Obranné technické prohlídky v praxi

Defensive technical inspections in practice

Jiří Malínek

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

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

Jméno a příjmení:	**Jiří MALÍNEK**
Osobní číslo:	**A09186**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Obranné technické prohlídky v praxi**

Zásady pro vypracování:

1. **Vysvětlete pojem obranná technická prohlídka (dále jen OTP) a jaký je její smysl provedení.**
2. **Uveďte a popište jednotlivé části OTP.**
3. **Informujte o postupu techniků na místě.**
4. **Popište a uveďte technické prostředky k realizaci OTP a typy technických prostředků určených k získávání informací.**
5. **Proveďte syntézu kontroly prostoru.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KAMENÍK, Jiří a František BRABEC. Komerční bezpečnost: Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostní agentur. Praha: ASPI, 2007. ISBN 978-80-7357-309-6.**
2. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-807-3188-894.**
3. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-807-3186-319.**
4. **BRABEC, František. Ochrana bezpečnosti podniku. 1. vyd. Praha: Eurounion, 1996, 203 s. ISBN 80-858-5829-0.**
5. **LAUCKÝ, Vladimír. Speciální bezpečnostní technologie. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 223 s. ISBN 978-807-3187-620.**
6. **LAUCKÝ, Vladimír. Řízení technologických procesů v průmyslu komerční bezpečnosti. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2005, 101 s. ISBN 80-731-8329-3.**

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

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **25. května 2012**

Ve Zlíně dne 24. února 2012

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ Fakulta aplikované informatiky

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Moje bakalářská práce je zaměřena na obranné technické prohlídky v praxi. V úvodu teoretické části práce je vysvětlen pojem, smysl provedení, primární a sekundární cíle OTP. Další část práce popisuje legislativní rámec, který vymezuje používání technických prostředků pro získávání informací (odposlechové prostředky) a provádění OTP v jednacích místnostech. Závěr teoretické části je věnován jednotlivým částem OTP, jak jdou, při kontrole prostoru, časově za sebou.

Úvod praktické části obsahuje popis typů odposlechových prostředků a technických prostředků k realizaci OTP. Na závěr praktické části je provedena syntéza kontroly prostoru dvou kanceláří se zakreslením možných míst umístění odposlechových prostředků.

Klíčová slova: obranná technická prohlídka, odposlechový prostředek, kontrola prostoru, systémy provedení obranné technické prohlídky.

ABSTRACT

My thesis is focused on the defensive technical inspections in practice. In the introduction to the theoretical part are explained concept, sense of design, primary and secondary targets of the defensive technical inspection. Next part of the work describes the legislative framework, which it defines use of technical means for obtaining information (listening devices) and implementing of the defensive technical inspection in meeting rooms. Finally, the theoretical part is dedicated individual parts of the defensive technical inspection, how they come a time when checking the area behind.

Introduction of the practical part contains description of the types of listening devices and technical means to implement of the defensive technical inspection. Finally, the practical part is performed synthesis area control two offices with the marking of possible locations of places listening devices.

Keywords: defensive technical inspection, listening device, area control, systems performance of defensive technical inspection.

PODĚKOVÁNÍ

Chtěl bych poděkovat svému vedoucímu JUDr. Vladimíru Lauckému za odbornou pomoc a poskytnutí potřebných informací při tvorbě bakalářské práce.

Dále bych chtěl ještě poděkovat rodičům za podporu a pomoc při studiu a své přítelkyni za porozumění během celého tříletého studia na vysoké škole.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….……

podpis diplomanta

OBSAH

ÚVOD

V dnešní přetechnizované a uspěchané době, kdy se firmy předhání v novinkách, jimi vytvořených na celosvětových trzích, mnohdy zapomínají na ochranu „know how“, výzkumu, vývoje či vynálezecké a zlepšovatelské činnosti nebo jiných důležitých a velmi citlivých informací firem, a tak dochází ke krádežím nápadů, které ještě mnohdy ani nebyly realizovány ve formě nového výrobku či nové služby. Tyto krádeže informací realizují firmy mezi sebou v rámci konkurenčního boje na trhu, a nebojí se k tomu použít legálních, pololegálních, ale i nelegálních prostředků z důvodu získání konkurenční výhody. Nelegálním prostředkem je zde myšlena ofenzivní zpravodajská technika (odposlechy, různé minikamery a další nežádoucí technické prostředky sloužící k tomuto účelu).

Jako ochrana proti úniku velmi citlivých latentních informací z firem za pomoci těchto nelegálních prostředků, a tím vzniku konkurenční výhody, nebo u osob k ochraně soukromí či informací, které by mohly poškodit jak danou osobu, tak firmu ve které pracuje, se provádějí obranné technické prohlídky (OTP). OTP se provádí především v kancelářích, jednacích místnostech, či jiných místnostech, kde by odposlechové prostředky mohly být nainstalovány. Jedná se především o místnosti ve firmách, organizacích u jednotlivců, ale i jednací oblasti státního charakteru. OTP zde zabraňuje obrovským finančním ztrátám a zároveň znemožňuje vnášet nejistotu do mezinárodních vztahů v místním nebo globálním měřítku.

Na druhou stranu jsou odposlechové prostředky využívány i ku prospěchu věci, a to Policií ČR, Bezpečnostní informační službou ČR, Úřadem pro zahraniční styky a informace a popřípadě Vojenskou policií ČR, při odhalování závažné trestné činnosti, kterými jsou např. korupce, drogová kriminalita, organizovaný zločin nebo násilná či daňová trestní činnost.

V teoretické části bakalářské práce je vysvětlen pojem a smysl OTP, cíle a legislativní rámec, který vymezuje používání odposlechových prostředků a provádění OTP v jednacích místnostech. Dále jsou popsány jednotlivé části OTP podle toho, jak jdou časově za sebou. Praktická část je zaměřena na typy technických prostředků k realizaci OTP a na typy odposlechových prostředků. Na závěr praktické části je provedeno zhodnocení kontroly prostoru kanceláří se zakreslením možných míst umístění odposlechových prostředků.

I. TEORETICKÁ ČÁST

1 POJEM OTP A JEJÍ SMYSL PROVEDENÍ

OTP je nedílnou součástí speciálních bezpečnostních technologií. Jedná se o soubor úkonů vedoucí k odhalení nechtěných technických prostředků, převážně odposlechů, minikamer či jiných zařízení určených k nedovolenému získávání informací, za účelem zabránění jejich šíření a následnému využití těchto informací v neprospěch firmy, osoby nebo státu.

V obecném smyslu lze OTP brát, jako komplexní kontrolu objektu s následným provedením určitých postupů, které by měly vést ke stanoveným cílům. V konkrétním smyslu se jedná o detailní kontrolu prostoru (jednací místnosti, oblasti, kanceláře apod.), jež je prováděna speciálně vyškolenými pracovníky za účelem dosažení primárních a sekundárních cílů.

Existují dva základní typy OTP:

- OTP vstupní (komplexní) - Provádí se jednorázově a výsledkem je doporučení konkrétního systému opatření, které vede k odstranění technických prostředků k získávání informací a k dlouhodobější ochraně proti těmto prostředkům.
- OTP periodická - Jedná se o komplexní OTP, která je prováděna v pravidelných časových úsecích. Tyto úseky se stanoví podle stupně rizik hrozících z hlediska možností uniku informací, pomocí nežádoucích technických prostředků. Většinou se jedná o interval 8 - 12 týdnů.[1]

Tyto dva základní typy OTP jsou prováděny v prostorách, které rozdělujeme podle využívání na permanentní a občasné.

1.1 Permanentní prostory

Permanentní prostory jsou takové, které jsou využívány každodenně, popř. v pracovní dny. Jedná se o prostory, kde kromě fyzické ostrahy bývá ještě ochrana doplňována technickými prostředky nebo režimovými opatřeními. Jsou-li zde tato ochranná opatření dodržována a nedošlo-li v zájmových prostorách k nějakým mimořádným událostem, je zde komplexní OTP zcela dostačující. Kdykoliv se však v chráněném prostoru provádějí nějaké rozsáhlejší úpravy (výměna nábytku) nebo opravy (na zdivu, elektrorozvodné instalaci, vodovodním či teplovodním systému), potom je tato činnost brána za mimořádnou událost, po které by měla následovat OTP.[2]

1.2 Občasné prostory

Občasné prostory jsou takové, které jsou využívány nahodile, nepravidelně nebo příležitostně. U občasných prostor se OTP provádí periodicky a to vždy před konáním jednání či po skončení všech přípravných prací. Nesmí docházet k tomu, aby se po provedení OTP děly takové činnosti jako je přinášení věcí do místnosti.[2]

1.3 Cíle OTP

Cíle prohlídek lze rozdělit na primární (základní) a sekundární (následné).

Primárním cílem prohlídek je odhalení nebo zamezení funkčnosti nechtěných technických prostředků (mikrofonů, kamer, datových odposlechů), ať už jsou v době OTP funkční či nefunkční (čekající na spuštění). Dalším primárním cílem je objevení různých úprav, které byly provedeny při instalaci těchto prostředků, a kdo tyto úpravy provedl. Tyto úpravy jsou zjišťovány ihned po odstranění technických prostředků určených k získávání informací.

Za sekundární cíl lze považovat ochranu proti následku použití těchto nežádoucích technických prostředků. Následek je v tomto případě jev, který přichází bezprostředně po vyzrazení důležitých informací.

Následky, které by mohly vzniknout při neodstranění prostředku:

- vznik konkurenční výhody (u firem),
- finanční úbytek,
- ztráta soukromí (u osob),
- ztráta suverenity státu,
- nejistota na poli mezinárodních vztahů.

2 LEGISLATIVNÍ RÁMEC

Používání odposlechových prostředků a provádění OTP je vymezeno v legislativě ČR.

2.1 Ochrana osobnostních práv

Základem ochrany osobnostních práv je zákon č. 2 /1993 Sb., Listina základních práv a svobod, ve kterém se mimo jiné píše o nedotknutelnosti osoby a jejího soukromí, ochraně listovního tajemství a o ochraně tajemství jiných písemností a záznamů. Právo na ochranu osobnosti může být tedy i porušeno nezákonným pořízením a použitím obrazových nebo zvukových záznamů pořízených pomocí odposlechových prostředků.

2.2 Možnosti pořizování záznamu

Portréty, fotografie, obrazové a zvukové záznamy, týkající se osoby, mohou být pořizovány:

1) se souhlasem zaznamenávané osoby,
2) bez souhlasu zaznamenávané osoby:
    a. Na základě soudního nařízení dle zákona č. 141/1961.
    b. Pro vědecké a umělecké účely.
    c. Na základě zpravodajské licence pro tiskové, filmové, rozhlasové a televizní zpravodajství.[5]

Za záznam je možné považovat zachycení obsahu komunikace, pomocí odposlechových či jiných technických prostředků k tomu určených, mezi různými osobami na nosičích, jako jsou CD, DVD, FLASH disky, SD karty, apod.

2.2.1 Souhlas s pořízením záznamu

Souhlas nemusí být výslovný, stačí, když je odvoditelný z okolností, za nichž byl pořízen. O nevýslovný (konkludentní) souhlas se jedná tehdy, pokud nevzbuzuje pochybnosti o tom, co chtěla dotčená osoba projevit.[5]

1. Pořizování záznamu v soukromých a veřejných prostorách

    U veřejných prostranství lze odvodit, že dotčená osoba vstupující do místa, jenž je monitorováno kamerou nebo jiným záznamovým zařízením, souhlasí s pořízením záznamu. U soukromých prostor lze nevýslovný souhlas odvodit z toho, je-li

zřejmé, že dotčená osoba o monitorování věděla a zároveň neprojevila nesouhlas.[5]

2. Zvukový záznam telefonního hovoru

   Dle stanoviska Ústavního soudu ČR ze dne 13. září 2006, má každý právo zaznamenávat své vlastní telefonické hovory. Obdobně jako další soudy vycházel z úvahy, že při existenci obecného povědomí o tom, že telefonáty mohou být technickou cestou účastníky běžně zaznamenávány. Z toho jde odvodit, že účastníci hovoru s možným pořízením zvukového záznamu nevýslovně souhlasí, pokud však neprojeví nesouhlas. Tímto nevýslovným souhlasem je splněna podmínka pořízení zvukového záznamu a tato podmínka doslova vylučuje zásah do práv na ochranu osobnosti.[6]

2.2.2 Nařízení použití odposlechových prostředků

Podle ustanovení § 88 odst. 1 zákona číslo 141/1961 Sb. je nařízen odposlech a záznam telekomunikačního provozu, je-li vedeno trestní řízení, pro zvlášť závažný zločin nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva. Odposlech a záznam telekomunikačního provozu provádí pro potřeby všech orgánů činných v trestním řízení Policie ČR.

Zločiny jsou všechny trestné činy, které nejsou dle trestního zákona přečiny. A zvlášť závažnými zločiny se rozumí úmyslné trestné činy, na něž trestní zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně deset let. [7]

Odposlech a záznam telekomunikačního provozu lze také nařídit, jestliže se jedná i o další obecné skutkové podstaty trestných činů, např. trestný čin obecného ohrožení, trestný čin ublížení na zdraví podle, trestný čin omezování osobní svobody.[8]

Nařídit odposlech a záznam telekomunikačního provozu je oprávněn předseda senátu a v přípravném řízení na návrh státního zástupce soudce. Příkaz k odposlechu a záznamu telekomunikačního provozu musí být vydán písemně a musí být odůvodněn, včetně konkrétního odkazu na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro úmyslný trestný čin, k jehož stíhání tato smlouva zavazuje.[9]

Příkaz k odposlechu a záznamu telekomunikačního provozu musí obsahovat:

- adresu uživatele,

- adresu zařízení,
- osoba uživatele (pokud je známa její totožnost),
- doba provozu odposlechu či telekomunikačního záznamu (nejdéle 4 měsíce, ale na základě vyhodnocení průběhu může být soudcem soudu vyššího stupně a na návrh státního zástupce soudcem krajského soudu tato doba prodloužena, a to i opakovaně, vždy však na maximálně 4 měsíce),
- odůvodnění (musí být uvedeny všechny skutkové okolnosti a podstata nařízení).[10]

Odposlech lze nařídit i bez tohoto příkazu, a to v případě trestných činů obchodování s lidmi, svěření dítěte do moci jiného, omezování osobní svobody, vydírání, únosu dítěte, násilí proti skupině obyvatelů a proti jednotlivci nebo nebezpečného vyhrožování, pokud s tím uživatel odposlouchávané stanice souhlasí.[9]

Policejní orgán je povinen průběžně vyhodnocovat důvody, které vedly k vydání příkazu k odposlechu a záznamu telekomunikačního provozu. Pokud tyto důvody pominuly, je povinen odposlech a záznam telekomunikačního provozu ihned ukončit. Tuto skutečnost je nutné bezodkladně písemně oznámit předsedovi senátu, který příkaz k odposlechu a záznamu telekomunikačního provozu vydal, a v přípravném řízení rovněž státnímu zástupci a soudci.[9]

2.3 Odposlechový prostředek jako důkaz

Zde se argumentuje § 89 trestního řádu[1], kde ve 2. odstavci je uvedeno, že za důkaz může sloužit vše, co může přispět k objasnění věci a každá ze zúčastněných stran může důkaz vyhledat, předložit nebo jeho provedení navrhnout.

Podobné pravidlo je v §125 zákona č. 99/1963 Sb., občanského soudního řádu, kde je uvedeno, že za důkaz mohou sloužit všechny prostředky, kterými lze zjistit stav věci.

Jestliže tyto dvě pravidla jsou vztaženy na použití záznamu z odposlechového prostředku jako důkazu, lze takový záznam použít za předpokladu dodržení právních předpisů, které garantují ochranu osobnosti a zabraňují zásahům do soukromí a osobnosti člověka, dle

[1] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: *Sbírka zákonů České republiky*. 1961.

