Elektronické komunikační prostředky soukromého osobního strážce

Electronic Communications Resources for Private Bodyguards

Bc. Mário Kovačovic

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

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

Jméno a příjmení:	**Bc. Mário Kovačovic**
Osobní číslo:	**A12764**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Elektronické komunikační prostředky soukromého osobního strážce**
Téma anglicky:	**Electronic Communications Resources for Private Bodyguards**

Zásady pro vypracování:

1. **Seznamte se s problematikou komunikace soukromého osobního strážce s pomocí elektronických komunikačních a signalizačních prostředků.**
2. **Specifikujte současné a perspektivní elektronické komunikační a signalizační prostředky, vhodné pro práci soukromého osobního strážce.**
3. **Definujte požadavky na komunikační a signalizační elektronické prostředky, vhodné pro soukromého osobního strážce.**
4. **Analyzujte vhodné druhy elektronických komunikačních a signalizačních prostředků, vhodných pro soukromého osobního strážce s důrazem na mobilní telefony a osobní signalizátory.**
5. **Zpracovat vhodné varianty komunikačního spojení pomocí mobilních telefonů a vhodných signalizačních prostředků pro práci soukromého osobního strážce.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAPKOVÁ, Dora a Zdeněk MALÁNÍK. Rozdělení zbraní a osobních prostředků. Bezpečnostní technologie, systémy a management II.: Teorie a praxe ochrany majetku a fyzické bezpečnosti. 1. vyd. Doc. Ing. Luděk Lukáš, CSc. Zlín: Radim Bačuvčík – VeRBuM, 2012, 142 – 155. ISBN 978-80-87500-19-4.**
2. **MALÁNÍK, Zdeněk. Profese osobního strážce v České republice. LUKÁŠ, Luděk et al. Bezpečnostní technologie, systémy a management III.: Teorie a praxe ochrany majetku a fyzické bezpečnosti. 1. vyd. Zlín: VeRBuM, 2013, s. 208-228. ISBN 978-80-87500-35-4.**
3. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.**
4. **LUKÁŠ, Luděk et al. Bezpečnostní technologie, systémy a mangement II.: Teorie a praxe ochrany majetku a fyzické bezpečnosti. 1. vyd. Zlín: Radim Bačuvčík – VeRBuM, 2012, 387 s. ISBN 978-80-87500-19-4. Dostupné z: www-verbum.name.**
5. **Šifrované volání a SMS. TANGO, spol. s r.o. Odposlechy.com [online]. 1999-2014 [cit. 2014-01-26]. Dostupné z: http://www.odposlechy.com/sifrovane-volani-a-sms-kategorie.**

Vedoucí diplomové práce: **Ing. Zdeněk Maláník**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cieľom práce je zoznámenie čitateľa s elektronickými komunikačnými a signalizačnými prostriedkami osobného ochrancu, ktoré využíva v jeho praxi. Práca je zameraná na ukázaní fungovania rádiostaníc, mobilných telefónov a signalizátorov. Hlavným cieľom práce je bezpečná komunikácia medzi osobným ochrancom a jeho klientom, kde používa rádiostanice, mobilné telefóny a tie sú zabezpečené šifrovacími prostriedkami pre utajenú komunikáciu.

Kľúčová slová: osobný ochranca, klient, rádiostanica, mobilný telefón, šifrovanie, utajená komunikácia

ABSTRACT

A target of this work is to inform reader about the electronic means of communication and signal means by private bodyguard which he uses in his practice. The work is focused to demonstrate the functioning of radio stations, cell phones and signal means. The mean target of the work is safe communication between bodyguard and his client, where they use radio stations, cell phones and they are secured encryption means for safe communication.

Keywords: bodyguard, client, radio station, cell phone, cryptography

Poďakovanie

Chcel by som sa poďakovať môjmu konzultantovi Ing. Zdeňkovi Maláníkovi za vedenie mojej práce, za rady a typy. Ďalej by som chcel poďakovať rodine za pomoc a podporu.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

S rozvojom slobodného podnikania vzrástol aj význam bezpečnostných služieb ako napríklad fyzická ochrana osôb. Pre túto činnosť významné miesto zastáva komunikácia osobného ochrancu a jeho klienta. Túto komunikáciu však treba zabezpečiť proti odpočúvaniu inými osobami.

Prácu som vybral z dôvodu osobnej niekoľkoročnej praxe s využitím komunikačných prostriedkov, konkrétne použitia rádiostaníc. Ďalší dôvod je, že v každej literatúre je písané o komunikačných prostriedkov osobného ochrancu, ale o ich zabezpečení je písané len okrajovo. Nemenej dôležitý faktor je aj cena kvalitných zariadení z tejto oblasti, ktoré sú pre bežných užívateľov ťažko dostupné.

Pri vytváraní práce nastali problémy pri využití konkrétnych teoretických zdrojov oblasti komunikácie, vzhľadom na obmedzený rozsah informačných materiálov pre bežného užívateľa, kde informácie sú len opísané čiastočne – technicky, napríklad použitých šifrovacích algoritmov. Vo väčšine literatúry je písane, že osobný ochranca používa komunikačné prostriedky a príslušenstvo, ale je obtiažne získať konkrétne návody na použitie.

Práca si kladie za úlohu upozorniť na rozpor medzi významom komunikácie osobných ochrancov a ich klientov a minimálnym rozsahom informačných zdrojov poskytujúci dostatočné informácie o použitých prostriedkoch, spôsoboch a princípe ich činnosti. Za hlavný nedostatok šifrovanej komunikácie považujem pomerne veľkú dostupnosť aplikácií s možnosťou dešifrovania daného programu. Úlohou práce je poukázať na možné lokalizovanie prebiehajúceho šifrovaného hovoru.

Cieľom je zhrnúť a zovšeobecniť odborné poznatky na úroveň bežného užívateľa. Týmto sa dosiahne vytvorenie manuálu, ktorý je možný použiť v pedagogickej činnosti a v praxi začínajúcich osobných ochrancov.

Riešený problém spadá do kontextu fyzickej ochrany osôb a utajenej komunikácie.

V postupoch sú použité metódy dedukcie (od všeobecných informácií ku konkrétnym), indukcie (od konkrétneho k všeobecnému), analýzy (využitie písomných textov),syntézy (spájanie poznatkov) a citácie.

Diplomová práca pozostáva z piatich kapitol, ktoré prvé dve sú v teoretickej časti a zvyšné tri kapitoly sa zaoberajú praktickým využitím.

V prvej kapitole teoretickej časti sú opísané základne pojmy a princípy sietí, šifrovania algoritmami a právne aspekty tejto oblasti.

V druhej kapitole teoretickej časti sú charakterizované komunikačné a signalizačné prostriedky a prostriedky na utajenie.

V prvej kapitoly praktickej časti sú vopred určené kritéria osobného ochrancu, nutné na úspešnú činnosť.

V druhej kapitole praktickej časti nasleduje analýza konkrétnych vybraných komunikačných a signalizačných prostriedkov a vlastnosti týchto prostriedkov.

Tretia kapitola praktickej časti pojednáva o návrhu utajenej komunikácie na konkrétnom príklade. Ďalej sú uvedené grafické schémata pre jednotlivé prostriedky.

I. TEORETICKÁ ČASŤ

1 ZOZNÁMENIE S PROBLEMATIKOU A TERMINOLÓGIOU POJMOV

Elektronické komunikačné prostriedky pre osobného ochrancu sú neoddeliteľnou súčasťou pre výkon jeho povolania. Každý osobný ochranca by mal vedieť s týmito prostriedkami zachádzať na vysokej úrovni, aby mohol plnohodnotne vykonávať svoju profesiu.

K uvedeniu do problematiky treba predstaviť niektoré pojmy, ktoré sú súčasťou pre jeho prácu, s ktorými sa osobný ochranca stretáva pravidelne a sú súčasťou zariadení pre výkon jeho povolania.

1.1 Siete rádiostaníc

Rádiostanice komunikujú formou rádiových sietí. Rádiové siete sú súborom stacionárnych a mobilných staníc zoskupených do sietí za účelom vytvorenia rádiových spojení medzi účastníkmi. Používajú sa na prenos analógových a digitálnych signálov v určených frekvenčných pásmach.

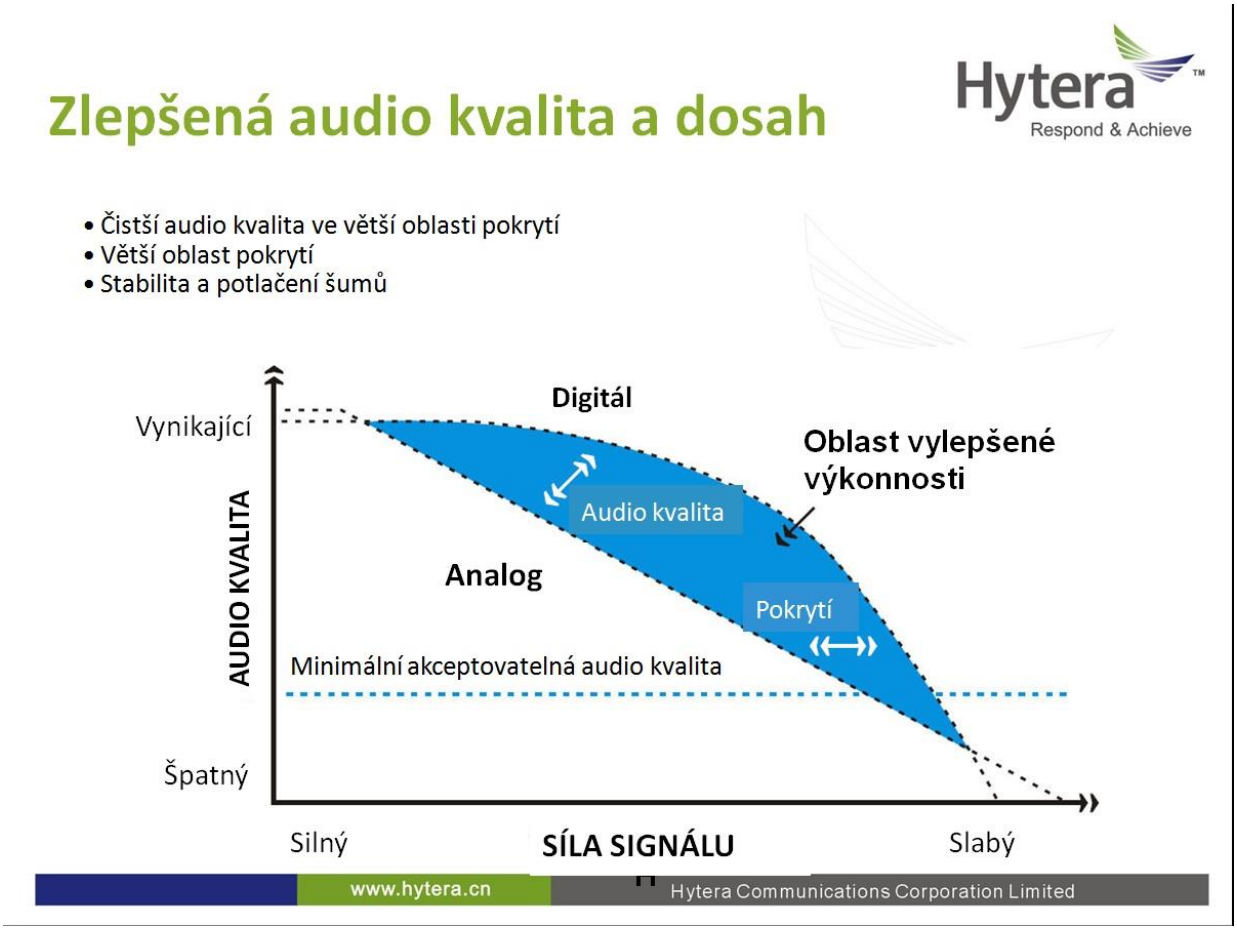
Analógová sieť

Analógová sieť umožňuje prenos signálov len v analógovej forme. Je to vlastne vysokofrekvenčná vlna modulovaná v závislosti na nízkofrekvenčnej vlne – teda na hlase hovoriacej osoby. Pracuje na určitých frekvenciách podľa toho, či sa jedná o profesionálne, občianske alebo PMR rádiostanice. [3]

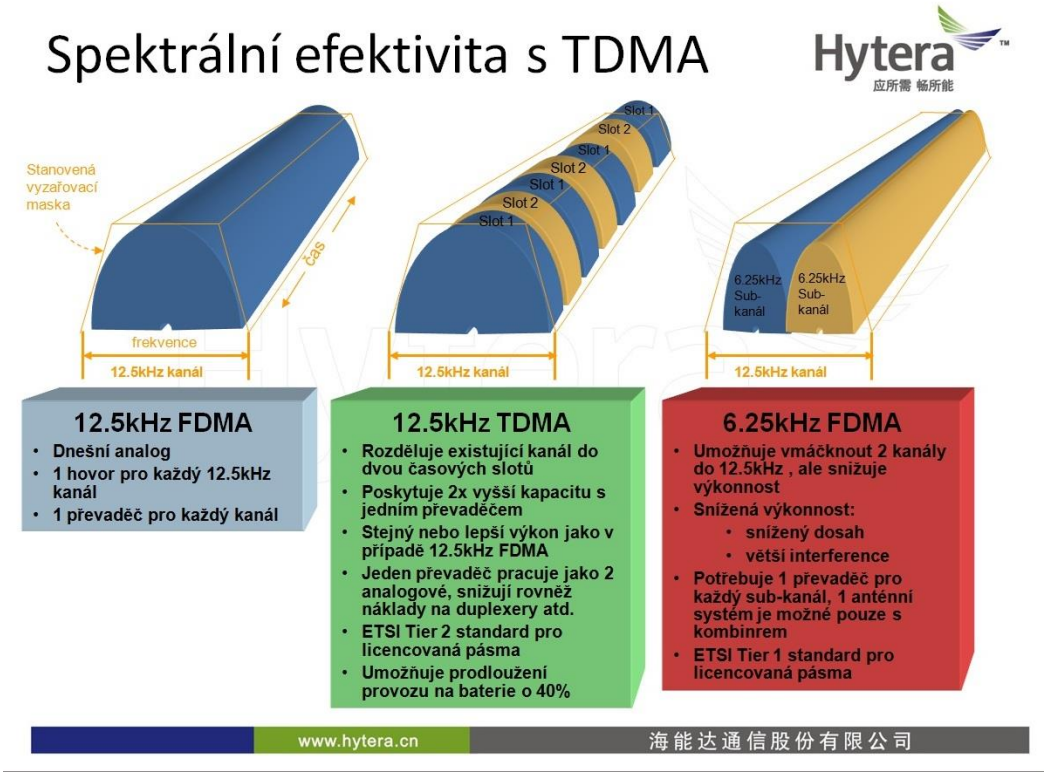
Digitálna sieť

Digitálna sieť vznikla za účelom zjednotiť komunikáciu IZS. V ďalších sférach bolo za potreby digitalizovať siete, pretože analógová sieť bola už zastaraná a hovory sa dali veľmi ľahko odpočúvať. Pre zobrazenie digitálnej siete je najvodnejšie poukázať na výrobcu Hytera. V roku 2005 vznikol štandard DMR pre profesionálne rádiostanice, ktorý vydal európsky inštitút ETSI TS 102 361. Rádiostanice aj celé rádiové siete rôznych

výrobcov vyrobené podľa tohto štandardu sú vzájomne kompatibilné. DMR štandard je rozdelený do 3 úrovní: Tiers I (voľné pásmo 446 MHz a výkon do 0.5W), Tiers II (licencované pásmo 66-960 MHz, vyšší štandard, 2 TDMA sloty 12,5 kHz kanálu) Tiers III (trunkové riešenie v pásme 66-960 MHz + textové správy + dáta). Kompletné riešenie pre DMR úroveň Tiers II aktuálne ponúka Motorola s výrobnou radou MotoTRBO a Hytera s výrobnou radou DMR. Výhodou DMR je komunikačný protokol, ktorý využíva dvojslotový časový multiplex TDMA podobne, ako využívajú GSM siete. TDMA časovo rozdelí kanál na dva sloty, pre každý slot je vyhradený časový úsek 30ms, každý slot má 1,5ms ochranný čas. Časový multiplex TDMA rozdeľuje prenosový kanál podľa času do rady relácií. Rada hlasových kanálov je pripojená do fyzického kanálu a priraďuje sa im čas v presne stanovenom poradí. Využitím tohto prístupu sa zdvojnásobí kapacita rádiovej siete pri súčasnom znížení investičných nákladov. [4]



