Metody informačního průniku v oblasti detektivních činností.

Methods of information intersection, in the area of dective activity.

František Šošolík

Bakalářská práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav automatizace a řídicí techniky
akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**František ŠOŠOLÍK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Automatické řízení a informatika**
Téma práce:	**Metody informačního průniku v oblasti detektivních činností.**

Zásady pro vypracování:

1. Seznámení se s problematikou právní podstaty odposlechu v oblasti detektivních činností.
2. Provést analýzu problematiky využití operativní techniky pro získávání citlivých informací.
3. Přehledně uvést základní rozdělení odposlechových prostředků, formy a typy odposlechu, speciální technika.
4. Realizujte přehledový materiál obsahující prvky E – learningu.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] Ivanka, J.: Technické prostředky bezpečnosti a elektromagnetická kompatibilita. In. Řešení krizových situací v specifickém prostředí. EDIS – Žilinská univerzita,Žilina, 2004, str.77-82, ISBN 80-8070-272-1

[2] Čandík, M., Ivanka, J. : Některé aspekty bezpečnosti multimediálních dat,In: Security magazin, roč.X, vyd.č.53, 3/2003, vyd. Familymedia, Praha, 2003, str.36-38, ISSN 1210-8723.

[3] Čandík, M., Ivanka, J. : Bezpečnost v informačních technologiích, In: Security magazin, Roč. X., vyd.53, 3/2003, vyd. Familymedia, Praha, 2003, str.50-51, ISSN 1210-8723

[4] Ivanka, J.: Tvorba elektronických studijních opor pro bezpečnostní technologie, systémy a management. Sborník příspěvků ze 7. konference, Internet a konkurenceschopnost podniku.,UTB ve Zlíně, Zlín , str. 67, ISBN 80-7318-269-6

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

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

Termín odevzdání bakalářské práce: **25. května 2007**

Ve Zlíně dne 13. února 2007

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této bakalářské práce je obecné seznámení s legislativou vztahující se k odposlechům v České republice a následné seznámení s problematikou odposlechových zařízení.

Dále obeznámení s problematikou právní podstaty odposlechu v oblasti detektivních činností. Analýza a základní rozdělení operativní techniky pro získávání citlivých informací a to jak v oblasti detektivních činností, tak i v oblasti občanského života.

Multimediální kurz se zabývá problematikou multimédií a tvorbou kurzů s prvky e-learningu.

Klíčová slova: Odposlechové zařízení, zabezpečení informace, prevence odposlechu, E-learning

ABSTRACT

The purpose of this work is the general familiarization with the legislative relative to tapping in the Czech Republic and the subsequent familiarization with the questions surrounding tapping devices.

Further identification with the questions and problems surrounding the legal nature of tapping in the areas of criminal a detective work. Analysis and basic division of operative techniques for retrieving sensitive information in areas such as detective / criminal work, and in areas of everyday life .

Multimedia course deals with the questions of multimedia and the creation of courses with elements of e-learning.

Keywords: Tapping devices, safeguarding information, prevention of tapping, e-learning

Tři cesty vedou k poznání: cesta zamyšlení – ta je nejušlechtilejší, cesta napodobování – ta je nejlehčí a cesta pokusů – ta je nejtrpčí

Konfucius (okolo 551 až 479 př. N. l.)

Chtěl bych poděkovat panu Ing. Jánu Ivankovi za odbornou pomoc a cenné rady vedoucí k vypracování této bakalářské práce. A dále bych rád poděkoval rodině a kamarádům za podporu a pomoc při studiu a zpracování této práce.

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

Ve Zlíně dne 31. srpna 2007 …….

František Šošolík

OBSAH

ÚVOD

V dnešní hektické době, kdy se člověk žene za úspěchem a dokončením co největšího množství stanovených úkolů a cílů zapomíná možná na jednu z nejdůležitějších věcí, a to zabezpečení svého pracovního zázemí.

O odposlechu a krádeži informací se velmi málo mluví, těžko se zjišťuje a jestě hůře dokazuje. Přestože je to nejnebezpečnější druh kriminální činnosti v oblasti komerční bezpečnosti.

Se vstupem České republiky do tržního prostředí Evropské unie a se zvýšeným rozvojem soukromého podnikání se objevují také první případy odposlechu a zcizování cenných informací. Mnoho firem si neuvědomuje nebezpečnost tohoto jednání a nedoceňují ochranu svých informací i svého vybudovaného know-how.

Cílem mé práce je vytvoření souhrnného přehledu zabezpečovacích systémů a obecného seznámení čtenáře s legislativou možného odposlechu a přehledem různých druhů speciálních bezpečnostních prostředků odposlouchávacích technologií a prostředků na ochranu proti nim.

1 PRÁVNÍ PODSTATA ODPOSLECHŮ

1.1 Vymezení pojmů odposlech a záznam telekomunikačního provozu

Náš právní řád neobsahuje vymezení pojmu telekomunikační provoz a to navzdory skutečnosti, že s tímto pojmem poměrně často pracuje. Tento pojem je tedy definován pouze v komentářích k trestnímu řádu, a to následovně: „Pod pojmem telekomunikační provoz se rozumí telefon, telefax, mobilní telefony, vysílačky i jiná telekomunikační zařízeni." Netřeba vysvětlovat, že nejde o vymezení zdařilé.

Při vymezení pojmu telekomunikační provoz resp. jeho záznam a odposlech, je patrně třeba vycházet z legálních definic bezprostředně souvisejících pojmů uvedených v zákoně č. 151/2000 Sb., o telekomunikacích, v platném znění (dále jen TelZ), zvláště pojmů telekomunikační služba (§2 odst.5 TelZ), telekomunikační síť (§2 odst.2 TelZ) a telekomunikační zařízení (§2 odst.1 TelZ). S přihlédnutím k těmto definicím lze pojem telekomunikační provoz vymezit jako „činnost telekomunikačních zařízení (např. telefonů, radiostanic, počítačových sítí atd.), která spočívá v přepravě nebo směrování jak obsahu komunikace (např. hovorů nebo písemných zpráv), tak i souvisejících provozních údajů (např. doprovodných dat identifikujících určité účastnické stanice apod.). Za samotný odposlech a záznam telekomunikačního provozu pak lze považovat „Zákonný postup oprávněných subjektů (Policie ČR, Bezpečnostní informační služby a Vojenského obranného zpravodajství) spočívající v přenosu údajů telekomunikačního provozu na média nesoucí záznam těchto oprávněných subjektů.“ Z výše uvedeného vymezení je zřejmé, že za telekomunikační provoz lze považovat i provoz realizovaný prostřednictvím počítačové sítě Internet a jejího monitorování za odposlech.[3]

1.2 Přehled úpravy

Ochrana soukromí (ať již v podobě telekomunikačního, listovního či jemu podobných tajemství) může být, jak ostatně již bylo výše uvedeno, prolomena pouze na základě zákona a za podmínek, které stanoví zákon. Zásahy do tohoto práva je možné provést pouze buď v průběhu trestního řízení, a to na základě zákona o policii (dále jen

ZoP) a trestního řádu (TrŘ) - jde o zjevně nejčastější případ, nebo mimo trestní řízení, a to podle zákona o Bezpečnostní informační službě (BIS) nebo zákona o Vojenském obranném zpravodajství (VOZ). V jiných případech nebo na základě jiných předpisů zásadně nelze provést zásah do práva na soukromí.

Technické podmínky pro připojení a provoz zařízení pro odposlouchávání a zaznamenávání telekomunikačních provozů pak stanoví příslušná vyhláška ministerstva vnitra č. 191/2000 Sb. Podmínky pro postup soudce při rozhodování o povolení použití operativní techniky jsou obecně upraveny v řadě souvisejících instrukcích Ministerstva spravedlnosti. Tyto instrukce se poté přiměřeně aplikují i na postup předsedů senátů vrchních soudů při rozhodování o povolení k použití zpravodajské techniky podle zákona o BIS a zákona o VOZ. [3]

1.3 Zásahy v průběhu trestního řízení

Jediným výlučně procesním předpisem, který umožňuje odposlech a záznam (dále jen záznam) telekomunikačního provozu k důkazním účelům, je pouze trestní řád. Samotná hranice pro pořízení a následné využití záznamu telekomunikačního provozu v rámci trestního řízení a mimo něj, je dána zahájením trestního stíhání, k němuž dochází sdělením obvinění obviněnému (§160 odst.1 TrŘ.), výjimečně též provedením neodkladných nebo neopakovatelných úkonů před zahájením trestního stíhání (§160 odst.2 TrŘ). Až na tuto výjimku je tedy odposlech přípustný až po sdělení obvinění konkrétní osobě, a to pouze je-li vedeno trestní řízení pro zvlášť závažný úmyslný trestný čin nebo pro jiný úmyslný trestný čin k jehož stíhání zavazuje vyhlášená mezinárodní smlouva. V takovém případě může *předseda senátu* (v přípravném řízení na návrh státního zástupce i *soudce)* nařídit odposlech a záznam telekomunikačního provozu, pokud lze důvodně předpokládat, že tím budou sděleny významné skutečnosti pro trestní řízení. (§88 TrŘ) V jiném případě odposlech a záznam nařídit nelze. Samotný soudní příkaz k odposlechu a záznamu telekomunikačního provozu pak musí splňovat, vyjma obecných požadavků (jako je např. označení orgánu, o jehož rozhodnutí jde, den a místo rozhodnutí, a konkrétní výrok s uvedením zákonných ustanovení jichž bylo použito, jakož i poučení o opravném prostředku), řadu zákonných náležitostí:

-musí být vydán písemně a odůvodněn;

-musí v něm být zřetelně uloženo provedení odposlechu a záznam příslušného druhu

telekomunikačního provozu (např. TCP/IP)

-musí v něm být specifikován druh a místo odposlechu a záznamu, majitel či uživatel telekomunikačního zařízení (a to s uvedením jména a příjmení, adresy, příp. i zaměstnání a dalších potřebných identifikačních údajů), jakož i trestný čin pro nějž se vede trestní řízení.

-musí zde být rovněž uveden účel takového odposlechu a záznamu a doba po kterou může být takto prováděn (ta nemůže být delší než šest měsíců – lze ji však prodloužit, a to i opakovaně).

Dodržení výše uvedených náležitostí je nezbytné, v mnoha ohledech totiž podmiňuje důkazní uplatnění samotného záznamu. Pokud při odposlechu a záznamu nebyly zjištěny skutečnosti významné pro trestní řízení, je nutno záznamy předepsaným způsobem zničit. (§88 odst.5 TrŘ).

Samotný odposlech a záznam telekomunikačního provozu provádí pro potřeby všech orgánů činných v trestním řízení Policie České republiky (§88 odst. 2 TrŘ), a to zejména na základě zákona o policii. Podle této úpravy jsou provozovatelé telekomunikační činnosti povinni na vlastní náklady zabezpečit v určených bodech oprávněným subjektům (tedy i mimo trestní řízení) připojení zařízení pro odposlouchávání a zaznamenávání telekomunikačního provozu (§86 odst.2 TelZ).

