Odposlechové zařízení v průmyslu komerční bezpečnosti

Sound detection apparatus in industry commercial safety

Ivan Domček

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

Jméno a příjmení:	**Ivan DOMČEK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Odposlechová zařízení v průmyslu komerční bezpečnosti.**

Zásady pro vypracování:

1. **Seznamte se s problematikou elektromagnetického záření odposlechových zařízení využívaných v PKB.**
2. **Uveďte a popište prostředky speciální odposlechové techniky.**
3. **Uveďte způsoby získavání informací využitím odposlechových systému, taktika nasazení zařízení do provozu.**
4. **Lokalizace odposlechových zařízení v prostoru.**
5. **Aplikace získaných poznatků a informací v oblasti odposlechových zařízení, nové trendy.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, F., KAMENÍK J. Komerční bezpečnost, Soukromná bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur, Nakladatelství Public History, ISBN 978-80-7357-309-6**
2. **BRABEC, F., LÁTAL, I. Bezpečnost pro firmu, úřad, občana, Nakladatelství Public History, Praha 2001, ISBN 80-86445-04-06**
3. **VÁŇA, J. Informace a ich ochrana, Bratislava, Akadémia Policajného zboru v Bratislave, 1999, ISBN 80-7318-269-6**
4. **LÁTAL, I. a kol. Ochrana informací, dat a počitačových systémů, Praha, Eurounion, 1996, ISBN 80-85858-32-0 2**
5. **ČECH B. Vybrané technické prostředky využívané v bezpečnostní praxi, skripta**
6. **PA ČR Praha, Praha 2000, ISBN 80-7251-115-7 3**

Vedoucí bakalářské práce: **Ing. Ján Ivanka**
Ústav elektrotechniky a měření

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

Termín odevzdání bakalářské práce: **20. května 2009**

Ve Zlíně dne 20. února 2009

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Předmětem bakalářské práce je seznámení s problematikou odposlechových zařízení, jejich instalaci do provozu, taktéž příjem signálu z odposlechů, získávaní citlivých informaci, provádění obranně technické prohlídky, vyhledávaní odposlechových prostředků za pomoci detektoru vysokofrekvenčního pole a paměťového radiového analyzátore. V práci je způsob jak za pomoci speciální techniky uchráníme informace v jednacích místnostech. V teoretické části se zajímám o elektromagnetického záření. V praktické části nasazuji speciální technické bezpečnostní prostředky.

Klíčová slova: odposlechové zařízení, nasazení odposlechových zařízení, obranně technická prohlídka

ABSTRACT

The subject of thesis is familiar with the issues sound detections apparatus, their installation commissioning, also receiving the signal from the sound detections apparatus, obtaining sensitive information, conduct technical inspections defense. Then search sounddetections devices with the help of high-frequency detector and spectral analyzer. Form how with the help of special techniques save information in the meeting room. In the theoretical part are interested of electromagnetic radiation. In the practical part instaling special technical security apparatus. Locates sounddetections facility with the help of Defense technical inspections at the premises in the U5.

Keywords: sounddetections equipment, instal sounddetections equipment, Defense Technical Inspection

Poděkování

Poděkování patří vedoucímu bakalářské práci panu Ing. Jánovi Ivankovi, za odborné rady, za vedení a za cenné připomínky.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

V dnešní době informační technologie a možností komunikace je zcela nevyhnutné chránit své informace. Průmyslová špionáž je v současné době velmi dobře placené řemeslo. Průmyslová špionáž se praktikuje ve všech úrovních a zabývají se ji vlády, mezinárodní organizace i jednotlivci. Dnešní vyspělá technika je na takové úrovni, že získat kvalitní prostředek speciální odposlechové a jiné dokumentační techniky je víc než jednoduché. Hlavně při konkurenčním boji se využívají nekalé praktiky s využitím odposlechové techniky. Každý manager by měl mít na mysli ochranu informací, prevence proti špionáži a dostatečně technicky vybavené prostory v jednacích místnostech před odcizením informací, únikem informací a zneužitím informací. Někdy bývá ztráta tajných informací tak závažná, že se jedná o finančních ztrátách v milionech.

V teoretické části se věnuji elektromagnetickému záření a elektromagnetickému spektru, které má významně využití v odposlechové technice. Na ochranu informací v jednacích místnostech známe více typů ochran. Mezi nejspolehlivější metody patří Faradayova klec. Žádný signál nepronikne dovnitř ani ven. Faradayova klec je velmi nákladné řešení je a proto se v praxi využívají detektory a deaktivátory mobilních telefonů a šumový generátor. Ochrana prostorů můžeme udělat i tak, že před jednáním si zkontrolujeme prostor, zda tam není odposlechové zařízení. Na detekci využíváme radiový analyzátor, detektor vysokofrekvenčního pole a detektor nelineárních přechodů. Táto prohlídka se nazývá obranně technická prohlídka. V práci se seznamuji se speciálními prostředky odposlechové techniky. Popisuji miniaturní mikrofony a speciální přijímače

Cílem práce je prakticky využít dosáhnuté poznatky. V jednací místností rušit GSM pásmo za pomoci rušičky. Odposlechové zařízení odborně instalovat do provozu, profesionálně přijímat audio informaci a následně provést obranně technickou prohlídku a lokalizovat odposlechové zařízení.

Všechny měření se provádí v prostorách budovy U5.

I. TEORETICKÁ ČÁST

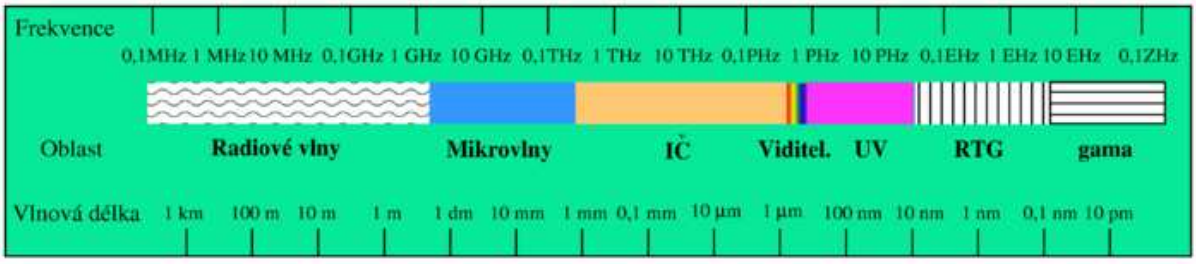
1 ELEKTROMAGNETICKÉ ZÁŘENÍ

1.1 DEFINICE ELEKTROMAGNETICKÉHO ZÁŘENÍ

Elektromagnetické pole je všude kolem nás. Elektromagnetické záření je kombinací příčného vlnění magnetického a elektrického pole tedy elektromagnetického. Elektromagnetické záření má velký rozsah vlnových délek, podle kterých rozlišujeme druhy elektromagnetického záření. Jakýkoli elektrický náboj pohybující se s nenulovým zrychlením vyzařuje elektromagnetické vlnění. Když vodičem (nebo jiným objektem, např. anténou) prochází střídavý elektrický proud, vyzařuje elektromagnetické záření o frekvenci proudu. Na elektromagnetické záření se stejně jako na cokoli jiného dá nahlížet jako na vlnu nebo proud částic. Jako vlnu je charakterizuje rychlost šíření (rovná rychlosti světla ve vákuu), vlnová délka a frekvence.[1]

1.2 ELEKTROMAGNETICKÉ SPEKTRUM

Elektromagnetické spektrum (někdy zvané Maxwellova duha) zahrnuje elektromagnetické záření všech vlnových délek. Elektromagnetické záření o vlnové délce λ (ve vakuu) má frekvenci f a jemu připisovaný foton má energii E.[2]



