

Niebezpiecznik

o bezpieczeństwie i nie...

szukaj...

-
-
- [Szkozenia](#)
- [5 PORAD](#)
- [Audyty & Pentesty](#)
- [Praca](#)
- [Kontakt](#)

17:35
4/1/2015

Jak nasłuchiwać łączność radiową polskich służb i firm?

Autor: redakcja | Tagi: [krótkofalarstwo](#), [policja](#), [radio](#), [służby](#)



Dziś na łamach Niebezpiecznika publikujemy artykuł jednego z naszych czytelników, Marcina, który opisał temat coraz bardziej popularnych i wykorzystywanych w Polsce systemów cyfrowej ruchomej łączności radiowej, przeznaczonych do zastosowań profesjonalnych, w tym służb.

Jak komunikują się służby?

Jako osoba zainteresowana tym tematem oraz jako pasywny krótkofalowiec (obecnie brak czasu na to hobby), chciałem przekazać Wam kilka informacji z tego zakresu. Mam nadzieję, że temat wywoła ciekawą dyskusję w komentarzach.

W Polsce, służby, takie jak **policja**, **straż pożarna**, **pogotowie**, **straż graniczna**, **straż miejska**, **PKP**, **WOPR**, **TOPR**, **GOPR**, lasy a także m.in. **firmy ochroniarskie**, **TAXI**, morskie, pracują głównie na sprzęcie pracującym w technologii analogowej i na częstotliwościach niekodowanych, które **bez problemu można podsłuchiwać** za pomocą [zwykłego skanera](#), pracującego w paśmie UKF/VHF.



Skaner Uniden

Wykaz znanych częstotliwości został świetnie opisany na [stronie Włodzimierza Gillera](#) — można z niej bez problemu odczytać częstotliwość pracy każdej ze służb w danym mieście/obszarze. Pomimo tego, że niektóre wpisy na stronie są dość archaiczne, większość częstotliwości nadal działa.

Przykładowo, policja pracuje na częstotliwościach 172,000 – 174,000 Mhz i naprawdę, posiadając skaner i antenę szerokopasmową (najlepiej dookólną na dachu) można usłyszeć przekazy zarówno z okolic jak i dalszych miejsc (30-50 km).

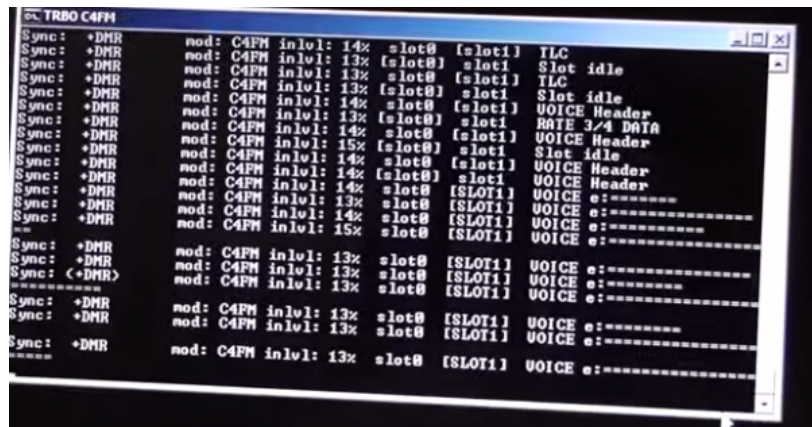


Na częstotliwości 169,000 MHz można w Poznaniu i okolicach usłyszeć **śmigłowiec ratunkowy** (Lotnicze Pogotowie Ratunkowe; por. [TVP ujawniła hasło do systemów ratowniczych LPR](#)), czyli tzw. **ratownik "9"**. W Polsce takich ratowników jest wiele.

Niektóre transmisje są szyfrowane

Jakiś czas temu, służba zdrowia na terenie Wielkopolski (nie wiem jak jest w innych woj.) zorganizowała przetarg na sprzęt umożliwiający komunikację dyspozytora z karetkami pogotowia za pomocą nowoczesnych urządzeń. Sprzęt szyfruje całą korespondencję standardem łączności **MOTOTRBO** autorstwa Motoroli — zamiast rozmowy usłyszymy przekaz zakodowany w postaci cyfrowej. Z tego samego systemu korzysta już w większych miastach policja w paśmie 172 MHz. Innym systemem jest TETRA, stosowana głównie w Warszawie.

W sieci pojawiły się jednak ciekawe programy, np. **DMR** do dekodowania sygnału MOTOTRBO (częstotliwości dla Wielkopolski to okolice 168 MHz, więc możliwe do podsłuchania skanerem).



Moto TROBO DMR Decoding

Ponieważ DMR to dekodery, to jedyne co robi to zamiana postaci cyfrowej na analogową — w dalszym ciągu zaszyfrowaną. Podejrzewam, że istnieją sposoby na odszyfrowanie takiego strumienia do postaci jawnej (przydatne informacje można znaleźć [tutaj](#) i [tutaj](#)).

Nasłuch jest legalny

Jak wiadomo, w Polsce nadawanie na częstotliwościach służb jest zabronione. Sam nasłuch nie jest nielegalny, o ile nie udostępniamy tych informacji osobom trzecim.

Dopisek redakcji:

Nie wymaga pozwolenia używanie urządzeń radiowych przeznaczonych wyłącznie do odbioru.

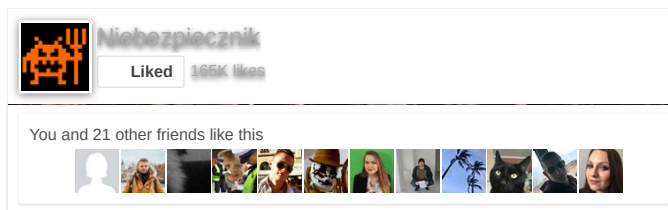
Ustawa z dnia 16 lipca 2004 r., Prawo telekomunikacyjne (Dz. U. Nr 171, poz.1800) DZIAŁ VI, Rozdział 2, Art. 144. p. 1.

Ciekawostką natomiast jest to, że w eterze na tych pasmach co chwile można usłyszeć **przekazywanie danych osobowych**. Ciekawe jak to się ma do ustawy o ochronie danych osobowych, skoro policja podaje nazwiska, adresy i nr PESEL w kanałach niezasyfrowanych i dostępnych dla każdego? (por. [Podsłuchiwanie numerów kart kredytowych transmitowanych przez samoloty](#)).

PS. Polecamy też 2 świetne artykuły autorstwa Wojciecha Bielaka (SQ9PBS) które zostały opublikowane na naszych łamach. Pierwszy opisywał [kunszt polskich radioamatorów podczas II wojny światowej](#) i to, jak utarli nosa Niemcom. Drugi zaś dotyczył czasów stanu wojennego i walki radioamatorów z cenzurą, m.in. z wykorzystaniem [piłek plażowych wypełnionych wodorem](#). Przy okazji przypominamy, że każdy z Was może publikować na naszych łamach — [chętnych zapraszamy do kontaktu](#). Może któryś z czytelników chciałby opisać swoje przygody z SDR?

Przeczytaj także:

- [Strajk policjantów może... zaszkodzić ochronie danych osobowych Polaków](#)
- [Plażowe piłki wypełnione wodorem i wstrzykiwanie sygnału TV, czyli walka radioamatorów ze stanem wojennym w Polsce](#)
- [Jak polscy radioamatorzy utarli nosa Niemcom w trakcie II wojny światowej](#)



131 komentarzy 🗨️

[Dodaj komentarz](#)

1.

Maciek 2015.01.04 17:52 | <#> | [Reply](#)

“Mocniejsza” niż ochrona danych osobowych jest tajemnica telekomunikacyjna i tajemnica korespondencji. Podsluchując czyjaś komunikację łamiemy obydwie. To niczym się nie różni od wpięcia krokodylkiem do szafy krosowej w piwnicy.

ps. czy >>echo date(“Y”);<< w Waszej stopce to jakiś tajny przekaz?

o

[linoskoczek](#) 2015.01.05 01:16 | <#> |

Było już wyjaśnione na łamach niebezpiecznie ;) luknij w source strony (ale ten prawdziwy, nie firebugowy).

o

Gość 2015.01.05 15:18 | <#> |

Stosując taką logikę możnaby równie dobrze uznać jakiegokolwiek środki bezpieczeństwa mające zapobiec kradzieży za zbyt wysokie, no bo skoro kradzież jest zabroniona to przecież nikt tego nie robi, tak? Na tej zasadzie np. banki również powinny zrezygnować z szyfrowania połączeń, argumentując że skoro przechwyt danych zawierających wrażliwe dane jest zabroniony, to zabezpieczenia nie są konieczne. Przyznasz zapewne, że to jednak mało sensowny punkt widzenia. Komunikacja przekazująca wrażliwe (w szczególności chronione prawnie) dane powinna być obowiązkowo szyfrowana, nie ma tu ani sensownej alternatywy, ani sensownego usprawiedliwienia zaniechania stosowania zabezpieczeń.

o

sw3 2015.01.05 15:47 | <#> |

Wpinając się w cudzy kabel czy otwierając cudzą kopertę łamiemy prawo, natomiast odbierając fale przebiegające przez nasze mieszkanie nie łamiemy prawa na co stosowny przepis masz podany w artykule.