Podle §37 odst.1 ZoP pak nesmí tyto prostředky, které jsou výslovně zákonem označeny jako operativně-pátrací, sledovat jiný zájem než získání informací důležitých k odhalení a objasnění trestných činů. Tím jsou dány též meze využití získaných poznatků. Odposlech a záznam telekomunikačního provozu a zjišťování údajů o telekomunikačním provozu jsou poté pro Policii ČR podrobněji upraveny čl. 59 Závazného pokynu.[3]

1.4 Zásahy mimo trestního řízení

1.4.1 Zákon o Bezpečnostní informační službě

Zákon o Bezpečnostní informační službě uvádí odposlech a záznam telekomunikačního provozu mezi zpravodajskými prostředky (jde o jednu z forem zpravodajské techniky). Bezpečnostní informační služba přitom získává, shromažďuje a vyhodnocuje informace důležité pro ochranu ústavního zřízení, významné ekonomické

zájmy, bezpečnost a obranu ČR; k tomuto účelu může zpravodajskou techniku použít pouze po předchozím písemném povolení předsedy senátu Vrchního soudu (podle sídla Bezpečnostní informační služby), pouze však za předpokladu, že by odhalování nebo dokumentování činností, pro něž má být použita, bylo jiným způsobem neúčinné nebo podstatně ztížené eventuálně v daném případě nemožné. Použití zpravodajské techniky nesmí překročit rozsah pověření soudce a nesmí zasahovat do práv a svobod občanů nad nezbytně nutnou míru.[3]

1.4.2 Zákon o Vojenském obranném zpravodajství

Rovněž zákon o Vojenském obranném zpravodajství dovoluje použití zpravodajské techniky pouze na základě předchozího písemného povolení k použití zpravodajské techniky, vydaného vrchním soudem (vydává předseda senátu vrchního soudu), a to pouze v případech, kdy odhalování a dokumentování činností, pro něž má být použita, je jiným způsobem neúčinné nebo podstatně ztíženo. Použití zpravodajské techniky smí omezit nedotknutelnost obydlí, listovní tajemství a tajemství dopravovaných zpráv jen v nezbytně nutné míře.[3]

1.5 Další související podrobnosti

Jednou z dalších, a to rozhodně však ne nevýznamných otázek, je povinnost uchovávat a případně i vydat doprovodné a související údaje o již uskutečněném telekomunikačním provozu. Je-li k objasnění skutečností důležitých pro trestní řízení třeba zjistit údaje o již uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, nařídí předseda senátu a v přípravném řízení soudce, aby je právnické nebo fyzické osoby, které vykonávají telekomunikační činnost, sdělily jemu a v přípravném řízení buď státnímu zástupci nebo policejnímu orgánu. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn. Výslovná a zřejmá povinnost archivovat tyto údaje však v našem právním řádu dosud zakotvena není, tudíž tato snaha nemusí být vždy efektivní. Na základě §84 odst.7 TelZ však musí být tato doprovodná data po uplynutí dvou měsíců od ukončení telekomunikačního spojení vymazána nebo učiněna anonymními.

Policie ČR je v tomto ohledu na základě §47a ZoP oprávněna žádat, a to již bez

přivolení soudu, v rozsahu potřebném pro plnění konkrétního úkolu policie od právnických a fyzických osob, které zajišťují telekomunikační činnost, předávání dat souvisejících s poskytováním telekomunikační služby způsobem umožňujícím dálkový a nepřetržitý přístup. Právnické a fyzické osoby, které zajišťují telekomunikační činnost, jsou tak povinny žádosti policie bez zbytečného odkladu vyhovět ve vyžádané formě a v rozsahu stanoveném TelZ. Provozovatel telekomunikační činnosti je totiž povinen na vlastní náklady sdělit oprávněným orgánům informace o skutečnostech, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, zejména údaje o veškeré komunikaci, kteréhokoli uživatele v uplynulých nejméně dvou měsících v rozsahu volané a volající číslo, použitá služba, datum, čas, doba trvání komunikace a místo připojení.

Z TrŘ a TelZ vyplývá tedy povinnost provozovatelů telekomunikačních síti vyhovět požadavku o sdělení provozních údajů. Zde je na místě poznamenat, že jednotliví provozovatelé telekomunikačních sítí, především operátoři mobilních či telefonních sítí, sice respektovali tyto zmiňované zákonné normy, avšak rozsah poskytovaných informací nebyl zdaleka jednotný. Touto problematikou se na základě stížnosti zabýval Ústavní soud. Z jeho nálezu vyplynulo, že předmětem vyžádání orgánů činných v trestním řízení, může být zejména:

- *číslo volané stanice,*
- *datum a čas počátku hovoru,*
- *doba jeho trvání a označení základové stanice, která zajišťovala hovor v okamžiku spojení, a označení základové stanice, která hovor zajišťovala v momentu (jako např. lokalizace komunikujících SIM karet, apod.)*

Jedním z dalších souvisejících otázek je mimo jiné otázka následného použití záznamu telekomunikačního provozu jako důkazu (ať již v občanskoprávním či veřejnoprávním řízení), které je, a to zejména z efektivní kontroly nad výše uvedenými pravidly, poměrně zásadně omezeno. Dalším tématem je poté problematika veřejné kontroly nad odposlechem a záznamem telekomunikačního provozu. Tato dvě, posledně jmenovaná témata, tedy dokazování a veřejná kontrola však nejsou předmětem této kauzy a bude zpracována formou samostatného článku.[3]

1.6 Shrnutí české legislativy

V České republice jsou tedy stanovena poměrně jasná pravidla pro odposlech

a záznam telekomunikačního provozu ze strany státních orgánů. Tato pravidla lze, až na výše zmíněné výjimky, resp. dílčí nejasnosti, považovat za fungující a jejich kontrolu za demokratickou a efektivní. Vyjasnění některých již zmíněných otázek by však bylo nesporně v zájmu samotných vyšetřovacích orgánů a odpadly by důvody pro podezřívání z resortního protekcionismu, který, ačkoliv v k němu patrně nedochází, je často zmiňován a negativně tak ovlivňuje důvěru v práci státních orgánů.

V tomto ohledu lze tedy zakončit tím, že stávající koncepce, resp. česká právní úprava odposlechu a záznamu telekomunikačního provozu odpovídá běžnému standartu, obvyklému v zahraničí, lze ji považovat za vyhovující a do budoucna za relativně neměnnou.

2 PROČ POUŽÍT SPECIALNÍ OPERATIVNÍ TECHNIKU

2.1 Konkurenční zpravodajství

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

- Legálním a etickým postupem shromažďovat informace ke svému užitku
- Objektivní analýzu informací, která se nevyhýbá nepříjemným závěrům
- Zajistit distribuci informací k těm kdo rozhodují.

Ochrana ekonomických zájmů však vyžaduje komplexní přístup, ale především je daleko širší než technická či fyzická ochrana objektů. Významným faktorem ovlivňujícím prosperitu, konkurence schopnost a exportní schopnost každé firmy (společnosti, podniku, instituce, organizace apod.) je nesporně schopnost předvídat a řešit krizové situace, schopnost odolávat nejrůznějším ohrožením zcizení informace, rizikům a nástrahám a to jak vnějšího tak vnitřního charakteru.[4]

2.1.1 Obranné konkurenční zpravodajství

Úkolem obranného konkurenčního zpravodajství je převážně:

- Zajišťování personální bezpečnosti, režimové bezpečnosti, bezpečnosti technických prostředků, bezpečnosti softwarových prostředků
- Zajišťování informační bezpečnosti
- Zajišťování bezpečnosti KNOW-HOW, ochranu technologických procesů
- Zajišťování provozní bezpečnosti

- Zajišťování bezpečnosti v obchodních vztazích

- Aktivní ochranu proti dezinformacím a působení vlivového zpravodajství konkurence

- Obrana proti ofenzivnímu konkurenčnímu zpravodajství konkurence

Prvotním úkolem k tomu, aby podnikatelský subjekt mohl úspěšně fungovat, je ochránit sám sebe. To znamená ochránit vlastní podnikatelský subjekt, jeho hmotný i nehmotný majetek, Know-How a jiné.

2.1.2 Aktivní konkurenční zpravodajství

Úkolem aktivního konkurenčního zpravodajství je převážně:

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

- Zajišťování informací marketingového charakteru;

- Zjišťování informací o konkurenci;

- Zjišťování informací o technologiích;

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

2.2 Bezpečnostní složky státu

Bezpečnostní složky státu musí mít moderní monitorovací a sledovací techniku, neboť v bezpečném a moderním státě je nepostradatelná pro účinnou a efektivní práci vojenské i civilní kontrašpionáže. Její nezbytnost potvrzují i zvyšující se aktivity teroristických organizací a mafiánských skupin operujících na území našeho i okolního státu. Kdo o nezbytnosti této speciální techniky dlouho pochyboval nebo ještě stále pochybuje, ať si vzpomene jaké důsledky měla neprecizní práce amerických tajných služeb před datem 11. září 2001.[4]

3 DĚLENÍ ODPOSLECHOVÝCH A SPECIÁLNÍCH PROSTŘEDKŮ

3.1 Dělení odposlechových zařízení

3.1.1 Rozdělení podle umístění v zájmovém prostoru

a) umístění s nutností narušení zájmového prostoru

b) bez nutnosti narušení zájmového prostoru

3.1.2 Rozdělení podle typu přenosové cesty

a) Po metalickém vedení

b) Bezdrátovou cestou

3.1.3 Rozdělení podle typu přenášené informace

a) zařízení na přenos audio signálu

b) zařízení na přenos video signálu

c) zařízení s kombinovaným přenosem audio i video signálu

3.2 Dělení speciálních prostředků

a) Šumové generátory

b) Radiové analyzátory

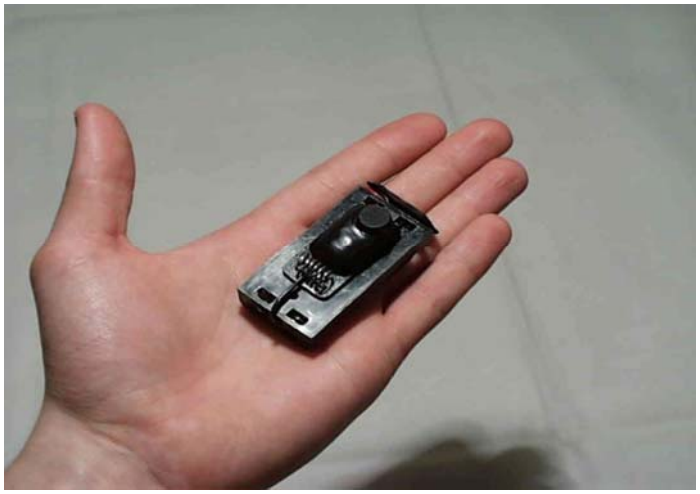
c) Detektor nelineárních přechodů

d) Jammer‘s – rušičky signálu

4 PŘÍKLADY ODPOSLECHOVÝCH ZAŘÍZENÍ

4.1 Radiové odposlechové zařízení R-100

R-100 je kompaktní radiové odposlechové zařízení napájené z 9V destičkové baterie. Příjem signálu je standardně v rozhlasovém pásmu FM-VKVII (kmitočtový rozsah 87,5-108 MHz) nebo na objednávku v pásmu "východní normy" FM-VKVI (66-73 MHz), případně pro zajištění maximální diskrétnosti poslechu lze dodat systém naladěný na specifickou frekvenci mimo rozsah veřejných komunikací spolu s dodáním speciálního přijímače.[10]



Obr. 1 Rádiové odposlechové zařízení R-100

Vlastnosti: Zařízení je všesměrové, velmi citlivé, jeho citlivost je v určitých mezích automaticky řízena podle síly okolních zvuků tak, aby nedocházelo ke zkreslení přenosu u silnějších signálů. Odposlech má vestavěn obvod napěťové stabilizace, lze jej tedy napájet jak z primárních článků, tak z dobíjecích (akumulátorů NiCd nebo NiMH). Přesto doporučujeme používat výhradně kvalitní alkalické články - např GP, Alkacell, Varta Alkaline, apod. Signál zachycený na přijímači lze běžným způsobem nahrávat na magnetofon apod.[10]

Dosah: Pro maximální dosah platí obecná zásada umístění vysílače pokud možno co nejvýše a co nejdále od vodivých předmětů-pozor na radiátory, drátěné ploty, panelové stěny, železné konstrukce apod. Tyto překážky silně pohlcují vyzařovanou energii a dosah se tím může podle podmínek podstatně zmenšit. Dosah je pochopitelně taktéž značně

ovlivněn vf citlivostí použitého přijímače. Poloha vysílací anténky není kritická, doporučuje se její svislé umístění. Z výroby je anténka nastavena na optimální délku, její zkrácení je možné, především v případech, kdy postačí menší dosah. Délka by přesto neměla být menší než 20 cm. V žádném případě se nedoporučuje "omotávání" anténky kolem zařízení – vysílací výkon silně poklesne. Při dodržení všech výše uvedených zásad je přibližný (!) dosah ve volném terénu 400-1000m (v zástavbě: 100-300m).