Obr. 1. Elektromagnetické spektrum.[2]

1.2.1 Radiové vlny

Radiové vlny jsou většinou vyzařovány anténami běžných délek, takže jejich vlnové délky jsou v rozmezí milimetrů až stovek metrů, tedy mají frekvence nižší než asi 300 GHz. Užívají se pro rozličné přenosy dat jako rádio, televize,mobilní telefony, amatérské rádio a mnoho jiných. Aby mohli přenášet data, nemůže byt signál stále stejný, ale musí byt modulován.[2]

1.2.2 Mikrovlny

Mikrovlny o frekvencích 3-300 GHz dělíme na SHF (3-30 GHz) a EHF (30-300 GHz). Mikrovlny jsou absorbovány molekulami tekutin, jež mají dipólový moment, zvláštně vody, toho se využívá k ohřívaní v mikrovlnné troubě. Mikrovlny se rovněž využívají pro bezdrátovou komunikaci zvanou Wi-Fi.[2]

1.2.3 Infračervené záření

Infračervené záření pokrývá frekvence 300 GHz až 400 THz. Dále se dělí na blízkou IČ, střední IČ , dalekou IČ.[2]

1.2.4 Viditelné světlo

Viditelné světlo o vlnových délkách 400-800 nm je světlo, na které je citlivé lidské oko. Viditelné světlo a blízce infračervené záření je absorbováno a emitováno elektrony v atomech a molekulách, když přecházejí mezi energetickými hladinami. Část elektromagnetického spektra se také označuje jako světelné spektrum. Jednotlivé barvy, vyskytující se ve světelném spektru se nazývají spektrálními barvami a odpovídají jim určité intervaly vlnových délek elektromagnetického záření.[2]

Barva	Vlnová délka	Frekvence
červená	~ 625 až 740 nm	~ 480 až 405 THz
oranžová	~ 590 až 625 nm	~ 510 až 480 THz
žlutá	~ 565 až 590 nm	~ 530 až 510 THz
zelená	~ 520 až 565 nm	~ 580 až 530 THz
azurová	~ 500 až 520 nm	~ 600 až 580 THz
modrá	~ 430 až 500 nm	~ 700 až 600 THz
fialová	~ 380 až 430 nm	~ 790 až 700 THz

Obr. 2. Viditelné světlo.[2]

1.2.5 Ultrafialové záření

Následuje ultrafialové záření o vlnových délkách 400-10 nm. Fotony tohoto záření mají vysokou energii a mohou proto ničit chemické vazby.[2]

1.2.6 Rentgenové záření

Rentgenové záření je záření o vlnových délkách 10-0,1 nm. Používá se pro dívání se přes některé materiály, rovněž tak v astronomii. Černé díry a neutronové hvězdy emitují rentgenové záření, což umožňuje jejich studium. Rentgenové záření využívají v medicíně a na letištích.[2]

1.2.7 Gama záření

Záření gama vznikající při radioaktivních a jiných jaderných a subjaderných dějích (jako je např. anihilace). Název vychází ze značení ionizujícího záření (ostatní druhy ionizujícího záření nejsou elektromagnetické povahy). Využívá se v neurochirurgie v přístroji Leksellův gama nůž.[2]

2 SPECIÁLNÍ TECHNIKA NA OCHRANU INFORMACÍ V JEDNACÍCH MÍSTNOSTECH

Důležitou části ochrany informací je zabezpečit jednací místnosti technickými prostředky bezpečnostního průmyslu. Po nainstalovaní speciální techniky je skoro nemožné získat informace nebo odposlouchávat takto zabezpečenou místnost.

2.1 Detektory a deaktivátory mobilních telefonů

Mobilní telefon je nedílnou součástí každého managera a může nám lehko sloužit jako odposlech. Odstínění GSM signálu je jednoduché řešení tohoto problému. Po zapnutí deaktivátora mobilních telefonů tzv. GSM Jammer se každý telefon dostane do stavu jako kdyby nebyla dostupná žádna síť. Rozsah zarušení 20-50 m v závislosti jaký je silní okolní signál mobilní sítě. V dnešní době se dostává do popředí síť 3. generácii UMTS, ale ten se dá vyrušit stejně jako GSM.

2.1.1 Příklad: Duální rušička mobilů GSM-2000 JAM

Duální rušička mobilů GSM-2000 JAM slouží k zarušení obou GSM pásem 900 MHz i 1800 MHz. Přenosná rušička je vybavená dvěmi laděními anténami s přibližně kulovou vyzařovací charakteristikou. Rušící signál je vysílán všesměrně. Systém je zabudován do hliníkové krabičky a je vybaven aktivním chladičem. Zařízení je vybaveno signalizací poruchy, která je aktivována v případě ztráty napájení nebo poruchy koncových zesilovačů.[3]

Technické parametry GSM-2000 JAM	
Frekvenční rozsah:	Pásmo GSM 900 MHz a 1800 MHz
Napájení:	12V / 0,7A
Přikon:	cca 8W, přistroj má aktivní chladič
Výstupní výkon (při 12V):	29-31 dBm na každé pásmo (cca 2 x 1W)
Rozměry:	72 x 75 x 35 mm (bez antén)

Délka všesměrových antén:	154 mm (900 MHz), 120 mm (1800 MHz)
Rozměry směrových antén (zisk 10 dB)	175 x 252 x 45 mm (900 MHz)
	99 x 141 x 30 mm (1800 MHz)
Vyzařovací úhel směrových antén:	cca 60° /horiz./ x 50° /vertik./ po pokles 3 dB

Obr. 3. Duální rušička mobilů GSM-2000 JAM.

2.2 Šumový generátor

Jednou z možností provádění odposlechu kontaktní či bezkontaktní snímaní akustických informací z skel nebo zdí objektu. Forma odposlechu nevyžaduje přímý průnik do zájmové oblasti. Pro svou činnost využívá skutečností, že zvuk je mechanické vlnění, které je možné na dálku snímat a zpětně převádět na užitečnou informací. Šumový generátor produkuje bílý šum, který dokáže hovor překrýt vlastním vlněním a zabránit tak, zpětnému převodu vlnění na akustickou informací. Nevýhodou je, že bílý šum je slyšitelný a uživateli se jeví jako zapnutá klimatizace.

2.2.1 Inteligentní výkonový šumový generátor SNG007

Šumový generátor SNG007 umožňuje připojení až 100 piezokeramických akustických měničů, 2-12 nízkoimpedančných reproduktorů nebo jich vzájemně kombinovat. Účinnost šumového generátoru SNG optimalizuje procesor, který v automatickém režime analyzuje zvuky v místností a zabezpečuje jenom takovú úroveň zašumění, která je nutně v závislostí na hlasitosti konverzací. Zařízení je konstruované k zavěšení na zeď nebo bok stolu v přímém dosahu uživatele. Z předního panelu je možné pomocí přepínačů zvolit nízký nebo vysoký výkon a obě úrovně je možné provádět manuálním nebo automatickým režimem.[4]

.

Technické parametry SNG007

Napájení:	12V
Odběr:	0,1-0,5 A
Výkon:	2 x 2 W /8 ohm
Kapacita:	100 piezomeničů
Výstupní signál:	spektrum až 40 V šš
Indikace:	5 x LED
Rozměry:	118 x 58 x 187 mm

Příslušenství: Piezokeramický akustický měnič, plastová krytka na akustický měnič, sada maskovacích reproduktorů.