Listiny základních práv a svobod. Není sporu o možnosti použití záznamu s výslovným či nevýslovným souhlasem, pokud zaznamenávaná osoba souhlasí s použití tohoto záznamu v důkazním řízení. Problém může nastat ve chvíli, kdy osoba s použitím v důkazním řízení nesouhlasí. Pokud nastane tento problém, v soudní praxi se posuzuje v každém skutečném případě, zda proti právu na ochranu osobnosti nestojí jiné právo, kterému by měla být poskytnuta větší ochrana.[5]

Pokud je záznam z odposlechového zařízení použit jako důkaz, musí se k němu připojit protokol s údaji o místě, času, způsobu a obsahu provedeného záznamu, včetně informací o orgánu, který záznam pořídil. Zdali při odposlechu či záznamu telekomunikačního provozu nebyly zjištěny skutečnosti významné pro trestní řízení, je policejní orgán, po souhlasu soudu či v přípravném řízení po souhlasu státního zástupce, povinen záznamy zničit po třech letech od pravomocného skončení věci. Protokol o zničení záznamu o odposlechu je následně zaslán státnímu zástupci, který věc pravomocně ukončil nebo předsedovi senátu, k založení do spisu.[9]

2.4 Legislativní rámec provedení OTP

2.4.1 OTP v jednací oblasti

Dle § 24 odst. 4 a § 26 zákona č.412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, je stanoveno, že utajovanou informaci stupně utajení Přísně tajné nebo Tajné lze projednávat pouze v jednací oblasti.

Utajované informace se podle § 4 zákona č.412/2005 Sb. dělí na čtyři stupně utajení:

- Přísně tajné - vyzrazení neoprávněné osobě nebo zneužití takové informace může způsobit mimořádně vážnou újmu zájmům České republiky.
- Tajné - vyzrazení neoprávněné osobě nebo zneužití takové informace může způsobit vážnou újmu zájmům České republiky.
- Důvěrné - vyzrazení neoprávněné osobě nebo zneužití takové informace může způsobit prostou újmu zájmům České republiky.
- Vyhrazené - vyzrazení neoprávněné osobě nebo zneužití takové informace může být nevhodné pro zájmy České republiky.

Opatření nutné pro jednání v jednací oblasti dle zákona o ochraně utajovaných informací:

- Je nutné zajistit, aby zde nedocházelo k ohrožení nebo úniku projednávaných utajovaných informací.
- Odpovědná osoba je povinna požádat Národní bezpečnostní úřad (dále jen NBÚ) o provedení OTP, zda v jednací oblasti nedochází k nedovolenému použití technických prostředků určených k získávání informací.
- OTP je následně prováděna v součinnosti se zpravodajskými službami a Policií České republiky.
- Vstup do jednací oblasti a výstup z ní musí být kontrolován dle § 27 zákona[2] (fyzická ostraha, režimová opatření, technické prostředky).
- Neoprávněná osoba může vstoupit do jednací oblasti pouze s osobou, která má do této oblasti vstup povolen.[10]

OTP jednacích oblastí se provádějí průběžně, nejméně však každých 12 měsíců[3]. Dále je nutno provádět prohlídku vždy po neoprávněném vstupu či podezření na něj a po odchodu pracovníků provádějících údržbu nebo úpravy oblasti.[10]

Požadavky na ochranu proti odposlechovým prostředkům v jednací oblasti:

- zvukotěsné stěny, dveře, podlaha a strop (útlum na hranici jednací oblasti minimálně 50 dB),
- okna, větrací otvory nebo prostupy klimatizace musí být chráněny technickými prostředky certifikovanými NBÚ typu 4 (odolnost proti násilnému vniknutí),
- jednací oblast musí být chráněna proti odezírání z míst nacházejících vně budovy, ve které se jednací oblast nachází,

---

[2] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. 1. 1. 2006.

[3] Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. 1. 1. 2006.

- nábytek a zařízení umístěné do jednací oblasti musí projít OTP a musí být evidováno (typ, sériové a inventární číslo, historie pohybu),
- v jednací oblasti není vhodné umísťovat telefonní přístroje, pokud je jejich instalace nutná, musí být vybaveny odpojovačem nebo musí být odpojovány ručně před jednáním,
- do jednací oblasti nelze vnášet mobilní telefony či jiná nahrávací, vysílací, testovací, měřící a diagnostická zařízení, to neplatí v případě zařízení, jenž je používané v rámci OTP.[11]

3 ROZDĚLENÍ OTP NA JEDNOTLIVÉ ČÁSTI A JEJICH POPIS

OTP lze rozdělit do několika samostatných částí:

- přípravná část – operativní a technická příprava,
- prováděcí část – postup techniků na místě,
- hodnotící část – zmapování a zhodnocení výsledků,
- navrhovací část – návrh zlepšení permanentní technické ochrany proti odposlechovým prostředkům,
- závěrečná část – návrh následných opatření po skončení OTP.[1]

3.1 Přípravná část

V přípravné části je důležité, aby se technici detailně seznámili s objektem, ve kterém se bude OTP provádět, včetně jeho okolí, režimu údržby, úklidu, návštěv, rozmístění nábytku, konstrukčního a stavebního řešení. Dále je nutné, aby se seznámili s umístěním elektrických a telefonních rozvodů v objektu.

Přípravnou část lze rozdělit do dvou navzájem provázaných skupin, a to na přípravu technickou a operativní.

3.1.1 Technická příprava

Je jedním ze základních pilířů následného úspěšného provedení OTP. Při technické přípravě je nutno si uvědomit tyto body:

- úroveň možného ohrožení,
- historii stavby budovy,
- snadnost přístupu do stěžejních prostor v objektu,
- snadnost přístupu do kontrolovaných prostor v objektu.[3]

V souvislosti s těmito body lze technickou přípravu shrnout do těchto skupin:

- kontrola funkčnosti jednotlivých technických prostředků, které slouží k vyhledávání odposlechových prostředků, jež jsou k dispozici,
- seznámení s některými novými trendy v oblasti systémů provedení včetně vyzkoušení nových technických prostředků,

- nastudování projektové dokumentace místnosti (včetně všech dostupných rozvodů a kabeláže vedoucích místností),
- obeznámení se s režimovými opatřeními, fyzickou a technickou ochranou v objektu,
- důkladné zmapování prostoru, ve kterém se bude OTP provádět (k prvotnímu zmapování mohou posloužit fotografie pořízené zadavatelem OTP),
- kontrola umístění prostoru z hlediska možnosti napadení,
- vyhodnocení technických prostředků, kterými je možné provést útok,
- vymezení technických prostředků a náročnosti prací specialistů (odvíjí se od velikosti a struktury kontrolovaného prostoru, systémů provedení OTP a množství finančních prostředků zákazníka).

3.1.2 Operativní příprava

Jedná se o pohotovou, pružně fungující přípravu, která je prováděna za účelem hladkého průběhu OTP. Skládá se z těchto částí:

- určení časového harmonogramu OTP,
- stanovení osob, které budou seznámeny s provedením OTP (včetně osoby dosazené zadavatelem OTP),
- dohoda se zákazníkem, jak postupovat při odhalení odposlechového prostředku.[1]

3.2 Postup techniků na místě

Technik při prohledávání prostoru, místnosti či osob by měl počítat s tím, že technický prostředek je mnohem lehčí nainstalovat, jak odhalit. Ve své podstatě lze postup techniků na místě OTP klasifikovat jako ohledání místa činu, které v tomto významu znamená zkoumání a hodnocení situace pomocí taktických postupů s využitím systémů provedení OTP, jehož výsledkem je odhalení odposlechových prostředků nainstalovaných v místnosti, u osob a ve vozidlech.

Při prohledávání prostorů je nutné, aby technik dodržoval následující zásady:

- zahájení prohlídky v čase, kdy se předpokládá aktivace odposlechových zařízení (v průběhu předstíraného jednání), z toho důvodu, že některé technické prostředky mohou být ovládány dálkově,
- vyhledávání musí být prováděno skrytě (technik provádějící odposlech by neměl během OTP komunikovat s kolegy či techniky, nastavovat přístroje, aby nedošlo k odhalení provádění OTP a při lokalizaci nechtěného technického prostředku by neměl technik dát signál, že došlo k odhalení odposlechu),
- je třeba vytvořit vhodné podmínky pro prohlídku (zatáhnout závěsy, žaluzie nebo rolety z důvodu eliminace možnosti pozorování, zapnout všechna světla a další přístroje z důvodu vytvoření běžného pracovního prostředí),
- všechny další OTP by měly být prováděny v pravidelných intervalech,
- při vyhledávání je třeba věnovat největší pozornost oblasti, kde se odehrávají důležité rozhovory (za psacím stolem, blízko tel. přístroje, faxu nebo PC), obvykle bývá nežádoucí technický prostředek umístěn v okolí 7 m od těchto míst.[3]

Postup techniků na místě se liší od jednotlivých systému provedení OTP, patří sem fyzická kontrola, metoda prostorové triangulace rádiového spektra, detekce nelineárních přechodů, metoda termografie. Pravděpodobnost odhalení nežádoucího technického prostředku určeného k získávání informací je ovlivněna množstvím systémů provedení, které v daném prostoru technik použije. Čím více systémů provedení je technikem použito, tím větší je pravděpodobnost odhalení takového prostředku.

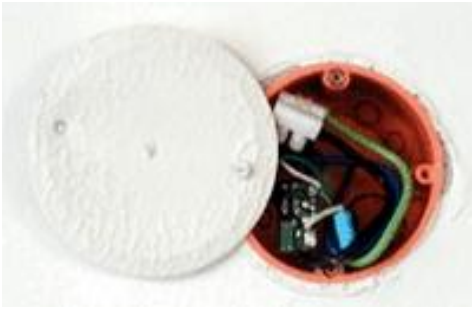
Jednotlivé systémy provedení jsou nasazovány dle požadavků zadavatele OTP, sortimentu technických prostředků, které má technik k dispozici a předpokladu technické náročnosti prostředků určených k získávání informací.

3.2.1 Fyzická kontrola

Jedná se o detailní kontrolu místnosti (podlah, stěn, stropů) a prakticky všech věcí (nábytku, obrazů, knih, apod.) i těžko přístupných (různé štěrbiny ve ventilaci nebo osvětlení, podhledy, apod.), které se v místnosti nachází. Dále mezi fyzickou kontrolu patří důkladné rozebrání elektrických přístrojů, síťových a elektrických rozvodů, zásuvek,

rozdvojek, světel a dalších přístrojů, v nichž by se mohl nacházet prostředek sloužící k nedovolenému získávání informací.

U fyzické kontroly se používá základní nářadí (lupa, šroubovák, klíč, apod.) a některé jednoúčelové a doplňkové přístroje určené pro lepší viditelnost odposlechového prostředku. Důležitou vlastností technika je u tohoto typu kontroly manuální zručnost, dobrý zrak a schopnost předvídat.

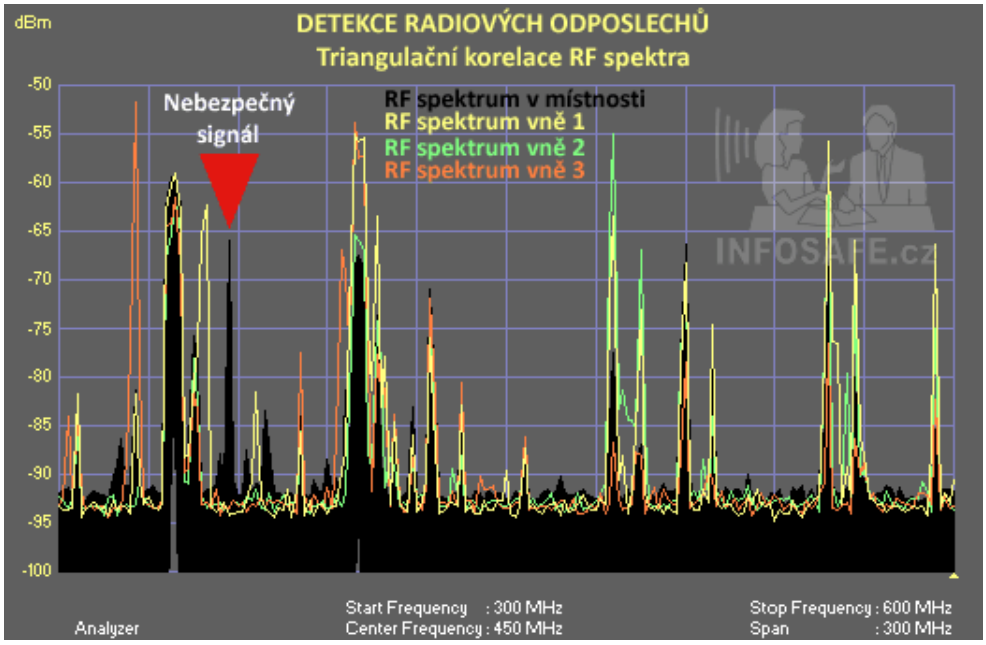


Obrázek 1 Radiový odposlech odhalený při fyzické kontrole[4]

3.2.2 Metoda prostorové triangulace radiového spektra

Jde o jednu z nejspolehlivějších metod detekce rádiové odposlechové techniky, pomocí níž je možné detekovat skryté mikrofony, kamery nebo nelegální datové přenosy. Tato metoda je založena na principu šíření elektromagnetických vln v prostoru (útlum vln s rostoucí vzdáleností). Měření je prováděno pomocí spektrálního analyzátoru, do kterého je načteno radiové pozadí na 3 místech v blízkém okolí od prověřovaných prostor a poté jsou tyto signály, pomocí speciálního softwaru, porovnávány s hodnotou naměřenou v prověřovaném prostoru. Pokud je signál naměřený v kontrolovaném prostoru řádově shodný, jako mimo tento prostor, lze takový signál označit za bezpečný. Naopak signály, jejichž intenzita je řádově rozdílná v kontrolovaném prostoru a mimo něj, lze označit za nebezpečné (viz Obrázek 2). Z toho vyplývá, že se v kontrolovaném prostoru, s největší pravděpodobností, nachází odposlech.[13]

[4] Zdroj: http://www.probin.cz/img/_/odhalene_instalace/inst_pevna.jpg



Obrázek 2 Porovnání naměřených frekvencí u metody prostorové triangulace radiového spektra[5]

3.2.3 Detekce nelineárních přechodů

Je založena na principu porovnání frekvence vyslaného signálu z detektoru nelineárních přechodů s frekvencí odraženého přijatého signálu od polovodičových či kovových součástek, jež jsou součástí každého technického prostředku, který je určen k nežádoucímu získávání informací. Frekvence vyslaného signálu je v rozmezí 800-1000 MHz, po odrazu od polovodičové součástky se přijatá frekvence změní na 2. harmonickou (1700-1800 MHz) a po odrazu od kovu se změní na 3. harmonickou (2500-2800 MHz). Přijetí 2. nebo 3. harmonické je signalizováno na displeji, poté si technik může ověřit přítomnost prostředku pro získávání informací ve sluchátkách, které jsou přímo připojeny k detektoru.[14]

Jde o nejpoužívanější metodu pro přesné odhalování nežádoucích technických prostředků, kterou je vhodné použít při vyhledávání těchto prostředků, v jejíž blízkosti se nenachází zařízení, jenž obsahuje polovodičové součástky (PC, telefon, fax, apod.). Následně mohou, z tohoto důvodu, na detektoru vznikat falešné signalizace. Pro vyhledávání u těchto

[5] Zdroj: http://www.infosafe.cz/obrazek/3/triangulacni-korelace-rf-spektra-gif/

zařízení je nutné použít důkladnou fyzickou kontrolu, metodu prostorové triangulace, snímání radiového spektra, metodu termografie.