Czy może powołując się na tajemnicę telekomunikacyjną zdelegalizujesz również CB radio i krótkofalowców? ;)

o



Kacper 2015.01.07 14:09 | <#> |

Wifi sąsiada też przelatuje przez moje mieszkanie i jakoś korzystanie z niego nie jest legalne...

o

BloodMan 2015.01.07 14:35 | <#> |

@Kacper: korzystanie nie jest legalne – ale słuchanie jest legalne. Tak samo możesz słuchać radyjka UKF, CB, WiFi, GSM ... co usłyszysz to Twoje. Ale korzystać (w znaczeniu używanie dwukierunkowe) nie można (w sumie nie dotyczy ogólnych kanałów CB).

2.

Zygi 2015.01.04 18:07 | <#> | [Reply](#)

Do słuchania SG wystarczy zwykły radioodbiornik RTV a i kiedyś w TV było słychać. Jak się rozgadali to nie można było nic oglądać ani słuchać.

3.

trolo 2015.01.04 18:17 | <#> | [Reply](#)

“Nie wymaga pozwolenia” odsłuchiwanie, tylko trzeba odbiornik zarejestrować i zapłacić abonament ...

4.

kayo 2015.01.04 18:26 | <#> | [Reply](#)

Warto tu wspomnieć o technice SDR i tanich odbiornikach DVB-T bazujących na chipsetach Realteka

<http://sdr.osmocom.org/trac/wiki/rtl-sdr>

<http://www.rtl-sdr.com/>

5.

Wojtek 2015.01.04 18:37 | <#> | [Reply](#)

Przypis redakcji na temat legalności jest o kant D – to dotyczy pozwolen na używanie urządzeń, a nie słuchania. Ja na przykład mam urządzenie i mam na nie pozwolenie – ale to mnie nie upoważnia do podsłuchiwania.

Podsłuchiwanie treści niekodowanych podpada wyłącznie pod tajemnicę telekomunikacyjną (czyli jeśli “przypadkiem” usłyszeliśmy, powinniśmy o tym natychmiast zapomnieć) – tak więc jest pol-legalne, głównie z powodu niewykrywalności tego czynu. Natomiast wszelkie kodowane transmisje (nawet jeśli kodowanie jest banalne) podpadają pod paragraf “kto przełamuje [...] zabezpieczenia...”.

o

troll 2015.01.04 18:49 | <#> |

UKE jest innego zdania: “prawo telekomunikacyjne zakazuje dalszego przekazywania informacji odebranych przez osobę nieuprawnioną. Stosownie do art. 160 ust. 3 osoba, która korzystając z urządzenia radiowego lub końcowego, zapoznała się z komunikatem dla niej nieprzeznaczonym, jest obowiązana do zachowania tajemnicy telekomunikacyjnej”.

Dodatkowo wg UKE “uzyskanie informacji nadawanych za pośrednictwem fal radiowych, telewizyjnych czy sygnału satelitarnego, nawet jeżeli jest dokonywane w paśmie zastrzeżonym, nie stanowi realizacji znamion z art. 267 § 1, chyba że odbiór tak nadawanych informacji uzależniony był od przełamania określonego kodu zabezpieczającego czy też posiadania specjalnego urządzenia odbiorczego”.

o

Ax 2015.01.04 19:50 | <#> |

Ale o jakich przełamaniach zabezpieczeń ty piszesz, skoro jak wynika z artykułu one nie są szyfrowne tylko jawne i teoretycznie na każdej radiostacji można odsłuchiwać czy to specjalnie czy przypadkowo, tylko kto udowodni to pierwsze?

Kilka dni temu na walkietalkie dla dzieci (model Tomas & Friends) jakimś sposobem słyszałem czyjeś głosy, a tam nie ma kompletnie żadnej regulacji jedynie on i off.

o

Olaf 2015.01.04 20:56 | <#> |

Szukasz czegoś na siłę gdy tymczasem rzeczywistość jest prosta – mając skaner możesz nasłuchiwać bez udostępniania tego innym. Koniec kropka.

o

Bolek 2016.11.29 19:39 | <#> |

Kolega ma zezwolenie chyba ba obsłuchiwać zipcyków, albo kanał udostępniany przy zakupie niektórych urządzeń radiokomunikacyjnych bo na pewno nie licencję amatorską. Bo, gdybyś takową miał, wiedziałbyś doskonale, co mówią na ten temat przepisy. Które przytoczyli zresztą inni panowie. Słuchać możesz sobie tego, co chcesz, o ile nie łamiesz szyfrowania i nie udostępniasz zasłyszanych informacji.

6.

troll 2015.01.04 18:40 | <#> | [Reply](#)

Sam nasłuch może być legalny, ale złamanie (deszyfrowanie) MOTOTRBO może podpadać pod art. 267 kk:

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

o

exti 2015.01.05 02:55 | <#> |

Trzeba odróżniać deszyfrowanie od dekodowania. Program wspomniany w artykule pozwala jedynie na dekodowanie niezabezpieczonych transmisji MOTOTRBO (i Digital Mobile Radio w ogólności). Nie radzi sobie z podstawowym ani rozszerzonym szyfrowaniem/maskowaniem transmisji (rozszerzonego używa np. Policja i SG). Sam sposób kodowania sygnału DMR jest opisany w otwartym i publicznie dostępnym standardzie ETSI (pomijając wokoder AMBE+2, który jest autorskim rozwiązaniem pewnej firmy).

Tak więc to, czy korzystanie z tego programu jest sprzeczne z art. 267 KK nie jest tak do końca pewne.

7.

bre 2015.01.04 19:00 | # | [Reply](#)

Art o SDR z wykupu <http://www.wykop.pl/artykul/1341289/rtlsdr-czyli-odbieraj-niemal-wszystko-z-tunera-dvb-t/>
Mam tuner za 10\$ z przesyłką i fajnie działa ale nie mam zew anteny a w mojej okolicy nuda :)

8.

henk 2015.01.04 19:00 | # | [Reply](#)

TETRA to nie tylko policja w Warszawie. Takie stwierdzenie to kłamstwo. Z TETRY korzysta nawet MPK w Krakowie

9.

AAA 2015.01.04 19:15 | # | [Reply](#)

Czy legalne było by udostępnianie tego typu sygnałów przez streaming online?

o

Robert 2015.01.06 19:58 | # |

To interesujące pytanie zwłaszcza poprzez pryzmat tego:
<http://tunein.com/search/?query=scanner>

10.

Marcin Maziarz 2015.01.04 19:38 | # | [Reply](#)

Czy można nadawać na dowolnej (w tym zarezerwowanej dla służb) częstotliwości, jeśli sygnał nie wychodzi poza budynek lub teren posesji?

o

[linoskoczek](#) 2015.01.05 01:18 | # |

Załóż, że nie wiesz nic o częstotliwościach stosowanych przez władze :)



o

[mmmc](#) 2015.01.05 07:24 | # |

@linoskoczek

Ignorantia legis non excusat



o

[dawciobiel](#) 2015.01.05 16:28 | # |

linoskoczek @ nieznajomość prawa niezwalnia z odpowiedzialności.

o

wikrap1 2015.01.06 23:10 | # |

Czy jeśli drzewo w lesie upadło, ale nikt nie widział upadku, to czy drzewo upadło? ;)



o

[dawciobiel](#) 2015.01.08 15:16 | # |

wikrap1@

1) to skąd wiadomo, że upadło?

2) drzewo upadło, bo samo o tym wie ;D

3) nawet jeżeli drzewo leży to i tak jest w pionie ;D

11.

Hast 2015.01.04 19:55 | # | [Reply](#)

No dobrze załóżmy że mam urządzenie i nasłuchuje na zakodowanej częstotliwości. Jak namierza mój sprzęt ?

o

fssfsdf 2015.01.05 10:26 | <#> |

Nie ma czegoś takiego jak "zakodowana częstotliwość". Na jakiejś częstotliwości jest jakiś sygnał albo go nie ma. A jak jest to może być zakodowany lub nie, analogowy lub cyfrowy wszystko zależy od zastosowanej technologii i interpretacji czym jest "zakodowanie". Samego słuchania nie da się wykryć, fale radiowe docierają wszędzie tam gdzie pozwolą jej prawa fizyki, jeśli akurat dotrą do ciebie i odpowiedniego sprzętu, który posiadasz to nie twoja wina. Inna sprawa to udostępniania usłyszanych informacji dalej.

o

yzq 2015.01.05 20:09 | <#> |

Mówicie, że nie da się wykryć nasłuchiwania? Da się wykryć oglądanie więc kto wie...

https://en.wikipedia.org/wiki/Television_licensing_in_the_United_Kingdom#Detection_technology.

o

Ef 2015.01.06 11:43 | <#> |

Wykrywają oglądanie, a nie odbieranie.

o

Gof 2015.01.08 22:08 | <#> |

Po częstotliwości heterodyny. Były takie przypadki jeszcze w poprzednim ustroju.