Obr. č. 1 Graf analógovej a digitálnej siete [4]



Obr. č. 2 Kanály komunikácie [4]

1.2 Sieť mobilných telefónov

Zvýšenie komfortu komunikácie si vyžiadalo spojenia v málo dostupných a vzdialených miestach, preto vzniklo mobilné telefónne spojenie, ktoré sa realizuje pomocou rádiových prostriedkov. Zostava mobilnej komunikácie pozostáva zo základňovej stanice a mobilnej stanice. Najskôr sa používala analógová sieť privátneho charakteru a neskôr vznikla sieť digitálneho charakteru s použitím bunkovej siete (celulárnej), ktorá sa používa dodnes. Digitálna sieť má štandardy na hlasovú, textovú a dátovú skupinu. [5]

GSM štandard

GSM štandard (označovaný ako 2G) je digitálny štandard bunkovej siete kompatibilný s ostatnými bunkovými sieťami po svete. Sieť tvoria tri základné časti, a to subsystém základňových staníc BSS, sieťový prepojovací subsystém NSS a operačný subsystém OSS. GSM štandard pracuje na frekvenciách 900, 1800 a 1900 MHz. V GSM štandarde je možná hlasová komunikácia a posielanie krátkych textových správ SMS. [6]

GPRS

GPRS (označovaný ako 2.5G) je systém dátového prenosu rýchlosťou až 172 kbit za sekundu a je súčasťou GSM. Prenos dát prebieha po viacerých menších častiach - paketoch. Prenos dát prebieha prostredníctvom viacerých kanálov. GPRS podporuje paketový protokol X.25 podporovaný hlavne v Európe. GPRS je spoplatňované počtom odoslaných a prijatých dát. [6]

EDGE

EDGE (označovaný ako 2.75G) je systém dátového prenosu rýchlosťou až 384 kbit za sekundu. Je to ďalšia súčasť vývoju GSM. Zvyšuje kapacitu siete a dátových rýchlostí. [6]

UMTS

UMTS (označovaný ako 3G) je nástupcom siete GSM. Prenosová rýchlosť siete UMTS môže dosahovať až 2 Mb za sekundu. Pre pozemný prístup sú určené pásma 1900-1980 MHz, 2010-2025 MHz a 2110-2170 MHz. Hlavnými službami sú rýchle pripojenie k internetu a rozličné multimediálne služby (hlasové a dátové služby, videá, vzdialená kontrola), telefónne služby, e-mail, videokonferencie, vysoká prenosová rýchlosť dát, roaming. V Amerike sa sieť UMTS nazýva CDMA 2000. [6]

HSDPA

HSDPA (označovaný ako 3.5G) je nadstavba siete 3G a rýchlosťou dátového prenosu sťahovania až do 14,4 Mb za sekundu. HSDPA ponúka možnosť prijímať veľké súbory. [7]

HSUPA

HSUPA (označovaný ako 3.75G) je nadstavba siete 3G a rýchlosťou dátového prenosu posielania až do 5,76 Mb za sekundu. HSUPA je vylepšenie pre dátový tok pre posielanie zo zariadenia na internet. [7]

LTE

LTE (označovaná ako 4G) je sieť novej generácie. Rýchlosť sťahovania je 172,8 Mb za sekundu a rýchlosť odosielania je 57,6 Mb za sekundu. Sieť LTE prebieha v pásmach 800, 1800 a 2600 MHz. [8]

1.3 Šifrovacie algoritmy

Šifrovacie algoritmy sú súčasťou zabezpečenia zariadení. Šifrovaním sa zaoberá kryptografia a lúštením šifier sa zaoberá kryptoanalýza. Šifrovací algoritmus je funkcia zostavená na matematickom základe a uskutočňuje samotné šifrovanie a dešifrovanie dát. [9]

AES

Algoritmus pre symetrické šifrovanie, ktorý používa jeden kľúč k zašifrovaniu aj dešifrovaniu dát a ktorý má dĺžku 128, 196 alebo 256 bitov. [10]

RSA

Šifrovací nesymetrický algoritmus, ktorý používa verejný a súkromný kľúč a je pomenovaný podľa jeho autorov Rivest, Shamir, Adleman. [10]

Twofish

Symetrická bloková šifra 128 bitového bloku a 256 bitovou dĺžkou kľúča. [11]

Diffie-Hellman

Algoritmus, ktorý slúži k dohodnutiu spoločného kľúča po nezabezpečenom kanále. Výmenu kľúča zabezpečí tak, že útočník, ktorý odpočúva linku, nebude schopný kľúč zrekonštruovať. [12]

End-To-End

Šifrovanie na koncových zariadeniach. Zašifrovanie pred odoslaním a dešifrovanie po prijatí.

RTP

Protokol štandardizujúci paketové doručovanie zvukových a obrazových dát po internete. Použitie tohto protokolu sa využíva v systémoch prúdového prenosu, najmä pre telefonovanie, videokonferencie a push to talk systémy. [14]

VoIP

Technológia, ktorá dokáže prenášať hlasovú komunikáciu prostredníctvom internetu. Aby účastník mohol telefonovať prostredníctvom VoIP, musí mať softwarový telefón SIP (program) alebo hardwarový telefón VoIP.[13]

SIP

Internetový protokol určený pre prenos signalizácie v internetovom telefonovaní. Protokol pre uskutočnenie VoIP spojenia pracuje v súčinnosti s ďalšími protokolmi. Vlastný prenos hovoru je uskutočňovaný pomocou protokolu RTP. Detaily o vlastnostiach zahajovaného prenosu popisuje protokol SDP, ktorý je prenášaný v tele SIP paketov. [15]

SDP

Internetový protokol určený k popisu vlastností relácie multimediálneho prenosu dát. Pomocou neho sa neprenášajú vlastné dáta, slúžia pre vyjednanie parametrov ako sú typy média, transportný protokol a typy kodeku alebo prenosová rýchlosť. [16]

SRPT

Protokol, ktorý umožňuje šifrovanie, možnosť overovať správy a integritu RTP prenášaných dát v unicast aj multicast aplikáciách. [17]

ZRPT

Kryptografický protokol, ktorý poskytuje dohodu a výmenu kľúčov pre šifrovanie medzi dvoma koncovými zariadeniami pri použití VoIP telefonovaniu založenej na komunikáciu v reálnom čase. Pri výmene kľúča použitý algoritmus Diffie-Hellman a pri šifrovaní sa používa SRPT. Použitie musí byť na oboch koncových zariadeniach. [18]

TLS

Kryptovací protokol, ktorý poskytuje možnosť zabezpečenej komunikácie po internete. Zabraňuje proti odpočúvaniu a posielania falošných správ. Poskytuje koncobodovú autentifikáciu a súkromie v komunikácií cez internet používaním kryptografie. Typicky je autorizovaný len server (identita je zaručená) zatiaľ čo klient ostáva neautorizovaný. To znamená, že koncový užívateľ (jednotlivec alebo aplikácia) si môže byť istý s kým komunikuje. [19]

1.4 Právne aspekty

Každý osobný ochranca musí byť zoznámený s právnym aspektom proti odpočúvaniu jeho zariadení a tak isto aj chránená osoba. Preto existuje právna ochrana osobnostných práv proti monitorovaniu a odpočúvaniu osôb a sú to:

- *Zákon č. 2/1993 Sb., Listina základných práv a slobôd*

  V ustanoveniu čl.7 odst. 1 je zakotvená zásada o nedotknuteľnosti osoby a jej súkromia. Tento princíp je ďalej špecifikovaný v ustanoveniach čl. 10 odst. 2 a čl. 13, ktoré upravujú ochranu listového tajomstva, rovnako ako tajomstvo iných písomností a záznamov. Táto ustanovenia zaručujú tiež tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením.

- *Zákon č. 40/1964 Sb., občiansky zákonník*

  Ustanovenia § 11a následne korešpondujú s úpravou obsiahnutou v Listine základných práv a slobôd. Zvláštna pozornosť je tu venovaná spôsobom nakladania s obrazovými a zvukovými záznamami, týkajúcimi sa fyzickej osoby alebo ich prejavov.

- *Dohovor o ochrane ľudských práv a slobôd, publikovaná pod č.209/1992 Sb.*

  Ustanovenia §11a následne korešpondujú s úpravou obsiahnutou v Listine základných práv a slobôd. Zvláštna pozornosť je tu venovaná spôsobom nakladania s obrazovými a zvukovými záznamami, týkajúcimi sa fyzickej osoby alebo ich prejavov. [2]

2 OPIS KOMUNIKAČNÝCH A SIGNALIZAČNÝCH PROSTRIEDKOV

Komunikačné a signalizačné prostriedky sú súčasťou povinnej výbavy každého osobného ochrancu a jeho klienta, preto musia byť zvolené vždy vhodné komunikačné prostriedky pre každú zákazku zvlášť. Každý prostriedok má iné využitie v daných podmienkach.

2.1 Mobilný telefón

Mobilný telefón je elektronické zariadenie, ktoré uskutočňuje telefonické hovory pomocou rádiových vĺn. Je určený na hlasovú, textovú a obrazovú komunikáciu. Podľa spôsobu pripojenia mobilného telefónu do telefónnej siete rozlišujeme na celulárne (bunkové), satelitné a bezšnúrové telefóny. Využívanie mobilných telefónov zahrňuje stále poplatky za telefonovanie, posielanie krátkych textových SMS a obrazových MMS správ, dátové služby podľa cenníka mobilného operátora. Mobilný telefón obsahuje základnú dosku, operačnú pamäť, displej, vysielač/prijímač GSM, u starších modelov klávesnicu, u novších modelov Bluetooth a Wi-Fi. [20]

2.1.1 Použitie mobilného telefónu

Použitie mobilného telefónu je prakticky možné všade tam, kde sa nachádza signál. Okrem telefonovania má výhodu SMS správ, kde v prípade nebezpečenstva alebo stretnutia na dohodnutom mieste sa pošle SMS osobnému ochrancovi. Ďalším využitím je GPS, ktoré môže mať funkciu nájdenia najkratšej cesty alebo môže zobrazovať polohu osobných ochrancov a klientov. Dnešné použitie smartphonov má využitie mobilných dát a Wi-Fi, ktoré môžu nahradiť klasické telefonovanie a posielanie správ cez aplikácie.

2.1.2 Výhody a nevýhody mobilných telefónov

Výhodou mobilných telefónov je, že sú prenosné a každý užívateľ, ktorý ho má pri sebe, je hneď dostupný na odovzdanie informácií. Ďalšia výhoda dnešných mobilných telefónov, konkrétne smartphónov, je dotykový displej, na ktorom okrem telefonovania a písania krátkych textových správ, sa dá prehliadať internet, elektronická pošta, využívajú

sa navigačné služby GPS. Dnešné mobilné telefóny majú aj kvalitné fotoaparáty, s ktorými sa dajú nafotiť fotografie vo veľmi slušnej kvalite.

Nevýhody dnešných mobilných telefónov sú hlavne v kapacite batérie, ktorý sa pokladá ako najväčší problém. Okrem kapacity batérie je nevýhodou životnosť mobilného telefónu, ktorý bez väčších problémov funguje približne dva roky.

Okrem hardwarových nevýhod sú nevýhody v oblasti komunikácie, kde sa dá pomerne ľahko odsledovať komunikácia medzi dvoma účastníkmi hovoru, poprípade zachytiť textové správy. V dnešnej dobe nevýhody smartphonov závisia hlavne od operačných systémov (kompatibilita medzi sebou) a možnosť sledovania celkovej aktivity Národnou Bezpečnostnou Agentúrou.

2.1.3 Príslušenstvo mobilných telefónov

Príslušenstvo mobilných telefónov je oproti ostatným zariadeniam dosť bohaté. Pre prácu osobného ochrancu a jeho klienta je treba starostlivo vyberať príslušenstvo. Pri danej práci v teréne sa nedá použiť každé príslušenstvo. Mobilný telefón pre prácu by mal obsahovať ochranné puzdro proti mechanickému poškodeniu, drôtové alebo bezdrôtové handsfree do ucha, poprípade ako zabudovaný doplnok do auta a v neposlednom rade ako záchranný prvok proti náhlemu vybitiu baterky treba mať autonabíjačku. Vhodným riešením by bola náhradná batéria alebo externý akumulátor v prípade náhleho vybitia telefónu. Externé antény slúžia ako doplnok pre prípad, že signál by bol slabý (málo osídlené miesta, terén so slabým signálom ako lesy, hory...)