Obrázek 3 Ukázka úrovní jednotlivých frekvencí u detekce nelineárních přechodů[6]

3.2.4 Metoda termografie

Tato metoda využívá toho, že každá věc, která má teplotu větší jak 0 K, vyzařuje určitou úroveň záření v infračerveném pásmu (tzv. teplotního pole). Provádí se pomocí prostředků termovizních systémů především však infrakamer. Úkolem infrakamery je snímání teplotního pole těles, jelikož je toto pole lidským okem neviditelné, zobrazuje se barevně či v odstínech šedi (např. na LCD displeji, jenž je součástí kamery). Takto pořízený infračervený snímek infrakamerou se nazývá termogram (viz Obrázek 4). [15]

U technických prostředků určených k získávání informací se při jejich detekci využívá toho, že obsahují prvky (např. odpor), které při funkčnosti vykazují, vzhledem k okolí, větší teplotu. A při použití termografie je následně na displeji infrakamery takový prostředek zobrazen červenou barvou (viz obrázek 4) charakteristickou pro objekty vyzařující větší teplo vzhledem k okolí. [15]

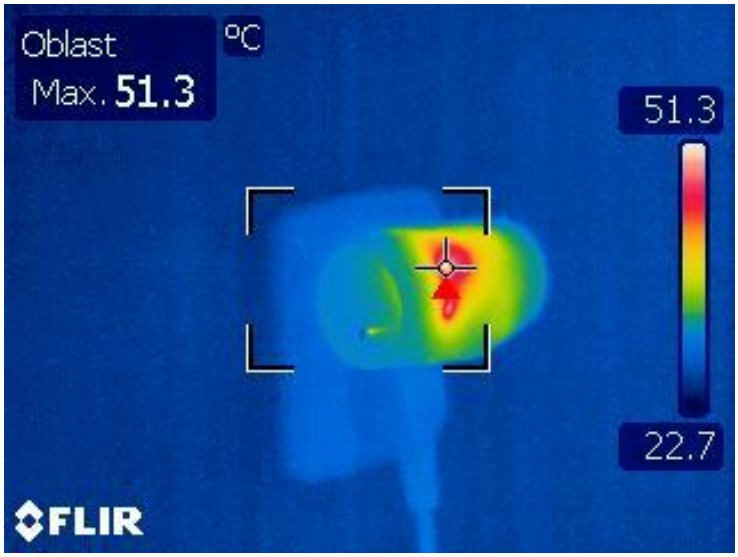
Při práci infrakamerami by měl technik OTP dodržovat určité zásady, které mu mají dopomoci k odhalení skrytého prostředku určeného k získávání informací.

[6] Zdroj: http://www.goldsilver.cz/detektor-nelinearnich-prechodu-nr-900e/

Zásady měření pomocí infrakamer:

- co nejkratší vzdálenost infrakamery (čím menší měřené těleso tím blíže) od měřeného tělesa,
- měření má 2 fáze – identifikace nežádoucího technického prostředku (počáteční měření – probíhá z větší vzdálenosti) a jeho změření (jedná se o již identifikovaný nežádoucí technický prostředek změřený z kratší vzdálenosti, provádí se z důvodu lepší viditelnosti tohoto prostředku na termogramu a zároveň k eliminaci možných chyb při identifikaci),
- správné nastavení úrovně emisivity (schopnost tělesa vyzařovat teplo) měřeného tělesa,
- správné zaměření a zaostření obrazu.[16]

Jednotlivé úrovně emisivity různých materiálů jsou tabulkové hodnoty, pokud však nastane při měření ta situace, že se emisivita daného materiálu v tabulkách nevyskytuje, stačí toto těleso postříkat černým sprejem nebo na něj nalepit černou pásku. Emisivita tohoto tělesa je známá (0,95).[16]



Obrázek 4 Odhalený odposlech s využitím infrakamery[7]

[7] Zdroj: http://www.goldsilver.cz/obranne-technicke-prohlidky-proti-odposlechu-proverky-bytu-kancelari-vozidel-sluzba-non-stop/

3.2.5 Přehledové snímání rádiového spektra

Jednoduchý radiový odposlech (např. VKV minivysílač, UHF odposlech apod.) funguje stejným způsobem jako rádiová stanice, snímá okolní zvuky a v otevřené podobě (bez šifrování) je vysílá do prostoru (pomocí frekvenční nebo amplitudové modulace). Takto vyslaný signál je odchytáván přehledovým snímačem (např. MRA-3). Ten má ve své paměti uloženy všechny bezpečné frekvence. Tyto hodnoty bezpečných radiových frekvencí je nutné předem do paměti přehledového snímače vložit a pro ověření správnosti by měly být ještě prověřeny pomocí spektrálního analyzátoru. Technik poté postupuje tak, že nejdříve zapne přehledový snímač v kontrolovaném prostoru do monitorovacího režimu, poté chvíli čeká, než přístroj projde všechny frekvence a porovná je s frekvencemi uloženými v paměti přístroje. Jestliže je objevena frekvence, která není v paměti přístroje, je technik vizuálně a akusticky upozorněn a s největší pravděpodobností se v zájmovém prostoru nachází odposlechový prostředek.[3]

3.2.6 Taktika vyhledávání v prostoru

Aby byly systémy provedení zcela účinné, je nutné při jejich používání dbát na taktiku vyhledávání v prostoru, která je nedílnou součástí práce technika.

Prohlídky místností se provádí v určitém algoritmu, nejprve se provádí tzv. zvuková kontrola. Kdy se technik pomocí stetoskopu snaží stanovit zvuky uvnitř místnosti, pokud to zvukové pozadí (hluk z ulice apod.) dovoluje. Dále se místnost rozdělí na pomyslné sektory a prohlídka následuje v určitých výškových sledech:

1. první sled – zpravidla pokrývá všechny předměty stojící na podlaze nebo vestavěné ve stěnách do výše středně vysokého nábytku. První sled je časově nejnáročnější a měl by rovněž zahrnovat prohlídku podložek, rohožek a koberců.
2. druhý sled – zahrnuje obvykle výšku od horních částí nábytku ke stropu. Jde převážně o prohlídku obrazů, plaket, nástěnných skříněk, elektrorozvodných krabic, síťových přepínačů, zásuvek apod. V této fázi lze kontrolovat i spodní díly stropních svítidel.
3. třetí sled – zahrnuje stropy, zavěšené stropy, žlaby nebo převisy nepřímého osvětlení, stropní svítidla aj. Tato fáze bývá někdy obtížná pro špatnou přístupnost některých částí.[2]

Jednotlivé taktiky vyhledávání se stanovují podle velikosti místnosti a předpokladu místa či počtu míst, kde by mohl být odposlechový prostředek umístěn.

3.3 Zmapování a zhodnocení výsledků

V této části se zpracovávají získané informace o výsledku OTP, které jsou zadavateli nejdříve sděleny ústně, a poté je mu zaslán protokol o provedené OTP. Tento protokol obsahuje, popis systémů provedení, které byly použity včetně prohlášení o výsledcích jednotlivých měření, prohlášení, že v průběhu OTP bylo odhaleno či neodhaleno technické zařízení určené k získávání informací, přibližná doba jeho umístění (v této souvislosti lze odhalit, kolik důležitých informací tímto způsobem uniklo), místo kde byl umístěn, jakým způsobem bylo s odhaleným nežádoucím technickým prostředkem po jeho objevení zacházeno, obsahuje také upozornění na rizika z hlediska možnosti opětovného napadení odposlechovými prostředky v daných podmínkách a na závěr jsou navrhnuty nová technická a režimová opatření. Je důležité si uvědomit, že výsledek OTP platí jen v okamžiku jejího ukončení. Příchodem osoby, do již zkontrolovaného prostoru, se může situace okamžitě změnit.[17]

3.3.1 Postup techniků při odhalení odposlechového prostředku

Při odhalení odposlechového prostředku nejdříve technik zapíše místo odhalení do protokolu o OTP, poté místo zdokumentuje pomocí fotoaparátu nebo kamery. Následně se technik spolu se zadavatelem dohodne, zda odposlechový prostředek odstranit a přivolat Policii ČR či ponechat k případné dezinformaci pachatele. Na závěr technik provede opětovnou kontrolu prostoru z důvodu možného umístění většího počtu technických prostředků určených k získávání informací.

3.4 Navrhovací část

V této části technik navrhuje nová technická a režimová opatření, jejichž úkolem je omezit či zamezit funkčnost opětovně nainstalovaným odposlechovým prostředkům v místnosti.

Mezi režimová opatření lze zařadit kontrolu a evidenci vstupu osob do vyhrazených místností, kterou je možné řešit instalací kvalitních přístupových systémů. Technickými opatřeními se v této souvislosti myslí instalace systémů pro stálou ochranu proti odposlechovým prostředkům (aplikace bílého či růžového šumu) či zlepšení současného

stavu technické ochrany objektu nebo kompletní přestavbou místnosti na tzv. Faradayovu klec.

3.4.1 Kontrola a evidence vstupu osob do vyhrazených místností

Je řešena instalací elektronické kontroly vstupu. Lze nastavit okruh lidí (časový nebo pohybový), kteří mají do určených prostor povolený či nepovolený vstup. Systém kontroly vstupu pomocí databáze zaznamenává pokusy o neoprávněný pohyb osob přes jednotlivé prostupy a další podezřelé situace. Dále porovnává údaje o pohybu osob, přes jednotlivé prostupy, s údaji uloženými v databázi. Přehled pohybu osob po objektu a neoprávněné prostupy do místností lze zpětně zobrazit prostřednictvím speciálního softwaru. Při vyšetřování pachatele, který umístil odposlechový prostředek, lze pomocí elektronické kontroly vstupu snadno zúžit počet zaměstnanců, se kterými pachatel přišel do styku.[18]

3.4.2 Aplikace bílého šumu

Bílý šum je nespojitý náhodný signál s rovnoměrnou výkonovou spektrální hustotou. Je způsoben nahodilým pohybem elektronů v krystalové mřížce, závisí pouze na teplotě, nezávisí na napětí, proudu ani frekvenci. Je nasazován, v podobě generátoru bílého šumu nebo piezoelektrických či elektrodynamických měničů, jako stálá ochrana proti odposlechovým prostředkům díky své schopnosti překrytí nahrávky vlastním vlněním a zabraňuje tak možnosti převodu zaznamenávané informace do použitelné podoby. Nepatrnou nevýhodou této aplikace je fakt, že bílý šum je pro člověka slyšitelný, z toho důvodu může probíhající jednání lehce rušit. Na druhou stranu v současnosti neexistují technické prostředky, kterými by šel bílý šum odfiltrovat.[3]

3.4.3 Aplikace růžového šumu

Růžový šum se vytváří v důsledku poruch v krystalové mřížce a nečistot v polovodiči. Projevuje se především na nižších kmitočtech. Jeho spektrální hustota klesá směrem k vyšším kmitočtům, a to s kmitočtovou závislostí 1/f, proto také někdy bývá tento šum označován jako šum 1/f. Je charakterizován stejným množstvím energie ve všech oktávách. Stejně jako u bílého šumu je nasazován ve formě generátoru šumu, piezoelektrických či dynamických měničů jako stálá ochrana proti odposlechovým prostředkům. Jeho využití je široké používá se v mnoha fyzikálních, biologických a ekonomických systémech.[19]

3.4.4 Faradayova klec

Jde o místnost, ve které jsou použity různá opatření (viz níže) vedoucí k úplnému odstínění nepřátelských signálů. Jedná se o jednu z nejúčinnějších metod ochrany proti odposlechovým či jiným prostředkům určených k získávání informací. Faradayova klec je svým způsobem preventivní opatření proti informačnímu úniku, je instalována po vstupní prohlídce, která je provedena pomocí systémů provedení OTP. Pokud je vytvořena místnost patřící do první nebo druhé kategorie, není nutné v takto zabezpečené místnosti instalovat žádné další prostředky pro zamezení odposlechů, kromě prostředků, které jsou zahrnuté v konstrukci místnosti, či není zde nutné provádět systémy provedení.

Princip této ochrany je založen na vytvoření kvalitního stínění zájmového prostoru pomocí technických prostředků k tomu určených (generátory šumu, akustické měniče, apod.). Signály odposlechových prostředků či jiných prostředků určených k získávání informací se z důvodu tak kvalitního stínění nemají kam šířit, a tak nedochází k úniku informací.[20]

Existují dvě kategorie Faradayových klecí (místností):

1. Absorpční místnosti – obsahují absorpční prvky, které zajišťují, že se přítomné signály při dopadu na absorpční materiál mění v tepelnou energii a snižuje se tím počet odrazů v místnosti. Pokud má být absorpce účinná (frekvence 150 MHz a výš), je důležité, aby bylo z každé strany místnosti alespoň 2 m místo. Čím vyšší je tato frekvence, tím je vzdálenost kratší.
2. Neabsorpční místnosti – zde přítomné signály jsou utlumeny několikanásobnými odrazy od stínících stěn. V těchto místnostech jsou pro síťové a jiné rozvody použity kvalitní filtry, které zabraňují obousměrnému průniku signálů. Tyto místnosti jsou při dokončení speciálních úprav vzhledově zcela stejné jako jakékoliv jiné kancelářské prostory.[20]

Kromě výše uvedených kategorií existují Faradayovy místnosti (klece), které nemají s pravými Faradayovými místnostmi vůbec nic společného. Jejich konstrukce jsou mnohdy amatérské se spoustou levných náhražek opravdových a kvalitních prostředků a instalace těchto prostředků je vykonávána nezkušenými konstruktéry. Tyto místnosti mohou tak způsobit značné bezpečnostní riziko.

Obrázek 5 Faradayova absorpční místnost[8]

3.5 Závěrečná část

Pokud je OTP prováděna jako preventivní opatření před důležitým jednáním, je nutné, aby po skončení prohlídky byly všechny vstupy do místnosti uzamčeny, zapečetěny a měly by být střeženy fyzickou ostrahou. Z toho vyplývá, že OTP by měla být posledním úkonem v zájmovém prostoru, jinak je tato činnost neefektivní. Dále se provádí kontrola frekvenčních pásem (přehledové snímání radiového spektra) po celou dobu jednání v zájmovém prostoru, většinou je prováděna v přilehlé místnosti co nejblíže prostoru, ve kterém probíhá jednání. Tato kontrola má vyloučit činnost dálkově ovládaných odposlechových prostředků, které při prohlídce mohly v klidovém stavu uniknout pozornosti a nebyly technickými prostředky pro realizaci OTP detekovány.[2]

Pokud je OTP prováděna za primárním účelem odhalení odposlechového prostředku, je možné pokračovat v instalaci prostředků určených pro permanentní ochranu z důvodu možného opětovného nasazení. Poté není nutné místnost nijak speciálně hlídat.[2]

[8] Zdroj: http://www.stinene-komory.cz/

II. PRAKTICKÁ ČÁST

4 TYPY TECHNICKÝCH PROSTŘEDKŮ URČENÝCH K ZÍSKÁVÁNÍ INFORMACÍ

Typy technických prostředků určených k získávání informací (neboli odposlechových prostředků) se dělí na skryté mikrofony (mikrodiktafony, GSM odposlechy, UHF odposlechy, VKV odposlechy, elektronické stetoskopy, laserové odposlechové zařízení, parabolické mikrofony), skryté minikamery a jiné technické prostředky určené k získávání informací, kterými jsou např. drátový a radiový odposlech telefonní linky.

Ceny jednotlivých odposlechových prostředků jsou uvedeny v příloze P I.

4.1 Mikrodiktafony

Jedná se o pasivní typy odposlechových prostředků, zaznamenané informace (zvuk, video) zůstávají v paměti zařízení (nejsou vysílány). Tyto záznamy jsou pak přes rozhraní USB nahrávány do PC. Přenos ze zařízení do PC lze zabezpečit heslem, bez jeho správného zadání se k nahrávkám nedostane oprávněná osoba.[21]

Osoba, jejímž úmyslem je odposlouchávat informace v místnosti, musí toto zařízení nepozorovaně vnést do místnosti, skrytě umístit a posléze zařízení s nahraným záznamem z místnosti nepozorovaně vynést. Dalším způsobem je umístění mikrodiktafonu přímo na osobě nebo v její bezprostřední blízkosti, z důvodu odposlechu informací při schůzce.

4.1.1 Mikrodiktafon B21 300 CZ

Jedná se o miniaturní digitální hlasový záznamník (hmotnost pouze 8 gramů). Obsahuje vysoce citlivý mikrofon, který je možné aktivovat k nahrávání časově či hlasově. Dále obsahuje kódovou ochranu pro přístup k záznamům a nastavení. Připojení k PC je realizováno pomocí rozhraní USB a prostřednictvím programu Record Manager je možné si stáhnout získané nahrávky do počítače. Všechny záznamy jsou označeny přesným datem a časem pořízení. Volitelně lze v record manageru nastavit kód PIN pro vstup k záznamům a k nastavení. Bez znalosti správného PIN kódu není umožněn přístup k záznamům ani k nastavení. Heslo je možné odstranit, v tomto případě však automaticky dochází k nevratnému vymazání všech záznamů a obnově továrního nastavení.[22]

Obrázek 6 Mikrodiktafon

B21 300 CZ[9]

Tabulka 1 Technické parametry Mikrodiktafonu B21 300 CZ[10]

Doba provozu	režim záznam - až 70 hodin pohotovostní režim - až 240 hodin stand-by režim (časová aktivace) - až 2 měsíce
Rozměry	40 x 10 x 15 mm
Vnitřní paměť	2 GB, až 300 hodin záznamu
Hmotnost	8 g (bez baterie)
Napájení	Jedna baterie alkalická AG 13 nebo vzduchově-zinková PR 44 1,4 V
Kompresní algoritmy	Bez komprese, µ-Law[11], ADPCM[12] (2 až 4 b)
Vzorkovací frekvence	5,5;8;11;16; nebo 22 kHz
Vzdálenost zdroje zvuku od mikrofonu	7-9 metrů všemi směry
Provozní teplota	0 °C až 40 °C
Režim záznamu	Mono

[9] Zdroj: http://wordpress.detekce.com/wp-content/uploads/2010/04/Mikroodposlech1.jpg

[10] Zdroj: http://www.odposlechy.com/mikro-diktafon-b21-cz-300-gen-2-serie-pro

[11] Nejběžnější kompresní algoritmu, tento typ se používá ke komunikaci po telefonních sítích v USA a Japonsku. Zdroj: http://cs.wikipedia.org/wiki/G.711

[12] Kompresní algoritmus s rozlišením 2 až 4 bity.

