Komunikat Polskiego Związku Krótkofalowców
nr
25
2022
z dnia 22 czerwca 2022 r.

Zabierz radio w teren!

Odwiedź Parki Narodowe w Polsce

Tatrzański Park Narodowy

3702,5 KHz +/- QRM

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 komunikat.pzk.org.pl

Redakcja Komunikatów PZK dziękuje za przesłane materiały: Broniusowi LY5O, Tadeuszowi SP9HQJ, Marcinowi SP3BBS, Stanisławowi SQ2EEQ, Krzysztofowi SQ8GBE, Pawłowi SP1MWN, Ryszardowi SP5EWY, Tomaszowi SP4GHL, Stefanowi SP1JJY, Januszowi SP1TMN, Kazikowi SP9GFI, Tomaszowi SP3QDM..

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.

W komunikacie 25/2022

Sprawy organizacyjne

Po Posiedzeniu ZG PZK
Po zebraniu Żuławskiego OT
Zostań naszym Ambasadorem
Pomoc walczącej Ukrainie

Wydarzenia

V Wolsztyńskie Spotkanie Krótkofalowców
35 rocznica powstania HKŁ SP8ZIV
VII Zlot PSZCZELNIK 2022
W hołdzie kapralowi Janowi Borkowi
1050 rocznica Bitwy pod Cedynią
Zaproszenie na litewski HAM FEST

Sport

Wiadomości nie tylko DX-owe
Zawody - UKF
Zaproszenie na Dni Morza 2022
SPCM SP Contest Maraton
Zawody Poznańskie

Inne

Informatyka i telekomunikacja
Silent Keys

Redakcja Komunikatów PZK:
Piotr SP2JMR, Zygi SP5ELA, Krzysztof SP5E
Jurek SP3SLU, także nadający komunikaty środowe.

Piotr SP2JMR

Po Posiedzeniu ZG PZK

Zgodnie z wcześniejszą informacją w dniu 18 czerwca 2022 w Warszawie w DBFO przy ul. Grochowskiej 262 odbyło się posiedzenie ZG PZK. W posiedzeniu uczestniczyło 23/33 członków ZG PZK co stanowiło 70 % składu ZG PZK. W posiedzeniu uczestniczył Przewodniczący GKR Stanisław SQ2EEQ. Obradom przysłuchiwało się także 2 gości w osobach Krzysztofa SP7WME oraz Tomka SQ5T. ZG podjął uchwały o odznaczeniu Złotymi Odznakami Honorowymi PZK kol. Stefana Jaworskiego SP1JJY oraz Marka Burego SP1JNY. Odznaki Honorowe PZK zostały nadane kol. Zygmuntowi Szumskiemu SP5ELA oraz Jerzemu Karczewskiemu SP1MWF.

Ponadto ZG PZK podjął nast. uchwały:
1. O przyjęciu protokołu z posiedzenia ZG PZK z dnia 04.09.2021
2. O zatwierdzeniu sprawozdania finansowego za rok 2021 r., w tym bilansu rocznego oraz rachunku zysków i strat, zamykających się kwotą sumy bilansowej w wysokości 611 623,60 zł oraz nadwyżką przychodów nad kosztami w wysokości 65 467,42 zł
3. O przeznaczeniu kwoty 65 467,42 zł stanowiącej wynik finansowy za rok 2021 na fundusz rezerwowy.
4. O przyjęciu budżetu Polskiego Związku Krótkofalowców na rok 2022 zawierającego kwotę przychodów 424890,44. zł oraz łączną kwotę wydatków 435044,04 zł.
Posiedzenie trwało ok. 5,5 godziny i przebiegało w bardzo konstruktywnej atmosferze. Po jego formalnym zakończeniu był czas na wystąpienia gości oraz dyskusje na temat przyszłości krótkofalarstwa i Polskiego Związku Krótkofalowców.

To temat bardzo istotny szczególnie w obliczu starzenia się społeczności krótkofalarskiej. Szczegółowy przebieg Posiedzenia będzie dostępny w protokole po jego otrzymaniu przez sekretariat ZG PZK oraz opublikowaniu.