Obr. 4. Šumový generátor SNG007.[5]

2.3 Faradayova klec

Jedná se o nejnáročnější a zároveň nespolehlivější ochranu proti odposlechu. Obvykle se postupe výběrem nejvhodnějších prostorů v objektů, provede se úprava elektroinstalací (do prostoru se přivede pouze jeden napájecí kabel, jsou odstraněna všechna ostatní síťová připojení, telefon a PC). Na toto vedení je připojen síťový filtr. Poté je na stěny místnosti instalována síť piezoiničů pro zamezení kontaktního snímaní informací z plašte místnosti, na ní je nalepená speciální měděná fólie. Táto fólie je překrytá omítkou, sádrokartonem. Do oken jsou instalovány speciální pokovená sklá a je provedena úprava dveří potažením samolepící fólií, případně se instalují speciální dveře a zárubně. Vše je uzemněno. Samozřejmě pro tuto místnost je naproste dodržování režimu vstupu a pobytu cizích osob v těchto prostorách. Optimální doplnění je rámový detektor kovů. Nevýhodou Faradayovy klece je finanční náročnost projektu.[6]

3 OCHRANA PROTI ODPOSLECHU

Za pomocí speciální techniky můžeme odposlechy lokalizovat a poté odinstalovat. Zařízení fungují na principů elektromagnetického záření. Je důležité zařízení dobře ovládat a velkou úlohu hraje prax v teto vyhledávající technice. Využívají ji speciálně vyškolení pracovníci při obranně technické prohlídky.

3.1 Radiový analyzátor

Odposlech bývá v praxi prováděn nejčastější pomocí miniaturních rádiových vysílačů. Rádiové analyzátory pracují na kontrole a vyhodnocení radiového spektra. Rádiovému odposlechu nezamezí, jej velmi spolehlivě lokalizuje a odhalí. Princip činnosti spočívá v zapsání aktivních rádiových signálů do paměti přístroje vyškoleným pracovníkem, vyhodnocení těchto signálů a zapnutí přístroje do polohy SCAN. Jednotka automaticky kontroluje rádiové spektrum a porovná aktuální rádiové signály se zaznamenanými. Když je nalezená frekvence, která není v paměti přístroje, je uživatel upozorněn vizuálně, případně akusticky. Při vyvolání poplachu lze lokalizovat zdroj signálu a poté deaktivovat.[6]

3.1.1 Paměťový radiový analyzátor MRA-3

MRA-3 je speciální přijímač určení k nepřetržitě ochraně prostoru a k okamžitému zjištění rádiového odposlechu. Ultra rychlý vyhodnocovací systém odhalí do místnosti vnesené nebo dálkově aktivovaný odposlech i v podmínkách silného vysokofrekvenčního pole místních rozhlasových a televizních vysílačů. MRA-3 umožňuje odhalení přítomnosti nového signálu během 6 sekund a uživatel je na přítomnost podezřelého signálu okamžitě upozorněn. K omezení falešných poplachů je MRA-3 vybaven tříúrovňovým poplachovým hlášením předpoplach-poplach-minulý poplach. Díky malým rozměrům a zcela kompaktnímu provedení přístroje, který obsahuje teleskopickou anténu a vnitřní baterii lze MR-3 snadno umístnit jak na nábytku kanceláře tak i skrytě. Největší výhodou přístroje je trvalá automatická ochrana místnosti.[7]

Technická specifikace MRA-3

- Kmitočtový rozsah 43-2700 MHz
- Citlivost pro SN= 10 dB 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
- Měřené síly pole 40 úrovní LCD čárový indikátor
- Měřené vzdálenosti vysílače 1 mW 150 m
- Paměť spektra zálohované baterií
- 512 multifrekvenčních kanálů záznamu spektra
- 16 průběžné aktualizovaných poplachových kanálů
- identifikační kód proti neoprávněné manipulaci
- jemné doladění + 1 multifrekvenční kanál
- automatické sceannováni 6 sekund/cykl
- měření kmitočtů v rozsahu 43-4000 MHz, rozlišení 0,1 MHz
- optická a akustická poplachová signalizace
- předpoplach (upozornění na přítomnost nového signálu po každém scannovacím cyklu)
- poplach po 10 (120) min. přítomnosti trvalého signálu
- časová informace o minulém poplachu: max. 999 min.
- regulovatelný audio výstup s vypínatelným reproduktorem
- napájení 9 V (vestavěná AKU baterie nebo 6F22 baterie)
- spotřeba: SCAN cca 44 mA, OFF pod 4 μA

- indikace poklesu baterie pod 7V
- nabíjecí vstup a externí napájení 12-25 V DC
- ochrana proti přepólování
- výsuvná teleskopická anténa
- rozměry: 136 x 49 x 137 mm
- váha: 620 g (včetně baterie)
- přístroj splňuje ČSN EN 50081-1 a ČSN EN 55022 (EMC- třída B. atest TESTCOM)

Obr. 5. Paměťový rádiový analyzátor MRA-3.[7]

3.2 Detektor vysokofrekvenčního pole

Současná radioelektronika nabízí řadu možností jak provést operativní odposlech, který je před vlastním VIP jednáním prakticky neodhalitelný. Řešením je systém permanentní ochrany proti odposlechu nebo operativní kontrola v průběhu jednání.

3.2.1 Detektor vysokofrekvenčního pole RFD-5

Optimalizovaná obsluha RFD-5 a zjednodušená VIP metodika umožňuje účinnou obranu proti operativnímu odposlechu i osobám, které nejsou specialisti v oboru. RFD-5 je lehký, kompaktní přístroj v odolném kovovém pouzdru především určený jako základní nástroj při provádění protiodposlechových prohlídek.[8]

Technická specifikace RFD-5

- Kmitočtový rozsah: 0,5 MHz až 25 GHz
- Typická citlivost: 0,06 μW ERP (400 MHz /5 cm/ 5 dílku)
- Dynamický rozsah: 43 dB základní, +40 dB útlum LOCAL
- Útlum KV: filtr HF OFF 10 MHz -26 dB
- Detekovatelné pulsy: >80 μs
- Regulace hlasitosti odposlechu: 4 úrovně (36 dB)
- Proměnný tón lokalizace vysílače: vypinatelní
- LCD display 2 x 12 znaků
- Okamžité vyhodnocení síly pole: čárkový indikátor (39 hodnot), numerický (251 hodnot)
- Vyhodnocení špičkové hodnoty: zpožděná čárka maxima (24 hodnot), zpožděný údaj PEAK (251 hodnot)
- Přepis max.hodnoty: nárůst 1 ms, pokles 6 s (zpožděná signalizace)
- Čítač poplachů: 99 událostí
- Paměť poplachů: 16 událostí včetně času a síly signálu
- Zpožděný záznamu následujícího poplachu: 70 s
- Vestavěná teleskopická anténa: nastavitelná od 1 cm do 37 cm
- Sluchátka: provedení stereo 32 ohm
- Indikace poklesu napětí baterie: < 7 V

- Externí napájení a dobíjení: 12 V až 20 V DC, nestabilizované
- Baterie: 9 V (6F22) nebo 9 V akumulátor
- Spotřeba: 3,5 až 6 mA
- Rozměry: 150 x 60 x 31 mm
- Váha: 295 g

Obr. 6. Detektor vysokofrekvenčního pole RFD-5.

3.3 Detektor nelineárních přechodů

Jedná se o prověřování prostor, bytů, kanceláři a vozidel proti odposlechu a skrytým kamerám. Skládá se z několika typů kontrol za použití speciálních přístrojů, které zachytí jakékoli polovodičové součástky, z kterých jsou tvořeny štěnice, videoštěnice, GSM pagerů či jiné speciální techniky, které přenášejí informace.

