", ČB, 380 řádků, f=5mm pinhole	3 338	4 072
617G	CMOS kamera 1/3", barevná, 380 řádků, f=3,6mm	4 462	5 444
264-P	CCD1/4", barevná, f=3,5mm-pinhole, zvuk, 12V DC	5 059	6 172
161/45e	1/4", barevná, f=4,5mm-pinhole, 330 TV řádek, napájení 5VDC	7 488	9 135
161/53e	1/4", barevná, f=4mm, 330 TV řádek, napájení 5VDC	9 048	11 039
Bezdrátový video-audio přenos			
Vysílače			
ProfiLink	Vysílač v hliníkovém pouzdru, 2,4 GHz, 25mW, Color+BW obraz, zvuk	11 638	14 198
ProfiLinkM3	Vysílač v hliníkovém pouzdru, 2,4 GHz, 25mW, Color+BW obraz, zvuk	11 638	14 198
ProfiLinkOEM	Minivysílač bez pouzdra, 2,4 GHz, 25mW, Color+BW obraz, zvuk	7 394	9 021
ProfiLink HO OEM	Minivysílač bez pouzdra, 2,4 GHz, 25mW, Color+BW obraz, zvuk	8 954	10 924
ProfiLink Outdoor	Vysílač - venkovní provedení, 2,4 GHz, 25mW, Color+BW obraz, zvuk	12 418	15 149
ProfiLink Cigar.box	Minivysílač v cigaretové krab., 2,4 GHz, 25mW, Color obraz, zvuk	29 297	35 742
Přijímače			
Profilink	Přijímač v hliníkovém pouzdru, 2,4 GHz, Color+BW obraz, zvuk	19 438	23 714
ProfiLinkM3	Přijímač v hliníkovém pouzdru, 2,4 GHz, Color+BW obraz, zvuk	14 758	18 004
ProfiLinkOEM	Minipřijímač bez pouzdra, 2,4 GHz, Color+BW obraz, zvuk	6 209	7 575
ProfiLink Outdoor DX	Přijímač - venkovní provedení, 2,4 GHz, Color+BW obraz, zvuk	26 863	32 773
ProfiLink LCD DX	Přijímač v Al pouzdru s LCD, 2,4 GHz, Color+BW obraz, zvuk	46 800	57 096

Speciální videotechnika			
SecurityLink 10W	Vysílač 10W, 2,3-2,4 a 2,4-2,5 GHz, v AL pouzdru, exter. Anténa	175 500	214 110
SecurityLink Multi	Přijímač pro SecurityLink 10W	46 706	56 982
SecurityLinkOEM160	Vysílač 160mW, nezapouzdřený, 2,3-2,6GHz, 16 kanálů, 12V	12 350	15 067
SecurityLinkHOOEM160	Vysílač 160mW, nezapouzdřený, 2,3-2,6GHz, 16 kanálů, 12V	12 350	15 067
SecerityLink OEM Rec	Přijímač nezapouzdřený, 16 kanálů, 2,3-2,6GHz, 7-30V DC	9 970	12 163
DTT 99	Generátor data, titulku, času DTT 99	1 750	2 135
VAM24N	Modulátor VAM24N	888	1 083
MRP LITE HW+SW	HW pro nahrávání 4 videosignálů na HD PC (Win2000/XP)	7 020	8 564
MRP LITE plus RT - HW+SW	HW pro nahrávání 4 videosignálů na HD PC v reálném čase (Win2000/XP)	8 190	9 992
MRP Standard SW+HW	SW pro nahrávání 9 videosignálů na HD PC	6 768	7 106
MRP Standard RT SW+HW	SW pro nahrávání 8 videosignálů na HD PC v reálném čase (Win2000/XP)	6 768	7 106
VDR ClipMaker	Přenosný digitální videorekorder	254 592	310 602
ViewLock	Utajovač bezdrátových videopřenosů	254 592	310 602
ViewLock audio	Utajovač bezdrátových video-audio přenosů	333 216	406 524

PŘÍLOHA P III: CENÍK PROHLÍDEK PROTI ODPOSLECHU

Probin s.r.o.

Stručný ceník, kompletní na www.probin.cz

Podlahová plocha (m^3)	Prohlídka	
	Základní	Kompletní
10	6 000 Kč	10 000 Kč
15	9 000 Kč	15 000 Kč
20	12 000 Kč	20 000 Kč
25	14 100 Kč	23 500 Kč
30	16 200 Kč	27 000 Kč
35	18 300 Kč	30 500 Kč
40	20 400 Kč	34 000 Kč
45	22 500 Kč	37 500 Kč
50	24 600 Kč	41 000 Kč
75	34 560 Kč	57 600 Kč
100	42 000 Kč	70 000 Kč
125	45 060 Kč	75 350 Kč
150	48 120 Kč	81 200 Kč
175	51 180 Kč	85 550 Kč
200	55 200 Kč	92 000 Kč
250	61 440 Kč	102 400 Kč
300	67 200 Kč	110 00 Kč
nad 300	dohodou	dohodou

Základní prohlídka proti zpravodajským technikám

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

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

Kompletní prohlídka proti zpravodajským technikám

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