Prezydium posiedzenia ZG PZK 18 czerwca 2022 od lewej: Piotr SP2LQP, Tadeusz SP9HQJ, Piotr SP2JMR, Tomasz SP3QDM, Michał SP2IQW, Marek SP3AMO.

Sala obrad w czasie Posiedzenia ZG PZK w dniu 18.02.2022 r.

Zdjęcia Stanisław SQ2EEQ

Stanisław SQ2EEQ

Po zebraniu Żuławskiego OT

4 czerwca 2022 w sali konferencyjnej Zespołu Szkół Technicznych w Malborku, po nieomal trzyletniej przerwie spowodowanej pandemią odbyło się Walne Zebranie Sprawozdawcze Żuławskiego Oddziału Terenowego PZK Nr 16. Zebranie rozpoczęło się w drugim terminie, ale frekwencja dopisała – 48 procent! Minutą ciszy uczciliśmy naszych Kolegów, którzy w czasie od ostatniego zebrania (grudzień 2019) opuścili nas na zawsze – Ryszarda SP2FAV, Piotra SP2AQP, Heńka SP2WDU i Janusza SP4ISX. Pierwszym punktem porządku zebrania było wręczenie 11 (!) nowym członkom naszego Oddziału legitymacji członkowskich PZK i pakietów startowych. To znaczące osiągnięcie; na przestrzeni 4 lat stan osobowy Żuławskiego Oddziału Terenowego PZK wzrósł z 66 do 81 członków. Niewiele oddziałów w Polsce może się pochwalić podobnym wynikiem. Kolejnymi punktami zebrania były sprawozdania prezesa OT Jurka, SP2GUB i skarbnika Grzegorza SQ2MTK.

Oba wystąpienia były krótkie, ale bardzo konkretne. Przewodniczący Oddziałowej Komisji Rewizyjnej, Włodek SP2HHX nie miał w swoim sprawozdaniu krytycznych uwag do pracy zarządu Oddziału, przedstawił jednak kilka zaleceń. Prowadzący zebranie Stanisław SQ2EEQ przedstawił niektóre problemy z działalności PZK, bowiem będąc przewodniczącym GKR PZK ma na ten temat wiedzę "z samego środka". Zebranie zakończyło się po dwóch godzinach i trzeba na koniec powiedzieć, że miłym, może nawet najważniejszym jego punktem było wspólne zdjęcie, na którym jest nas prawie 50 osób Zebranie nie mogło trwać długo, bo chcieliśmy zdążyć na finałowy mecz naszej Igi, która walczyła na korcie w Paryżu o swój drugi tytuł wielkoszlemowy. Już wiemy, że go zdobyła, więc nasz doping okazał się skuteczny, hi... Dziękujemy komendantowi Hufca ZHP Malbork, hm. Tadeuszowi Orzęckiemu, który pomógł w organizacji zebrania, załatwieniu sali i opiekował się nami podczas całego spotkania. A w kuluarach nie wykluczył podejścia do egzaminu na świadectwo operatora..

Krzysztof SP5E

Zostań naszym Ambasadorem

Zostań naszym ambasadorem. To naprawdę fajne uczucie, kiedy dzięki Tobie ktoś też odkrywa w sobie nową pasję i zostaje krótkofalowcem. Już dziś odnajdź profil PZK facebook.com/polskizwiazek krotkofalowcow. Polub nas. Jeśli w kolejnych dniach, tygodniach zobaczysz post kierowany do nowych osób np. SUPER MOCE możesz pomóc. Udostępniaj go! Dla Ciebie to kilka sekund. Wspólnie mamy wielką moc i ogromny zasięg. Możesz pomóc nam mówić o krótkofalarstwie. Chcesz porozmawiać o akcji? Napisz śmiało do mnie sp5e@pzk.org.pl