Ačkoliv jde o optimálně nastavené zařízení, jeho obvodová koncepce je poměrně jednoduchá a nemůže tak být pochopitelně konkurentem frekvenčně řízeným systémům, jejichž nejjednodušší verze začínají na úrovni třicetinásobku této ceny. Mini vysílač je nicméně vyroben s velkou pečlivostí a díky své překvapivé citlivosti je velmi oblíben ve většině aplikací, kde postačí statické umístění .[10]

Příklady použití:

- skrytý odposlech zájmových prostor
- ostraha majetku (aut, objektů, místností, předmětů)
- hlídání dětí apod.
- monitoring prostor ve Vaší nepřítomnosti, menších prodejen a "krámů", místností, čekáren apod.
- s výhodou lze používat dvě zařízení pracující na různých místech a různých frekvencích ke vzájemnému dorozumívání dvou osob - tzv. duální provoz.
- lze používat i více odposlechů najednou. Například v kombinaci se speciálním přijímačem vybaveným pamětmi tak dostaneme velice operativní prostředek pro kontrolu více místností v budovách apod. Pouhým navolením čísla paměti je pak uživatel schopen okamžitě přepínat odposlechy jednotlivých prostor. Tato možnost je jistě velmi zajímavá především pro hlídací a detektivní agentury.

Často je možné se setkat s laickým názorem, že může být provozováno více odposlechů (např. různých místností) na jedné frekvenci. Toto je ovšem bohužel mylná představa. Každý takový odposlech musí pracovat zásadně na jiné frekvenci. Týká se to ovšem obecně jakýchkoliv vysílacích zařízení. Pro speciální komunikační přijímače vybavené pamětmi není ovšem příjem (a mžikové přelaďování) více odposlechových zařízení žádným problémem.[10]

4.2 Rádiový odposlech zabudovaný v rozdvojce R-200 AC

R-200 AC je radiové odposlechové zařízení zabudované do plně funkční síťové rozdvojky a napájené z rozvodu 230V~ . Příjem signálu z vysílače je snadný s pomocí speciálního přijímače v pásmu AIR (kmitočtový rozsah 115 - 135 MHz).

Obr. 2 Rádiové odposlechové zařízení R-200 AC

Vlastnosti:

- Žádné problémy s výměnou napájecích článků – žádné nejsou !
- Dokonalá kamufláž – zařízení je zcela ukryto v rozdvojce a prakticky jej nelze náhodně odhalit.
- Nikde „nečouhá“ anténa – je kamuflovaná přímo v rozdvojce.
- Maximálně jednoduchá instalace - po zasunutí do síťové zásuvky stačí naladit příslušnou frekvenci na přijímači a poslouchat.
- Rozdvojka je plně funkční pro připojení elektrospotřebičů.
- Protože umístění vysílače v síťové zásuvce je neměnné, je oproti jiným jednoduchým vysílačům frekvence stabilnější.
- Dosah vysílače má smysl uvažovat jen v bytové zástavbě (ztížené podmínky šíření) a pohybuje se cca do 100 m. Protože šíření signálu napomáhá síťové vedení, je tato štěnice vhodná pro použití např. i v panelových domech, kde bývá jinak velký útlum signálu vlivem železobetonové konstrukce.

- Častým neduhem jednoduchých štěnic napájených ze sítě bývá průnik síťového rušení, čímž je značně ovlivněna kvalita přijímaného zvuku. ! POZOR ! Tuto skutečnost někteří prodejci mlčky přehlíží. R-200 AC má síťové rušení účinně potlačeno do té míry, že při příjmu není téměř rozeznatelné !
- Zcela zanedbatelné náklady na provoz – cca 1,40 Kč/měsíc při NON-STOP provozu a ceně elektřiny 4Kč/kWh

4.3 Telefonní odposlech TO-Line (odposlech pevné linky)

Malý adaptér k diktafonu pro automatické přímé nahrávání telefonních hovorů na pevné telefonní lince. Diktafon je spouštěn zvednutím sluchátka telefonu nebo v okamžiku zvonění telefonu. Záznam se dočasně přeruší při odmlčení a automaticky aktivuje po promluvení. Přípravek se připojuje paralelně na telefonní linku kdekoliv po délce jejího vedení (není třeba jejího rozpojení). Nepotřebuje zvláštní napájení, je napájen přímo z telefonní linky. Pro zajištění maximální flexibility je připojení možné prostřednictvím třech typů výměnných koncovek: koncovky standard , koncovky propichovací nebo koncovky telefonní typ RJ. Vhodný pro všechny typy diktafonů. Součástí balení jsou propichovací koncovky.[10]

Obr. 3 Telefonní odposlech TO-Line

4.4 Rádiový systém odposlechu telefonní linky

Ne vždy máme možnost se napojit na telefonní vedení mimo odposlechový prostor. Zbývá možnost napojení telefonní linky přímo v účastnické zásuvce nebo v telefonním přístroji a drátovým vedením propojit skrytý magnetofon. Pravidelná kontrola nahrávky a tím i četnost pohybu poblíž nebo přímo v odposlechovém prostoru není vhodná a proto se volí způsob, který přenáší telefonní hovor vzduchem po radiových vlnách. Používají se miniaturní radio-vysílače, místo mikrofonu je zde adaptér pro napojení na telefonní linku. Napájení radio-vysílače můžeme volit z baterie, nebo použít k napájení 60 V z telefonní sítě. Klasická telefonní štěnice je krabička rozměru 2 x 2 x 1 cm se dvěma drátky na připojení. Telefonní vedení nahrazuje zdroj signálu - mikrofon, napájecí zdroj i anténu. Kvalitnější telefonní radio-vysílače jsou dvoukanálové, jeden kanál snímá a vysílá telefonní hovor a druhý snímá zvuky z místnosti.[16]

Obr. 4 Druhy zabudovaných telefonních radiovysílačů

4.5 Štěnice s neomezeným dosahem R-N3310

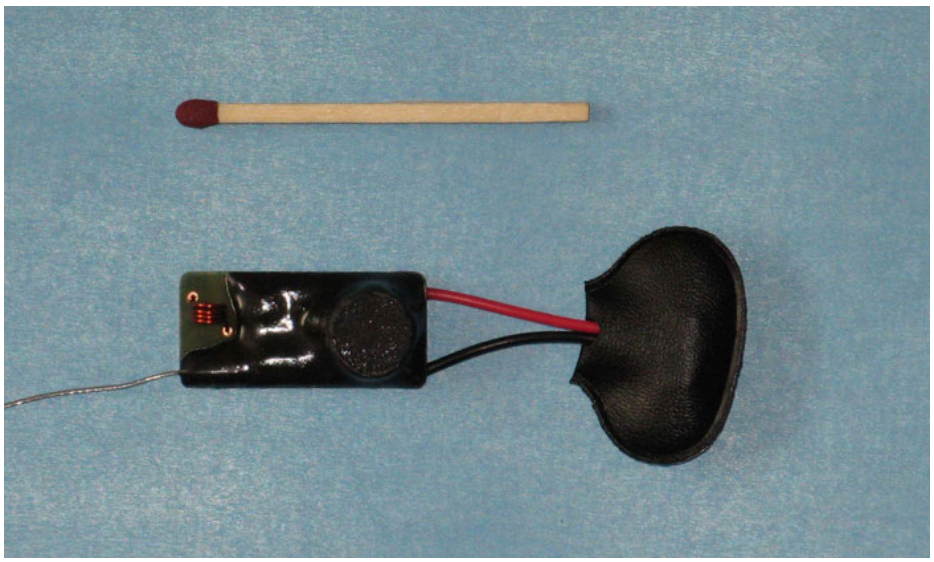
R-N3310 je speciálně upravený mobilní telefon Nokia 3310 určený pro skrytý odposlech zájmového prostoru na neomezenou vzdálenost. Pro aktivaci odposlechu stačí vytočit jeho telefonní číslo. Telefon hovor automaticky diskrétně přijme a aktivuje odposlech - neustále se však "tváří" jako vypnutý, nezvoní, nevibruje.

Mikrofon telefonu je schopen zachytit tichý hovor na vzdálenost až 10 m. Díky GSM přenosu informací je dosah R-N3310 neomezený. Telefon pak stačí někde "zapomenout" nebo skrytě umístit. Baterie vydrží přístroj napájet až 10 dnů v pohotovostním režimu nebo až 12 hodin nepřetržitého odposlechu.[15]

Obr. 5 Mobilní telefon s instalovaným mikrofonem

4.6 Odposlechový vysílač R-250

Miniaturní vysílač s větším dosahem určený především ke skrytému odposlechu hovorů. Zařízení bylo vyvinuto s cílem uspokojit poptávku po kvalitním a dostupném výrobku srovnatelným s některými zahraničními produkty, přitom ale nabídnout velmi přijatelnou cenu. Výrobek tak splňuje některé specifické požadavky kladené na zpravodajskou techniku tohoto typu: stabilita, citlivost, dosah, velikost.



Obr. 6 Odposlechová štěnice R-250

Dostatečná **STABILITA** vysílací frekvence, umožňuje umístit odposlech i přímo pod oděv, do zavazadla, jedoucího vozidla apod., aniž by se frekvence více měnila a tím byl znemožněn příjem (častý problém většiny amatérských výrobků).

Dobrá **CITLIVOST** umožňuje zachytit i tiché rozhovory v běžné místnosti cca 6 x 6m, přičemž umístění vysílače není kritické. Dobré šumové vlastnosti jsou dány především pečlivým výběrem osazeného subminiaturního mikrofonu.

DOSAH vysílače je v porovnání s „průměrnou“ nabídkou jiných zařízení na trhu podstatně větší. V bytové zástavbě cca 250 až 600 m, na přímou viditelnost 600 až 1000 m.