2.2 Rádiostanica

Rádiostanice patria medzi telekomunikačné zariadenia, ktoré umožňujú komunikáciu pomocou šírenia elektromagnetického vlnenia a sú bezdrôtové. Rádiostanice nie sú závislé na sieti prevádzačov, ako mobilné telefóny, pretože sieť prevádzačov u mobilných telefónov zvyšujú ich signál. Dosah rádiostanice je menší ako u mobilných telefónov, ale je, že nie je nutné platiť žiadne poplatky za užívanie, pokiaľ nie sú pridelené telekomunikačnými úradmi na profesionálne využitie. Rádiostanice nemajú konkurovať mobilným telefónom, slúžia v podstate na rýchlu komunikáciu, kde stačí len stlačiť tlačidlo a hovoriť. Rádiostanice komunikujú v analógovej a digitálnej sieti. [1]

2.2.1 Profesionálna ručná a mobilná rádiostanica

Profesionálne ručné a mobilné rádiostanice pracujú vo frekvenciách približne 80 MHz, 170 MHz, 450 MHz. Profesionálne rádiostanice používajú štátne zložky, súkromné bezpečnostné zložky a veľké podniky. V tomto prípade sú frekvencie udeľované komunikačnými úradmi, konkrétne v Českej republike Českým telekomunikačným úradom. U rádiových sietí sa potom platia určité poplatky podľa počtu rádiostaníc. U týchto profesionálnych rádiostaníc sa dá pracovať bez účasti ČTÚ na tzv. zdieľaných kmitočtoch a bez poplatkov. To umožňuje , že si každý môže zakúpiť a používať profesionálnu ručnú vysielačku bez obmedzenia. Tieto vysielačky sú veľmi výkonné a odolné proti nárazom a nepriaznivému počasiu, ale nevýhodou je vyššia obstarávacia cena. [1]

2.2.2 Amatérske rádiostanica

Amatérska rádiostanica slúži ako aj profesionálna rádiostanica na komunikáciu medzi dvomi alebo viacerými osobami. Výhodou je, že amatérske rádiostanice neplatia žiadne poplatky za užívanie. Amatérska rádiostanica má dve základné delenia a to občianske rádiostanice CB (Citizen Band) a PMR 446. Toto delenie závisí od použitej frekvencie a použitia. [1]

Občianska rádiostanica CB

Občianska CB rádiostanica pracuje na frekvencií 26,565 – 27,405 MHz na 80 kanálov pri maximálnom výkone 4 W. Je určené pre občanov a firmy bez obmedzenia, ale za predpokladu, že bude dodržaná legislatíva, za ktorú ručí dovozca aj predajca. Občianska rádiostanica CB môže byť ručná, vozidlová a základňová. [21]

Tab. č. 1 Frekvencie CB rádiostaníc [22]

Kanál číslo	Frekvencia [MHz]	Kanál číslo	Frekvencia [MHz]	Kanál číslo	Frekvencia [MHz]	Kanál číslo	Frekvencia [MHz]
1	26,965	21	27,215	41	26,565	61	26,765
2	26,975	22	27,225	42	26,575	62	26,755
3	26,985	23	27,255	43	26,585	63	26,785
4	27,005	24	27,235	44	26,595	64	26,795
5	27,015	25	27,245	45	26,605	65	26,805
6	27,025	26	27,265	46	26,615	66	26,815
7	27,035	27	27,275	47	26,625	67	26,825
8	27,055	28	27,285	48	26,635	68	26,835
9	27,065	29	27,295	49	26,645	69	26,845
10	27,075	30	27,305	50	26,655	70	26,855
11	27,085	31	27,315	51	26,665	71	26,865
12	27,105	32	27,325	52	26,675	72	26,875
13	27,115	33	27,335	53	26,685	73	26,885
14	27,125	34	27,345	54	26,695	74	26,895
15	27,135	35	27,355	55	26,705	75	26,905
16	27,155	36	27,365	56	26,715	76	26,915
17	27,165	37	27,375	57	26,725	77	26,925
18	27,175	38	27,385	58	26,735	78	26,935
19	27,185	39	27,395	59	26,745	79	26,945
20	27,205	40	27,405	60	26,755	80	26,955

Rádiostanice PMR 446

Ručné rádiostanice PMR 446 fungujú na frekvencií 446,00625 až 446,09375 MHz na osem kanálov pri maximálnom výkone 0,5 W. Sú to moderné miniatúrne a lacné ručné vysielačky pre širokú verejnosť bez obmedzenia a bez poplatkov, ktoré sa vyznačujú veľmi malými rozmermi, slušným vysielacím výkonom, veľmi dobrými dosahmi (približne sedem kilometrov v závislosti od prostredia), veľkým množstvom funkcií a zaujímavými doplnkami. [23]

Tab. č. 2 Frekvencie PMR rádiostaníc [23]

Kanál číslo	Frekvencia [MHz]	Kanál číslo	Frekvencia [MHz]
1	446,00625	5	446,05625
2	446,01875	6	446,06875
3	446,03125	7	446,08125
4	446,04375	8	446,09375

2.2.3 Použitie rádiostaníc

Rádiostanica slúži k rýchlej komunikácie medzi užívateľmi bez zbytočných poplatkov za hovor a zdĺhavého čakania na vytočenie a spojenie ako u mobilných telefónov. Rádiostanice sa skôr využívajú pri akciách, kde je viacero osobných ochrancov alebo pre komunikáciu medzi osobným ochrancom a klientom.

2.2.4 Výhody a nevýhody rádiostaníc

Výhodou rádiostaníc je najmä v to, že viaceré z nich po zakúpení nemajú ďalšie poplatky za hovor ako u mobilných telefónov. Okrem dorozumievania majú výhodu v tom, že netreba vytáčanie čísel, tým pádom komunikácia medzi účastníkmi je veľmi rýchla.

Nevýhodou rádiostaníc je ľahké odpočúvanie hlavne u analógového prenosu. Preto je nutné hovoriť kódovou rečou alebo používať utajovače.

2.2.5 Príslušenstvo rádiostaníc

K rádiostaniciam sa dá dokúpiť veľké množstvo príslušenstva, ako napríklad slúchadlá s mikrofónom, externé mikrofóny, náhradné akumulátory, stolné a prenosné nabíjačky, autonabíjačky do auta, nabíjacie adaptéry, púzdra, prídavné antény a kabeláž .

2.3 Tiesňové tlačidlo a osobný alarm

Tiesňové tlačidlo slúži ako improvizovaný prostriedok. Väčšinou má využitie u seniorov kvôli rýchlemu privolaniu zdravotnej služby, ale v tomto prípade môže slúžiť

klientovi k privolaniu osobného ochrancu. Tiesňové tlačidlo využívajú aj osobný ochrancovia v prípade takej situácie, keď je napríklad zranený a podobne, tak ním kontaktuje preventistu[1].

Ďalšie zariadenie ako improvizovaný prostriedok je osobný alarm. Je to ručný obranný prostriedok, ktorý na útočníka pôsobí akusticky v rôznej frekvencií a hlasitosti. Slúži k pasívnemu pôsobení proti protiprávnemu útoku človeka. [35]

2.3.1 Použitie tiesňového tlačidla a osobného alarmu

Tiesňové tlačidlo je doplnok k lepšiemu štandardu ochrany a vhodné použitie môže byť v priestoroch s veľkou koncentráciou ľudí, ako napríklad nákupné strediská, divadlo, kino, koncerty a festivaly. Taktiež je vhodné použitie, keď klient má vo večerných hodinách stretnutie v bočných uličkách, parkoch, diskotékach, oblastiach so zvýšenou kriminalitou a cíti sa byť ohrozený. Taktiež môžu byť tieto prostriedky použité, pokiaľ osobný ochranca nie je priamo v miestnosti s klientom, ale po aktivovaní mu príde na pomoc.

2.3.2 Výhody a nevýhody tiesňového tlačidla a osobného alarmu

Výhodou tiesňového tlačidla a osobného alarmu sú malé rozmery, ktoré sa dajú ľahko skryť, pokiaľ ich chce klient alebo osobný ochranca použiť.

Nevýhodou je to, že sa napájajú na malú baterku a tým pádom sa nevie, dokedy budú mať tieto zariadenia životnosť. Okrem toho je tu aj nevýhoda mylného stlačenia tiesňového tlačidla alebo vytrhnutie šnúrky osobného alarmu.

2.3.3 Príslušenstvo tiesňového tlačidla

Príslušenstvo pre tiesňové tlačidlo na trhu nie je v dostatočnom množstve. Dajú sa kúpiť náhradné baterky, klipsne na zachytenie o opasok alebo náramok na nosenie ako náramkové hodinky.

---

[1] Preventista – fyzická osoba, ktorá spolupracuje s osobným ochrancom,

2.4 Prostriedky utajovania komunikácie rádiostaníc a mobilných telefónov

Pri komunikácií cez rádiostanicu a mobilný telefón je dôležité, aby v danej situácii nebola možnosť odsledovať hovor medzi osobným ochrancom a klientom. Preto existujú prostriedky na utajenie hovoru. Tie majú rôznu formu v závislosti od prostriedku, s ktorým sa komunikuje. Utajenie komunikácie je softwarové a hardwarové.

2.4.1 Utajenie rádiostanice

Pri utajení rádiostaníc má dvojaké použitie, záleží, či pracujú v analógovej alebo v digitálnej forme. Pri analógovej forme je priamo v rádiostanici integrovaný Voice Scrambler. Ten pracuje na princípe upravovania alebo invertovania signálu v rádiostanici za účelom utajenia. Príkladom integrovaného utajovača sú Motorola P165 a P185. Pri digitálnej forme rádiostanice môže obsahovať Voice Scrambler, ale využíva sa šifrovanie pomocou šifrovacích algoritmov, konkrétne šiframi AES, RSA. [24]

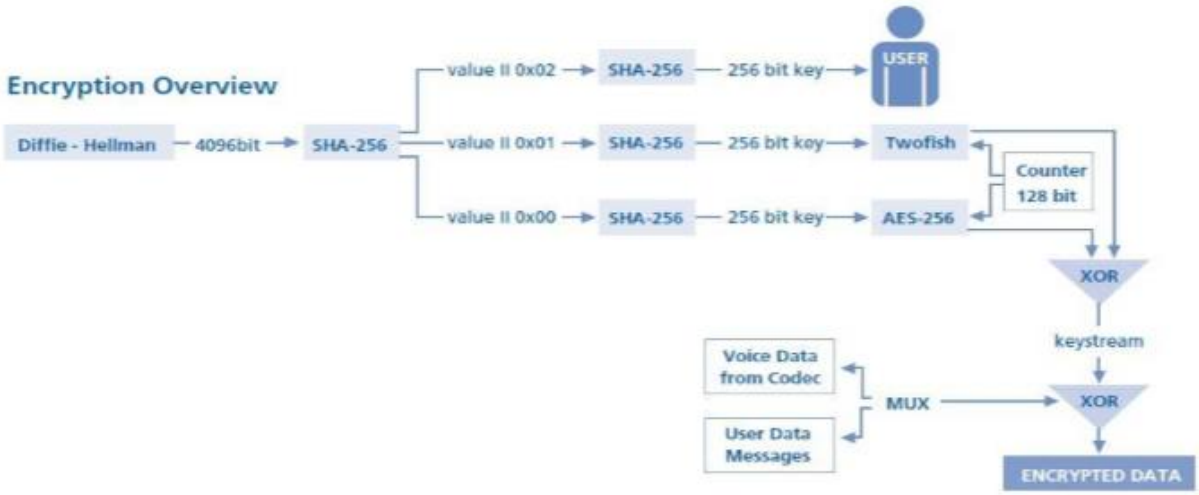
2.4.2 Utajenie mobilného telefónu

Komunikácia mobilným telefónom je v dnešnej dobe dosť nebezpečná a ľahko odsledovateľná. Pre utajenie existujú tri spôsoby šifrovania, a to špeciálne upravenými telefónmi, hardwarovými prvkami a softwarovými aplikáciami.

Špeciálne upravený telefón

Špeciálne upravený telefón na hlasovú komunikáciu používa šifrovacie algoritmy a špeciálne upravený operačný systém Android, do ktorého je priamo integrovaný firewall chrániaci telefón pred útokmi a pri zistení útoku automaticky spustí obranný mechanizmus. Špeciálne upravený telefón má otvorený zdrojový kód, pri ktorom sa dá zistiť bezpečnosť celkového softwaru. Metóda šifrovania takéhoto telefónu spočíva vo viacerých postupoch. Je to napríklad kombináciou algoritmov AES256 a Twofish pre hlasovú komunikáciu, výmena kľúča prebieha pomocou 4096 bit Diffie-Hellman algoritmu s SHA256 hash funkciou. Efektívna dĺžka kľúča by mala mať 256 bitov. Pri každom hovore sú vytvorené efektívne kľúče a po ukončení hovoru sú automaticky zničené. Príkladom takéhoto telefónu je Cryptophone 500 zo Spy obchodu. [25]

Obr. č. 3 Cryptophone 500 [25]



Obr. č. 4 Prehľad kryptovania [25]

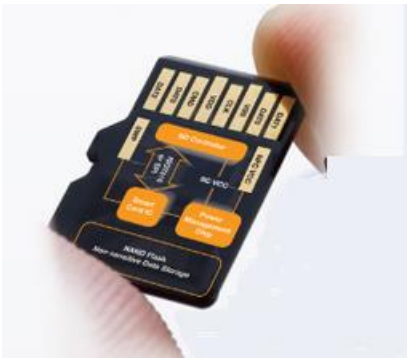
Šifrované hardwarové prostriedky

Šifrovanie pomocou hardwarových prostriedkov môže byť dvojaké. Prvý spôsob šifrovania pomocou hardwarovým prostriedkom je Voice Protector-om. Hlavnou funkciou tohto zariadenia je zabezpečenie mobilnej komunikácie, je kompatibilný s väčšinou telefónov s 3,5 mm slúchadlovým jack-om, šifrovanie prebieha na hlasovom kanáli, funguje bez dátového spojenia a nie je tu žiadne oneskorenie ako u iných šifrovacích riešení. Používa šifrovanie end-to-end. Nevýhodou tohto zariadenia je, že pokiaľ chce byť šifrovaný hovor, musia mať obe strany toto zariadenie. [26]

Obr. č. 5 Voice Protector [26]

Obr. č. 6 Použitie Voice Protector [26]

Ďalším riešením hardwarového šifrovania je čip priamo implementovaný na MicroSD karte. Toto riešenie je vhodné najmä na také mobilné telefóny, ktoré majú možnosť rozšírenia pamäte MicroSD kartami. Nevýhodou tohto zariadenia je to, že v dnešnej dobe veľa mobilných telefónov neobsahuje rozšíriteľnú pamäť MicroSD kartami a tak treba nájsť inú možnú alternatívu zabezpečenia telefónov proti odpočúvaniu. Ďalšou nevýhodou je prvotná cena, ktorá sa pohybuje v niekoľkých desiatkach tisíc korún (stoviek eur), ale po zakúpení má vlastník doživotnú bezplatnú licenciu. V poslednom rade, aby šifrovanie vôbec mohlo fungovať, je potrebné mať na oboch zariadeniach tento čip implementovaný do MicroSD karty. Ale na druhej strane toto zariadenie kombinuje niekoľko šifrovacích algoritmov (AES, RSA), šifruje hovory aj správy, obsahuje bezpečnostné certifikáty (napríklad EAL5+) a je kompatibilné s väčšinou telefónov s operačným systémom Android. [27]



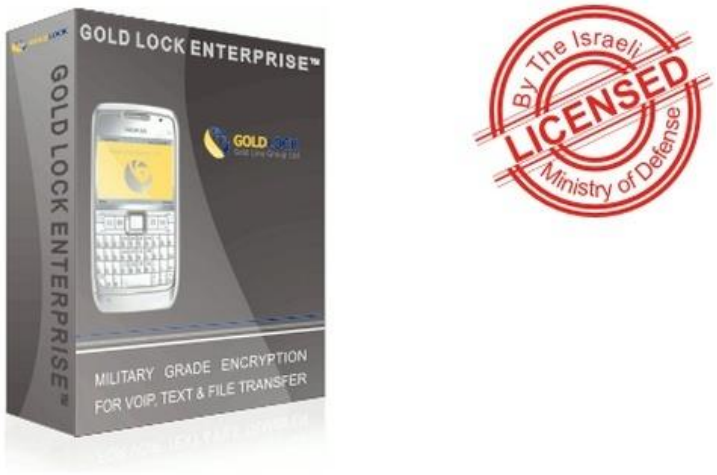
Obr. č. 7 VIP Call secure chip [27]

Šifrované softwarové aplikácie

Pre väčšinu telefónov s operačnými systémami Android, iOS, Windows Phone, Symbian, Black Barry existuje možnosť šifrovania hovorov, správ a súborov pomocou špeciálnych aplikácií. V dnešnej dobe je tento druh šifrovania najobľúbenejším vďaka pohodlnému používaniu a vysokej miere zabezpečenia. Nevýhodou oproti hardwarovým šifrovacím prostriedkom je mať nainštalovaný antivírusový program hlavne kvôli vírusom typu trójsky kôň a zakúpenie ročnej licencie. Existujú aj aplikácie tretích strán, ktoré sa

dajú stiahnuť v Google play alebo App Store a nie sú tak finančne náročné, ale nezaručujú ani stopercentnú garanciu ochrany proti odpočúvaniu.