Prezydium ZG PZK

Pomoc walczącej Ukrainie

W związku z krytyczną sytuacją po napaści Rosji na Ukrainę apelujemy do wszystkich krótkofalowców SP o wsparcie ludności Ukrainy. PZK nie ma w swoim statucie działalności pomocowej lub charytatywnej proponujemy dokonywanie wpłat na pomoc Ukrainie, którą należy wpłacać na konta stowarzyszeń i fundacji zajmujących się statutowo taką działalnością. Przykładowo są to: Polska Akcja Humanitarna (PAH), Caritas Polska, Polski Czerwony Krzyż (PCK), Fundacja „Siepomaga", fundacja „Polskie Centrum Pomocy Międzynarodowej" PCPM i wiele innych. Zbiórki prowadzą także niektóre podmioty gospodarcze w tym sieci sklepów. Wiele z nich prowadzi także punkty przyjęć pomocy rzeczowej, zbierając odzież, art. spożywcze, higieniczne oraz sprzęt survivalowy. Szczegółowe informacje znajdziecie na ich stronach internetowych. Szczegółowe aktualne informacje na temat potrzeb w zakresie pomocy podaje Narodowy Instytut Wolności pod adresem http://cutt.ly/PomocUchodzcomzUkrainy pod którym znajduje się zaktualizowana baza informacji, gdzie aktualnie pomoc uchodźcom z Ukrainy jest najbardziej potrzebna z określeniem, jaki rodzaj pomocy jest obecnie najbardziej pilny. Zawiera ona bieżące zapotrzebowanie przesyłane przez pełnomocników wojewodów ds. organizacji pozarządowych. Decyzją MSWiA udział NGO w pomocy dla uchodźców jest koordynowany regionalnie. Każdy wojewoda wyznaczył koordynatora do tego zadania. Lista pełnomocników wojewodów jest dostępna pod adresem www.gov.pl/pozytek/dlaukrainy. Przypominamy, że kontakt telefoniczny należy podejmować tylko w sytuacjach wymagających bezpośredniego kontaktu, aby nie blokować linii telefonicznych. W innym przypadku prosimy o zgłaszanie oferowanej pomocy za pośrednictwem rządowej strony internetowej www.pomagamukrainie.gov.pl. Z góry dziękujemy za każdą formę pomocy i zaangażowania, także poprzez przekazywanie niniejszej wiadomości osobom i organizacjom, które mogą włączyć się w akcję #PomagamUkrainie. Na bazie informacji Komitetu ds. Pożytku Publicznego NIW.

Tomek SP3QDM

V Wolsztyńskie Spotkanie Krótkofalowców

Sobota 25.06.2022 O 11:00, Camping Ustronie Karpicko. Będziemy tam już od piątku aż do niedzieli. Zapraszamy członków klubu jak również sympatyków i krótkofalowców z OT-32 i OT-8 czy każdego kto znajdzie chwilkę czasu by nas odwiedzić. Jest gdzie rozbić namiot a i jezioro w pobliżu. Zapraszamy SP3PWL Więcej informacji: https://www.facebook.com/events/548889096630666

Tadeusz SP9HQJ
i Piotr SP2JMR

35 rocznica powstania HKŁ SP8ZIV

Polski Związek Krótkofalowców Zarząd Oddziału Terenowego w Jarosławiu wspólnie z Harcerskim Klubem Krótkofalowców SP8ZIV przy Komendzie Hufca ZHP w Jarosławiu organizują OKOLICZNOŚCIOWE SPOTKANIE KRÓTKOFALOWCÓW z okazji 35-tej rocznicy działalności Klubu SP8ZIV. Spotkanie odbędzie się w dniu 24 czerwca 2022 r. o godz. 17,00 w Sali Narad Starostwa Powiatowego w Jarosławiu ul. Jana Pawła II 17 II piętro. Spotkanie ma charakter podwójnie uroczysty ponieważ w tym roku przypada także 20 rocznica powstania Jarosławskiego OT PZK. Gratulujemy prezesowi OT 35 oraz klubu SP8ZIV Zbyszkowi SP8AUP i życzymy dalszej owocnej pracy na rzecz rozwoju krótkofalarstwa w rejonie Jarosławia.

