POLSKI ZWIĄZEK KRÓTKOFALOWCÓW
Organizacja Pożytku Publicznego

KOMUNIKAT PZK

KOMUNIKAT Polskiego Związku Krótkofalowców

NR 52/2021 z dnia 29 grudnia 2021 r.

Witamy wszystkich Słuchaczy i Odbiorców naszych cotygodniowych komunikatów. Komunikaty PZK są nadawane w każdą środę o godzinie 18:00 czasu lokalnego na częstotliwości 3702,5 KHz +/- QRM, oraz publikowane na portalu PZK, a także rozsyłane na listę wysyłkową. Zautomatyzowane archiwum komunikatów znajduje się na osobnym serwerze: **https://komunikat.pzk.org.pl/**

TO OSTATNI KOMUNIKAT PZK ROKU 2021

Nowy Rok

Z okazji nadchodzącego Nowego Roku 2022 redakcja Komunikatów życzy wszystkim odbiorcom i czytelnikom naszych Komunikatów zdrowia, szczęścia oraz sukcesów zarówno w życiu osobistym, zawodowym ,jak w naszym wspaniałym hobby - krótkofalarstwie.

Redakcja Komunikatów PZK

I. Sprawy organizacyjne

1. YOTA jeszcze raz

Krajowy konkurs PZK dla młodych krótkofalowców pod nazwą "Miesiąc YOTA SP 2021" trwa, podobnie jak akcja IARU "December YOTA Month 2021". Stacje z sufiksem YOTA cieszą się na pasmach dużym wzięciem.
Być może nie wszyscy słyszeli o zawodach "YOTA Contest 2021" (regulamin na

stronie https://www.ham-yota.com/contest/#rules). Trzecia (ostatnia) runda zawodów odbędzie się 30 grudnia 1200-2359 UTC, emisje CW i SSB. Może w nich uczestniczyć każdy, podając w raporcie swój wiek. Za stacje z wiekiem powyżej "25" otrzymuje się 1 punkt (3 za DX), natomiast stacje młodzieży są punktowane bardzo wysoko - od 10 do 13 punktów. Uwaga - stacje młodzieżowe startujące
w zawodach niekoniecznie muszą mieć sufiks YOTA!
Powodzenia w zawodach!

W imieniu PZK - Mirek SP5GNI

2. Składka ulgowa dla członka zwyczajnego od 71 roku życia

W uzupełnieniu informacji o składkach członkowskich na 2022 rok, w związku z pytaniami o interpretację zapisu o "Składce ulgowej dla członka zwyczajnego od 71 roku życia" wyjaśniam.
Wszystkim urodzonym przed 15 stycznia 1952 roku w 2022 roku przysługuje prawo opłacenia - składki ulgowej dla członka zwyczajnego od 71 roku życia. Przysługuje takie prawo, ale nie mają takiego obowiązku.
Urodzeni po 15 stycznia 1952 roku, ale przed 15 lipca 1952 roku mają prawo opłacić - składkę ulgową dla członka zwyczajnego od 71 roku życia, za drugie półrocze 2022 roku.

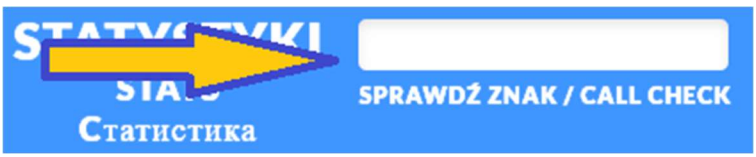
Jan Dąbrowski - Skarbnik PZK

II. Wydarzenia

3. Podsumowanie akcji dyplomowej: „20 lat aktywnej służby amatorskiej radiokomunikacyjnej na Międzynarodowej Stacji Kosmicznej”

Akcja dyplomowa trwała w okresie od 13 listopada do 21 grudnia 2020 roku. 11 stacji pracowało na 14 pasmach radiowych używając 10 różnych emisji. Stacje te nawiązały ponad 20 000 łączności radioamatorskich z ponad 10 000 rożnymi stacjami ze 136 krajów. Osoby które spełniły warunki otrzymania specjalnego spersonalizowanego i numerowanego dyplomu pamiątkowego https://ariss.pzk.org.pl/20yHAMonISS/#dyplom mogą go wciąż pobrać przez Internet z systemu LOGSP https://ariss.pzk.org.pl/20yHAMonISS/#dyplom

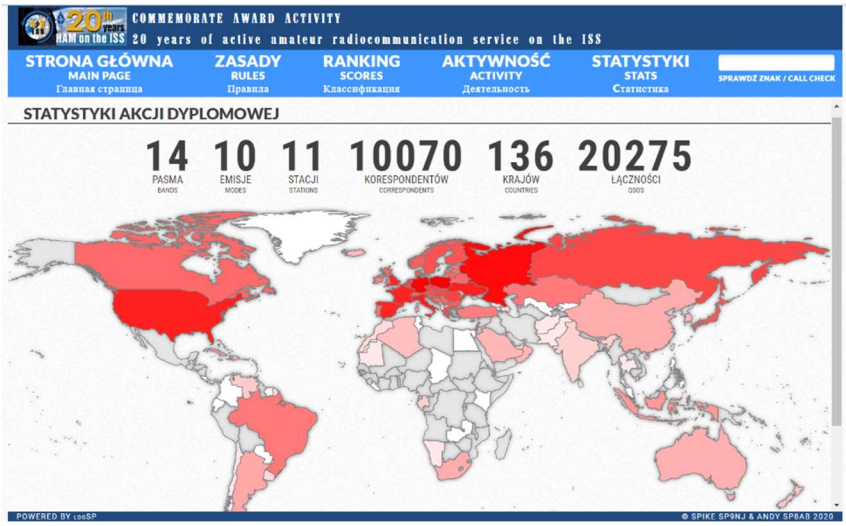
W tym celu na stronie LOGSP należy w polu „sprawdź znak” wpisać swój znak.



Nagroda jest dostępna w dwóch językach angielskim i rosyjskim.

Bardzo dziękuję wszystkim operatorom, którzy nawiązali łączności w ramach akcji przypominającej ten historyczny moment i obchodzili w ten sposób dwadzieścia lat używania w sposób ciągły sprzętu radioamatorskiego na stacji kosmicznej. Ponieważ dwukierunkowe łączności nawiązali wszyscy radiooperatorzy, nie tylko pasjonaci ARISS, prosimy o rozpowszechnianie wśród swoich koleżanek i kolegów informacji o możliwości pobrania nagrody, za co

z góry dziękujemy.



Aktywność radioamatorska w tym okresie została zorganizowana w celu upamiętnienia i promocji najważniejszych wydarzeń związanych z obchodami 20-lecia umieszczenia sprzętu krótkofalarskiego na Międzynarodowej Stacji Kosmicznej (ang.: ISS, pl.: MSK). W 1996 roku ARISS (Krótkofalarstwo na Międzynarodowej Stacji Kosmicznej) rozpoczęło prace nad przygotowaniem amatorskiego sprzętu radiowego i umieszczeniem go na stacji orbitalnej. W 1999 roku w kosmosie połączono pierwsze moduły stacji orbitalnych wyprodukowane w Rosji i USA. Na początku listopada 2000 roku w ramach pierwszej wyprawy na MSK, pierwsza załoga przeprowadziła udane próby nawiązania łączności przy użyciu amatorskiego sprzętu radiowego ze stacji kosmicznej ze stacjami naziemnymi na całym świecie. Próby te rozpoczęły się 13 listopada 2000 roku i trwały kilka dni. W dniu 21 grudnia 2000 roku odbyła się pierwsza wcześniej zaplanowana łączność ze szkołą (ARISS school contact). Podczas tej rozmowy uczniowie ze szkoły w USA otrzymali na swoje pytania, odpowiedzi bezpośrednio z kosmosu od astronauty z pokładu MSK. Od tego czasu zorganizowano ponad 1300 edukacyjnych łączności ARISS na całym świecie, w tym dwadzieścia jeden dla uczniów z placówek oświatowych w Polsce.
Dla upamiętnienia tych historycznych wydarzeń, krótkofalowcy z polskich klubów krótkofalarskich: SP2ZIE, SP3POW, SP3YOR, SP5PMD, SP7POS, SP8YAY, SP9PKS (w porządku alfabetycznym), które wcześniej organizowały szkolne łączności ARISS, prowadzili łączności, posługując się unikalnymi okresowymi znakami wywoławczymi swoich stacji. Akcja została zorganizowana przy pomocy 27 Oddziału Terenowego Polskiego Związku Krótkofalowców (PZK) Południowa Wielkopolska, Zarządu Głównego PZK oraz Stowarzyszeniu Radioamatorów i Krótkofalowców „Delta”. Przedsięwzięcie zostało zorganizowane w ścisłej współpracy z ARISS, przy wsparciu stacji naziemnej IK1SLD ARISS we Włoszech oraz ISS FanClub (F4KLX, TM20ISS).

Operatorzy stacji SN20ISS: Dariusz Mankiewicz SP2HQY, Robert Koralewski SQ2WHH.

Operatorzy stacji HF20ISS: Wiesław Paszta SQ5ABG, Ewa Michałowska SP5HEN, Krzysztof Morawski SP5DU, Artur Błachowiak SQ5ABF.

Operatorzy stacji HF7ISS: Ryszard Gawron SP7SEW, Paweł Piotrowski SP7AH, Marek Kwiecień SP7DPV, Marian Matynia SP7RJI.

Operatorzy stacji HF8ISS: Jacek Kotowski SQ8AQO, Waldemar Pisarczyk SP9MZX, Wiesław Świerczyński SQ8CBM, Cezary Wroński SQ8MXC, Tomasz Kurczyński SQ8MXE.

Operatorzy stacji HF9ISS: Piotr Staniek SP9TPZ, Antoni Kuźnik SP9SM, Piotr Górny SP9TPV. Operatorzy stacji SN3ISS: Marcin Trawiński SP3BBS, Piotr Skowronek SP3QDX, Jarosław Rokicki SP3AYA, Dariusz Florczyk SP3TYJ, Paweł Modlitowski SQ3POS, Piotr Błaszczyk SP3OS.

Operatorzy stacji 3Z20ARISS: Olgierd Pilarczyk SQ3SWF, Armand Budzianowski SP3QFE, który był również operatorem stacji SO1SS.

Claudio Ariotti był operatorem stacji IK1SLD.

Operatorzy stacji F4KLX: Micol Ivancic IU2LXR, Carlo Castellacci IK5JRZ, Juergen Keller DL4YCD, Sylvain Valat F1UJT, Michel Nawrocki F1AFW, Marc Renaud F0FHU.

Operatorzy stacji TM20ISS: Gilles Gary F4UJU, Nicolas Nolhier F5MDY, Pierre-Marie Thomas F4FCE, Sylvain Valat F1UJT, Michel Nawrocki F1AFW, Marc Renaud F0FHU.

Oprócz operatorów, zaangażowani byli wolontariusze: Frank Bauer KA3HDO, Сергей Самбуров (Sergiej Samburow), RV3DR, Oliver Amend DG6BCE, Sławomir Szymanowski SQ3OOK, Rosalie White, K1STO, Jacek Gowin SQ5RJG, Andrzej Bojan SP8AB, Spike Rendchen SP9NJ, Paweł Olgierd SWFRA7 SQ3OOK Krystyna Dąbrowska, Piotr Skrzypczak SP2JMR, Jan Dąbrowski SP2JLR, Tadeusz Pamięta SP9HQJ, Kuba Witkowski, Magdalena Sosnowska, Radosław Chróścicki SP5ADX, a także wielu innych.

Jako koordynator tego wydarzenia jestem wdzięczny wszystkim osobom zaangażowanym w to przedsięwzięcie. Bardzo dziękuję za Wasz wolontariat i bez-dochodową pracę (pracę non-profit). Bardzo to doceniam. Po raz kolejny dziękujemy wszystkim osobom zaangażowanym z SIM w Kole, które od prawie 10 lat wspierają polskie wydarzenia promujące edukację poprzez ARISS i dają specjalne zniżki dla PZK na ten cel promocyjny. Podziękowania kierujemy również do ISS Fan Clubu (nie mylić z jakimś tworem o nazwie ISS Fan Club Poland, który nie jest związany z ISS Fan Club https://issfanclub.eu/) za promocję tego wydarzenia oraz za to, że z okazji tego przedsięwzięcia ustanowili też nagrodę dla tylko dla nasłuchowców (SWL).
Dziękuję PZK za wsparcie finansowe ze środków, które pierwotnie były przeznaczone na konferencję o ARISS w 2020 roku, a która nie odbyła się z powodu pandemii COVID-19. Środki te zgodnie z ustalonymi zasadami zostały przeznaczone na wydruk kart QSL dla polskich stacji klubowych PZK, a także na podziękowania w formie dyplomu oraz koszulek spersonalizowanych dla większości osób zaangażowanych. Dziękuję również osobom, które również dofinansowały to wydarzenie. To dzięki nim mogliśmy dokonać wydruku kart QSL dla pozostałych stacji polskich, oraz przygotować kilkanaście pamiątkowych spersonalizowanych koszulek polo ze znakiem okolicznościowym 3Z20ARISS. Koszty transportu nagród podziękowań zostały pokryte z funduszy zarówno PZK, jak i z innych źródeł.

