ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

Katedra zdravotnických oborů a ochrany obyvatelstva

Obrana proti odposlechovým prostředkům a nezákonnému získávání informací

Defending Against a Wiretapping and an Illegal Information Gathering

Diplomová práce

Studijní program: Magisterský studijní program

Studijní obor: Civilní nouzové plánování

Autor diplomové práce: Bc. Jan Straka

Vedoucí diplomové práce: Ing. Václav Navrátil

Kladno 2020

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Straka**	Jméno:	**Jan**	Osobní číslo:	**484195**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Ochrana obyvatelstva**				
Studijní obor:	**Civilní nouzové plánování**				

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Obrana proti odposlechovým prostředkům a nezákonnému získávání informací

Název diplomové práce anglicky:

Defending Against a Wiretapping and an Illegal Information Gathering

Pokyny pro vypracování:

Předmětem diplomové práce bude rozbor činností, metod a postupů při provádění obranných technických prohlídek, díky kterým je možné odhalit odposlechové prostředky, které jsou nezákonně umístěny v prostorách za účelem neoprávněného získávání informací nebo jiných údajů. Budou uvedeny a podrobně rozebrány přístroje a vybavení nezbytné k provádění obranných technických prohlídek a zařízení určená k prevenci proti vnesení takového zařízení do zájmového prostoru. Dále bude provedeno zhodnocení současného stavu trhu s volně dostupnými odposlechovými prostředky, které lze zařadit k tzv. komerčním a které bývají často zneužívány k získávání informací. Jsou to i zařízení tzv. chytré domácnosti s přístupem na internet, vybavená kamerami a mikrofony, které lze využít k potenciálnímu útoku na jejich uživatele. V praktické části bude provedeno měření s detektory nelineárních přechodů, jejich penetrace různými materiály a konstrukcemi a pomocí Multikriteriální analýzy bude na základě výsledků provedeno posouzení jednotlivých přístrojů. V závěru práce bude návrh pro činnost s detektory nelineárních přechodů a doporučení k možnostem ochrany proti odposlechovým prostředkům a prevence proti možným hackerským útokům na zařízení tzv. chytré domácnosti.

Seznam doporučené literatury:

[1] BRABEC, František, Bezpečnost pro firmu, úřad, občana, Praha: Public History, 2001, 400 s., ISBN 80-86445-04-6
[2] NĚMEC, Miroslav, Kriminalistická taktika pro policisty a studenty Policejní akademie České republiky v Praze, Praha: Abook, 2017, 548 s., ISBN 978-80-906974-0-9
[3] CHURAŇ, Milan, Encyklopedie špionáže, Praha: Libri , 2000, 432 s., ISBN 978-80-7277-020-5

Jméno a příjmení vedoucí(ho) diplomové práce:

Ing. Václav Navrátil

Jméno a příjmení konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **23.09.2019**
Platnost zadání diplomové práce: **18.09.2021**

prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c.
podpis vedoucí(ho) katedry

prof. MUDr. Ivan Dylevský, DrSc.
podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student(ka) bere na vědomí, že je povinnen(a) vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

27.9.2019
Datum převzetí zadání

Podpis studenta(ky)

PROHLÁŠENÍ

Prohlašuji, že jsem diplomovou práci s názvem Obrana proti odposlechovým prostředkům a nezákonnému získávání informací vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 09.05.2020

Bc. Jan Straka

PODĚKOVÁNÍ

Mé poděkování patří mému vedoucímu práce Ing. Václavu Navrátilovi za jeho odbornou pomoc, konstruktivní připomínky a věnovaný čas při psaní práce. Poděkovat musím také své rodině za podporu, trpělivost a pochopení.

ABSTRAKT

Diplomová práce pojednává o způsobech obrany proti odposlechovým prostředkům a o možnostech ochrany informací a soukromí.

V první části se zabývá současnými, běžně dostupnými odposlechovými a sledovacími zařízeními určenými ke skrytému získávání informací, která jsou volně dostupná na českém trhu. Zmíněny jsou i kybernetické hrozby, které jsou potenciálním nebezpečím.

Zvláštní část je věnována speciální technice, kterou lze použít k vyhledávání odposlechových a jiných sledovacích zařízení. Popsány jsou činnosti a metody užívané při provádění zvláštních technických kontrol směřujících k vyhledání uvedených prostředků.

V praktické části je zpracována problematika samotného vyhledávání ukrytých odposlechových zařízení pomocí detektorů nelineárních přechodů. Multikriteriální analýzou jsou vybrány tři typy detektorů k následnému testování. Jejich schopnosti jsou prověřeny při měření penetrace různými stavebními materiály, které byly zvoleny tak, aby představovaly domácí a kancelářské prostředí. Provedeno bylo také ověření schopnosti detekce elektronických zařízení ukrytých na různých místech představujících reálné použití.

Klíčová slova

Detektor; Informace; jednací místnost; kontrola; obrana; odposlech

ABSTRACT

The graduation thesis discusses ways of defense against eavesdropping devices and alternatives of information and privacy protection.

In its first part, the thesis deals with current listening and tracking devices freely available on the czech market designed for the purpose of obtaining information covertly. It also refers to cyber attacks as potential threats.

An extra part of the thesis focuses on special technique that can be used to detect eavesdropping and other tracking devices. It also describes activities and methods used during special technical controls aimed at detecting the above stated mechanism.

The practical part of the thesis concetrates on the issue of detecting of covert listening devices by nonlinear junction detectors. Based on a multi-criteria analysis, three types of detectors were selected for further testing. Their abilities were examined when measuring the penetration through various building materials chosen to represent home and office background. The detection ability of electronic devices hidden in different places simulating real use was examined as well.

Keywords

Detector; Information; conference room; control; defence; eavesdropping;

Obsah

1 ÚVOD

Informace jsou nejmocnějšími zbraněmi dnešní doby. Pakliže je někdo nemá a chce je získat, nabízí se možnost opatřit si je nelegální cestou pomocí špionážní techniky. Instalaci a obsluhu některých prostředků zvládne i naprostý laik. Takové tvrzení však neplatí pro odhalení, neboť pro člověka nic netušícího, neznalého této problematiky, ale i člověka odborně zdatného je odhalení nesnadné, ne-li nemožné. Zpravidla se jedná o miniaturní zařízení, která lze velmi snadno ukrýt nebo zakomponovat do různých předmětů, které se běžně vyskytují v budovách, kancelářích a domácnostech. Je tedy na místě opatrnost a přijetí opatření s cílem zabránit jejich použití.

Svou prací bych chtěl zjistit více o možnostech a způsobech ochrany před odposlechy a možnostech trvalé ochrany informací před jejich zcizením. Chtěl bych poukázat na rizika dnešní doby, kdy je možné si zakoupit téměř jakákoliv zařízení, kterými je možné nahrávat obrazové a zvukové záznamy a narušovat tak právo na svobodu a ochranu soukromí každého jedince. Mnoho zařízení každodenního používání a vybavení tzv. chytré domácností je připojeno na internet a stává se potenciální hrozbou pro své, mnohdy neopatrné uživatele.

Motivací k psaní práce je pro mě zjištění možných rizik, jejich uvědomění si a popsání možností ochrany společnosti před potenciální hrozbou ztráty soukromí, informací apod.

2 CÍLE PRÁCE A HYPOTÉZY

Cílem diplomové práce je popsání možností obrany proti odposlechovým prostředkům a nezákonnému získávání informací. Popisem činností a metod při provádění obranných technických prohlídek, které se provádí za účelem odhalení skrytě umístěných odposlechových prostředků bych chtěl přiblížit a zjistit aktuální možnosti obrany před těmito zařízeními a možnosti eliminace rizika jejich použití. Uvedu spektrum současné speciální techniky, která je nezbytná k provedení komplexní kontroly zaměřené na vyhledání ukrytých odposlechových a sledovacích prostředků. Svou pozornost zaměřím na nejčastěji nabízenou a dostupnou špionážní techniku, která může být snadno zneužita k neoprávněnému získávání informací.

V praktické části provedu měření s detektory nelineárních přechodů, kterými prověřím schopnosti penetrace různými materiály. Současně ověřím jejich schopnosti při vyhledání a označení místa instalace pěti nejdostupnějších odposlechových prostředků, které budou uschovány na různých místech. Konkrétní detektory k provedení praktické části vyberu za pomoci multikriteriální analýzy.

2.1 Hypotézy

HYPOTÉZA Č.1

Všechny typy odposlechové a sledovací techniky lze odhalit pomocí detektorů nelineárních přechodů;

HYPOTÉZA Č.2

Odhalení profesionálně umístěného odposlechového prostředku laikem není možné;

HYPOTÉZA Č.3

Detektor nelineárních přechodů detekuje všechna zařízení vybavená polovodičovými součástkami.

3 PŘEHLED SOUČASNÉHO STAVU

V následující kapitolách se budu věnovat odposlechové technice z pohledu ofenzívy a defenzívy. Uvedu volně dostupné odposlechové prostředky, které dle prodejců špionážní techniky patří k nejprodávanějším na našem trhu. Profesionální zařízení nezmiňuji, nejsou běžně dostupná jako ta komerční. Zvolená zařízení blíže popíši a to zejména s ohledem na možnosti a principy jejich použití. V části věnované obraně proti odposlechovým a sledovacím zařízením uvedu a přiblížím techniku, která se používá při obranných technických prohlídkách. Dále budu věnovat pozornost metodám a postupům k odhalování skrytě umístěné odposlechové techniky a možnostem trvalé ochrany před těmito zařízeními.

3.1 Krádež informací

Některé informace jsou velmi cenné. Pro někoho jsou tak důležité, že je pro jejich získání schopen se dostat až za hranu zákona. Nabídka trhu, detektivních kanceláří a soukromých bezpečnostních služeb nabízí mnoho způsobů, jak tajně získat informace. Ten, kdo se v problematice trestního práva orientuje tak ví, že není snadné podezřelé z takového jednání usvědčit a skutek dokázat. Špionážní techniku lze v dnešní době sehnat v tuzemských kamenných nebo internetových obchodech. Zahraniční e-shopy mají nabídku ještě širší a podstatně nižší cenovou hladinu a tak díky současným přepravním službám není problém takové zboží objednat z téměř jakékoliv části světa. Nákup těchto produktů není v naší zemi nijak kontrolován ani zakázán.

3.2 Odposlechová a sledovací zařízení

Odposlech je slovo známé odedávna. V současnosti je skloňované v mediálně známých kauzách, u kterých se díky legálním policejním odposlechům podařilo rozkrýt závažnou trestnou činnost. Jde-li o užívání

zpravodajské techniky státními bezpečnostními složkami, neměla by být obava z těchto prostředků na místě. Ty jsou používány v souvislosti s vyšetřováním nebo se zajištěním vnitřní bezpečnosti České republiky v souladu s příslušnými zákony pod dohledem státních zástupců. V soukromí však jde o nelegální činnost. Bývá to zpravidla k získání kompromitujících nahrávek při nevěře, rozvodu, dědickém řízení apod. V pracovní sféře se použití nabízí jako konkurenční boj, získání důležitých informací apod. [1]

Při použití této techniky je trestné až získání informací a jejich zneužití. Samotné držení, prodej a používání odposlechové techniky zákon nijak neřeší, pakliže není do prostoru vstoupeno protiprávně nebo za použití násilí.

3.2.1 Místa instalací

Způsob ukrytí záleží na místních možnostech a čase, po který má být zařízení využíváno. Zda se jedná o jednorázové použití na jednání, poradu apod., nebo jde o dlouhodobý provoz. Od toho se odvíjí napájení a způsob umístění. V prvním případě zpravidla postačí baterie, v druhém případě se nabízí využití místních elektrických rozvodů, které jsou vhodné k dlouhodobému provozu zařízení. Technická úroveň odposlechové techniky je v dnešní době na vysoké úrovni. Dovedou zachytit zvuk vzdálený i několik metrů od zařízení. Samozřejmě čím blíže je ke zdroji zvuku, tím kvalitnější je záznam. V případě použití odposlechového a sledovacího zařízení (dále jen OSZ), od kterého je požadován i video přenos, je nezbytné zařízení umístit v zorném poli a zároveň skrytě, což protistraně komplikuje situaci a snižuje možnosti k bezpečnému uschování a snížení rizika odhalení.
K napájení je vhodné použít běžné rozvodné sítě 230 V kvůli energetické náročnosti některých zařízení. Umístění OSZ je tak vhodné do elektroinstalačních krabic, rozvodných lišt, zásuvek, vypínačů, prodlužovacích přívodů apod. V podstatě do veškerého trvale připojeného elektrického

zařízení, které může poskytovat elektrickou energii. Nábytek, stropní svítidla a podhledy se nabízí jako místo vhodné k audio i video snímání informací. Kapitolou samotnou jsou OSZ, která jsou integrována do běžného průmyslového zboží již z výroby. Můžou to být prodlužovací kabely, nabíječky, adaptéry, lampy, běžná elektronika atd. Ty bývají vybaveny GSM moduly a zpravidla stačí zasunout do příslušného místa SIM kartu bez PIN kódu, aktivovat a jsou připraveny k provozu. Sledovací zařízení s přenosem obrazu i zvuku jsou dnes integrována i do klasické neprůhledné LED žárovky, která se jen trochu liší od běžné. Dále například do meteostanic, radiobudíků, klíčů, propisek a dalšího spotřebního zboží. V případě malých OSZ se jedná spíše o záznamníky, které ukládají zaznamenané nahrávky na vnitřní paměť nebo paměťovou kartu. V případě větších zařízení nebo zmíněné žárovky, je možné údaje přenášet také prostřednictvím Wi-Fi sítě. Některé firmy prodávají nejenom OSZ již zabudované do zmíněných produktů, ale nabízejí také montáž do předmětů dodaných zákazníkem s garancí anonymity.

3.2.2 Komerční odposlechové prostředky

Ve své práci se věnuji OSZ, která jsou volně dostupná, která lze zakoupit v kamenných nebo internetových obchodech. Vzhledem k tomu, že prodej této techniky není nijak omezen ani regulován a ceny základních modelů začínají od desítek korun v případě nejprimitivnějších rádiových zařízení, tak každý, kdo má zájem si je může snadno opatřit. Nabízené produkty se liší pořizovací cenou, provedením, napájením a z toho plynoucí možnou délkou provozu, způsobem ukládání nebo přenosu získaných informací. Napájení bývá řešeno napojením na běžnou 230 V rozvodnou síť nebo za použití akumulátorů. Ty ale limitují časovou výdrž zařízení. Tu lze zvýšit za pomoci dodatečného zdroje, např. v podobě power banky nebo užitím zařízení s funkcí VOX, která odposlech aktivuje při detekci hluku, který překročí hranici od cca 45 dB výš. Šetří tak energii a snižuje zároveň možnost odhalení v době nečinnosti.

V případě GSM odposlechů lze zařízení využívat jako jednostranný telefon, na který lze zavolat a zvuky z prostoru přenášet prostřednictvím mobilní sítě a poslouchat jako běžný hovor pouze v konkrétní době nebo za využití funkce VOX.