Tato kontrola je důležitá z hlediska nalezení zpravodajských prostředků, takových, které jsou dálkově ovládány nebo přenášejí informace paketově, to znamená, že informace uchovávají ve své paměti a po uplynutí periody je dokáži přenést ve velmi krátkem

okamžiku, to jsou pasivní prostředky nebo přenášejí informace ze zájmového prostoru jiným způsobem. Především ve starších budovách jsou tímto detektorem odhalovány i prostředky, které jsou napájené ze síťového rozvodu a jsou zazděné.[9]

3.3.1 Detektor nelineárních přechodů NR 900 E

Přenosný pulsní detektor nelineárních přechodů, který umožňuje porovnávání úrovní druhé a třetí harmonické odraženého signálu od polovodičového přechodu. Operátor může ovládat celý detektor pomoci klávesnice s ergonomicky umístněnými ovládacími prvky. Na klávesnici se nachází LCD display, který přehledně poskytuje množství velmi důležitých informací. Detektor má výstup pro stereofonní sluchátka.[10]

Vlastnosti NR 900 E	
Detekční vzdálenost	0,5-2m
Přesnost	0,1m
Vysílaná frekvence	900MHz
Vyzářený výkon pulsně – režim 300Hz	150W
Vyzářený výkon pulsně – režim 20kHz	20W

Obr. 7. Detektor nelineárních přechodů NR 900 E.[10]

4 SPECIÁLNÍ PROSTŘEDKY ODPOSLECHOVÉ TECHNIKY

4.1 Drátové mikrofony

Drátová mikrofony jsou supercitlivé elekretové mikrofony, které dokáží bez problémů monitorovat i šepot v místnosti 6x6 m. Mikrofony lze připojit k nahrávači a potom si již jenom chodit pro získané nahrávky. Jsou vhodné spíše jako doplněk pro digitální i analogová záznamová zařízení nahrávající zvuk z daného prostoru. Také se umístňují na tělo, do oděvu, do kufříku. Pro přenos informace se používají metalická vedení i optická vedení. Na konci vedení se nachází reproduktory nebo záznamové zařízení. Při výběru drátového odposlechu třeba brát ohled na velikost zařízení a na parametry jako přenášené frekvenční pásmo, směrovost, citlivost a impedance.

4.2 Radiové mikrofony

Radiové mikrofony jsou mikrofony s přenosem informací rádiovou cestou. Radiomikrofony jsou značně miniaturizované s vlastním vysílačem, které snímají hlasy ve svém okolí a přenáší do vzdálenosti i několika kilometrů. Většina radiomikrofonů pracuje v pásmu 30MHz – 25 GHz. Kvůli složitější detekci se používají atypické modulace (pulzní kódové, digitální, subnosné, modulace rozprostřeném pásmu, tradiční AM a FM modulace jsou snadno odhalitelné, proto se téměř neobjevují). Z hlediska vlastního přenosu se dělí do dvou základních kategorií, a to na prostředky analogové a digitální.

4.2.1 Radiový mikrofon RM-M5

Je to miniaturní analogový radiomikrofon. RM-M5 přenáší akustické informace na frekvencích 417-418MHz. Přenášený signál může být přijímán určeným přijímačem UNIVERSAL.[13]

Technické specifikace RM-M5	
Operační frekvence	417,5MHz, 418MHz
Modulace	FM
Odchylka	15KHz
Napájení	2-6V
Výstupní výkon	7-50mW
Rozměry	37x10x3mm

4.2.2 Radiový mikrofon ND-M2

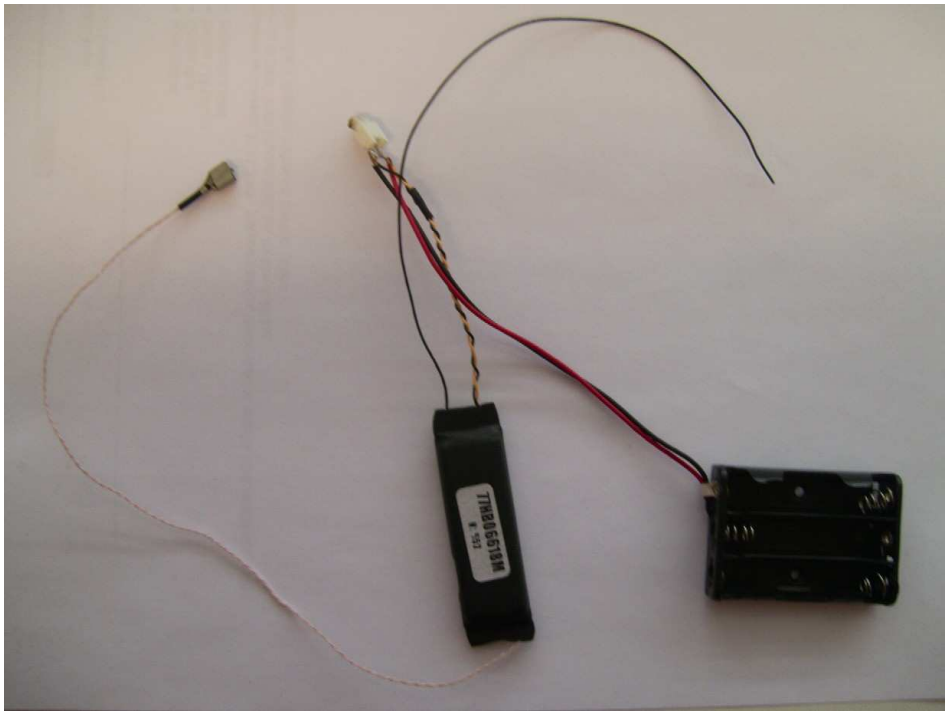
ND-M2 se skládá ze dvou částí, samotní radiomikrofon, který je digitální a přijímač se zabudovaným dálkovým ovládáním. Zařízení pracuje na frekvencích 410-424MHz. Operátor může na klávesách zařízení nastavit frekvenci v tomto rozmezí.[13]

Technické specifikace ND-M2	
Frekvenční rozsah	416-421,5MHz
Modulace	FM
Rychlost přenosu dat	100kbps
Dynamický rozsah přenosu dat	45dB
Dynamický rozsah mikrofonového vstupu	89dB
Šířka pásma	200-6000Hz
Napájení	3,5-12V
Citlivost	1μV
Rozměry	51x17x6mm

Technické specifikace dálkového ovládaní ND-M2

Modulace	AM
Výstupní výkon	1000mW
Napájení (4xAAA baterie)	6V
Spotřeba proudu	400mA
Provozní frekvence	315MHz
Rozměry	145x45x20mm
Provozní vzdálenost	100m

Obr. 8. Dálkového ovládaní ND-M2.



Obr. 9. Rádiový mikrofon ND-M2.

4.3 Radiové přijímače

Radiové přijímače jsou nedílnou součástí odposlechové techniky. Jedná se o vysocecitlivé přijímače, které si umí zapamatovat frekvence a někdy umí u nahrát záznam.