VELIKOST vysílače je díky použité moderní technologii SMD jen cca 28 x 12 x 6 mm! [10]

Další informace:

Vysílač je standardně dodáván pro VKV Air pásmo (110-135MHz); k příjmu signálu je tedy nutný přijímač s tímto vlnovým rozsahem. Vysílací frekvenci je možné v případě potřeby upravit: Mírným roztažením závitů cívky frekvence stoupne a naopak. Upozorňujeme, že manipulaci s cívečkou je nutné provádět pouze nekovovými předměty (např. seříznutou sirkou) a s maximální opatrností - lakovaný vodič cívky se nesmí poškodit !

Pozn.: Není-li nutno vysílací frekvenci např. z důvodu narušení kanálu měnit, pak je bezpečnější tuto úpravu raději vůbec neprovádět.

Při časté manipulaci s napájecím klipsem 9V může dojít k jeho poškození. Výrobce si je této skutečnosti vědom, bohužel však kvalitu klipsu neovlivní. Pro případ poškození je proto přiložen klips náhradní. Při jeho event. výměně nezaměňte jeho polaritu. Zařízení může být napájeno z jakéhokoliv externího zdroje 9V ss.

TECHNICKÉ ÚDAJE

Napájení: 9V alkalická, životnost cca 36 hodin provozu

Frekvenční pásmo: 115-135 MHz

Typ modulace: F3, WFM

Vysílací výkon: cca 50mW

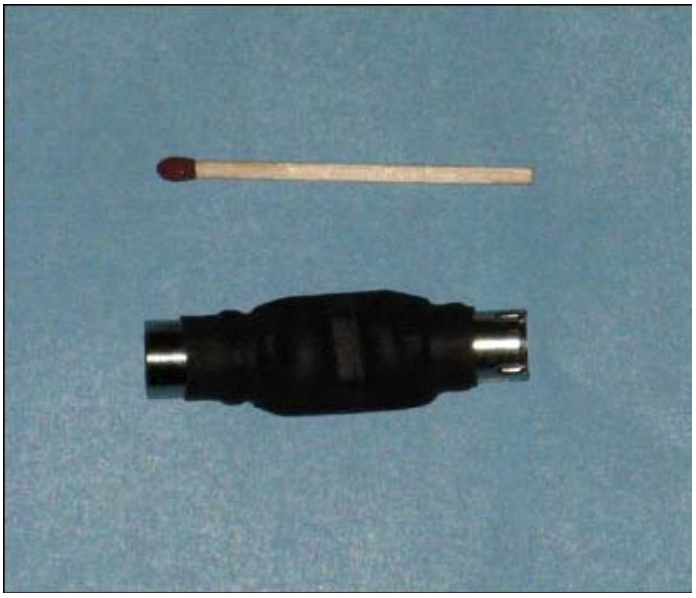
Dosah signálu: 250-600m / 600-1000 m (bytová zástavba / volný prostor)

Velikost: 28 x 12 x 6 mm

Pozn.: Údaje o dosahu se mohou od uváděných údajů podle podmínek i výrazněji lišit směrem nahoru i dolů. Doporučuje se anténku nezkracovat (v žádném případě neomotávat kolem vysílače) a ponechat ji pokud možno svěšenou svisle dolů. Dosah zkracuje blízkost el. vodivých (především kovových) předmětů, ale i lidského těla. Významný vliv má rovněž vf citlivost použitého přijímače a přijímací anténa. [10]

4.7 Odposlech klávesnice – KEYlog

Odposlech klávesnice KEYlog je malá „redukce“ mezi klávesnicí a počítačem, která zaznamenává do své vlastní paměti vše, co se na klávesnici připojené k vašemu počítači napíše – například aktuálně zadávané webové adresy, obsah emailových zpráv, dokumenty, komunikace ICQ a všechna hesla. KEYlog Vám tedy umožňuje mít kompletní přehled a kontrolu nad vším, co se na počítači děje ve vaší nepřítomnosti.



Obr. 7 Odposlech klávesnice KEYlog

Princip KEYlog:

Po připojení mezi klávesnici a počítač začne automaticky nepřetržitě monitorovat činnost klávesnice a všechny stisknuté klávesy zaznamenává. Integrovaný mikroprocesor s vlastní pamětí zajišťuje bezproblémový chod zařízení nezávisle na počítači. KEYlog nevyžaduje žádnou softwarovou instalaci nebo jiné nastavení počítače, neovlivňuje běh žádného programu a nelze jej zjistit žádným „obranným“ programem (antivirem, apod.). Stačí pouze připojit a je ihned připraven k použití.

KEYlog pracuje ihned po zapnutí počítače, lze jím tedy zjistit i hesla k BIOSU nebo hesla potřebná k odemknutí pevného disku, která je nutné zadat ještě před startem operačního systému.

Prohlížení obsahu paměti je možné na libovolném počítači včetně toho, který KEYlog aktuálně „monitoruje“. Jednoduše otevřete poznámkový blok, který je základní součástí windows, a napíšete „heslo“ (stejným způsobem jako by jste chtěli „normálně“ psát) KEYlog toto heslo rozpozná a vypíše obsah paměti jako klasický text, který je poté možné prohlížet, ukládat nebo tisknout.

Zařízení bylo vyvinuto s důrazem na maximální jednoduchost obsluhy, práci s ním tedy bez problémů zvládne i úplný laik.

KEYlog lze používat na libovolném počítači, bez ohledu na druh operačního systému nebo konfiguraci hardware. Jedinou podmínkou je PS2 konektor pro připojení klávesnice, který je v současnosti nejpoužívanější a jsou jím vybaveny všechny běžné stolní počítače. Vhodný i pro použití s bezdrátovou nebo multimediální klávesnicí. [10]

Na přání lze KEYlog zabudovat do dodané klávesnice. V takovém případě je prakticky neodhalitelný i fyzickou prohlídkou počítače odborníkem.

4.8 Leserový mikrofon

Laser patří mezi mladší vynálezy 20. století. Přesto, že mu bude příští rok teprve 40 let, stal se nedílnou součástí našeho života. Laser si našel velmi rychle cestu i v oblasti vojenské techniky (navádění střel a bomb) a špionážní techniky (laserový mikrofon). Vedle štěnicových instalací existují také elegantnější cesty, jak odposlouchávat místnost. Laserové odposlechové zařízení se řadí do optoelektronických odposlechových zařízení. K odposlechu na dálku je určen laserový vysílač, jehož laserový paprsek je zaměřen na okno odposlouchávané místnosti a okenním sklem odražený paprsek je zachycen laserovým přijímačem. Zvukové vlny vyvolané hovorem uvnitř místnosti rozechvějí okenní tabule ke slabé vibraci. Laserový paprsek dopadající na tabuli skla je těmito vibracemi modulován a po zachycení v přijímači je opět demodulován do srozumitelné řeči. Normálně je tato technika nasazena jen High-Tech - odposlechovými experty. Tento typ odposlechu má velmi problematické využití – z platnosti fyzikálních zákonů je obtížné

najít optimálně kolmý přístup k okenním tabulkám a v zájmovém prostoru musí být použita čirá skla. Při splnění těchto podmínek je pak laserový odposlech velmi nebezpečný. Dosah zařízení je okolo 200 metrů. Nevýhodou jsou velmi vysoké pořizovací náklady. Odposlechová laserová technika může být smontována také s heliovým - neonovým paprskem, nebo polovodičovým laserem a levným laserovým přijímačem. Systém může být pro náročné uživatele doplněn puškohledem pro monitorování a nahrávání pohybujících se objektů. Komunikace pomocí modulovaných světelných paprsků není žádná nová myšlenka. Právě v 80. letech 19. století experimentoval Graham Bell s pokusným přístrojem s popisem „fotofonu". Tento přístroj se hodil k modulaci slunečního paprsku. K tomu má přístroj druh hubice s ozrcadlenou membránou. Při rozhovoru byl na membráně řízený sluneční paprsek vychýlen v rytmu řečové frekvence. Na místě příjmu reflektovaného paprsku může být udělán hlas pomocí solárního článku a citlivého sluchátka opět slyšitelným. Komerčnímu využití tohoto komunikačního způsobu bylo však zabráněno vzhledem k pohybu slunce a mračen. Na základním principu Grahama Bella se i v moderní době nic nezměnilo. Úkol slunečního paprsku přebírá teď laserův paprsek s koherentním světlem. Profesionální laserové odposlechové přístroje obsahují infračervené laserové zdroje. Infračervené světlo nemůže být vnímáno lidským okem. Aby se docílilo také na velké vzdálenosti ještě dobrých odposlechových výsledků, pracuje se s zářivým zdrojem o výkonu až 35mW. Kdo se náhodně podívá při tomto zářivém zdroji z odposlechového okna do paprsku, může si odnést těžké poškození zraku. Laserové světlo, ať viditelné nebo neviditelné, se značně odlišuje od normálního světla. Světlo žárovky nebo zářivky obsahuje široké spektrum různých vlnových délek, přičemž vyzařování se koná spontánně a náhodně ve všech možných směrech. U laserového zdroje jde záření jen jedním směrem a obsahuje jen jedinou vlnovou délku. Toto dává paprsku ostré svazkování a typickou barvu. Když se setkají dva laserové paprsky stejné vlnové délky, mohou buď zhasnout nebo zesílit. Tento vypínací nebo zesilovací efekt může být vyhodnocen při pohybu reflektujícího povrchu prostřednictvím interferometru. Na polopropustném zrcadle (tzv. Beam-Splitter), je přeladěna část nastupujícího paprsku. V přijímači může být paprsek srovnán ze zdroje cílovým reflektorem přicházejícího paprsku fázově, popř. výchylkově. Hlavní problémy u tohoto interferenčního odposlechového postupu záleží na skutečnosti, že přes paprskovou štěpinu může být řízena na cíl jen část laserové energie. Toto vede k omezení dosahu. Dále reaguje interferometr nejen na okenní vibrace, ale i na vibrace zdroje laserového záření a samotného

interferometru. Proto se u profesionálních přístrojů dává přednost přímé reflexi podle Graham Bellova fotofonního principu. Nezávisle na funkčním principu je nutný v každém případě zdroj laserova paprsku. Kvůli jednoduchosti se používá v této aplikaci heliovo-neonový laser typu ETS 4200 firmy Heathkit (při našem vývoji požíváme jiný). Podobné lasery mohou být cenově výhodně obstarány u firmy ELV. Výchozí výkon obsahuje asi 0,9 mW. Ve vzdálenosti 70 m promítá laser světelnou skvrnu 35 mm průměru na cílový objekt. Také při nepatrném paprskovém výkonu 0,9 mW by se neměl paprsek dostat do oka. Toto platí také pro provozování reflektujícího paprsku prostřednictvím zaměřovače, nebo dalekohledu. Jen když paprsek nastoupí na reflektující plochu, např.bílý list papíru, může být provozován bez nebezpečí.

Obr. 8 Laserový mikrofon

Obr. 9 Příklad použití laserového odposlechu

4.9 Maskovaný vysílač MUD – Pero

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

Obr. 10 Maskovaný vysílač MUD v kuličkovém peru

4.10 CXL - Směrový mikrofon

Souprava velmi citlivého mikrofonu s úzce směrovou charakteristikou určená pro bodové snímaní zvuku z nepřístupních míst na větší vzdálenosti.