12.

Matt 2015.01.04 20:07 | <#> | [Reply](#)

"Art 267

...

§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym."

Co do tego zdania są podzielone, moim zdaniem to najlepiej jest zrobić licencję radiowca postawić maszt i będzie święty spokój (A to co robimy w eterze to już nasza sprawa, byle w drodze rozsądku).

o

Matt 2015.01.04 20:12 | <#> |

A po za tym policja powinna szyfrować swoje rozmowy, a nie mieć potem pretensje do ślepego.

o

BloodMan 2015.01.05 10:20 | <#> |

@matt: ale odbiornik nie jest urządzeniem podsłuchowym. Niezależnie co byś nie próbował udowodnić ;) Zwykle radyjko UKF też ma pokrętło do strojenia – więc się zagalopowałeś ;p

13.

Alex 2015.01.04 20:07 | <#> | [Reply](#)

Ani słowa o warszawskich EDCS?

14.

Tadeusz 2015.01.04 20:11 | <#> | [Reply](#)

Z tym MOTOTRBO to nie do końca jest jak piszecie. Istnieje kilka programów dzięki którym możemy posłuchać transmisji głosowych jak również odebrać inne dane (położenie radiotelefonu, bo niektóre modele mają GPS). Szukajcie pod dsd albo dsdplus. Jednak MOTOTRBO może mieć włączone dodatkowo tzw maskowanie (proste lub rozszerzone) i takiej transmisji już nie podsłuchamy przy użyciu w/w programów. Jak nie stac kogos na porządny skaner to za 40zł można kupić tuner DVB-T (musi mieć chipset RTL2832U) na USB i z softem typu SDR np #SDRSHRP można smigać po pasmach. Pokrywa to zależnie od modelu od ok 25-1600 MHz i mamy widok na widmo o szerokości nawet 4 MHz. Instrukcje jak to pobrać można znaleźć tu <http://www.rtl-sdr.com/>

15.

Tomek 2015.01.04 20:15 | <#> | [Reply](#)

Niech was zatrzyma patrol z zaprogramowaną częstotliwością policji to z automatu macie sprawę o łamanie zabezpieczeń teleinformatycznych, dostęp do informacji nie przeznaczonej dla ciebie i konfiskatę oraz przepadek sprzętu. Nie jedna już taka sprawa była i wyrok zawsze skazujący.

- o Artur 2015.01.05 02:43 | <#> |

konkrety podaj. gdzie, kogo, z jakiego paragrafu.

- o duzak 2016.01.22 11:59 | <#> |

Wybaczenie archeologii ;)

Niedawno w powiecie pod Warszawa, za sam nasłuch, nie wiem czy EDACS, czy konwencja. Sprawa z art. 267kk paragraf 1 i 3. W toku. Więcej danych nie podam, więc jak nie chcesz wierzyć to proszę bardzo :)

- o Piotrek 2016.01.22 22:44 | <#> |

Hahaha ja już miałem sprawę o skaner i nic mi nie zrobili. Próbowali na siłę mi zarzucić “dostęp do informacji niejawnej/nieprzeznaczonej dla mnie” itd., albo co lepsze “dostęp do radiostacji poprzez przełamanie zabezpieczeń” hahahah i nic! Uniewinnili mnie, a skaner oddali. Takie wasze oburzenie się w komentarzach i straszenie nie wiadomo czym ma tylko na celu nasłuchowców zastraszyć i zadziałać prewencyjnie. Przejdźcie wszyscy na łączności cyfrowe i szyfrowane, to problem nasłuchu policji zniknie. Ostatecznie wszystkie kwestie sporne reguluje tutaj UKE, a nie policja czy prokuratura. Sąd nie może orzekać wbrew obowiązującemu prawu telekomunikacyjnemu. Dlatego właśnie wygrałem z policją sprawę. Mówię jak jest, stwierdzam fakty, a nie opieram się na jakichś teoretycznych zagadnieniach i paragrafach, którymi możesz sobie do woli straszyć. Nie strasz bo się :)



16. Michał 2015.01.04 20:17 | <#> | [Reply](#)

a jaki skaner polecacie na początek? A może jakiś SDR do komputera?

17. Marcin 2015.01.04 20:21 | <#> | [Reply](#)

Wojtek nie myl podsłuchiwanie z nasłuchiowaniem bo jedno nie ma z drugim wiele wspólnego.

18. abcd 2015.01.04 20:42 | <#> | [Reply](#)

Możecie polecić jakiś w miarę dobry skaner radiowy, oczywiście w rozsądnej cenie dla początkującego?

19. Spider_std 2015.01.04 20:42 | <#> | [Reply](#)

Stanowisko UKE odnośnie podsłuchiwania: <http://www.ifp.pl/index.php?name=PNphpBB2&file=viewtopic&t=2228&start=103>

20. Arek 2015.01.04 20:42 | <#> | [Reply](#)

To co mówi Wojtek to prawda, dekodowanie DMR czy MOTOTRBO podpada pod przełamywanie zabezpieczeń. Jeżeli chodzi o te “walkietalkie”, to są najpewniej radiotelefony LPD, nie ma tu mowy o odkodowywaniu transmisji.

21. ugvujhvb 2015.01.04 21:23 | <#> | [Reply](#)

Mogę opisać skanowanie satelitów w celu poszukiwania derywów i oglądanie sobie wielu niedostępnych w Polsce meczów różnych dyscyplin, koncertów i innych wydarzeń, które są przez kogokolwiek dosyłane z wykorzystaniem satelitów. Filozofii w tym wielkiej nie ma. Wczoraj i dziś np. było mnóstwo meczów Pucharu Francji, a także nagrałem sobie jakiś koncert klasyczny.

22. T 2015.01.04 21:27 | <#> | [Reply](#)

Podsłuchiwać można legalnie-analogowo (nie kodowane transmisje), pytanie czy jeżeli zdekodujemy zaszyfrowaną modulowaną cyfrowo transmisję – czy nadal to jest legalne. Jak to jest z kodowanym sygnałem np. DVB rozkodujemy pakiety TransportStream znając algorytmy generujące klucze CW (algorytmy zaszyte w smartcard lub sharing dostarczający klucze CW) desklamblerem ECD.

23.

Hilary 2015.01.04 21:29 | # | [Reply](#)

Na swoim starym walkietalkie miałem kiedyś idealne dostrojenie do policyjnych częstotliwości. Od nowości tak miała- czy łamałem prawo? No chyba jednak nie, to jakby mi ktoś przed nosem machał transparentem i próbował wmówić, że nie wolno mi na niego patrzeć ;)



24.

djsamiryi 2015.01.04 21:32 | # | [Reply](#)

SDR'y to świetna sprawa. Polecam stronę <http://websdr.org> gdzie można posłuchać stacji SDR z całego świata (poprzez wybranie odpowiedniego linku). Ja osobiście przysięgam się do zakupu (zrobić to jednak trochę czasu by pochłonoło) takiego SDR'a żeby podłączyć ją do mojej anteny (5/8 f z 3 przeciwwagami) do której obecnie podłączony jest uniden pc-122.

25.

Tomek 2015.01.04 21:44 | # | [Reply](#)

Co to za walkietalkie?

26.

Neevor 2015.01.04 21:48 | # | [Reply](#)

Przecież z tego analogowego sygnału już nic nie można wyciągnąć.
Tam leżą ramki kontrolne i inne takie. To jak zgrywanie programów na Spectrum z audycji Harcerskiej Rozgłośni Radiowej w końcówce lat 80.
Z tą jedynie różnicą, że programy na ośmiobitowce nie były szyfrowane ;)
I szczerze, to jest mocne szyfrowanie – a cały sprzęt do tego jest na tyle drogi, że nie każda służba go u siebie wdroży ;)

NRTC63 pozdrawia Motorolowy InfraSec ;P

o

T 2015.01.13 21:01 | # |

A kto powiedział że transmisja była niekodowana? ZX Spectrum miał kodowanie "na czas" stan wysoki przez okreslony x TStatow procesora to 1 lub y TStatow to logiczne 0.Co nieoznaczało że zawarte tam bity/bajty nie mogły zostać przejechane jakimś algorytmem kodowania.Np ArtStudio było kodowane w przelśle ON AIR trywalnym kodowaniem a dopiero odpalenie okreslonego kodu z wczytanego bloku danych Z80 pozwalało na przywrócenie orginalnej maszynowki i uruchomienie programu.

27.