Stefan SP1JJY

VII Zlot PSZCZELNIK 2022

Po trzyletniej przerwie Myśliborski Klub Łączności PZK SP1PMY wspólnie z Zarządem ZOT PZK w Szczecinie w dniu 16 lipca br. organizuje otwarty VII Zlot Krótkofalowców "Pszczelnik 2022", który tradycyjnie odbędzie się na terenie Ośrodka Harcerskiego nad jeziorem Myśliborskim. W tym roku tematami przewodnimi zlotu będą: 75 rocznica powstania Zachodniopomorskiego Oddziału Terenowego PZK w Szczecinie z tej okazji do końca sierpnia trwa akcja dyplomowa i 89 rocznica przelotu przez Atlantyk samolotu "Lituanica" z dwoma litewskimi pilotami Steponasem Dariusem i Stasysem Girenasem, którzy 17 lipca 1933 r zginęli w katastrofie lotniczej w lesie obok miejscowości Pszczelnik (6 km od Myśliborza). Z tej okazji, w lipcu stacja klubowa będzie pracowała pod znakiem wywoławczym SN89LOT. W programie zlotu między innymi znajdą się konkurencje takie jak: strzelanie z broni pneumatycznej, rzut granatem do celu, przeciąganie liny, konkursy nadawania znaków Morse'a, wiedzy historycznej i operatorskiej. Będą opowieści, prelekcje. Spotkanie zakończymy tradycyjnym ogniskiem. Wszyscy uczestnicy zlotu zostaną poczęstowani grochówką. Więcej informacji o zlocie można znaleźć na stronie ZOT PZK pod adresem OT14.pzk.org.pl Tam znajduje się również link umożliwiający zarejestrowanie swego przyjazdu na zlot. Uczestnicy zlotu będą mogli również zwiedzić wystawę p.n. 75 LAT ZACHODNIOPOMORSKIEGO ODDZIAŁU TERENOWEGO PZK. KRÓTKOFALARSTWO W POWIECIE MYŚLIBORSKIM, która znajduje się w pomieszczeniach Miejskiej i Powiatowej Biblioteki Publicznej w Myśliborzu. Wystawę można oglądać do końca sierpnia b.r. Serdecznie zapraszamy

Krzysztof SQ8GBE

W hołdzie kapralowi Janowi Borkowi

Jan Borek zginał w październiku 1946 r., jak bohater. Pochowano go po kryjomu, jak wroga państwa polskiego, gdzieś w leśnej kniei w okolicach Andrychowa, w Beskidzie Małym. 15 maja 2022 r., blisko Lubatowej. 76 lat po tych smutnych wydarzeniach, polskie społeczeństwo pożegnało jednego ze swoich synów, którzy nie wahali się powiedzieć „nie" nieludzkiemu systemowi. Stanęli z bronią w rękach przeciwko tym, którzy zdradzili swój naród i poszli na współpracę z rosyjskim okupantem. Stanęli w jednym szeregu, aby strzec prawdziwej wolności i niepodległości Rzeczpospolitej Polskiej. Ten dzień, to ważna data, nie tylko dla nas mieszkańców Lubatowej, ale i dla całego ruchu niepodległościowego w powojennej Polsce. W tym dniu, w naszej miejscowości miał miejsce powtórny pochówek kaprala Jana Borka ps. "Jastrząb", żołnierza Armii Krajowej. Uroczystości rozpoczęły się w kościele parafialnym uroczystą Mszą świętą, w której uczestniczyła najbliższa rodzina, osoby ze świata polityki, naukowcy pracujący w Instytucie Pamięci Narodowej oraz wielu mieszkańców Lubatowej. Przy skromnej trumnie ze szczątkami naszego bohatera wartę honorową zaciągnęli żołnierze z podkarpackiej brygady „Podhalańczków" z Rzeszowa, poczty sztandarowe Ochotniczych Straży Pożarnych i szkół działających na terenie Gminy Iwonicz Zdrój. Następnie szczątki zostały uroczyście odprowadzone na miejscowy cmentarz komunalny, gdzie zostały złożone w grobie poświęconym przez ks. proboszcza Ryszarda Królickiego. Na koniec uroczystości naszemu bohaterowi oddali hołd żołnierze, strażacy, harcerze i władze naszego regionu.