4.2 GSM odposlechy

Jde o prostředek bezdrátového odposlechu, který lze díky rozlehlosti mobilní sítě GSM využít na neomezenou vzdálenost. Jeho omezení je dáno pouze kapacitou baterie, ze které je napájen. Eliminovat tento problém lze použitím trvalého napájení z elektrické sítě nebo zabudováním do elektrického permanentně napájeného elektrického spotřebiče. GSM odposlech je v takovém případě schopen pracovat nepřetržitě.[23]

4.2.1 GSM bezdrátový odposlech G500

Jedná se o profesionální odposlechové zařízení, do kterého je možné vložit libovolnou SIM kartu českého nebo zahraničního operátora a po vytočení jejího čísla lze ihned provádět odposlech prostoru až do vzdálenosti 10 metrů od polohy zařízení. Z jakéhokoliv místa na světě lze poslouchat, co se děje v prostoru kolem zařízení. Společně s odposlechem v reálném čase lze provádět záznam pomocí funkce mobilního telefonu, ze kterého je odposlechový hovor realizován.[24]

Tabulka 2 Technické parametry GSM bezdrátového odposlechu G500[13]

Doba provozu	při nepřetržitém odposlechu 6 až 8 hodin v pohotovostním režimu 6 dní
Rozměry	43 x 35 x 17 mm
Hmotnost	40 g
Napájení	Integrovaný Li-ion akumulátor 100-240 V AC[14] (automatické přepínání)
Podporované sítě GSM	850/900/1800/1900 MHz
Hardware pro zvýšení kvality odposlechu	Zvukový procesor DSP[15], Hlasový zesilovač se systémem filtrace okolních ruchů
Citlivost mikrofonu	až 10 metrů

[13] Zdroj: http://www.odposlechy.com/gsm-bezdratovy-odposlech-g500

[14] AC – označení střídavého proudu.

[15] Digitální signálový procesor je mikroprocesor používaný při zpracování digitálních signálů. Zdroj: http://cs.wikipedia.org/wiki/Digit%C3%A1ln%C3%AD_sign%C3%A1lov%C3%BD_procesor

Obrázek 7 GSM odposlech G500[16]

4.3 UHF odposlechy

UHF odposlechy (štěnice) jsou technické prostředky určené pro odposlech rozhovorů v místnosti na dálku v reálném čase. Dosah těchto prostředků je až 300 metrů v bytové zástavbě a až 750 metrů ve volném prostoru. Systém je složen z vysílače (štěnice) a přijímače. Vysílač je umístěn v prostoru a funguje jako skrytý mikrofon, který následně vysílá signál, jenž obsahuje mikrofonem zachycené informace, do prostoru. Tento signál lze poslechnout pomocí UHF přijímače, ke kterému je možno připojit diktafon pro nahrávání záznamu nebo libovolná sluchátka pro tichý odposlech. Možností je provádět poslech a záznam současně.[25]

Osoba, jež chce odposlouchávat pomocí UHF odposlechu, musí tento odposlech nepozorovaně vnést do místnosti a tam, co nejlépe umístit. Tyto odposlechy bývají přímo zabudovány v předmětu, který v místnosti stačí pouze vyměnit a odposlouchávaná osoba na první pohled prakticky nic nepozná.

UHF odposlech lze zabudovat skoro do každého předmětu denní i osobní potřeby, dle přání zákazníka. A tak je možno tento odposlech skrýt např. do vázy, sošky, popelníku, kalkulačky, zápisníku, plnicího pera, hodinek, cigarety, mobilního telefonu, zapalovače,

[16] Zdroj: http://www.odposlechy.com/thumbnails/4de7bc88-c20c-443f-b330-4506c113b31f/750x750

rozdvojky apod. Dále je možné tyto štěnice, skrytě umístit na těle osoby, v šatech nebo osobních věcech určené na monitorování hovoru při schůzce.[3]

Obrázek 8 Propiska se zabudovaným UHF odposlechem[17]

4.3.1 UHF bezdrátový odposlech R500 CR

Tabulka 3 Technické parametry UHF odposlechu R500 CR[18]

Doba provozu	60 hodin na běžnou baterii CR 123
Rozměry	30 x 22 x 15 mm + 30 mm anténka
Dosah	v zástavbě až 300 metrů, ve volném prostoru 750 metrů
Napájení	Lithiová 3V baterie CR 123
Vysílací frekvence	UHF (ultra vysoká frekvence) pásmo (350-450 MHz)
Kompatibilní přijímače	UHF přijímač Alinco S UHF přijímač Alinco MK
Doplňkové funkce	Automatické vyrovnávání citlivosti

[17] Zdroj: http://spycity.com.au/images/products/detail/FPK-250.jpg

[18] Zdroj: http://www.odposlechy.com/uhf-bezdratovy-odposlech-r500-cr

Obrázek 9 UHF odposlech
R500 CR[19]

4.3.2 UHF přijímač Alinco S

Jde o malý digitální přijímač pro příjem signálů z UHF bezdrátových odposlechů řady R400 a R500. Je upraven pro připojení sluchátek a diktafonu. Při propojení s diktafonem lze pořizovat prakticky nepřetržitý záznam z UHF odposlechu. Nejlepší možností je připojení diktafonu s hlasovou aktivací, která šetří cenné místo v paměti.[26]

Tabulka 4 Technické parametry UHF přijímače Alinco S[20]

Doba provozu	trvalý příjem signálu - 6 hodin, režim stand-by - 11,5 hodin, připojení na síť - neomezená
Rozměry	57 x 98 x 28 mm + 16 cm všesměrová anténa
Frekvenční rozsah	433 až 446 MHz
Napájení	2x AA baterie
Hmotnost	164 g

[19] Zdroj: http://www.odposlechy.com/thumbnails/4d96fff2-9f74-4ac1-9844-7a40c113b31f/750x750

[20] Zdroj: http://www.odposlechy.com/uhf-prijimac-alinco-s

Obrázek 10 UHF přijímač Alinco
S s připojeným diktafonem[21]

4.4 VKV minivysílače

Tyto typy odposlechových prostředků jsou určené pro odposlech rozhovorů z cílového prostoru (kanceláře, bytu, apod.) na vzdálenost od 10 do 300 m. Hlavní výhodou u těchto technických prostředků je nízká cena, malé rozměry a rychlá instalace, velmi dobrý zvuk a uspokojivost mluveného slova. Nevýhodou u těchto minivysílačů bývá životnost napájecího zdroje.[3]

Systém, aby fungoval, musí obsahovat vysílač (VKV minivysílač) a k němu kompatibilní přehledový snímač.

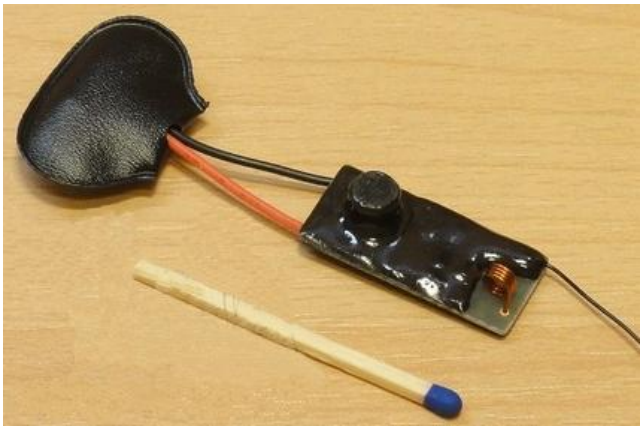
4.4.1 VKV minivysílač LCBUGmini

Tento odposlechový prostředek je konstruován za pomocí SMT technologie, kdy vývody součástek se pájí přímo na povrch plošného spoje. Jeho vysílací frekvence je v neveřejném Air (leteckém) pásmu. Signál nelze zaznamenat na běžném přijímači a fungování prostředku je proto diskrétní. K poslechu je nutný speciální přijímač pro tento typ pásma. Ideálním je přehledový přijímač (digitální scanner).[27]

[21] Zdroj: http://www.odposlechy.com/thumbnails/4da5d146-df84-4dfe-9ee8-4ca7c113b31f/750x750

Tabulka 5 Technické parametry VKV minivysílače LCBUGmini[22]

Doba provozu	alkalická baterie 9 V - okolo 36 hodin 9V baterie 1200 mAh - okolo 180 hodin
Rozměry	28 x 12 x 6 mm
Vysílací frekvence	110 až 136 MHz
Napájení	Baterie 9V
Dosah	v zástavbě - až 100 metrů, ve volném prostoru - až 250 metrů



Obrázek 11 VKV minivysílač LCBUGmini[23]

4.4.2 VKV přijímač M9 Air

Jedná se o analogový přijímač určený pro příjem a poslech signálu z VKV minivysílačů. Přijímač je vybaven teleskopickou (výsuvnou) anténou, analogovou stupnicí, vyhledávačem signálu, regulátorem hlasitosti a regulovatelnou šumovou bránou (tzv. squelch, určuje minimální úroveň přijímaného signálu nad úrovní šumu, který bude reprodukován). Pro poslouchání slouží vestavěný reproduktor, případně pro diskrétní poslech lze připojit sluchátka. Přijímaný signál z VKV minivysílače je možno nahrávat na vhodný diktafon.[28]

[22] Zdroj: http://www.odposlechy.com/vhf-bezdratovy-odposlech-r250

[23] Zdroj: http://www.infosafe.cz/obrazek/2/odposlech-lcbugmini-1-jpg/

Tabulka 6 Technické parametry přijímače M9[24]

Rozměry	63 x 154 x 41 mm
Frekvenční pásmo	neveřejné pásmo Air - 110 až 136 MHz, CCIR[25] - 87 až 108 MHz, OIRT[26] - 66 až 73 MHz
Napájení	4 x baterie AA, pro 6 V síťové napájení
Hmotnost	155 g (bez baterií)
Doba provozu	okolo 8 hodin (alkalické baterie)
Anténa	teleskopická všesměrová

Obrázek 12 Přijímač M9[27]

[24] Zdroj: http://www.odposlechy.com/vhf-prijimac-m9-air

[25] Pásmo, v němž vysílají běžná FM rádia.

[26] Pásmo, v němž vysílali rádia od roku 1958 do roku 1995. Dnešní rádia už toto pásmo nenaladí.

[27] Zdroj: http://www.infosafe.cz/obrazek/2/prijimac-m9-air-1-jpg/

4.5 Elektronické stetoskopy

Toto zařízení lze použít pro odposlech přes zdi nebo jiné objekty. Zařízení obsahuje vysoce citlivý keramický mikrofon, který je vyroben z nerezové oceli. Senzor v mikrofonu je tvořen magnetickou částí, která je propojena s keramickým senzorem, který převádí vibrace do audio signálu a zesiluje je.[29]

4.5.1 Odposlech přes zdi – Elektronický stetoskop

Tabulka 7 Technické parametry elektronického stetoskopu[28]

Rozměry	85 x 54 mm
Napájení	9 V baterie
Hmotnost	145 g
Doba provozu	55 až 60 hodin
Anténa	Teleskopická všesměrová
Vstup a Výstup	3,5 mm jack

Obrázek 13 Elektronický stetoskop[29]

[28] Zdroj: http://www.odposlechy24.cz/odposlech-pres-zdi-stetoskop/

[29] Zdroj: http://www.odposlechy24.cz/files/images/odposlech_pres_zdi.jpg

4.6 Laserové odposlechové zařízení

Toto zařízení slouží k odposlouchávání osob na dálku bez nutnosti vstupu do cílového prostoru. Funguje na principu odrazu infračerveného paprsku od vibrující okenní tabule. Vibrace jsou způsobeny komunikací osob v odposlouchávané místnosti. Laserové odposlechové zařízení se skládá ze tří částí, a to laserového vysílače, přijímače a kvalitního zesilovače. Infračervený paprsek je vyslán z laserového vysílače a odráží s od skleněné tabule, která se chvěje ve frekvenci mluveného hlasu v místnosti. Přijímač následně tento modulovaný (modulace je dána vibrací tabule) paprsek přijme a automaticky ho převede na elektrický signál (hlasovou informaci). Poté je signál filtrován a v zesilovači zesílen popřípadě v diktafonu zaznamenán.[30]

Velkou nevýhodou tohoto zařízení je jeho robustnost a náročnost na instalaci. Dosah takového zařízení je okolo 200 m.[3]

4.6.1 Laser EMAX – 3500

Laserové odposlechové zařízení EMAX – 3500 se skládá ze tří částí:

- Laserový vysílač,
- Laserový přijímač,
- Zesilovací a nahrávací jednotka.

Tabulka 8 Technické parametry laserového vysílače Laser EMAX - 3500[30]

Proudové zatížení	100 mA
Napájení	8 x 1,5 V AAA baterie, ze sítě
Vlnová délka	750 - 840 nm
Doba provozu	na baterie - okolo 10 hodin, ze sítě - nepřetržitě
Montáž	Standardní - na stativ
Objektiv	135 mm
Výstupní výkon	5 mW

[30] Zdroj: http://www.electromax.com/laser.html

Obrázek 14 Laserový vysílač Laser EMAX - 3500[31]

Tabulka 9 Technické parametry laserového přijímače Laser EMAX – 3500[32]

Objektiv	500 mm
Napájení	9 V baterie
Proudové zatížení	10 až 30 mA
Doba provozu	15 až 50 hodin (v závislosti na nastavené hlasitosti)
Montáž	Standardní - na stativ

Obrázek 15 Laserový přijímač Laser EMAX -3500[33]

Laserová zesilovací a nahrávací jednotka EMAX - 3500 je propojena s laserovým přijímačem, má nastavitelné zesílení a je možné k ní připojit sluchátka nebo reproduktory přes klasický 3,5 mm jack. Dále obsahuje nastavitelný ekvalizér a vestavěný hlasový záznamník.

[31] Zdroj: http://gadgets.vtm.zive.cz/Getfile.aspx?id_file=843624339

[32] Zdroj: http://www.electromax.com/laser.html

[33] Zdroj: http://www.electromax.com/images/Laser3500%20-%20Big%20K%20rzd.jpg

Obrázek 16 Zesilovací a nahrávací technika Laser EMAX – 3500[34]

Obrázek 17 Laserové odposlechové zařízení EMAX - 3500[35]

[34] Zdroj: http://www.electromax.com/images/Laser3500%20-%20Item%20rzd.jpg

[35] Zdroj: http://www.electromax.com/images/laser3500.jpg

4.7 Parabolické mikrofony

Tyto mikrofony jsou založeny na principu parabolické odrazné plochy a koncentrace akustické energie do ohniska paraboly. Parabolické mikrofony mají tvar satelitní antény, kdy v ohnisku paraboly se nachází kvalitní mikrofon spojený s velmi citlivým zesilovačem. Nevýhodou těchto zařízení je, že snímá všechny zvuky, které jsou na trase sledování. Ideální použití mikrofonu je tedy v noci (nízká hladina okolního ruchu) a na otevřeném prostranství s nízkým okolním hlukem, např. v parku v lese, na louce nebo na hřišti.[3]

4.7.1 Parabolický mikrofon Spektra G50 PRO

Profesionální odposlechové zařízení s možností digitálního záznamu určené pro odposlech zvuků na delší vzdálenosti. Jelikož se jedná o mikrofon na „statickém stanovišti“ jeho dosah může být až okolo 500 m.