Základem soupravy je směrový mikrofon typu "long gun" (dlouhá puška). Použitím technologie zvukových vlnovodů a zejména celkovou precizností výroby je dosaženo vysoce směrového účinku a výtečné citlivosti při současné zachování velmi nízkého vlastního šumu. Mikrofon se vyznačuje velmi vyrovnanou frekvenční charakteristikou v širokém pásmu akustických kmitočtů 40Hz až 20kHz.

Phantomové napájení je realizováno přídavným modulem s basovým filtrem zasunutým do konce těla mikrofonu, který je napájen z jednoho článku R6. Výstup z mikrofonu se připojuje k nízkošumovému předzesilovači se speciálně navrženými kmitočtovými korekcemi. Ty selektivně zdůrazňují některá frekvenční pásma a jiná potlačují, čímž je směrový účinek mikrofonu dále umocněn. Na výstup zesilovače lze připojit sluchátka, nebo jiné záznamové zařízení.[10]

5 PŘÍKLADY POUŽITÍ SPECIÁLNÍCH ZAŘÍZENÍ

5.1 Ochrana proti snímání informací z oken nebo zdí chráněného objektu

Generátor bílého šumu je prostředek, který generuje bílý (v některých případech růžový) šum. Šumová ochrana proti odposlechu spočívá v přímém mechanickém zašumění míst pomocí piezoelektrických nebo elektrodynamických měničů, kde lze zvuky snímat (zdi, okna) nebo zašumění částí nábytku kde lze operativní prostředky skrytě umístit. Jako doplněk tohoto přístroje se může instalovat souprava reproduktorů, která dokáže překrýt nahrávku pořizovanou na diktafony. Bílý šum prochází všemi frekvencemi lidské řeči a vzhledem ke skutečnosti, že zvuk je mechanické vlnění se do užitečného signálu „přimíchá“ a nelze jej v současné době dostupnými prostředky odstranit. Jedná se o efektivní zařízení, které dokáže velmi spolehlivě zabránit provádění odposlechu pomocí stetoskopických mikrofonů, laserových mikrofonů a při použití reproduktorů i nahrávání informací na diktafony. Za nevýhodu můžeme považovat to, že bílý šum je ve slyšitelném spektru a tudíž šumový generátor působí jako novodobá náhrada tekoucích vodovodů. Při ochraně zdí chráněných prostorů je nutné počítat i se stavebními úpravami, proto je nutné na tento druh ochrany pamatovat již při výstavbě nebo rekonstrukci.[16]

5.2 Jammer zabudovaný v kufříku

Přenosný jammer zabudovaný do diplomatického kufříku. Slouží k zarušení radiové komunikace ve svém nejbližším okolí. Je vhodný k rušení provozu mobilních telefonů na sítích NMT-450 a GSM, k rušení radiových odposlechových prostředků, radiostanic a jiných komunikačních zařízení. Jammer je vybaven vlastními akumulátory, které zaručují provoz na cca 4 hodiny plného výkonu. Akumulátory lze dobíjet přes konektor vyvedený na plášť kufříku. Zapínání a vypínání rušení se provádí vypínačem umístěným pod jeho držadlem. Vyzářené spektrum je rozděleno do 5 pásem, která se dají jednotlivě zapínat nebo vypínat páčkovými přepínači uvnitř kufříku. Pásma se navzájem překrývají tak, aby při všech zapnutých generátorech nezůstala žádná nezarušená frekvence. Uvnitř kufříku je též signalizace stavu akumulátorů.

Obr. 11 Jammer umístěný v diplomatickém kufříku

5.3 Paměťový radiový analyzátor MRA-3

MRA-3 je speciální skanovací přijímač určený k nepřetržité chraně prostoru a k okamžitému zjištění radiového dposlechu. Ultra-rychlý vyhodnocovací systém odhalí do místnosti vnesený nebo dálkově aktivovaný odposlech i v podmínkách silného vysokofrekvenčního pole místních rozhlasových a televizních vysílačů.

Především bankéři, makléři, významní podnikatelé a další, jež únik informací může poškodit, by si měli uvědomit, že prostorová radiová štěnice je nejsnazší, nejlevnější, právně obtížně prokazatelnou a tudíž nejpoužívanější formou odposlechu.

MRA 3 umožňuje odhalení přítomnosti nového signálu během 6 sekund a uživatel je na přítomnost podezřelého signálu okamžitě upozorněn. K omezení falešných poplachů je MRA 3 vybaven tříúrovňovým poplachovým hlášením předpoplach - poplach - minulý poplach. Díky malým rozměrům a zcela kompaktnímu provedení přístroje, který obsahuje vestavěnou teleskopickou anténu a vnitřní baterii, lze MRA 3 snadnou umístit jak na nábytku kanceláře tak i skrytě. Pro skryté použití je z přístroje vyveden signál alarm umožňující připojení externí LED, která upozorňuje uživatele na ohrožení rádiovým odposlechem. Ochrana prostoru, jež je hlavní funkcí MRA-3, je z hlediska obsluhy zjednodušena na dvoutlačítkové ovládání usnadněné přehlednou informací na displeji přístroje. Použití dalších ovládacích prvků umožňuje specialistovi provést velmi rychlé operativní prověření celého kmitočtového spektra a bezkonkurenčně rychlé odhalení aktivních rádiových štěnic.[18]

Obr. 12 Paměťový radiový analyzátor MRA-3

Cílem vývoje zcela unikátního přístroje MRA-3 bylo uvést na trh dosud chybějící účinný automatický detekční a ochranný systém schopný ochránit kancelář proti rádiovému odposlechu i v nejtěžších podmínkách rádiového rušení. Zároveň bylo snahou maximálně respektovat požadavek jednoduché obsluhy snadno zvládnutelné i osobou bez jakéhokoliv technického vzdělání.

Běžně používané širokopásmové detektory sice mají relativně jednoduchou obsluhu, ale stále se zvyšující úroveň rádiového pozadí od TV a FM vysílačů, mobilních komunikací, GSM, datových přenosů atd. znemožňuje jejich praktické využití k jakékoliv permanentní ochraně. Tyto jsou pak degradovány pouze na vyhledávání odposlechu postupem bod po bodu s tím, že rozlišení směsi signálů se vzhledem k novým komunikačním systémům stává problémem i pro specialistu.

Další kategorií jsou velmi nákladné speciální přístroje vyžadující propojení více komponentů, aplikaci složitého softwaru i hardwaru se značným množstvím ovládacích prvků mnohdy zaplňující více než jeden speciální detekční kufr. Takové přístroje sice bývají univerzálně použitelné, ale jejich vlastnosti dokáže využít pouze specialista. Navíc je jejich permanentní instalace pro ochranu např. VIP kanceláře prakticky nemožná.

Technický kompromis mezi výše uvedenými jednoduchými a komplikovanými přístroji je prakticky nemožný a proto byl vyvinut zcela nový kompaktní ultra-rychlý skanovací systém MRA zaměřený zejména na trvalou ochranu VIP kanceláří. Hlavní funkcí tohoto systému je okamžitě zareagovat na přítomnost nového signálu způsobeného aktivací rádiového odposlechu v monitorovaném spektru a to i za předpokladu, že tento

nový signál je podstatně slabší než signály rádiového pozadí. Nejnovější z úspěšné řady přístrojů MRA - MRA 3 je špičkový přístroj vycházející z výše uvedené koncepce k jehož vývoji významně přispěly i připomínky a zkušenosti mnohých ze stovek uživatelů starších přístrojů řady MRA.[18]

5.4 Optické systémy – minikamery, kamery a systémy

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

Mini kamery s čipem CCD: Současně používané malé kamery, od průmyslových po policejní a špionážní jsou osazeny výhradně CCD čipy a tím i odpovídajícími vlastnostmi. Kamery jsou malé, s dobrou rozlišovací schopností, pevným objektivem, velkou citlivostí a zpravidla s automatickou clonou. Kvalitnější typy jsou vybaveny možností výměny objektivu. Kamery jsou velikosti krabičky zápalek nebo dokonce kostky cukru a mohou se zabudovat do různých předmětů, jejich použití není vázáno na otvory ve zdi. Na objektiv běžně používaných kamer stačí velikost otvoru asi 5 mm, u dírkových objektivů asi 1 mm. Kamery je možno zabudovat do nábytku, televizoru, radiopřijímače, obrazů, různých plastik a ozdobných předmětů, hodin, knih a hraček. Vhodným místem pro skrytou kameru jsou osvětlovací tělesa, požární a zabezpečovací čidla, krabice telefonních rozvodů a rozvodů 230 V. Kamery se mohou ukrýt do umělých květin, telefonů, faxů a počítačů. Pro ukrytí kamery je limitujícím faktorem velikost přístroje a velikost otvoru objektivu. Zmenšení objektivu se provádí použitím jehlových objektivů, optickou soustavou, která zmenšuje vstupní otvor objektivu na velikost asi čtyř milimetrů. Jehlový objektiv má pevnou délku, od 10 cm do 50 cm, světelnost objektivu je asi 1,8 úhel záběru je od 40 do

80 stupňů. Jehlové objektivy mohou být zabudovány přímo v tělese kamery, (což je výhodnější) nebo mohou být jako vnější přídavné zařízení. Nevýhodou je však poněkud větší energetická náročnost než je u vysílačů pouze na zvuk. Proto lze očekávat, že videoštěnice bude nainstalována v nějakém elektrickém spotřebiči trvale připojeném v síti. Další možností prodloužení objektivu je použití světlovodného kabelu. Kabely mohou být pevné, nebo pružné, dají se prostrčit jakýmkoliv otvorem ve zdi, jsou ohebné bez ztráty kvality, mají nižší světelnost (asi 4). I u světlovodných kabelů platí, že pro speciální aplikace je možno do jedné trubice zabudovat optický i akustický systém. [16]

5.4.1 Barevná bezdrátová kamera se zvukem

Skryté kamery vám umožní sledovat veškeré dění, u kterého zrovna nemůžete být. Zde naleznete nabídku několika nejběžněji používaných systémů, které vám pomohou získat cenné informace nebo ochránit váš majetek.

Obr. 13 Barevná bezdrátová kamera se zvukem

Miniaturní barevná kamera s integrovaným vysílačem a mikrofonem umožňuje monitorovat zájmový prostor až na vzdálenost 30m v bytové zástavbě. Ideální na hlídání kanceláří, recepcí, čekáren, menších provozoven, atd. Kamera je vybavena mikroobjektivem o průměru 2 mm, lze ji tedy schovat prakticky kamkoliv. Výstup z přijímače lze jednoduše připojit k běžnému televizoru, videorekordéru, počítači nebo notebooku.

Kamera je vybavena obvodem pro řízení stability vysílací frekvence. Dodávaný přijímač podporuje čtyři vysílací kanály, které jsou pevně nastaveny, a jejich volba je

prováděna pomocí přepínače. Není tedy nutné provádět manuální doladění, jako tomu bylo u starších frekvenčně nestabilních modelů. [10]

Technické parametry:

- Barevná CCD kamera 380 TV řádků, 4 lux
- Objektiv: 90°
- Vysílací výkon: 200 mW
- Vysílací frekvence: 2,4 GHz
- Napájení kamery: 9V baterie nebo 9V síťový zdroj
- Napájení přijímače: 12V síťový zdroj

Upozorňuji, že kamera je primárně určená k monitorování obrazu. Zvuk zachycený a přenášený vestavěným mikrofonem může být, vzhledem k absenci zesilovače, značně zkreslený.