Nasz bohater – kapral Jan Borek spoczął wreszcie wśród swoich bliskich i krewnych na lubatowskiej ziemi. Czekał aż 76 lat na godny pogrzeb i żołnierskie honory. Szkoda, że jego rodzice nie doczekali tej podniosłej chwili. Szkolny Klub Krótkofalowców SP8PZI działający przy placówce oświatowej w Lubatowej, dla upamiętnienia tak podniosłego wydarzenia, jaką był uroczysty pogrzeb żołnierza niepodległościowego, zorganizował w dniach 15-29 maja 2022 r., pracę okolicznościowej stacji krótkofalowej i ultrakrótkofalowej – SP46JB. Znak wydany przez Urząd Komunikacji Elektronicznej w Warszawie nawiązywał do daty śmierci oraz imienia i nazwiska partyzanta. Informację o stacji okolicznościowej zamieszczono na kilku portalach krótkofalarskich: z USA – QRZ.com, HamCall.net oraz z Polski w tym QRZ.PL.
Dwaj radioamatorzy, tj. Wojciech Jakieła znak SQ8W oraz Krzysztof Więch znak SQ8GBE – członkowie Szkolnego Klubu Krótkofalowców SP8PZI - pracując różnymi technikami łączności: fonia, emisje cyfrowe i na różnych zakresach fal krótkich i ultrakrótkich nawiązało blisko 1100 łączności z Polską oraz krajami i wyspami Afryki, Azji, Europy i USA. Ich liczba osiągnęła 47. Lista podmiotów DXCC, które nawiązały łączność ze stacją SP46JB przedstawia się następująco: Anglia, Austria, Belgia, Białoruś, Bośnia i Hercegowina, Bułgaria, Chorwacja, Czechy, Dania, Estonia, Finlandia, Francja, Grecja, Guernsey, Hiszpania, Holandia, Indonezja, Irlandia, Irlandia Północna, Japonia, Kanaryjskie Wyspy, Kazachstan, Litwa, Luksemburg, Łotwa, Mołdawia, Monako, Niemcy, Norwegia, Polska, Rosja Azjatycka, Rosja Europejska, Rumunia, Serbia, Słowacja, Słowenia, Sardynia, Szkocja, Szwajcaria, Szwecja, Ukraina, USA, Walia, Węgry, Włochy, Zjednoczone Emiraty Arabskie. Dziękuję Panu Dyrektorowi Szkoły Podstawowej im. Jana Pawła II w Lubatowej, Jerzemu Staroniowi za zmotywowanie nas do pracy w eterze pod znakiem okolicznościowym.

Moje wyrazy wdzięczności wyrażam kolegom krótkofalowcom z Podkarpackiego Oddziału Krótkofalowców w Krośnie, w osobie Stanisława Irzyka SP6FEK oraz z sekretarzowi PZK koledze Piotrowi Skrzypczakowi SP2JMR. Moje podziękowanie kieruję także na ręce pracowników Urzędu Komunikacji Elektronicznej w Warszawie, którzy w trybie przyśpieszonym wydali zgodę dla klubu na pracę pod znakiem okolicznościowym SP46JB. Cieszę się, że w ten szczególny sposób mogliśmy oddać hołd bohaterowi z naszej miejscowości, który poświęcił swoje młode życie w walce o wolność i niepodległość naszej Ojczyzny – Polski.

Warta honorowa podczas uroczystości pogrzebowej Jana Borka.

Paweł SP1MWN

1050 rocznica Bitwy pod Cedynią

W 1050 rocznice bitwy pod Cedynią członkowie z klubu SP1KZE w dniu 25 czerwca 2022 roku będą nadawać z góry Czcibora pod okolicznościowym znakiem SP1050CED. W załączeniu awers karty QSL.