Tabulka 10 Technické parametry parabolického mikrofonu Spektra G50 PRO[36]

Typ mikrofonu	elektretový
Charakteristika mikrofonu	kardiodní[37]
Frekvenční rozsah	48 až 18000 Hz
Délka mikrofonu	15 až 50 hodin (v závislosti na nastavené hlasitosti)
Formát výstupu z nahrávání	MP3[38] soubor 44,1 kHz 392 kb/s
Doba záznamu	1 hodina a 15 min při nejlepší kvalitě záznamu

[36] Zdroj: http://www.bestparabolicmicrophones.com/documents/G4-G50brochure.pdf

[37] Kardioidní charakteristika - potlačuje příjem zvuků za mikrofonem.

[38] MP3 - je formát ztrátové komprese zvukových souborů.

Obrázek 18 Parabolický mikrofon
Spektra G 50 PRO - EX[39]

4.8 Skryté minikamery

Jedná se o miniaturní odposlechové prostředky zaznamenávající současně obraz i zvuk ve vysoké kvalitě. Tyto minikamery mohou být opatřeny pohybovým (automatické zapnutí záznamu při detekci pohybu), časovým (minikamera je zapnuta ve zvoleném času) a hlasovým aktivačním (aktivace kamery hlasem) systémem. Jelikož je průměr objektivu minikamery okolo 1 mm, lze takovou kameru umístit do kamufláže, a umocnit tak nepozorované odposlouchávání. Nejčastější kamufláží jsou oděvy (knoflík, kravata, sako), příruční zavazadla (kufřík, kabelka, taška) a běžné předměty nacházející v každé kanceláři (šanon, hodiny, lampička) nebo v domácnosti (kniha, dekorační předměty, budík). Vybrané minikamery je možné rozšířit o GPS modul, kdy k výslednému záznamu jsou připojeny GPS souřadnice míst, kde byl záznam pořízen.[31]

[39] Zdroj: http://www.bestparabolicmicrophones.com/documents/G4-G50brochure.pdf

4.8.1 Pero s minikamerou

Tabulka 11 Technické parametry minikamery kamuflované v peru[40]

Rozlišení videa	720 x 480 px
Rozlišení fotografií	1280 x 960 px
Zvuk	128 kbps PCM[41]
Paměť	Micro SD karta[42]
Napájení	Li - Ion baterie - nabíjení přes USB kabel
Doba záznamu	40 až 90 min
Rozměry	140 mm x 13 mm
Podporované operační systémy	Windows, Linux, MAC OS
Přenos dat	rozhraní mini USB nebo přes SD kartu

Obrázek 19 Pero s minikamerou[43]

[40] Zdroj: http://www.odposlech-tech.cz/product/pero-s-kamerou-pamet-sd-karta-akce-306/

[41] PCM – je modulační metoda převodu analogového zvukového signálu na signál digitální.

Zdroj: http://cs.wikipedia.org/wiki/Pulzn%C4%9B_k%C3%B3dov%C3%A1_modulace

[42] Micro SD karta - je paměťová karta používaná v přenosných zařízeních.

Zdroj: http://cs.wikipedia.org/wiki/Secure_Digital

[43] Zdroj: http://www.odposlech-tech.cz/product/pero-s-kamerou-pamet-sd-karta-akce-306/

4.8.2 Hodinky s kamerou

Tabulka 12 Technické parametry minikamery kamuflované v hodinkách[44]

Rozlišení videa	1280 x 960 px
Rozlišení fotografií	1280 x 960 px
Kódování videa	M - JPEG[45]
Paměť	vestavěná 4 GB
Formát fotografie	JPEG[46]
Kapacita baterie	200 mAh
Hmotnost	115 g
Podporované operační systémy	Windows, Linux, MAC OS
Přenos dat	rozhraní USB

Obrázek 20 Hodinky s minikamerou[47]

[44] Zdroj: http://www.odposlech-tech.cz/product/hodinky-s-kamerou-stribrne-provedeni-hd-234/

[45] M – JPEG - je formát videa, který je nejčastěji používán v digitálních a IP kamerách. Každý snímek je zde komprimován zvlášť podle standardu JPEG. Zdroj: http://cs.wikipedia.org/wiki/MJPEG

[46] JPEG - je standardní metoda ztrátové komprese používané pro ukládání počítačových obrázků ve fotorealistické kvalitě. Zdroj: http://cs.wikipedia.org/wiki/JPEG

[47] http://www.odposlech-tech.cz/resize/domain/odposlech/files/obruc/obruc4.jpg?w=640&h=480

4.8.3 Sluneční brýle s minikamerou

Tabulka 13 Technické parametry minikamery kamuflované ve slunečních brýlích[48]

Hmotnost	okolo 50 g
Výdrž baterie	100 až 150 min
Volitelný režim	zvukové nahrávky, video + zvuk, fotografie, web kamera
Paměť	vestavěná 4 GB
Formát fotografie	JPEG
Video formát	AVI[49]
Rozlišení fotografie	1600 x 1200 px
Přenos	rozhraní USB
Typ baterie	Dobíjecí Li - Ion baterie

Obrázek 21 Sluneční brýle s kamerou[50]

[48] Zdroj: http://www.odposlech-tech.cz/product/slunecni-bryle-s-kamerou-242/

[49] AVI – je multimediální souborový formát. Může obsahovat video i zvukovou stopu a umožňuje jejich synchronní přehrávání. Zdroj: http://it-slovnik.cz/pojem/avi

[50] Zdroj: http://www.odposlech-tech.cz/resize/domain/odposlech/files/bryle/brylec1.jpg?w=640&h=480

4.8.4 Klíčenka s minikamerou

Tabulka 14 Technické parametry minikamery kamuflované v klíčence[51]

Rozměry	50 x 35 x 12 mm
Baterie	Li - Ion výdrž až 60 min
Formát videa	AVI
Paměť	8 GB SD karta
Formát fotografie	JPEG
Rozlišení fotografie	4032 x 3024 px
Rozlišení videa	1280 x 720 px
Dobíjení a přenos dat	rozhraní USB

Obrázek 22 Klíčenka s minikamerou[52]

4.9 Drátový odposlech telefonní linky

Takový odposlech skládá ze dvou vodičů (obvykle speciálně upravené propichovací svorky), které se připojují paralelně (paralelní propojení může zajistit i rozdvojka na dva konektory RJ 11[53]) k telefonnímu vedení. Na konci takových vodičů je umístěno sluchátko nebo diktafon. Nespornou výhodou tohoto odposlechového prostředku je možnost napájení

[51] Zdroj: http://www.odposlech-tech.cz/product/klicenka-s-kamerou-hd-rozliseni-novinka-308/

[52] Zdroj: http://www.odposlech-tech.cz/product/klicenka-s-kamerou-hd-rozliseni-novinka-308/

[53] RJ 11 – standardní konektor (2 páry – 4 dráty), který je využíván pro telefonní vedení. Zdroj: http://www.tech-faq.com/rj-11.html

přímo z telefonní linky, díky kterému je zaručeno dlouhodobé odposlouchávání. Některé typy těchto technických prostředků obsahují funkci aktivaci hlasem, která umožňuje lepší a jednodušší zpracování záznamu. Odposlech lze, pro poslech či záznam, připojit k reproduktorům nebo k diktafonu.

4.9.1 Odposlech pevné linky TO LINE 1

Jedná se o odposlechový prostředek, který se připojuje na telefonní linku pomocí propichovacích svorek, není tedy třeba jejího rozpojení. Tento technický prostředek nepotřebuje zvláštní napájení, napájení je realizováno přímo z telefonní linky.[32]

Obrázek 23 Odposlech pevné linky TO LINE 1[54]

4.9.2 Odposlech pevné linky TO LINE 2

Jedná se o odposlechový prostředek určený pro automatické a skryté nahrávání telefonních hovorů na pevné telefonní lince. Adaptér se připojuje na telefonní linku pomocí konektoru RJ 11. Odposlech je napájen přímo z telefonní linky. Odposlech lze, pro poslech či záznam, připojit k reproduktorům nebo k diktafonu.[33]

[54] Zdroj: http://www.odposlechy.com/thumbnails/4db17956-e040-40a8-8fb2-7659c113b31f/750x750

Obrázek 24 Odposlech pevné linky TO LINE 2[55]

4.9.3 Digitální diktafon Olympus

Jedná se o hlasový záznamník určený pro propojení s přijímači odposlechové techniky, ale i s drátovými a radiovými odposlechy pevné linky. Dále disponuje zejména nastavitelnou funkcí aktivace záznamu hlasem. Pokud je aktivace hlasem zapnutá, spustí se nahrávání v okamžiku, kdy přístroj zaregistruje zvuk. Nahrávání se pozastaví, pokud není slyšet žádný zvuk. Díky tomu přehrávač zbytečně nenahrává ticho a zároveň šetří místo v paměti.[34]

[55] Zdroj: http://www.odposlechy.com/thumbnails/4dbab1e5-9880-4a73-8ee7-1479c113b31f/750x750

Tabulka 15 Technické parametry digitálního diktafonu Olympus[56]

Formát nahrávek	MP3/WMA[57]
Napájení	2x AAA baterie 1,5 V, trvalé napájení pomocí USB rozhraní
Doba provozu (vestavěná paměť)	nahrávání až 51 h, přehrávání až 19 h
Rozměry	110 x 38,9 x 16 mm
Hmotnost	84 g
Paměť	vestavěná 4 GB, rozšíření kartami typu Micro SD/SDHC[58]

Obrázek 25 Digitální diktafon Olympus[59]

4.10 Radiový odposlech telefonní linky

Jedná se o odposlech telefonní linky, který slouží k odposlouchávání telefonních hovorů na dálku, pomocí UHF vysílače, který je uzpůsoben tak, aby snímal zvuky z telefonní linky, a následně je pomocí radiových vln (okolo 433 MHz) odesílal. Tento signál je možné přijmout na běžném přijímači UHF frekvencí (např. Alinco S). UHF vysílač je umístěn v obalu či kamufláži a připojen k telefonní lince, a to buď sériově, nebo paralelně. Paralelní zapojení má tu výhodu, že má menší spotřebu proudu a tedy i menší možnost

[56] Zdroj: http://www.odposlechy.com/digitalni-diktafon-olympus-4-gb

[57] WMA - je komprimovaný zvukový formát vyvinutý jako součást Windows Media. Zdroj: http://cs.wikipedia.org/wiki/WMA

[58] Micro SDHC – novější typ Micro SD karty s kapacitou od 4 GB.

[59] Zdroj: http://www.odposlechy.com/thumbnails/4da99b98-3450-42ec-89d0-25abc113b31f/750x750

odhalení a možnost připojení kdekoliv na trase telefonní linky. U sériového způsobu se přeruší bílý vodič telefonní linky a propojí se s UHF vysílačem. Prostředek je napájen ze sítě (nepřetržitý provoz) nebo pomocí baterií (omezený provoz kapacitou baterie). Příkladem radiového odposlechu telefonní linky jsou Radiový odposlech pevné linky – rozbočka (viz Obrázek 26) a Radiový odposlech pevné linky – parazit (viz Obrázek 27).[35]

Obrázek 26 Radiový odposlech pevné linky – rozbočka[60]

Obrázek 27 Radiový odposlech pevné linky - parazit[61]

[60] Zdroj: http://www.odposlechy24.cz/files/images/linka001.jpg

[61] Zdroj: http://www.odposlechy24.cz/files/images/uhf_parazit.png

5 TYPY TECHNICKÝCH PROSTŘEDKŮ K REALIZACI OTP

Úkolem těchto technických prostředků je co největší pomoc technikům při vyhledávání odposlechových prostředků (spektrální analyzátory, detektory nelineárních přechodů, infrakamery, doplňkové jednoúčelové přístroje, radiové analyzátory, detektory vysokofrekvenčního pole), popřípadě zamezení funkce odposlechových prostředků (generátory šumu).

5.1 Spektrální analyzátory

Spektrální analyzátor je měřicí přístroj, který měří ve frekvenční doméně a graficky zobrazuje frekvenci a výkonovou úroveň signálu s definovanou opakovatelnou přesností. Měření takovým přístroje je velmi složité, proto je nutné, aby přístroj ovládal pouze zkušený technik, jenž OTP provádí. Tento přístroj využívá k měření metodu triangulace radiového spektra.[36]

Slouží k odhalování aktivních odposlechových prostředků s bezdrátovým radiovým přenosem.

Základními parametry spektrálních analyzátorů jsou:

- frekvenční rozsah (až několik desítek GHz),
- typ frekvenční stupnice (lineární a logaritmická),
- dynamický rozsah (určen šumovým prahem a úrovní maximálního měřeného signálu).[37]

5.1.1 Spektrální analyzátor OSC – 5000 DELUX OSCOR

Kompaktní souprava mikropočítačem řízeného přijímače se spektrálním analyzátorem v kufříku, která slouží k odhalování prakticky všech druhů radiových odposlechů včetně odposlechů, které používají k přenosu infračervené záření. Dále je možné změřit veškerá vedení v prostoru (silnoproud i slaboproud) a odhalit tak prostředky, které vykonávají svoji činnost pomocí tohoto napojení. Při připojení PC přes rozhraní USB je možné pomocí speciálního softwaru pracovat s naměřenými údaji (exportovat data do tabulek, exportovat grafy apod.).[38]

Přístroj zpracovává všechny druhy modulací, má aktivní přepínání antén (včetně sondy na kontrolu magnetofonů), umožňuje kontrolu síťových kabelů a telefonních linek, obsahuje LCD displeje a tříbodový lokátor vyzařovaného signálu.[38]

Tabulka 16 Technické parametry spektrálního analyzátoru OSC – 5000 DELUX OSCOR[62]

Frekvenční rozsah	10 kHz až 3 GHz
Typy antén	smyčková anténa - 10 až 500 kHz, aktivní Whip - 500 kHz až 1500 MHz, všesměrová anténa Discone - 1,5 až 3 GHz, sonda na kontrolu rozvodů – 10 kHz až 5 MHz
Audio výstup	pro poslech možno připojit sluchátka
Displej	128 x 256 px
Napájení	interní baterie (výdrž 3 hodiny), ze sítě
Rozměry	15,9 cm x 47 cm x 36,8 cm
Hmotnost	13,2 kg
Přenos dat a komunikace	rozhraní USB
Dynamický rozsah	90 dB

Obrázek 28 Spektrální analyzátor OSC – 5000 DELUX OSCOR[63]

[62] Zdroj: http://www.securo.cz/files/OSCOR.pdf

[63] Zdroj: http://wordpress.detekce.com/wp-content/uploads/2011/02/Oscor.jpg

5.2 Detektory nelineárních přechodů

Slouží k prověřování prostor, bytů, kanceláří, ve kterých je předpoklad umístění odposlechového prostředku. Je schopný odhalit prakticky všechny typy odposlechových prostředků, v jejíž bezprostřední blízkosti se nenachází přístroj obsahující polovodičové součástky. Jeho nespornou výhodou je, že dokáže vyhledat odposlechové prostředky, které do okolí nevyzařují žádný radiový signál (detekuje polovodičové součástky obsažené v odposlechovém prostředku), což metody zaměřené na radiové frekvenční spektrum neumí. Obsahuje v sobě vysílač, který vysílá určitou frekvenci do prostoru, a přijímač následně vyhodnocuje frekvenci odraženou (princip detekce viz kapitola 3.2.3).