Janek 2015.01.04 21:53 | # | [Reply](#)

Bardzo ostrożnie bym podchodził do treści tego artykułu ! – zawiera nieprawdziwe informacje co do możliwej odpowiedzialności karnej za podsłuchiwanie np. Policji a już łamanie szyfrowanej transmisji jest NAPEWO NIEZGODNE Z PRAWEM. Mają tu zastosowanie:

1. art. 208 ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne
2. Art. 267. § 3 KODEKSU KARNEGO !!!

i choć zdarzał się przypadek w którym SN był innego zdania, a jak wiadomo wyroki SN są wykładnią prawa, to każdy przypadek jest indywidualny a w tym – używanie specjalistycznego oprogramowania do dekodowania transmisji zapewne było by inaczej potraktowane

28.

Ivvan 2015.01.04 22:10 | # | [Reply](#)

Znam takiego który podsłuchuje 24/h wszystko to co się dzieje w mieście. Moznaby powiedzieć że ma najswieższe info ;D
Ciekawostka: ma żółte papiery i jest rencistą ;D



29.

SpeX 2015.01.04 22:47 | # | [Reply](#)

W policji, już chyba nie tylko Warszawa działa na Tetrze.

o

Neevor 2015.01.04 22:54 | # |

Tetra jest standardem europejskim w odróżnieniu od amerykańskiego Astro. Różnią się generalnie mocą nadajników.

o

Tomek 2015.01.04 23:16 | # |

W Polsce Warszawa, Łódź i Kraków korzysta z Tetra. Astro to rozwiązanie firmowe Motoroli. A standard to Apco P25

o
vanitas 2015.01.05 09:04 | <#> |

W Warszawie – ani policji, ani nawet strażaków miejskich, straży pożarnej, czy PKP na analogu nie słyszałem:-)

30.
Artur 2015.01.04 23:35 | <#> | [Reply](#)

Poznańska policja jeszcze dużo jedzie w analogu, ale słysząc jak przechodzi z serwera cyfrowego, nieraz fajnie się ciągnie i szatkuje sygnał.

o
Robert 2015.01.06 16:21 | <#> |

Jedzie jedzie ;) Ale słysząc jak wysyłają patroli do żuli w bramach. Od czasu jak się pokapowali że sprawdzamy sobie rejestracje fajnych panienek w ich bazie to wszystko ważne załatwiali przez komórki ;)

31.
Andrzej Sporadik 2015.01.04 23:42 | <#> | [Reply](#)

Wojtek, czepiasz się :)

32.
Bleju 2015.01.04 23:46 | <#> | [Reply](#)

W dzisiejszych czasach nie trzeba nawet inwestować w scanner. Wszystkie wymienione rodzaje transmisji, modulacji i większość pasma załatwia tuner USB na RTL2832U pracującego jako SDR. :-) Tetra, Trunking, Analog ,ADS-B (transpondery w samolotach na 1.2GHz) itd. Wszystko programowo. Koszt około 100zł. Pomijam antenę, ale przy odrobinie pomysłowości wszystko da się zrobić. Ja osobiście stroje antenę od tego tunerka przy pomocy tulejek dystansowych :-)

o
Luzik 2015.01.06 09:29 | <#> |

Chcesz powiedzieć, że TETRĘ podsłuchujesz ? Czy tylko oglądasz :)

33.
owopo 2015.01.05 00:21 | <#> | [Reply](#)

A w radijkach amatorskich które można sobie zabrać w góry itp gdzie zasięg można stracić też jest szyfrowanie ?

34.
Krzysiek 2015.01.05 00:23 | <#> | [Reply](#)

kiedyś za łebka mieliśmy z kolegami walkie talkie i w jednym miejscu na mojej ulicy (pod przewodami telefonicznymi) było zawsze słyszeć jakieś rozmowy telefoniczne (niestety tylko jedna strona rozmawiającą) zawsze się zastanawialiśmy jakim cudem ściągało takie coś na sprzęcie za 30zł. Był to rok 1995-1996

o
[linoskoczek](#) 2015.01.05 01:24 | <#> |

Ja się nasłuchiwałem na podobnym walkie talkie jak to ktoś mieszkający niedaleko kupował traktor :) ciekawa sprawa jest też z przejeżdżającymi pociągami, gdy jest się z 10km od dworca: tam prawie zawsze ktoś gada :D

o
MAD 2015.01.05 01:39 | <#> |

Na słupie mógł być przekaznik do telefonu tak zwanego radiowego. Radiolinia zastępowała kabel tam gdzie instalacja kabla była nieopłacalna lub niemożliwa. W 91 to mogły być analogowe komórki Centertel. Świetnie odbierały np na telewizorach.

o
exti 2015.01.05 03:06 | <#> |

To było takie bezprzewodowe przedłużenie linii telefonicznej, które swego czasu instalowała Telekomunikacja Polska. Urządzenia pracowały na częstotliwościach ok. 450 i 460 MHz w systemie NMT 450. A słyszałeś to w walkie-talkie dlatego, że odbiorniki w takich zabawkach były kiepskiej jakości i nie wytłumiały w odpowiednim stopniu wyższych harmonicznych odbieranego sygnału.

o dza 2015.01.05 08:51 | <#> |

zgadza się, pamiętam jak za młodego można było trafić na rozmowę telefoniczną na zwykłej zabawce. Zabawną historię miałem jak w któregoś pięknego dnia trafiłem na rozmowę dwóch lasek, od samego słuchania uszy były czerwone, mimo, że jeszcze zbyt dużo się jeszcze nie rozumowało... I wydaje mi się, że było słychać obie strony, ale ręki nie dam sobie uciąć.

Inną zabawką było zakłócanie fal radiowych, ile radochy było jak trafiło na mohera zaklinającego dzieciaków przeszkadzających w odbiorze jedyne słusznego radia

o Luzik 2015.01.06 09:19 | <#> |

Rozmów telefonicznych dalej można bez problemu słuchać w eterze. Zmieniły się tylko częstotliwości i trzeba mieć już nieco inny sprzęt. Dalej jednak ludzie rozmawiają w otwartych, niekodowanych kanałach, których można słuchać. Aż dziw, że nie zrobiono z tym porządku.

o Robert 2015.01.06 16:27 | <#> |

Coś tak mi się kojarzy że Idea czy jak to tam się zwało dawało jakiś czas temu stare telefony NMT w gratisie do telefonów komórkowych – w końcu infrastruktura działała nadal, więc nadal można było słuchać pierdół bab gadających o zakupach przez 3 godziny...

o Luzik 2015.01.07 08:41 | <#> |

No nie wiem czy zawsze są to pierdoły... Moim zdaniem operatorzy, którzy idą na łatwiznę i puszczaają telefonię w eter bez kodowania powinni zostać za to ukarani. Ludzie robią różne rzeczy przez telefon. NIEŚWIADOMIE autoryzują usługi, sprawdzają stany kont, podają dane osobowe w urzędach, szpitalach czy bankach. To przecież idzie w eter i praktycznie każdy przy odrobinie wysiłku może tego słuchać. Może tym powinien zająć się niebezpiecznik? a nie pierdołami typu podsłuchiwanie taxi.

35. Radioaktywny 2015.01.05 04:43 | <#> | [Reply](#)

“który opisał temat coraz bardziej popularnych i wykorzystywanych w Polsce systemów cyfrowej ruchomej łączności radiowej,” A kiedy kolega opíše łączność nieruchomą?

36. sniezynkobzik 2015.01.05 06:13 | <#> | [Reply](#)

W większości transmisje służb są szyfrowane i możemy zapomnieć o tym że szyfr zostanie złamany. Jak wspomnieli koledzy u nas w Polsce jest TETRA także jeżeli ktoś zna jak działa kodowanie ACELP byłby w stanie zdekodować nieszyfrowaną transmisję. Ale czy ktoś nie szyfruje jak można szyfrować? Jak dla mnie na dzisiejsze realia artykuł jest nieaktualny. Jakby był pisany 10 lat temu to wtedy jak najbardziej OK.

o Luzik 2015.01.06 09:36 | <#> |

Potwierdzam. Jeszcze 5 lat temu można było dużo słuchać służb w eterze. Popularny EDACS był bardziej zabawką niż systemem utrudniającym podsłuch. W tej chwili nawet drogówka, karetka itp... wszystko jest przeniesione na cyfrowe kanały kodowane. Można sobie posłuchać wodociągów, taxi i ochroniarzy, choć też coraz mniej już idzie otwartym kanałem. Niedługo pozostaną tylko elektroniczne nianie :) U mnie na osiedlu jest kilkanaście takich pudełek, które wysyłają w eter wszystko, co dzieje się w domu.

Ci, którzy twierdzą, że podsłuchują TETRĘ po prostu piszą bzdury.

o z 2016.12.12 03:49 | <#> |

Bzdury piszesz. Tetrę (nieszyfrowaną a taka jest w PL) można nasłuchiwać softem Telive. Do MOTOTRBO / DMR są już skanery.

37. Damien 2015.01.05 10:13 | <#> | [Reply](#)

Wystarczy jak posiadasz skaner np. firmy baofeng uv-5r masz częstotliwość i klucz posłuchasz i pogadasz z Policją to najłatwiejszy sposób.