5.4.2 Maskovaná minikamera

Kamera barevná miniaturní v provedení „knoflík“ (na obrázku v porovnání s tužkovou baterií) objektiv je dírkový ve středu knoflíčku, mikročip CMOS, citlivost 3 luxy, úhel záběru 90º diagonálně, napájení 7-12 V.

Obr. 14 Barevná maskovaná minikamera

5.4.3 Desková kamera VCM 36

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

Obr. 15 Desková kamera VCM 36

5.4.4 Kamerový bezpečnostní nahrávací systém

Kamerový bezpečnostní nahrávací systém Vám umožní připojení až 16 kamer s možností současně zobrazovat i nahrávat jejich signál na PC. Pokročilá technologie detekce pohybu umožňuje zaznamenávat pouze objekty, jež jsou v pohybu, což šetří čas a náklady na souvislé nahrávání, které nabízejí tradiční bezpečnostní systémy. Jedná se o uživatelsky velmi příjemný a komfortní systém s řadou výhod proti analogovému nahrávání. Ke každé kameře lze nahrávat i zvuky z monitorovaného prostoru.

Systém naprosto spolehlivě pracuje v jakémkoliv prostředí, je využíván i pro dálkovou správu objektu a jeho kontrolu pomocí vzdáleného připojení, kdy uživatel může z jednoho místa kontrolovat více pracovišť na různých místech.

Kamerový systém může pracovat s různými typy kamer - lez použít skryté, kamuflované, i běžné kamery, každá kamera může být doplněna i citlivým mikrofonem.

Obr. 16 Přehledový obraz všech kamer

Tento kamerový počítačový bezpečnostní systém vítězí především díky velmi vysokému rozlišením bodů, vysokou kvalitou a špičkovou kompresí záznamu. Rychlost záznamu lze nastavit pro každou kameru (platí i při max. 16-ti kamerovou verzi). Systém je špičkově zpracován pro provoz na sítích LAN,WAN,INTERNET pracujících na TCP/IP protokolu. Přenos systému na těchto sítích dosahuje rychlostí až 10 snímků/sec na kameru zobrazovaných na klientské stanici při zachování vysoké kvality obrazu. Systém umožňuje nastavit několikanásobnou úroveň přístupových práv pro jednotlivé lokální a vzdálené uživatele. Systém umožňuje nahrávat záznam i se zvukem ve velmi vysoké kvalitě. Každá karta systému má 4x videovstupy a 2x audio vstupy (verze RT 4x audio). V max. verzi 16-ti kamerového systému, je tak umožněno nahrávat 8x zvukových kanálů (u verze RT 16x zvuk.kanálů). Lze kombinovat barevné a černobílé kamery. Systém lze kdykoliv rozšířit ze 4 kamerových vstupů na 8,12 nebo 16 vstupů pouhým dokoupením další karty, která se přidá do volného PCI slotu v PC. Systém podporuje ovládání SPEED DOME kamer a práci se vstupy a výstupy i po síti. Pro každý kamerový vstup lze nastavit zvlášť jeho parametry, druh záznamu, detekci pohybu v obraze s vlastní citlivostí, titulky, způsob pořizování záznamů: alarmově při pohybu nebo kontinuální záznam nebo kombinace obojího. Nově lze využívat alarmové vstupy a výstupy pomocí modulu I/O pro V-Guard XP a RT (8-32 vstupů a 8-32 výstupů). Systém pracuje pod operačními systémy Windows 2000 a XP (klient i pod Win98, Win98SE a Win ME) Lokalizace do českého jazyka je k dispozici. [10]

Obr. 17 Ukázka PC karet na připojení sledovacích kamer

6 POPIS ODPOSLECHU V MOBILNÍ SÍTI

6.1 Odposlech mobilních telefonů

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

Legální odposlechy realizuje Policie ČR v součinnosti s telekomunikačními operátory a pro jejich realizaci nepotřebuje vynaložit příliš velké úsilí, neboť operátoři jsou povinni poskytnout za tímto účelem policii přístup ke své síti. Problém nastává v případě těch, kteří se rozhodnou porušovat naše zákony a provádět odposlech mobilního telefonu v nesouladu s § 88 Trestního řádu, neboli odposlech nelegální. Možnost uplacení zaměstnance u mobilního operátora, který by prováděl na nelegální odposlechy stejným technickým postupem jako policie, je v podstatě vyloučena. Všichni zaměstnanci našich mobilních operátorů, kteří mají co do činění s aktivací odposlechů pro Policii ČR, mají za sebou bezpečnostní prověrky NBÚ. Všechna místa v mobilní síti, kde by šlo hovory odposlouchávat, jsou navíc pod neustálým přísným dohledem a je téměř na 100 % jisté, že pokud by se nějaký zaměstnanec pokusil o nelegální odposlech, byl by velmi rychle odhalen. [12]

V médiích se objevily obrovské titulky, které říkaly, že šifra A5.1, kterou používají mobilní sítě pro šifrování hovorů byla prolomena a že dešifrovací program je volně přístupný na internetu. Lidé z toho pak logicky odvozovali, že pokud někdo má dešifrovací program na A5.1, tak může kdykoliv kohokoliv odposlouchávat. Skutečnost je však odlišná. Je pravda, že existuje program na dešifrování A5.1, který je dokonce volně přístupný na Internetu. Pokud by tedy měl zájemce o odposlech vyhovující hardware, pak by skutečně byl schopen v relativně krátkém čase nějaký ten hovor dešifrovat. Problém je však v tom, jak onen hovor nalézt. [13]

Komunikace mobilního telefonu (MS) se základ-novou stanicí (BTS) v síti GSM probíhá na dvou frekvencích (přesněji kanálech): jedné pro příjem a druhé pro vysílání hovoru. Každá z těchto frekvencí je však rozdělena v čase na časové úseky o délce 0,577 ms (TDMA frame). Každý TDMA frame se skládá z 8 timeslotů, neboli časových rámců, kdy telefon vysílá. Tyto rámce jsou očíslovány od 0 do 7. Jeden timeslot je dlouhý cca 0,072 ms. Každý volající telefon má přidělen právě jeden timeslot. Mobilní telefony se ve

vysílání na dané frekvenci pravidelně střídají v pořadí podle čísla timeslotu, který jim byl přidělen. Díky této technologii nazývané TDMA je možné, aby jednu frekvenci využívalo několik telefonů najednou.Ve skutečnosti tedy, i když si myslíte, že slyšíte hovor naprosto plynule a spojitě, tak z něj slyšíte vždy jen jeho osminu - díky nedokonalosti lidské-ho sluchu to nevadí. Z hlediska odposlouchávání hovoru to ovšem znamená, že se musí monitorovat dvě frekvence, na kterých se může nacházet klidně i osm hovorů; ty je nutné dešifrovat samostatně a následně je sestavit dohromady.To vše by bylo poměrně jednoduché, kdyby neexistovala technologie frekvenčních skoků (frequency hopping), která, zjednodušeně řečeno, slouží ke zlepšení kvality hovoru (respektive omezení možného rušení určitých frekvencí). Díky této technologii, kterou používají všichni naši operátoři, vysílá mobilní telefon pokaždé na jiné frekvenci, která se mění každých 0,577 ms podle jednoho ze 64 možných, pevně stanovených schémat.Ve skutečnosti by tedy kvůli odposlechu jednoho mobilního telefonu z komunikace mezi MS a BTS bylo nutné odposlouchávat všechny frekvence BTS najednou, odhalit číslo tzv. hoppovacího schématu každého z probíhajících hovorů, dešifrovat veškerý zachycený provoz, poskládat jednotlivé hovory k sobě, a následně najít ten správný hovor. To vše navíc za předpokladu, že jsme někde poblíž odposlouchávané osoby a v případě jejího pohybu takto odposloucháváme hned několik BTS v okolí najednou. Takovýto odposlech by byl velmi časově a finančně náročný, ale navíc by vyžadoval neustálé sledování odposlouchávané osoby. Odposlech na tomto principu by byl však mnohem snazší v případě, že bychom vlastnili identickou kopii odposlouchávané SIM karty. Pak by jen stačilo se pohybovat v okolí odposlouchávané osoby a s patřičným vybavením "poslouchat" komunikaci mezi MS a BTS. Na rozdíl od předchozího případu bychom totiž měli k dispozici dešifrovací klíč přímo a věděli bychom také přesně, na jakých frekvencích máme hovor hledat. [12]

Mnohem snazší a reálnější je odposlech v další části mobilní sítě, tedy mezi BTS a řadičem základnových stanic (BSC - spravuje vždy několik BTS najednou) či mezi BSC a "mobilní telefonní ústřednou" (MSC - je k ní připojeno několik BSC a případně i další MSC). Mezi těmito prvky sítě totiž probíhá komunikace prostřednictvím bezdrátových či optických spojů, a to naprosto nešifrovaně. V okamžiku, kdy zjistíme, kudy daný spoj prochází, není v případě bezdrátového spoje příliš těžké se do něj napojit. Problém je v tom, že v takovém spoji probíhají desítky (u BTS - BSC) až stovky (u BSC - MSC) hovorů najednou navíc obohacených o řadu dalších informací, které si tyto prvky mobilní sítě mezi sebou vyměňují. Je tedy velmi náročné v takovéto změti dat identifikovat právě

hovor, který hledáte. Výhoda je však v tom, že již není třeba přímo v okolí odposlouchávané osoby. Při odposlechu komunikace mezi BSC a MSC by stačilo být ve stejném okrese jako odposlouchávaná osoba (s tím, že bychom pak daný hovor museli umět "najít"). Menší problém je ovšem v tom, že pokud by odposlouchávaná osoba volala někomu ze stejné mobilní sítě, kdo by byl ve stejném okrese, pak by hovor přes spoj BSC - MSC vůbec neprocházel, neboť by jej spojilo přímo BSC samo. A co že z toho všeho vyplývá? Nelegální odposlech mobilních telefonů je technicky a finančně velmi náročná věc (pokud není "štěnice" přímo v telefonu). I když lze mobilní telefony odposlouchávat, tak v žádném případě není reálná představa, že lze odkudkoliv odposlouchávat kohokoliv. Téměř vždy se musí odposlouchávající nacházet ve větší či menší blízkosti odposlouchávaného.[12]

GSM Interceptor – Je jednokanálová souprava pro odposlech jednoho mobilního telefonu GSM. Pracuje s jakýmkoli typem kódování, vč. A5.1 a A5.2. Nepotřebuje žádnou podporu ze strany operátora sítě. Zařízení je mobilní a je zabudované do kufříku. Telefon je identifikován podle IMSI, TMSI, IMEI, Classmark, MSISDN. Při první relaci si uloží všechny údaje o monitorovaném telefonu a pokud se některý z těchto identifikačních prvků objeví v relaci, začne monitorovat. Proto systému nevadí ani změna SIM karty. Hovor je nahráván na HDD řídicího laptopu.Vytváří seznam volaných čísel a volajících (pokud jsou přístupná). [14]

6.2 Obrana proti odposlechu mobilních telefonů

Odposlechové zařízení v mobilní síti se musí formálně jevit jako běžná základnová stanice BTS, aby se minimalizovala možnost identifikace a lokalizace. Pak nemá uživatel velkou šanci zjistit, že kromě normální sítě mobilního operátora, zpracovává jeho hovory i falešná BTS. Zdá se, že jedinou stoprocentně bezpečnou cestou pro utajení obsahu hovoru je tzv. kryptoGSM-telefon se zabudovaným interním šifrovacím mechanizmem nezávislým na architektuře a konfiguraci mobilní sítě, v níž stanice pracuje. Někteří výrobci mobilních telefonů proto nabízejí nové modely s vysokým stupněm ochrany, s implementovaným digitálním kódováním, možností ověření pravosti uživatele během šifrované korespondence a s kontrolou přístupu. Nevýhodou uvedeného principu je fakt, že i přijímací strana musí být vybavena zařízením pro příjem digitálně kryptovaných signálů, ať už to je mobilní telefon, terminál PSTN/ISDN v pevné síti, terminál v satelitní síti atd.