5.2.1 Detektor nelineárních přechodů NJE – 4000 ORION

Jde o velmi citlivý detektor se širokou škálou možných nastavení, určený pro operativní vyhledávání odposlechových prostředků, skryté elektroniky, minikamer, různých elektronických součástek, které jsou použity v odposlechových a monitorovacích prostředcích.[39]

Výhody:

- nízká hmotnost, vyvážený ergonomický design pro snadné používání,
- vysoký vysílací výkon určený pro vyhledávání ve velkých oblastech,
- obsahuje bezdrátová sluchátka a grafický displej,
- minimální čas pro nastavení,
- neobsahuje žádné kabely nebo objemné přijímače,
- standardní typ baterie s dlouhou dobou výdrže,
- dynamická regulace výkonu pro vyhledávání hrozby, automatické nebo ruční ovládání,
- kruhová polarizovaná anténa zkracuje dobu hledání a zvyšuje spolehlivost,
- duální harmonické algoritmy minimalizují falešné poplachy.[39]

Tabulka 17 Technické parametry detektoru nelineárních přechodů NJE – 4000 ORION[64]

Vysílač	kmitočtové pásmo: 880 až 1005 MHz
Výkon vysílače	až 1,4 W
Přijímač	kmitočtová pásma: 2. (1760 až 2010 MHz) a 3. (2640 až 3015 MHz) harmonická
Hmotnost	1,54 kg
Napájení	akumulátor 7,2 V typu NiMH (výdrž 3 hodiny), nabíjení ze sítě
Sluchátka	bezdrátová, ovládání hlasitosti přes hlavní jednotku

Obrázek 29 Detektor nelineárních přechodů NJE – 4000 ORION[65]

[64] Zdroj: http://www.odposlechy24.cz/detektor-nelinearnich-prechodu-nje-4000-orion/

[65] Zdroj: http://www.odposlechy24.cz/files/images/252_230_nje4000_001.jpg

5.3 Infrakamery

Jsou úspěšně používány již několik desetiletí v několika různých odvětvích. V dnešní době jsou používány také při OTP, kdy velkou měrou napomáhají k odhalování aktivních odposlechových prostředků, které při své funkčnosti, vykazují vzhledem k okolí větší teplotu (princip viz metoda termografie kapitola 3.2.4) a jsou proto snadno odhalitelné.[40]

5.3.1 Infrakamera Flir i7

Tento typ infrakamery je vhodný především pro základní měření v elektrotechnice, stavebnictví, ale i při OTP. Kamera je vybavena nechlazeným maticovým detektorem o rozlišení 140 x 140 px a speciální optikou, která umožňuje velice snadné a přesné měření na kratší vzdálenosti.[41]

Tabulka 18 Technické parametry termokamery Flir i7[66]

Rozlišení detektoru	140 x 140 px
Citlivost	<0,1 °C
Zorné pole	29° x 29°
Hmotnost	365 g (včetně baterie)
Teplotní rozsah měření	-25 až 250 °C
Displej	2,8" LCD
Formát termogramu	JPEG
Ukládání dat	Karta micro SD
Baterie	nabíjecí typu Li-Ion (výdrž 5 hodin)

Obrázek 30 Infrakamera Flir i7[67]

[66] Zdroj: http://www.tmvss.cz/pdf/termovize-eshop/i-series.pdf

[67] Zdroj: http://www.tmvss.cz/e-shop/vyrobci/flir/flir-i7.png

5.4 Doplňkové a jednoúčelové přístroje

Jedná se o nástroje, které pomáhají technikovi objevit odposlechový prostředek při fyzické kontrole (viz kapitola 3.2.1).

5.4.1 OTK 4000 – Kufřík s nástroji pro vyhledávání

Kufřík obsahuje UV značkovače, 2 zrcadla, 4 sondy, ruční detektor kovů, voltmetr, kladivo, kleště, drátové řezačky, metr, svítilnu, vrtáky na stěny, tester pro kontrolu kabelů, univerzální šroubovák a univerzální nůž Leatherman.[42]

Obrázek 31 OTK 4000 – Kufřík s nástroji pro vyhledávání[68]

5.4.2 BORESCOP - Optický přístroj na prohlížení nepřístupných dutin

Sonda se zasouvá do dutiny vyvrtaným otvorem, jehož průměr je minimálně 5 mm. Pohled je možný v přímém směru nebo v pravém úhlu. Možnost přisvícení.[43]

Obrázek 32 BORESCOP[69]

[68] Zdroj: http://www.trisektor.com/images/stories/otk-4000_2.jpg

[69] Zdroj: http://www.safecom.cz/doplnkove.html

5.4.3 VPX-64

Jedná se o kameru umístěnou na teleskopické tyči. Zařízení slouží k prozkoumávání nepřístupných prostor, např. podhledy, šachty, vzduchotechnické potrubí aj. Na konci teleskopické tyče je umístěna černobílá nebo barevná kamera s možností natáčení. U rukojeti tyče je LCD monitor, který zobrazuje obraz, jejž snímá kamera na konci tyče. Délka tyče v rozloženém stavu je 4 m.[43]

Obrázek 33 VPX - 64[70]

5.5 Radiové analyzátory

Radiové analyzátory kontrolují a vyhodnocují radiové spektrum v zájmovém prostoru (princip viz přehledové snímání radiového spektra kapitola 3.2.6). Funkčnost radiového odposlechu nezamezí, pouze jej velmi spolehlivě odhalí a lokalizují. Tyto zařízení lze použít jak při OTP, kdy je možné okamžitě odhalit aktivní odposlechové prostředky s bezdrátovým přenosem (např. UHF odposlech, GSM odposlech, VKV minivysílač, radiový odposlech telefonní linky apod.). Dále je možné tyto zařízení použít pro permanentní (stálou) ochranu proti odposlechovým prostředkům, kdy je toto zařízení trvale a skrytě umístěno v zájmovém prostoru a ihned reaguje na spuštění výše uvedených odposlechových prostředků.[44]

Svým tvarem a velikostí připomínají občanské radiostanice. Jednotlivé typy se liší zejména šířkou pásma, které dokážou kontrolovat a v rychlosti této kontroly. Na trhu je mnoho takových přístrojů např. MRA-3 apod.[3]

[70] Zdroj: http://www.safecom.cz/foto/detekce/7/vpx.jpg

5.5.1 Radiový analyzátor MRA-3

MRA-3 paměťový radiový analyzátor je speciální určený k nepřetržité ochraně prostoru a k okamžitému zjištění radiového odposlechu. Ultra-rychlý vyhodnocovací systém odhalí do místnosti vnesený nebo dálkově aktivovaný odposlech i v podmínkách silného vysokofrekvenčního pole místních rozhlasových vysílačů, GSM, datových přenosů atd. MRA-3 umožňuje odhalení přítomnosti nového signálu během 6 s, poté je technik ihned na přítomnost podezřelého signálu akusticky nebo vizuálně upozorněn. K omezení falešných poplachů je přístroj vybaven tříúrovňovým poplachovým hlášením předpoplach – poplach – minulý poplach. Hlavní funkcí MRA-3 je ochrana prostoru, která je navíc zjednodušena na dvoutlačítkové ovládání usnadněné přehlednou informací na displeji přístroje.[3]

Tabulka 19 Technické parametry radiového analyzátoru MRA-3[71]

Kmitočtový rozsah	43 až 2700 MHz
Displej	LCD 2x16 znaků alfanumerický
Předpoplach	po každém scannovacím cyklu (6 s/cyklus)
Poplach	po 10 min trvalého signálu
Signalizace poplachu	akusticky (zpětná vazba), vizuálně (LED dioda nebo informace na displeji)
Spotřeba	při skenování okolo 44 mA, při vypnutí pod 4 μA
Identifikační kód	proti neoprávněné manipulaci (65536 stavů)
Napájení	9 V (vestavěný akumulátor nebo 9 V baterie)
Nabíjecí vstup a externí napájení	12 až 25 V DC[72]
Audio výstup	regulovatelný s vypínatelným reproduktorem
Anténa	Výsuvná teleskopická
Rozměry	136 x 49 x 137 mm
Hmotnost	620 g (včetně baterie)

[71] Zdroj: http://www.infosafe.cz/produkt/mra-3-pametovy-radiovy-analyzator/

[72] DC – stejnosměrný proud.

Obrázek 34 Radiový analyzátor
MRA-3

5.6 Detektory vysokofrekvenčního pole

Jedná se o zařízení kapesního formátu, které signalizuje na displeji, pomocí LED, případně akusticky zvýšenou intenzitu elektromagnetického pole, kterou generuje každý radiový odposlech (UHF odposlech, GSM odposlech, VKV minivysílač, skryté kamery s bezdrátovým přenosem signálu, radiový odposlech telefonní linky apod). Některé kvalitnější detektory umožňují poslech zachyceného signálu pomocí sluchátek. Jednotlivé přístroje se liší především kmitočtovým rozsahem a citlivostí měření.[45]

5.6.1 Detektor VF pole RFD-5

Jde o širokopásmový, vysoce citlivý detektor vysokofrekvenčního pole s mimořádně velkým kmitočtovým a dynamickým rozsahem určený k vyhledávání odposlechových prostředků na špičkové a profesionální úrovni.[3]

RFD-5 je navržen především pro kontrolu prostoru v rámci OTP, ale lze jej také využít jako prostředek pro permanentní ochrany prostoru. Pro tento účel je vybaven funkcí automatického porovnávání uloženého radiového pozadí s aktuálně naměřenými hodnotami.[46]

Při měření je nutné zařízení nastavit do základního módu MEASURE (měření). Dále je důležité mít vysunutou teleskopickou anténu. Pokud je vše nastaveno, tak se pomalými pohyby prověřuje zájmový prostor. Jestliže v některém místě dochází k prudkému nárůstu

intenzity VF pole, mohlo by se jednat o místo, kde se nachází odposlechový prostředek.[47]

Tabulka 20 Technické parametry detektoru VF pole RFD-5[73]

Kmitočtový rozsah	0,5 MHz až 25 GHz
Typická citlivost	0,06 μW (400 MHz, 5 cm, 5 dílků)
Dynamický rozsah	43 dB základní
Detekovatelné pulsy	více jak 80 μs
Displej	LCD 2 x 12 znaků
Anténa	teleskopická od 1 do 37 cm
Paměť poplachů	16 událostí (včetně času a síly signálu)
Napájení	9 V (akumulátor nebo 9 V baterie)
Nabíjecí vstup a externí napájení	12 až 20 V DC
Audio výstup	stereo sluchátka
Spotřeba	3,5 až 6 mA
Rozměry	150 x 60 x 31 mm
Hmotnost	295 g

Obrázek 35 Detektor VF pole RFD-5[74]

[73] Zdroj: http://www.elbi.cz/common/doc/rfd5/rfd5-spec10cz.doc

[74] Zdroj: http://www.kontraodposlech.cz/fotky16166/fotos/_vyr_1rfd5.jpg

5.7 Generátory šumu

Šumový generátor je zařízení, které znemožňuje nahrát pomocí odposlechu použitelná data. Funguje na principu vytváření bílého šumu (viz aplikace bílého šumu kapitola 3.4.2), který způsobuje rozvibrování membrány mikrofonu a tím prakticky znemožní pořízení nahrávky. Toto zařízení patří skupiny technických prostředků určených pro aktivní permanentní ochranu prostoru proti mikrofonním odposlechovým prostředkům.(např. mikrodiktafony, GSM odposlechy, UHF odposlechy, VKV odposlechy, elektronické stetoskopy, laserové odposlechové zařízení, parabolické mikrofony). Šumová ochrana proti odposlechovým prostředkům spočívá v přímém mechanickém zašumění míst, kde lze zvuky snímat (např. okna) nebo zašumění částí nábytku, kde lze operativní prostředky skrytě umístit.[48]

5.7.1 SNG – inteligentní šumový generátor

SNG je velmi kvalitní inteligentní šumový generátor umožňující připojení až 100 piezokeramických akustických měničů, 2 až 12 nízkoimpedančních reproduktorů, nebo jejich vzájemnou kombinaci. Účelem zašumění je zajistit ochranu prostoru proti odposlechu všech forem snímání zvuku. Instalací piezoměničů na vnitřní stěny nábytku, stolů a dalších předmětů uvnitř kanceláře, lze realizovat vhodnou doplňkovou ochranu proti operativně přenosným odposlechovým prostředkům (např. mikrodiktafony).[48]

Účinnost SNG optimalizuje vestavěný procesor, který v automatickém režimu analyzuje zvuky z místnosti a zajišťuje jen takovou úroveň zašumění, která je nutná v závislosti na hlasitosti konverzace.[49]

SNG je konstruován k zavěšení na zeď, nebo bok pracovního stolu, nejlépe v přímém dosahu uživatele. Z předního panelu lze pomocí tří ovládacích přepínačů zvolit, zapnutí nebo vypnutí generátoru, výkonovou úroveň a automatický nebo manuální režim.[49]

Tabulka 21 Technické parametry SNG – inteligentního šumového generátoru[75]

Napájecí napětí	12 V DC (10 až 15 V)
Spotřeba	0,1 až 0,5 A podle zatížení
Výkon	2 x 2 W
Kapacita	100 piezoměničů nebo 12 reproduktorů
Výstupní signál	šumové spektrum až 40 V
Indikace stavu	5x LED včetně testu procesoru
Rozměry	118 x 58 x 187 mm

Obrázek 36 SNG – inteligentní šumový generátor[76]

[75] Zdroj: http://www.infosafe.cz/soubor/sng-technicka-specifikace-pdf/

[76] Zdroj: http://wordpress.detekce.com/wp-content/uploads/2010/04/SNG.jpg

6 SYNTÉZA KONTROLY PROSTORU

Syntéza je jev, při kterém je poznáváno nebo definováno určité fungování neboli chování systému a hledá se taková struktura systému, která by byla pro toto chování, fungování adekvátní.[50]

Vzájemné vazby mezi chováním a strukturou systému je možné zajišťovat a zabezpečovat několika způsoby:

- Základní přístup – představuje opakované zkušenostní pozorování vztahů mezi chováním a struktury systému.
- Konstruktérský přístup – jedná se o představu fyzické reality konstruktérského výkresu. Nemusí zde dojít k pochopení toho, proč je systém konstruován.
- Inženýrský přístup – zahrnuje projektování složitých systémů, které nelze zabezpečit bez pochopení systému a určité znalosti teorie.
- Teoretický či vědecký přístup – je tvořen soubory vědeckých znalostí o systému, jeho organizaci, chování, vazbách mezi organizací a chováním apod.[50]

Syntéza kontroly prostoru zde spočívá v zakreslení možnosti umístění odposlechových prostředků do dvou fotografií kanceláří, spočítání celkové plochy jednotlivých kanceláří dle výkresové dokumentace (viz přílohy P III a PIV). Podle podlahové plochy jednotlivých kanceláří je v příloze P V uveden cenový rozpočet OTP od 4 různých firem, které se OTP zabývají.

Odposlechové prostředky jsou ve fotografiích označeny červenými písmeny a) až z) nebo červenými čísly 1. až 20.

6.1 Kancelář č. 1

Jedná se o kancelář sekretářky firmy Technické služby města Kuřim. Obsahuje 2 psací stoly, židle, 2 počítače, skříň, ve které se nachází trezor (u dveří ke skladu), nástěnku, tiskárnu, rádio, skartovač, psací stroj, doplňky interiéru (např. květiny) a ostatní nábytek. Do kanceláře je možné vstoupit vstupními dveřmi pouze z chodby (viz obrázek 37). Druhými dveřmi je možné se dostat do skladu s oblečením (viz obrázek 38).

Obrázek 37 Fotografie kanceláře č. 1 (vyfotografováno směrem k vchodovým dveřím) se zakreslenými odposlechovými prostředky[77]

a) Vnesený VKV minivysílač umístěný v lustru.

b) Vnesený VKV minivysílač přilepený za hodinami.

c) Elektronický stetoskop – odposlech přes zeď z chodby.

d) Vnesený UHF odposlech umístěný ve vypínači.

e) Vnesený VKV minivysílač přilepený pod stolem.

[77] Zdroj: vlastní fotografie.

f) Vnesený VKV minivysílač umístěn ve skříni nebo za skříní, vnesený mikrodiktafon umístěný v květináči.

Obrázek 38 Fotografie kanceláře č. 1 (vyfotografováno směrem od vchodových dveří) se zakreslenými odposlechovými prostředky[78]

1. Vnesený mikrodiktafon umístěný v květináči.
2. Síťově napájený GSM odposlech umístěný v elektrickém rozvaděči.
3. Vnesený VKV minivysílač přilepený za skříní.

[78] Zdroj: vlastní fotografie.

4. Elektronický stetoskop – odposlech přes zeď z jiné místnosti.
5. Vnesený VKV minivysílač přilepený za nástěnkou nebo vnesená minikamera skrytá ve šroubku, který nástěnku drží.
6. Vnesený VKV minivysílač přilepený za skříní nebo ve skříni.
7. Vnesená propiska se zabudovaným UHF odposlechem nebo vnesené pero s minikamerou.
8. Vnesený cigaretový balíček se zabudovaným UHF odposlechem.
9. VKV minivysílač přilepený pod psacím stolem.
10. Vnesený Mikrodiktafon skrytý ve skartovači.
11. Laserový odposlech (použití při zavřeném okně) nebo parabolický mikrofon (použití při otevřeném okně).