3.3 Rozdělení a způsoby přenosu informací

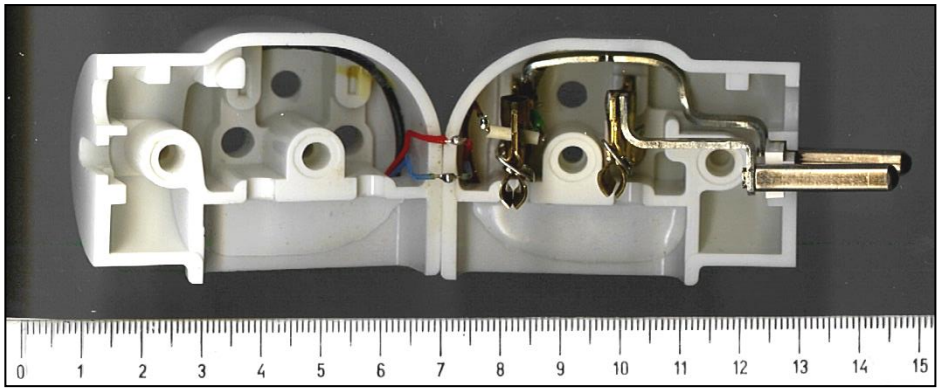
Jsou různé druhy odposlechových prostředků a stejně tak různé způsoby přenosu získaných informací. Nejčastější a nejvyužívanější způsob přenosu zachycených informací je pomocí linkového vedení, rádiových vln, za využití GSM, 3G a 4G sítí, Wi-Fi a Bluetooth signálů. Ve výše zmíněných případech se jedná o OSZ invazivní, které je nutné vnést a umístit, případně instalovat do požadovaného prostoru. Zároveň jsou ale nejdostupnější, nejpoužívanější a nejkomfortnější pro útočníka, který má možnost přístupu do kontrolovaného prostoru. Existují také OSZ neinvazivní, mezi které řadíme laserový odposlech, stetoskopický a směrový mikrofon. První dva zmíněné snímají akustický tlak z předmětů, které rozechvívá probíhající hovor a následně tento převádí na zvuk. V případě laserového odposlechu se jedná o složitou technologii převodu laserového paprsku do přijímacího zařízení, které paprskem zachycené vibrace převede zpět na řeč. Takové zařízení nelze zařadit mezi komerční OSZ, protože není volně prodejné. Navíc vyžaduje přímou, viditelnost do zájmového prostoru. Jako další neinvazivní způsob odposlechu lze použít směrový mikrofon, který je však určen k použití v exteriérech. Na volném prostranství dokáže zachytit zvuk až na vzdálenost 500 metrů. Stetoskopický mikrofon zase vyžaduje být poblíž zájmového prostoru. [5]

3.3.1 Radiomikrofony

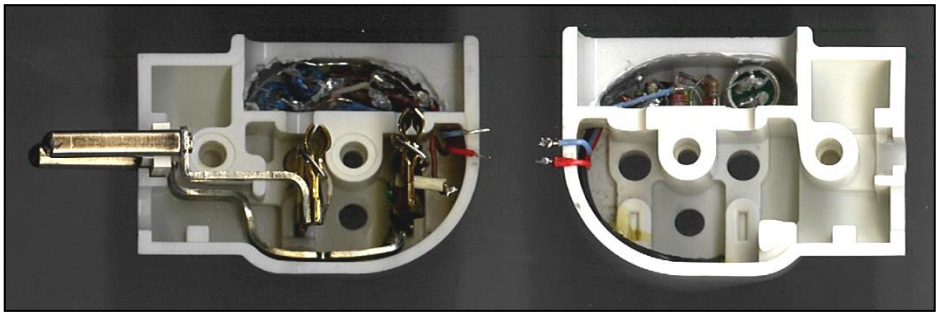
Jsou odposlouchávací zařízení, která pomocí vysoce citlivého mikrofonu zachytávají zvuk a ten následně pomocí rádiového signálu přenáší směrem

k přijímači. Samotné odposlechové zařízení se skládá z mikrofonu, napájecího obvodu, zdroje, zesilovače a vysílače. Přijímačem zachyceného signálu může být u jednoduchých zařízení běžný rádiový přijímač, na kterém lze naladit vysílaný signál v rozsahu 85-115 MHz. Nevýhodou je malý dosah (desítky metrů) a riziko, že zachycený signál může slyšet kdokoliv v blízkém okolí, kdo bude mít na totožném kmitočtu naladěn běžný rádiový přijímač v pásmu, kde vysílají FM rádia. Výhodou jsou velmi nízké pořizovací náklady v řádech desítek až stovek korun. Sofistikovanější typy radio mikrofonů vysílají v pásmu UHF od 0,3 GHz až 3 GHz. K příjmu signálu se používá speciálních UHF přijímačů, nehrozí tak náhodné zachycení při poslechu rádia. Dosah mají zpravidla až stovky metrů v závislosti na anténě, umístění a okolní zástavbě. Doba provozu je dána kapacitou baterií, v případě, že je připojen do elektrické sítě je provoz téměř neomezený.

Obrázek 1. FM vysílač (s anténou a napájecím konektorem na 9 V baterii).



Obrázek 2. Radiový odposlech integrovaný do funkční rozbočovací zásuvky (s měřítkem).



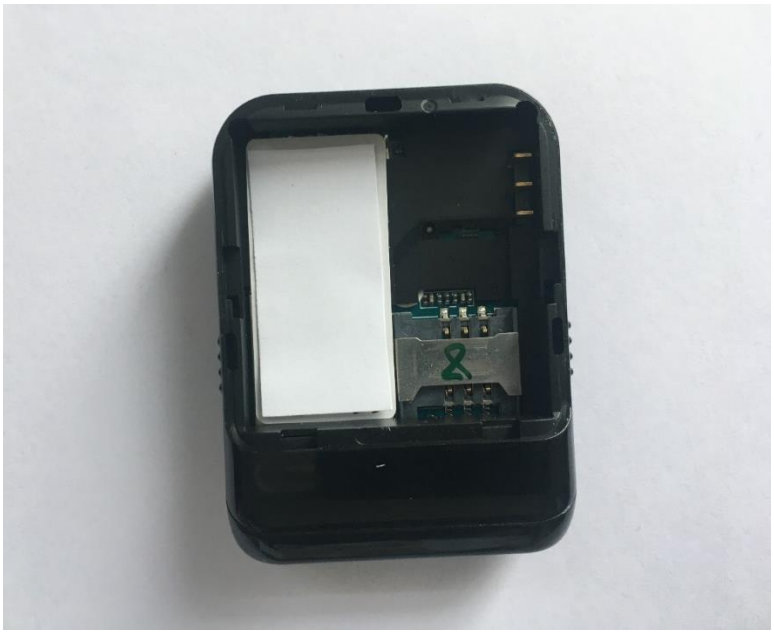
Obrázek 3. Radiový odposlech integrovaný do funkční rozbočovací zásuvky.

3.3.2 GSM odposlech

Zařízení pracující na principu běžného mobilního telefonu. Dosah je téměř neomezený, limitovaný jen pokrytím signálu mobilních operátorů. Jedinečnost spočívá v tom, že je možné odposlouchávat v dobré kvalitě přenášeného zvuku na druhém konci země s minimálním rizikem možného odhalení. Aktivace se provádí nastavenou úrovní hluku a zavoláním na předem uložené telefonní číslo, na které je zachycený zvuk přenášen. Možné je také zavolat na číslo vložené sim karty a poslouchat, co se děje v okolí zařízení. Nespornou výhodou je neomezený dosah, okamžitý provoz bez rušení, malé rozměry, které umožňují instalaci do věcí denní potřeby nebo běžného vybavení domácností, kanceláří apod. Předplacená SIM karta také zaručuje jistou dávku anonymity.

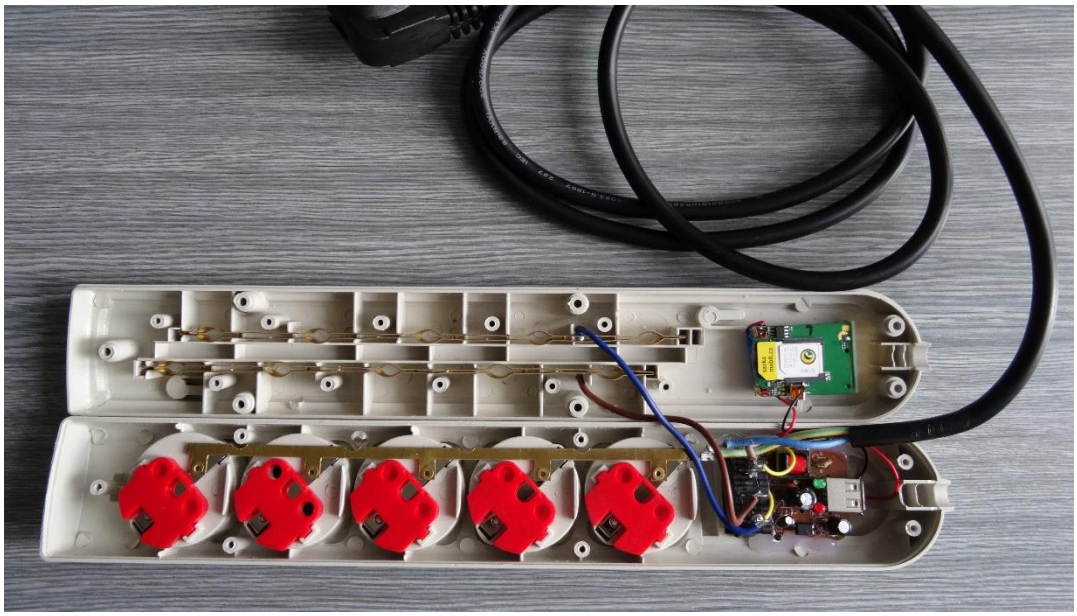
Kamuflované OSZ lze již zakoupit hotové. Nevýhodou je především vyšší energetická náročnost při používání na baterie.

Obrázek 4. GPS s GSM vzdáleným odposlechem (produkt tuzemského mobilního operátora).



Obrázek 5. GPS s GSM vzdáleným odposlechem (pohled na slot pro SIM kartu).

Obrázek 6. Funkční zásuvková lišta se zabudovaným GSM modulem.



Obrázek 7. Pohled na zabudovaný GSM modul.

3.3.3 Wi-Fi odposlech

Provedením a funkcemi je totožný s GSM odposlechy. Rozdíl je v tom, že zachycené informace předává prostřednictvím vlastní sítě Wi-Fi na nedaleko vzdálený přijímač, kterým může být např notebook. Nasbírané datové pakety ukládá a v nastavených intervalech odesílá k dalšímu použití.

Obrázek 8. Odposlech integrovaný v nabíječce. Získané údaje odesílá prostřednictvím Wi-Fi signálu.

3.3.4 Záznamníky

Jsou zařízení, která umožňují zaznamenat a uložit vše, co se děje v jejich okolí. Citlivé mikrofony umožní zachytit hovor i na vzdálenost větší než deset metrů. Odposlechový záznamník je možné umístit do čehokoliv díky miniaturním rozměrům. Na rozdíl od zařízení přenášejících signál po radiových nebo mobilních sítích záznamníky pouze ukládají na vnitřní paměť, nic nevysílají. Pro útočníka je nutné mít možnost opakovaného přístupu do prostoru, kde je zařízení umístěno, aby získal nashromážděné informace. Použití se nabízí v situacích, kdy není nutný online přenos, ale postačuje samotné zaznamenání. Tato domnělá nevýhoda je obrovskou výhodou pro útočníka, neboť zařízení nevysílá žádný signál, tudíž není zjistitelné pro frekvenční přijímače a analyzátory. V kamuflovaném provedení se od běžných předmětů liší pouze miniaturními otvory pro přívod zvuku k mikrofonu. Pro laika téměř nezjistitelné.

Obrázek 9. Funkční flash disk se záznamníkem zvuku (umožňuje cca 50 hod záznamu).

3.3.5 Linkové odposlechy

Vedení v kontrolovaném prostoru může být zneužito nejen k napájení OSZ, ale také k přenosu informací. Například připojením miniaturní krabičky na přívodní kabel k telefonu lze zabudovaným rádio vysílačem přenášet hovory z pevných linek. Spuštění se provede pouhým zvednutím sluchátka telefonního aparátu nebo příchozím vyzváněním a rádiovým signálem se hovor přenese k nedaleko vzdálenému přijímači. Lze také na vedení připojit mikrofon a po vedení přenést zachycený zvuk do bezpečného prostoru.

3.3.6 Skryté kamery

Jsou miniaturních rozměrů stejně tak jako odposlechy, ale navíc umožňují přenos videa a v některých případech i audia. Na rozdíl od odposlechových zařízení, musí být umístěny s výhledem na sledovaný objekt nebo prostor, což značně znemožňuje útočníkovi možnosti k umístění, oproti samotnému odposlechu, kterému stačí jen přístup zvuku.

Obrázek 10. Minikamera se záznamníkem ukrytá ve funkčním peru (objektiv kamery se nachází v černém čtverečku nad sponou).

Obrázek 11. Atrapa autoklíče s kamerou s mikrofonem.

3.4 Kybernetické útoky

Kybernetickými útoky nemusí být jen proniknutí do počítačové sítě a poukázání na její nízké zabezpečení nebo zviditelnění samotného hackera, který nemá žádný zájem na získání informací nebo na finančním zisku. Takovým útokem je možné získat informace, data, ale také přístup do sítí a do zařízení samotných a ty ovládat na dálku.

Všudypřítomný internet a zařízení na něm závislá včetně zařízení chytré domácnosti, nazývána zařízení internetu věcí nabízí možnost ke zneužití protistranou. Dnes je většina mobilních telefonů, tabletů, chytrých hodinek apod. zařízení trvale připojena na internet. Naše auta, domy a jejich vybavení také a díky tomu můžeme využívat komfortní funkce. Hlasově nebo vzdáleně je ovládat, vědět o místě výskytu svých blízkých, vzdáleně můžeme kontrolovat svůj dům pomocí kamer, ovládat klimatizaci, zkontrolovat teplotu v chladničce, vzdáleně ovládat některé funkce moderního automobilu atd. To vše jsou věci, které můžeme využívat samy pro svůj užitek, ale stejně tak je může i někdo zneužít proti nám.

Získávání informací a dat z mobilních telefonů, počítačů, ze síťového provozu pomocí instalovaného softwaru nabízí dnes řada firem a internetových prodejců. Jejich přítomnost v zařízení není snadné odhalit. Pro nic netušícího uživatele je to téměř nemožné. Útočník může mít online přehled o činnosti na těchto zařízeních nebo jen dodatečně může zjistit, které klávesy byly zmáčknuty na klávesnici PC. Například díky zařízení, které se jen připojí do USB portu (tzv. keylogger). [2]

Obrázek 12. Odposlech klávesnice Keylog USB TIME s podporou českých znaků a časovým razítkem [3]

3.5 Obranná technická prohlídka

Obranná technická prohlídka (dále jen OTP) je specializovaná činnost prováděná za účelem vyhledání odposlechového nebo jiného sledovacího zařízení. V naší zemi ji provádí specializované soukromé bezpečnostní služby (dále jen SBS), zpravodajské služby a Policie České republiky k obraně a ochraně proti úniku informací pomocí technických zařízení. V soukromém sektoru se provádí výhradně bezpečnostními agenturami, které jsou personálně a technicky vybaveny k poskytování těchto služeb. Ve státní správě se provádí k ochraně důležitých objektů, informací a zájmů naší země. Tato činnost je prováděna státními subjekty, kterými jsou zpravodajské služby a Policie České republiky. V trestním řízení se provádí jako úkon důležitý pro vyšetřování a

jedná se o činnost výhradně prováděnou Policií České republiky, Službou kriminální policie a vyšetřování.

Provádění obranných technických prohlídek směřujících k ochraně informací před jejich únikem po technických kanálech je nutno realizovat specialisty vybavenými speciální technikou (technika pro odhalování úniku informací na technických kanálech). Vedle těchto obranných technických prohlídek je třeba průběžně provádět kontrolu vybranými a zaškolenými pracovníky zařazenými na konkrétních chráněných úsecích činnosti. Tito pracovníci se pak při průběžné ochranné technické kontrole se zaměřují především na:

1. funkčnost obranných technických prostředků proti úniku informací;
2. dodržování režimových a organizačních opatření chránících daný úsek před únikem informací;
3. provádění technických prohlídek s využitím jednoduchých zařízení ke zjišťování možných úniků informací po technických kanálech. [4]

„Každý, kdo chce uchovat svá tajemství musí vycházet z předpokladu, že někdo může mít o takováto tajemství zájem. Proto se musí vážně věnovat ochraně proti možnému úniku informací. K tomu je nezbytné věnovat pozornost provádění obranných technických prohlídek, které jsou součástí systému speciální ochrany, před možným únikem informací“. [4, s. 166]

3.5.1 Zásady OTP

Tak jako jiná specializovaná činnost, tak i OTP by měla mít své postupy a specifika, kterými se pracovníci řídí, aby byli při své činnosti úspěšní a odvedli profesionální práci. Jde především o:

- Provedení prohlídky v době, kdy se předpokládá, že bude zařízení aktivní. Pracovní doba, domluvené jednání, návrat domů, víkend apod. Dálkově ovládané odposlechy nemusí být snadné odhalit, naopak jejich

odhalení v neaktivním stavu klade vysoké nároky na práci se speciální technikou, která může tato zařízení pouze slabě detekovat.