4.3.1 Unikum

Přístroj je určen k přenosu audio dat s digitálním kódováním přes síť (220V). Skrytý vysílač se skládá z vnějšího mikrofonu, vysílače a adaptéru. Vedení (220V) využívá k napájení a přenosu audio signálu. Zařízení využívá přizpůsobivou Delta-modulaci a digitální zakódování. Datový přenosový poměr je 100 kbps. Data jsou zachycovány přijímačem. Data mohou být přijímaná když je přijímač galvanicky připojen se sítí, vedením (220V) nebo přes vnější teleskopickou anténu. K poslechu je možno použít sluchátka nebo vestavěný reproduktor. Zvuková data jsou ukládána na vestavěnou flash paměť. Zařízení je vybaveno audio výstupem pro spojení s vnějším záznamovým zařízením. Přijímač lze napájet za pomocí vedení (220V) nebo baterií. Přijímač může pracovat se jedním nebo se dvou přenosových kanálů. Je vybaven dvěma kanály, tudíž dva přenosové kanály lze použit uvnitř jedné sítě.[13]

Technické specifikace UNIKUM

Vysílač:

Napájení	185-260V
Výstupní signál	0,7V
Rozměry, vysílač	48x23x8mm
Rozměry, napájecí zdroj	14x29x9mm

Přijímač:

Napětí	2-5V
Spotřeba	1,3W
Přijímací citlivost	1mW
Počet kanálu	2
Nahrávaní zvuku z vestavěné paměti	3-12 h
Rozměry	152x83x35mm

Obr. 10. Unikum.

4.3.2 Universal

Universal je malé zařízení na přijímaní a nahrávaní zvukových signálů z analogových a digitálních radiomikrofonů. Přijímač je pozoruhodný svou vysokou citlivostí, selektivitou a nastavitelným stupněm zvukové redukce. Přijímač je schopen si zapamatovat 10 frekvenčních pásem uvnitř operačního rozsahu. Zvukovou informací je schopen nahrát do vestavěné paměti. Dostupná je reprodukce zvukového záznamu. Malé rozměry přijímače umožňují pohodlné využití a je ideální pro bezpečnostní aplikace.[13]

Technické specifikace UNIVERSAL	
Frekvenční rozsah	410-424MHz
Modulace	FM
Frekvenční krokování	5,10,25kHz
Citlivost	1,5µV
Napájení	1,8-3,5V
Počet kanálů v paměti	10
Rozměry	139x60x33mm

Obr. 11. Universal.

5 TAKTIKA NASAZENÍ ZAŘÍZENÍ DO PROVOZU

Průmyslová špionáž je jedním z nejvýznamnějším druhem zpravodajské činnosti. Proto je taktika nasazení zařízení důležitá. Jako první je zapotřebí promyslet kam a jaký tip odposlechového zařízení umístnit. Musíme si promyslet jestli je možné se do zájmové místnosti fyzicky dostat a umístnit zařízení nebo budeme muset odposlouchávat z povzdáli. Do prostoru můžeme instalovat štěnice trvalé nebo štěnice které jsou napájený baterií a po určité době budeme muset vyměnit baterii nebo odposlech ukončit. Při výběru odposlechu dbáme na přenos informací, volíme drátový přenos nebo bezdrátový přenos. Čím blíž je odposlechové zařízeni k zájmové oblasti nebo k pachatelovi, tím je kvalita odposlechu lepší, proto se snažíme vhodně umístnit zařízení, napr. při psací stůl, při počítač nebo v zasedací místnosti. Nedílnou součástí je maskováni odposlechové techniky.

5.1 Dělení odposlechových prostředků

5.1.1 Podle umístění v zájmovém prostoru

- s nutností průniku do prostoru
- bez nutnosti průniku do prostoru

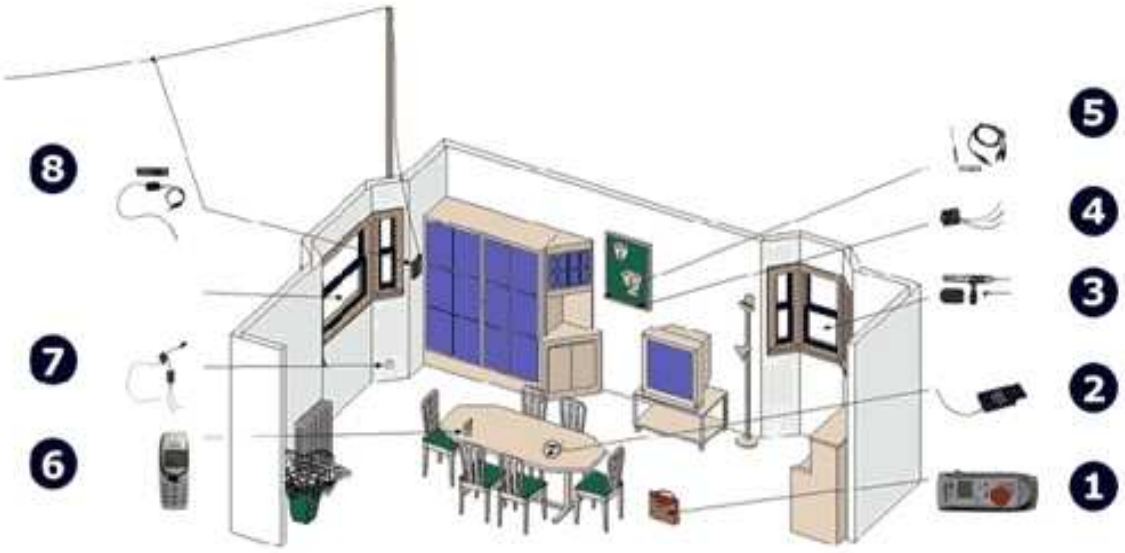
5.1.2 Podle typu přenášené informace

- audio prostředky
- video prostředky
- kombinované prostředky audio/video

5.1.3 Podle typu přenosu informace ze zájmové oblasti k záznamu

- drátově
- bezdrátově

5.2 Místa instalace odposlechové techniky



Obr. 12. Místa instalace odposlechové techniky.[11]

Popis obrázku:

1. Diktafon s odposlechem
2. Miniaturní radiomikrofon, 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. Radiomikrofon 220V
8. Radiomikrofon na telefonní lince

5.2.1 Diktafon s odposlechem

Diktafon si vložíme do pracovního zavazadla, které máme u sebe v jednací místnosti. Pokud je před jednáním vykonávaná prohlídka, tak se táto možnost nedoporučuje z důvodu odhalení.

5.2.2 Miniaturní radiomikrofon, dálkový odposlech

Vzhledem k minimálním rozměru zařízení je možné umístnit kdekoli. Do jednací místnosti se musíme dostat před jednáním a skryt tohle zařízeni. Potom už můžeme odposlouchávat z povzdáli které je podmíněno dosahem odposlechu.

5.2.3 Laserový odposlech

Jedná se o bezpečný odposlech z pohledu špiona, protože může být venku, nemusí pronikávat fyzicky do jednací místnosti, ale podmínkou je, aby táto místnost měla skleněné plochy.

5.2.4 Miniaturní sledovací kamera s odposlechem

Zařízení se instaluje na zeď nebo někam do rohu místnosti pro nejlepší vizuální kontakt. Výhodou odposlechu je to, že můžete slyšet a zároveň vidět všichni účastníky jednáni. Kamera s odposlechem může být napájená s vedlejší místnosti a také ve vedlejší místnosti můžeme drátově odposlouchávat.

Obr. 13. Instalace kamery v osvětlení [11].

5.2.5 Speciálně upravený mobilní telefon doplněný odposlechem

Při odposlechu s mobilním telefonem je nutnost průniku do zájmové oblasti. Odposlech probíhá jednoduše, telefon si položíte na stůl a náhodou se postavíte a půjdete na toaletu s tím, že telefon necháte ležet na stole. Zatím co vy jste na toalete, můžete vše slyšet přeš odposlech v mobilu.