Można też kupić motorole ewentualnie kenwood są profesjonalne firmy ale częstotliwość i klucz wpisujemy przez program komputerowy (potrzebny kabelek). Robiłem to ale mnie jakoś o nie ciekawi. Klucze i częstotliwości są dostępne w internecie trzeba sobie poszukać ;-)

I Pobawić się w takich dwóch co udawali gliniarzy :)

Nie wiem komu to potrzebne ale każdy ma swoje Kretki :)

o

Tomek 2015.01.06 10:27 | <#> |

“Wystarczy jak posiadasz skaner np. firmy baofeng uv-5r masz częstotliwość i klucz posłuchasz i pogadasz z Policją to najłatwiejszy sposób.”
Przecież ty nie masz o tym pojęcia...

o

vanitas 2015.01.07 17:31 | <#> |

- Baofeng UV-5r to transceiver (urządzenie nadawczo-odbiorcze) nie skaner.
- to urządzenie nie obsługuje szyfrowania (więc “kluczy” nie “wgrasz”), kluczy nie znajdziesz też w internecie
- “kretki” – to takie skrzyżowanie kreta z fretką?

38.

gonzo 2015.01.05 10:18 | <#> | [Reply](#)

Dodatkowo wg UKE “uzyskanie informacji nadawanych za pośrednictwem fal radiowych, telewizyjnych czy sygnału satelitarnego, nawet jeżeli jest dokonywane w paśmie zastrzeżonym, nie stanowi realizacji znamion z art. 267 § 1, chyba że odbiór tak nadawanych informacji uzależniony był od przełamania określonego kodu zabezpieczającego czy też posiadania specjalnego urządzenia odbiorczego”.

Specjalnym urządzeniem odbiorczym staje się komputer z zainstalowanym oprogramowaniem do dekodowania sygnału cyfrowego np. MOTOTRBO.

PC oprogramowanie to tak samo jakby zakupić specjalistyczny odbiornik pracujący na pasach i w standardach kodowania (niezależnie czy szyfrowanych czy też nie) używanych przez policję

39.

Żoliborz 2015.01.05 13:15 | <#> | [Reply](#)

Chodzi mi o praktyczne wykorzystanie tej wiedzy. Jeśli idę napaść na bank to warto mieć przy sobie odbiornik częstotliwości policyjnej czy raczej to pic na wodę?

o

miki 2015.01.05 23:27 | <#> |

Kto pierwszy przyjeżdża na miejsce wypadku:

- a) policja,
- b) pogotowie ratunkowe
- c) laweta

o

Robert 2015.01.06 16:34 | <#> |

Ha ha ha brawo dla tego Pana! 10/10 odp c) ;)



o

[Lukasz032](#) 2015.01.06 20:21 | <#> |

Najczęściej straż pożarna.

40.

[Dawid](#) 2015.01.05 13:50 | <#> | [Reply](#)

Nasłuchiwanie łączności radiowych polskich służb? Z pewnością ta częstotliwość jest zmieniana co pewien czas

o

BloodMan 2015.01.05 13:59 | <#> |

Jasne, a informacje o tym jaka częstotliwość jest “dzisiaj” przekazywana jest telefonicznie – po czym wszyscy lecą do swoich papug żeby je przestroić – dokładnie o wpół do dziesiątej w Polsce.
BP,NNMSP ;)



41. modInfo 2015.01.05 14:33 | # | [Reply](#)

Ale wiecie, że to nielegalne, nawet na egzaminie mówili o tym.

o

BloodMan 2015.01.05 14:46 | # |

To źle mówili. <http://www.ifp.pl/index.php?name=PNphpBB2&file=viewtopic&t=2228&start=103>



42. [kszeze](#) 2015.01.05 17:23 | # | [Reply](#)

Nie wiem co jest powodem tego, że w mojej okolicy nic nie mogę złapać nic z 172-176 MHz. Może antena za słaba a może nie odpowiednia do tej częstotliwości. Kontakt z Niebezpiecznik.pl jest trudny. Wiele razy już pisałem email i zero odzewu, więc w wniosek jest taki, że po co pisać skoro i tak nie odpiszą...

43. Neevor 2015.01.05 21:16 | # | [Reply](#)

Dla strefy w ramach jednej częstotliwości wydzielone jest kilka kanałów. Pierwszy jest zwykle kontrolny i wszystkie radia go słuchają. Na tym kanale między innymi nadawana jest informacja gdzie jest impreza czyli na którym z pozostałych kanałów radio ma operować. Kanały jednym kliknięciem przełącza goście w centrali zgodnie ze swoim widzimisie. I to jest ta mityczna zmiana częstotliwości.

44. Tomasz 2015.01.06 00:28 | # | [Reply](#)

Ciekawy temat...Zacznijmy od tego, że można nasłuchiwać ale nie wolno dzielić się informacją. Czyli jak już kiedyś zapadł wyrok na kierowcę autobusu... w domu mógł słuchać ale włączanie nasłuchu w autobusie tak, że ktoś inny mógł usłyszeć było przestępstwem...

Żeby zlokalizować częstotliwość można wykorzystać skaner Uniden i funkcję close call czyli wyszukiwanie najmocniejszych sygnałów w okolicy. Można odpalić SDR RTL i obserwować wykres wave :) Najprościej zrobić skanowanie w skanerze czy też radiu najlepiej z krokiem 12,5kHz. Wszystkie głosowe analogowe transmisje są nadawane w fm, no nie licząc samolotów.

Jeśli już uda się złapać sygnał ale nie będzie to sygnał analogowy... usłyszymy "brzęczenie". W tym wypadku oznacza to:

- transmisja serwisowa np. z "wodociągów"
- MPT 1327 – to nas dzisiaj nie interesuje ;)
- TETRA – póki co ten standard łączności nie został złamany. Korzysta parę służb ale ze względu na koszty i niekompatybilność odchodzi się od niej. Np. ZTM Gdańsk posiada radia TETRA w swoich tramwajach i autobusach.

- dPMR – w skrócie wielodostęp z podziałem częstotliwości. Jest to "prostsze DMR – połówka" Z tego standardu korzysta się na autostradzie, w zakładach, prywatnej łączności. "Na jednej częstotliwości z krokiem 6,25kHz jest możliwość 2 rozmów". Podział kanału na 2 według potrzeby. W analogu wykorzystuje się 12,5 do jednej rozmowy. Tutaj jest to zagęszczone i łatwiej przydzielany dostęp do wolnego "kanału"

- DMR – w skrócie wielodostęp z podziałem czasowym. Czyli na jednej częstotliwości rozmowy mogą prowadzić 2-3 osoby jednocześnie. To jakby wykorzystane 25kHz w jednym momencie :) Stosowany kodek AMBE+2. Z tego standardu korzysta policja, inne służby, TOPR, GOPR. Świetna jakość głosu, smsy + lokalizacje gps, łączności alarmowe i priorytetowe, grupy itd :) Tą łączność wykorzystywała policja na euro.

Nie pisałbym, że rozmowy cyfrowe są KODOWANE. Przykładowo standard DMR zapewnia możliwość szyfrowania rozmów ale to, że na analogowym radiu nie usłyszymy rozmowy a tylko brzęczenie nie oznacza SZYFROWANIA rozmów :) Służby nie będą stosować SZYFROWANIA rozmów bo jest to za drogie. Sam standard DMR to świetnie zarządzana łączność. Straż Graniczna korzysta z szyfrowania rozmów i już nawet znalezienie częstotliwości i standardu nadawania nie oznacza sukcesu...

Największa różnica radio analogowe a cyfrowe:

- analog – zawsze coś słychać i trzeszczy(nawet na skraju zasięgu)
- cyfra – albo jest albo nie ma

Aaa i co do szyfrowania rozmów w tanich radiach chińskich. Funkcja scramble + wybór grupy 1-9. Nie jest to szyfrowanie rozmów w sensie wymiany klucza pomiędzy urządzeniami. Rozmowa jest ogólnodostępna. Jest to: inversion scrambling – polegające na odwróceniu częstotliwości wokół stałej wybranej częstotliwości. Czyli to co jest tonem wysokim, będzie niskim i na odwrót. Działa pomiędzy radiami różnych producentów.

Jeśli chodzi o skanery radiowe... najlepsze ma uniden ale działają one w analogu ewentualnie APCO P25(to w EU nie przyda się – standard USA) no i może EDACS – wykorzystywany w wawie na lotnisku i czasami jeszcze przez policję. Można wykorzystać do analogu, samolotów, statków + ew jako zamiennik SDR RTL – czyli odbieranie DMR poprzez kartę dźwiękową ale to bez sensu.

Do odnalezienia częstotliwości można także wykorzystać Measuring radio frequency – koszt 30-60\$.

Nie ma póki co skanerów DMR, dPMR – jeśli chcesz korzystać z tego standardu musisz zaopatrzyć się w takie radio. Chinczyk koszt ok 700zł a w Polsce firmówka ok 2000zł.