- Pravidelnost provádění následných prohlídek by měla být samozřejmostí, jejich plánování by nemělo být taxativně vymezené, ale naopak náhodně provedené mohou mít úspěch.
- Činnost pracovníků při prohlídce musí být v naprosté konspiraci, protistraně se nesmí dát signál o tom, že je prováděna OTP. Přístroje vydávají charakteristické zvuky, které je člověk znalý problematiky schopen rozlišit a zjistit, že je prováděna kontrola, je vhodné používat k přístrojům se zvukovou odezvou sluchátka nebo tichý režim. Pakliže nejsme schopni při práci zajistit naprosté ticho, je lepší standartní hluk typický pro daný prostor, např. poslech hudby, puštěný televizor, předstírané jednání apod. Stejně tak domlouvání prohlídky se zákazníkem by nemělo probíhat z kontrolované místnosti, neboť by mohlo dojít k demontáži, vypnutí apod. Zajistit takové postupy je velmi složité, neboť zákazníci netuší, co prohlídky obnáší nebo jak kvalitní mikrofony jsou v dnešní době k dispozici (schopnost snímat zvuk na několik metrů ve výsledné vysoké kvalitě).
- S příchodem pracovníků provádějících OTP by měl být seznámen pouze úzký okruh osob, pro případ, že by se mezi nimi nacházela osoba, která by měla na odposlechu zájem.
- Úspěch při provádění prohlídky je závislý hlavně na lidském faktoru. Odborných znalostech a důslednosti pracovníků provádějících kontrolu.
- Nezbytností je technické vybavení na vysoké úrovni, reagující na vývoj OSZ. [5]

3.5.2 Druhy prohlídek

Rozlišují se na komplexní a periodické. První spočívá v celkové kontrole zájmového prostoru s cílem odhalení sledovacího zařízení, případně zjištění

technických cest úniku informací. Součástí je doporučení nutných personálních opatření, technických úprav a opatření k zajištění lepší a efektivnější ochraně prostoru.

Periodická spočívá v pravidelném, předem dohodnuté opakování obranných technických kontrol, které již nejsou v tak velkém rozsahu jako u předešlé, ale jedná se o dílčí nezbytné úkony.

Doporučován je interval 6-8 týdnů, ale záleží na zabezpečení a režimu daného prostoru. Zpravidla je vhodná před důležitým jednáním nebo k monitorování jednání, aby bylo zjištěno případné použití odposlechového zařízení. [6]

3.5.3 Příprava a provedení

OTP lze provést okamžitě bez přípravy, hrozí-li nebezpečí z prodlení nebo vyžaduje-li to situace. V ideálních podmínkách musí být možnost se seznámit s vnitřním i vnější prostředím, s uspořádáním kontrolovaných prostor, stavební a technickou dokumentací. Také režim daného prostoru hraje důležitou roli, neboť podle toho lze předvídat, jaké by mohlo být instalováno zařízení, konkrétně jeho umístění. Zda bude tzv. dobře odloženo nebo důmyslně ukryto invazivním způsobem. Jiné možnosti pro instalaci budou v nehlídané volně přístupné místnosti a jiné v uzamčené bezpečnostní zámkem, zajištěné elektronickou signalizací, monitorovacím zařízením, ostrahou apod.

Etapy OTP

Obranná technická prohlídka má své etapy, které je vhodné dodržovat.

Přípravná etapa

- Domluvení termínu provedení OTP;
- zjištění důvodů k provedení OTP;
- zjištění možných cest úniku informací;
- předem dohodnutá osoba obeznámená s provedením OTP;

- časový rozvrh akce;
- požadavky na zadavatele ohledně obstarání technické a stavební dokumentace, případné zajištění přístupu do sousedících technických a jiných prostor;
- stanovení postupu v případě nálezu odposlechového zařízení nebo cesty úniku informací;
- změření frekvenčního spektra v blízkém okolí pro možnost porovnání se zjištěným stavem v prověřovaném prostoru.

Realizační etapa

- Samotné provedení OTP v požadovaném prostoru.

Hodnotící etapa

- Vyhodnocení získaných informací;
- porovnání žádoucího a skutečného stavu;
- soupis zjištěných ohrožujících nedostatků a odhalených prostředků nebo cest úniku informací.

O**vlivňovací etapa**

- Odstranění zjištěných únikových cest po technických kanálech;
- doporučení k efektivní ochraně prostoru;
- organizační a režimová opatření. [6]

3.6 Speciální technika na vyhledávání odposlechových prostředků

Nabídka defensivní techniky na trhu je oproti ofenzivní minimální. Značný rozdíl je také v pořizovací ceně. Ta je v případě obranné techniky vyšší o dva až tři řády pořizovacích cen OSZ. Vzhledem ke skutečnosti, že odposlechové prostředky se neustále vyvíjejí a jejich výrobci se také snaží jejich odhalení znemožnit nebo alespoň snížit, musí jít i vývoj obranných přístrojů vpřed. Udržet vzájemné tempo je tak pro obranu velmi nákladné a není finančně

únosné techniku pořizovat pro soukromé, byť i opakované použití. Některá technika není ani určena pro komerční využití a zakoupit ji mohou pouze výrobcem určené orgány státní správy.

3.6.1 Kontrola frekvenčního prostředí

Provádí se pomocí spektrálních analyzátorů nebo frekvenčních přijímačů. Zařízení načtou veškeré dostupné signály v prověřovaném prostoru. Některé je možné ustanovit dle kmitočtové tabulky Českého telekomunikačního úřadu nebo osobní znalosti obsluhy, demodulovat je nebo dohledat jejich zdroj, případně je vyloučit, pakliže by se jednalo o vzdálený signál. Většina legálních signálů je obsluze známa. Ať jde o pásma rozhlasů, televize, radioamatérských stanic, leteckého provozu, komunikačních přenosů, mobilní, Wi-Fi sítě apod. Kontrola frekvencí je vysoce specializovaná činnost, která vyžaduje znalosti nejen fyzikální, ale také znalost ofenzivních prostředků, které se používají k získávání informací. Nutné je povědomí o jejich provozním režimu, používaných kmitočtech apod. Frekvence používané odposlechovými prostředky jsou důsledně kontrolovány, neboť ty se mohou pohybovat také v pásmu legálních kmitočtů a mohou se v jejich blízkosti skrývat. Pozornost je věnována silným a netypickým podezřelým signálům, které značí možnou přítomnost odposlechového zařízení. Za využití směrových antén je možné dohledat zdroj signálu, nachází-li se v budově. [4]

Spektrální analyzátor OSCOR

Jde o přenosný kompaktní analyzátor elektromagnetického spektra s integrovanými anténami od amerického výrobce REI. Pracuje v rozsahu 10kHz – 24 GHz, ve kterém umožňuje analýzu naměřených hodnot v reálném čase. Umožňuje audio modulace AM, FM, SSB s vlnovým rozsahem od 2 kHz po 800 kHz. U videa podporuje standart SECAM, PAL, NTSC s vlnovým

rozsahem 12,75 MHz a 6,375 MHz a umožňuje tak zachytit některé bezdrátové kamery. Skenování spektra probíhá s rychlostí 24 GHz/1sec, je tedy možné detekovat krátké přenosy. Je vybaven dotykovým displejem, který nabízí zobrazení frekvencí v tzv. špičkách (peak) nebo vodopádové zobrazení (waterfall), které generuje spektrogram vysílacích signálů v čase. Nabízí analýzu spektra nebo jednotlivých signálů, které je možné porovnat s naměřenými hodnotami v blízkém okolí nebo při předchozím provedeném měření. Samozřejmostí je možnost ukládání naměřených hodnot a připojení hardwaru pomocí USB portu.

Obrázek 13. Oscor Green

(právě probíhající analýza nastaveného rozsahu frekvenčního prostředí)

Frekvenční přijímač PR – 100

Je přenosný frekvenční přijímač německého výrobce Rohde&Schwarz umožňující kontrolu spektra v rozsahu 9 kHz – 7,5 GHz. Je vhodný pro monitorování prostředí a lokalizaci vysílačů za pomoci směrové antény, je možné využít i všesměrovou a širokopásmovou anténu. Umožňuje zobrazení 10 MHz IF spektra a audio modulace AM, FM s vlnovým rozsahem od 150 Hz po 500 kHz. Signály jsou zobrazeny ve spektru nebo ve spektrogramu vysílacích signálů v čase. Vysoká citlivost přijímače umožňuje detekování i velmi slabých signálů. Funkce skenovaní předem nastaveného kmitočtového rozsahu umožnuje samočinné nalezení signálu, jehož úroveň je vyšší než nastavená úroveň prahu umlčení šumu. Tato funkce je vhodná pro déletrvající sledovaní zájmového prostoru, zda se zde nenachází podezřelý signál.

Přijímač RF signálu RFD – 5

Jedná se o širokopásmový detektor vysokofrekvenčního pole (dále jen VF) určený k vyhledávání všech druhů rádiových odposlechových a sledovacích prostředků v pásmu od 0,5 MHz až 25 GHz. Pracuje na principu detekce VF pole, které odposlechové prostředky při svém provozu kolem sebe vytváří. Detektor je schopen jej při určité vzdálenosti od zdroje zachytit. Detekce se přenáší do vestavěného reproduktoru nebo do sluchátek a dále se zobrazuje na LCD displeji. VF pole kolem sebe vytváří mobilní telefony, rádio přijímače, televizory, Wi-Fi routery apod., je tedy nutno detekované signály prověřit a dohledat zdroj vyzařování. RFD-5 dokáže přesně najít zdroj pomocí tří filtrů, které má přednastaveny. Vzhledem k tomu, že ve městech je úroveň VF pozadí vyšší je vhodné prostor prohlédnout postupně se všemi filtry. Samotné dohledání je nutné korelací délky antény a útlumu citlivosti. Při konkrétní lokalizaci je úroveň zvuku a signálu na LCD v maximální úrovni. Je také vhodný pro operativní použití a rychlou kontrolu prověřovaného prostoru.

Při překročení nastavené úrovně radiového pole vyhlásí poplach (díky funkci PROTECT, která načte radiové pozadí ve střeženém prostoru. Rovněž je vhodný pro zabezpečení jednací místnosti nebo automobilu apod. [7]

Obrázek 14. RFD-5

(nastavená kontrola vysokofrekvenčního vyzařování)

3.6.2 Kontrola místností

Zahrnuje kontrolu nelinearit, frekvenčního spektra, ale především kontrolu fyzickou. Při té je kontrolováno vše. Od stavební konstrukce, oken, dveří, stěn, podlah, stropů. Pozornost je zaměřena také na veškeré vybavení a zařízení kontrolovaného prostoru. Rizikem je veškerá síťově napájená elektronika, která poskytuje dostatek prostoru k instalaci odposlechové a sledovací techniky a

zároveň zajištění jejího trvalého napájení, které je nezbytným předpokladem pro její funkci. Prostředky napájené bateriemi nebo akumulátory jsou limitovány dobou provozu v závislosti na kapacitě oproti těm, které jsou připojené k trvalému zdroji elektrické energie. Je nezbytné zkontrolovat veškeré zásuvky, přívodní a prodlužovací přívody, světla, elektronické zabezpečovací systémy (dále jen EPS), rozvodné krabice a ostatní elektronické vybavení. Taková místa umožňují bezpečné uložení s ohledem na možné odhalení a v podstatě neomezený provoz OSZ. Většina uživatelů nikdy do takových míst nevstupuje. Pakliže ano, nemusí vůbec poznat, že je zde zařízení, které je navíc. Zde mají výhodu profesionální pracovníci, kteří vědí co, kde a jak hledat. [8]

3.6.3 Kontrola elektrických rozvodů a přenosových linek

Zahrnuje kontrolu slabo i silnoproudých rozvodů, telefonních, faxových a LAN rozvodů. Vedení k vnitřním rozhlasům, domovní zvonky, telefonní vedení atp. mohou být zneužity k přenosu informací.

Ke kontrole rozvodů je vhodné využít technickou dokumentaci objektu k následné verifikaci se skutečným stavem. Stejně tak provést kontrolu veškerých přívodních vodičů. Přítomnost starých nepoužívaných rozvodů v objektech je riziková a zároveň ideální pro útočníka k instalaci linkových OSZ. Po takovém vedení je možné přenést zvuk zachycený na mikrofon, který je na vedení umístěn. Ke kontrole vedení je vhodné mít přístup k začátku i konci vodiče s přístupem po celé délce, aby mohla být provedena kontrola, zdali na vedení není připojeno parazitní zařízení. Přístroje určené ke kontrole vedení dovedou takové místo napojení odhalit a určit přibližné místo, kde se takové napojení nachází.

3.6.4 Přístroje ke kontrole vedení

Talan

Jde o profesionální analyzátor výrobce REI (provedením podobný spektrálnímu zařízení Oscor viz. obr. 14), který slouží ke kontrole vedení. Je vybaven audio osciloskopem s aktivním vstupem v pásmu 20 Hz až 20 KHz. Je schopen provádět testy napětí, proudu, odporu, kapacity, demodulaci digitálních linek a měřit RF spektrum až do 8 GHz. Funkce nelineárního detektoru spojení umožňuje detekování jakékoliv elektroniky připojené ke kontrolovanému vedení. V případě více žilových kabelů provádí testy všech kombinací párů. Díky Fourierově transformaci (dále jen FFT) převádí síťový provoz do spektrálního pohledu s možností uložení a následného možného porovnání při dalším měření. K připojení hardwaru je k dispozici USB port. [9]

Linkový adapter LTA – 3

Jedná se o doplněk k detektoru RFD – 5, který slouží k odhalení linkových odposlechů pracujících v nízkofrekvenčním spektru v pásmu od 20 kHz až 41 MHz (mikrofony, reproduktory). Lze odhalit i přítomnost digitálních odposlechových prostředků, ale i přenosy jako ADSL, ethernet po síti apod. Připojením kontrolovaných vodičů na zařízení lze poslechem ve sluchátkách zjistit, zda z kontrolovaného prostoru neodchází zvuk. Analogové telefonní linky jsou při vyzvednutí sluchátka velmi dobře slyšet.

3.6.5 Detektory nelineárních přechodů

Jedná se o ruční mobilní zařízení určené k vyhledávání a přesné lokalizaci aktivních a pasivních odposlechů. Je vybaven směrovou anténou, která vysílá signál na různé frekvenci, dle typu a výrobce. Funkce spočívá ve vysílání spojitého nebo pulsního detekčního vysokofrekvenčního signálu (harmonický

signál sinusového napětí s definovanou frekvencí) a poté zpětně vyhodnotí vyzářené elektromagnetické vlnění. Pokud prověřovaný objekt (zeď, nábytek apod.) obsahuje polovodičové součástky, jsou na PN přechodech (polovodičové součástky – jednosměrně propustné) těchto součástek generovány vyšší harmonické frekvence. Jsou to násobky základní frekvence vyslaného signálu a jsou vyzařovány volně do okolí. V praxi se využívá detekce druhé a třetí vyšší harmonické frekvence, kterou používá většina výrobců detektorů nelineárních přechodů (dále jen DNP). Polovodičové prvky umělého původu mají vyšší úroveň druhé harmonické složky, zatímco polovodičové prvky přírodního původu (např. zoxidované vrstvy) mají vyšší úroveň třetí harmonické složky. [10] Význam práce s DNP při OTP je prostý. Veškeré odposlechové, sledovací a přenosová zařízení musí být ke své činnosti vybavena polovodičovými prvky. Zařízení nemusí být v aktivním stavu a lze ho najít díky součástkám, které obsahuje. Znalá obsluha dokáže dle úrovně signálů 2. a 3. harmonické frekvence rozlišit, zda se jedná o polovodiče nebo nelineární přechod vytvořený kovovými součástkami (nábytková kování, stropní konstrukce, pořadníky v šanonech, konektory apod.). DNP jsou vybavené optickou signalizací a doplněny zvukovou signalizací s různou úrovní zvuku pro rozlišení detekovaného předmětu. Podezřelé přechody je nutno prověřit a opakovaně proměřit. Někdy postačí k odstranění přechodu poklepání na místo, kde je signál detekován, jindy je potřeba rozebrat a zkontrolovat prověřovaný objekt. V krajním případě je nutné použít destruktivní metodu. Není-li možný invazivní postup, nabízí se možnost lokalizované nepřístupné zařízení zničit samotným DNP, který při maximálním výkonu může poškodit polovodičové součástky nalezeného zařízení nebo jen přerušit přechod, který se vytvořil.