5.2.6 Radiomikrofon v pevné síti 220V

Odposlechový prostředek s miniaturním transformátorem pro snížení napětí je instalován do zdi. Prostředek modulující informaci na frekvenci elektrické sítě 50 Hz. Možnost příjmu odposlechu až na vzdálenost 300m. Vysílač pracuje díky napájení ze sítě.[11]

Obr. 14. Radiomikrofon v pevné síti.[11]

5.2.7 Radiomikrofon na telefonní lince

Radiovysílač pracující po vyzvednutí telefonního sluchátka, vysílající informaci do vzdálenosti 50 m. Instalace odposlechu byla provedena výměnou předem připraveného napíchnutého telefonu za telefon původní.[11]

Obr. 15. Radiomikrofon na telefonií lince.[11]

6 LOKALIZACE ODPOSLECHOVÝCH ZAŘÍZENÍ

V souvislosti z růstem kancelářských prostor vzrůstá i počet odposlechových prostředku na získaní tajných firemních informací. Lokalizace odposlechových zařízení patří k prevenci nekalé krádeži informací. Lokalizace by se mněla provádět za přísného utajení.

6.1 Obranně technická prohlídka

Cílem obranné technické prohlídky je odhalení skrytých odposlechových prostředků, které mohou být v době provádění OTP aktivní nebo neaktivní. OTP provádí profesionální společnost s vyškoleními pracovníky nebo ji může provádět taky zadavatel sám po prostudování manuálu.[12]

6.1.1 Určení místa provádění prohlídky

Ochrana proti nelegálnímu odposlechu se aplikuje především v místnostech, v nichž probíhají jednání a v kancelářích pracovníku vyššího managementu. Zjišťování interních informací o jednotlivých zakázkách, klientech, rozvojových plánech s využitím prostředků odposlechu umožňuje protivníkovi získat velmi rychle přehled o aktivitách 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 instalaci technických prostředků, které mají zabránit takovému získávání informaci 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.[12]

6.1.2 Utajení prohlídky

Jednotlivé informace týkajíce se prohlídky by měl vědět jen velmi úzký okruh lidí a to až do chvíle, kdy má být vlastní prohlídka uskutečněna, pokud je 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.[12]

6.1.3 Průběh obranné technické prohlídky

- Fyzická prohlídka místnosti je orientovaná na kontrolu telefonních a elektrických rozvodů, počítačových sítí a elektrospotřebičů, nábytku, podlah, stěn, stropu.
- Radiová kontrola je zaměřena na odhalení všech radiových prostředků, které by mohli být v činnosti a na vytvoření frekvenční mapy prostoru. Prověření všech elektrických a telefonních rozvodů a kontrola všech signálů vysílaných po metalickém vedeních. Radiová kontrola se provádí za pomoci spektrálního analyzátora.
- Detekce nelinearit se provádí za pomoci detektoru nelineárních přechodů. Detekce využívá princip,že žádný odposlechový prostředek nebyl doposud vyroben bez polovodičové součástky. Detekce nelinearit odhalí všechny polovodičové součástky.[12]

6.1.4 Postup při odhalení útočného prostředku

Pokud je odhalen odposlechový prostředek je nejprve řádně zakresleno do situačního plánu místo odhalení odposlechového prostředku. Stejně místo nálezu je zadokumentováno fotograficky. Poté je prostředek demontován a celý prostor ještě jednou řádně prověřen. Specialisté společnosti jsou do vysoké míry schopní určit druh a původ odposlechového prostředku. Z tohoto důvodu společnost doporučuje osobní asistence zodpovědného pracovníka zadavatele, čímž se předejde 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.[12]

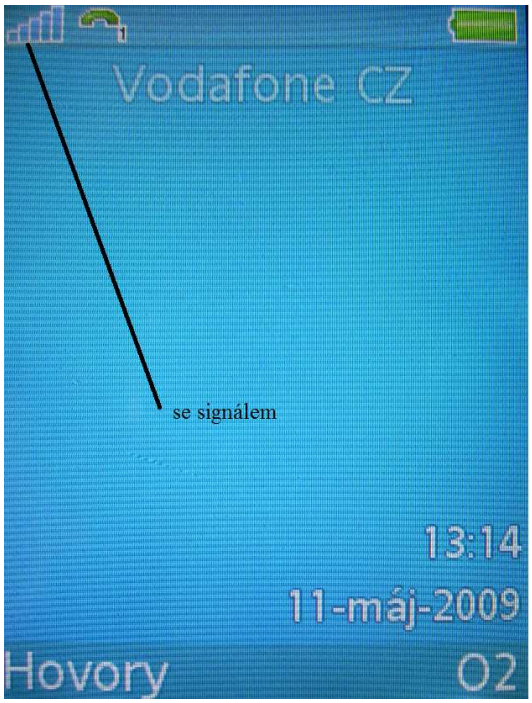
II. PRAKTICKÁ ČÁST

7 MĚŘENÍ

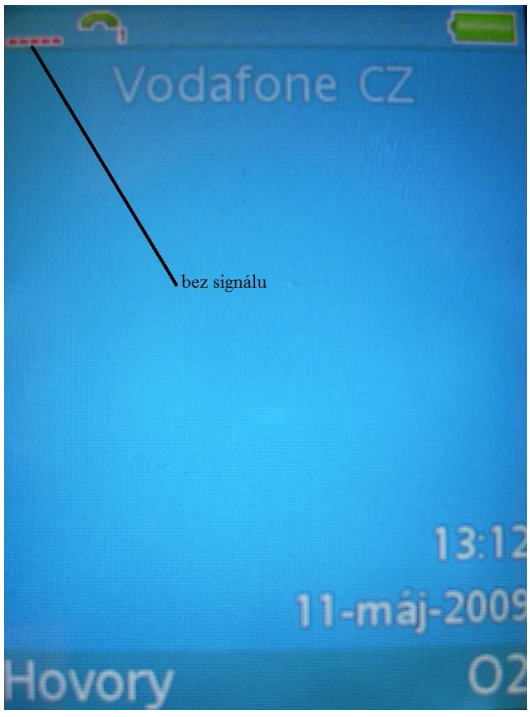
Měření se bude soustředit na problematiku nasazení odposlechových zařízení, získávaní akustických informací, provádění obranně technické prohlídky, rušení GSM signálu v jednacích místnostech

7.1 Rušení GSM signálu v jednací místnosti

Na měření byla použitá GSM jammer rušička, která umožňuje rušení obou GSM pásem, které operátoři využívají pro mobilní komunikaci. Rušení signálu jsem testoval v prostorách budovy U5 a to přesněji v stupni hale. Rušička byla umístněná ve výšce 1m nad zemí. Pomocí běžných mobilních telefonů jsem zjišťoval dosah rušícího signálu. Rušící signál je vysílán všesměrně. Přenosná rušička je vybavená dvěmi anténami. Jedna ruší signál v pásmu 900 MHz a druhá ruší signál v pásmu 1800 MHz. Před zapojením rušičky jsem zkontroloval intenzitu GSM signálu. Po zapojení rušičky do obvodu se automaticky vyrušil signál v okruhu 15 m. Požádal jsem okolní studenty, aby zahájili hovor nebo poslali správu, ale ani jedinému se to nezdařilo. Rušička je spolehlivá při chránění informací v jednacích místnostech a její instalace do provozu je velmi jednoduchá i pro laika.