SDR RTL – za ok 10-15\$ mamy fajne urządzenie do zabawy. Pamiętajcie jednak, że do tego jest potrzebny w miarę szybki komp + antena na zewnątrz. Na tym co dają w zestawie... szkoda zachodu. Antenki można kupić gotowe albo poszukać na google jak zrobić np. z rury miedzianej – przykładowo: j pole antenna :)

Udanych nasłuchów! :D i oby ostatnim usłyszonym przez Was słowem nie było: zadzwoń do mnie – bo tu już by trzeba słuchać GSM ;)

45.

Tomek 2015.01.06 10:30 | <#> | [Reply](#)

“Służby nie będą stosować SZYFROWANIA rozmów bo jest to za drogie.”

DMR, NXDN, Tetra stosowana przez polskie służby jest zawsze szyfrowana.

- o

Tomasz 2015.01.06 16:29 | <#> |

DMR, NXDN, Tetra stosowana przez polskie służby jest zawsze szyfrowana. – BZDURA :)

DMR, NXDN – w standardzie nie jest szyfrowane. Posiadając radio np. systemu DMR będziesz w stanie słuchać co ktoś mówi przez inne radio DMR. Abyś nie usłyszał co ktoś mówi na innym radiu DMR, osoba ta powinna mieć w radiu opcjonalny moduł szyfrujący. A to już kosztuje... Inne kwestia colour code – ale to wykorzystywane raczej z przemiennikami.

46.

satanistik 2015.01.06 11:20 | <#> | [Reply](#)

Co do wykrywania nasłuchu – w starszych odbiornikach pracował generator heterodyny o stosunkowo dużej mocy. Bardzo czuły odbiornik dawał radę wykryć to z kilkuset m. Sam wykonałem nadajnik TV pracujący na 900Mhz z heterodyny głowicy tunera SAT. Zasięg to kilkadziesiąt m bez wzmacniacza, jako odbiornik drugi taki tuner. Oczywiście każde urządzenie elektroniczne emituje jakieś zakłócenia – można np nadać jakiś sygnał i szukać jakiś jego cech w emisjach i zakłóceniach od domniemyanych odbiorników.

47.

Bohrystrojka 2015.01.06 23:55 | <#> | [Reply](#)

Po co specjalny skaner. Wystarczy stary telewizor (np. elemis) + antena inna niż szerokopasmowa – ustawiamy na początku zakresu VHF-3 i słuchamy do woli Policję i dane osobowe. Stroić telewizor należy ręcznie w trybie powolnym – automatyczne ominie.

48.

Gal 2015.01.07 08:36 | <#> | [Reply](#)

Zawsze miałem niebezpiecznika za profesjonalny serwis. Wstyd za ten artykuł :(

Primo. Autor zaledwie “liznął” temat (choć mając moją wiedzę do liźnięcia nawet się nie zbliżył). Jakby trochę bardziej pogrzebał co ciekawego dzieje się w powietrzu + miał trochę wiedzy co, gdzie i JAK działa, to by dopiero osiwił z przerażenia!!!! i pewnie piał w internecie jak kogut o poranku.

Secundo. Łamanie MOTOTRBO, czy nawet trunkingu MPT1327, czy nawet analogowych scramblerów Motoroli, czy nawet podsłuchanie kodu CTCSS.

PODPADA POD ŁAMANIE ZABEZPIECZEŃ!!!! Koniec i kropka. Na nic się tutaj zdadzą tłumaczenia w sądzie iż jest to marne zabezpieczenie, bo jest marne ale jednak zabezpieczenie. Są oficjalne stanowiska UKE, MSW i innych instytucji.

Tezo. Jeżeli nie ma żadnych zabezpieczeń, można używać skanera (i uniknąć kłopotów) pod warunkiem iż jest on homologowany przez UKE jako urządzenie odbiorcze. Teraz się podniesie wrzawa iż urządzeń nasłuchowych się nie homologuje. Tak, ale jak was nakryją i skierują sprawę do sądu, to po WASZEJ stronie jest udowodnienie iż urządzenie jest tylko urządzeniem odbiorczym, ekspertyza jest po waszej stronie. Dlaczego to jest ważne – choćby dlatego iż dla marnej jakości skanerów mogą wam udowodnić promieniowanie z obwodów pośredniej częstotliwości. I już leżycie za nadawanie w niedozwolonym pasmie A teraz uwaga druga – w niektórych skanerach jest potrójna pośrednia, szczególnie dla tych > 800MHz, zdarza się iż ta trzecia pośrednia obniża 1600MHz do pasma 127-129MHz i wchodzą wtedy następne pośrednie. Jeżeli udowodnią wam promieniowanie z pośredniej w tym kawałku – na dzień dobry macie zarzut NIEUMYŚLNIEGO SPROWADZENIA ZAGROŻENIA W RUCHU LOTNICZYM!!!! Włókno miło mieć na wszelki wypadek odpowiedni papier z samego trzewia hydry która będzie was ścigać. A teraz pokażcie mi który skaner posiada taki komplet dokumentów.

Quarto. Włodek Giller miał już mnóstwo nieprzyjemności z racji ujawnienia częstotliwości z podsłuchu – tak, samych częstotliwości!!!!, które non omen są publikowane na stronach UKE – oczywiście w mniej szczegółowej formie. Jednym z zarzutów było naruszenie tajemnicy państwowej.

Quinto. Uważam iż niebezpiecznik powinien się obracać w ramach tematów które zna a nie ujawniać w sposób nieprzemyślany informacji, od tak dla zasady.

Skrytykowałem waszą redakcję już za ten sposób działania – choćby w przypadku ujawnienia dziur w stymulatorach serca. Są pewne informacje na temat których można pogadać na odpowiedniej hack konferencji, poprowadzić badania, zaśmiać się pod nosem i zasłonić informację kotarą milczenia, a nie zachowywać się jak TVN24 – bezpieczeństwo to również odpowiedzialność, a ten artykuł narusza dobro najwyższe czyli bezpieczeństwo obywateli.

- o

sw3 2015.01.07 10:21 | <#> |

Widać Ty musiałeś dużo liczyć skoro masz taką wiedzę, że CTCSS uważasz za rodzaj zabezpieczenia.

Jeśli już to “łamanie” CTCSS jest zabezpieczaniem bo bez “złamania” (czyli używając odbiornika, który nie wie co to CTCSS) słyszysz wszystko a po “złamaniu” tylko wybraną grupę.

Co do “skanerów nadawczych” to nie twierdzą, że tak nie jest ale chyba w naszym kraju obowiązuje jeszcze zasada domniemania niewinności. Jeśli więc ktoś będzie chciał oskarżyć użytkownika skanera o nadawanie to chyba on będzie musiał udowodnić, że ten skaner sieje a nie użytkownik że nie sieje.

- o

Robert 2015.01.07 12:19 | <#> |

W prawie karnym tak. Więc jest szansa że wezmą to pod uwagę – zależy od sądu.

Tak się stało przypadku ostatniej afery hazardowej z zagranicznymi kasynami – sąd przerzucił konieczność udowodnienia gry na UKS który nie jest przyzwyczajony do udowadniania czegokolwiek bo to obywatel musi się przed nimi tłumaczyć. Kolano dla sędziego, widzę cień nadziei dla tego kraju... Generalnie raczej będą szukali haka żeby Cię udupić nawet w błahych sprawach – sprawdziłem organoleptycznie – 2 lata walczyli żeby mnie udupić za bzdurę przeciw której się sprzeciwiłem. Klika ekspertyz, zapytań do innych instytucji żeby zamknąć sprawę 130zł kosztów sądowych... Padłem na plecy jak to usłyszałem. Na moje oko proces kosztował państwo min. 5-10tys zł ale przecież trzeba pokazać obywatelowi gdzie jego miejsce zamiast zamknąć sprawę na pierwszej rozprawie uzasadniając niską szkodliwość czynu i dużą ilością wątpliwości w sprawie. Ktoś powie, przecież nie można pobić nawet drobnym występkiem – owszem zgadzam się ale jeśli sąd nie daje rady obrobić drobnych spraw i przez to cierpią grube sprawy – przedawniają się, nie znajdują winnych, świadkowie mataczą to jest przegięcie i wolę aby drobne sprawy były załatwiane szybko na korzyść obwinionego a żeby sąd przyłożył się przy tych które tego naprawdę wymagają...

P.S.

Co do CTCSS kolega Gal się naprawdę rozpędził...

Parę komentarzy wyżej BloodMan podał link do wyczerpującego opisu tego co jest “urządzeniem specjalnym” przy pomocy którego można uzyskać dostęp do “informacji zabezpieczonych przed dostępem osób postronnych” co podlega karze.

o

vanitas 2015.01.07 17:48 | <#> |

@gal

– w prawie zawsze ciężar dowodu leży po stronie prokuratury – inaczej wszyscy siedzielibyśmy za gwałt

– nawet jeśli urządzenie siało by na paśmie ATC – i tak prokurator musi udowodnić, że działało na częstotliwości na której tak sieje.