DNP ORION typ. 2.4 HX

Jde o přístroj amerického výrobce REI, pracující v úrovni 2.4 GHz, který je určený k vyhledávání aktivních i neaktivních zařízení. Je vhodný k přesné

lokalizaci GSM zařízení, kamer, diktafonů, ale také miniaturní elektroniky jako jsou USB disky a SIM karty, čipové karty. Je vybavený dotykovým displejem, kterým se provádí nastavení výkonu, útlumu, hlasitosti apod. Při zobrazení se nabízí ukazatel 2. a 3. harmonického signálu nebo histogram s časovým rozpětím od 10 sec po 1 minutu měření a graficky znázorňuje naměřené hodnoty. To je vhodné především v případech, kdy by obsluha nezaregistrovala proběhlou detekci elektroniky. Signalizace detekce probíhá zvukově, graficky a vibračně. Výkon lze nastavit automaticky nebo ručně. [9]

Obrázek 15. DNP Orion HX

(na pravé stupnici se zobrazuje detekovaná 3.harmonická)

DNP ST-402 Cayman

Jde o profesionální DNP ruského výrobce pracující v úrovni 2–3 GHz. Jedná se o multifrekvenční budící rozsah, který umožňuje nalezení běžných elektronických přístrojů, ale také miniaturních součástek jako jsou SIM karty, čipové karty a USB disky. Vyznačuje se jednoduchou obsluhou, která nevyžaduje pokročilé technické znalosti. Ovládací prvky jsou umístěné na rukojeti. Zobrazení detekovaných signálů je umístěno v zorném poli operátora. Signalizace detekce 2. a 3. harmonické frekvence pomocí LED a zvuku do zabudovaného reproduktoru nebo přiložených sluchátek. Navíc zobrazuje pomocí LED intenzitu odrazu signálu od kovových předmětů. Díky pokročilým algoritmům zpracování a analýzy signálů minimalizuje míru falešných poplachů. [11]

Obrázek 16. ST-402 Cayman

DNP Lornet – 36

Jedná se o specifický detektor pracující v pásmu 3,6 GHz, s technologií DPF (dvojitá vzorkovací frekvence), která umožňuje odhalit malá elektronická zařízení na vzdálenost až 17 metrů, SIM karty na vzdálenost až 1 metru. Parabolická anténa umožňuje přesné detekování zařízení obsahující polovodičové prvky na velké vzdálenosti. Přesnost a určení konkrétního místa prověřování označuje bodový laser. Veškeré ovládání provozních režimů, výkonu, hlasitosti a zobrazení se nachází na rukojeti přístroje. Grafické zobrazení 2. a 3. harmonické frekvence pomocí LED se nachází na anténě v zorném poli obsluhy. Zvukový signál lze vysílat do zabudovaného reproduktoru nebo do bezdrátových sluchátek. [11]

3.6.6 Technika na vyhledávání skrytých kamer

Skrytě umístěné kamery jsou vyšším nebezpečím než samotná odposlechová zařízení, která přenášejí pouze zvuk. Pouhý zvuk z místnosti nezajistí protistraně celkový přehled o dění a situaci v místnosti. Díky obrazu je možné vidět vše, co je v zorném poli kamery. Nejen osoby a věci zde přítomné, ale také jejich činnost. Zejména v případech, ve kterých hrozí odhalení špionážní techniky při provádění OTP, je možné některá zařízení dálkově vypnout a znemožnit tak jejich odhalení.

Lze ale předpokládat, že kamera bude umístěna v místě, kde bude mít dostatečný rozhled, ale zároveň dobré podmínky pro to, aby nebyla odhalena. Vzhledem k miniaturizaci současné odposlechové techniky nelze předpokládat, že by bylo možné objektiv velikosti špendlíkové hlavičky odhalit pouhým okem. Umístění lze provést nejen do stěn a stropů, ale také do předmětů. Objektivu postačí necelý milimetr průzoru, takže instalace je možná do čehokoliv (televizor, rádio, květináč, světlo, obraz apod.) [12]

Za totalitního režimu bylo velmi oblíbené místo státní bezpečnosti v mřížce reproduktoru televizního přijímače, kam byla technika instalována ještě před samotným prodejem díky spolupracovníkům státní bezpečnosti nebo dodatečně. Poloha a umístění televizoru zpravidla zajišťovalo velmi dobrý výhled. [13] Šťastný majitel nového televizoru si tak domů donesl i bonus od StB v podobě sledovacího zařízení, které napájel vlastní elektrickou energií.

Zařízení k vyhledávání objektivů využívají optického principu odrazu vysílaného světelného toku od osvětlených objektivů. Dojde k jeho rozzáření v místě instalace. Při takové kontrole dochází ke spoustě planých poplachů, neboť odrazy vytváří především kovový spojovací materiál, použité třpytivé barvy apod. To vše se musí fyzicky prověřit a následně vyloučit.

OPTIC II

Jde o detektor skrytých kamer určený k detekci a lokalizaci skrytých objektivů a kamer. Postupnou kontrolou celého prostoru včetně vybavení je schopen odhalit objektiv bez ohledu na to, v jakém provozním stavu se nachází. Princip detekce je založen na zpětnému odrazu světla super svítivých diod od skrytých objektivů. Zobrazí se jako zelená nebo červená tečka, dle zvoleného přísvitu zařízení. Je zde možnost trvalého nebo přerušovaného osvětlení kontrolovaného prostoru. Každý režim má jinou vlnovou délku světla a poskytuje širší možnost odhalení skrytě umístěného objektivu.

Parametry

- Rozsah detekce 0.5 – 50 metrů;
- zvětšení 6,5 krát;
- akumulátor, výdrž 4 hod;
- hmotnost 450 g.

Obrázek 17. Optic II

(v detekčním režimu za pomoci zeleného světla)

WCD-2

Zařízení, které samočinně nebo ručně provádí skenování na předdefinovaných frekvencích v kontrolovaném prostoru a blízkém okolí. Kontrolu provádí v pásmu 900-3000 MHz a 5000-6000 MHz, kde dochází k přenosu obrazu z bezdrátových a CCTV kamer. Při detekování přenosového signálu se tento zobrazí a automaticky uloží v interní paměti i se zjištěnou frekvencí.

Obrázek 18. WCD-2

(právě probíhající skenování prostředí)

3.6.7 Ostatní technika a vybavení

Termokamera

Kontrola spočívá v aktivním vyhledávání rozdílů tepelného vyzařování kontrolovaných předmětů, veškerého vybavení a stavebních konstrukcí vůči teplotě okolí. Princip je založen na tom, že všechny předměty vyzařují energii ve formě elektromagnetického záření, které nazýváme tepelné záření. To je způsobeno termickým pohybem částic, ze kterého je objekt tvořen. Intenzita

elektromagnetického záření je závislá na povrchové teplotě objektu, který toto záření vydává. Je tak možné změřením intenzity záření stanovit povrchovou teplotu objektu. Při provádění OTP mají nezastupitelné místo, protože každé OSZ, které je napájené elektrickou energií, se při své činnosti zahřívá a zároveň prohřívá i hmotu kolem sebe. Je možné tak odhalit zařízení, která byla v činnosti ještě před započetím OTP a byla na dálku vypnuta, aby nedošlo k jejich dekonspiraci. Zbytkové teplo vyzařuje energii až desítky minut po vypnutí.

Obrázek 19. Termokamera Ti 300

(na displeji v horní části za záclonou zapnutý Wi-Fi router a pod ním přívod teplé vody do radiátoru)

Endoskop

Slouží pro nepřímou vizuální kontrolu těžko přístupných míst. Miniaturní kamera může být umístěna i na několik metrů dlouhé sondě, která má možnost všesměrového natáčení operátorem, a umožňuje velkou flexibilitu v kontrolovaném prostoru. Nabízí funkce jako přiblížení obrazu, dodatečné přisvícení zorného pole nebo prodlouženou expozici. Snímky či videozáznam jsou zobrazovány na displej, je možnost záznam uložit na paměťovou kartu a se záznamem dále pracovat.

3.6.8 Vybavení pro fyzickou kontrolu

Zrcadla, svítilny a ruční nářadí jsou neodmyslitelnou součástí pro provedení fyzické prohlídky prostoru a špatně přístupných a osvětlených míst. Ideální řešení nabízí svítilny s LED technologií, které umožnují dávkování světelného výkonu, regulaci toku světla. U zrcadla je k prohlídkám vhodný zakřivený parabolický tvar s přisvětlením, který umožní velký pozorovací úhel v kontrolovaném prostoru. Umístění na teleskopické rukojeti umožní kontrolu ve vzdálenějších místech.

3.6.9 Kybernetická bezpečnost

Komplexní prohlídka zahrnuje softwarovou kontrolu počítačů, tabletů, mobilních telefonů, počítačových sítí a internetového připojení. Analýzou síťového provozu se zjišťuje, zda nedochází k zachycování provozu na speciální zařízení nebo ke skryté extrakci dat. U Wi-Fi routerů, mobilních telefonů a tabletů je vhodné v případě pochybností uvést zařízení do továrního nastavení. Poté se nachází ve stavu, v jakém byl zakoupen.

Kontrola by měla být zaměřená na to, aby neprobíhala skrytá extrakce dat z počítačové sítě, prověření přítomnosti skrytých aplikací běžících na pozadí počítačů nebo chytrých telefonů, které zaznamenávají činnost uživatelů,

případně je odesílají útočníkovi na jeho zařízení. Jsou schopné monitorovat prostor kolem PC a to akusticky i opticky. Monitorují veškeré úkony prováděné na počítači, včetně monitoringu stisku kláves, otevíraných souborů, odesílaných souborů, provádí skrytě snímky obrazovky. Dovedou využít komunikační programy typu Skype, Facebook apod. Přes tyto může mít dokonalý přehled o dění v okolí telefonu, tabletu nebo počítače, neboť dokážou skrytě běžet na pozadí, bez vědomí nic netušícího uživatele. [2]

Fyzickou kontrolou se provádí kontrola hardwaru, zda neobsahuje parazitní součástky nebo kamuflovaný hardware, který je na zařízení připojen a monitoruje a zachycuje činnost uživatele. Současná zařízení nabízejí hlasové ovládání, které umožňuje zabudovaný mikrofon, který se může stát cílem kyberútoku a umožnit tak odposlouchávání uživatele. Stejně tak i zabudované kamery. Nejde už jen o „chytré telefony" a tablety, ale také televizory, osvětlení, chladničky, bezdrátové kamery apod. To vše nabízí možnost potenciálního zneužití. [14]

3.7 Zásady ochrany proti úniku informací

Zabezpečení objektu je nezbytné pro komplexní zajištění bezpečnosti. Ve zpravodajské praxi se používá pro ochranu objektu před násilným napadením a vyzrazením utajovaných skutečností. Opatření pro zabezpečení se liší podle stupně důležitosti objektu a významu chráněných informací. [1]

3.7.1 Fyzická ochrana

Je nejčastější formou zajišťování ochrany a bezpečnosti objektu proti nedovoleným činnostem směřujícím k narušení objektu. Oproti pasivní ochraně umožnuje v případě potřeby provést zásah nebo jiné opatření k zabránění dalších škod a provádí dohled nad pasivní obranou. [15]

Ideální fyzickou ochranou je nepřetržitá služba, prováděná spolehlivými, prověřenými a důvěryhodnými lidmi. A i přes to, že lidský faktor není neomylný, zůstává nenahraditelnou ochranou. Má-li být fyzická ochrana zaměřena na kontrolu proti neoprávněnému vnesení a instalování OSZ do chráněných prostor, musí mít jisté povědomí o OSZ a technice.

3.7.2 Pasivní ochrana

Je nezbytná ke komplexnímu zajištění chráněných prostor proti neoprávněnému vniknutí. Jde především o elektronické zabezpečovací zařízení (dále jen EZS), které má za úkol včas varovat o narušení objektu nebo o pokusu o vniknutí do chráněného prostoru. S jeho pomocí je možno zajistit celé budovy, místnosti, okna, dveře, úložné a úschovné prostory. Možné je zajistit i nejbližší okolí jako zahrady apod. Hlavní součástí je ústředna, na kterou jsou napojena PIR čidla, detektory apod. a ústředna vyhodnocuje poplach, který je dále vyslán do sirény, na ústřednu, na mobilní telefon apod.

Doplněním o různé detektory, např. destrukčních projevů lze detekovat rozbití skleněných výplní, otevření dveří a oken, dále je možné signalizovat přítomnost kouře, CO_2, vody apod. Lze doplnit skrytými prostředky, např. kamerami, signalizací vstupu do chráněného prostoru apod. Využit lze i k případné skryté kontrole osob provádějících fyzickou ostrahu, neboť i tyto osoby mohou za jistých okolností vnést OSZ do zájmových prostor.

Neodmyslitelnou součástí je možnost zakrytí oken a skleněných výplní chráněných místností žaluziemi a těžkými závěsy k zabránění odposlechu přes okenní tabulky kontaktním nebo laserovým mikrofonem. V případě, že je do místnosti vidět, zabrání útočníkovi v možnosti odezírání a minimálně zamezí přehledu o dění v místnosti. Dále zajištění mechanickou ochranou jako jsou kovové mříže, bezpečnostní skla apod. Technickými zábrannými prostředky jsou:

1. bezpečnostní dveře (oplechované, plechové, pancéřované, požární);
2. bezpečnostní uzamykací systémy (normální, dozické, cylindrické, kódové, čipové, elektronické, přídavné zámky;
3. úschovná místa (plechové skříně, trezory). [15]

3.7.3 Fyzická kontrola při vstupu

Jde o fyzickou kontrolu vstupujících osob do objektu, kterou vykonávají pracovníci objektu, případně elektronický vstupní systém, umožňující vstup pouze konkrétním osobám. Účelem je zabránit neoprávněnému vstupu, případně vjezdu vozidel a vnášení či vynášení nedovolených předmětů do nebo z hlídaných prostor nebo z nich. Nedovolené předměty určuje charakter objektu, prováděné činnosti či charakter podnikatelských aktivit a z toho plynoucí rizika. Nutná je především evidence osob, které vstoupily do objektu nebo se nacházejí v objektu. Nezbytný je doprovod návštěv a cizích osob, je důležité znát důvod jejich vstupu. Provádět dohled nad jejich pohybem a jasně určit prostor se zapovězeným vstupem. To je nutné u prostor, kde probíhají jednání, řeší se tajné a strategické informace apod. Nelze totiž zabránit vnesení OSZ, neboť jejich rozměry jsou minimální a bez kontroly rentgenem, detekčním rámem a na to navazující osobní prohlídkou nelze zajistit, že osoba u sebe něco nemá. Komplexní prohlídku osob si lze představit u významných strategických objektů. [4]

3.7.4 Ochrana informací v oblasti personální

Vyzrazení informací je další možností k opatření si informací. Není k tomu nutné použití OSZ, pronikání do objektu ani nic podobného. U osoby poskytující informace je možné si jako důvody představit finanční profit, pomstu zaměstnavateli, vydírání nebo jen prostou upovídanost. Zaměstnanci mohou být pod falešnými záminkami kontaktováni a vytěžováni k citlivým

informacím. Zabránit fingovaným zaměstnáváním cizích osob od konkurence nebo protistrany je nelehký úkol. Prověřování a kontrola nových zaměstnanců by mělo být standardem.

Je nezbytné určení rozsahu oprávnění pro přístup k informacím a ke vstupům do prostor, kde se takové informace nacházejí, ukládají nebo projednávají. Ne každý pracovník musí mít přístup do všech prostor a mít povědomí o všech informacích.