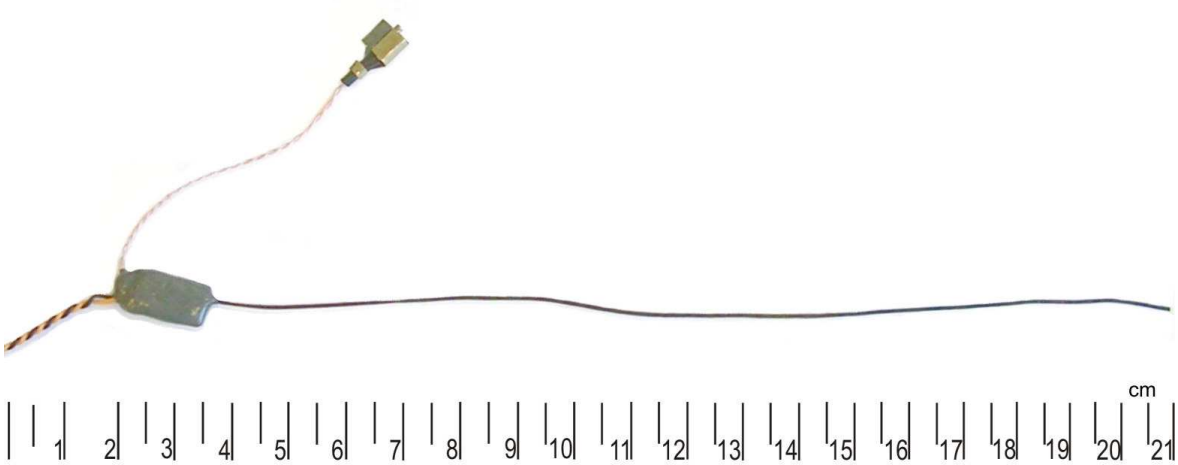
Obr. 16. Displej mobilního telefonu před zapojení GSM rušičky.



Obr. 17. Displej mobilního telefonu po zapojení GSM rušičky.

7.2 Nasazení odposlechového zařízení do provozu

Při nasazení „štěnice“ jsem použil analogový radiový mikrofon MR-3 určený k provádění audio monitoringu. Informace je vysílaná za pomoci malé drátové antény jako radiový kanál (FM modulace) ve frekvenčním pasme 417-432 MHz. Zařízení má od výrobce stanovenu pevní frekvenci 418 MHz, která je stála. Zařízení je napájeno 9 V baterii. Výrobce udává na přijímaní signálu přístroj „Universal“. Odposlech má miniaturní rozměry a proto je vhodný pro skryté umístnění. Při taktice a nasazení odposlechu do provozu jsem zvolil místa pod stolem v kanceláři . Lepící páskou jsem připevnil odposlechové zařízení o spodní stranu stolu. Druhé místo jsem zvolil zadní část tabule ve třídě při profesorským stolem. Při porovnání kvality signálu byla lepší slyšet „štěnice“ umístěná na zadní straně tabule než „štěnice“ umístěna na spodní straně stolu v kanceláři. Důvod byl výskyt rušivých signálu z počítače.



Obr. 18. Radiomikrofon MR-3.

7.3 Příjem a odposlech vysílacího signálu

Pro příjem vysílacího signálu jsem zvolil podle výrobce zařízení Universal, Je to malé přenosné zařízení na příjímání a nahrávaní zvukových signálů z analogových a digitálních radiomikrofonů. Přijímač je schopen si zapamatovat 10 frekvenčních pásem uvnitř operačního frekvenčního rozsahu. Zvukovou informaci je schopen nahrát do vestavěné flash paměti. Přístroj se zapíná tlačítkem ON. Protože jsem věděl frekvenci na které vysílalo odposlechové zařízení, tak jsem zvolil rychli přístup k přijímací frekvenci. Vstupní

hodnotu frekvence: stlačit a podržet tlačítko F. Pomocí šipek, vpravo a vlevo jsem posouval kursor do požadované pozice a za pomoci šipek nahoru a dolů jsem nastavil přesně frekvenci, kterou jsem potřeboval. Stiskem ENT jsem potvrdil uchování této frekvence. Zjistil jsem, že daná frekvence není moc dobrá, tak jsem jemním laděním zkoušel co nejbližší frekvence. Na frekvenci 417,9 MHz byl signál nejkvalitnější.

7.4 Lokalizace odposlechového zařízení

Předem nastřežené odposlechové zařízení jsem lokalizoval za pomoci paměťového radiového analyzátora a k zpřesnění místa výskytu odposlechového zařízení jsem použil detektor vysokofrekvenčního pole.

7.4.1 Obranně technická prohlídka za pomoci paměťového radiového analyzátora MRA-3

Paměťový radiový analyzátor MRA-3 je speciální skenovací přijímač určení k nepřetržitě ochraně prostoru a k okamžitému zjištění rádiového odposlechu. Je přenosný a lehko ovladatelný. Při provádění OTP jsem postupoval tak, že jsem vstoupil do místnosti, kde bylo předem nainstalováno odposlechové zařízení. Jeho přesná poloha byla neznáma. MRA-3 jsem položil na stůl a zapojil do obvodu. Zvolil jsem variantu skanování radiového spektra. Automatické skenování jsem nastavil za pomoci tlačítka MODE na polohu SCAN. Automaticky přistroj začal skenovat radiové spektrum, na displeji ukazovalo průběh skenování v procentech, na předním panelu byla signalizační červená dioda, které krátkým blikáním oznamovala předpoplach. Při dokončení skenování dioda svítila nepřetržitě a byl slyšet trvalý tón. To naznačovalo poplach a výskyt odposlechového prostředku v místnosti. Při zapnutí možnosti AUDIO bylo slyšel zvuk z odposlechového zařízení přes vstavěné reproduktory nebo za pomoci sluchátek.

7.4.2 Zpřesnění lokalizace odposlechu při OTP za pomoci detektoru vysokofrekvenčního pole RFD-5

Při obranně technické prohlídky jsem už věděl, že se v místností nachází odposlechové zařízení, ale nevěděl jsem přesně lokalizovat místo nasazení odposlechu. Pro dohledání jsem použil detektor vysokofrekvenčního pole RFD-5. Je to přenosné zařízení určené právě na dohledání odposlechového zařízení. Postupoval jsem systematicky od dveří. Přešel jsem

obvod místnosti a za pomoci sluchátek jsem slyšel intenzitu vysokofrekvenčního pole. Displej ukazoval hodnotu PEAK od 0 až do 251. Hodnota 251 znamená co nejbližší výskyt odposlechového zařízení. Lokalizace odposlechu byla provedena třikrát a pokaždé úspěšně.

ZÁVĚR

Kvalitní odposlechové zařízení je v dnešní době lehkou záležitostí. Stačí k tomu počítač a internet. Na internetovém odchodě si můžeme vybrat přesně to odposlechové zařízení, jaké potřebujeme. Dovezou nám ho domů i s potřebním manuálem. Po nastudovaní manuálu lze začít s instalací a samotním odposlechem. Anebo k nejjednodušší odposlechu můžeme použít mobilní telefon, který má funkci automatického vyzvednutí příchozího hovoru. Je to nejjednodušší „štěnice“. Nenápadně necháme mobilní telefon v saku a odejdeme na toaletu a tam prostě zavoláme na mobil a slyšíme rozhovor v jednací místnosti.

Česká Republika patří mezi první příčky průzkumu odhalení „štěnic“ a zkontrolované plochy v kancelářích. To svědčí o vysoce míře špionáží. Na českém trhu je několik desítek firem, které poskytují obranně technickou prohlídku na vysoké úrovni.