– pomijam, że moc nadawana takiego skanera musi być tak gigantyczna, że ze 100m może i cośby zakłóciło (przy braku innych sygnałów). Czyli – pewnie nie wsiadł bym z tym włączonym do samolotu (a przynajmniej do kokpitu – jeden przez r kwadrat się kłania). Powyżej 1 km od lotniska – to se mogą skarżyć każdego posiadacza samochodu (bo rozrusznik z całą pewnością zakłóca silniej niż skaner...)

– po trzecie w skanerach z potrójną przemianą częstotliwości 1 pośrednia to 266 MHz z hakiem (albo wręcz 4xx MHz) – nikt pośredniej na pasmo lotnicze nie robi. Chyba, że myślisz o jakiejś samoróbce.

– mam niejasne przecucie, że mylisz częstotliwości pośrednie z harmonicznymi – ale to tylko przecucie...

– jeśli CTSS uznajesz za kodowanie, to tym bardziej np. modulacje (albo kluczowanie). A to już absurd nawet na nasze państwo.

49.

Piotrek 2015.01.07 19:15 | <#> | [Reply](#)

<http://www.wykop.pl/link/2147154/pobity-za-skaner-nasluchowy/>

<http://i.imgur.com/eBFCxeF.jpg>

Sprawa przeciwko policji nadal w toku.

50.

sq1ktu 2015.01.07 21:24 | <#> | [Reply](#)

Ten koleś chyba nic nie kuma... Kolega który pisze o legalnym słuchaniu tylko, oczywiście ma rację. Co innego jak byśmy pracowali na tych pasmach lub nagrywali i udostępniali osoba trzecim. pozdrawiam... licenjonowany radioamator

51.

Wojtek 2015.01.08 12:17 | <#> | [Reply](#)

5 lat temu kupiłem Unidena BC346XT z grtisowo wgranymi częstotliwościami dla Warszawy. Miałem wszystko, Policję, Straż Pożarną, SM, Pogotowie. Kupiłem z myślą o nasłuchu Okęcia i PKP (lubię kolej). Czasem łapałem jakąś rozmowę przez tel. bezprzewodowy, raz udało się usłyszeć transmisję z ISS. Najciekawsze były jednak rozmowy chłopaków z Policji siedzących na budkach pod ambasadami, rozmawiających jak to się ostatnio najebali, albo jak by tu koleżankę z pracy puknąć.

52.

Andre 2015.01.12 19:04 | <#> | [Reply](#)

Koledzy, a jeśli będzie się w domowym zaciszu nasłuchiwać służb (straży, policji itp.) na BAOFENG UV-5R bez nadawania, to jest to legalne, czy nie? Przede wszystkim – czy jest to bezpieczne, mogą dorwać nas w domu?

o

nnnnnnn 2015.09.26 16:33 | <#> |

A po co chcesz tego słuchać? To głupoty które normalnego człowieka nudzą po 5min. nasłuchu.

53.

noway 2015.01.21 23:28 | <#> | [Reply](#)

już od dawna penalizowane jest “odszyfrowywanie” zmieniony Art. KK brzmi:

“Art. 267 kk § 1 Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2 Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3 Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4 Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5 Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.”

54.

Silvio 2015.02.12 10:10 | <#> | [Reply](#)

A słyszeliście o projekcie (w fazie rozwoju) urządzenia AOR o nazwie AR-DV1 . To może być (mam nadzieję) dla nasłuchowców piękna sprawa- DMR,dPMR,NXDN, Apco25 itp! Swoją drogą to cena będzie się raczej zaczynać od 4 kółek w górę !

55.

a 2015.08.21 16:08 | <#> | [Reply](#)

z ta tetra niemożliwa do podsłuchania to sie troche zagalopowaliscie (chodzi mi o stan ze stycznia/lutego 2015, kiedy byly pisane komentarze pod artykulem).

milo by bylo jakby jeden z drugim ekspert wpisal w google “tetra decoding” albo “tetra decoding radioreference” przed napisaniem komentarza. oprogramowanie jest publicznie dostepne od listopada 2014

56.

osmanbts-usrp 2015.09.05 02:10 | <#> | [Reply](#)

tetra jest zlamana tylko oficjalnie osman sie juz niewychyli..za złamanie tetry dostal od NSA dyplomy uznania z podsłuchem w ramie co umiescil na fot..wypuscil urzadzenie i tetra jest w standardzie uniego. usrp sluchasz wszystko.

57.

Adam 2015.09.10 10:12 | <#> | [Reply](#)

Gdzie mozna znalezc aktualne aktualne czestotliwosci sluzb?

58.

nnnnnnn 2015.09.26 16:31 | <#> | [Reply](#)

Bzdury, systemy cyfrowe same w sobie nie dadzą się podsłuchać analogowymi skanerami, dodatkowo transmisję szyfruje się kluczem, zdekodowanie jest trudne/b.trudne i jest nielegalne o czym “pasywny krótkofalowiec” a raczej pseudokrótkofalowiec napisać zapomniał bo nie zgłębił się w przepisy. Dekodowanie przekazu zaszyfrowanego podlega art. o tajemnicy korespondencji. Na szczęście coraz więcej służb idzie w DMR i wszystkie oszołomy i inni frustraci którzy onанизują się podawanymi numerami pesel w policyjnych komunikatach będą słyszeć w swoich tanich chińskich skanereach “piły” i “bulgoty” cyfry:-)

o

Tomasz 2016.02.09 10:43 | <#> |

witam a mozesz komus pomuc ,jak cyfrowke nasluchac?? pomodrogowa”

59.

dddsa 2015.09.27 12:10 | <#> | [Reply](#)

“Wszystkie wymienione rodzaje transmisji, modulacji i większość pasma załatwia tuner USB na RTL2832U pracującego jako SDR” mam ten tuner, ale parametry ma strasznie słabe – odporność na intermodulację itp. nie warto się w to bawić

60.

Abc 2015.10.04 23:10 | <#> | [Reply](#)

Co bedzie najbardziej odpowiednie do podsłuchu policji, strazy granicznej. Jestem z gdanska.

o

gość 2015.10.18 19:42 | <#> |

Ucho będzie najlepsze. A po co chcesz tego słuchać? Jesteś normalny? Poza tym masz zerową wiedzę w temacie.

61.

Tomasz 2016.02.09 10:35 | <#> | [Reply](#)

Witam w moim miescie zlyzby przeslyzy na cyfrowke” mam problem bo moj skaner poprostu przestal dzialac ,,-zarabiac”) czy moze ktos z Was mi pomoc , czytam wasze posty i cos rozumiem ale wolał bym kupic gotowy sprzet do nasluchu z gory dziekuje

62.

fakir 2016.09.19 19:03 | <#> | [Reply](#)

oj nie bardzo adres pesel i imie i nazwisko jest tylko czesc np imie = pesel lub adresnie pelny bez immienia., bez przesady, nadto nie podaje sie numeru dokumentow wiec te dane nie sa pelne, drodzy przyjaciele kredytu na to niedostaniecie

63.

Piotr 2016.11.23 14:14 | <#> | [Reply](#)

Teraz nie posluchasz kolego, kodowane jest w BP lub EP . Jak EP to masz raczej pozamiatane. To juz wyzsza szkola.

64.

Maciek 2017.01.09 20:51 | <#> | [Reply](#)

Niektórzy rzucają jakimiś paragrafami. Po co? Prawo nigdy nie służyło, nie służy i nie będzie służyło do straszenia. Ludzie którzy wykorzystują faktycznie nasłuch mają to głęboko w dupie. Z tym jest jak z mandatami, większe gadanie o nich powoduje tylko większą agresję i chęć łamania prawa.

65.

Piotr 2017.01.23 18:02 | <#> | [Reply](#)

Nie jest prawdą, że nasłuchiwanie służb jest w Polsce legalne. Tzn. prawda, samo posiadanie urządzenia odbiorczego jest, ale już nasłuch służb narusza tzw. tajemnicę telekomunikacyjną (Art 159 ustawy Prawo Telekomunikacyjne). A to co autor artykułu zaznacza “o ile nie przekazujemy tych informacji osobom trzecim” to już w ogóle pomylenie wszystkiego z art. 267 § 4 Kodeksu Karnego (który dotyczy informacji *pozyskanej poprzez złamanie zabezpieczenia*). Tak więc... urządzenia nasłuchowe można posiadać, można używać do nasłuchu informacji (za ustawą Prawo Telekomunikacyjne) “ze swej istoty jawnych, z przeznaczenia publicznych lub ujawnionych postanowieniem sądu, (...) prokuratora (...) lub na podstawie odrębnych przepisów”, czyli można sobie słuchać stacji radiowych, krótkofalowców itp. ale nie służby (ich komunikacja jest objęta tajemnicą telekomunikacyjną, nawet jeśli nie jest szyfrowana).

66.

Maja 2017.04.11 11:43 | <#> | [Reply](#)

TETRA jest stosowana “głównie w Krakowie”, a nie “głównie w Warszawie”.