3.8 Ochrana informací – trvalé zajištění jednacích místností

Nejen režimová a bezpečnostní opatření nám zaručí bezpečný prostor. Elektronické zabezpečovací zařízení, ani bezpečnostní pracovníci nejsou zárukou toho, že do prostoru někdo neumístí odposlechové nebo sledovací zařízení. Po provedení OTP specialisty je vhodné k trvalému udržení „čistého“ prostoru využít některá podpůrná zařízení, která zvládne ovládat proškolený personál. Ta dokážou odhalit případná vnesená zařízení nebo znemožnit jejich činnost, přenos dat apod.

3.8.1 Šumové generátory

Umožňují rušení mikrofonů v mobilních telefonech, diktafonech, odposleších atp. Generováním silného šumu v ultrazvukovém pásmu zahltí mikrofony a předzesilovače a znemožní zachycení hovoru. Například zařízení SNG svým tónem maskuje užitečný akustický signál hovorové řeči do uměle vytvořeného šumu, který svou intenzitou převyšuje zvuk hovoru v místnosti. Jedná se o tzv. růžový šum, který obsahuje všechny frekvence hovorového spektra a z případné nahrávky ho nelze odfiltrovat, neboť bychom odfiltrovali i samotný hovor v tomto šumu maskovaný. Pro správnou funkci je nezbytné, aby šum generátoru byl přenesen do všech tuhých předmětů v místnosti za pomoci nízko impedančních reproduktorů, ale také do zdiva a skleněných

tabulí oken. U zdiva jde o reproduktory s tuhou membránou, které jsou kotevním šroubem zapuštěny do zdiva, do kterého je vysílán šum. Okna a dveře se zajišťují pomocí piezo keramických akustických měničů, které se lepí na skleněné tabule oken a samotné dveře a přenosem zvuku způsobuji vibraci, která znemožňuje použití kontaktního mikrofonu. Stejným způsobem lze zabezpečit potrubí procházející místností, které může posloužit jako zvukovod. V panelových domech lze pouhým přiložením ucha k teplovodním trubkám zachytit přenesený zvuk ze sousedního bytu. V případě použití kontaktního mikrofonu lze slyšet zvuk z bytu o několik pater níže. [15] Také se využívají zařízení generující tzv. Bílý šum, který frekvenčně značně přesahuje frekvenční rozsah lidské řeči a nelze ji tak zachytit na mikrofon, který je neodmyslitelnou součástí OSZ.

Nevýhodou těchto zařízení je, že svou ochrannou činností vytváří v místnosti hluk, což může být pro někoho neakceptovatelné.

Obrázek 20. Kontaktní mikrofon

Obrázek 21. Šumový generátor

Obrázek 22. Piezo měnič přilepený na sklo (k přenesení vibrací do skleněné tabule okna).

3.8.2 Frekvenční paměťový přijímač

K trvalé ochraně před vnesením rádiových odposlechů je možné použít přijímač, který se umístí do chráněného prostoru, ve kterém načte všechny zde přítomné kmitočty, které si uloží do paměti. Ideální situace je, když se uložení provede po OTP, zejména po kontrole spektrálním analyzátorem, aby se

vyloučila přítomnost vysílajícího OSZ. Následně při zapnutí automatického monitorovacího režimu dochází k verifikaci uloženého a opakovaně měřeného frekvenčního pozadí. Zjistí-li přístroj neuloženou frekvenci, je vyhlášen poplach. V případech, kdy se signál vyskytne na krátkou chvíli, např. při průjezdu vozidla s vysílačkou, je vyhlášeno pouze varování. Uživatel vidí na displeji naměřenou novou frekvenci v poplachové paměti a může poslechem zjistit o jaké vysílání se jedná. Při delším výskytu nové frekvence je vyhlášen poplach. [5]

3.8.3 Rušení telekomunikačního provozu

V prostředí, ve kterém jsou potlačena komunikační pásma a brání průchodu signálů se jeví jako ideální řešení, neboť by bylo zabráněno OSZ přenášet data ze zájmového prostředí. Ale není to tak jednoduché, jak se na první pohled zdá. Výjimky na rušení frekvenčních pásem má pouze Ministerstvo vnitra a Ministerstvo obrany České republiky k plnění speciálních úkolů v rámci trestního řízení a zajištění bezpečnosti. Jakékoli rušení jinými subjekty za účelem zabránění komunikace je v České republice nepřípustné, dohled provádí Český telekomunikační úřad. Takovou činností by bylo narušeno efektivní využívání oprávněnými provozovateli. Mobilní operátoři, kterým by byly způsobeny značné škody ušlým ziskem, by byli mezi prvními poškozenými. I přes výše popsané skutečnosti existují prodejci, kteří rušičky prodávají. Upozorňují kupujícího, že zboží není určeno pro provoz v České republice a na území EU a je určeno pro export. Zakoupení by mělo být umožněno pouze podnikatelským subjektům a vybraným složkám státní správy. Existuje však možnost si jakékoliv zařízení obstarat ze zahraničí. S oblibou je používají zloději, kteří se tak snaží vyrušit případný signál GPS u odcizeného automobilu nebo poplachový signál EZS.

Nejčastěji rušená pásma : GSM, CDMA, 3G, 4G LTE, 4G WIMAX, Wi-Fi 2.4G, Bluetooth, Wi-Fi 5.2G, Wi-Fi 5.8G, GPS, VHF, UHF a další specifická pásma.

Obrázek 23. Nastavitelná rušička signálů [16]

3.8.4 Stíněné komory

Jsou založeny na principu Faradayovy klece, popsané v 19. století anglickým fyzikem Michaelem Faradayem. Ten zjistil, že elektrický náboj je pouze na povrchu vodiče, nikoliv v celém jeho objemu, že uvnitř vodiče nepůsobí žádné elektrické nebo elektromagnetické pole. Využití principu Faradayovy klece tak dokáže ochránit např. zdravotnické přístroje před působením elektromagnetické pole zvenčí nebo v případě ochrany informací před únikem elektromagnetického záření z klece. Vysílače nejsou schopné přenášet svůj signál mimo klec (místnost) a jsou tak elektromagneticky

odizolovány od okolních prostor. Takto upravené místnosti jsou ve své podstatě místnosti v místnosti a poskytují uživatelům nejvyšší možnou ochranu projednávaných informací. [17] Konstrukce, podlahy, stěny a stropy jsou tvořeny materiály, které snižují propustnost elektromagnetického záření a plně využívají Faradayova objevu. Jde o technologicky složitý celek, u kterého musí být zajištěno utlumení na všech vstupech a výstupech, včetně speciálně upravených stíněných dveří. Přívod elektrické energie do vnitřku se provádí přes síťový filtr, aby se zabránilo případnému odposlechu po vedení, celý objekt je uzemněn. Ostatní sítě se zpravidla nepřivádí z taktických důvodů. Pro doplnění ochrany se stěny osazují piezo měniči napojenými na generátor šumu. V okolí místnosti je vhodné taktéž generovat bílý šum k zamezení zaznamenání případného prostupujícího hluku z jednací místnosti. Vybavení interiéru by mělo být jednoduché, umožňující kontrolu pouhým pohledem. Zajištění režimu vstupu a zabránění vstupu neoprávněným osobám by mělo být samozřejmostí, stejně tak jako kontrola prostoru před jednáním. [18]

3.9 Legislativa

Ochranu před neoprávněným narušením soukromí a získáváním informací zaručuje Listina základních práv svobod a Trestní zákoník. Povinnost ochrany informací označených konkrétním stupněm utajení ve státní správě je dána zákonem č. 412/2005 Sb. Ochranu běžných informací nenařizuje fyzickým a právnickým osobám žádný dokument. Zajištění bezpečnosti je na zvážení každého jedince nebo organizace.

Legislativa řešící problematiku ochrany informací je Listina základních práv a svobod, Trestní zákoník a Zákon o ochraně utajovaných informací.

3.9.1 Listina základních práv a svobod

Je ústavním zákonem č. 2/1993. Jedná se o nejvyšší českou právní normu, ve které jsou zakotveny základní práva a svobody občanů. Užívání informací řeší Článek 7, který zaručuje nedotknutelnost osoby a jejího soukromí. Článek 10 zajišťuje právo na lidskou důstojnost, osobní čest, dobrou pověst a ochranu jména. Chrání před neoprávněnými zásahy do soukromého a rodinného života a neoprávněným shromažďováním a zveřejňováním údajů ke své osobě. Článek 13 řeší ochranu listovního tajemství a jiných písemností a záznamů a zaručuje zachování tajemství i u zpráv podávaných telefonem nebo jinými podobnými zařízeními. Narušení osobní nedotknutelnosti a soukromí smí být omezeno jen v případech stanovených zákonem (např. nařízené policejní odposlechy).

3.9.2 Trestní zákoník č. 40/2009 Sb.

V případě podezření na možné umístění nebo zjištění výskytu OSZ zajišťují podporu poškozeným orgány činné v trestním řízení, které přijímají oznámení od občanů a provádějí nezbytná šetření a úkony.

Dokazování v takových případech je velmi složité. Chybí-li důkazy (např. záznam z bezpečnostní kamery), není snadné označit konkrétní osobu(y), která se jednání dopustila(y). Přilepením odposlechu na spodní část stolu nezanechá mnoho stop důležitých pro vyšetřování a označení viníka. Kam a jakým směrem odcházejí informace, se ve většině případů lze jen domnívat. Samotné umístění OSZ není trestným činem. Pakliže k jeho umístění bylo neoprávněně vniknuto do objektu překonáním překážky, lze využít ustanovení paragrafu 178 tr. zákoníku *Porušování domovní svobody*. V případě získání informací přenášených elektronickou cestou připadá v úvahu naplnění skutkové podstaty trestného činu *Porušení tajemství dopravovaných zpráv* dle § 182. [19]

3.9.3 Zákon č. 412/2005 Sb.,

Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti řeší problematiku utajovaných informací na území České republiky. Upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu. Zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

§ 26 Projednávání utajovaných informací

4. odst. 1 ukládá povinnost odpovědné osobě zajistit, aby v jednací oblasti, kde lze pravidelně projednávat utajované informace stupně tajné a přísně tajné, aby nedošlo k ohrožení nebo úniku projednávaných utajovaných informací;
5. odst. 2 osoba odpovědná za bezpečnost je povinna požádat Úřad o provedení kontroly, zda v jednací oblasti nedochází k nedovolenému použití technických prostředků určených k získávání informací; o provedení této kontroly může odpovědná osoba požádat rovněž u zabezpečené oblasti kategorie Tajné nebo Přísně tajné. Tuto kontrolu Úřad zajistí v součinnosti se zpravodajskými službami a Policií České republiky. Pro své potřeby si zpravodajské služby a policie kontrolu provádějí samy. [20]

4 METODIKA

K provedení praktické části jsem stanovil dva vlastní způsoby měření za použití tří vybraných typů detektorů nelineárních přechodů (od každého výrobce zvolen jeden typ detektoru.) Získané naměřené hodnoty budou zapsány do tabulek k následnému porovnání. K provedení prvního experimentu bylo vybráno a použito šest typů zařízení, které lze běžně zakoupit a je možné je použít jako odposlechový a sledovací prostředek. Jednotlivá zařízení byla postupně instalována na místa, která by mohla být užita k jejich uschování a následnému získávání informací (zvoleno dle vlastní zkušenosti pracovníků zabývajících se OTP a dále webové stránky Detektivní-expert.cz). Zároveň musela být splněna podmínka přístupu zvuku k samotnému zařízení a pro útočníka časová nenáročnost na umístění. Jako OSZ byly použity:

1. GPS Lokátor typ T300 s funkcí vzdáleného odposlechu prostřednictvím sítě GSM (viz. obr. 4, str. 18);
2. pero se skrytou kamerou a mikrofonem, nahrávání na vnitřní paměť (viz. obr. 10, str. 22);
3. záznamník zn. Sony typ. ICD-MS515;

Obrázek 24. Záznamník zn. Sony

4. mobilní telefon Nokia 6610i;

Obrázek 25. Mobilní telefon Nokia

5. mobilní telefon iPhone 6S;

Obrázek 26. Mobilní telefon iPhone

6. radiový odposlech pracující v pásmu VKV 108 MHz (viz. obr. 1, str. 16).

Druhý experiment spočíval v měření penetrace jednotlivých DNP a jejich schopnost prostupu různými stavebními a konstrukčními materiály. Pro detekci byly vybrány výše uvedené OSZ s čísly 1 a 6.

4.1 Vyhodnocení pomocí multikriteriální analýzy

Tato analýza (dále jen MCDA) je podpůrný nástroj, využívaný ve složitých situacích, v nichž se výsledky rozhodnutí hodnotí podle více kritérií. Byla zvolena k vybrání nejvhodnějšího detektoru nelineárních přechodů určených k provádění obranných technických prohlídek v interiérech a exteriérech. Rozhodnutím by měla být vybrána ideální varianta s nejpříznivějšími parametry pro činnost při různých požadavcích na detekci. Vybráno bylo osm

typů detektorů, které byly porovnávány na základě kritérií, kterými budou vysílací výkon, hmotnost samotného zařízení (má vliv na výdrž obsluhy při déletrvající činnosti), pořizovací cena (v případě soukromého používání je důležitým kritériem), možnost připojení sluchátek k zajištění tichého provozu (znalá protistrana by mohla dle charakteristických zvuků přístrojů zjistit, že probíhá OTP, přičemž bezdrátová sluchátka byla hodnocena sto procenty, klasická osmdesáti procenty). Poslední hodnocenou kategorií byl komfort ovládání DNP (rozšířené možnosti nastavení, ovládání a zobrazování naměřených hodnot a aby emitovaly shodný signál v pásmu kolem 2.4 GHz). Vysílací frekvence měla výrazný vliv na celkové hodnocení položky komfort, neboť výrobci a prodejci tuto frekvenci deklarují jako schopnou odhalit většinu elektronických zařízení. Ve spojení s dobrým ovládáním a možnostmi různého nastavení a zobrazení mohli dosáhnout hodnocení až 100 %.

Volba optimální varianty je individuálním činem, který záleží na postojích a názorech samotného rozhodovatele provádějícího pokus. [21]

4.2 Analyzované typy DNP

K porovnání pomocí MCDA jsem vybral 8 druhů DNP, jedná se o:

1. **JJN EDD 24T**
   - Frekvenční rozsah 2400 - 2425 MHz;
   - maximální výkon 1 W;
   - hmotnost 700 g;
   - citlivost - 120dBm.
2. **LORNET 900**
   - Frekvenční rozsah 880 - 906 MHz;
   - maximální výkon 1 W;
   - hmotnost 1 kg;
   - citlivost - 120 dBm.
3. **LORNET 24**
   - Frekvenční rozsah 2400 - 2483 MHz;
   - maximální výkon 0,2 W;
   - hmotnost 0.7 kg;
   - citlivost - 108 dBm.

4. **LORNET 36**
    - Frekvenční rozsah 3580 - 3620 MHz;
    - maximální výkon 20 W;
    - hmotnost 1.4 kg;
    - citlivost - 110 dBm.
5. **ORION HX 24**
    - Frekvenční rozsah 2404 - 2472 MHz;
    - maximální výkon 3,3 W;
    - hmotnost 1.75 kg;
    - citlivost - 140 dBm.
6. **ORION HX 900**
    - Frekvenční rozsah 905 - 925 MHz;
    - maximální výkon 1.4 W;
    - hmotnost 1.6 kg;
    - citlivost - 130 dBm.
7. **ORION NJE 4000**
    - Frekvenční rozsah 880 - 1005 MHz;
    - maximální výkon 1.4 W;
    - hmotnost 1.54 kg;
    - citlivost - 133 dBm.
8. **ST 402 CAYMAN**
    - Frekvenční rozsah cca 2000 - 3000 MHz;
    - maximální výkon 2 W;
    - hmotnost 1.4 kg;
    - citlivost -v80 dBm.