Bronius LY5O

Zaproszenie na litewski HAM FEST

Litewskie Stowarzyszenie Radioamatorów (LRMD) zaprasza radioamatorów z Litwy i innych krajów do udziału w corocznym HAMFEST od 30 lipca do 31 lipca 2022 roku. Hamfest lokalizacja: Marijampole Camping, Kempingo g. 44, Marijampolė, Litwa https://marijampoletic.lt/en/accommodation/rural-tourism/marijampole-camping/ Współrzędne GPS: 54.520054 23.342152 Data. HAMFEST Rozpoczyna się o 9.00 rano 30 lipca (sobota), kończy się o 15.00 31 lipca (niedziela). Więcej informacji pod linkiem: https://lrmd.lt/en Organizatorzy zapraszają już od piątku 29 lipca 2022 r. godzin południowych HAMFEST gospodarz: Marijampole Radio Club "HERCAS". Kontakt LY2SA (tel. +370-699-29030) – informacje ogólne. LY2AT (tel. +370-698-58105) – informacja o lokalizacji. Możliwy przyjazd w piątek 29 lipca.

Marcin SP3BBS

Wiadomości nie tylko DX-owe

5R - Madagaskar: Bernard F9VO przeprowadził się na Madagaskar 26 grudnia 2021 r. Od 17 czerwca będzie aktywny jako 5R8BM z Nosy Be (AF-057).

6O - Somalia: Ali, EP3CQ oczekuje, że będzie w Mogadishu w Somalii 16 czerwca i będzie aktywny ponownie jako 6O1OO przez około miesiąc. W wolnym czasie będzie aktywny na FT8, FT4 i delikatnie na CW w pasmach 80 do 15m QSL direct na adres Ali Solhjoo, Freienwalderstr. 35, 13359 Berlin, Germany.

7P - Lesotho: Mark, KW4XJ jest aktywny jako 7P8AB z Maseru w Lesotho. Jego żona Arina KO4PZT ma znak 7P8NB. Mark jest aktywny na digi, SSB i CW. QSL na adres Mark A. Brewer, 2340 Maseru Pl, Dulles VA 20189-2340, USA.

7X - Algieria: Stacje 7R19MG (QSL via IK2DUW) i 7Y19MG (QSL via 7X2VFK) będą aktywne od 25 czerwca do 5 lipca z okazji 19 edycji Igrzysk Śródziemno-morskich w Oranie. Igrzyska Śródziemno-morskie to międzynarodowa impreza sportowa organizowana co cztery lata wśród sportowców z krajów leżących nad Morzem Śródziemnym w Afryce, Azji i Europie.

A9 - Bahrajn: Członkowie Bahrain Amateur Radio Society będą aktywni jako A91PSD od 17 do 23 czerwca celem uczczenia UN Public Service Day.

CT9 - Madera: Joe HA2EAV i Csaba HA2KMR będą aktywni w stylu wakacyjnym jako CT9/HA2EAV i CT9/HA2KMR z Madery (Af-014) między 24 i 28 czerwca. Będą uczestniczyć w zawodach King of Spain SSB (25 - 26 czerwca) jako CR3DX.

F - Francja: Radio Club Abbevillois będzie używał znaku TM2YT w dniach 25 - 26 czerwca celem uczczenia pamięci przyjaciela Paul-Joel Herbeta F2YT który odszedł 31 grudnia 2021. QSL via F5KRH.

F - Francja: Guillaume, F1IEH będzie aktywny jako TM72LMC od 19 czerwca do 3 lipca z okazji 10 edycji Le Mans Classic. QSL via znak domowy.

HP - Panama: Rafael EA5XV będzie obecny w eterze od 28 czerwca do 12 września na stacji HP1/EA5XV na SSB na pasmach KF. QSL via EA5XV.

JD1 - Ogasawara: Nadchodzące aktywacje Chichijima (AS-031), Ogasawara:

* Harry, JG7PSJ jako JD1BMH od 18 do 26 czerwca na CW, SSB i RTTY, pasma 40 do 10m. QSL via JD1BMH (biuro) lub JG7PSJ (direkt). Brak LoTW lub PayPal.