Na koniec podkreślam, że bardzo doceniam wsparcie, jakiego ARISS udzieliło na to wydarzenie, a także to, że jego członkowie którzy pomogli w przygotowaniach do tego wydarzenia. Przypomnę, że jeśli ktoś chce wesprzeć działania ARISS, to zapraszam na stronę internetową: https://www.ariss.org/donate.html

Koordynator wydarzenia

Armand Budzianowski SP3QFE

4. Ekspedycja 66

Jesteśmy w trakcie trwania Misji: Ekspedycja-66 "Eksploracja Księżyca", która będzie trwać do końca tego roku czyli do 31.12.2021.

W tym czasie mamy możliwość odbierania obrazów telewizji Slow Scan (SSTV) przesyłanych z Międzynarodowej Stacji Kosmicznej na częstotliwości 145.800 MHz, gdzie załączam przykładowy obraz odebrany w dniu 28.12.2021

Ponadto nadmieniam, że każdy z nas może się ubiegać o oficjalną nagrodę ARISS SSTV Award, którą ja już otrzymałem.

73 Adam SQ9DHS

5. Józef Stankiewicz ps. Ziutek – konstruktor radiostacji wojennej

Na stronie https://um.warszawa.pl/-/odslonieto-tablice-pamiatkowa-jozefa-stankiewicza-ps-ziutek czytamy:

ODSŁONIĘTO TABLICĘ PAMIĄTKOWĄ JÓZEFA STANKIEWICZA PS. ZIUTEK

)

Autor: fot. Rafał Motyl

Na ścianie budynku przy ul. Ordynackiej 13 odsłonięto tablicę pamiątkową poświęconą genialnemu konstruktorowi – Józefowi Stankiewiczowi ps. Ziutek, który zginął dokładnie w tym miejscu w 1943 roku.

Działalność konspiracyjną rozpoczął już w październiku 1939 roku, kiedy Niemcy kazali warszawiakom, pod groźbą śmierci, oddawać aparaty radiowe. Zamontował więc odbiornik radiowy pod talerzem walizkowego adapteru. Wiadomości z alianckich audycji radiowych przekazywał rodzinie, a ci zaufanym znajomym. Taką drogą informacje rozchodziły się błyskawicznie – tak wspominała zasłużonego warszawiaka Renata Kaznowska, wiceprezydentka m.st. Warszawy.
Józef Stankiewicz miał w środowisku opinię zdolnego i doświadczonego konstruktora. Oficer Wojska Polskiego Stefan Korboński dowiedział się o nim i wiosną 1941 roku zaproponował mu zbudowanie radiostacji, która umożliwiłaby nawiązanie bezpośredniej łączności z Londynem. Po raz pierwszy udało się to 2 sierpnia 1941 roku, i jak podkreślał Korboński – radiostacja Ziutka działała bez zarzutu. Był to początek regularnych szyfrowanych połączeń radiostacji „Świt", później wspartych wiedzą wojskowych radiotelegrafistów.
Pod koniec 1941 roku Józef Stankiewicz skonstruował trzystuwatową radiostację, z której w przeddzień Bożego Narodzenia, nadana została pierwsza audycja przeznaczona dla Polaków w Anglii. Na aparatach konstrukcji Józefa Stankiewicza komórka radiowa Kierownictwa Walki Cywilnej pracowała do końca wojny.
„Ziutek" w czasie wojny naprawiał radiostacje dla działających w konspiracji organizacji wojskowych i cywilnych. Zapotrzebowanie na urządzenia radiowe było w tym czasie bardzo duże. Pracował całymi dniami organizując jednocześnie konspiracyjne dostawy części radiowych.

Józef Stankiewicz nie doczekał wolnej Polski. Poległ 9 maja 1943 r. przy ul. Ordynackiej 13 w starciu z niemieckim patrolem. Miał zaledwie 22 lata. Pośmiertnie został odznaczony Krzyżem Walecznych oraz Krzyżem Armii Krajowej.
W uroczystości odsłonięcia pamiątkowej tablicy wzięli udział: wiceprezydentka m.st. Warszawy – Renata Kaznowska, burmistrz dzielnicy Śródmieście – Aleksander Ferens, zastępcy burmistrza – Tomasz Bratek i Magdalena Wojciechowska, Jerzy Mindziukiewicz – wiceprezes Związku Powstańców Warszawskich oraz rodzina Józefa Stankiewicza, w tym córka – Józefa Stankiewicz-Botton.
Urząd m.st. Warszawy, pl. Bankowy 3/5, 00-950 Warszawa

Na stronie https://business.facebook.com/dz.srodmiescie/ czytamy:
„Przy ul. Ordynackiej 13 pojawiła się dziś tablica, upamiętniająca Józefa Stankiewicza ps. „Ziutek" - radiotelegrafistę i konstruktora pierwszej radiofonicznej stacji nadawczej Kierownictwa Walki Cywilnej. To dzięki jego wyjątkowemu talentowi, ale też niebywałej odwadze, możliwe było odnoszenie sukcesów łącznościowych.
Miejsce zawieszenia tablicy pamiątkowej nie jest przypadkowe. Właśnie przy ul. Ordynackiej 13 - 9 maja 1943 r. podczas strzelaniny - Józef Stankiewicz zginął. Pośmiertnie został odznaczony Krzyżem Walecznych oraz Krzyżem Armii Krajowej."

Obszerna informacja na temat działalności konspiracyjnej Józefa Stankiewicza znajduje się w książkach Stefana Korbońskiego, jego dowódcy:
- "W imieniu Rzeczypospolitej".
- "Polskie Państwo Podziemne".
- "Bohaterowie Państwa Podziemnego - jak ich znałem".
Krótkie informacje zawarte są również w książkach:
- Maciej Kwiatkowski "Polskie radio w konspiracji 1939-1944".
- Władysław Bartoszewski "Warszawski pierścień śmierci 1939-1944".

P.S.
Powyższą informację telefonicznie uzyskał Tadeusz SP9HQJ od córki Józefa Stankiewicza - Józefy Stankiewicz-Botton. Józef Stankiewicz był prawdopodobnie przedwojennym krótkofalowcem, ale nie zdołano ustalić jego znaku nadawczego. Może komuś się to uda. Skonstruowana przez Józefa Stankiewicza radiostacja była jako pierwsza wykorzystana do łączności radiowej z Londynem. Potem była radiostacja „Błyskawica" i „Burza".

Info. Tadeusz SP9HQJ

III. Sport

6. Wiadomości nie tylko DX-owe

6W - Senegal: Od 29 grudnia do 22 lutego Jacques F6HMJ będzie QRV jako 6W7/F6HMJ z Senegalu. QSL via znak domowy.

DL - Niemcy: Stacja klubowa DL0IMO nadaje pod znakiem okolicznościowym DR50BAWA z okazji 50-lecia systemu monitorowania pasm DARC https://www.intruder-monitoring.de/ , który powstał w 1972 roku na potrzeby IARU. QSL via biuro.

EI - Irlandia: Z okazji 90-lecia powstania Irlandzkiego Związku Krótkofalowców (Irish Radio Transmitters Society) nadaje staja okolicznościowa EI90IRTS. QSL via EI6AL.

F - Francja: F1PHB, F5BQU, F5TLZ, F6BGH i F8EFU będą QRV jako TM57HNY od 29 grudnia do 12 stycznia z okazji nowego roku. QSL via F-11734.

FS - Święty Marcin: David F8AAN od 1 do 20 stycznia będzie aktywny jako FS/F8AAN z Saint Martin NA-105.

G - Anglia: GB100BBC nadaje z okazji 100 rocznicy British Broadcasting Corporation tj. głównego brytyjskiego publicznego nadawcę radiowo-telewizyjnego. QSL przez biuro.

Z okazji 70 rocznicy wstąpienia na tron królowej Elżbiety II przez 2022 r. będą aktywne dwie stacje okolicznościowe GB8HRM i GB8PJE.

I - Włochy: Od stycznia 2022 roku usłyszymy stacje okolicznościowe II1WRTC, II2WRTC, II3WRTC, II4WRTC, II5WRTC, II6WRTC, II7WRTC, II8WRTC,

II9WRTC i II0WRTC, które promują zbliżające się od 6 - 11 lipca 2022 roku Mistrzostwa Świata (World Radiosport Team Championship).
Do zdobycia okolicznościowe certyfikaty https://www.wrtc2022.it/en/wrtc2022-award-19.asp

OX - Grenlandia: Nils SM3UQK do 4 stycznia przebywa na Grenlandii NA-018, skąd jest aktywny jako OX/SE3A. QSL via SM3UQK.

OZ - Dania: Królowa Małgorzata II wstąpiła na tron duński po śmierci ojca Fryderyka IX 14 stycznia 1972. Znakiem okolicznościowym OZ50Q obchodzony jest Złoty Jubileusz Królowej. W styczniu do zdobycia będzie szereg certyfikatów. Szczegóły https://www.qrz.com/db/OZ50Q

Stacja OZ50DDXG nadaje z okazji 50-lecia Danish DX Group, która powstała 27 maja 1972 r. QSL via OZ1ACB. Do zdobycia certyfikaty, których regulamin dostępny jest na stronie https://www.qrz.com/db/OZ50DDXG

PJ7 - Święty Marcin: Jeff VA3QSL od 4 stycznia do 6 lutego spędzi wakacje na Sint Maarten NA-105, skąd będzie aktywny jako PJ7/VA3QSL.

SP - Polska: Z okazji nowego, 2022 roku, uruchomiona została stacja okolicznościowa HF22NY. Za 4 QSO do pobrania okolicznościowy kalendarz. Szczegóły na qrz.com oraz http://hf22ny.org/

Na stronie https://www.qrz.com/db/hf9field opublikowano regulamin Field Day Award 2022.

UA0 - Rosja: Stacja okolicznościowa R075F będzie aktywna od 1 stycznia do 28 lutego z okazji 75 rocznicy oblast Sakhalin. QSL via LoTW.

UN - Kazachstan: Świętując nadjeście nowego roku 2022 stacje okolicznościowe UP2022HNY, UO2022HNY, UN2022HNY i UP2022SG przydzielają punkty do różnych dyplomów. Szczegóły https://hamlog.online/

W - USA: Klub Straight Key Century Club od 2 do 31 stycznia będzie QRV z okazji powstania klubu w 2006 roku. Aktywna będzie stacja okolicznościowa K3Y, która będzie łamana przez okręgi K3Y/0 do K3Y/9, oraz /KH6, /KL7 i /KP4. Szczegóły na https://skccgroup.com/k3y/k3y.php

Z3 - Macedonia: Michael DF8AN od 29 grudnia do 5 stycznia będzie aktywny jako Z38/DF8AN z Skopje. QSL via znak domowy.