4.3 Postup měření

V prvním experimentu bylo umístění jednotlivých OSZ prováděno v interiéru, v prázdném laboratorním prostředí bez jakýchkoliv elektronických součástek a zařízení a bez kovových součástek a mechanismů, které by mohly vytvářet falešné přechody, které by DNP mohl nesprávně vyhodnotit jako polovodičovou součástku. Zařízení interiéru tvořil pouze potřebný nábytek a vybavení pro účely měření. Bylo vybráno šest variant pro umístění, jednalo se o umístění ve vnitřním prostoru:

1. pod dřevotřískovou deskou kancelářského psacího stolu;
2. za zadní stěnou dřevotřískové šatní skříně;

3. v kancelářském kartonovém šanonu;
4. ve stropním půlkulatém skleněném světle s klasickou žárovkou;
5. v keramickém květináči;
6. ve stropním perforovaném podhledu z minerální vlny.

V kontrolovaném prostoru byla třikrát prověřována výše popsaná místa, ke kterým se v různých vzdálenostech od cca 50 cm do 0 cm přibližovaly postupně v různých směrech všechny tři výše zmíněné DNP a bylo ověřováno, zda detekují v okruhu cca 50 cm zde uložené OSZ. Všechny DNP byly nastaveny na 50% vysílací výkon. Podařilo-li se detekovat signálem 2. harmonické frekvence (signalizující přítomnost P/N přechodů) uschované zařízení v místě uložení, byť i minimálním signálem, byl naměřený výsledek zaznamenán jako pozitivní. Nepodařilo-li se naměřit žádnou hodnotu, byl DNP přepnut do plného výkonu a měření bylo zopakováno a výsledky zaznamenány.

V druhém experimentu bylo umístění jednotlivých OSZ (GSM odposlech a VKV rádio mikrofon) provedeno v interiéru staršího domu, který v době měření procházel kompletní rekonstrukcí. Představoval pro mě laboratorní prostředí, které bylo bez elektrických rozvodů, bez elektronických zařízení, pro detekci se jednalo o tzv. „čisté“ prostředí. Bylo vybráno šest variant pro umístění, jednalo se o umístění ve vnitřním prostoru domu, za zdmi různých šířek a materiálů, jednalo se o:

1. cihlová vnitřní zeď široká cca 30 cm;
2. cihlová vnější zeď široká cca 50 cm;
3. tvárnice značky Ytong, vnitřní zeď široká cca 30 cm;
4. sádrokartonová vnitřní stěna široká 15 cm;
5. dřevěná stěna z OSB desek široká 20 cm.

5 VÝSLEDKY

Při výběru detektorů nelineárních přechodů k provedení praktické části jsem vycházel z internetového katalogu firmy Spy Shop Praha, kde se nachází kompletní nabídka mnou vybraných přístrojů. Po provedení MKA budou zvoleny tři detektory, se kterými bude provedeno měření v laboratorních podmínkách k ověření jejich schopností detekce.

5.1 Multikriteriální analýza

K provedení analýzy byla vybrána následující kritéria, která jsem určil jako významná. Jedná se o: vysílací výkon, hmotnost, cena, možnost připojení sluchátek k zajištění tichého režimu detekce a komfort ovládání a ergonomie držení, která je nezbytná pro déletrvající manipulaci s přístrojem. Přičemž hmotnost a cena jsou kritéria minimalizační a výkon, komfort ovládání a tichý režim kritéria maximalizační.

Tabulka 1 – Seznam DNP s parametry

DNP	VÝKON	HMOTNOST	CENA	TICHÝ REŽIM	KOMFORT
LORNET 24	1 W	0.7 kg	215 000 Kč	100 %	100 %
ORION 2.4 HX	3.3 W	1.75 kg	721 000 Kč	80 %	100 %
ST 402 CAYMAN	2 W	1.4 kg	326 000 Kč	80 %	100 %
LORNET 36	20 W	1.4 kg	320 000 Kč	100 %	50 %
JJN EDD 24T	1 W	0.7 kg	307 000 Kč	100 %	80 %
ORION NJE	1.4 W	1.54 kg	623 000 Kč	80 %	50 %
ORION 900 HX	1.4 W	1.6 kg	721 000 Kč	80 %	60 %
LORNET 900	1 W	1.0 kg	215 000 Kč	100 %	50 %

(*ceny zjištěny v internetovém srovnávači cen Heureka.cz)

Tabulka 2 – Bodové hodnocení kritérií

DNP	*VÝKON*	HMOTNOST	CENA	TICHÝ REŽIM	KOMFORT
BODY	***7***	*6*	*5*	*4*	*8*

Tabulka 3 – Ideální a bazální varianta

DNP	*VÝKON*	*HMOTNOST*	*CENA*	*TICHÝ REŽIM*	*KOMFORT*
H	***20***	***0.7***	***215000***	***100***	***100***
D	***1***	***1.75***	***721000***	***80***	***50***

Tabulka 4 – Normalizované hodnoty

DNP	VÝKON	HMOTNOST	CENA	TICHÝ REŽIM	KOMFORT
LORNET	***0***	***1***	***1***	***1***	***1***
ORION 2.4 HX	***0,12***	***0***	***0***	***0***	***1***
ST 402 CAYMAN	***0,05***	***0,3432***	***0,78***	***0***	***1***
LORNET 36	***1***	***0,33***	***0,79***	***1***	***0***
JJN EDD 24 T	***0***	***1***	***0,82***	***1***	***0,6***
ORION NJE	***0,02***	***0,14***	***0,19***	***0***	***0***
ORION 900	***0,02***	***0,14***	***0***	***0***	***0,2***
LORNET 900	***0***	***0,71***	***1***	***1***	***0***
VÁHY	***0,23***	***0,2***	***0,17***	***0,13***	***0,27***

Tabulka 5 – Hodnoty váženého součtu

DNP	VÁŽENÝ SOUČET
LORNET 24	0,77
ORION HX 2.4	0,2976
ST 402 CAYMAN	0,4821
LORNET 36	0,5603
JJ EDD 24 T	0,6314
ORION NJE	0,0649
ORION 900	0,0866
LORNET 900	0,442

Tabulka 6 – Pořadí variant

DNP	VÁŽENÝ SOUČET
LORNET 24	0,77
JJ EDD 24 T	0,6314
LORNET 36	0,5603
ST 402 CAYMAN	0,4821
LORNET 900	0,442
ORION HX 2.4	0,2976
ORION 900	0,0866
ORION NJE	0,0649

[22]

K laboratornímu měření jsem po provedené MCDA vybral tři typy DNP, které pracují s frekvencí v rozsahu 2-3 GHz. Tyto budou procházet testy. Zmíněnou úroveň signálu výrobci deklarují jako schopnou odhalit rádiové vysílače, registrační zařízení, mobilní telefony, kamery, GPS lokátory a další druhy moderní odposlechové techniky.

Vybrán byl Lornet 24, Orion HX 2.4 pro moderní a vyspělé ovládání s pokročilými funkcemi a ST 402 Cayman pro snadné ovládání, dobrou ergonomii držení, která je nezbytná pro déletrvající činnost v prověřovaném

prostoru. Detektor JJ se mi v době prováděného testování bohužel nepodařilo sehnat, neboť jej prodejce aktuálně neměl k dispozici.

Detektory Lornet 36 a Lornet 900 jsem záměrně nevybral k testování i přes dobré umístění v tabulce, neboť jsem stanovil požadavek na otestování detektorů od různých výrobců.

5.2 Detekce OSZ

Získané výsledky jsou zapsané v pořadí provedeného měření (poloviční/plný výkon). Nejprve bylo se všemi DNP měřeno na 50% výkon a pakliže se nepodařilo detekovat ukryté zařízení, bylo měření zopakováno se 100% výkonem. Při pozitivní detekci 2. harmonické frekvence bylo v tabulce vyznačeno znakem (●), při negativním (×).

Vybrány byly výše zmíněné tři typy detektorů. Jednalo se o zánovní modely, které již byly před mým testováním používány. Funkčnost vybraných detektorů jsem ověřil na zkušebních vzorcích (2. a 3. harmonické frekvence – jedná se o uzavřené plastové tuby, ve kterých jsou uložené polovodičové součástky v případě druhé harmonické frekvence nebo s kovovými součástkami, které mají představovat třetí harmonickou frekvenci). Tyto testery jsou jako příslušenství dodávány od výrobce spolu s detektorem. U všech třech DNP se funkčnost ověřila.

Při praktickém měření byly porovnávány nejprve dle schopností odhalení konkrétního OSZ v potenciálně reálných umístěních, posléze byla zjišťována schopnost penetrace různými stavebními materiály.

V níže uvedených tabulkách jsou zaznamenány naměřené údaje získané při pokusu o detekci vybraných šesti odposlechových zařízení, která byla postupně ukrývána na zvolená místa.

Tabulka 7 – Detekce GSM/GPS odposlechu

DNP	Stůl kancelářský	Skříň kancelářská	Stropní světlo	Šanon	Květináč	Stropní podhled
Lornet	×/●	×/●	×/×	●	×/●	●
Orion	×/×	●	●	●	●	●
Cayman	×/●	×/●	×/×	×/×	×/×	×/●

Kombinace vysílače v uzavřeném pouzdře a silné nebo lesklé překážky odrážející elektromagnetické vlny činila detektorů problém.

Tabulka 8 – Detekce kamery skryté v peru

DNP	Stůl kancelářský	Skříň kancelářská	Stropní světlo	Šanon	Květináč	Stropní podhled
Lornet	×/×	×/×	×/×	×/×	×/×	×/×
Orion	×/●	×/●	×/×	●	×/●	×/●
Cayman	×/×	×/×	×/×	×/×	×/×	×/×

Kamera se podařila odhalit ve vybraných případech pouze detektoru Orion HX.

Tabulka 9 – Detekce záznamníku Sony

DNP	Stůl kancelářský	Skříň kancelářská	Stropní světlo	Šanon	Květináč	Stropní podhled
Lornet	×/●	●	×/●	●	×/●	●
Orion	●	●	●	●	●	●
Cayman	×/●	×/×	×/●	×/●	×/●	●

Odhalení klasického záznamníku nečinilo zvoleným detektorům problémy.

Tabulka 10 – Detekce MT Nokia

DNP	Stůl kancelářský	Skříň kancelářská	Stropní světlo	Šanon	Květináč	Stropní podhled
Lornet	●	×/×	×/●	●	×/●	●
Orion	●	×/●	×/●	●	×/●	●
Cayman	×/×	×/×	×/×	×/●	×/×	×/●

Starší typ mobilního telefonu v plastovém obalu nečinil při detekci problém. Největší překážku tvořila 50 cm široká šatní skříň (prázdná).

Tabulka 11 – Detekce MT iPhone

DNP	Stůl kancelářský	Skříň kancelářská	Stropní světlo	Šanon	Květináč	Stropní podhled
Lornet	×/●	×/×	×/×	●	×/×	×/●
Orion	●	×/●	×/●	●	×/●	×/●
Cayman	×/×	×/×	×/×	×/×	×/×	×/×

Mobilní telefon v kovovém obalu znesnadňoval detekci, stejně tak jako silná nebo lesklá překážka, která brání průchodu vysílaného signálu.

Tabulka 12 – Detekce VKV rádio mikrofonu

DNP	Stůl kancelářský	Skříň kancelářská	Stropní světlo	Šanon	Květináč	Stropní podhled
Lornet	×/●	×/×	×/●	●	●	●
Orion	●	×/●	×/●	●	●	●
Cayman	×/●	×/×	×/×	●	×/●	●

Rádiový odposlechový prostředek je vybaven nezbytnou externí anténou. Ta usnadňuje detekci polovodičových součástek, od kterých je vyvedena mimo obal samotného zařízení.

5.3 Měření penetrace

Schopnost penetrace vysílaného signálu a následného zpětného zachycení a vyhodnocení detektorem jsem ověřil na vybraných běžně používaných stavebních materiálech. Naměřené údaje jsou zaznamenané v tabulkách.

Tabulka 13 - Cihlová zeď, šířka 30 cm

DNP	GSM	Rádiový odposlech
Lornet	●	●
Orion	●	●
Cayman	×/●	●

Cihlová třiceticentimetrová zeď představuje vnitřní zdi interiéru, detektorům nečiní problém.

Tabulka 14 - Cihlová zeď, šířka 50 cm

DNP	GSM	Rádiový odposlech
Lornet	×	×
Orion	×	×
Cayman	×	×

Cihlová padesáticentimetrová zeď představuje obvodové zdi domů, bytů apod. Detektorům znemožňuje detekci.

Tabulka 15 – Tvárnice značky Ytong, šířka 30 cm

DNP	GSM	Rádiový odposlech
Lornet	●	●
Orion	●	●
Cayman	●	●

Tvárnice z lehkého betonu představují obvodové nebo vnitřní zdi. DNP nečiní problém.

Tabulka 16 - Sádro kartonová stěna, šířka 15 cm

DNP	GSM	Rádiový odposlech
Lornet	●	●
Orion	×/●	●
Cayman	●	×/×

Sádrokarton se využívá pro stavbu vnitřních zdí a stropů.

Tabulka 17 - Stěna z OSB desek, šířka 20 cm

DNP	GSM	Rádiový odposlech
Lornet	✕/●	●
Orion	●	●
Cayman	✕/●	●

OSB desky se využívají pro stavbu vnitřních stěn a stropů.

5.4 Ověření hypotéz

H 1 Všechny typy odposlechové a sledovací techniky lze odhalit pomocí detektorů nelineárních přechodů.

HYPOTÉZA Č. 1 BYLA VYVRÁCENA

(*k vyvrácení došlo měřením uvedeným v tabulce 8 a 11)*

H 2 Odhalení profesionálně umístěného odposlechového prostředku laikem není možné.

HYPOTÉZA Č. 2 NEBYLA VYVRÁCENA

(nebyla vyvrácena neboť žádné z provedených měření neukazuje na to, že by bylo možno hypotézu vyvrátit)

H 3 Detektor nelineárních přechodů detekuje všechna zařízení vybavená polovodičovými součástkami.

HYPOTÉZA Č. 3 BYLA VYVRÁCENA

(to, že detektory dokážou odhalit všechna zařízení vybavená polovodičovými součástkami je nepravda, což je dokázáno na základě výsledků měření v tabulce č.8 a 11)

6 DISKUZE

V předložené práci jsem se snažil zmapovat současné trendy a možné způsoby odposlouchávání a získávání informací. Především pak možnosti ochrany a způsoby odhalení těchto prostředků.

6.1 Odposlechová technika

V České republice se nabízí odposlechové prostředky od základních rádiových v pásmu VKV po vyspělé v pásmu UHF s dosahem stovek metrů, zaručující kvalitní přenos signálu a snadné pronikání zdmi budov. Jsou vybavené digitální modulací signálu, která poskytuje přenášené informaci ochranu při jejím zachycení neoprávněnou osobou. Díky vědecko-technickému pokroku jsou odposlechová zařízení miniaturní, kvalitní, levná a tím pádem dostupná. Security magazín ročník 2002 na str.8,9 [23] uvádí v této době jako nejčastěji využívané systémy rádiové odposlechy v pásmu VKV, které jsou nejrozšířenější a specializované firmy je nabízejí k instalaci do jakýchkoliv předmětů. Dnes je naopak využíváno frekvenční pásmo UHF a pásmo mobilních telefonů. Montáž odposlechových prostředků do různých předmětů nabízejí firmy nadále, ale jedná se spíše o technologii GSM, která se v té době teprve začínala využívat v podobě soudobých upravených mobilních telefonů. Mé tvrzení potvrzuje článek Magazínu Security na str.16 [24] Cenová hladina některých OSZ je v současné době nastavena v některých případech i 100krát níže [23]. GSM odposlechům a registračním zařízením-záznamníkům patří na trhu největší díl v celkové nabídce [25]. Vyrábějí se v různých provedeních, zpravidla v černém plastovém obalu. Liší se rozměry, provedením a samotným vzhledem. Odlišnou mají délku výdrže na jedno nabití, zpravidla dle velikosti a kapacity akumulátoru. Nabízí se základní provedení, až po ty vybavené detekcí pohybu, zvuku apod. Jsou v provedení předmětů denní potřeby nebo v předmětech, které se nachází v téměř každé domácnosti nebo kanceláři.