6.1.1 Podlahová plocha kanceláře č. 1

Délka a = 4,705 m

Šířka b = 2,7 m

Podlahová plocha S =?

Rovnice 1 Výpočet podlahové plochy kanceláře č. 1

$$S = a \times b$$
$$S = 3{,}755 \times 2{,}7$$
$$S = 10{,}1385 m^2 \doteq 10{,}14 m^2$$

Rozměry kanceláře č. 1 jsou použity z její výkresové dokumentace, která se nachází v příloze P III.

6.2 Kancelář č. 2

Jedná se o kancelář ředitele firmy Technické služby města Kuřim. Obsahuje psací stůl, židle, počítač, reproduktory k počítači, skříně, nástěnku, meteorologickou stanici, věšák, doplňky interiéru (např. květiny, kalendář apod.) a ostatní nábytek. Do kanceláře je možné vstoupit pouze vstupními dveřmi z chodby (viz obrázek 39).

Obrázek 39 Fotografie kanceláře č. 2 (vyfotografováno směrem k vchodovým dveřím) se zakreslenými odposlechovými prostředky[79]

a) Vnesený VKV minivysílač přilepený za trhacím kalendářem.

b) Vnesený VKV minivysílač umístěný do skříně nebo přilepený za skříň.

c) Síťově napájený GSM odposlech umístěný v elektrickém rozvaděči.

d) Síťově napájený UHF odposlech umístěný v zásuvce.

e) Vnesený UHF odposlech umístěný v šanonu.

f) Vnesený mikrodiktafon umístěn v květináči.

g) Laserový odposlech (použití při zavřeném okně) nebo parabolický mikrofon (použití při otevřeném okně).

[79] Zdroj: vlastní fotografie.

Obrázek 40 Fotografie kanceláře č. 2 (vyfotografováno směrem od vchodových dveří) se zakreslenými odposlechovými prostředky[80]

1. Vnesený mikrodiktafon umístěný v květináči.
2. Vnesený VKV minivysílač přilepený na zdi za nástěnkou.
3. Vnesený VKV minivysílač umístěný v lustru.

[80] Zdroj: vlastní fotografie.

4. Vnesený VKV minivysílač přilepený na zdi za nábytkem.
5. Vnesený UHF odposlech umístěný v šanonu.
6. Vnesený VKV minivysílač přilepený pod stolem.

6.2.1 Podlahová plocha kanceláře č. 2

Délka a = 4,705 m

Šířka b = 2,7 m

Podlahová plocha S =?

Rovnice 2 Výpočet podlahové plochy kanceláře č. 2

$$S = a \times b$$
$$S = 4{,}705 \times 2{,}7$$
$$S = 12{,}7035 m^2 \doteq 12{,}70 m^2$$

Rozměry kanceláře č. 2 jsou použity z její výkresové dokumentace, která se nachází v příloze P IV.

ZÁVĚR

S odposlechovými prostředky se každý člověk setkává několikrát ročně, ať už ho zasahují okrajově v médiích nebo se s nimi setkává aktivně (pracuje s nimi nebo je odhaluje). Získání odposlechových prostředků je dnes velmi snadné, stačí si je objednat přes internetový obchod. Jelikož není jejich dovoz a prodej v ČR žádným způsobem omezen, má pachatel v tomto směru volné pole působnosti. Ke koupi odposlechového prostředku ho neodradí ani jeho příliš vysoká cena, ta se pohybuje mezi 2000 a 18000 Kč. A tak pachatel nemá problém s odposlechovým prostředkem za 10000 Kč ukrást informace, jejichž cena je v řádu jednotek milionů korun.

K vyhledávání odposlechových prostředků slouží OTP. V ČR existuje spousta firem zabývající se OTP. A díky konkurenci není její cena vzhledem k ceně odposlechových prostředků nebo finanční újmě, kterou mohou způsobit, příliš vysoká. Jak je v práci vidět, v menší kanceláři s výměrou 11 m^2 stojí kompletní OTP v rozmezí mezi 20000 a 30000 Kč. V dnešní době dokonce některé z firem uvádí více než 90% úspěšnost odhalení odposlechových prostředků při provedení kompletní prohlídky, což je vzhledem ke stále se vyvíjejícím technologiím velmi vysoké číslo.

Mnohem těžší je však někoho z nelegálního použití odposlechového prostředku usvědčit. Největším problémem v tomto směru je stáří zákonů, které nezákonné používání odposlechových prostředků vymezují. Například zákon o trestním řízení soudním č. 141/1961 Sb. byl vydán v roce 1961 a část zabývající se odposlechem a záznamem telekomunikačního provozu nebyla dodnes novelizována. Dalším problémem je nejednotnost posuzování soudů při použití odposlechového prostředku v důkazním řízení. V dnešní době je větší zájem o to, co je na odposlechovém prostředku nahráno, než aby byl potrestán pachatel za nelegální pořízení záznamu.

Práce se zabývá problematikou vysvětlení pojmu a smyslu provedení OTP, analýzy legislativního rámce a průběhu OTP, popisu odposlechových prostředků a technických prostředků k realizaci OTP a problematikou možnosti umístění odposlechových prostředků. Cílem práce bylo vytvořit metodický postup při OTP v praxi. Při zpracování práce byly využity tyto vědecké metody: dedukce, analýza a syntéza. Práce může být po úpravě využita k E-learningu nebo jako ucelený materiál ke studiu problematiky OTP.

ZÁVĚR V ANGLIČTINĚ

Getting of listening devices is very easy now, just it order them through the online store. Because it is not their importation and sale in the Czech Republic in any way restricted, the offender has in this course free rein. Purchase of listening device discourages him neither price is too high, that it is between 2000 and 18000 CZK. So the offender has no problem with listening device for 10000 CZK steal information, the price is of the order of millions of crowns.

Defensive technical inspection is used for searching listening devices. There are plenty of companies engaged in the defensive technical inspection in the Czech Republic. Price of the defensive technical inspection is not due to eavesdropping or financial harm they can cause too high due to the competition. Complete defensive technical inspection cost in small office with an area 11 square meters in the range between 20000 and 30000 CZK, as seen at work**.** Nowadays, even any of the firms lists more than 90% success rate in detection listening devices performs a complete examination, which it is due to the ever-evolving technologies very high number.

Much more difficult it is someone from using illegal listening device to convict**.** The age of laws is the biggest problem in this direction that it defined illegal use of listening devices. For example, the Code of Criminal Procedure No. 141/1961 Coll. was issued in 1961 and part of dealing with the interception and recording of telecommunications traffic was not still being amended. Another problem is the inconsistency assessing of the courts for using listening devices in the evidence procedure. Today, it is more interested in what is recorded in the listening device, than offender was to be punished for illegally acquiring the alert.

The work deals explanation of the issue of the concept a sense of design of the defensive technical inspection, analysis, legislative framework and during of the defensive technical inspection, description listening devices and technical means to implement of the defensive technical inspection and location problems listening devices. The aim was to create a methodology for defensive technical inspection in practice. When processing these works was used by the scientific method: deduction, analysis and synthesis. Work can be used to modify the E-learning or as an integrated material to study the issue of OTP.

SEZNAM POUŽITÉ LITERATURY

[1] BRABEC, František. *Ochrana bezpečnosti podniku*. 1. vyd. Praha: Eurounion, 1996, 203 s. ISBN 80-858-5829-0.

[2] TUREČEK, Jaroslav. *Policejní technika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2008, 316 s. ISBN 978-807-3801-199.

[3] LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 223 s. ISBN 978-807-3187-620.

[4] KAMENÍK, Jiří a František BRABEC. *Komerční bezpečnost*: *Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostní agentur*. Praha: ASPI, 2007. ISBN 978-80-7357-309-6.

[5] Právní rozbor. *Odposlechy.com - profesionální odposlech a ochrana před odposlechy* [online]. © 1999-2012 [cit. 2012-03-13]. Dostupné z: http://www.odposlechy.com/pravni-rozbor/

[6] Záznam telefonního rozhovoru pořízený jeho účastníkem jako důkaz v občanskoprávním řízení. *IPrávník* [online]. 2009[cit. 2012-03-15]. Dostupné z: http://www.ipravnik.cz/cz/clanky/obchodni-pravo/default.aspx

[7] Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů České republiky*. 1. 1. 2010.

[8] ŠÁMAL, Pavel. *Trestní řád*: *komentář*. 6., doplněné a přepracované vyd. V Praze: C.H. Beck, 2008, 23011 s. ISBN 978-807-4000-430.

[9] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: *Sbírka zákonů České republiky*. 1961.

[10] Jednací oblast – Informace. *Národní bezpečnostní úřad* [online]. [2006] [cit. 2012-03-22]. Dostupné z: http://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost/jednaci-oblast--informace/

[11] Novela vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, vyhláška č. 454/2011 Sb. In:*Sbírka zákonů České republiky*. 1. 1. 2012.

[12] Praxe v boji proti odposlechu a úniku informací. *Mudroch LABS s.r.o.* [online]. [2009] [cit. 2012-01-20]. Dostupné z: http://mudrochlabs.sk/cz/odposlech_v_praxi.htm

[13] Triangulace korelace RF spektra. *Jak zjistit odposlech ?* [online]. © 1997-2011 [cit. 2012-01-31]. Dostupné z: http://www.infosafe.cz/inpage/triangulacni-korelace-rf-spektra/

[14] REJDÍK, Martin. *Vyhledávání odposlechových prostředků s využitím detektoru nelineárních přechodů*. Univerzita Tomáše Bati ve Zlíně, 19. 5. 2010. Dostupné z: http://dspace.knihovna.utb.cz/bitstream/handle/10563/11538/rejd%c3%adk_2010_bp.pdf?sequence=1. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky.

[15] PAVELEK, Milan, Eva JANOTKOVÁ a Josef ŠTĚTINA. *Vizualizační a optické měřicí metody* [online]. VUT v Brně, 2007 [cit. 2012-02-07]. Dostupné z: http://ottp.fme.vutbr.cz/users/pavelek/optika/. Elektronická skripta. VUT v Brně, FSI.

[16] KANČO. Praktické rady při práci s termokamerami. *Pro revize – portál o elektro revizích a diagnostice* [online]. © 2010 [cit. 2012-02-07]. Dostupné z: http://www.prorevize.cz/termodiagnostika/148-prakticke-rady-pri-praci-s-termokamerami

[17] LOVEČEK, Tomáš. *Odhalování skrytých odposlechových prostředků pro hlasovou komunikaci* [online]. Univerzita Tomáše Bati ve Zlíně, 2009-06-12 [cit. 2012-02-21]. Dostupné z: http://hdl.handle.net/10563/10934. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, FAI.

[18] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7 (BROž.).

[19] Pink noise. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-02-28]. Dostupné z: http://en.wikipedia.org/wiki/Pink_noise

[20] Faradayova místnost, Faradayova klec. *Mudroch LABS s.r.o.* [online]. [2006] [cit. 2012-02-14]. Dostupné z: http://www.mudrochlabs.sk/cz/faradayova_mistnost_klec.htm

[21] Mikro diktafony, mikrodiktafony - Odposlechy.com. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy*[online]. © 1999-2012 [cit. 2012-03-26]. Dostupné z: http://www.odposlechy.com/mikro-diktafony

[22] Mikro diktafon B21 CZ 300 GEN 2 série PRO. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy*[online]. © 1999-2012 [cit. 2012-03-26]. Dostupné z: http://www.odposlechy.com/mikro-diktafon-b21-cz-300-gen-2-serie-pro

[23] GSM odposlech. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy* [online]. © 1999-2012 [cit. 2012-03-26]. Dostupné z: http://www.odposlechy.com/gsm-odposlech

[24] GSM bezdrátový odposlech G500. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy* [online]. © 1999-2012 [cit. 2012-03-26]. Dostupné z: http://www.odposlechy.com/gsm-bezdratovy-odposlech-g500

[25] UHF vysílače a přijímače. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy* [online]. © 1999-2012 [cit. 2012-03-27]. Dostupné z: http://www.odposlechy.com/uhf-vysilace-a-prijimace

[26] UHF přijímač Alinco S. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy* [online]. © 1999-2012 [cit. 2012-03-27]. Dostupné z: http://www.odposlechy.com/uhf-prijimac-alinco-s

[27] Radiový odposlech LCBUGmini. *Jak zjistit odposlech ?* [online]. © 1997-2011 [cit. 2012-03-29]. Dostupné z: http://www.infosafe.cz/produkt/radiovy-odposlech-lcbugmini/

[28] Přijímač M9 Air. *Jak zjistit odposlech ?* [online]. © 1997-2011 [cit. 2012-04-03]. Dostupné z: http://www.infosafe.cz/produkt/prijimac-m9-air/

[29] Odposlech přes zdi - Stetoskop. *Odposlechy mobilních telefonů - Odposlechy24.cz* [online]. [2010] [cit. 2012-04-03]. Dostupné z: http://www.odposlechy24.cz/odposlech-pres-zdi-stetoskop/

[30] "Laser Listening Systems". *Electromax Int'l Surveillance, Countersurveillance and Personal Protection* [online]. © Copyright 1998 [cit. 2012-04-17]. Dostupné z: http://www.electromax.com/laser.html

[31] Skryté kamery a mikrokamery. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy* [online]. © 1999-2012 [cit. 2012-04-20]. Dostupné z: http://www.odposlechy.com/skryte-kamery-a-mikrokamery

[32] Odposlech pevné linky TO LINE 1. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy* [online]. © 1999-2012 [cit. 2012-04-23]. Dostupné z: http://www.odposlechy.com/odposlech-pevne-linky-to-line-1

[33] Odposlech pevné linky TO LINE 2. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy* [online]. © 1999-2012 [cit. 2012-04-23]. Dostupné z: http://www.odposlechy.com/odposlech-pevne-linky-to-line-2

[34] Digitální diktafon Olympus 4 GB. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy* [online]. © 1999-2012 [cit. 2012-04-23]. Dostupné z: http://www.odposlechy.com/digitalni-diktafon-olympus-4-gb

[35] *Odhalování skrytých odposlechových prostředků pro hlasovou komunikaci*. Univerzita Tomáše Bati Zlín, 2009. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky.