Jednou z najlepších aplikácií, ale aj finančne náročnejších je izraelská aplikácia Gold-Lock, ktorá je kompatibilná so všetkými operačnými systémami mobilných telefónov a počítačov. Výhodou tejto aplikácie je, že stačí ju mať len na jednom telefóne. Konkurenčné aplikácie na šifrovaný hovor, SMS a súbory musia mať obe zariadenia. Táto aplikácia je certifikovaná izraelským ministerstvom obrany, má 3-úrovňové šifrovanie, zmena kľúča prebieha každé štyri sekundy a podporuje všetky prenosové siete. V tejto aplikácií je veľa šifrovacích algoritmov ako AES 256 Bit, Deffie-Hellan 4096 Bit, 16384 Bitová autentizácia, Elliptic Curve 384 Bit (ekvivalent pre RSA 7680 Bit). [28]



Obr. č. 8 Gold-Lock [28]

Ďalšou aplikáciou na šifrovanie je Phone-X, finančne menej náročný variant k aplikácií Gold-Lock, ktorý dokáže šifrovať hovory, SMS a v PRO verzií aj súbory. Má viac úrovní na šifrovanie, zabezpečuje adresár telefónu, pri každom telefonáte je generovaný unikátny kľúč, ktorý sa automaticky zničí po dokončení hovoru. Pri tejto aplikácií sa každý rok musí zakúpiť nová licencia. [29]

Obr. č. 9 Phone-X [29]

Treťou najobľúbenejšiou aplikáciou je SILENTEL 6, ktorá má certifikáciu NATO CONFIDENTIAL. Táto aplikácia je totožná s aplikáciou Phone-X, čo sa týka zabezpečenia a funkcií. SILENTEL 6 ponúka celkové zabezpečenie hovorov, SMS a súborov s licenciou na jeden mesiac alebo na celý rok pre jedného užívateľa, ale dá sa zaobstarať konkrétna licencia na ochranu len hovorov alebo len SMS, alebo SMS a súborov taktiež pre všetky varianty jeden užívateľ na jeden mesiac alebo jeden rok. [30]

Obr. č. 10 SILENTEL 6 [30]

Na trhu existujú neplatené aplikácie, ktoré sa dajú stiahnuť zadarmo z obchodov Google Play a AppStore. Tieto aplikácie sú väčšinou obmedzené v používaní (napríklad len utajené hovory alebo SMS) a vyžadujú registráciu na stránkach výrobcov. Medzi ne patrí aplikácia Babel, ktorá pracuje na podobnom princípe ako ostatné aplikácie a jej výhodou je, že pracuje na všetkých zariadeniach s rôznymi operačnými systémami. Pokiaľ chceme plnohodnotne využiť túto aplikáciu, je nutné zakúpenie licencie.

Pokiaľ osobný ochranca a chránená osoba nechcú využívať spomínané aplikácie a zariadenia, existuje variant pre zariadenia s operačným systémom iOS od firmy Apple, kde už sú nainštalované aplikácie FaceTime a iMessage, ktoré už majú v sebe natívne zabudované kryptovacie funkcie.

II. PRAKTICKÁ ČASŤ

3 KRITÉRIA OSOBNÉHO OCHRANCU A CHRÁNENEJ OSOBY

Kritéria osobného ochrancu a chránenej osoby musia byť splnené už na začiatku dohody. Aby práca bola efektívna, musia mať obe strany technické vybavenie na vyššej úrovni, ako mobilný telefón a rádiovú stanicu. Je možnosť, pokiaľ klient nemá dostačujúci prostriedok na komunikáciu, osobný ochranca má možnosť mu zapožičať dané prostriedky na dobu ich pracovného vzťahu.

Mobilný telefón môže osobný ochranca zapožičať, pokiaľ chránená osoba nemá adekvátny mobilný telefón k zabezpečeniu (napríklad nemá slot na MicroSD kartu kvôli zabezpečovaciemu čipu alebo nemá taký istý program ako osobný ochranca).

Každý osobný ochranca s chránenou osobou pri práci s rádiostanicou si musia určiť kódové slová, ktoré musia byť v počte max. päť slov na ľahké zapamätanie. Príklady slov sú na situácie ako nebezpečenstvo, na stretávku na určité miesto, presun a iné, na ktorých sa dohodnú vopred.

3.1 Určenie dosahu rádiostaníc

Každá rádiostanica má určitý dosah, ktorý závisí od rozličných podmienok, ktoré sú na prvom mieste šírenie krátkych vĺn, na druhom mieste typy a umiestnenia antén a na treťom mieste dosah ovplyvňuje daný typ rádiostanice, čiže jej kvalita modulácie. Taktiež záleží od počasia a od terénu, kde sa rádiostanice nachádzajú. Dosah zariadení nie je určený presne, dá sa len odhadnúť na aktuálnych podmienkach a v akom prostredí sa nachádza osoba.

3.1.1 Profesionálne rádiostanice

Profesionálne rádiostanice s prevádzačmi pre komerčné použitie je nutné požiadať Český telekomunikačný úrad o udelenie individuálneho oprávnenia k využívaniu rádiových kmitočtov. Za poplatok sa dá vytvoriť rádiová sieť s dosahom až desiatky kilometrov iba pre danú firmu. Orientačne sa dá povedať, že ročný poplatok za jeden vlastný kmitočet pre rádiovú sieť s dosahom približne dvadsaťpäť kilometrov je približne 8 000,- Kč. [31]

3.1.2 Občianske rádiostanice

Občianske rádiostanice, ktoré nie sú spoplatňované pásmami, pracujú medzi sebou na vzdialenostiach, ktoré vysielajú a prijímajú signál medzi dvomi a viacerými anténami.

CB rádiostanice

CB rádiostanice pracujú v rozsahu frekvencií 26,565 – 27,405 MHz na osemdesiat kanálov pri maximálnom výkone 4 W. Dosah CB rádiostaníc je znázornený v nasledujúcej tabuľke:

Tab. č. 3 Dosah CB rádiostaníc [21]

Stanica 1	Stanica 2	Orientačný dosah
Ručná stanica (anténa 25 cm)	Ručná stanica (anténa 25 cm)	0,5-2 km
	Mobilná stanica v aute (anténa 1 m)	1-5 km
	Základňová stanica (anténa 5,5-6,5 m)	3-10 km
Mobilná stanica v aute (anténa 1 m)	Mobilná stanica v aute (anténa 1 m)	5-20 km
	Základňová stanica (anténa 5,5-6,5 m)	15-40 km
Základňová stanica (anténa 5,5-6,5 m)	Základňová stanica (anténa 5,5-6,5 m)	20-50 km

PMR rádiostanice

PMR rádiostanice pracujú v rozsahu frekvencií 446,00625 až 446,09375 MHz, k dispozícií je osem kanálov a má výkon 0,5 W. V PMR rádiostaniciach je rozhodujúca citlivosť prijímacieho modulu a veľkosť antény. Dosah rádiostanice je znázornený v nasledujúcej tabuľke s orientačnými hodnotami pri použití rádiostanice Cobra 975:

Tab. č. 4 Dosah PMR rádiostaníc [32]

Terén	Dosah
Otvorený bez prekážok	12 km
So stromami	Do 6 km
Zástavba	Do 2 km
Mesto	Niekoľko 100 metrov
Z kopca na kopec	Desiatky kilometrov

3.1.3 Mobilné telefóny

Mobilné telefóny, ktoré pracujú vo frekvenciách GSM 900, 1800, 1900 MHz komunikujú ako mobilná stanica so základňovou stanicou. Územie je rozdelené na elementárne časti, ktoré sa nazývajú bunky. Uprostred každej bunky je umiestnená základňová stanica, ktorá zaisťuje spojenie všetkých mobilných staníc so systémom. Každá bunka má iný tvar, záleží od veľkosti a hustoty osídlenia terénu. Dosah základňových staníc je pri výkone 50W 15 – 40 km a mobilný telefón sa pripojí na najbližšiu stanicu v každej bunke. [33]

3.1.4 Tiesňové tlačidlo a osobný alarm

Tiesňové tlačidlo pracuje v rozsahu komunikačného pásma 868 Mhz. Dosah tiesňového tlačidla by mal byť na priamu viditeľnosť približne 50 m. [43]

Dosah osobného alarmu závisí od použitých decibelov, väčšinou býva v rozsahu 110-130 dB. 110 dB by sa dalo prirovnať k strelnej zbrani alebo pneumatickému kladivu a do 130 dB štart prúdového lietadla. Z týchto informácií vyplýva, že použitie zvukového osobného alarmu je dosť hlučné a tým pádom vzdialenosti sa dajú určiť na veľký rozmer. Taktiež závisí aj od prostredia a terénu, kde sa osobný alarm využije. [34]

4 ANALÝZA KOMUNIKAČNÝCH A SIGNALIZAČNÝCH PROSTRIEDKOV

Osobný ochranca pri svojej práci využíva komunikačné a signalizačné prostriedky, ktoré sú jeho povinnou výbavou pre výkon povolania. Každý osobný ochranca by mal mať kurzy spojenia, aby zvládol obsluhu rádiostanice a vedel šifrovane komunikovať v rádio rozhovoroch. Tak isto je dôležité, aby okrem rádiostaníc využíval mobilný telefón na komunikáciu s chránenou osobou, prípadne dispečingom alebo inými dôležitými kontaktmi. Pre osobných ochrancov je typické, že majú dva mobilné telefóny. V primárnom telefóne má uložené všetky kontakty a poznámky a sekundárny telefón využíva k jednorazovým účelom, aby nenastala možnosť odsledovania. Tiesňové tlačidlá používajú osobní ochrancovia ako doplnok buď pre prípad zranenia alebo pre svojho klienta, ktorý sa nachádza v nebezpečenstve a tým privolá osobného ochrancu. Tiesňové tlačidlo vo forme osobného alarmu slúži ako ochranný prostriedok pre pasívne chránenie seba samého, kedy vyvolá akustický alarm o rôznej frekvencií a hlasitosti. [35][36]

4.1 Technické parametre komunikačných a signalizačných zariadení

Každé zariadenie je odlišné. Každý výrobca rádiostaníc, mobilných telefónov a signalizačných prostriedkov má svoje charakteristické prvky, a preto sa parametre týchto zariadení môžu odlišovať. Komunikačné a signalizačné prostriedky pracujú na svojich princípoch a preto sa musia odlišovať v používaní.

4.1.1 Mobilný telefón Samsung Galaxy S4

Tento mobilný telefón roku 2013/2014 je jeden z najlepšie vybavených smartphonov s operačným systémom Android. Využíva na dnešnú dobu najnovší hardware aj software.

Pre prácu osobného ochrancu je vhodný najmä tým, že má veľký displej, kde môže pracovať s kontaktmi, zaznamenávať stretnutia, využívať GPS a prehliadanie internetu.

Pre šifrovanú komunikáciu má tento smartphone výhodu v tom, že sa tu dajú použiť všetky šifrovacie hardwarové aj softwarové techniky.

Taktiež je k telefónu možnosť dokúpenia veľkého množstva príslušenstva ako sú drôtové a bezdrôtové handsfree, ochranné puzdra a fólie, náhradné baterky a pridané akumulátory.

Obr. č. 11 Samsung Galaxy S4 [37]

Tab. č. 5 Technické parametre Samsung Galaxy S4 [37]

Displej	SUPER AMOLED, 4,99``
Rozmery	136,6 x 69,8 x7,9 mm
Hmotnosť	130 g
Akumulátor	2600 mA
Pamäť	16/32/64 GB
RAM	2 GB
Pamäťové karty	áno, do 64 GB
Chipset	Qualcomm Snapdragon 600
Procesor	4×1,9 GHz
Grafika	Adreno 320

Tab. č. 6 Sieťová a dátové parametre Samsungu Galaxy S4 [37]

GMS pásma	850/900/1800/1900 MHz
3G pásma	850/900/1900/2100 MHz
LTE pásma	800/850/900/1800/2100/2600 MHz
GPRS/EDGE	áno
HSPA	42 / 5,76 Mb/s

4.1.2 Ručná profesionálna rádiostanica Hytera PD785 – VHF, UHF

Táto profesionálna ručná digitálna rádiostanica značky Hytera, pracujúca v štandardu DMR s funkciou GPS dokáže pracovať v digitálnom aj analógovom móde. Výber tejto rádiostanice pozostáva podľa funkčnosti, použitej technológie a možnosťou pracovania v oboch módoch.

Táto profesionálna ručná rádiostanica je vhodná pre osobného ochrancu z dôvodov použitia analógovej aj digitálnej siete, novými vylepšenými technológiami (lepší zvuk, pridané GPS, posielanie krátkych správ, prenos dát, aktualizovaný software, pokročilé nastavovanie funkcií rádiostanice) a spĺňa náročné vojenské normy MIL a stupeň krytia IP57.

Štandardné príslušenstvo v balení obsahuje akumulátor Li-Ion o kapacite 2000 mA, napájač, rýchlo-nabíjač, dlhý klip na opasok, kožené púzdro a anténu. Pre efektívnejšie využitie je vhodné dokúpenie externého mikrofónu alebo slúchadla s mikrofónom. [38]

Obr. č. 12 Ručná rádiostanica Hytera PD785G – VHF, UHF [38]

Tab. č. 7 Technické parametre Hytera PD785G [38]

Frekvencia	400-470 MHz
Počet kanálov	256
Počet zón	32
Napájanie	7,4 V
Rozmery	119 x 55 x 33 mm
Hmotnosť	320 g
Pracovná teplota	-30°C až + 60°C

Tab. č. 8 Parametre prijímača Hytera PD785G [38]

Citlivosť (Analógová)	0,3-0,4 µV / 12-20 dB SINAD
Citlivosť (Digitálna)	0,3 µV/BER 5%
Selektivita	60-70 dB
Výkon	0,5 W

Tab. č. 9 Parametre vysielača Hytera PD785G [38]

Výstupný výkon	4 W/1 W
FM šum	40-45 dB/ 12,5-25 kHz

4.1.3 Vozidlová profesionálna rádiostanica Hytera MD 785G – VHF, UHF

Profesionálna vozidlová rádiostanica, ktorá je vysoko odolná, pracuje v štandarde DMR, s funkciou GPS komunikuje v digitálnom aj analógovom móde, má stupeň krytia IP 54 a vojenské MIL štandardy.