Zawody 1-2 stycznia 2022 r.
AGCW HNY Contest http://alt.agcw.de/index.php/en/contests-and-cw-activities/happy-new-year-contest
WW PMC Contest http://www.s59dcd.si/index.php/sl/ww-pmc/ww-pmc-contest-rules
Orginal QRP Contest http://www.qrpcc.de/contestrules/oqrpr.html

W dniu 30 grudnia odbędą się ostatnie w tym roku zawody YOTA Contest https://www.ham-yota.com/contest/

Nowy Rok z Russian CW Club - RCWC. Od 30 grudnia do 5 stycznia członkowie przydzielają punkty do okolicznościowych dyplomów.
Szczegóły http://rcwc.ru/2802-regulations-on-the-days-of-activity-new-year-with-rcwc-2022.html

Zgłaszamy wyniki za 2021 rok do współzawodnictwa DX Marathon, które jest prowadzone przez CQ Magazine https://dxmarathon.com/

Mapy propagacji tropo http://aprs.mennolink.org/

"DREAM BIG AND DARE TO FAIL" to książka wydana przez Cezara Trifu VE3LYC, w której opisuje swoje wyprawy IOTA.
Książka zawiera 240 stron, pełny kolor, 516 ilustracji. Będzie dostępna do zakupu na początku stycznia, a zamówienia przyjmowane są przez PayPal.
Strona internetowa https://ve3lyc-book.weebly.com/ Wszelkie zapytania i wyrażenia można kierować do autora na ve3lyc@hotmail.com

2022 CONTEST UNIVERSITY odbędzie się 19 maja 2022 roku
https://www.contestuniversity.com/

Pozdrawiam Adam SQ9S

7. Ekspedycja Jacka SP5EAQ na Australe

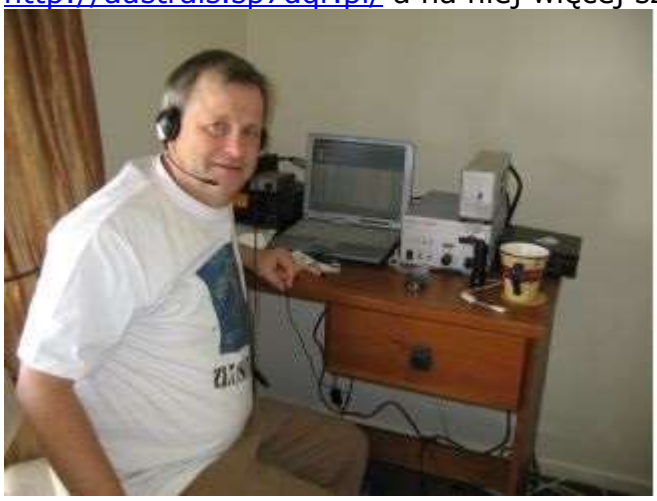
Poniżej trochę szczegółów o organizacji ekspedycji na Australe

Jacek napisał: Możesz to też traktować jako aplikację o dofinansowanie ze strony OT73, które zawsze było dla mnie hojne.*
Od ponad dwóch lat obywałem się bez planów ekspedycyjnych - to stanowczo za długo. Pierwszym impulsem był telefon od Marcina SP5ES, z którym byłem na mojej ostatniej ekspedycji na Norfolk. Zapytał mnie o plany, sondując przy okazji czy byłbym chętny pojechać razem z nim na Spratly. Powiedziałem Marcinowi, że pandemia wprowadza wiele niewiadomych i nie stać mnie na podjęcie takiego ryzyka. Coś jednak drgnęło i po kilku dniach zacząłem sprawdzać jak wygląda Timor Wschodni (Leste), który także jest odrębnym i poszukiwanym podmiotem DXCC. Spratly byłoby koszmarnie kosztowne (tylko jedno miejsce w archipelagu uważane jest za bezpieczne a specjalizuje się wyłącznie w organizacji pobytów pod kątem nurkowania). Timor (chociaż owiany historią zamachów terrorystycznych) wydał mi się obecnie całkiem bezpieczny, sporo tańszy
a w dodatku wygodny - transport poprzez Bali (Indonezja) byłby niezbyt trudny organizacyjnie. Szybko jednak okazało się, że z powodów pandemicznych Indonezja jest zamknięta dla turystyki. Odpuściłem więc sprawę. Kilka tygodni później kolega w pracy powiedział, że jedzie żeglować na Bora-Bora (Polinezja Francuska). Próbowałem go od tego odwieść, ale pojechał i wrócił zachwycony. Problemów pandemicznych, poza koniecznością testów i niewpuszczenia jachtu

na jedną z wysp, nie było. To dało mi do myślenia. Wprawdzie Polinezja Francuska to jedno z najbardziej kosztownych miejsc na dxpedycję, ale żyje z turystów - jest więc bardzo zainteresowane tym, żeby nie wprowadzać całkowitej izolacji w związku z pandemią. No i Australe (archipelag będący jej częścią) są na czterdziestym miejscu jeśli chodzi o zapotrzebowanie w Europie na QSO na SSB, a więc wydawało się, że być może będzie łatwiej z dofinansowaniem.

Wydawało się, bo już pierwszy potencjalny sponsor odpisał, że w związku z Omikronem ekspedycja stanowi zbyt duże ryzyko a QSO na SSB z Europą będzie bardzo trudne (o tym zresztą wiem, dlatego chcę się tam wybrać). Najpierw skontaktowałem się z krótkofalowcem, który całkiem niedawno nadawał z Polinezji na 6 metrach. Miałem szczęście, bo natychmiast zasypał mnie użytecznymi informacjami. Okazało się, że kiedyś pomagałem mu znaleźć odpowiednie miejsce na ekspedycję EME na Fiji (o czym zupełnie zapomniałem).
Między innymi dał mi kontakty (poprzez Facebooka) do miejscowych ludzi na Rimatara (mała wysepka wulkaniczna na Australach). Po kilku sesjach na Messengerze (na szczęście daję sobie radę po francusku) dostałem propozycję wynajęcia malutkiego domku z jednym pokoikiem, za pieniądze znacząco mniejsze niż za pośrednictwem jakiejkolwiek agencji turystycznej (co na Polinezji jest praktycznie obowiązkowe). Jest to wprawdzie wciąż koszmarnie duży wydatek, no i małe pojedyncze pomieszczenie wyklucza udział drugiej osoby, ale zdecydowałem się. Nie stać mnie było jednak na pełne wyżywienie, ale cóż. Zaplanowałem pobyt na cały miesiąc obejmujący CQ WW WPX Contest SSB. Pracuję wyłącznie emisją SSB a ostatnio wielu moich przyjaciół skarżyło się, że większość DXów przeniosła się na emisje cyfrowe i zapotrzebowanie na SSB wielokrotnie wzrosło. Zabukowałem więc miejsce i zająłem się biletami lotniczymi (także drogimi, gdyż standardowe bilety nie obejmują większego bagażu, który jest koniecznością). Było to kłopotliwe, bo na wyspę dolatuje mniejszy samolot dowożąc miejscowych z i do Papeete (stolica Polinezji Francuskiej) ale tylko z małym bagażem. Musiałem więc przeorganizować transport bagażu i gdy okazało się to potencjalnie możliwe, kupiłem bilety. Potem wystąpiłem o okolicznościowy znak na zawody TX5AQ (do pracy poza zawodami mogłem korzystać z licencji CEPT używając FO/SP5EAQ). Następnie zacząłem się ubiegać o zezwolenie na przywóz sprzętu radiowego (K3

nie ma znaczka CE, a więc znowu problemy). Biorąc pod uwagę francuską biurokrację, przedsięwzięcie (on-line) nie było łatwe. Natomiast dzięki przyjaciołom inne sprawy potoczyły się szybko. Mirek SP5ENA pożyczył ICOMa IC-7100 jako backup w razie awarii mojego K3, Tomek SP5UAF zaprojektował loga wyprawy (aż 2!) i zajął się projektem kart, Marek SP7DQR zgodził się być QSL managerem, no a Waldek SP7GXP obiecał skonstruować nową wersję wielopasmowego verticala znacznie lżejszą od obecnych. Najważniejsze, to mieć przyjaciół. Jeśli jeszcze trochę sponsorów się znajdzie, będzie lżej. Pozostaje największe ryzyko, czyli pandemia - wszystko może rozsypać się z powodu pandemicznych ograniczeń. Mogę po prostu nie dojechać (albo co gorsza nie wrócić😁). Ale to się okaże dopiero za dwa miesiące albo trochę później. Dla zainteresowanych strona wyprawy (znów dzięki SP7DQR) to http://australs.sp7dqr.pl/ a na niej więcej szczegółów.



Jacek SP5EAQ przy swojej stacji ekspedycyjnej.
*Ekspedycja jest dotowana przez: PZK, VOT PZK (OT73), kluby HF5L, SP5PBE i sponsorów indywidualnych. Loga sponsorów (lub znaki) są (lub będą) wykazane na portalu ekspedycji i rewersie karty QSL ekspedycji. Współpraca jest bilateralna.

Info: SP5ELA (na podstawie materiału dostarczonego przez SP5EAQ)

8. Z CQWW stacja TK0CW - wesoła drużyna!

Nadesłane: K1CC (Lista SN0HQ)

9. UKF – zawody

W najbliższym czasie:

AGCW VHF/UHF Contest – *noworoczne zawody telegraficzne UKF w paśmie 144 i 432 MHz organizowane przez niemieckich krótkofalowców* ***1 stycznia 2022****, w godz. 14:00 - 18:00 UTC. Zawody o wieloletniej tradycji; Koledzy z DL serdecznie zapraszają polskich sympatyków CW do jak najliczniejszego udziału.*

Regulamin:

https://www.agcw.de/index.php/en/contests-and-cw-activities/vhf-uhf-contest albo http://alt.agcw.de/index.php/en/contests-and-cw-activities/vhf-uhf-contest

SPAC–144 MHz *– zawody aktywności UKF – wtorek, 4 stycznia 2022, godz. 18:00-22:00 UTC*

Regulamin:

https://pk-ukf.pl/wp-content/uploads/2020/05/SPAC_regulamin_PL.pdf

Zawody ***SPAC*** *prowadzi i rozlicza* ***Stowarzyszenie Polski Klub UKF.***

Dzienniki w formacie EDI prosimy wysyłać na adres**:** http://spac.pk-ukf.pl/

VHF-FT8 Activity – *zawody aktywności FT8 – 144 MHz, środa 5 stycznia 2022, godz. 17:00-21:00 UTC, regulamin: https://www.ft8activity.eu/index.php/en/*

Stanisław SQ2EEQ

==========

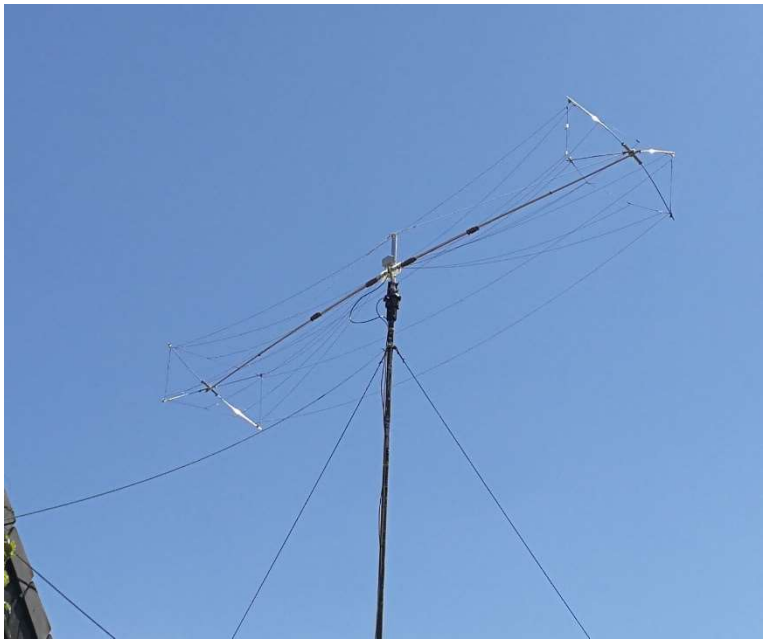
IV. Technika

10. Anteny opracowywane przez Jacka SP3L Ciąg dalszy..

Autor opracowań antenowych – Jacek SP3L (ex SP3LFV)

Ant 1
Antena pionowa tylko nieco dłuższa niż ćwierć fali z przeciwwagami w pobliżu radiatora. Dedykowana na sytuacje, kiedy nie ma miejsca na rozciągnięcie przeciwwag ani systemu uziomów promienistych.

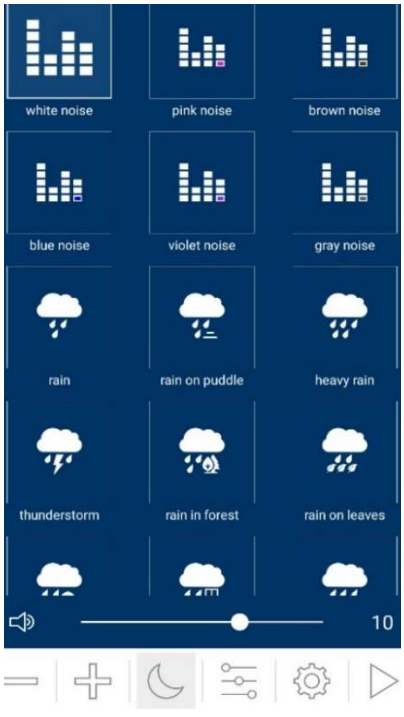
Ant 2
Antena „Kocie wąsy” pokrywa w sposób ciągły zakres 14-30 MHz z niskim SWR i dwukierunkową charakterystyką promieniowania. Zysk nieco większy niż dipol półfalowy. Opisana w Świecie Radio nr 1/2017. Antena zdobyła 2 miejsce w konkursie zorganizowanym przez miesięcznik QST w 2018 roku.



Ant 3. Doublet wielopętlowy - kompaktowa antena pokrywająca w sposób ciągły zakres 14-30 MHz z niskim SWR i dwukierunkową charakterystyką promieniowania. Tylko 6,6 m długości. Lekka, ale wytrzymała. Zysk zbliżony do dipola.