67.

marcus 2018.10.11 19:28 | <#> | [Reply](#)

Co za lamer napisał takie bzdety. Częstotliwość można modulować , zmieniać ale kodować .. może ktoś mi wyjaśni o co chodzi ? Kodować można przesyłane informacje ale nie częstotliwość !! Może autor zakoduje częstotliwość prądu 50 Hz :-)

o

Piotr 2018.10.12 01:07 | <#> |

@marcus Owszem, można kodować częstotliwość. Po pierwsze w paśmie RF (radiowym) można na przykład szybko przeskakiwać (kilka razy na sekundę) po iluś tam częstotliwościach wg konkretnego klucza (hint: frequency hopping) co powoduje, że nasłuchiwanie typowym skanerem jest niemożliwe bądź mocno utrudnione (skaner musiałby w taki sam sposób zmieniać częstotliwość odbiorczą, czyli musiałby mieć odpowiedni klucz kodujący częstotliwości). Po drugie można stosować technologię tzw. rozpraszania widma (hint: spread spectrum) czyli częstotliwość “podstawowa” jest mieszana iloczynowo z pseudolosowym szumem (z odpowiednio szerokim widmem częstotliwości), odbiornik musi mieć analogiczny generator pseudosumu z analogicznym kluczem (aby generował dokładnie identyczny szum) – to tak na prawdę też jest swego rodzaju frequency hopping, tylko nie skokowy lecz ciągły (częstotliwość jest przestrajana cały czas a nie skokowo). W obydwu przypadkach (to tylko przykłady, technologii tego typu jest więcej, na przykład poczytaj jak działa Bluetooth czy LoRa w części radiowej :D) jest zarówno kodowanie informacji (najczęściej) jak i kodowanie częstotliwości na której akurat w danej chwili przebiega komunikacja (i która się zmienia skokowo bądź ciągle wg klucza kodującego).

Zanim nazwiesz kogoś lamerem najpierw się zastanów, czy to nie jest obszar Twojej nieświadomej niekompetencji (czegoś, o czym... nie wiesz, że nie wiesz :D).

o

Piotr 2018.10.12 01:23 | <#> |

Kodowanie częstotliwości polega na jej zmianie w czasie wg ustalonego wcześniej klucza kodującego. Dwie najczęstsze metody to szybka zmiana kanałów (frequency hopping), zwykle kilka razy na sekundę wg pseudolosowego klucza kodującego kanał/częstotliwość, oraz rozpraszanie widma (spread spectrum) czyli mieszanie iloczynowe częstotliwości “wyjściowej” z jakimś generatorem, najczęściej pseudosumu, to powoduje, że częstotliwość wyjściowa zmienia się nie w sposób skokowy, tylko ciągły. W obydwu przypadkach tą zmianę częstotliwości wyjściowej “w takt” losowych kluczy (dyskretnych bądź ciągłych) nazywa się w uproszczeniu kodowaniem częstotliwości (czyli dla ewentualnego podsłuchującego tajemnicą staje się nie tylko sama treść, ale też konkretna częstotliwość na jakiej w danej chwili nadaje nadawca i jak ta częstotliwość się zmienia nawet jeśli w jakiejś krótkiej chwili uda się złapać na moment sygnał).

Warto przed wyzwaniem kogoś od lamerów sprawdzić wpierw zakres swojej nieświadomej niekompetencji (rzeczy o których... nie wie się, że się nie wie :D). Owszem, w artykule jest kilka błędów (między innymi są powielone mity na temat obowiązującego w Polsce prawa) ale akurat kodowanie częstotliwości istnieje (i nawet jest całkiem powszechne, oparte są o to sieci komórkowe 3G i 4G, jest stosowane w Bluetooth czy WiFi, w podstawowym zakresie w sieciach LoRaWAN itp.).

68.

Lol 2019.01.03 00:54 | <#> | [Reply](#)

Piszcie dalej o prawie – spieracie się wzajemnie o prawo ustalone przez oprawce! Jaki w tym sens drodzy na w pol przebudzani....

69.

power 2019.03.13 17:38 | <#> | [Reply](#)

juz jest z glowy, analog działał do konca 12 marca 2019 we Wrocławiu, pozamiane

70.

power 2019.03.15 00:23 | <#> | [Reply](#)

teraz słyhać pierdzenie na 172.600.000 :D kodowane, drogówki już nie posłuchamy, choć można inne :) lecz tam mało gadają no i trudności ze słuchaniem obydwu stron, moc skręcona, chyba ze na sdr to można tetrę i edacs kulawo, radyjko do szuflady na wypadek W
pozdrawiam z Wrocka

o

Dudi 2019.04.25 21:22 | <#> |

A czego uzywa teraz Wroclawska policja ? przeszli na DMR czy cos innego ?

71.

Bo 2019.04.28 22:52 | <#> | [Reply](#)

Przeszli na DMR`a ale chyba kodowanego, bo na SDR jest bełkot, po mimo używanej wtyczki dsd...

72.

Noga 2019.05.07 13:32 | <#> | [Reply](#)

A w Warszawie też już oficjalnie jest cyfrowy?

73.

fg 2019.06.13 23:49 | <#> | [Reply](#)

“To co mówi Wojtek to prawda, dekodowanie DMR czy MOTOTRBO podpada pod przełamywanie zabezpieczeń” – arek ty podpadasz pod przypadek ciężkiego idioty, który nie odróżnia dekodowania od deszyfrowania.

74.

Adam 2019.09.21 10:01 | <#> | [Reply](#)

Znam jedną stację B468UR

Twój komentarz

Imię*: Email*: URL:

zając komentarz akceptujesz [regulamin dodawania komentarzy](#). Przez moderację nie przejdą: wycieczki osobiste, komentarze nie na temat, wulgaryzmy.

☐ Chcę otrzymywać powiadomienia e-mail o nowych komentarzach

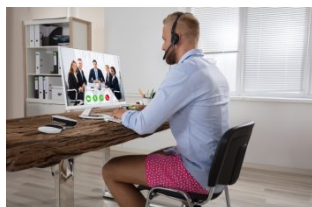
[RSS dla komentarzy:](#) 

• Zamów nasz wykład dla twojej firmy!



[Posłuchaj jednego z naszych 8 cyberwykładów. Wiedza podana z humorem i w przystępny dla każdego pracownika sposób. Kliknij tu i zobacz opisy wykładów!](#)

• Zobacz nasze webinary!



[Praktyczna wiedza i przystępny, zrozumiały dla każdego język. Kliknij tutaj i zobacz nasze webinary, o bezpieczeństwie pracy zdalnej, ochronie przed wyciekami danych i zabezpieczaniu kont w serwisach internetowych przed włamaniami!](#)

• Artykuły na e-mail

Aby raz dziennie otrzymać info o nowych postach, wpisz swój e-mail:

lub śledź nas za pomocą:



• [Aktywne ataki \(Polska\)](#)

- [\[P\] SMS-y od InPost](#)
- [\[P\] SMS-y od PZU](#)

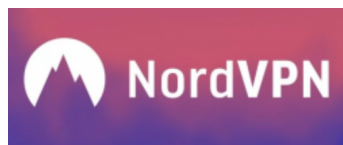
• [*ptr \(czyli nasz linkblog\)](#)

- [** Telekomy ujawnia dane o lokalizacji – zobacz projekt przepisów](#)
- [** 7 zasad dla technologii do walki z koronawirusem](#)
- [** Ruszył hackaton przeciwko COVID-19](#)
- [** Aplikacja “Kwarantanna domowa” będzie obowiązkowa, ale nie otwarta](#)
- [** Sprzedawca prosi o PIN do karty “bo koronawirus”](#)
- [** Jak tworzenie softu na terminale płatnicze w Polsce wyglądało](#)
- [** Przybywa oszustw na BLIK-a](#)

• Archiwum

Archiwum

• Polecamy ten VPN:



Z NordVPN korzystamy sami i nazywamy go “najlepszym z najtańszych” (zwłaszcza w wariantcie [na 3 lata, gdzie wychodzi 3,29USD za miesiąc](#)). W ramach licencji możesz go zainstalować na 6 urządzeniach, więc zabezpieczysz sprzęt całej rodziny. Ma aż 5500 serwerów z 59 krajów, więc jesteś w stanie wyjść na świat np. z USA i oglądać serie Netflix dostępne tylko tam i często zmieniać IP. Pozwala na używanie torrenta. Nie trzyma logów, a siedzibę ma w Panamie, poza prawną jurysdykcją Polski. Wykupując go [po tym linku](#), wspierasz redakcję Niebezpiecznik.pl

[Kontakt](#) | [Reklama](#) | [Praca](#) | [Audyty bezpieczeństwa](#) | [Szkozenia](#)

Wszelkie prawa zastrzeżone © 2009- echo date("Y");

Niebezpiecznik.pl

ul. Armii Krajowej 12/64, 30-150 Kraków
tel. 12 44 202 44; e-mail: biuro@niebezpiecznik.pl