Táto vozidlová profesionálna rádiostanica je vhodným riešením pre osobného ochrancu použitia v aute. Má podobné parametre ako ručná profesionálna rádiostanica Hytera PD785G – VHF, UHF. [39]

Obr. č. 13 Vozidlová rádiostanica Hytera MD 785G – VHF, UHF [39]

Tab. č. 10 Technické parametre Hytera MD 785G [39]

Frekvencia	400-470 MHz
Počet kanálov	256
Počet zón	32
Napájanie	16,6 V
Rozmery	174 x 60 x 200 mm

Hmotnosť	1,7 kg
Pracovná teplota	-30°C až + 60°C

Tab. č. 11 Technické parametre prijímača Hytera MD 785G [39]

Citlivosť (Analógová)	0,22-0,4 µV / 12-20 dB SINAD
Citlivosť (Digitálna)	0,3 µV/BER 5%
Selektivita	60-75 dB
Výkon	3 W

Tab. č. 12 Technické parametre vysielača Hytera MD 785G [39]

Výstupný výkon - nízka frekvencia	400-470 MHz, 5-25 W
Výstupný výkon - vysoká frekvencia	400-470 MHz, 5-45 W
FM šum	40-45 dB/ 12,5-25 kHz

4.1.4 Ručná CB rádiostanica ALAN 42 MULTI

Ručná CB rádiostanica, má multifunkčné využitie. Okrem toho, že je ručná, dá sa pripojiť k 12V napájaniu v aute a externej anténe.

Táto rádiostanica bola vybraná z dôvodu cenovej dostupnosti, možnosti kombinácie ručnej a vozidlovej rádiostanice, možnosti úpravy rádiostanice na vyšší počet kanálov a bohatého príslušenstva, ako napríklad sieťová nabíjačka, klip na opasok, anténa BNC, vozidlový adaptér na pripojenie externej antény a napájania, obal a puzdra na akumulátory . [40]

Obr. č. 14 Ručná CB rádiostanica ALAN 42 MULTI [40]

Tab. č. 13 Technické parametre ALAN 42 MULTI [40]

Frekvencia	26,965-27,405 MHz
Kanál	80
Modulácia	AM/FM
Napájanie	7,2 - 13,8 V
Rozmery	70 x 140 x 30 mm
Hmotnosť	190 g

Tab. č. 14 Parametre vysielača ALAN 42 MULTI [40]

Výstupný výkon	Hi/Lo 4/1 W(12V) 1,5/0,7 W (7,2V)
Kmitočtový zdvih	2 kHz

Tab. č. 15 Parametre prijímača ALAN 42 MULTI [40]

Citlivosť	0,25 µV/10 dB SINAD
Frekvenciový zdvih	10,695 MHz/455 kHz
Výkon zosilovača	500 mW/8Ω

4.1.5 Vozidlová CB rádiostanica ALBRECHT AE 5290

Komfortná vozidlová rádiostanica s možnosťou výberu podsvietenia ponúka Scan, pamäť, možnosť vysielania AM/FM, výber z 80 kanálov, ovládanie kanálov na mikrofóne s bohatým príslušenstvom. Táto rádiostanica je schválená k používaniu štátmi CEPT.

Pre prácu osobného ochrancu je výhoda, že si môže nastaviť z 80 kanálov, dokáže si vybrať podsvietenie displeja a taktiež si môže prepínať modulácie AM/FM.

Príslušenstvo tejto rádiostanice je v balení obsiahle, je tu dodávaný mikrofón, držiak stanice, napájací kábel, držiak mikrofónu a dokumentáciu. [41]

Obr. č. 15 Vozidlová CB rádiostanica ALBRECHT AE 5290 [41]

Tab. č. 16 Technické parametre ALBRECHT AE 5290 [41]

Frekvencia	26,565-27,405 MHz
Kanál	80 AM/FM 12 AM/FM
Modulácia	AM/FM
Napájanie	13,8 V
Rozmery	185 x 40 x 140 mm
Hmotnosť	0,83 kg

Tab. č. 17 Technické parametre prijímača ALBRECHT [41]

Citlivosť	0,65 µV/20 dB SINAD
Selektivita	65 dB
Frekvencia medzirozhrania	10,695 MHz/455kHz
Výkon	2W/8Ω

Tab. č. 18 Technické parametre vysielača ALBRECHT [41]

Výstupný výkon	1/4 W AM/FM
Výkon zosilovača	2,5W/1kΩ
Frekvenciový zdvih	2 kHz

4.1.6 Motorola TLKR T60

Motorola TLKR T60 je PMR rádiostanica vo vyššej triede. Táto rádiostanica je vhodná pre outdoorové aktivity, je vodotesná a nárazuvzdorná, má výkonnejšiu anténu pre väčší dosah až desať kilometrov.

Táto PMR rádiostanica bola vybraná kvôli tomu, že patrí do vyššej triedy a tým pádom je aj drahšia. V balení obsahuje dva kusy rádiostaníc, príslušenstvo dvoch kusov nabíjacích akumulátorov, stolný nabíjač 220 V a dva kusy klipu na opasok.

Použitie osobným ochrancom a jeho klientom je vhodná možnosť pri zlyhaní všetkých komunikačných prostriedkov a tým, že má outdoorové vlastnosti, nie je problém chrániť klienta aj pri turistike.

Okrem klasických funkcií obsahuje funkcie typu Room Monitor, TOT, Scan, Vox, Auto Squelch, Roger Beeb, Power safe, Chanel Busy Alert, Stopky, DW. [42]

Obr. č. 16 PMR rádiostanica Motorola TLKR T60 [42]

Tab. č. 19 Technické parametre Motorola TLKR T60 [42]

Frekvencia	446,00625 - 446,09375 MHz
Kanál	8
Napájanie	4x UM3/AAA
Rozmery	55 x 200 x 30 mm
Výkon	0,5 W
Pracovná teplota	-20°C až + 55°C

4.1.7 Tiesňové tlačidlo Jablotron RC - 87

Tiesňové tlačidlo od firmy Jablotron RC – 87 umožňuje na diaľku aktivovať tiesňový poplach. Tlačidlo komunikuje bezdrôtovým protokolom Oasis a je napájané z batérie. Toto tlačidlo sa môže nosiť ako náramkové hodinky alebo prívesok na krku. Pokiaľ sa chce nosiť na krku, musí mať mechanickú poistku, na ktorú treba vynaložiť 40 N a viac pre rozpojenie.[43]

Obr. č. 17 Tiesňové tlačidlo RC-87 [43]

Tab. č. 20 Technické parametre RC – 87 [43]

Frekvencia	868 MHz, protokol Oasis
Napájanie	Lithiová batéria typu CR 2032 (3V)
Krytie	IP 44
Pracovné teplota	-20°C až + 50°C

Osobný alarm Konig SEC – APS 10 umožňuje vyvolať akustický zvuk vo výške 130 dB. Slúži ako improvizovaný prostriedok pre klienta, keď sa nachádza v inej miestnosti ako osobný ochranca. [44]

Obr. č. 18 Osobný alarm Konig SEC – APS 10 [44]

Tab. č. 21 Technické parametre Konig SEC – APS 10 [44]

Hlučnosť	130 dB
Napájanie	2 x AAA batérie
Rozmery	52 x 105 x 17 mm
Hmotnosť	53 g
Dĺžka pútka	155 mm

4.2 Užívateľský komfort nosenia komunikačných a signalizačných zariadení

Užívateľský komfort závisí vždy od podmienok danej akcie a od oblečenia, kde sa osobný ochranca a chránená osoba nachádzajú. Väčšinu klientov, ktorí si objednávajú služby osobných ochrancov, sú vysokopostavení ľudia, ktorí chodia väčšinou v primeranom spoločenskom odeve, ale nastávajú také situácie, kedy chodia aj v civilnom odeve. Preto sa osobný ochranca musí prispôsobiť svojmu klientovi svojim odevom pre danú situáciu.

4.2.1 Prenosná rádiostanica

Použitie prenosnej rádiostanice nie je v bežnom živote úplne prirodzené. Použitie závisí od toho, o akú akciu sa jedná a od použitia odevu pre danú akciu. Pri spoločenskom odeve ochrancovia nosia prenosné rádiostanice prevažne v rukách s použitím slúchadla s mikrofónom. Pokiaľ nastane nežiaduca situácia, prenosné rádiostanice si pripnú na opasok a idú do akcie. Ďalšia možnosť je taká, že ich majú celý čas pripnuté klipom na opasku s použitím slúchadla s mikrofónom.

4.2.2 Mobilný telefón

Mobilný telefón je zariadenie, ktoré sa používa denne. Vo väčšine prípadov nie je problém nosenia (záleží od rozmerov). Mobilný telefón môže byť nosený vo vrecku nohavíc, v saku alebo v puzdre na opasku, a tým pádom je to úplne normálna vec, ktorá nespôsobuje žiadne podozrenie, pretože mobilný telefón v dnešnej dobe má každý človek.

4.2.3 Tiesňové tlačidlo

Tiesňové tlačidlo má malé rozmery, takže nie je žiaden problém ho nosiť v bežnom odeve. Môže mať formu náramkových hodiniek, prichytené klipom na opasku, zavesené na krku, ženy ho nosia vložené v kabelke alebo ho majú zavesené na kabelke.

4.3 Vlastnosti komunikačných a signalizačných prostriedkov

Každý komunikačný a signalizačný prostriedok by mal mať vlastnosti, ktoré sa hodia na prácu u osobného ochrancu a jeho klienta. Preto pri výbere vhodných prostriedkov by sa mali naštudovať ich vlastnosti, porovnať viacerých výrobcov a modely a vybrať najvhodnejšie prostriedky.

4.3.1 Vlastnosti rádiostaníc

Rádiostanice podľa určenia by mali spĺňať požiadavky na prácu osobného ochrancu. Občianske rádiostanice nie sú tak náročné, ako tie profesionálne, a preto sa u občianskych rádiostaníc dajú tolerovať menšie nároky ako na profesionálne rádiostanice. Väčšina profesionálnych rádiostaníc je testovaná podľa amerických armádnych noriem MIL-STD 810 C, D a E na použitie v prostredí s nízkym tlakom, nízkou a vysokou teplotou, s prudkými teplotnými zmenami, odolnosťou proti slnečnému žiareniu, dažďu, slanému prostrediu, prachu, vlhkosti a nárazom a samozrejme použitie stupne krytia IP XX, čiže proti vniknutiu mechanických častí do zariadení a vniknutie vody do zariadení. Profesionálne rádiostanice majú stupeň krytia IP54/55. To znamená, že u IP 54 sú chránené pred prachom a proti striekajúcej vode, IP55 sú chránené proti prachu a proti striekajúcej vode v rôznych smeroch. Niektoré modely majú dokonca stupeň krytia IP67, čo znamená, že sú prachotesné a majú ochranu proti účinkom dočasného ponorenia do kvapaliny. [31]

4.3.2 Vlastnosti mobilných telefónov

Vlastnosti mobilných telefónov sú dôležitou súčasťou práce osobného ochrancu a chránenej osoby. V súčasnosti je na trhu mnoho druhov mobilných telefónov rôznych veľkostí, tvarov, použitých materiálov, prevedenia konštrukcie (nárazuvzdornosť, pogumovanie, stupeň krytia IP XX proti prachu a vode).

Väčšina mobilných telefónov je klasických a špeciálne vlastnosti odolnosti sa môžu nahradiť zakúpením špeciálneho príslušenstva (napríklad outdoorový kryt, vodotesný kryt, fólie na displej).

4.3.3 Vlastnosti tiesňových tlačidiel a osobných alarmov

Tiesňové tlačidlá a osobné alarmy majú funkciu ako doplnok alebo ako improvizovaný charakter, takže tieto potom nemusia spĺňať až také náročne podmienky ako rádiostanice a mobilné telefóny. Pri týchto signalizačných prostriedkoch môže byť určitá nárazuvzdornosť, stupeň krytia IP XX proti prachu a vode a mechanická odolnosť.

4.4 Improvizované spôsoby

Improvizované spôsoby nastávajú pri ako zlyhaní komunikačných prostriedkov. Zlyhanie môžu byť nasledovné:

- mechanické poškodenie
- elektronické poškodenie
- poškodenie prachom a vodou (pokiaľ nespĺňajú krytie IP XX)
- vybitie akumulátora následkom zimy
- spálenia akumulátora následkom tepla
- stratou, odobraním alebo ukradnutím zariadenia

Improvizovaným spôsobom môže byť napríklad krátky telefonát z pevnej linky alebo použitie rádiostaníc PMR, ktoré sa dajú kúpiť v každom obchode s elektronikou. Pokiaľ osobný ochranca a chránená osoba sa nachádzajú vo viditeľnej blízkosti, môžu na seba upozorniť signálom (gesto, slovo, veta, zvuk) pre prípadne nebezpečenstvo alebo evakuáciu.

Dosť netradičným spôsobom môže byť použitie chemického svetla ako znamenia pre určitú udalosť (nebezpečenstvo alebo evakuácia).

5 NÁVRH UTAJENEJ KOMUNIKÁCIE

Utajená komunikácia v súčasnosti je dôležitým spôsobom medzi chránencom a chránenou osobou, a preto by mala byť navrhnutá možnosť používania utajenej komunikácie. V utajenej komunikácií je dôležitým faktorom čas, kedy osobný ochranca a chránená osoba si dajú medzi sebou vedieť o rôznych situáciách a spoliehajú sa na to, aby nebolo možné odsledovať ich aktuálnu polohu pri komunikácií napríklad mobilným telefónom. Preto by sa mali navrhnúť možnosti utajenia komunikácie, najideálnejšie pomocou mobilných aplikácií určených pre tento účel. Mobilné aplikácie za účelom šifrovania hovorov, správ a súborov pracujú viac-menej na rovnakom princípe s nejakými vlastnými detailmi (použitie šifrovacích algoritmov rôznych bitových dĺžok, metódy šifrovania, platenými licenciami). Ako ukážku použitia mobilnej aplikácie som vybral aplikáciu Phone-X, ktorá je v nasledovných kapitolách komplexne popísaná. Ostatné šifrovacie aplikácie pracujú na rovnakom princípe, s malými zmenami od programátorov (napríklad iné dĺžky šifrovacích kľúčov, použité algoritmy, odlišné funkcie...).