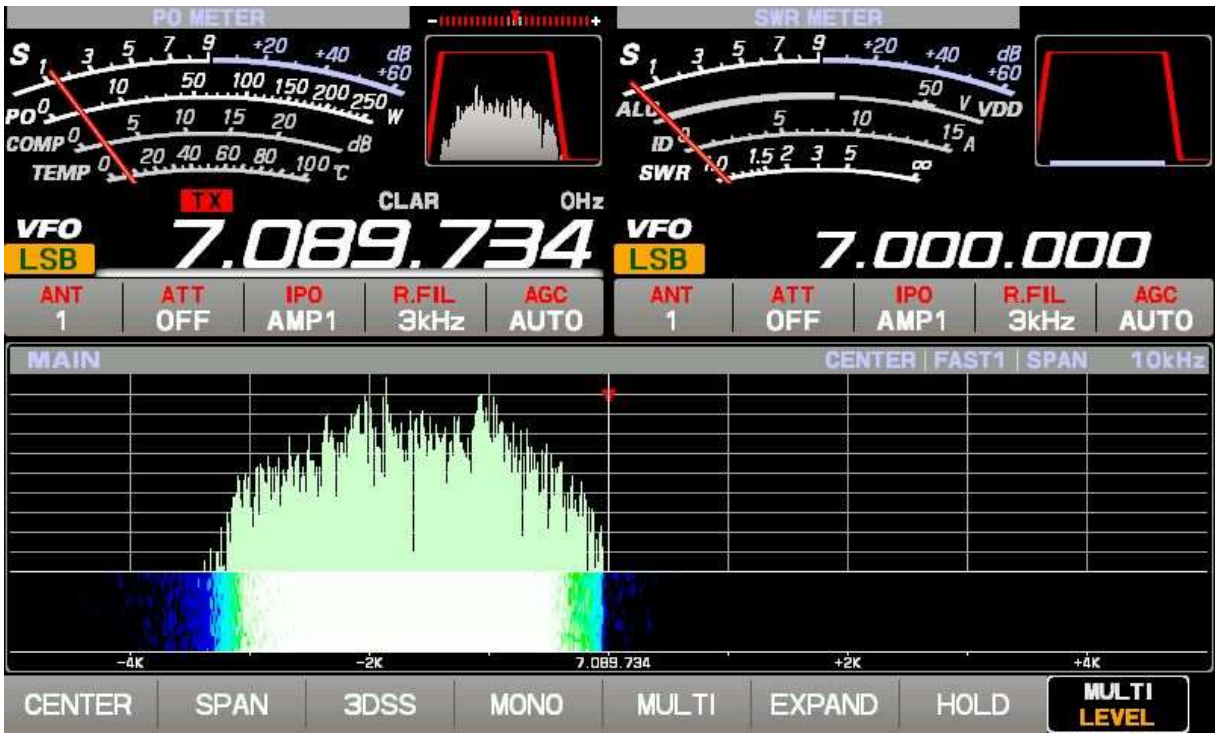
Info: SP5ELA. Materiał dostarczony przez Jacka SP3L.

11. Pomiary toru nadawczego transceivera metodą szumową



Metody szumowe są często wykorzystywane w pomiarach systemów transmisyjnych (np. metoda NPR badania odporności rx-ów). Omawiany przypadek pomiaru, to taki, gdzie do modelowania i kontroli toru nadajnika wykorzystywany jest sygnał szumu dostarczany do mikrofonu TRX-a. Zbliżamy źródło dźwięku (szumu), którym jest smartfon z zainstalowanym oprogramowaniem generatora szumu* do mikrofonu na optymalną odległość (kilka centymetrów). Badamy charakterystykę całego toru nadajnika TRX-a od mikrofonu, poprzez wzmacniacz mikrofonowy, EQ** mikrofonowy, układ kształtowania pasma toru nadajnika, EQ toru TRX-a, modulator, i aż do stopnia mocy. TRX pracuje ze zredukowaną mocą wyjściową (5W) na sztuczne obciążenie. Sygnał RF obserwujemy za analizatorze zewnętrznym lub wbudowanym w TRX, w zależności od sytuacji.

Pomiary tego typu bazują na pewnych uproszczeniach założeń. Interesuje nas pasmo akustyczne od 0Hz – 4000Hz.
Przetwornik smartfona symulujący źródło sygnału szumu służy „normalnie” do komunikacji werbalnej i do przenoszenia ludzkiego głosu (czasem muzyki). Przyjęto założenie, że przenosi pasmo akustyczne 100-6000Hz. Charakterystyka przetwornika (głośniczka) jest nieznana.

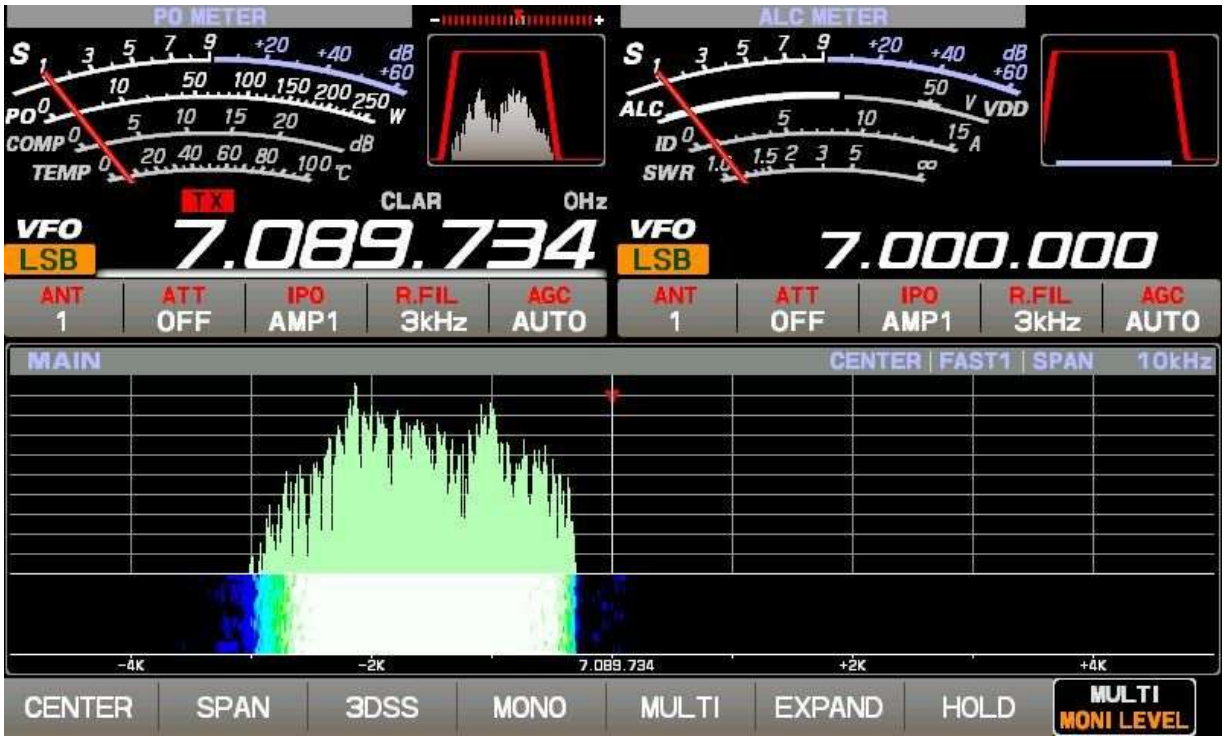


Charakterystyka przejściowa toru TRX-a. Moc wyjściowa ograniczona do 5W. Teoretyczne pasmo przenoszenia toru 200-2800 Hz. 5db/działkę na ekranie.

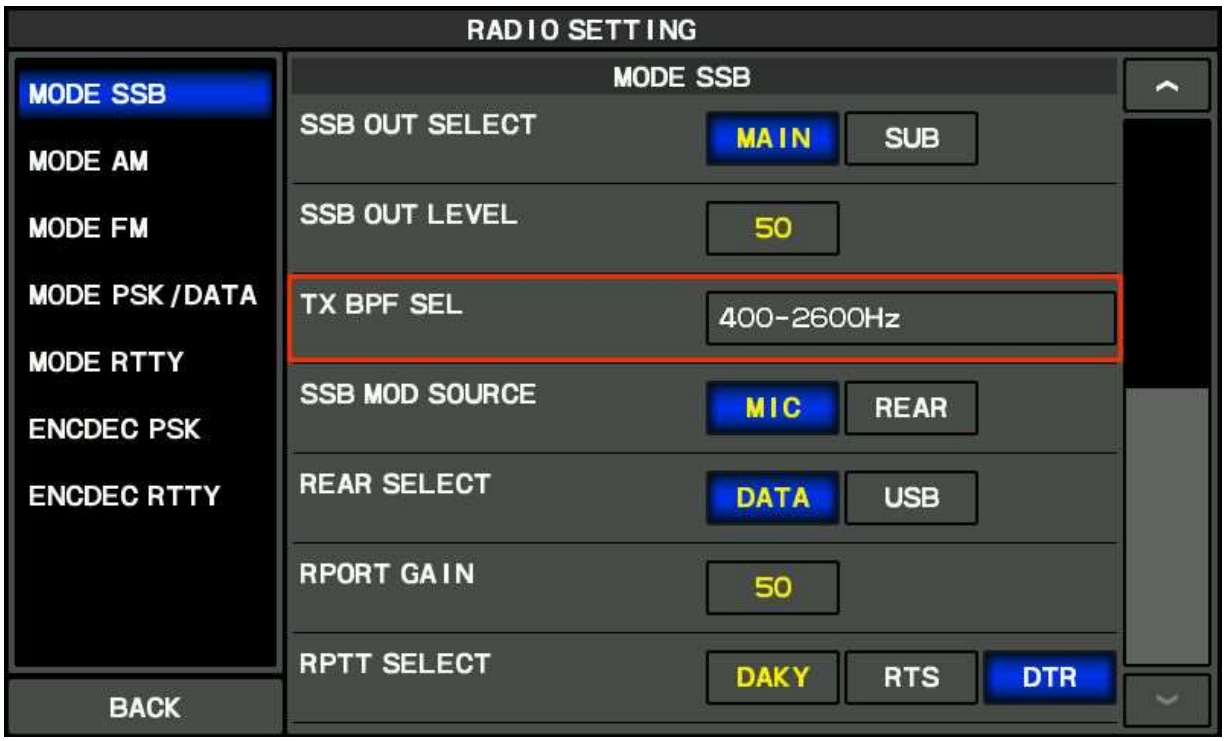
Realna charakterystyka toru TRX-a odbiega od charakterystyki teoretycznej - idealizowanej. Należy pamiętać, że sygnał akustyczny i w efekcie sygnał RF wyjściowy z definicji jest zdegradowany w pobliżu „ZERA” częstotliwości i powyżej 3/4/5KHz. Nie jest to „prostokąt”. Jak widać na powyższym ekranie sygnał szumu ma wypełnienie w całym paśmie z oczywistym spadkiem charakterystyki 0-200Hz oraz 2800Hz i powyżej. Kształtowanie widmowej charakterystyki sygnału SSB jest odrębnym i złożonym zagadnieniem.

Kolokwialnie rzecz ujmując – zamiast gwizdać do mikrofonu, liczyć lub „wyć”, za pomocą generatora szumów można szybko sprawdzić poziom wysterowania, działania systemu ALC i poziom mocy wyjściowej TRX-a.

Należy pamiętać, że sygnał jednowstęgowy nigdy nie osiągnie stałego poziomu mocy maksymalnej transceivera. Zawsze jest mniejszy od „1” (<1), gdzie „1”, to moc maksymalna urządzenia. Moc nominalna jest tylko wtedy pokazywana, jeżeli np. reflektometr ma opcją PEP (moc szczytowa).