[36] Technika používaná pre boj proti odpočúvaniu. *Mudroch LABS s.r.o.* [online]. [2009] [cit. 2012-04-24]. Dostupné z: http://mudrochlabs.sk/technika_proti_odpocuvaniu.htm

[37] *Spektrální analyzátory*. SPŠ a VOŠ Chomutov, [2010]. Dostupné z: http://web.spscv.cz/~kaderabek/osciloskopy/spektralni_analyzatory.pdf

[38] OSC5000E Profesionální jednotka s detekčním rozsahem 10kHz - 3GHz.*Odposlechy mobilních telefonů - Odposlechy24.cz* [online]. [2010] [cit. 2012-04-24]. Dostupné z: http://www.odposlechy24.cz/osc5000e-profesionalni-jednotka-s-detekcnim-rozsahem-10khz-3ghz/

[39] Detektor nelineárních přechodů NJE - 4000 ORION. *Odposlechy mobilních telefonů - Odposlechy24.cz* [online]. [2010] [cit. 2012-04-30]. Dostupné z: http://www.odposlechy24.cz/detektor-nelinearnich-prechodu-nje-4000-orion/

[40] Energetika a Strojírenství. *Měřicí přístroje a diagnostika pro energetiku i průmysl, termovize* [online]. 2007- [cit. 2012-05-02]. Dostupné z: http://www.tmvss.cz/Aplikace/termovize/energetika2.html

[41] FLIR i7. *Měřicí přístroje a diagnostika pro energetiku i průmysl, termovize* [online]. 2007- [cit. 2012-05-02]. Dostupné z: http://www.tmvss.cz/e-shop/vyrobci/flir/flir-i7.html

[42] KONTROLNÍ NÁSTROJE PRO NELINEÁRNÍ JUNCTION DETEKTORŮ (OTK-4000).*Trisektor - Alternativní energie, Chemikálie, Moc, Zabezpečení,*

Telecom, IT, Zkušební a PME Produkty a řešení - Český, Česká republika [online]. © 2012 [cit. 2012-05-02]. Dostupné z: http://www.trisektor.com/cs/products-page/counter-surveillance/inspection-tools-for-non-linear-junction-detectors-otk-4000/

[43] Doplňkové a jednoúčelové přístroje. *Safecom s.r.o.* [online]. 2010 [cit. 2012-05-02]. Dostupné z: http://www.safecom.cz/doplnkove.html

[44] Permanentní ochrana. *IN IN s.r.o. - INDEPENDENT INVESTIGATIONS : IN IN s.r.o. - nezávislé vyšetřování* [online]. 2008 - 2009 [cit. 2012-05-03]. Dostupné z: http://www.nezavisle-vysetrovani.cz/nezavisle-vysetrovani/permanentni-ochrana/

[45] VF detektory. *Jak zjistit odposlech ?* [online]. © 1997-2011 [cit. 2012-05-03]. Dostupné z: http://www.infosafe.cz/kategorie/vf-detektory/

[46] Univerzální detektor odposlechových zařízení RFD-5. *Odposlechy.com – profesionální odposlech a ochrana před odposlechy* [online]. © 1999-2012 [cit. 2012-05-05]. Dostupné z: http://www.odposlechy.com/detektor-rfd-5

[47] *RFD-5 popis a návod k použití*. 2003. Dostupné z: www.elbi.cz/common/doc/rfd5/rfd5-man10cz.doc

[48] SNG rušička mikrofonů – inteligentní šumový generátor – efektivní prostředek proti odposlechu hovoru. *GoldSilver | mluviti stříbro, mlčeti zlato* [online]. [2008-2012] [cit. 2012-05-09]. Dostupné z: http://www.goldsilver.cz/sng-inteligentni-sumovy-generator-efektivni-prostredek-proti-odposlechu-hovoru/

[49] *Ochrana proti odposlechu SNG inteligentní šumový generátor*. © 1997-2012. Dostupné z: http://www.infosafe.cz/soubor/sng-technicka-specifikace-pdf/

[50] LAUCKÝ, Vladimír. *Řízení technologických procesů v průmyslu komerční bezpečnosti*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2005, 101 s. ISBN 80-731-8329-3

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AC	Alternating Current
ADPCM	Adaptive Differential Pulse Coded Modulation
AVI	Audio Video Interleave
CCIR	Comite Consultatif International des Radiocommunications
CD	Compact Disc
ČR	Česká republika
DC	Direct Current
DPH	Daň z přidané hodnoty
DSP	Digitální Signálový Procesor
DVD	Digital Video Disc
FM	Frequency Modulation
GPS	Global Positioning Systém
GSM	Global System for Mobile communications
SDHC	Secure Digital High Capacity
JPEG	Joint Photographic Expert Group
LCD	Liquid Crystal Display
LED	Light Emitting Diode
Li-Ion	Lithium-Iontová baterie
MAC OS	Macintosh Operating Systém
M-JPEG	Motion Joint Photographic Expert Group
MP3	Motion Picture experts group - layer 3 (MPeg layer 3)
NBÚ	Národní Bezpečnostní Úřad
NiMH	Nickel Metal Hydride cell
OIRT	Organisation Internationale de Radiodiffusion et de Télévision

OTP	Obranná technická prohlídka
PC	Personal Computer
PCM	Pulse-Code Modulation
PIN	Personal Identification Number
px	Pixel
RF	Radio Frequency
RJ	Registered Jack
SD	Secure Digital
SMT	Surface Mount Technology
UHF	Ultra-High Frequency
USB	Universal Serial Bus
VF	Vysokofrekvenční
VKV	Velmi krátké vlny
WMA	Windows Media Audio

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ROVNIC

SEZNAM PŘÍLOH

PŘÍLOHA P I: CENOVÝ ROZPOČET ODPOSLECHOVÝCH PROSTŘEDKŮ

Název	Cena s DPH[81]	Odkaz na e-shop
Mikro diktafon B21 CZ 300 GEN 2	15 772 Kč	www.odposlechy.com
GSM bezdrátový odposlech G500	23 760 Kč	www.odposlechy.com
UHF bezdrátový odposlech R500 CR	11 244 Kč	www.odposlechy.com
UHF přijímač Alinco S	7 128 Kč	www.odposlechy.com
Radiový odposlech LCBUGmini	2 388 Kč	www.infosafe.cz
VHF přijímač M9 AIR	1 848 Kč	www.odposlechy.com
Odposlech přes zdi – Elektronický stetoskop	9 490 Kč	www.odposlechy24.cz
Laser Audio Surveillance*	53 264 €	www.spycatcheronline.co.uk
SPECTRA G-50 PRO-FLEX	77 500 Kč	www.spionazni-technika.cz
Pero s kamerou (paměť SD karta)	690 Kč	www.odposlech-tech.cz
Hodinky s kamerou - stříbrné provedení	2 290 Kč	www.odposlech-tech.cz
Sluneční brýle s kamerou	2 190 Kč	www.odposlech-tech.cz
Klíčenka s kamerou (HD rozlišení)	2 490 Kč	www.odposlech-tech.cz
Odposlech pevné linky TO LINE 1	2 808 Kč	www.odposlechy.com
Odposlech pevné linky TO LINE 2	2 808 Kč	www.odposlechy.com
Digitální diktafon Olympus 4 GB	5 640 Kč	www.odposlechy.com
Radiový odposlech pevné linky - rozbočka	3 890 Kč	www.odposlechy24.cz
Radiový odposlech pevné linky - parazit	3 690 Kč	www.odposlechy24.cz

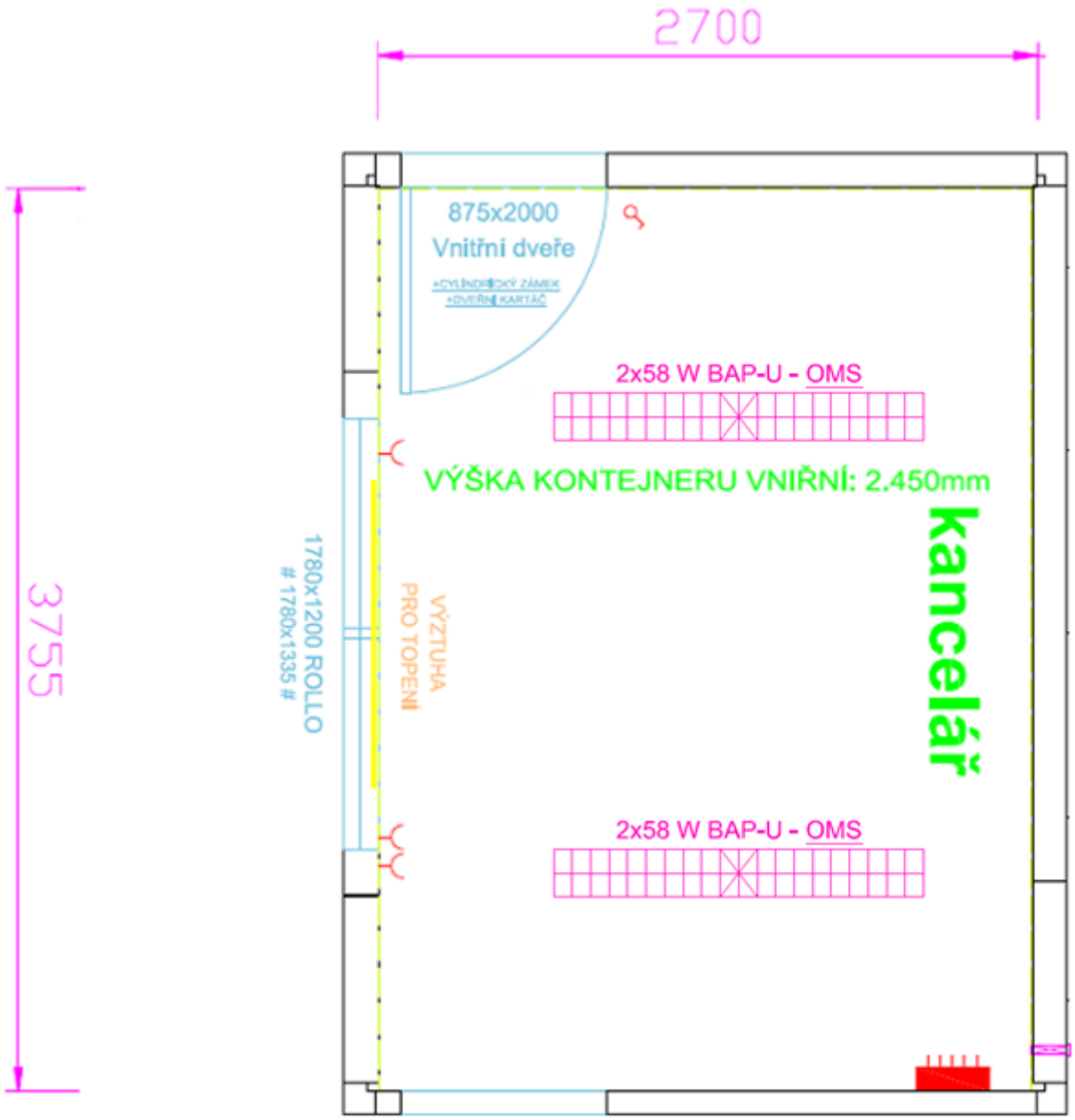
* Jedná se o laserový odposlech Laser EMAX - 3500. Je prodejný na internetových stránkách firmy z Velké Británie. Po přepočítání dle aktuálního kurzu (26 Kč za 1 €) se jeho cena pohybuje okolo 1 400 000 Kč.

[81] DPH – Daň z přidané hodnoty. Základní sazba: 20%, snížená sazba: 14%. V práci je použita pouze základní sazba.

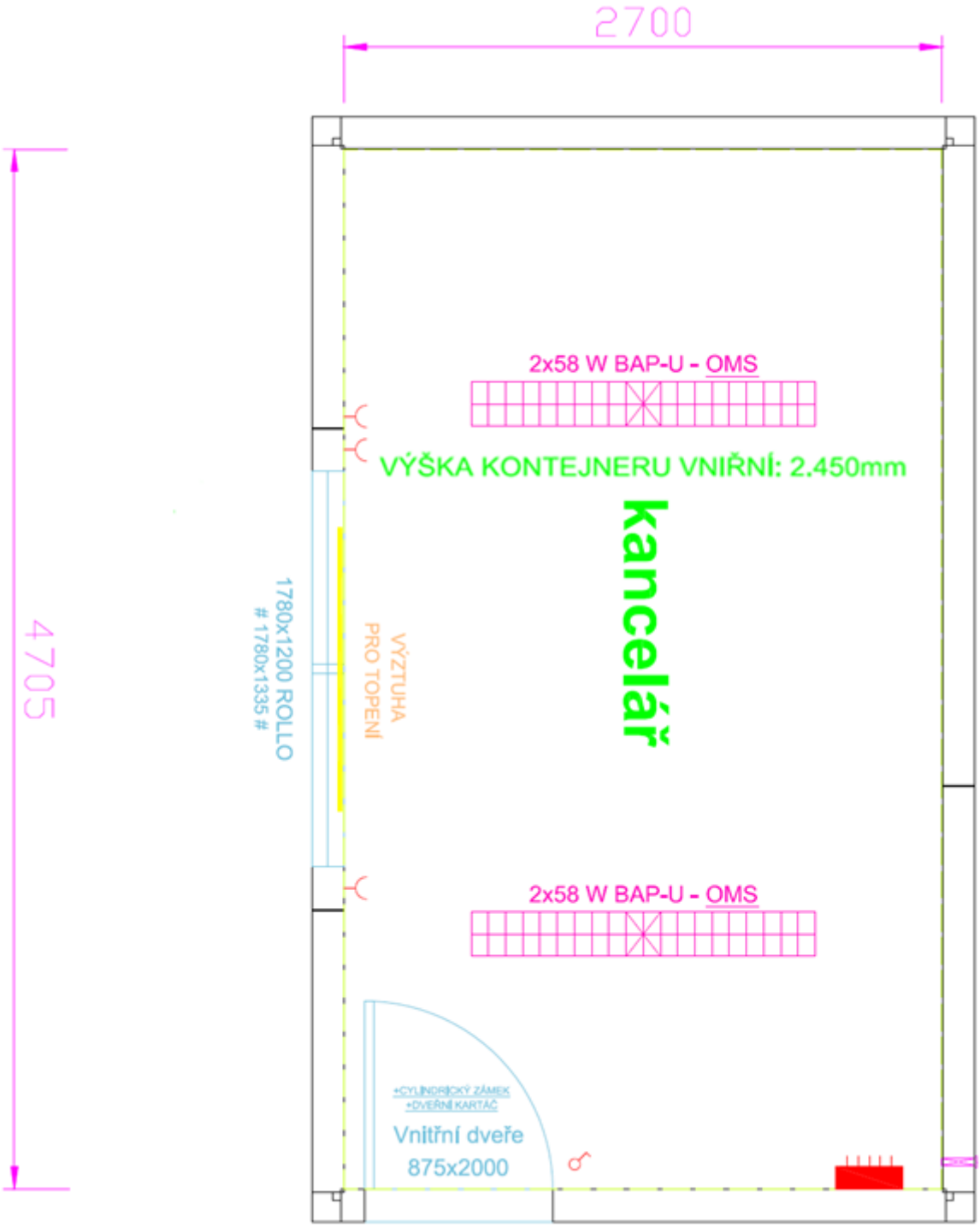
PŘÍLOHA P II: CENOVÝ ROZPOČET ZÁKLADNÍCH TECHNICKÝCH PROSTŘEDKŮ PRO REALIZACI OTP

Název	Cena s DPH	Odkaz na e-shop
Spektrální analyzátor - OSC-5000 DELUX	532 800 Kč	www.safecom.cz
Detektor nelineárních přechodů – NJE-4000 ORION	423 377 Kč	www.safecom.cz
Infrakamera - FLIR i7	59 988 Kč	www.termogram.cz
OTK-4000 – Kufřík s nástroji pro vyhledávání	70 741 Kč	www.safecom.cz
BORESCOP	22 777 Kč	www.safecom.cz
VPX-64	77 593 Kč	www.safecom.cz
Radiový analyzátor - MRA-3	28 176 Kč	www.infosafe.cz
Detektor VF pole - RFD-5	22 356 Kč	www.infosafe.cz
Síťový zdroj 12V/300mA (RFD-5, MRA-3)	150 Kč	www.infosafe.cz
Inteligentní šumový generátor - SNG	13 980 Kč	www.odposlechy.com

PŘÍLOHA P III: VÝKRESOVÁ DOKUMENTACE KE KANCELÁŘI Č. 1



PŘÍLOHA P IV: VÝKRESOVÁ DOKUMENTACE KE KANCELÁŘI Č. 2



PŘÍLOHA P V: CENOVÝ ROZPOČET OTP V KANCELÁŘÍCH Č. 1 A Č. 2

Typ prohlídky	Firma	Cena (s DPH) OTP v kanceláři č. 1	Cena (s DPH) OTP v kanceláři č. 2
Kompletní	Tango, spol. s r.o.	30 660 Kč	30 660 Kč
Základní	Tango, spol. s r.o.	20 040 Kč	20 040 Kč
Analýza RF spektra	SAFECOM, spol. s r.o.	8 988 Kč	9 441 Kč
Kontrola nelineárních přechodů	SAFECOM, spol. s r.o.	8 683 Kč	9 361 Kč
Kompletní	PROBIN s.r.o.	18 475 Kč	21 115 Kč
Základní	PROBIN s.r.o.	12 688 Kč	14 275 Kč
Analýza RF spektra	Mudroch LABS s.r.o.	16 200 Kč	16 200 Kč
Kompletní	Mudroch LABS s.r.o.	21 240 Kč	21 240 Kč

Kompletní prohlídka od firmy Tango, spol. s r.o. zahrnuje detailní analýzu RF spektra, kontrolu termokamerou, fyzickou prohlídku, závěrečnou zprávu a bezpečnostní doporučení.

Základní prohlídka od firmy Tango, spol. s r.o. zahrnuje základní analýzu RF spektra a závěrečnou zprávu a bezpečnostní doporučení.

Kompletní prohlídka od firmy PROBIN s.r.o. zahrnuje detekci nelineárních přechodů, analýzu RF spektra a fyzickou kontrolu.

Základní prohlídka od firmy PROBIN s.r.o. zahrnuje analýzu RF spektra a fyzickou kontrolu.

Kompletní prohlídka od firmy Mudroch LABS s.r.o. se skládá z: kontroly a triangulace rádiového spektra, termovizní kontroly prostoru, prověrky vedení měřením a fyzickou kontrolou a fyzického prověření zadaného prostoru a jeho vybavení.