5.1 Phone-X

Phone-X je mobilná aplikácia, ktorá umožňuje šifrovať hlasové hovory a súčasne posielať zašifrované správy na zariadeniach s operačným systémom Android. Okrem zašifrovaných hovorov a správ dokáže bezpečne posielať súbory, má bezpečne uložené kontakty s on-line stavom prítomnosti užívateľa, má jednoduchý a bezpečný systém a systém je funkčný aj na technológií EDGE pritom s možnosťou plynulého hovoru za plného šifrovania. [45]

5.1.1 Výhody a nevýhody používania Phone-X

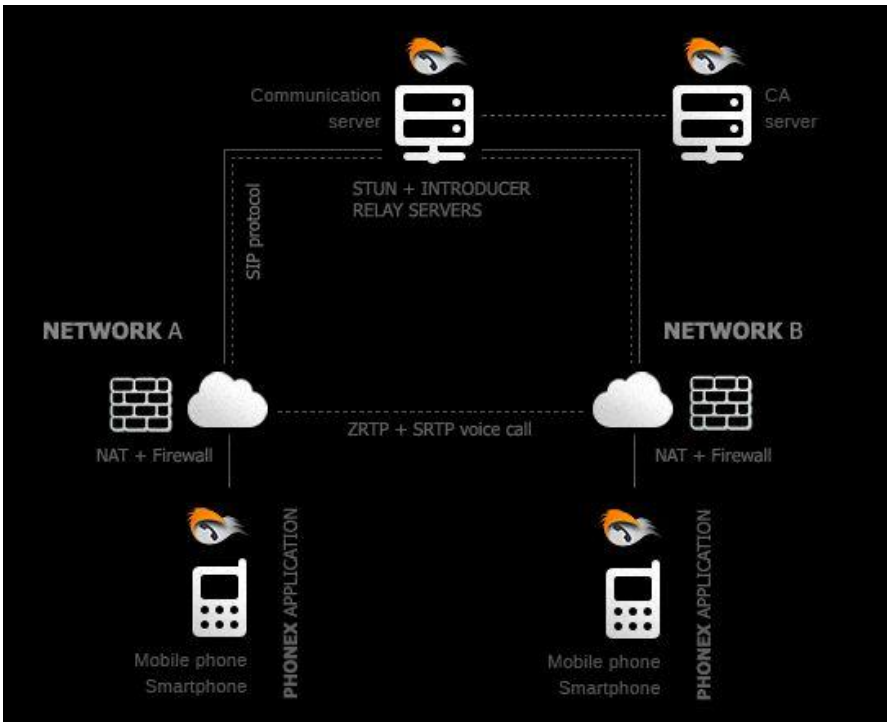
Výhodou používania aplikácie Phone-X je to, že jedna licencia je kompatibilná s celým svetom, nepočuť ozvenu počas hovoru, nie je tu žiadny ľudský administrátor, zabraňuje útoku men-in-the-middle, šifrovanie funguje na princípe End-To-End s AES 256 a Twofish, server nevidí a nepočuje komunikáciu, nezálohuje sa na žiadnom serveri, používanie mobilných dát a WIFI, funguje aj pre roamingové hovory a má veľmi jednoduché ovládanie.

Nevýhodou tejto aplikácie je, že sa musí obnovovať licencia, či už mesačne alebo ročne, pričom náklady sú pomerne vysoké. Ďalšou nevýhodou je, aby aplikácia správne fungovala, teda aby bolo efektívne šifrovanie, musia mať túto aplikáciu nainštalované obe strany. [45]

5.1.2 Princíp fungovania Phone-X

V jednoduchosti Phone-X funguje anonymne, bezpečne, jednoducho a mobilne. V širšom zmysle je to nasledovné:

- Každý užívateľ má vlastný X.509v3 certifikát, podpísaný svojím serverom. Ten získa po prvom prihlásení do aplikácie. Generuje sa v zariadení klienta a na server sa pošle podpis. Je tu využívaná symetrická šifra.
- Komunikácia so serverom je ďalej šifrovaná pomocou TLS, prebehne overenie certifikátu serveru a klienta .
- Použitie protokolu SIP.
- Protokol ZRPT je použitý na ustanovení jednorazových kľúčov v prvých sekundách spojenia hovoru medzi dvoma stranami. Po ukončení sú kľúče zničené. Hovor je šifrovaný symetrickou šifrou AES a Twofish.
- Server počas hovoru neprijímá ani neodosiela žiadne dáta.
- Man-in-the-middle obrana proti ZRPT – obe strany si navzájom povedia SAS reťazec. Kontroluje sa tiež zhoda ZRPT hash v ZRPT protokolu a súčasne získaný hash v SDP session pri ustanovení hovoru.
- Správy sú šifrované verejným kľúčom cieľovej osoby a podpísané privátnym kľúčom CA.
- Prijatá správa je dešifrovaná privátnym kľúčom, podpis sa overuje verejným kľúčom odosielateľa. V prípade chyby sa zobrazuje upozornenie.
- V prípade narušenia sa hovor ukončí.
- Phone-X používa zašifrované SQLCIPHER úložisko pre ukladanie citlivých dát v telefóne, čiže v prípade odcudzenia telefónu nie je možné zistiť privátny kľúč alebo ostatné dáta bez hesla [46]



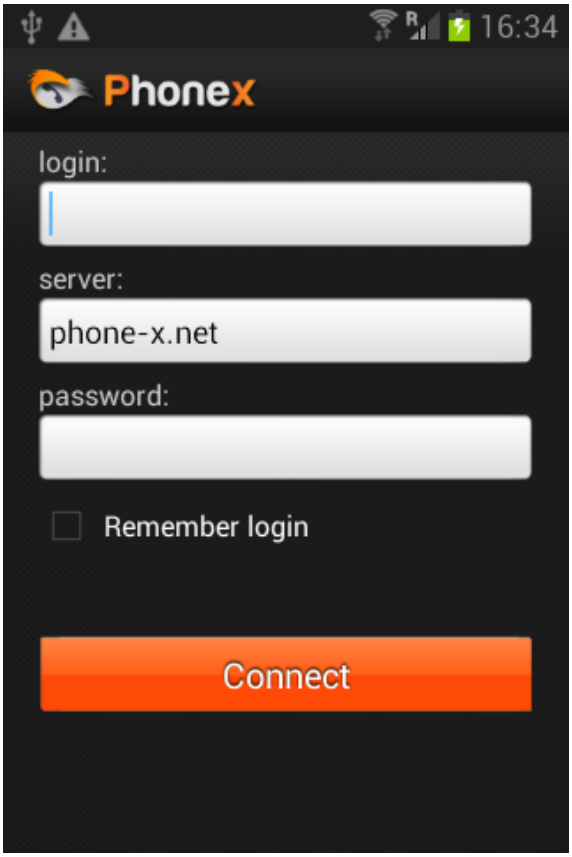
Obr. č. 19 Komunikačné schéma [46]

5.1.3 Inštalácia Phone-X

Prvotným krokom k získaniu aplikácie Phone-X je inštalácia z Google Play. Po pripojení na internet mobilným telefónom treba nájsť aplikáciu PhoneX – Bezpečná komunikácia a tú stiahnuť do mobilu. Ďalším krokom je potreba na stránke *http://www.phone-x.net/cz/objednavka* si vybrať licenciu, ktorá sa bude používať. Na výber je možnosť mesačnej alebo ročnej licencie. Posledným krokom je objednanie a zaplatenie a tým pádom je celkový proces inštalácie ukonený. [47]

5.1.4 Prihlásenie

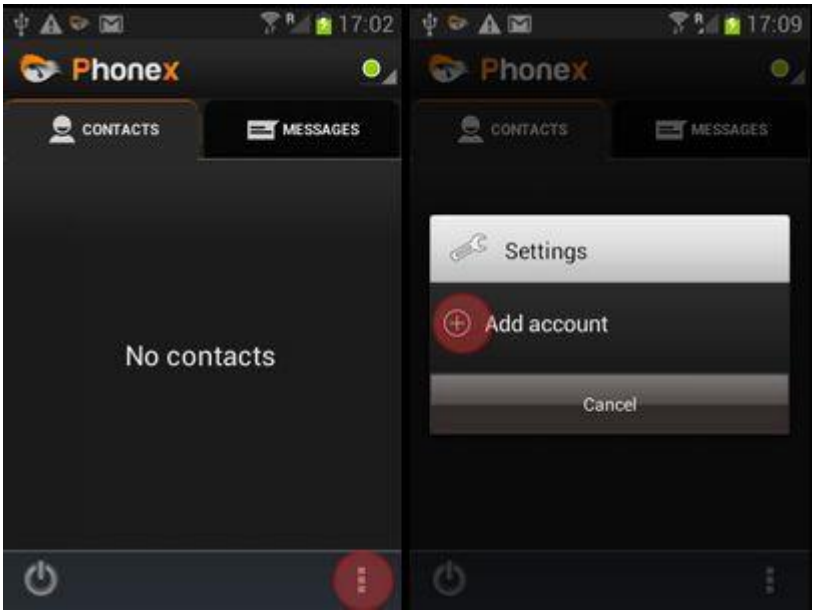
Pri prvom spustení aplikácie je potreba prihlásiť sa. Údaje o prihlasovacom mene a hesle sú následne priradené po zakúpení licencie. Po prvom prihlásení je na ďalšej obrazovke výzva k zmeneniu hesla, ktoré si aplikácia môže alebo nemusí pamätať, záleží len na užívateľovi. Po zmene hesla sa spustí do hlavnej obrazovky. [48]



Obr. č. 20 Prihlasovanie do Phone-X [48]

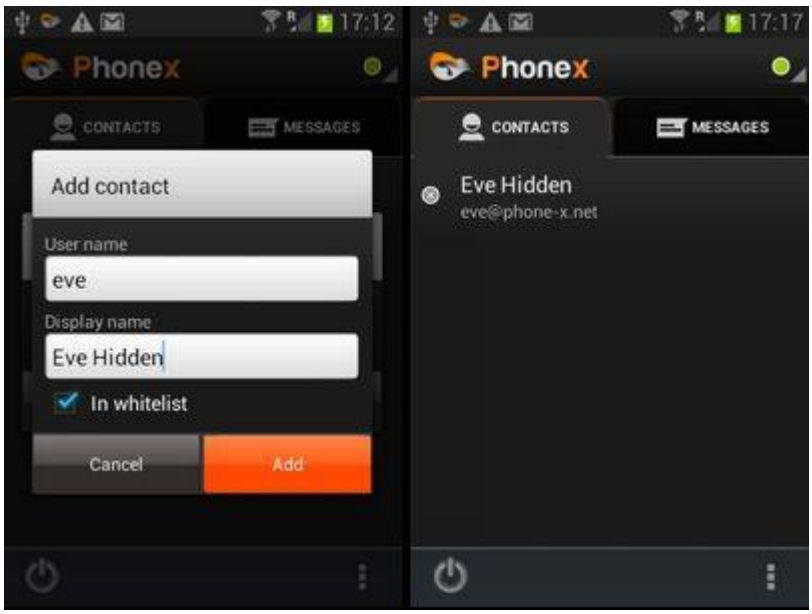
5.1.5 Pridanie kontaktov

V tomto postupe je ukázané, ako sa dvaja užívatelia môžu vzájomne pridať do aplikácie. Užívateľ "XYZ" chce pridať nového užívateľa s názvom "Eve" do svojho zoznamu kontaktov. Je treba kliknúť na tlačidlo v *pravom dolnom rohu* (ľavá strana obrázka) a potom potvrdiť tlačidlom *Add account* (pravá strana obrázka). [48]



Obr. č. 21 Vytvorenie kontaktu pre utajenú komunikáciu [48]

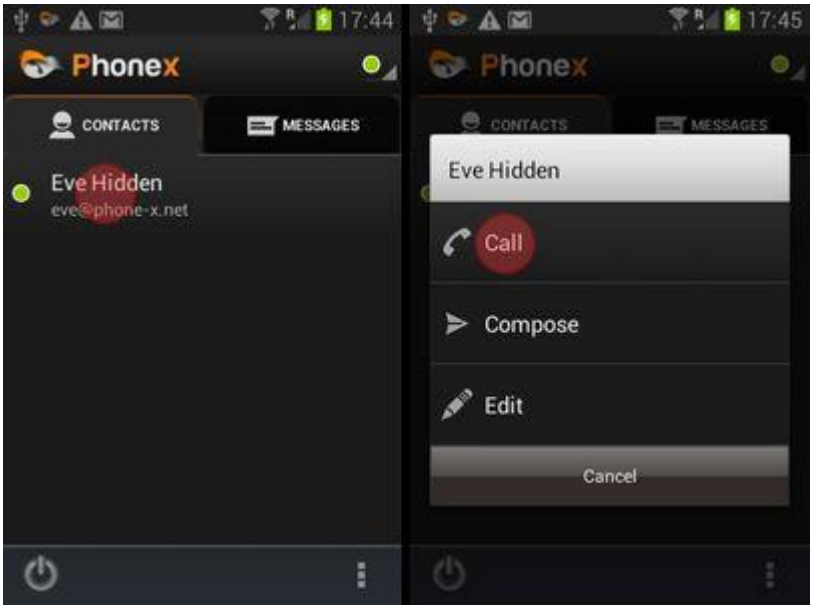
V dialógovom okne sa zadá do políčka *User name* užívateľské meno kontaktu - "Eve", kde sa môže tiež vyplniť políčko *Display name*, čo znamená prezývka kontaktu, ako sa má zobraziť (ľavá strana obrázku). Na záver je treba kliknúť na tlačidlo *Add* a tým pádom sa pridá novo vytvorený kontakt (pravá strana obrázku). [48]



Obr. č. 22 Vytvorený kontakt [48]

5.1.6 Šifrovaný hovor

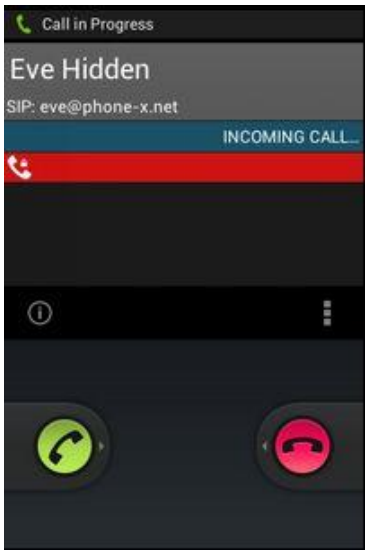
Podmienkou pre šifrovaný hovor je mať oboch účastníkov v kontaktoch aplikácie. Pre uskutočnenie hovoru je potrebné vybrať kontakt (ľavá strana obrázka), kliknúť naň a vybrať voľbu *Call* (pravá strana obrázka). [48]



Obr. č. 23 Utajené telefonovanie [48]

Po spojení oboch strán sa objaví obrazovka hovoru s červeným pruhom (ľavá strana obrázka) a to znamená, že ešte šifrovaná komunikácia nebola nadviazaná. Čas na naviazanie šifrovanej komunikácie trvá približne tri sekundy. Po nadviazaní šifrovania telefón zavibruje a informačný pruh zmení farbu z červenej na zelenú. Pre ukončenie hovoru treba stlačiť červené tlačidlo v dolnom rohu na obrazovke. Pokiaľ sme na strane volaného, tak postupujeme ako u klasického prijatia/nepriatia hovoru ako na telefónoch so systémom Android (obrázok). [48]

Obr. č. 24 Priebeh volania [48]