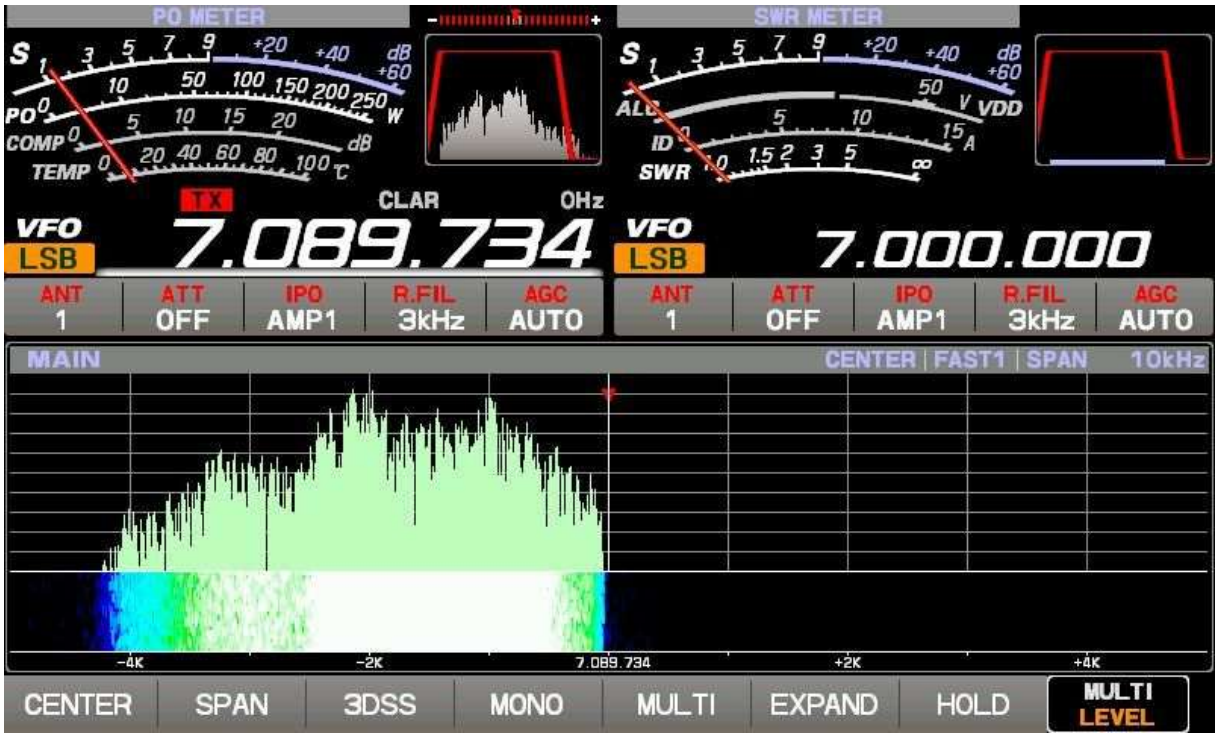


Ograniczenie charakterystyki sygnału do pasma 400-2600Hz. Wyraźnie widoczne stłumienie częstotliwości pasma akustycznego od 0-400Hz.



Odpowiadające powyższemu obrazowi ustawienia pasma TX BPF.

„Zestaw" pomiarowy: smartfon, mikrofon, TRX. Widoczny ekran TRX-a z sygnałem wyjściowym RF.



Przykład ustawień sygnału TTBF. (ESSB). Wyraźnie widać pasmo przenoszonego sygnału do 4000Hz. Widać również, że „góra" jest nieco obcięta. Ale widmo jest 4KHz. Skalowanie 5dB/działkę ekranu.

*Aplikacja na Androida (APK). White Noise, wersja 1.35 jest bezpłatna.
**EQ – equalizer *korektor charakterystyki)

Autor tego opracowania dziękuje Marcinowi SP5IOU za inspirację!

Zygi SP5ELA

V. Informatyka i oprogramowanie

12. Logger32 i CW Machine

Wszelkie podejmowane próby konfiguracji modułu „CW Machine” w opcji „software keying” nic nie dawały do tej pory. Nigdy przez ostatnie 15 lat nie udało mi się tego uruchomić i chyba nikomu innemu również. Wdałem się tylko w lekkie awantury na liście Loggera32 z kowbojami.

Od wersji Logger32 V4 zaczął działać terminal software CW (CW Machine) w Logger32.

Przykładowo jest używana konfiguracja po kablu USB – TRX FT-991. Sterowniki Yaesu (de facto Silicon Labs CP26xx) generujące porty COM standard i enhanced. Kluczowanie TRX-a z CW Machine, to tzw. „software keying”.
W czasie prowadzenia łączności telegraficznych z lokalizacji SP5ELA/8 (Ryki) nadawałem częściowo manipulatorem ręcznym i częściowo z klawiatury komputera z programu Logger32, w zawodach WHUPW z programu N1MM+.
W CW Machine można kształtować sygnał telegraficzny, przykładowo stosunek kropki-kreski-spacji. Przy pewnych ustawieniach i sprytnym używaniu, wygląda to na nadawanie na kluczu ręcznym lub tzw. „bugu” (uwaga SP3CW).

73 Zygi SP5ELA/8

VI. Prawo i przepisy

13. Ministerstwo Cyfryzacji. Pismo DRC do PZK*

MINISTER CYFRYZACJI
Mateusz Morawiecki
DRC.WL.06110.53.2021

Szanowni Państwo,

zgodnie z § 36 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów, w załączeniu przesyłam pismo Ministra Cyfryzacji oraz ***projekt rozporządzenia Rady Ministrów w sprawie wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa (RD472)***
z uprzejmą prośbą
o przedstawienie stanowiska (w tym w wersji edytowalnej) do projektu **w terminie do 7 dni od dnia doręczenia niniejszego pisma**.

Z poważaniem,

Departament Regulacji Cyfrowych

*Dokumenty są załącznikami do Komunikatu PZK 52/2021. PZK wg rozdzielnika MC jest jedną ze społecznych organizacji - konsultantów. Warto przynajmniej wiedzieć nad czym MC pracuje i jakie będą tego konsekwencje.

VII. Humor w PZK

14. Humor telegrafisty

Autor nieznany, oczywiście z Internetu.

VIII. Propagacja fal radiowych

15. Prognoza NOAA na 27 dni

```
:Product: 27-day Space Weather Outlook Table 27DO.txt
:Issued: 2021 Dec 27 0409 UTC
# Prepared by the US Dept. of Commerce, NOAA, Space Weather Prediction Center
# Product description and SWPC contact on the Web
# https://www.swpc.noaa.gov/content/subscription-services
#
#      27-day Space Weather Outlook Table
#                Issued 2021-12-27
#
#   UTC      Radio Flux   Planetary   Largest
#  Date       10.7 cm      A Index    Kp Index
2021 Dec 27     125           5          2
2021 Dec 28     125          12          4
2021 Dec 29     122          12          4
2021 Dec 30     120           8          3
2021 Dec 31     120           8          3
2022 Jan 01     115           8          3
2022 Jan 02     110           8          3
2022 Jan 03     100           5          2
2022 Jan 04      95           5          2
2022 Jan 05      90           5          2
2022 Jan 06      90           5          2
2022 Jan 07      92           5          2
2022 Jan 08     100           5          2
2022 Jan 09     105           5          2
2022 Jan 10     110           5          2
2022 Jan 11     115          10          3
2022 Jan 12     115          10          3
2022 Jan 13     115           5          2
2022 Jan 14     118           5          2
2022 Jan 15     118           8          3
2022 Jan 16     122          12          4
2022 Jan 17     128           8          3
2022 Jan 18     130           8          3
2022 Jan 19     130           5          2
2022 Jan 20     125           5          2
2022 Jan 21     125           5          2
2022 Jan 22     120           5          2
```

Info: SP5ELA

XI. Silent keys

SP3HRQ SK

Dnia 18 grudnia 2021 r. zmarł w wieku 74 lat nasz kolega **Tadeusz Kukuła SP3HRQ**. Tadeusz SP3HRQ od 1974 do 2008 roku był kierownikiem Radioklubu LOK SP3KCL w Gorzowie Wielkopolskim. Prowadząc sekcję łączności i w późniejszym czasie też sekcję modelarstwa wychował wielu znanych krótkofalowców, którzy są znakomitymi DX-menami i byli też zdobywcami wielu głównych nagród w telegrafii szybkiej.
Tadeuszu, zapisałeś się dobrze w historii krótkofalarstwa polskiego. Będzie nam Ciebie brakowało - Spoczywaj w pokoju.

Mietek SP3CMX

*Pogrzeb odbył się 23 grudnia 2021 na Cmentarzu Głównym w Gorzowie Wielkopolskim, przy ulicy Żwirowej.

SP2BG SK

W dniu 23.12.2021 zmarł przegrywając walkę z rakiem nasz serdeczny kolega, krótkofalowiec i dziennikarz **Bogusław Matuszkiewicz SP2BG**.
Wyrazy współczucia dla rodziny od kolegów z Środkowopomorskiego Oddziału PZK.

Cześć Jego pamięci!

Msza pożegnalna dla przyjaciół i znajomych w środę 29 grudnia o godzinie 9:00 w kościele Mariackim w Słupsku. Ceremonia pogrzebowa w dniu 30 grudnia
o godz. 12:00 na cmentarzu komunalnym Konin/Morzysław.

Jurek SQ2NIA

SQ6NSM SK

W dniu 13 grudnia 2021 r. zmarł nagle w wieku 75 lat nasz serdeczny przyjaciel **Edward Martyniuk SQ6NSM**, wieloletni członek PZK i Klubu SP6PZG w Świdnicy. Jego pogrzeb odbył się 23 grudnia 2021 r. na cmentarzu komunalnym w Świdnicy przy ul. Słowiańskiej.

Niech odpoczywa w Pokoju Wiecznym!

Info: Franciszek SP6GTN

Redakcja Komunikatów PZK dziękuje za przesłane materiały: Adamowi SQ9S, Stanisławowi SQ2EEQ, Mirkowi SP5GNI, Tadeuszowi SP9HQJ, Ryszardowi K1CC, Mieczysławowi SP3CMX, Armandowi SP2QFE, Jackowi SP3L, Adamowi SQ9DHS, Tadeuszowi SP9HQJ, Jurkowi SQ2NIA, Franciszkowi SP6GTN. Wykorzystano materiał z MC.

Informujemy, że Prezydium ZG PZK podjęło decyzję, aby wszyscy członkowie PZK zarejestrowani w bazie systemu OSEC otrzymywali Komunikat PZK „z urzędu", jako tzw. wartość dodaną. Komunikaty są od lat robione i nadawane w paśmie 80m sporym wysiłkiem osób będących w składzie Redakcji.

Jednocześnie Redakcja Komunikatu prosi o niewysyłanie na adres dystrybucyjny odpowiedzi i listów. Prosimy je kierować na indywidualne adresy e-mail członków Redakcji.

*Wszyscy Ci, którzy otrzymali Komunikat PZK, są już prenumeratorami Komunikatu (jest to logiczne, skoro go dostali) i nie ma potrzeby zapisywania się na listę dystrybucyjną drugi raz.

Materiały do **Komunikatu PZK** na kolejną środę powinny być przesłane nie później niż do wtorku, godz. 15:00. Materiały prosimy nadsyłać jednocześnie na adresy: **sp2jmr@pzk.org.pl**, **sp5ela@rf.pl**. W przypadku przesłania ich później mogą znaleźć się w następnym środowym komunikacie czyli za tydzień.
Teksty wymagające autoryzacji przed publikacją powinny być dostarczone przynajmniej 24 godziny wcześniej, czyli do poniedziałku, godz. 15:00.

Uwaga! Dostarczane do publikacji zdjęcia muszą mieć opisy oraz informację dotyczącą praw autorskich. W przypadku wizerunku osób małoletnich wymagana jest zgoda opiekunów ustawowych. Materiał fotograficzny należy dostarczać w postaci plików graficznych niezależnych od opisu tekstowego (osobne pliki jpg, png, niezagnieżdżone w strukturze tekstu), zdjęcia muszą być opisane.

Redakcja Komunikatu PZK zastrzega sobie prawo do dokonywania skrótów i korekt nadsyłanego materiału, także prawo do dokonywania w nadesłanych materiałach zmian tytułów, skrótów, poprawek stylistyczno-językowych oraz do usuwania usterek innego typu (np. terminologicznych lub dotyczących warstwy dokumentacyjnej), także do odrzucenia artykułu bez podania przyczyny.

Nie będą przyjmowane teksty nie spełniające podstawowych wymogów poprawności językowej.

Komunikaty PZK są nadawane w każdą środę o godzinie 18:00 czasu lokalnego na częstotliwości 3702,5 KHz +/- QRM, a materiał w nich zawarty jest wykorzystywany przez Redakcję Krótkofalowca Polskiego.

Redakcja Komunikatów PZK:

Piotr SP2JMR, Zygi SP5ELA i Jurek SP3SLU - także nadający komunikaty środowe.

***Motto Redakcji**

Odpowiedzialność za słowo jest ważnym etycznie wymaganiem odnoszącym się do człowieka, szczególnie kiedy występuje w przestrzeni publicznej i także w stowarzyszeniu. Służba prawdzie jest zatem nie tylko słusznym oczekiwaniem od Władz PZK i osób funkcyjnych ze strony wszystkich członków i niezrzeszonych radioamatorów, ale i jej moralnym obowiązkiem. Dotyczy to również Redakcji Komunikatów PZK.