Možnost odhalení je pro neznalou osobu nemožná. V případě instalací do prodlužovacích zásuvek, počítačových myší, klávesnic apod. je jejich životnost limitována výdrží zařízení samotného nebo odposlechového. Při poruše se zpravidla nahradí novým, a tak jejich uživatel ani nemusí zjistit, že byl odposloucháván. Někteří prodejci nabízí možnost instalace do předmětů, které si přinesl sám zákazník. Odposlouchávané osobě tak v místnosti nic „nepřibyde“ a hledá-li při podezření „krabičku“ přilepenou pod deskou stolu, končí pátrání brzy neúspěchem.

Sehnálek ve své diplomové práci z roku 2009 na str. 19 [26] uvádí nejčastěji využívané rádiové odposlechy, především pak v pásmu UHF. GSM odposlechy zmiňuje spíše jako speciálně upravené mobilní telefony sloužící jako OSZ a další způsob využití GSM pásma uvádí odposlech mobilního telefonu zachycováním komunikace prostřednictvím IMSI Catcheru. Tento způsob ve své práci v teoretické části pouze zmiňuji, neboť se jedná o zařízení určené pro bezpečnostní a zpravodajské složky státu, které není volně dostupné k prodeji. Takto prováděnému odposlechu se nelze ubránit, což pokládám za správné, je-li splněna podmínka předchozí věty.

6.2 Kybernetická bezpečnost

Internetové připojení, které dnes využívá většina smartphonů, tabletů, počítačů nebo zařízení internetu věcí přináší nová rizika a nové cesty pro útočníky. Je možné jejich prostřednictvím zachytávat zvuk, obraz nebo data. Kybernetické útoky tak nejsou jen doménou filmů nebo velkých firem, na jejichž systémy útočí hackeři. S internetem věcí může být obětí každý uživatel této fascinující techniky.

Jak ukazuje článek M. Stančíka Odposlechy chytrých televizí. [27] Některé modely televizorů Samsung vybavené hlasovým ovládáním mohou být pro své uživatele potenciálním rizikem, neboť hlasové pokyny se prostřednictvím

zabudovaného mikrofonu předávají třetí straně. Samsung v prohlášení uvedl, že funkce je pro uživatele bezpečná, volitelná a lze ji vypnout. Problém kybernetických útoků na mikrofony internetu věcí potvrzuje též článek v Chip magazínu [28], který poukazuje na možnost zneužití hlasového ovládání zařízení nejen od firmy Samsung.

Podobný problém je s GPS lokátory, které si lidé dobrovolně pořizují pro své děti, zvířata, věci, o které mají strach a chtějí mít přehled o jejich aktuálním výskytu. Na některé typy je možné zavolat a poslouchat, co se děje v jejich okolí. Přístup k datům tak může mít nejen uživatel, ale někdy také třetí strana. Společnost Avast ve svém článku [29] uvádí, že statisíce levných GPS lokátorů z asijské produkce nemá žádné nebo jen slabé zabezpečení a získaná data odesílají do cloudu, včetně přesných do souřadnic v reálném čase.

Každý by měl zvážit, zda opravdu potřebuje mít zařízení, které má přístup na internet a jeho prostřednictvím přenáší data. Pakliže ano, je nutné věnovat patřičnou péči zabezpečení. Především u zařízení internetu věcí mít nejnovější verzi firmwaru do všech zařízení v síti a provádět pravidelné aktualizace. Centrálou chytré domácnosti je Wi-Fi router, jeho zabezpečení pomocí silného hesla je nezbytností. Mé tvrzení potvrzuje článek časopisu Chip [30], ve kterém odborníci doporučují minimálně 15 - 20 znaků z náhodně poskládaných slov.

Nikdo z nás by nechtěl zjistit, že cizí osoba má přístup do našeho počítače, telefonu, k záznamu domácí IP kamery, že někdo poslouchá naše děti přes interaktivní hračky nebo že někdo může ovládat vybavení našeho domu bez našeho přičinění apod. Na to vše by měl každý myslet a ochrana by měla být stejně tak sofistikovaná, jako možnosti zařízení, jak uvádí také D. Řeháček ve svém článku. [31]

Ne vždy je nutné a účinné použití speciálních přístrojů nebo softwaru k zamezení činnosti mikrofonů a kamer. Má-li někdo obavu z jejich zneužití na svém zařízení, nabízí se prosté řešení. Zaslepení kamery a mikrofonu běžnou lepicí páskou. Účinnost zaslepení mikrofonu lze ověřit příslušným hlasovým

povelem, který by při správném přelepení neměl být splněn. V případě kamery tuto lze překrýt posuvnou krytkou, která bývá někdy součástí kamer nebo jde dokoupit jako samostatné příslušenství.

6.3 Rozbor praktické části

Provedení praktické části jsem směřoval na použití OSZ laiky nebo odborně zdatnými amatéry v běžném soukromém nebo pracovním životě. Jde-li o získání informací, zaznamenání průběhu jednání, získání kompromitujících nahrávek, nabízí se možnost použití komerčních, volně dostupných OSZ nebo zařízení, které lze k tomuto účelu použít. Místa instalace jsem zvolil tak, aby byla dobře přístupná a umožňovala možnost rychlé instalace. V laboratorních podmínkách jsem nasimuloval šest možných způsobů ukrytí OSZ a pokoušel se detekovat jejich přítomnost vybranými detektory nelineárních přechodů. Ty jsem zvolil na základě provedené multikriteriální analýzy, která dle mnou nastavených kritérií určila nejvhodnější přístroje. V současnosti jsou na trhu k dispozici DNP ve frekvenčním spektru od 900 MHz po 3600 MHz. Security magazín v roce 2002 na str. 20 [23] a M. Sehnálek v roce 2009 na str. 43 [26] se zmiňují pouze o DNP pracujících v pásmu 900 MHz. Dnes se naopak využívá multifrekvenčního spektra a různé typy detektorů s rozdílným frekvenčním pásmem by měly umět vyhledávat různé druhy elektroniky. Dříve používané typy DNP jsou stále v prodeji s mírnými úpravami, což svědčí o jejich opodstatnění při vyhledávání různých typů elektroniky. Výrobci Elvira [32], REI [9] a prodejce Spy obchod [33] uvádí vysílací frekvenci 2400 MHz vhodnou ke spolehlivé detekci moderních miniaturních polovodičových nelineárních součástek, kterými jsou osazovány moderní odposlechová zařízení. Z tohoto důvodu jsem dal této frekvenci vysokou prioritu při výběru DNP. Stejný parametr frekvence považuji za rovné podmínky pro detekci.

Na prvním místě v MCDA se umístil DNP ruského výrobce Elvira typ Lornet 24, který výrobce [32] a prodejce Odposlechy.com [33] označuje za detektor spolehlivě detekující odposlechové prostředky všech typů. Polovodičové prvky jako jsou diody, tranzistory, mikročipy apod. ke kterým jsou přivedeny antény.

Druhým detektorem pro měření byl ST 402 Cayman [11], který vysílá v multifrekvenčním pásmu 2000 – 3000 MHz, u kterého výrobce [32] a prodejce [33] deklaruje schopnost detekování jak registračních zařízení, tak odposlechů předávajících informace rádiovou cestou.

Jako třetí typ jsem zvolil Orion HX 24 [9], neboť emituje shodnou vysílací frekvenci 2400 MHz, která dle výrobců aktivuje polovodičové nelineární součástky a je vhodnější k detekci moderních elektronických obvodů. Umožňuje efektivní detekci a lokalizaci každého elektronického zařízení a měl být schopen odhalit miniaturní, vyspělá odposlechová zařízení. [33]

Provedeným měřením schopností detekce jsem zjistil, že různé detektory mají různé schopnosti.

Vezmu-li detektor Lornet 24, tak po provedeném měření konstatuji, že dokázal dle deklarace prodejce [33] odhalit mobilní telefony, GSM odposlech a některá zařízení vybavená polovodičovými součástkami. V případech, kdy jsou ukryté je nutné využít plného výkonu k jejich detekci. Nepodařilo se odhalit při žádném měření skrytou kameru v peru, která je vyrobena za pomoci miniaturních integrovaných obvodů technologií SMD (povrchová montáž miniaturních součástek), které jsou uložené v pouzdře, kterým elektromagnetické vlny neprojdou. Částečně se podařilo odhalit ukrytý mobilní telefon iPhone. Problémem ve všech případech byla kancelářská skříň, která bránila průchodu záření. Při měření penetrace různými materiály obstál ve všech měřeních, až na 50 cm silnou cihlovou zeď, kterou ale neprozářil žádný z testovaných detektorů.

Orion HX 24 dosáhl při laboratorním měření nejlepších výsledků. Jako jediný dokázal detekovat skrytou kameru v peru. Neodhalil ji pouze v případě, kdy byla ukrytá ve stropním svítidle. V tomto případě byl skleněný kryt světla překážkou pro volný průchod elektromagnetických vln, tak jako v případě, kdy byl GSM odposlech ukrytý pod deskou kancelářského stolu. Při měření penetrace dosáhl téměř totožných výsledků jako Lornet 24, ale k detekci mu dostačoval nastavený poloviční výkon.

Detektor ST 402 Cayman měl s detekcí ukrytých zařízení největší problémy, především pak se zařízeními novodobými, typu mobilní telefon iPhone nebo skrytá kamera v peru. Dle deklarace výrobce a prodejce uspěl při detekci odposlechů, využívající k přenosu informací rádiovou cestu, ne však při detekci registračního zařízení, za které lze považovat skrytou kameru se záznamem zvuku a telefon iPhone. Při měření penetrace měl problém pouze v případě odhalení rádiového odposlechu, který byl ukryt za sádro kartonovou zdí.

Po provedeném měření konstatuji, že tvrzení prodejců a výrobců o tom, že detektory dokážou odhalit veškerou elektroniku, lze použít pouze v případě, že by byly volně položené a DNP k němu měl přímý přístup. V případě, že jsou elektronická zařízení skryta nebo elektronické obvody jsou uloženy v pouzdře, kterým obtížně prochází elektromagnetické vlny, je detekce obtížná nebo nemožná. Nelze se tedy při prováděné obranně technické prohlídce spolehnout na měření DNP, ale je nutná kombinace různých metod, včetně fyzické kontroly. Ta je nezbytná v případech, kdy se kontrola DNP provádí v místě, kde se nachází jiná elektronika, která při prověřování spouští pozitivní detekci, která je způsobena samozřejmou přítomností polovodičových součástek. Je tedy nezbytné tuto elektroniku prověřit, zda v sobě neobsahuje navíc umístěné nežádoucí zařízení. Druhý zásadní problém při činnosti s DNP spatřuji v činnosti při využití plného potenciálu detektoru, který byl při některých měřeních nezbytný. Režim plného výkonu detekuje elektronická zařízení v širším okolí a neposkytuje tak objektivní informace o kontrolovaném

prostoru, neboť velmi často signalizuje detekci polovodičových součástek v širším okolí. Reálná činnost v běžně vybaveném prostoru v takovém režimu není možná. Režim na plný výkon si lze představit v prázdném prostoru bez elektronických zařízení jak v kontrolovaném prostoru, tak např. i za zdmi kontrolovaného prostoru. Po provedeném měření penetrace je jisté, že DNP detekují i elektroniku umístěnou za zdí.

Ideální prostředí pro měření penetrace vybraných detektorů se pro mé pokusné měření nacházelo v rekonstruovaném starém domě, kde se nacházely různě silné obvodové a vnitřní zdi z různých stavebních materiálů. Dva typy odposlechových zařízení (GSM a VKV) jsem připevnil na zeď a z druhé strany se pokoušel zařízení detekovat. Bylo tak nasimulováno použití OSZ v případě, že není možné se dostat do zájmového prostoru a je nutné skrz zeď vyvrtat do prostoru miniaturní otvor pro průchod plastové nebo kovové trubičky, která slouží jako zvukovod, na jehož konci je umístěn citlivý jehlový mikrofon, který snímá zvuk z prostoru. Takovou technologii popisuje Magazín Security str. 7 [23]. Otvory se vrtají mimo zorné pole, dle umístění šikmo dolů nebo nahoru pro zabránění odhalení. Měřením bylo zjištěno, že prostup signálu třiceticentimetrovou zdí z cihel nebo tvárnic je možný. Stejně tak v případě zdí z OSB desek nebo sádrokartonu. Sádrokarton byl překážkou pouze pro ST-402, který nedetekoval rádiový odposlech. Sádrokarton je tvořen rozemletou sádrou a kartonem, případně doplněný skelnými vlákny. Tato kombinace může mít negativní vliv na prostup signálu v kombinaci s plechovými sešroubovanými profily, na které jsou panely přichyceny. Jedná se o nehomogenní prostředí, které je technicky nevhodné pro průchod elektromagnetických vln, jak je uvedeno v článku Elektromagnetické vlny v nevodivém izotropním prostředí na str. 97 [34]

V případě obvodové 50 cm široké zdi se detekce již nezdařila ani při použití plného výkonu. Žádný DNP nedokázal detekovat za zdí uložený odposlechový prostředek.

6.4 Hypotézy

Hypotéza č. 1 *Všechny typy odposlechové a sledovací techniky lze odhalit pomocí detektorů nelineárních přechodů*.

Provedeným měřením bylo zjištěno, že určitými typy detektorů nelineárních přechodů není možné odhalit některé odposlechové prostředky. Mé zjištění je v rozporu s tvrzením prodejce DNP, který uvádí na svých webových stránkách, že určité typy DNP odhalí veškeré druhy sledovacích zařízení. [33]

Hypotéza č. 2 *Odhalení profesionálně umístěného odposlechového prostředku laikem není možné.*

Nebyla vyvrácena, protože žádné z provedených měření neukazuje na to, že by bylo možno hypotézu vyvrátit. Mé tvrzení o nemožnosti odhalení profesionálně umístěného odposlechu laikem potvrzuje článek J. Schmidta ze společnosti Probin na str.17 [24] a článek společnosti EO Security [35]. Obě společnosti se zabývají profesionálním vyhledáváním OSZ.

Hypotéza č. 3 *Detektor nelineárních přechodů detekuje všechna zařízení vybavená polovodičovými součástkami*.

Měřením bylo prokázáno, že ne všechna zařízení tvořená polovodičovými součástkami lze odhalit detektory nelineárních přechodů. Především v případech, jsou-li v obalech a v pouzdrech, které odráží vyslaný signál, jak potvrzuje článek o průchodu elektromagnetického záření n str. 97. [34]

Měření bylo prováděno mnou vybranými detektory, které jsem měl zapůjčené k laboratornímu měření. Jednalo se o zánovní přístroje, které již byly používané. Nelze tedy vyloučit, že měření jiným detektorem stejného typu by mohlo mít odlišné výsledky. Nelze ani vyloučit, byť i menší vnitřní poškození např. antény, způsobené užíváním, které by mohlo mít případný vliv na měření a zkreslit tak výsledky.

6.5 Lze vůbec najít odposlech?

Jak je vlastně možné zjistit, že je někdo odposloucháván a lze vlastně najít vlastními silami odposlech? Máme-li podezření, že z našeho soukromí nebo pracovních jednání unikají informace, které jsme dále nesdělovali, máme důvod k obavám. Indicií by mohlo být zjištěné neoprávněné vniknutí do objektu, nápadné stavební úpravy, změny v místnosti (nová malba nebo její část, zbytky omítky) nebo neobvyklá manipulace s vybavením a nábytkem. Zní to paranoidně, ale možné signály to jsou. Přítomnost OSZ mohou značit i případné interference (rušení) u elektrických zařízení, např. při poslechu rádia nebo televizoru. Ty by mohly být způsobeny případným vysílačem.

Příčinou úniku informací může být také špatná osobní bezpečnostní hygiena. Užívání mobilních telefonů a počítačů, které nemáme plně ve své moci a může tak do nich někdo nainstalovat škodlivý software. Stejně tak slepé a oddané otevírání emailů od neznámých adresátů, stahování programů a aplikací z nedůvěryhodných zdrojů, které mohou obsahovat malware a infikovat tak používané zařízení. Problémem je dobrovolný souhlas k předávání informací třetím stranám při užívání různých zařízení nebo aplikací také není nejbezpečnější činností a neměli bychom ho dělat automaticky, jen proto, že se nám nechce číst smluvní podmínky.