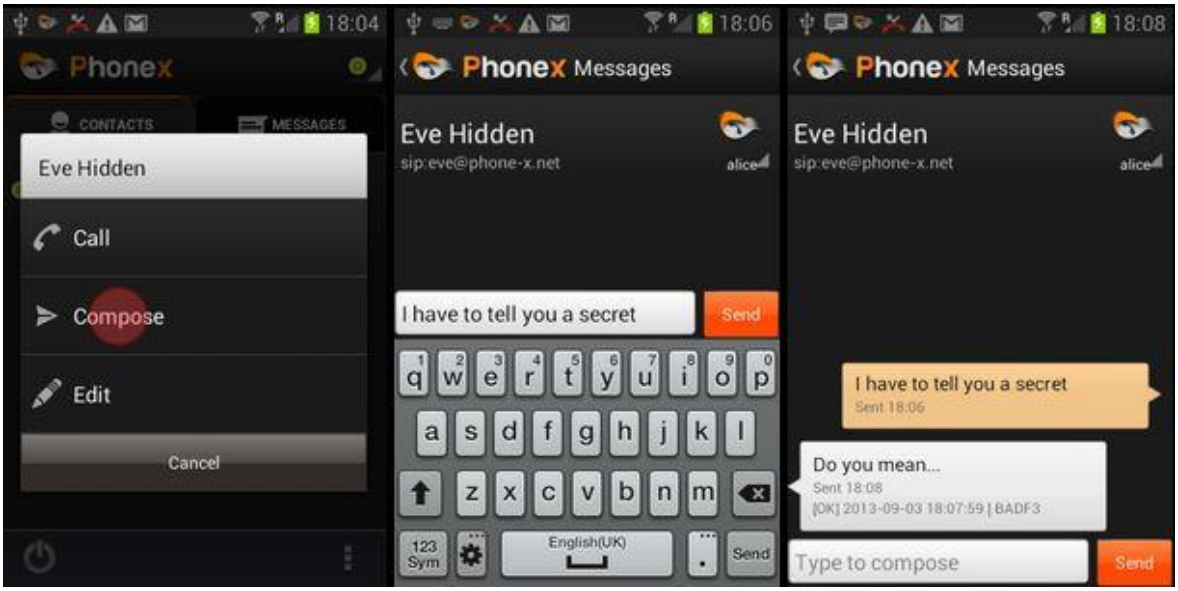


Obr. č. 25 Výber možnosti prijať/odmienúť hovor [48]

5.1.7 Šifrovaná správa

Posielanie šifrovaných správ prebieha podobne ako u klasických správ. Základnou podmienkou je mať uložené kontakty oboch účastníkov konverzácie, aby mohlo dôjsť k šifrovanej správe. Postup je taký, že sa vyberie kontakt, na ktorý sa klikne, v ponuke stlačíme tlačidlo *Compose (ľavá strana obrázka)*. Objaví sa pole s klávesnicou (stred

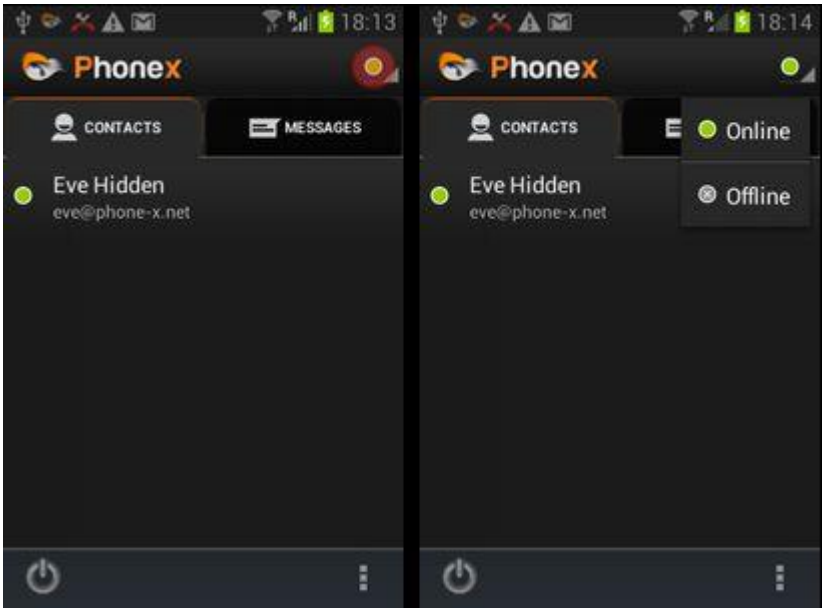
obrázka), napíše sa správa a nakoniec sa odošle po kliknutí tlačidla *Send* (pravá strana obrázka). [48]



Obr. č. 26 Vytvorenie SMS správy [48]

5.1.8 Status užívateľa

Aplikácia Phone- X má možnosť prepínania medzi statusmi *Online/Offline*. Po prihlásení do aplikácie sa automaticky užívateľ prepne do statusu Online a všetci prihlásení užívatelia uvidia novo prihláseného ďalšieho užívateľa. Pri funkcií Offline je užívateľ, ktorý nechce byť videný pred ostatnými užívateľmi. V tomto režime sa dajú stále prijímať hovory a správy. [48]



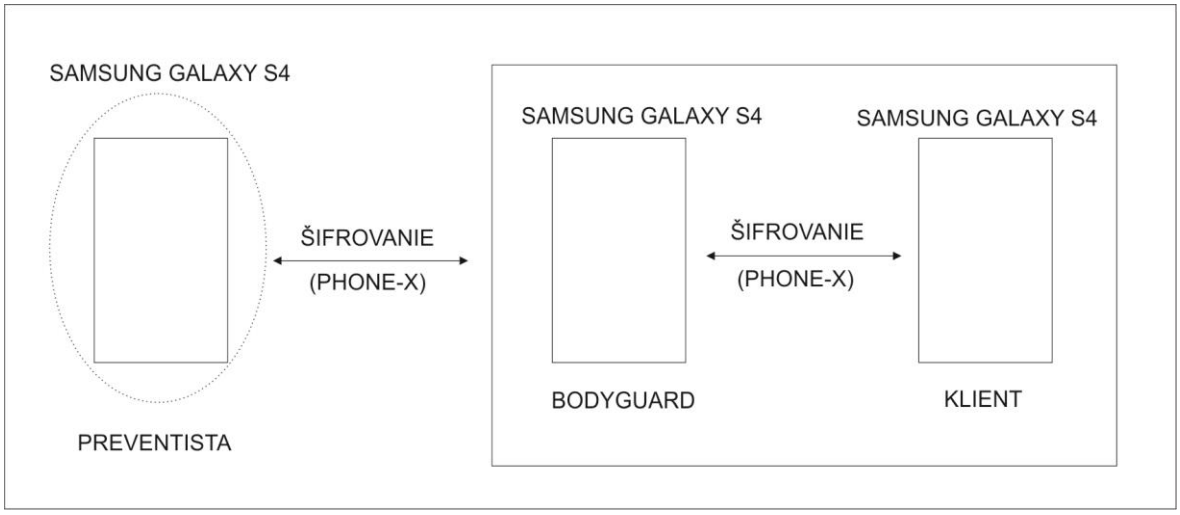
Obr. č. 27 Status užívateľa [48]

5.2 Grafické znázornenie komunikácie

Grafické znázornenie komunikácie je rozdelené do troch častí, a to ako komunikuje osobný ochranca s klientom, poprípade s klientovými rodinnými príslušníkmi a s preventistom, ktorý úzko spolupracuje s osobným ochrancom.

5.2.1 Mobilná komunikácia

Pomocou mobilnej komunikácie sa dá komunikovať prakticky nonstop medzi osobnými ochrancami, klientmi a preventistami. Mobilná komunikácia si vyžaduje určité šifrovanie, aby nevznikla možnosť odsledovania hovoru. Znázornenie je v nasledujúcom obrázku:



Obr. č. 28 Schéma komunikácie s mobilným telefónom

5.2.2 Komunikácia rádiostanicami

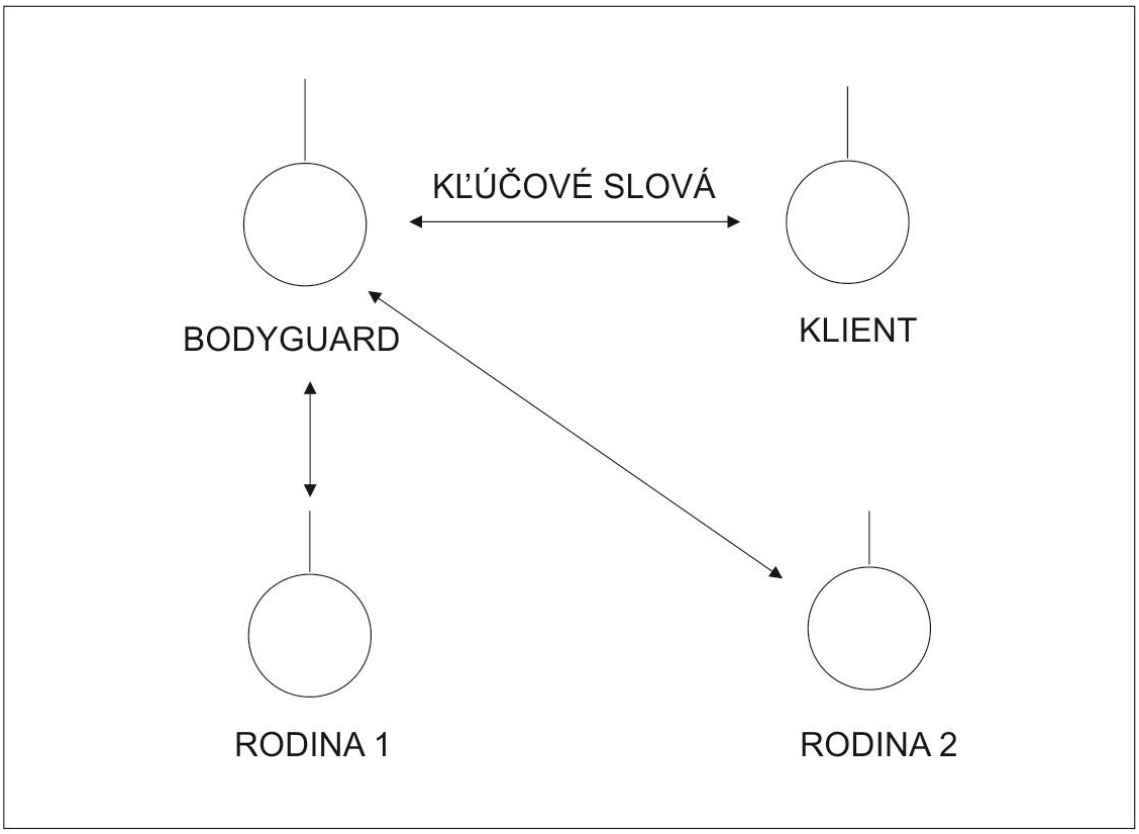
Komunikácia pomocou rádiostaníc je druhá možnosť komunikácie medzi osobnými ochrancami a klientmi. Komunikácia prebieha pomocou CB alebo PMR rádiostaníc. Narozdiel od mobilných telefónov, ktoré sú nonstop zapnuté, rádiostanice sa používajú len obmedzený čas. Najskôr sa dohodne konkrétny čas (začiatok akcie, stretnutia a podobné) a potom sa určí čas podľa strávenej situácie.

Počet použitých rádiostaníc záleží od klienta, a či je potreba chrániť tiež jeho rodinných príslušníkov. Pokiaľ áno, väčšinou sa používajú štyri až päť rádiostaníc, pričom jednu rádiostanicu má vždy osobný ochranca. Rozloženie rádiostaníc je videné na obrázku číslo 29.

Najdôležitejšou súčasťou pre komunikáciu je dohodnutie si kódových slov, ktoré každé slovo znamená inú vec. Príkladom je toho nasledovná tabuľka:

Tab. č. 22 Ukážka kódových slov

Č.	Kľúčové slovo	Význam slova
1	Kontinent	Presun
2	Líška	Potenciálne nebezpečenstvo
3	Vlk	Nebezpečenstvo
4	Jednorožec	Čistý priestor
5	Slnko	Ukončenie hrozieb

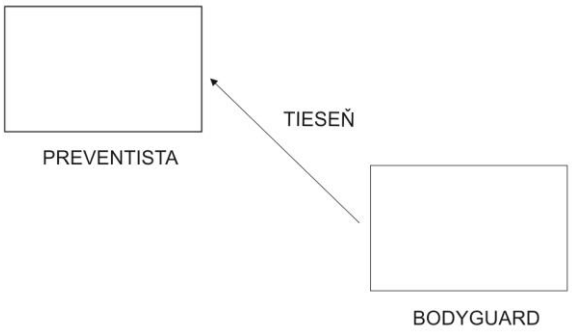


Obr. č. 29 Schéma komunikácie pomocou rádiostaníc

5.2.3 Použitie tiesňového tlačidla a osobného alarmu

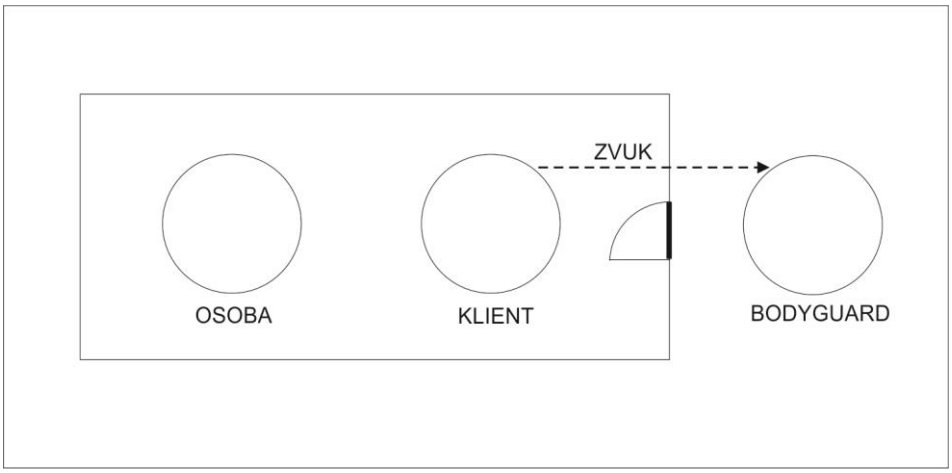
Použitie tiesňového tlačidla a osobného alarmu má dvojaké využitie. Môžu nastať nasledovné veci a to:

1. Osobný ochranca je zranený a vyšle signál preventistovi, ktorý sa postará o zabezpečenie záchrannej služby a poprípade iných zložiek.



Obr. č. 30 Schéma použitia tiesňového tlačidla

2. Klient je na schôdzke, ktorej sa osobný ochranca nemôže zúčastniť, tak tým pádom čaká za dverami, poprípade sa môže nachádzať na toaletách. Po spustení osobného alarmu klientom osobný ochranca vtrhne do danej miestnosti a ďalej si vykonáva svoju prácu.