W nawiązaniu do tej zasady informujemy, że Redakcja Komunikatów PZK dokłada wszelkich starań, aby ww. kryteria zostały spełnione. Otrzymywany materiał „z terenu" często jest obarczony błędami, zawiera pewne nieścisłości. Korekty materiału wymagane są w prawie każdym cośrodowym wydaniu Komunikatu PZK.

Piotr SP2JMR od KZD PZK w Kołobrzegu w 2000 roku, kiedy został wybrany Prezesem PZK rozpoczął wydawanie Komunikatu PZK (nazywanego wcześniej „Komunikatem sekretariatu ZG PZK"). Od 2009 roku do redakcji dołączył Zygmunt SP5ELA, a od roku 2013 Jurek SP3SLU nadający komunikaty przez radio na 3702.5 KHz o godz. 18-tej z lokalizacji Mariantów).

Redakcja Komunikatów PZK

UWAGA! Komunikaty środowe PZK – subskrypcja

Komunikaty PZK (środowe), wcześniej tzw. Komunikaty sekretariatu ZG PZK są wysyłane pocztą elektroniczną w każdą środę w ramach subskrypcji (e-mail) do osób zainteresowanych wiadomościami organizacyjnymi Polskiego Związku Krótkofalowców oraz informacjami dot. innych podmiotów, ale związanymi z krótkofalarstwem. Do roku 2018 adresy e-mail subskrybentów (około 400) dopisywał administrator. Od marca 2018 r. subskrypcja komunikatów została zautomatyzowana.

Aby otrzymywać Komunikat PZK (środowy), należy wysłać wiadomość (e-mail) na adres:

komunikat-pzk@pzk.org.pl z tekstem "subscribe" w temacie wiadomości (subscribe - bez apostrofów). Aby zrezygnować z subskrypcji należy wysłać wiadomość z tekstem "unsubscribe"

w temacie (unsubscribe - bez apostrofów).

Załącznik: MC – DRC

MINISTER CYFRYZACJI

Mateusz Morawiecki

DRC.WL.06110.53.2021

wg rozdzielnika

Szanowni Państwo,

zgodnie z § 36 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r.
– Regulamin pracy Rady Ministrów, uprzejmie informuję, że w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny udostępniony został ***projekt rozporządzenia Rady Ministrów w sprawie wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa (RD472)***.

Mając na uwadze powyższe zwracam się z uprzejmą prośbą o przedstawienie stanowiska (w tym w wersji edytowalnej) do projektu **w terminie do 7 dni od dnia doręczenia niniejszego pisma**. Stanowiska proszę przekazywać również na adres: sekretariat.drc@mc.gov.pl.

Jednocześnie uprzejmie informuję, że brak stanowiska w wyznaczonym terminie potraktowany zostanie, jako rezygnacja z przedstawienia stanowiska.

Skrócony termin na zaopiniowanie projektu wynika z konieczności wykonania upoważnienia zawartego w art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. *o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa* (Dz. U. poz. 2333), które wchodzi w życie w dniu 1 stycznia 2022 r. Wskazana ustawa wprowadziła świadczenie teleinformatyczne, które umożliwi utrzymanie i pozyskanie wykwalifikowanych specjalistów z zakresu cyberbezpieczeństwa, co jest niezwykle istotne ze względu na wzrastającą liczbę incydentów oraz pojawiające się nowe zagrożenia w tym obszarze. Projektowane rozporządzenie określa w załączniku m.in.: zadania, za których wykonywanie będzie mogło zostać przyznane świadczenie teleinformatyczne (np. analiza szkodliwego oprogramowania), doświadczenie zawodowe w realizacji zadań w zakresie cyberbezpieczeństwa oraz przedziały kwotowe wysokości świadczenia teleinformatycznego.

Projektowane rozporządzenie nie generuje nowych kosztów dla budżetu, ponieważ te zostały przewidziane we wspomnianej ustawie.

Z poważaniem

z up. Janusz Cieszyński

Sekretarz Stanu

w Kancelarii Prezesa Rady Ministrów

/podpisano kwalifikowanym podpisem elektronicznym/

Otrzymują:

1) Amercian Chamber of Commerce in Poland;
2) Federacja Konsumentów;
3) Busines Centre Club;
4) Fundacja im. Stefana Batorego;
5) Fundacja Bezpieczna Przestrzeń;
6) Fundacja Moje Państwo;
7) Fundacja Instytut Mikromakro;
8) Fundacja MY Pacjenci;
9) Fundacja Nowoczesna Polska;
10) Fundacja Panoptykon;
11) Fundacja Projekt: Polska;
12) Stowarzyszenie „Archiwizjoner”;
13) Fundacja im. Kazimierza Pułaskiego;
14) Związek Pracodawców Branży Internetowej IAB Polska;
15) Klaster #CyberMadeInPoland;
16) Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego UW;
17) Stowarzyszenie ISACA;
18) Izba Gospodarki Elektronicznej;
19) Konfederacja Lewiatan;
20) Krajowa Izba Gospodarcza;
21) Krajowa Izba Gospodarki Cyfrowej;
22) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
23) Krajowa Izba Gospodarki Morskiej;
24) Krajowa Izba Komunikacji Ethernetowej;
25) Krajowa Izba Rozliczeniowa S.A.;
26) Krajowe Stowarzyszenie Ochrony Informacji Niejawnych;
27) Naczelna Organizacja Techniczna;
28) Naczelna Rada Zrzeszeń Handlu i Usług;
29) Ogólnopolskie Porozumienie Organizacji Radioamatorskich;
30) Polskie Górnictwo Naftowe i Gazownictwo;
31) Polskie Koleje Państwowe S.A.;
32) PKP TELKOL sp. z o.o.;
33) Polska Federacja Szpitali;
34) Polska Izba Handlu;
35) Polska Izba Informatyki i Telekomunikacji;
36) Polska Izba Komunikacji Elektronicznej;
37) Polska Izba Producentów Urządzeń i Usług na Rzecz Kolei;
38) Polska Izba Radiodyfuzji Cyfrowej;
39) Polska Organizacja Handlu i Dystrybucji;
40) Polska Organizacja Niebankowych Instytucji Płatności;
41) Polska Rada Biznesu;
42) Polska Wytwórnia Papierów Wartościowych;
43) Polski Związek Krótkofalowców;
44) Polski Związek Pracodawców Przemysłu Farmaceutycznego;
45) Polskie Związek Przemysłu Motoryzacyjnego;
46) Polskie Centrum Badań i Certyfikacji S.A.;
47) Polskie Stowarzyszenie Marketingu SMB;
48) Polskie Towarzystwo Informatyczne;

49) SABI – stowarzyszenie inspektorów ochrony danych;
50) Stowarzyszenie Inżynierów Telekomunikacji;
51) Sieć Obywatelska Watchdog Polska;
52) Towarzystwo Gospodarcze Polskie Elektrownie;
53) Związek Banków Polskich;
54) Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego – ZIPSEE Cyfrowa Polska;
55) Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM;
56) Związek Pracodawców Mediów Publicznych;
57) Związek Przedsiębiorców i Pracodawców;
58) Związek Telewizji Kablowych w Polsce – Izba Gospodarcza.

PROJEKT Z DNIA 27 GRUDNIA 2021 R.

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia .....

w sprawie wysokości świadczenia teleinformatycznego osób realizujących zadania
z zakresu cyberbezpieczeństwa

Na podstawie art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 2333) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) szczegółowe zadania z zakresu cyberbezpieczeństwa i podział ich na grupy;
2) doświadczenie zawodowe lub wymóg posiadania specjalistycznej wiedzy z zakresu cyberbezpieczeństwa wymagane do realizacji zadań z poszczególnych grup;
3) przedziały kwotowe wysokości świadczenia teleinformatycznego w związku z podziałem zadań z zakresu cyberbezpieczeństwa na grupy, o których mowa w pkt 1.

§ 2. Ustala się tabelę szczegółowych zadań z zakresu cyberbezpieczeństwa oraz doświadczenia zawodowego lub posiadania specjalistycznej wiedzy w zakresie cyberbezpieczeństwa, a także przedziały kwotowe wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa, stanowiącą załącznik do rozporządzenia.

§ 3. Rozporządzenie wchodzi w życie po upływie 5 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

Za zgodność pod względem prawnym,

legislacyjnym i redakcyjnym

Michał Frączkiewicz

Dyrektor Departamentu Prawnego

w Kancelarii Prezesa Rady Ministrów

Załącznik do rozporządzenia Rady Ministrów z dnia……(poz. …)

Tabela szczegółowych zadań z zakresu cyberbezpieczeństwa oraz doświadczenia zawodowego lub posiadania specjalistycznej wiedzy w zakresie cyberbezpieczeństwa a także przedziały kwotowe wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa

Lp.	Doświadczenie zawodowe w realizacji zadań w zakresie cyberbezpieczeństwa, w latach	Przedziały kwotowe wysokości świadczenia teleinformatycznego	Szczegółowe zadania z zakresu cyberbezpieczeństwa	Wymóg posiadania specjalistycznej wiedzy w zakresie cyberbezpieczeństwa, o której mowa w poniższych dokumentach
1.	do 3 lat	12000	• Analiza szkodliwego oprogramowania • Badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania • Ocena bezpieczeństwa systemów IT – w tym testy penetracyjne i audyty bezpieczeństwa • Prowadzenie specjalistycznych analiz cyberbezpieczeństwa i wykrywanie nowych podatności • Rozwijanie specjalistycznych narzędzi technicznych wspomagających realizację zadań z obszaru cyberbezpieczeństwa	CASP+, CCFE, CEH, CEH Master, CPENT, CSSLP, CHFI, CMFE, CPT, eCDFP, eCMAP, CISSP, GASF, GAWN, GCCC, GCDA, GCFA, GCPN, GCTI, GNFA, GPEN, GREM, GREM, GSAF, GSNA, GMOB, GSSP, GWAPT, GWEB, GXPN, LPT, OSCE3, OSCP, OSED, OSEP, OSEE, OSMR, OSWA, OSWE, OSWP, PenTest+ lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament[1], • Cyber Defense NetWars[2],
	od 3 do 5 lat	18000		
	powyżej 5 lat	30000		
		2000		

1 https://www.sans.org/cyber-ranges/netwars-tournaments/core/

2 https://www.sans.org/cyber-ranges/netwars-tournaments/cyber-defense/

					• DFIR NetWars Tournament[3], • Grid NetWars Tournament[4], • ICS NetWars Tournament[5]
2.	do 3 lat	2000	12000	• Kierowanie jednostką organizacyjną przeznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa z wyłączeniem kierownika podmiotu • Prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo • Zaawansowana obsługa incydentów	BTL2, CASP+, CEH Master, CISM, CISSP, CPENT CySA+, GCCC, GCDA, GCIH, GCPM, GCSA, GDAT, GISP, GPYC, GSLC, GSOM, GSTRT, GXPN, GWEB, PenTest+, OSCP, OSEE, OSEP lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
	od 3 do 5 lat		18000		
	powyżej 5 lat		25000		
3.	do 3 lat	2000	8000	• Analiza powłamaniowa • Badanie i ocena bezpieczeństwa rozwiązań ICT • Budowa i utrzymanie systemów monitorowania i detekcji incydentów oraz wsparcia funkcjonowania SOC • Kierowanie komórką organizacyjną przeznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa	BTL1, BTL2, CAP, CASP+, CAWFE, CEH, CEH-Master, CISM, CCFE, CDRP, CFSR, CISSP, CHFI, CPENT, CSSLP, CNFE, CySA+, eCDFP, eCMAP, GCCC, GCDA, GCFA, GCFE, GCIH, GCSA, GISP, GMON, GNFA, GSAF, GSE, GSLC, GSOC, GSOM, GWEB, OSCP, OSEE, OSEP, PenTest+, Security+, SSCP
	od 3 do 5 lat		12000		

3 https://www.sans.org/cyber-ranges/netwars-tournaments/digital-forensics-incident-response/