V teoretické části jsou popsaný fyzikální principy šíření elektromagnetického vlnění. Rozebral jsem elektromagnetické spektrum. V práci jsem se seznámil se speciálními technickými bezpečnostními prostředky. V tomto dílu jsou shrnutý všechny informace potřebné k správnému výběru odposlechového zařízení a nasazení a instalace do provozu a přijímaní audio informace. Popisuji jak profesionálně chránit jednací místnosti a kanceláře za pomoci speciální technické bezpečnostní techniky a důležitost chránění zájmového prostoru. Další části práci je obranně technická prohlídka. Je popsaný podrobní postup obranně technické prohlídky. Vyjmenoval jsem speciální technické odposlechové prostředky, které se využívají při obranně technické prohlídky.

V praktické části je provedena řada měření s odposlechovými prostředky. Jedná se o nasazení odposlechového zařízení a příjem audio signálu a následně lokalizace „štěnice“. V práci bylo měřeno :

- rušení GSM signálu v jednacích místnostech
- nasazení odposlechového zařízení
- příjem a odposlech vysílacího signálu
- provádění obranně technické prohlídky

Všechna měření byla provedeny v prostorách budovy U5.

ZÁVĚR V ANGLIČTINĚ

Quality sound detections apparatus is now easy matter. Just to the computer and the Internet. On the Internet can you choose exactly sounddetections equipment, what we need. They imported home with needed manual. After performing the manual can start the installation and listen. Or the simplest sound detections can use a mobile phone that has auto-pick up an incoming call. This is the easiest way to "bug". Inconspicuously leaving a mobile phone in the jacket and leave the toilet and then just call the cell phone and hear a conversation in the meeting room.

Czech Republic belongs among the top rungs of the survey revealing "bugs" and checked the area offices. This example determined the high level of espionage. On the Czech market is many companies that provide defense technical inspection at a high level.

In the theoretical section describes the physical principles of electromagnetic waves and electromagnetic spectrum. At work, I met with special technical means of security. In this work are summarized all the information necessary for proper selection of equipment and sound detections deployment and installation to service and receive audio information. It also describes how to protect a professional meeting room and offices with the help of special technical security and the importance of protecting an area of interest. Next work is part of the defense technical inspection. It is described in detail the procedure defense technical inspection. I listed sounddetections special technical devices which are used in the defense technical inspection.

In the practical part are numbers of measurements sound detections apparatus. This is a installation sound detections device and receive audio signal and then positioning "bug".

Measurement:

- Destroy GSM signal in the meeting room
- Instalation sound detections equipment
- Receive and listen to signal
- Implementation of Defense technical inspections

All measurements were made on the premises of the U5.

SEZNAM POUŽITÉ LITERATURY

[1] *Elektromagnetické záření* [online]. 2009 [cit. 2009-02-04]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Elektromagnetick%C3%A9_z%C3%A1%C5%99en%C3%AD>.

[2] *Elektromagnetické spektrum* [online]. 2009 [cit. 2009-02-04]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Elektromagnetick%C3%A9_spektrum>.

[3] *Duální rušička mobilů GSM-2000JAM* [online]. 2009 [cit. 2009-03-09]. Dostupný z WWW: <http://www.infosafe.cz/oblib_te/jammer.htm>.

[4] *SNG Inteligentní šumový generátor* [online]. 2008-2009 [cit. 2009-03-09]. Dostupný z WWW: <http://www.probin.cz/cz/sng-inteligentni-sumovy-generator>.

[5] *SNG007 inteligentný výkonový šumový generátor* [online]. 2007-2009 [cit. 2009-03-09]. Dostupný z WWW: <http://www.market.sk/obchod/technika-proti-odpocuvaniu-a-sledovaniu/rusice-digitalnych-aj-analogovych-diktafonou-a-skrytych-mikrofonov-stenic-mimo-eu/sng007-inteligentny-vykonovy-sumovy-generator.html>.

[6] *Faradayova klec* [online]. 2008-2009 [cit. 2009-04-20]. Dostupný z WWW: <http://www.probin.cz/cz/permanentni-ochrana>.

[7] *MRA-3, pamäťový rádiový analyzátor* [online]. 2009 [cit. 2009-04-20]. Dostupný z WWW: <http://www.identity.sk/ucho/mra3.htm>.

[8] *Detektor vysokofrekvenčního pole* [online]. 2009 [cit. 2009-04-20]. Dostupný z WWW: <http://209.85.129.132/search?q=cache:CTiAtaDu-j0J:www.elbi.cz/common/doc/rfd5/rfd5-spec10cz.doc+Detektor+vysokofrekven%C4%8Dn%C3%ADho+pole+RFD-5&cd=3&hl=sk&ct=clnk&gl=sk&client=firefox-a>.

[9] *Kontrola nelinearit* [online]. 2004 [cit. 2009-04-23]. Dostupný z WWW: <http://www.bbs.eu/vyhled_odposlechu.htm>.

[10] *Detektor nelineárních přechodů* [online]. 2009 [cit. 2009-04-23]. Dostupný z WWW: <http://www.detekce.com/technika_proti_odposlechu_odposlech.htm>.

[11] *Místa instalací odposlechové techniky* [online]. 2008-2009 [cit. 2009-05-02]. Dostupný z WWW: <http://www.probin.cz/cz/odhalene-instalace>.

[12] *Služby - Prověrky prostor* [online]. 2007 [cit. 2009-05-12]. Dostupný z WWW: <http://www.safecom.cz/sluzby.html>.

[13] Novo. *Novo catalogue* [online]. 2008 [cit. 2009-05-07].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Hz	Hertz
SHF	Super High Frequency
EHF	Extremely High Frequenci
Wi-Fi	Wireless Fidelity
IČ	Infra červené
m	Meter
GSM	Global Systém for Mobile Communications
UMTS	Universal Mobile Telecommunications System
V	Volt
A	Ampér
W	Watt
dB	Decibel
PC	Personal computer
LCD	Liquid Crystal Display
AM	Amplítudová modulace
FM	Frekvenční modulace
MAX	Maximum
MIN	Minimum
DC	Direct current
g	Gram
ČSN EN	Česká Státní Norma Europská Norma
EMC	Elektromagnetic compatibility
Kbps	Kilo bit per second
OTP	Obranně technická prohlídka

LED	Light Emitting Diode
VIP	Very Important Person

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: CENÍK PROHLÍDEK PROTI ODPOSLECHU OD FIRMI PROBIN S.R.O.

Podlahová plocha (m^2)	Prvotní prohlídka		Bezpečná kancelář, čtvrtletní náklady		
	základní	kompletní	Cena služeb celkem	1.-3. čtvrtletí	4. čtvtletí
10	6000 Kč	10000 Kč	18000 Kč	6000 Kč	0 Kč
20	12000 Kč	20000 Kč	36000 Kč	12000 Kč	0 Kč
30	16200 Kč	27000 Kč	48600 Kč	16200 Kč	0 Kč
40	20400 Kč	34000 Kč	61200 Kč	20400 Kč	0 Kč
50	24600 Kč	41000 Kč	73800 Kč	24600 Kč	0 Kč
60	28800 Kč	48000 Kč	86400 Kč	28800 Kč	0 Kč
70	32640 Kč	54400 Kč	97920 Kč	32640 Kč	0 Kč
80	36480 Kč	60800 Kč	109440 Kč	36480 Kč	0 Kč
90	39240 Kč	65400 Kč	117720 Kč	39240 Kč	0 Kč
100	42000 Kč	70000 Kč	126000 Kč	42000 Kč	0 Kč
200	55200 Kč	92000 Kč	165600 Kč	55200 Kč	0 Kč
300	67200 Kč	110000 Kč	201600 Kč	67200 Kč	0 Kč