Vývoj a výroba mobilních krypto-telefonů vyžaduje kromě nejmodernějších technologií a investičních prostředků i spolupráci řady specializovaných firem. Příkladem může být model MW 3026S určený pro síť GSM (900 MHz) i DCS (1800 MHz) vyvinutý francouzskou firmou Sagem ve spolupráci se švýcarskou softwarovou společností Crypto AG. Jako každý mobilní telefon komunikuje ve standardním módu (v režimu hlasové služby) a dovoluje také prostřednictvím kryptovacího modulu používat šifrovací technologii pro kódovaný provoz (v rámci aktivace datových služeb v asynchronním transparentním módu s přenosovými rychlostmi 4800 nebo 9600 b/s pro vyhrazená čísla). Hlasový signál je digitalizován, zašifrován, přenesen jako data, přijat a dešifrován v přijímacím modulu volaného telefonu. [11]

7 E-LEARNING

Celoživotní vzdělávání je již nějaký čas nezbytným předpokladem pro "přežití" v dnešním světě, v němž je informace hybnou silou všeho. Pro firmy je stejně důležité vzdělávání zaměstnanců, partnerů a samozřejmě - v přeneseném slova smyslu - také zákazníků. Jak ale tyto potřeby naplnit v době, která je zároveň hyperaktivní a množství volného času se stále citelněji zmenšuje? Jednou z možností je e-learning. E-learningem přitom rozumíme alternativní způsob vzdělávání, kdy procesy výuky a učení probíhají prostřednictvím elektronických prostředků. Přidáme-li ještě definici ryze technologickou, tak e-learning znamená počítačové výukové programy (CBT, resp. WBT) a výukové řídicí systémy (LMS) včetně komunikačních nástrojů. Stojí za povšimnutí, že tyto definice nezdůrazňují Internet. V e-learningu nemusí totiž hrát rozhodující roli. Výuku mohou zajišťovat i CBT programy, distribuované např. na CDROM. Systém může být i bez komunikace mezi účastníky, mnohdy ani k tomu není důvod. Nicméně již téměř implicitně vidíme v e-learningu výuku prostřednictvím Internetu, v podnikovém pojetí pak v rámci intranetu. Včetně komunikace uvnitř systému (žák-žák či žák-učitel).

7.1 Technologie e-learnigu

E-learning můžeme implementovat ve variantách

• klasické CBT programy, instalované na jednotlivých PC či v lokální síti počítačové učebny. Takový přístup není náročný na provoz, potřebujeme multimediální PC. Výuka obvykle probíhá v run-time prostředí vývojových systémů, či v prostředí internetovských prohlížečů.

• programy WBT používáme prostřednictvím Internetu, na podnikové úrovni v prostředí podnikových intranetů. Potřebujeme opět multimediální PC, ale připojené na síť. Protože metodika a dnešní technologie umožňují aplikaci multimedií ve výuce, hraje zde velkou roli průchodnost sítě. Problémy jsou viditelné, chceme-li absolvovat kursy WBT některého poskytovatele výuky prostřednictvím Internetu a naše PC je připojeno pomoci modemu. To dnes určitě nemá smysl. Kvalita technologií nesmí ovlivňovat kvalitu výuky.

Doporučuje se vždy vyzkoušení funkčnosti výukových programů na provozovaných technologiích. Nespokojit se pouze s doporučeními prodejce.

Uživatele systémů ERP je třeba upozornit na trend producentů, kteří začleňují řešení e-learningu jako jeden z modulů svých systémů. A to ať vlastním řešením nebo častěji akvizicí produktů LMS a počítačové výuky. Viz např. SAP a Siebel. Rovněž velcí podnikoví konzultanti z Big Five se spojují s producenty LMS či vyvíjejí vlastní e-learningová řešení.

7.2 Proč používat E-learnig?

Podle Jay Crosse (Internet Time Group) je e-learning cílovým modelem podnikového vzdělávání a klíčovým faktorem přežití organizací. Z tohoto pohledu lze také chápat tvrzení Clarka Aldriche z Gartner Group, že výuka nepřechází na on-line formy, protože tak bude lepší, ale proto, že bude levnější a měřitelnější.

Současně Saul Carliner (Bentley College) připomíná, že e-learning není o technologii, ale o výuce a učení. To chceme v dnešním období technologizace procesů zdůraznit. Autor článku vidí hlavní důvod zavedení e-learningu ve zvýšení efektivnosti učení a výuky. Máme zde na mysli fakt, že učením v pojetí e-learningu se zvětší množství a kvalita osvojených vědomostí a dovedností. Uvedené očekávání vychází z předpokladu vysoké didaktické kvality výukových programů, což znamená, že výukový program je zpracován za účasti špičkových specialistů jak co do obsahu, tak co se týče didaktických metod. To rovněž znamená, že při vývoji je důsledně použita praxí ověřená metodika návrhu výuky, např. ISD neboli ADDIE, opírající se o některou psychologickou teorii učení. Jen tehdy získáme záruku, že výukový program učí, a že se nejedná pouze o propojené texty či pohyblivé obrázky.

Pokusme se odpovědět na tuto otázku porovnáním. Porovnáním klasického způsobu výuky a výuky v prostředí e-learningu. Porovnání provedeme se zaměřením na vzdělávání v organizaci, nicméně mnohé bude platné i pro školství či komerční poskytovatele výuky.

Nejprve stanovíme srovnávací kriteria. Vyjdeme přitom z pohledu na užitečnost e-learningu.

7.3 Srovnávací kritéria

1) **Kvalita obsahu výuky** (budeme jí rozumět úroveň obsahu z hlediska odborného,expertního)

2) **Didaktická kvalita výuky** (efektivnost způsobů výuky jak učí učitel / program)
3) **Rychlost zavedení nového tématu** (rozumíme tím rychlost nasazení nového kurzu; rychlost návrhu kursu je stejná pro oba způsoby dodání; vývoj kursu je v e learnigovém prostředí několikanásobně delší)
4) **Rychlost přístupu k informacím a jejich rozsah** (použijeme srovnání s klasickou knihovnou, kde jsou rozdíly velmi zřetelné)
5) **Zpětnovazební mechanismy** (využívání zpětné vazby při řízení výuky)
6) **Individuální přístup** (práce učitele s jednotlivými účastníky)
7) **Diference** (výuka podle vstupních znalostí a schopností účastníků)
8) **Názornost výuky** (využívání pomůcek, ukázek, zobrazení)
9) **Vyhovění stylům učení** (vizuální, poslechový, kinestetický)
10) **Spolupráce** (kolaborativnost, práce v týmu, ve skupině)
11) **Sdílení času a prostoru** (nutnost být ve stejné učebně ve stejný čas, cestování za zdroji výuky)
12) **Možnost automatizovaného zpracování informací** (automatizované zpracování statistik a zpráv o stavu a výsledcích výuky)
13) **Náklady** (náklady na vývoj, přípravu, nasazení)

Podle uvedených kriterií provedeme dále srovnání obou způsobů výuky. E-learningem přitom budeme v tomto pojednání rozumět výuku pomocí elektronických prostředků v síti. Klasickou výukou máme na mysli výuku ve třídě s učitelem.

Kritérium	Klasická metoda	Metoda e-learingu
1.	Odborná stránka je specifikována osnovami, učebnicemi. Výuka však probíhá prostřednictvím učitele a jím je ovlivněna i odborná úroveň.	Témata mohou být zpracována a odborně garantována uznávanými experty jednotlivých oborů.
2.	Proces, silně ovlivněný kvalitou učitele. Rozdílná úroveň je patrná zejména u školitelů bez pedagogického vzdělání, kdy výuka je často nahrazována presentací.	I zde je proces výuky silně ovlivněn přístupy návrháře. Nicméně proces výuky lze algoritmizovat a tím těsně a důsledně adaptovat na zvolenou teorii učení.
3.	V klasické výuce je však nižší rychlost zavedení či nasazení kursu, která se odvíjí zejména od přípravy učitelů.	Kurs je možné nasadit po celé organizaci prakticky okamžitě.
4.	Omezený rozsah; rychlost ovlivněna obvykle slabou obsluhou; vyhledávání pouze jmenné a předmětové, a obvykle ruční.	Na jedné straně jsou dostupné ohromné celosvětové zdroje, na straně druhé existují efektivní vyhledávací mechanismy. Informační zdroje jsou prakticky nevyčerpatelné.
5.	Pokud je zpětná vazba vyžívána, pak maximálně na úrovni třídy. Navíc její frekvence je ve většině případů nedostatečná.	Zpětná vazba je nedílnou součástí výukových programů. Její výsledky lze vyžívat k řízení výuky na individuální úrovni. Frekvence jejího využívání je možná tak, aby docházelo k potřebnému počtu zpevnění získaných znalostí a dovedností.
6.	Individuální přístup je snem většiny učitelů. Je však limitován	Zdá se být paradoxem, ale e-learning poskytuje mnohem více prostoru pro

	standardní velikostí třídy co se týče počtu žáků a nutnými interferencemi.	individuální přístup. E-tutor (pokud existuje) může se studentem komunikovat mnohem více a mnohem záměrněji než v klasické výuce.
7.	Diferenciovaný přístup jde ruku v ruce s přístupem individuálním. V klasické třídě je jen obtížně použitelný.	Adaptivní výukové programy jsou skutečnou cestou k využívání schopností jednotlivců. Již větvený program umožňuje vyžívat zpětnou vazbu k diferenciované výuce.
8.	Zásada názornosti je vyžívána podle toho, jaké existují pomůcky, modely. Můžeme však již rovněž využívat multimedia PC.	Multimediální PC je ideální prostředek názorného vyučování. Se svými nástroji pro zpracování a zobrazení textu, grafiky, zvuku a videa umožňuje jak znázornění reálného světa, tak jeho modelování.
9.	Využívání stylů učení k jeho větší efektivitě není ve svém komplexu možné, výuka se v zásadě zaměřuje na jeden z nich.	Možnosti spojení multimediálních prvků se styly učení přináší vyšší efektivitu procesu učení. Každý žák si tak může najít způsob výuky podle svého preferovaného stylu učení.
10.	Skupinové vyučování je klasická metoda, přinášející efekt i přípravu na práci. Výuka směřuje ke spolupráci, nutnosti komunikovat student versus pedagog.	Teleworking, každodenní potřeba komunikace. To vše e-learning podporuje. Vychází to vstříc současnému životnímu a mnohdy i pracovnímu stylu.
11.	V klasické výuce je nutná vazba na čas a místo. Přináší to velké plus v sociálních metodách učení. Lze možná dodat – ne vždy. Ale určitě je sociální kontakt velmi	Umožnění asynchronního přístupu ve výuce se mnohdy udává jako jeden z největších přínosů e-learningu. Vypočítávají se úspory za cestovné, ubytování, noclehy. Není třeba opouštět