4 https://www.sans.org/cyber-ranges/netwars-tournaments/power-grid/

5 https://www.sans.org/cyber-ranges/netwars-tournaments/industrial-control-system-security/

	powyżej 5 lat		20000	• Korelacja danych, prowadzenie analiz lub tworzenie map sytuacyjnych • Monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym • Prowadzenie analiz incydentów poważnych, powiązań pomiędzy incydentami oraz opracowywanie wniosków • Przyjmowanie zgłoszeń i obsługa incydentów poważnych • Reagowanie na incydenty oraz ich klasyfikacja • Szacowanie ryzyka w obszarze cyberbezpieczeństwa • Analiza i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania • Koordynacja obsługi zgłoszonych incydentów • Obsługa zgłoszeń i analiza treści przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych • Opracowywanie i wdrażanie planów ciągłości działania i odbudowy oraz systemu zarządzania bezpieczeństwem informacji • Specjalistyczne zadania realizowane w ramach SOC lub NOC obejmujące: monitoring bezpieczeństwa (analiza i korelacja logów), identyfikację i wstępną obsługę incydentów • Nadzór nad procesem szacowania ryzyka w obszarze cyberbezpieczeństwa • Przygotowywanie rekomendacji, standardów i dobrych praktyk w zakresie cyberbezpieczeństwa w szczególności podnoszących poziom bezpieczeństwa systemów IT będących w dyspozycji podmiotów krajowego systemu cyberbezpieczeństwa	lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
	do 3 lat		6000		
	od 3 do 5 lat		9000		BTL1, BTL2, CASP+, CEH, CEH Master, CISSP, CPENT, CySA+, GCIH, GCDA, GDAT, GISP, GMON, GSLC, GSOC, MGT, OSCP, Security+, SSCP lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
4.	powyżej 5 lat	2000	15000		
	do 3 lat		5000		CAP, CASP+, CEH, CISA, CISSP, GISP, GSE, GSLC, GSNA, SSCP lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
	od 3 do 5 lat		8000		
5.	powyżej 5 lat	2000	12000		

6.	do 3 lat od 3 do 5 lat powyżej 5 lat	2000	4500 6000 10500	• Bieżące utrzymanie i rozwój własnych, istotnych systemów IT • Poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych • Wstępna obsługa incydentów • Zabezpieczenie śladów cyfrowych • Rozpoznawanie zagrożeń cyberbezpieczeństwa	BTL1, CASP+, CEH, CEH-Master, CISA, CPENT, CSSLP, CySA+, ITIL Managing Professional, OSCP, OSEE, OSEP, GBFA, GCIH, GOSI, GMON, PenTest+, Security+, SSCP lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament
7.	do 3 lat powyżej 3 lat	2000	6000 8000	• Identyfikacja oraz prowadzenie postępowań wobec operatorów usług kluczowych • Nadzór nad podmiotami krajowego systemu cyberbezpieczeństwa • Nadzór nad podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa • Prowadzenie akcji podnoszących świadomość w obszarze cyberbezpieczeństwa w szczególności organizacja ćwiczeń i szkoleń • Prowadzenie analiz w zakresie funkcjonowania krajowego systemu cyberbezpieczeństwa w tym w zakresie rozwiązań prawnych, organizacyjnych, standardów oraz certyfikacji w obszarze cyberbezpieczeństwa wraz z przygotowywaniem projektów aktów normatywnych • Prowadzenie analiz w zakresie spełniania przez podmioty z sektora lub podsektora warunków kwalifikujących podmiot jako operatora usługi kluczowej • Prowadzenie kontroli w podmiotach krajowego systemu cyberbezpieczeństwa, w tym w podmiotach świadczących	CASP+, CEH, CGAP, CIA, CISA, CISM, CISSP, GISP, GSLC, Security+ lub w dokumencie potwierdzającym zajęcie pierwszego miejsca w: • Core NetWars Tournament, • Cyber Defense NetWars, • DFIR NetWars Tournament, • Grid NetWars Tournament, • ICS NetWars Tournament

usługi z zakresu cyberbezpieczeństwa
- Współpraca krajowa lub międzynarodowa w obszarze cyberbezpieczeństwa

Zestawienie wymienionych w tabeli certyfikatów:

BTL1 – Security Blue Team Level 1

BTL2 – Security Blue Team Level 2

CAP – Certified Authorization Professional

CASP+ – CompTIA Advanced Security Practitioner

CAWFE – Certified Advanced Windows Forensic Examiner

CCFE – Certified Computer Forensics Examiner

CCFE – Certified Computer Forensics Examiner

CDRP – Certified Data Recovery Professional

CEH – Certified Ethical Hacker

CEH Master – Certified Ethical Hacker Master

CFSR – Certified Forensic Security Responder

CGAP – Certified Government Auditing Professional

CHFI – Certified Hacking Forensic Investigator

CIA – Certified Internal Auditor

CISA – Certified Information Systems Auditor

CISM – Certified Information Security Manager

CISSP – Certified Information Systems Security Professional

CMFE – Certified Mobile Forensics Examiner

CNFE – Certified Network Forensics Examiner

CPENT – Certified Penetration Testing Professional

CPT – Certified Penetration Tester

CSSLP – Certified Secure Software Lifecycle Professional

CySA+ – CompTIA CySA+

eCDFP – eLearnSecurity Certified Digital Forensics Professional

eCDFP – eLearnSecurity Certified Digital Forensics Professional

eCMAP – eLearnSecurity Certified Malware Analysis Professional

GASF – GIAC Advanced Smartphone Forensics

GAWN – GIAC Assessing and Auditing Wireless Networks

GBFA – GIAC Battlefield Forensics and Acquisition

GCCC – GIAC Critical Controls Certification

GCDA – GIAC Certified Detection Analyst

GCFA – GIAC Certified Forensic Analyst

GCFE – GIAC Certified Forensic Examiner

GCIH – GIAC Certified Incident Handler

GCPM – GIAC Certified Project Manager

GCPN – GIAC Cloud Penetration Tester

GCSA – GIAC Cloud Security Automation

GCTI – GIAC Cyber Threat Intelligence

GDAT – GIAC Defending Advanced Threats

GISP – GIAC Information Security Professional

GMOB – GIAC Mobile Device Security Analyst

GMON – GIAC Continuous Monitoring Certification

GNFA – GIAC Network Forensic Analyst

GOSI – GIAC Open Source Intelligence

GPEN – GIAC Penetration Tester

GPYC – GIAC Python Coder

GREM – GIAC Reverse Engineering Malware

GSE – GIAC Security Expert

GSLC – GIAC Security Leadership

GSNA – GIAC Systems and Network Auditor

GSOC – GIAC Security Operations Certified

GSOM – GIAC Security Operations Manager

GSSP – GIAC Secure Software Programmer

GSTRT – GIAC Strategic Planning, Policy, and Leadership

GWAPT – GIAC Web Application Penetration Tester

GWEB – GIAC Certified Web Application Defender

GXPN – GIAC Exploit Researcher and Advanced Penetration Tester

LPT – EC Council Licensed Penetration Tester

OSCE3 – Offensive Security Certified Expert 3

OSCP – Offensive Security Certified Professional

OSED – Offensive Security Exploit Developer

OSEE – Offensive Security Exploitation Expert

OSEP – Offensive Security Experienced Penetration Tester

OSMR – Offensive Security macOS Researcher

OSWA – Offensive Security Web Assessor

OSWE – Offensive Security Web Expert

OSWP – Offensive Security Wireless Professional

PenTest+ – CompTIA PenTest+

Security+ – CompTIA Security+

SSCP – Systems Security Certified Practitioner

UZASADNIENIE

Projekt stanowi realizację upoważnienia ustawowego do wydania aktu wykonawczego przez Radę Ministrów, na podstawie art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 2333), zwanej dalej „ustawą".

Rozporządzenie określa:

1) szczegółowe zadania z zakresu cyberbezpieczeństwa i podział ich na grupy;
2) doświadczenie zawodowe lub wymóg posiadania specjalistycznej wiedzy z zakresu cyberbezpieczeństwa wymagane do realizacji zadań z poszczególnych grup;
3) przedziały kwotowe wysokości świadczenia teleinformatycznego w związku z podziałem zadań z zakresu cyberbezpieczeństwa na grupy, o których mowa w pkt 1.

Wzrastająca liczba incydentów cyberbezpieczeństwa oraz pojawiające się nowe zagrożenia, jak również coraz większa dostępność usług publicznych online, powodują, że instytucje publiczne odpowiedzialne za cyberbezpieczeństwo państwa potrzebują dysponować wysoko wykwalifikowaną kadrą. Rynek specjalistów z zakresu cyberbezpieczeństwa jest jednak rynkiem bardzo konkurencyjnym. Wynagrodzenia oferowane w sektorze prywatnym znacznie przewyższają wynagrodzenia oferowane przez instytucje publiczne, które są ograniczane określonymi widełkami płacowymi. Szczególnie negatywnym zjawiskiem jest odpływ kadr z sektora publicznego na rzecz podjęcia pracy na rynku prywatnym. Niezbędne jest zatem wprowadzenie odpowiednich rozwiązań, które pozwolą na utrzymanie specjalistów z zakresu cyberbezpieczeństwa w sektorze publicznym, w szczególności poprzez polepszenie ich sytuacji ekonomicznej.

Wprowadzane świadczenie teleinformatyczne, finansowane z Funduszu Cyberbezpieczeństwa, zapewni konkurencyjne wynagrodzenia dla specjalistów zajmujących się cyberbezpieczeństwem w sektorze publicznym. Rozwiązanie to

wpisuje się w cele określone w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zgodnie z którą podjąć należy działania zwiększające zarobki pracowników administracji publicznej, zajmujących się cyberbezpieczeństwem, do poziomu, jaki mogliby uzyskać zatrudniając się w sektorze prywatnym[1)].

W tabeli zawartej w załączniku do rozporządzenia, określone zostały zadania, za których wykonywanie będzie mogło zostać przyznane świadczenie teleinformatyczne, takie jak m.in.: analiza szkodliwego oprogramowania, czy analiza powłamaniowa (*forensic*), wykrywanie zagrożeń lub incydentów (*cyber threat intelligence*), a także tworzenie rekomendacji technicznych oraz ogólnych z obszaru cyberbezpieczeństwa, czy prowadzenie nadzoru nad podmiotami krajowego systemu cyberbezpieczeństwa. Do tych zadań zostały dodane zadania techniczne związane z zapewnianiem cyberbezpieczeństwa w samych jednostkach administracji, w szczególności obsługa incydentów, a także inne zadania pomocnicze, które realizują ten cel.

Zadania zostały ułożone w grupy według maksymalnych kwot, jakie będą mogły zostać przyznane za ich realizację. Wykaz zadań zawartych w rozporządzeniu ma charakter zamknięty. Katalog ten powinien zostać w przyszłości poddawany stosownym przeglądom.

Do grup o najwyższych kwotach zostały przyporządkowane najważniejsze zadania z zakresu cyberbezpieczeństwa, takie jak: ocena bezpieczeństwa systemów IT – w tym testy penetracyjne i audyty bezpieczeństwa, analizowanie szkodliwego oprogramowania, czy też kierowanie jednostką organizacyjną przeznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa. Są to zadania kluczowe z punktu widzenia zapewnienia cyberbezpieczeństwa we wszystkich kluczowych podmiotach. Realizacja tych zadań wymaga również posiadania szczególnej, specjalistycznej wiedzy.

Do kolejnych grup przyporządkowano istotne zadania wymagające wiedzy oraz umiejętności technicznych i analitycznych, takie jak: przygotowywanie

---

1)Pkt 8.1 załącznika do uchwały nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. poz. 1037).

rekomendacji, standardów i dobrych praktyk w zakresie cyberbezpieczeństwa, w szczególności podnoszących poziom bezpieczeństwa systemów IT będących w dyspozycji podmiotów krajowego systemu cyberbezpieczeństwa, czy też utrzymanie i rozwój istotnych systemów IT w ramach organizacji.

Do ostatniej grupy zaliczono zadania wspierające oraz administracyjne, takie jak m.in.: prowadzenie postepowań wobec operatorów usług kluczowych, sprawowanie nadzoru nad podmiotami krajowego systemu cyberbezpieczeństwa oraz prowadzenie akcji podnoszących świadomość w obszarze cyberbezpieczeństwa. Tego typu zadania są również niezwykle istotne z punktu widzenia sprawnego działania całego systemu cyberbezpieczeństwa w Polsce.

W zależności od stopnia skomplikowania danego zadania oraz szczególnych kompetencji, jakie są wymagane do jego wykonywania, kwoty świadczenia zostały zróżnicowane w zależności od posiadanego doświadczenia, tj. podzielono je na 2 lub 3 przedziały. Większa liczba przedziałów została wyodrębniona w przypadku szczególnie istotnych zadań oraz takich, gdzie korzystne będą dodatkowe zachęty do zdobywania doświadczenia w danej, szczególnie wysokospecjalistycznej dziedzinie.

Progi finansowe zostały przygotowane w taki sposób, by zapewnić najwyższe wartości świadczeń dla wąskiej grupy specjalistów zajmujących się technicznymi aspektami cyberbezpieczeństwa. Tych specjalistów jest niewielu i są oni szczególnie poszukiwani na rynku pracy. Ustalane rozporządzeniem przedziały i wartości świadczenia teleinformatycznego znajdują uzasadnienie w tej sytuacji rynkowej.