Obr. č. 31 Schéma použitia osobného alarmu

ZÁVER

Práca osobného ochrancu vyžaduje komplexné znalosti komunikácie a jej foriem. Nutnosťou je ucelený prehľad o dostupných prostriedkoch pre vykonávanú prax, ovládať ich použitie, vlastnosti, poprípade improvizáciu pri zlyhaní. V neposlednom rade je nevyhnutnosťou znalosť právnych aspektov a prípadných legálnych dôsledkov vyplývajúcich z tejto činnosti.

Na trhu je mnoho prostriedkov pre utajenie komunikácie, ale tie najkvalitnejšie sú zároveň aj finančne najnáročnejšie a používanie týchto aplikácií je podmienené nutnosťou každoročnej obnovy licencie za poplatok. Preto je na zváženie kúpa komunikačného prostriedku s možnosťou rozšírenia pamäte pomocou MicroSD karty, čo umožňuje hardwarové zabezpečenie telefónu jednorazovým poplatkom. Zároveň doporučujem uvažovať s potrebnou finančnou rezervou pre zakúpenie prostriedkov ešte na začiatku pracovného vzťahu, ktoré môže osobný ochranca poskytnúť svojmu klientovi.

V úvode som stanovil hypotézu týkajúcu sa lokalizovania a dešifrovania utajenej komunikácie. Podľa mojich poznatkov a praktických skúseností hypotézu vyvraciam – v súčasnosti nie je možné danú aplikáciu s bežne dostupnými prostriedkami dešifrovať alebo lokalizovať. Pokiaľ by nastalo dešifrovanie a lokalizovanie hovoru po nejakom čase, tak tým pádom už na tom nezáleží, pretože sa jedná o neaktuálne informácie.

Z praxe a z minulosti je dané, pokiaľ je aplikácia dostupná pre širokú verejnosť, bude časom jej celková bezpečnostná štruktúra odhalená a narušená. Vzniká riziko hromadného odhalenia a úniku informácií. Preto doporučujem do budúcnosti vyriešiť problematiku dostupnosti aplikácií. Ako príklad je možno uviesť prístroj Enigma, ktorý bol využívaný počas 2. svetovej vojny. Jeho štruktúra bola odhalená, čomu vďačíme za vytvorenie internetu.

Snahou mojej práce bolo upozorniť na teoretické a praktické aspekty používania elektronických komunikačných a signalizačných prostriedkov, princíp fungovania jednotlivých prostriedkov, výhody a nevýhody prostriedkov a použitie v teréne. Závery by mohli slúžiť ako pomôcka pri spracovaní prehľadných inštrukčných materiálov pre budúcu prax osobných ochrancov alebo ako študijné materiály pre informačné technológie, komunikačné systémy a bezpečnostný menežment.

ZÁVER V ANGLIČTINE

The job of the personal guardian requires knowledge of all forms of communicative skills and abilities. It is important to have compex view about available means for doing this prax, knowledge how to use them, qualities or improvisation in failure as well. It is necessity the knowledge of legal aspects and potential legal conseguences as a result of this activity.

There are lots of means for secret communication on the market, but those which are the qualitiest are the most expensive as well and the usage of these aplications are conditional on necessity to renew their licence for rate every year. That´s why it is important to consider the fact of purchase of communication aid with posibility to wide memory with MicroSD card, which allows hardware protection of phone with one time rate. I also recommed to consider with essential financial reserve for aid purchase at the beginning of labour relation that the personal guardian can provide to a client.

In the introduction I outlined a hypothesis referring to localize and decode of secret communication. According to my knowledge and practical experience I contradicted the hypothesis. Nowadays it is not possible to decode or localize that application with commonly available aids. If it occures decoding or localized of call after some time then it does not matter because it will bargain for not actual information.

According to the praxis and from the past experience, it is given if the application is available for the general public, its whole security structure will be exposed and disrupted. It can be the risk for the expose and leak of information. That´s why I recommend to solve that problem of available applications in the future. As the example it is possible to mention the equipment Enigma which was used during 2 World War. Its structure was disclosed, thanks to this fact the Internet was created.

This diploma thesis deals with theoretical and practical aspects of electronical communication and signaling aids usage, principle of functioning of various aids, advantages and disadvantages of aids and their usage in terrene. Conclusions could be used as a device for well arranged and instruction materials for the future prax of personal protectors or study materials for information technology, communication system and security management as well.

ZOZNAM POUŽITEJ LITERATÚRY

[1] VYSÍLAČKY MILÍN. *Co je radiostanice* [online]. 2004 [cit. 2014-04-16]. Dostupné z:http://vysilackymilin.cz/informace/co-je-to-radiostanice/

[2] ODPOSLECHY.COM. *Právní rozbor* [online]. 1999-2014 [cit. 2014-04-16]. Dostupné z:http://www.odposlechy.com/pravni-rozbor/

[3] JŮZL, Lukáš. *Bezdrátová komunikace – normy, frekvenční pásma, zařízení*. Zlín, 2011. Bakalářská práce. UTB ve Zlíně, Fakulta aplikované informatiky,. Vedoucí práce Ing. Lubomír Macků, Ph.D

[4] *Hytera DMR standart* [online]. 2012-2014 [cit. 2014-05-04]. Dostupné z: http://www.radiostanice-hytera.cz/dmr-standart/

[5] *Telekomunikácie: Mobilné siete* [online]. 2009-2014 [cit. 2014-05-04]. Dostupné z:http://www.spsnmnv.sk/prace/janis/stranka5.html

[6] *Mobilná komunikácia, siete, mobilné telefóny* [online]. 2014 [cit. 2014-05-04]. Dostupné z:http://referaty.atlas.sk/ostatne/informatika/11981/?print=1

[7] *Základné info HSDPA* [online]. 2009 [cit. 2014-05-04]. Dostupné z: http://www.fony.sk/clanky/355-

[8] LTE. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2014 [cit. 2014-05-04]. Dostupné z: http://cs.wikipedia.org/wiki/LTE

[9] *Šifrování - úvod do problematiky* [online]. 1999 [cit. 2014-05-04]. Dostupné z:http://www.root.cz/clanky/sifrovani-uvod-do-problematiky/

[10] *Slovník* [online]. 1998-2014 [cit. 2014-05-04]. Dostupné z: http://www.svethardware.cz/slovnik/

[11] Twofish. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2014-05-04]. Dostupné z: http://cs.wikipedia.org/wiki/Twofish

[12] *Diffie-Hellman* [online]. 2008-2014 [cit. 2014-05-04]. Dostupné z: http://www.algoritmy.net/article/84/Diffie-Hellman

[13] *Definice technologie VOIP* [online]. 2005-2014 [cit. 2014-05-20]. Dostupné z: http://www.3cx.cz/voip-sip/voip-definition/

[14] Real-time Transport Protocol. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2014-05-04]. Dostupné z: http://cs.wikipedia.org/wiki/Real-time_Transport_Protocol

[15] Session Initiation Protocol. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2014-05-04]. Dostupné z: http://cs.wikipedia.org/wiki/Session_Initiation_Protocol

[16] Session Description Protocol. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2014-05-04]. Dostupné z:http://cs.wikipedia.org/wiki/Session_Description_Protocol

[17] SRTP. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2014 [cit. 2014-05-04]. Dostupné z: http://cs.wikipedia.org/wiki/SRTP

[18] ZRPT. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2014 [cit. 2014-05-04]. Dostupné z: http://cs.wikipedia.org/wiki/ZRTP

[19] Transport Layer Security. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2014-05-04]. Dostupné z: http://cs.wikipedia.org/wiki/TLS

[20] Mobilný telefón. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2014 [cit. 2014-05-04]. Dostupné z: http://sk.wikipedia.org/wiki/Mobiln%C3%BD_telef%C3%B3n

[21] *Radiostanice CB* [online]. 1998-2014 [cit. 2014-05-04]. Dostupné z: http://mve.energetika.cz/krizove-situace/CB-radiostanice.htm

[22] *Seznam CB frekvencí: Česko* [online]. 2014 [cit. 2014-05-20]. Dostupné z:http://www.cbmonitor.cz/cb_frekvence/frekvence_tabulka.php

[23] *Kanály a frekvence PMR* [online]. 2004-2014 [cit. 2014-05-20]. Dostupné z:http://vysilackymilin.cz/informace/kanaly-a-frekvence-pmr/

[24] *Motorola P165 & P185* [online]. 2007-2010 [cit. 2014-05-20]. Dostupné z: http://www.centernet.cz/vysilacky-motorola-p165-p185.html

[25] *Cryptophone 500* [online]. 2010 - 2014 [cit. 2014-05-20]. Dostupné z: http://www.spyobchod.sk/cryptophone-500/

[26] *Voice Protector* [online]. 2010 - 2014 [cit. 2014-05-20]. Dostupné z: http://www.spyobchod.sk/voice-protector/

[27] *VIP Call secure chip* [online]. 2010 - 2014 [cit. 2014-05-20]. Dostupné z: http://www.spyobchod.sk/vip-call-secure-chip/

[28] *Gold-Lock - šifrovanie hovorov, SMS a súborov* [online]. 2010 - 2014 [cit. 2014-05-20]. Dostupné z:http://www.spyobchod.sk/gold-lock-sifrovanie-hovorov-sms-a-suborov/

[29] *Phone-X šifrovanie hovorov a SMS* [online]. 2010 - 2014 [cit. 2014-05-20]. Dostupné z:http://www.spyobchod.sk/phone-x-sifrovanie-hovorov-a-sms/

[30] *Bezpečné volání, textové zprávy a přenos souborů - software SILENTEL 6 pro většinu telefonů, certifikace NATO, licence 1 uživatel / 12 měsíců* [online]. 1999-2014 [cit. 2014-05-20]. Dostupné z:http://www.odposlechy.com/bezpecne-volani-textove-zpravy-a-prenos-souboru-software-silentel-6-pro-vetsinu-telefonu-certifikace-nato-licence-1-uzivatel-12-mesicu

[31] *Profesionální radiostanice* [online]. 2014 [cit. 2014-05-20]. Dostupné z:http://radiostanice.cz/radiostanice/profi/

[32] *Dosah vysielačiek PMR* [online]. 2004–2012 [cit. 2014-05-20]. Dostupné z:http://www.slovhron.sk/vysielacky/pouzitie.html

[33] *Mobilný telefón*. Žilina, 2007. Dostupné z: fyzika.uniza.sk/~melo/PHYSICS3/mobil.doc. Seminárna práca. Žilinská univerzita v Žiline.

[34] *Hluk a vibrácie* [online]. 2005 [cit. 2014-05-20]. Dostupné z: http://referaty.aktuality.sk/hluk-a-vibracie/referat-1938#

[35] LAPKOVÁ, Dora a Zdeněk MALÁNÍK. Rozdělení zbraní a osobních prostředků. Bezpečnostní technologie, systémy a management II.: Teorie a praxe

ochrany majetku a fyzické bezpečnosti. 1. vyd. Doc. Ing. Luděk Lukáš, CSc. Zlín: Radim Bačuvčík - VeRBuM, 2012, 142 - 155. ISBN 978-80-87500-19-4.

[36] MALÁNÍK, Zdeněk. Profese osobního strážce v České republice. LUKÁŠ, Luděk et al. Bezpečnostní technologie, systémy a management III.: Teorie a praxe ochrany majetku a fyzické bezpečnosti. 1. vyd. Zlín: VeRBuM, 2013, s. 208-228. ISBN 978-80-87500-35-4.

[37] *Samsung Galaxy S4: Specifikace* [online]. 2013 [cit. 2014-05-20]. Dostupné z:http://mobilenet.cz/katalog/samsung-galaxy-s4/specifikace

[38] *Ruční radiostanice Hytera PD785 - VHF, UHF Více zde: http://www.radiostanice-hytera.cz/products/radiostanice-hytera-pd785-vhf/* [online]. 2012 - 2014 [cit. 2014-05-20]. Dostupné z:http://www.radiostanice-hytera.cz/products/radiostanice-hytera-pd785-vhf/

[39] *Vozidlová radiostanice Hytera MD785G - VHF, UHF Více zde: http://www.radiostanice-hytera.cz/products/vozidlova-radiostanice-hytera-dm785g-vhf/* [online]. 2012 - 2014 [cit. 2014-05-20]. Dostupné z: http://www.radiostanice-hytera.cz/products/vozidlova-radiostanice-hytera-dm785g-vhf/

[40] *ALAN 42 MULTI* [online]. 2014 [cit. 2014-05-20]. Dostupné z: http://www.shop3000.cz/product.php?id_product=16

[41] *ALBRECHT AE 5290* [online]. 2014 [cit. 2014-05-20]. Dostupné z: http://www.shop3000.cz/product.php?id_product=23

[42] *MOTOROLA TLKR T60* [online]. 2014 [cit. 2014-05-20]. Dostupné z: http://www.shop3000.cz/product.php?id_product=1818

[43] *RC-87* [online]. 2009 [cit. 2014-05-20]. Dostupné z: http://www.axlelectronics.cz/zabezpeceni-objektu/system-oasis-868mhz/ovladace/rc-87-tisnove-tlacitko-253/

[44] *Konig SEC-APS10, osobný bezpečnostný alarm 130 dB* [online]. 2013 [cit. 2014-05-20]. Dostupné z:http://www.nay.sk/konig/d-303852/?utm_source=heureka&utm_medium=feed&utm_campaign=h_porovnanie

[45] *Proč používat PhoneX?* [online]. 2013-2014 [cit. 2014-05-20]. Dostupné z: http://www.phone-x.net/cz/proc-pouzivat-phonex

[46] *Jak to funguje?* [online]. 2013-2014 [cit. 2014-05-20]. Dostupné z: http://www.phone-x.net/cz/jak-to-funguje

[47] *PhoneX pro OS Android* [online]. 2013-2014 [cit. 2014-05-20]. Dostupné z: http://www.phone-x.net/cz/phonex-pro-android

[48] *Časté dotazy (FAQ)* [online]. 2013-2014 [cit. 2014-05-20]. Dostupné z: http://www.phone-x.net/cz/faq

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

č. číslo

Sb. Sbírka

DMR Digital Mobile Radio

GSM Global System for Mobile Communications

PMR Personal Mobile Radio

TDMA Time Division Multiple Access

FDMA Frequency-Division Multiple Access

BSS Base Station Subsystem

NSS Network Switching Subsystem

OSS Operation and Support Subsystem

SMS Short Message Service

GPRS General Packet Radio Service

HSDPA High Speed Downlink Packet Access

HSUPA High Speed Uplink Packet Access

UMTS Universal Mobile Telecommunication System

AES Advanced Encryption Standart

RSA Rivest Shamir Adleman

SDP Session Initation Protocol

EAL5+ Evaluation Assurance Level 5+

EDGE Enhanced Data rates for GSM Evolution

LTE Long Term Evolution

WIFI Wireless Fidelity

RTP Real-time Transport Protocol

VoIP Voice over Internet Protocol

TLS Transport Layer Security

SRPT Secure Real-time Transport Protocol

ZRPT Zimmermann Real-time Transport Protocol

SIP Sessios Initiation Protocol

SAS Short Authentication String

CA Certification Authority

CEPT European Conference of Postal and Telecommunications Administration

SINAD Signal-To-Noise and Distortion Ratio

GPS Global Positioning System

AM Amplitúdová modulácia

FM Frekvenčná modulácia

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

CD