	důležitý.	pracoviště. I když my vidíme přínosy e-learningu jinde, jak je patrno z uspořádaní srovnávacích kriterií, je pravdou, že zejména v pobočkově organizovaných podnicích jsou ušetřené částky významné.
12.	Sběr známek, poznámek, pochval, trestů atd. je nejen postrachem, ale i přehlídkou ztracených informací. Obvykle jsou časově omezené a dále nezpracovávané a tím nevyužívané.	Informace o průchodech programy, způsobech odpovídání, výsledcích testů informují nejen o progresu studentů, ale i o slabých místech programů. Tak je můžeme korigovat. To vše provádí programy, tzv. výukové řídicí systémy (LMS – Learning Management Systems)
13.	Náklady na vývoj se odhadují cca 5 - 10x nižší než u počítačové výuky. Náklady na realizaci kursu však rostou multiplikativně.	Náklady je třeba zvážit postupem ROI (Return of Investment). Vstupní náklady na vývoj kursu jsou vysoké. Přímých úspor dosahujeme vícenásobným používáním, snížením nákladů na organizaci školení, snížením nákladů na cestování pracovníků. Přínosů pak dosahujeme kvalitou a rychlostí.

E-learning je systém, který zajistí vše od sdělení informace, přes její správné pochopení a uvedení do souvislostí, až po otestování toho, jak účinné předání informace bylo. V rámci testů a dalších forem zkoušení tak systém nejen zařadí posluchače na vhodnou úroveň, ale vyloučí i ty znalosti a informace, které již zná z výuky.

ZÁVĚR

Speciální a odposlouchávací technika prochází neustálým vývojem a je stále rafinovanější. Vědci přišli na způsob, jak ukrýt zprávy mezi molekuly DNA. Dalším zařízením na zjišťování důležitých informací jsou satelity, které krouží nad celou naší zemí. Moderní satelit umí díky infračerveným paprskům zjistit teplotní rozdíly s přesností na desetiny stupě. Tudíž pro něho není problém zjistit, kde před hodinou tábořil vojenský tábor, nebo zda jsou sledované automobily v pohybu. Dálkově ovládaná minikamera černá vdova, pojmenovaná po jedovatém americkém pavoukovi, nejmenším, nejlehčím, víceúčelovým, plně proporčním řídicím systémem na světě. Ten při třech gramech hmotnosti zabírá plochu jen 6,5 čtverečných centimetrů. Kamera, která i z výšky několika set metrů poskytuje křišťálově čistý barevný obraz přenášený do vzdálenosti až dvou kilometrů, má hmotnost dvou gramů. Miniaturní ornitoptéra by mohla diskrétně vlétnout do objektu, zaparkovat někde v rohu místnosti a v přímém přenosu pak vojákům zprostředkovávat například velitelskou poradu protivníka.

Obrovské možnosti pro špiony z celého světa dnes nabízí internet. Již dnes se hackeři a počítačový piráti nabourávají do počítačových síti firem zpracovávajících citlivé informace jako jsou například banky, vojenské instituce, vláda apod. Drobná odposlouchávací zařízení jsou dnes velmi dostupná, jsou miniaturní a nevyžadují umístění v bezprostřední blízkosti zařízení. Řada z nich má zabudovaný vysílač a dokáže hovor přenášet na vzdálenost až několika kilometrů. Nejmenší z nich se dají umístit do propisky nebo na kreditní kartu. Největší hrozbou dnešní špionáže se mohou zdát mobilní telefony. Stačí, abyste nastavili mobilní telefon tak, aby bez vyzvánění automaticky přijal hovor, zapomněli v kapse u saka, v kanceláři, a odejdete třeba na toaletu. Pak už jen stač vytočit číslo z jiného mobilního telefonu a můžete v klidu poslouchat, co si o vás povídají za vašimi zády. Ale taky můžeme pomocí mobilního telefonu lokalizovat hledané osoby.

Ve své práci jsem potvrdil názor, že odposlech a získávání důležitých informací není žádný velký technický problém a to jak pro soukromou detektivní kancelář, tak i pro obeznámeného laika. Vzhledem k jeho malé finanční náročnosti v porovnání s možnou cenou zcizených informací se stává i u nás velice účinným nástrojem nekalého konkurenčního boje. Každá firma by tedy měla zvážit možnosti ochrany svých důvěrných informací, protože investice do této ochrany mohou být jen minimálním zlomkem ceny odcizené informace.

ZÁVĚR V ANGLIČTINĚ

Special and other tapping devices are constantly being innovated and they continue to be fine-spun. Scientists have found a way, how to hide data in-between DNA molecules. Another device used for retrieving important information are satellites, which orbit around our planet. Modern satellites due to infrared rays, are able to find temperature differences with perfection of tenths of degrees. Hence for them it is not a problem to find out where a troop of soldiers was camped an hour ago, or if a monitored cars are in motion. A minicamera „black widow“ that is controlled by remote, received this name in association with the same named poisonous American spider, it is the smallest, lightest, multipurpose, full proportion control system in the world. At three grams weight, it covers an area of 6,5 square centimetres. The camera, that even from a distance of several hundred meters, can provide a crystal clear colourful picture, transmitted to a distance of up to two kilometres, it has a weight of two grams. Miniature ornithopter could discreetly fly up to an object, park somewhere in the corner of a room and send a live transmission to troops and transmit for example a commanders conference of the opponents.

The internet offers large possibilities for spying from around the world. Today hackers and computer pirates hack into companies systems, who process sensitive information for instance banks, military institutes, governments etc. Small tapping devices today are very available, they are small and they do not need to be situated in direct contact with the equipment. Many of them have an integrated transmitter, and they are able to transmit up to a distance of several kilometres. The smallest ones can be integrated into pens or on credit cards. The greatest danger today is the tapping of mobile phones. All that needs to be done is to set the mobile phone to automatically answer all incoming calls without the phone ringing, and to leave the phone (foe example) in the pocket of your coat in the office, and leave the room. All that has to be done is call the phone left in the office from another phone and you can listen to what other people in the office are discussing. We can also use mobile phones to help locate missing or fugitive persons.

In my work, I have confirmed the opinion, that tapping and acquiring important information is not a large technical problem for private detectives or even for ordinary people who have little information. In respect of its small financial demand, in comparison with the possible cost of alienation of information, this is even in our country, has become a very effective instrument of mischievous competitive contest. Every company should carefully consider the possibilities of safeguarding their confidential information, because investments into this protection can be the fraction of the cost that can be cost of the loss of information.

SEZNAM POUŽITÉ LITERATURY

[1] Šámal, K., Král, V., Baxa, J., Púry, F., Trestní řád – komentář, I. Díl, C.H.Beck, 2001,

[2] Souček, J., Škrabalová, A., Odposlech a záznam telekomunikačního provozu z pohledu de lege lata i de lege ferenda, Trestní právo, 4/2002,

[3] Internet_a_svoboda_projevu___kauza.rtf , IT Law, IT právo, JUDr. Ján Matejka

[4]Použití speciálních bezpečnostních prostředků v praxi podniků komerční bezpečnosti,prostředky speciální, odposlechové techniky a jejich odhalování a obrana proti nim, Marián Sehnálek, Bakalářská práce 2007

[5] Zákon č. 13/1993 Sb., Celní zákon

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

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

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

[9] § 88 trestního řádu

[10] Security Systems Odposlechy.com, Elektronické systémy. [online],

http://www.odposlechy.com/

[11] www.probin.cz

[12] Portal-x.cz, Špionážní technika. [online],

http://www.portal-x.cz/odposlechy/aktuality

[13] 21. století, Nesnesitelná lehkost špionáž, [online],

http://www.21stoleti.cz/

[14] SPY VPH, Speciální technika a služby, [online],

http://spy.vph.cz/

[15] Bezpečnostní agentura BESO s.r.o. Zlín,

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

http://www.safecom.cz/

[17] Detekce odposlechů, rušičky signálu http://www.detekce.com

[18] ELBI Electronics, Výrobce přístrojů proti odposlechu

http://www.elbi.cz

[19] Ivanka, J.: Technické prostředky bezpečnosti a elektromagnetická kompatibilita. In. Řešení krizových situací v specifickém prostředí. EDIS – Žilinská univerzita,Žilina, 2004, str.77-82, ISBN 80-8070-272-1

[20] Čandík, M., Ivanka, J. : Některé aspekty bezpečnosti multimediálních dat,In: Security magazin, roč.X, vyd.č.53, 3/2003, vyd. Familymedia, Praha, 2003, str.36-38, ISSN 1210-8723.

[21] Nováková Hana, Význam a využití mikroprocesorů jako prvků pro el. Ochranu osobních motorových vozidel, 2006

[22] Čandík, M., Ivanka, J. : Bezpečnost v informačních technologiích, In: Security magazin, Roč. X., vyd.53, 3/2003, vyd. Familymedia, Praha, 2003, str.50-51, ISSN 1210-8723

[23] Ivanka, J.: Tvorba elektronických studijních opor pro bezpečnostní technologie, systémy a management. Sborník příspěvků ze 7. konference, Internet a konkurenceschopnost podniku.,UTB ve Zlíně, Zlín , str. 67, ISBN 80-7318-269-6

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

TelZ	Zákon o telekomunikacích
ZoP	Zákon o policii
TrŘ	Trestní řád
BIS	Bezpečnostní Informační Služba
VOZ	Vojenském Obranném Zpravodajství
SIM	Subscriber Identity Module - účastnická identifikační karta
FM-VKV	Frekvenční modulace – velmi krátké vlny
Pásmo AIR	neveřejné pásmo vhodné pro diskrétní provoz
GSM	Globální Systém pro Mobilní komunikaci (Groupe Spécial Mobile)
SMD	součástky určené pro povrchovou montáž (surface mount device).
LED	světlo vyzařující dioda (Light-Emitting Diode)
CCD	elektronická součástka pro snímání obrazové informace (Charge-Coupled Device)
CMOS	Technologie na výrobu čipů (Complementary Metal–Oxide–Semiconductor)
LAN	místní síť (Local Area Network)
WAN	rozsáhlá síť" (Wide Area Network)
TCP/IP	primární transportní protokol - TCP/protokol síťové vrstvy – IP (Transmission Control Protocol/Internet Protocol)
PCI	Počítačová sběrnice pro připojení periferií k základní desce (Peripheral Component Interconnect)
NBÚ	Národní bezpečnostní úřad
BTS	Základnová převodní stanice (*Base Transceiver Station*) je vysílač a přijímač radiových signálů
TDMA	metoda digitálního multiplexování (Time Division Multiple Access)

SEZNAM OBRÁZKŮ