Przedziały kwotowe wysokości świadczenia teleinformatycznego mają zapewnić wynagrodzenia konkurencyjne dla osób realizujących zadania w obszarze cyberbezpieczeństwa na rynku prywatnym. Uwzględniono również konieczność zapewnienia zasobów kadrowych odpowiednich do efektywnej i skutecznej realizacji zadań, a zatem posiadających specjalistyczną wiedzę dotyczącą metod i narzędzi wykorzystywanych do zapewnienia odporności systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Osoby wykonujące zadania w ramach instytucji odpowiedzialnych w szczególny sposób za bezpieczeństwo państwa, otrzymają świadczenia adekwatne do ich roli.

Zgodnie z art. 8 ust. 6 ustawy kierownik podmiotu może odstąpić od przeprowadzenia sprawdzianu wiedzy w przypadku przedłożenia przez osobę realizującą albo mającą realizować zadania z zakresu cyberbezpieczeństwa, aktualnego dokumentu potwierdzającego posiadanie specjalistycznej wiedzy z zakresu cyberbezpieczeństwa w zakresie zgodnym z zadaniami na stanowisku. W związku z tym w załączniku wskazano dokumenty na podstawie, których weryfikowane będzie specjalistyczna wiedza niezbędna do wykonywania poszczególnych zadań. Wskazane zostały międzynarodowe certyfikaty oraz dokumenty odwołujące się wprost do norm z dziedziny bezpieczeństwa informacji. Ich wskazanie zapewni, że świadczenie otrzymają wykwalifikowani specjaliści, kluczowi dla bezpieczeństwa całego systemu cyberbezpieczeństwa.

Rozporządzenie wejdzie w życie po upływie 5 dni od dnia ogłoszenia. Z uwagi na przyjęte w projekcie rozwiązania prawne proponowany termin wejścia w życie niniejszego rozporządzenia nie narusza zasady demokratycznego państwa prawnego.

Ponadto, należy podkreślić, że rozporządzenie jest niezbędne dla prawidłowego funkcjonowania ustawy, która wejdzie w życie w dniu 1 stycznia 2022 r.

Projektowane przepisy zostały przeanalizowane pod kątem wpływu na małe i średnie przedsiębiorstwa. Przyjęte w projekcie rozwiązania nie będą miały wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców, stosownie do przepisu art. 66 ust. 1 pkt 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2021 r. poz. 162 i 2105).

Projektowane rozporządzenie nie będzie mieć wpływu na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie wymaga notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej

(Dz. U. z 2021 r. poz. 743).

Projekt nie wymaga przedstawienia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt rozporządzenia został udostępniony w Biuletynie Informacji Publicznej.

W projekcie nie zawarto przepisów o charakterze przejściowym ze względu na brak stosunków prawnych powstałych przed datą wejścia w życie tego rozporządzenia, na które projektowane rozporządzenie miałoby wpływ.

OCENA SKUTKÓW REGULACJI

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa. **Ministerstwo wiodące i ministerstwa współpracujące** Kancelaria Prezesa Rady Ministrów **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński, Sekretarz Stanu w KPRM **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl	**Data sporządzenia** 27 grudnia 2021 r. **Źródło:** Upoważnienie ustawowe z art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. **Nr w wykazie prac**: RD472

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projekt rozporządzenia stanowi wykonanie upoważnienia ustawowego zawartego w art. 8 ust. 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (zwana dalej „ustawą").

W rozporządzeniu ustalane są szczegółowe zadania z zakresu cyberbezpieczeństwa w podziale na grupy, doświadczenie zawodowe lub wymóg posiadania specjalistycznej wiedzy wymagane do realizacji zadań z poszczególnych grup oraz przedziały kwotowe wysokości świadczenia teleinformatycznego.

Projektowana regulacja umożliwi wyrównanie wynagrodzeń ww. osób do wynagrodzeń jakie mogłyby otrzymać na rynku, tym samym ograniczając odpływ specjalistów z administracji publicznej. W konsekwencji projektowane rozwiązanie pozytywnie wpłynie na poziom cyberbezpieczeństwa w Rzeczypospolitej Polskiej.

Rozwiązanie to wpisuje się w cele określone w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zgodnie z którą podejmowane mają być działania zwiększające zarobki pracowników administracji publicznej, zajmujących się cyberbezpieczeństwem, do poziomu, jaki mogliby uzyskać, zatrudniając się w sektorze prywatnym.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rozporządzenie określa:

1) szczegółowe zadania z zakresu cyberbezpieczeństwa i podział ich na grupy;
2) doświadczenie zawodowe lub wymóg posiadania specjalistycznej wiedzy z zakresu cyberbezpieczeństwa wymagane do realizacji zadań z poszczególnych grup;
3) przedziały kwotowe wysokości świadczenia teleinformatycznego w związku z podziałem zadań z zakresu cyberbezpieczeństwa na grupy, o których mowa w pkt 1.

W tabeli zawartej w załączniku do rozporządzenia określone zostały zadania, za których wykonywanie będzie mogło zostać przyznane świadczenie teleinformatyczne, takie jak m.in. analiza szkodliwego oprogramowania, czy analiza powłamaniową (forensic), wykrywanie zagrożeń lub incydentów (cyber threat intelligence), a także tworzenie rekomendacji technicznych oraz ogólnych z obszaru cyberbezpieczeństwa, czy prowadzenie nadzoru nad podmiotami krajowego systemu cyberbezpieczeństwa. Do tych zadań zostały dodane zadania techniczne związane z zapewnianiem cyberbezpieczeństwa w samych jednostkach administracji, w szczególności obsługa incydentów, a także inne zadania pomocnicze, które realizują ten cel.

Ustalane rozporządzeniem maksymalne wartości świadczenia teleinformatycznego znajdują uzasadnienie w sytuacji rynkowej. Jednocześnie wzmocnienia wymagają także zasoby kadrowe odpowiedzialne za funkcjonowanie pod względem prawnym i organizacyjnym krajowego systemu cyberbezpieczeństwa.

Wymóg doświadczenia zawodowego został zróżnicowany w zależności od zadania. W przypadku zadań wymagających największej wiedzy i kwalifikacji, odnosząc się do doświadczenia dodatkowo oparto się na rozwiązaniach rynkowych stosowanych w branży IT.

Tak przygotowane rozporządzenie będzie stanowiło podstawę do przyznawania świadczeń teleinformatycznych już od 2022 r. Przygotowane rozwiązania zapewniają, że nowe środki wzmocnią instytucje odpowiedzialne za cyberbezpieczeństwo państwa i pozwolą im utrzymać obecnych pracowników jak i zatrudnić nowych ekspertów w dziedzinie cyberbezpieczeństwa.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Brak danych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
osoby, które będą mogły otrzymać świadczenie teleinformatyczne	ok. 1000	Szacunki KPRM	Pozytywne, osoby te otrzymają świadczenie teleinformatyczne
Minister właściwy do spraw informatyzacji	1	Informacja ogólnodostępna	Minister właściwy do spraw informatyzacji będzie dysponentem Funduszu Cyberbezpieczeństwa.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W ramach konsultacji projekt został skierowany do zaopiniowania do:

1) Amercian Chamber of Commerce in Poland;
2) Federacja Konsumentów;
3) Busines Centre Club;
4) Fundacja im. Stefana Batorego;
5) Fundacja Bezpieczna Przestrzeń;
6) Fundacja Moje Państwo;
7) Fundacja Instytut Mikromakro;
8) Fundacja MY Pacjenci;
9) Fundacja Nowoczesna Polska;

10) Fundacja Panoptykon;
11) Fundacja Projekt: Polska;
12) Stowarzyszenie „Archiwizjoner”;
13) Fundacja im. Kazimierza Pułaskiego;
14) Związek Pracodawców Branży Internetowej IAB Polska;
15) Klaster #CyberMadeInPoland;
16) Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego UW;
17) Stowarzyszenie ISACA;
18) Izba Gospodarki Elektronicznej;
19) Konfederacja Lewiatan;
20) Krajowa Izba Gospodarcza;
21) Krajowa Izba Gospodarki Cyfrowej;
22) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
23) Krajowa Izba Gospodarki Morskiej;
24) Krajowa Izba Komunikacji Ethernetowej;
25) Krajowa Izba Rozliczeniowa S.A.;
26) Krajowe Stowarzyszenie Ochrony Informacji Niejawnych;
27) Naczelna Organizacja Techniczna;
28) Naczelna Rada Zrzeszeń Handlu i Usług;
29) Ogólnopolskie Porozumienie Organizacji Radioamatorskich;
30) Polskie Górnictwo Naftowe i Gazownictwo;
31) Polskie Koleje Państwowe S.A.;
32) PKP TELKOL sp. z o.o.;
33) Polska Federacja Szpitali;
34) Polska Izba Handlu;
35) Polska Izba Informatyki i Telekomunikacji;
36) Polska Izba Komunikacji Elektronicznej;
37) Polska Izba Producentów Urządzeń i Usług na Rzecz Kolei;
38) Polska Izba Radiodyfuzji Cyfrowej;
39) Polska Organizacja Handlu i Dystrybucji;
40) Polska Organizacja Niebankowych Instytucji Płatności;
41) Polska Rada Biznesu;
42) Polska Wytwórnia Papierów Wartościowych;
43) Polski Związek Krótkofalowców;
44) Polski Związek Pracodawców Przemysłu Farmaceutycznego;
45) Polskie Związek Przemysłu Motoryzacyjnego;
46) Polskie Centrum Badań i Certyfikacji S.A.;

47) Polskie Stowarzyszenie Marketingu SMB;
48) Polskie Towarzystwo Informatyczne;
49) SABI – stowarzyszenie inspektorów ochrony danych;
50) Stowarzyszenie Inżynierów Telekomunikacji;
51) Sieć Obywatelska Watchdog Polska;
52) Towarzystwo Gospodarcze Polskie Elektrownie;
53) Związek Banków Polskich;
54) Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego – ZIPSEE Cyfrowa Polska;
55) Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM;
56) Związek Pracodawców Mediów Publicznych;
57) Związek Przedsiębiorców i Pracodawców;
58) Związek Telewizji Kablowych w Polsce – Izba Gospodarcza.

Stosownie do art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz art. 52 § 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów projekt ustawy został udostępniony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2021 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0

pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Źródła finansowania	Fundusz Cyberbezpieczeństwa utworzony na mocy ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa											
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wejście w życie projektu rozporządzenia nie spowoduje dodatkowych obciążeń finansowych dla sektora finansów publicznych, w tym dla budżetu państwa i budżetów jednostek samorządu terytorialnego.											

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki								
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z 2021 r.)	duże przedsiębiorstwa	-	-	-	-	-	-	-
	sektor mikro-, małych i średnich przedsiębiorstw	-	-	-	-	-	-	-

	rodzina, obywatele oraz gospodarstwa domowe	-	-	-	-	-	-	-
	(dodaj/usuń)	-	-	-	-	-	-	-
W ujęciu niepieniężnym	duże przedsiębiorstwa	Projekt nie ma wpływu na duże przedsiębiorstwa.						
	sektor mikro-, małych i średnich przedsiębiorstw	Projekt nie ma wpływu na sektor mikro-, małych i średnich przedsiębiorstw.						
	rodzina, obywatele oraz gospodarstwa domowe	Projekt będzie miał pozytywny wpływ na cyberbezpieczeństwo Państwa, co pozwoli na zapewnienie bezpiecznych cyfrowych usług publicznych dla obywateli.						
	(dodaj/usuń)							
Niemierzalne	(dodaj/usuń)							
	(dodaj/usuń)							
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy

☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy
Komentarz:	

9. Wpływ na rynek pracy

Projekt pozytywnie wpłynie na podmioty publiczne zajmujące się cyberbezpieczeństwem Państwa, które będą mogły zaoferować specjalistom z zakresu cyberbezpieczeństwa konkurencyjne warunki finansowe, w stosunku do warunków oferowanych przez sektor prywatny.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Wprowadzenie rozporządzenia podniesie poziom cyberbezpieczeństwa Państwa poprzez odpowiednie wynagrodzenie kadry specjalistów oraz zwiększenie możliwości zatrudnienia przez podmioty określone w art. 5 ustawy, wysoko wykwalifikowanej kadry z obszaru cyberbezpieczeństwa.

11.Planowane wykonanie przepisów aktu prawnego
Rozporządzenie stanowić będzie podstawę do sporządzenia i złożenia przez kierownika podmiotu, o którym mowa w art. 5 ustawy wniosku, celem uzyskania środków z Funduszu Cyberbezpieczeństwa na sfinansowanie świadczenia teleinformatycznego dla pracowników tego podmiotu. Pierwsze wnioski będą mogły być złożone do 21 stycznia 2022 r.
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?
W ciągu roku od dnia wejścia w życie rozporządzenia zostanie przeprowadzona analiza mająca na celu zweryfikowanie wykazu zadań ujętych w załączniku do rozporządzenia.
13.Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)