6.6 Porovnání legislativy v České a Slovenské republice

Prostorový odposlech má nezastupitelné místo v trestním řízení při vyšetřování závažné trestné činnosti. Poskytuje orgánům činným v trestním řízení nezkreslené informace o trestné činnosti. Zároveň je to ale velmi hrubý zásah do soukromí, který musí mít pádný důvod. Nasazení prostorového odposlechu je povoleno na stanovenou dobu soudcem a samotné vyšetřování je vedeno pod dohledem státního zástupce. Zde se však zmiňuji o zákonném, legálním odposlechu. V běžném životě nic takového potřeba není. Samotné

použití OSZ není v České republice trestným činem. Pomoc od orgánů činných v trestním řízení lze očekávat pouze v případě, že bylo k jeho umístění neoprávněně vniknuto do objektu překonáním překážky. Nedotknutelnost obydlí chrání ustanovení *§ 178 tr. zákoníku Porušování domovní svobody*. V případě, že někdo získá informace, které jsou přenášené elektronickou cestou (datové, textové, zvukové zprávy), připadá v úvahu skutková podstata trestného činu *Porušení tajemství dopravovaných zpráv dle § 182 tr. zákoníku.* To je zaručeno čl.13 Základní listiny práv a svobod. [19] Mé tvrzení podporuje také článek Security magazínu**.** [23]

Inspirací by pro nás mohlo být slovenské trestní právo, které je v ochraně soukromí dále. Trestný zákon Slovenské republiky č. 300/2005 Z.z. řeší stejně tak jako naše právo, porušování domovní svobody, ale také použití OSZ samostatným paragrafem *194a TZ Trestný čin ochrany súkromia v obydlí,* který chrání soukromí, soukromý a rodinný život v obydlí jako osobní hodnotu. Trestný čin naplní úmyslné porušení práva jiného na jeho soukromí v obydlí, na jeho soukromý a rodinný život, a to neoprávněným sledováním jeho obydlí, poznatky o jeho životě a životě osob, které se v obydlí zdržují. Řeší použití informačně technických prostředků a jiných technických prostředků.
Porušování tajemství přepravovaných zpráv řeší třemi samostatnými paragrafy. Přičemž § 196 a § 197 poskytuje ochranu informacím přenášeným prostřednictvím elektronické komunikace nebo přenos neveřejných dat, které ještě nebyly doručeny nebo které doručeny již byly. Paragraf 198 TZ *Porušovania tajomvstva prepravovaných správ* řeší ochranu informací přenášených prostřednictvím elektronické komunikace, které pachatel zachytí na zařízení způsobilé odposlechu nebo zaznamenání přenášených informací. [36]

Slovenské právo by mělo být inspirací pro naše zákonodárce, kteří by měli zajistit větší ochranu společnosti před lidmi, kteří se nebojí ohrožovat a narušovat právo na soukromí. Dle mého názoru se nikdo nebude ostýchat

používat odposlechová a sledovací zařízení, pakliže bude vědět, že mu za takové jednání nehrozí žádný, nebo jen minimální postih.

Náš právní řád neposkytuje jinou ochranu než tu, kterou jsem zmínil. Je tak na každém, aby se o svou bezpečnost postaral sám a nedal šanci jedincům, kteří nemají zábrany před uvedeným jednáním. Na našich zákonodárcích je, aby tuto mezeru v zákoně vyplnili a aby případným pachatelům hrozil trestní postih, který je odradí od takového jednání.

6.7 Shrnutí

Jak účinná může být obrana proti odposlechovým prostředkům? Dnešní trh nabízí nepřeberné množství techniky a zařízení, vůči kterým je obtížné se bránit. Defenzíva bude vždy pozadu, protože ofenzivní prostředky lze konstruovat tak, aby odolávaly odhalení současnou obrannou technikou, některé dokonce odhalit nelze. Šance na odhalení ale vždy bude, neboť fyzikální jevy a zákonitosti nezmizí.

Důležité je profesionální, soudobé vybavení, odborné proškolování a neustálé vzdělávání v dané oblasti.

Je však nutné počítat s tím, že některá zařízení k získávání informací, jako laserový odposlech nebo IMSI Catcher (systém simulující základnovou stanici GSM sítě tzv. BTS, které slouží k přenosu signálu mobilních telefonů a je tak možné zachytávat jejich komunikaci), se mohou také vyskytovat. Takovým způsobům odposlechu se nelze bránit. Hodnota informace, která má být získána, se musí rovnat cenám použité techniky, neboť použití takových zařízení nebude levnou záležitostí, když pořizovací cena je v milionech korun. Možnost použití IMSI Catcheru nebude veřejnou záležitostí, neboť je to zákonem zakázáno. I přes to, že se jedná o techniku určenou pro státní bezpečnostní složky, není vyloučeno její vlastnictví některými bezpečnostními agenturami.

Z toho plyne, že důležité informace by se neměly projednávat po telefonu, komunikačních aplikacích, v rizikových a neprověřených místech. Někdy však postačí zabránit přítomnosti nedůvěryhodných a upovídaných lidí.

7 ZÁVĚR

Cílem předložené diplomové práce bylo popsat možnosti obrany proti odposlechovým prostředkům a jiným nezákonným způsobům získávání informací.

Vyhledávání ukrytých odposlechových prostředků jsem v teoretické části přiblížil popisem metod a činností, které vedou k jejich odhalení. Uvedl jsem speciální techniku určenou k provádění obranných technických prohlídek. Obranná technika je, oproti té odposlechové, řádově v deseti až stonásobcích dražší než samotné útočné prostředky.

Provedeným přehledem současných trendů v komerční odposlechové a sledovací technice jsem zjistil, že soudobá odposlechová zařízení jsou vybavena moderními technologiemi, jsou levná, sofistikovaná a volně dostupná. Tudíž je může kdokoliv zakoupit, vlastnit a používat. Do budoucna budou největší hrozbou kybernetické útoky, díky všudypřítomnému internetu.

V praktické části jsem pomocí multikriteriální analýzy vybral tři typy detektorů nelineárních přechodů a s nimi následně otestoval schopnosti vyhledávání ukrytých odposlechových prostředků. K tomu jsem si stanovil tři hypotézy. Po provedených měřeních se mi podařilo dvě hypotézy vyvrátit a jednu se mi vyvrátit nepodařilo.

Práce mě utvrdila v tom, že nalezení odposlechového prostředku a samotné zjištění, že nás někdo sledoval, nebude pro nikoho příjemnou záležitostí. Je to zásah do osobní svobody a značná ztráta soukromí, které bereme ve svých domácnostech a kancelářích za samozřejmost. Ochranu bych očekával po právní stránce, kdy by měla být jasně dána výše hrozícího trestu pro případného pachatele.

Ochrana před odposlechovými prostředky a kybernetickými útoky bude vždy složitější než samotný útok, ale možná je. Záleží na konkrétní situaci, jakou formu obrany a ochrany kdo zvolí. Udržet nezbytné vzájemné tempo se

stále se vyvíjejícími odposlechovými prostředky bude ale pro obranu finančně nákladné.

Psaní práce pro mě bylo velkým přínosem. Jsem rád, že jsem mohl prostudovat mnoho informačních zdrojů, zabývajících se ochranou informací, a že jsem mohl hovořit s lidmi zabývajícími se bezpečnostní problematikou. Také, že jsem mohl absolvovat testování s detektory nelineárních přechodů a zjistit jejich reálné možnosti.

V budoucnu by bylo vhodné samostatné zpracování rizika kybernetických hrozeb od stále se vyvíjejících a rozšiřujících se zařízení chytré domácnosti a osobních „chytrých“ zařízení, která mají lidé neustále při sobě.

8 SEZNAM POUŽITÝCH ZKRATEK

ADSL přístup na internet přes vedení telefonní linky

AM\FM amplitudová \ frekvenční modulace

DNP detektor nelineárních přechodů

EZS elektronický zabezpečovací systém

GPS celosvětový polohový systém (družicový)

GSM nejrozšířenější systém globální mobilní komunikace

IMSI jednoznačné identifikační číslo účastníka

IMSI Catcher zařízení umožňující odposlech mobilních telefonů

IP kamera síťová kamera přenášející záznamy přes IP síť

MALWARE škodlivý software

MCDA vícekriteriální rozhodovací analýza

MT mobilní telefon

OSZ odposlechové a sledovací zařízení

OTP obranná technická prohlídka

SBS soukromá bezpečnostní služba

SIM identifikační karta účastníka v mobilní síťi (částečně slouží jako paměť)

UHF frekvenční rozsah – ultra krátké vlny

USB univerzální sběrnice pro připojení periferií k PC, mobilu apod.

VF vysoko frekvenční

VOX systém detekce hluku

Wi-Fi bezdrátové lokální sítě pracující v bezlicenčním frekvenčním pásmu

9 SEZNAM POUŽITÉ LITERATURY

1. CHURAŇ, Milan. *Encyklopedie špionáže*. Vydání druhé. Praha: Libri, 2000. 432 s. ISBN 80-7277-020-9.
2. Chip. Magazín o digitálních technologiích. Břeclav: Moravia press, 2019. ISSN 2336-4793.
3. Stránky spol. Tango s.r.o.: Odposlech klávesnice Keylog USB TIME s podporou českých znaků a časovým razítkem [online]. [cit. 2020-03-29]. Dostupné z: https://www.odposlechy.com/odposlech-klavesnice-keylog-usb-time-s-podporou-ceskych-znaku-a-casovym-razitkem-stara-verze
4. BRABEC, František a kol. *Ochrana bezpečnosti podniku*. Vydání první. Praha: Eurounion, 1996. 203 s. ISBN 80-85858-29-0.
5. Security magazín. Praha: FAMily media, 2002. ISSN 1210-8723.
6. BRABEC, František a kol. *Bezpečnost pro firmu, úřad, občana*. Vydání první. Praha: Public History, 2001. 400 s. ISBN 80-86445-04-6.
7. Stránky spol. Tango s.r.o. Technický list produktu RFD-5 [online]. [cit. 2019-11-07]. Dostupné z: https://www.odposlechy.com/univerzalni-detektor-odposlechovych-zarizeni-rfd-5
8. PACNER, Karel. *Velmistři špionáže*. Vydání první. Praha: Plus, 2015. 438 s. ISBN 978-80-259-0464-0.
9. Stránky spol. Research Electronics International, LLC. Detektory nelineárních přechodů Orion 2.4 HX [online]. Cookeville, USA [cit. 2020-02-29]. Dostupné z: https://reiusa.net/nljd/orion-2-4-hx-nljd/
10. Stránky spol. Tango s.r.o. Detektory nelineárních přechodů [online]. [cit. 2019-11-07]. Dostupné z: https://www.odposlechy.com
11. Stránky spol. Selcom security. Detektory nelineárních přechodů [online]. Litva [cit. 2020-02-29]. Dostupné z: https://www.selcomsecurity.com/en/products/data-leakage-channels-detection/itemlist/category/51-nljd-non-linear-junction-detectors

12. STILWELL, Alexander. *Hon na člověka*. Vydání první. Praha: Naše vojsko, 2016. 320 s. ISBN 978-80-206-1629-6.
13. POVOLNÝ, Daniel. *Operativní technika v rukou StB*. Vydání první. Praha: Úřad dokumentace a vyšetřování zločinů komunismu PČR, 2001. 110 s. ISBN 80-902885-3-7.
14. Bezpečnost s profesionály. Praha: KPKB ČR, 2019. ISSN 2336-4793.
15. KAMENÍK, Jiří a František BRABEC. *Komerční bezpečnost*. Vydání první. Praha: ASPI, 2007. 340 s. ISBN 978-80-7357-309-6.
16. Stránky společnosti Signal profi: Nastavitelná rušička (all-in-one+5G) [online]. [cit. 2020-04-02]. Dostupné z: https://www.signalprofi.cz/Nastavitelna-rusicka-all-in-one-5G-70m-d118.htm
17. Stránky spol. Techniserv s.r.o. Stíněné komory [online]. [cit. 2020-01-20]. Dostupné z: http://www.stinene-komory.cz/
18. Stránky spol. ST Probin a.s. Stíněné komory - Faradayovy klece [online]. [cit. 2020-01-11]. Dostupné z: http://www.stprobin.cz/
19. JELÍNEK, Jiří. *Trestní zákoník a trestní řád*. Praha: Leges, 2016. 1280 s. ISBN 978-807-5020-499.
20. DVOŘÁK, Jan. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha: Wolters Kluwer, 2018. 480 s. ISBN 978-807-5980-168.
21. DOUBRAVOVÁ, Hana. *Vícekriteriální analýza variant a její aplikace v praxi* [online]. České Budějovice, 2009 [cit. 2020-02-20]. Dostupné z: https://theses.cz/id/6citbe/downloadPraceContent_adipIdno_11361.
22. FÁBRY, Jan. *Matematické modelování*. Vydání první. Praha: Professional Publishing, 2011. 180 s. ISBN 978-80-7431-066-9.
23. Security magazín. Praha: FAMily media, 2002. ISSN 1210-8723.
24. Security magazín. Praha: Security media, 2014. ISSN 1210-8723.
25. Stránky spol. Spy shop Praha: Odposlechy-štěnice. Odposlechy [online]. [cit. 2020-03-21]. Dostupné z: https://www.spyshop24.cz/odposlechy-29

26. SEHNÁLEK, Marián. *Odhalování skrytých odposlechových prostředků pro hlasovou komunikaci* [online]. Zlín, 2009 [cit. 2020-02-20]. Dostupné z:http://digilib.k.utb.cz/bitstream/handle/10563/10934/sehn%E1lek_2009_dp.pdf?sequence=1
27. Computerworld deník pro it profesionály: Odposlechy chytrých televizí? Samsung reaguje na obvinění [online]. [cit. 2020-03-29]. Dostupné z: https://computerworld.cz/securityworld/odposlechy-chytrych-televizi-samsung-reaguje-na-obvineni-51777
28. Chip. Počítačový magazín. Praha: Vogel Publishing, 2019. ISSN 1210-0684.
29. Avast blog. Tisíce GPS lokátorů mají chybu, prozrazují polohu uživatelů včetně dětí [online]. [cit. 2020-03-29]. Dostupné z: https://blog.avast.com/cs/unsecure-child-trackers
30. Chip. Počítačový magazín. Praha: Vogel Publishing, 2018. ISSN 1210-0684.
31. SystémOnLine: S příchodem internetu věcí už nebude v bezpečí vaše auto ani hračky pro děti [online]. 2016 [cit. 2020-03-29]. Dostupné z: https://www.systemonline.cz/clanky/rizika-souvisejici-s-prichodem-internetu-veci.htm
32. Stránky spol. Elvira: Lornet 24 [online]. Rusko, Moskva [cit. 2020-03-21]. Dostupné z: https://lornet-elvira.com/en/lornet24
33. Stránky spol. Spy shop Praha. Detektory nelineárních přechodů [online]. Praha [cit. 2020-02-29]. Dostupné z: https://www.spyshop24.cz/
34. MYSLÍK, Jiří. *Elektromagnetické pole*. Vydání první. Praha: BEN-technická literatura, 1998. 160 s. ISBN 80-860-5643-0.
35. Bydlení raz dva. Skryté odposlechy mohou být i u vás doma [online]. 2018 [cit. 2020-03-29]. Dostupné z: https://www.bydleni12.cz/skryte-odposlechy-mohou-byt-i-u-vas-doma/
36. CENTÉS, Jozef. *Odpočúvanie, procesnoprávne a hmotnoprávne aspekty*. Vydání první. Bratislava: C.H. Beck, 2013. 250 s. ISBN 978-80-89603-09-1.

37. NĚMEC, Miroslav. *Kriminalistická taktika pro policisty a studenty Policejní akademie České republiky v Praze.* Vydání první. Praha: Abook 2017. 547 s. ISBN 978-80-9069-74-09.
38. KAMENÍK, Jiří a František BRABEC. *Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. Vydání druhé. Praha: Wolters Kluwer, 2019. 344 s. ISBN 978-80-7357-309-6.

10 SEZNAM POUŽITÝCH OBRÁZKŮ

11 SEZNAM POUŽITÝCH TABULEK