* Koh, JA1ADT jako JD1AJD od 24 czerwca do 2 lipca na CW, FT8 i FT4, pasma 20 do 6m ze szczególnym uwzględnieniem Europy i Ameryki Północnej na 6m.

* JD1BQI (JE3GRQ) i JD1/JR3DVL od 30 czerwca do 8 lipca wyłącznie na 6m z uwzględnieniem EME i multi-hop sporadic E, głównie Ameryka Północna i Europa. Należy spodziewać się aktywności na 50323kHz FT8 i w okolicach 50200kHz Q65-60A (EME).

OA - Peru: Daniel IK2SGL wraca do Peru i będzie aktywny jako OA9DVK do 31 sierpnia. Po tym czasie opuści Peru na dobre. Skoncentruje swoje działania na SSB i CW. QSL via LoTW, eQSL i ClubLog OQRS, lub via IK6BFH (preferowane biuro).

OJO - Market Reef: Henri OH3JR i Pertti OG2M będą aktywni jako OJ0JR i OJ0MR z Market Reef (EU-053)

między 26 czerwca i 6 lipca. OJ0JR będzie aktywny na górnych pasmach a OJ0MR skoncentruje się na paśmie 6m FT8, CW i SSB z uwzględnieniem obydwóch ameryk i Azji.

ON - Belgia: Czlonkowie Club Radio Durnal (ON4CRD) będą aktywni jako OO22FLY między 25 a 26 czerwca podczas "Fly'in Festival" w bazie lotniczej Saint-Hubert na różnych pasmach emisjami CW i SSB. Qsl via biuro.

SV - Grecja: Alex SQ9UM jest aktywny w stylu wakacyjnym jako SV2/SQ9UM z Paliouri między 16 i 24 czerwca na CW, SSB, FT8 i FT4 w pasmach 80 do 6m. QSL via znak domowy i ClubLog.

VK0/M - Macquarie Island: Matt VK5HZ będzie aktywny jako VK0MQ z Macquarie Island (AN-005) od 11 czerwca i spędzi tutaj "kilka miesięcy". Będzie aktywny na SSB i FT8. QSL via LoTW i ClubLog

VP8 - Falklandy: Bob VP8ADR i inni będą aktywni jako VP8GGM z Goose Green War Museum na East Falkland Island (SA-002) między 24 i 26 czerwca na FT8/FT4 i trochę SSB, 80 do 10m.

Z2 - Zimbabwe: Stacja Z21RU będzie aktywna z Zimbabwe pomiędzy 17 i 29 czerwca. Zespół (R7AL, R9LR, RA1ZZ i RW9JZ) będzie aktywny na pasmach od 160 do 6m a także na satelicie QO-100, emisjami CW, SSB i digi. QSL via ClubLog OQRS i LoTW.

Wyniki zawodów:
CW Fieldday raw score:
https://dxhf2.darc.de/~fdcwlog/user.cgi?fc=loglist&form=referat&lang=de

Nadchodzące zawody:
His Maj. King of Spain Contest, SSB:
25.06.2022, 12:00 UTC
-26.06.2022 12:00 UTC.
https://concursos.ure.es/en/s-m-el-rey-de-espana-ssb/bases/

Stanisław SQ2EEQ

Zawody - UKF

W najbliższym czasie:
SPAC- 2.3 GHz i wyżej - zawody aktywności UKF - wtorek, 28 czerwca 2022, godz. 17:00 - 21:00 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/

Janusz SP1TMN

Zaproszenie na Dni Morza 2022

Zachodniopomorski Odział Terenowy i Środkowopomorski Oddział Terenowy PZK zapraszają do udziału w 51 edycji zawodów „Dni Morza 2022". Zawody odbędą się 26 czerwca 2022 r. /niedziela/ Czas trwania od godz. 05.00-07.00 UTC. Pasma 80 i 40 m, emisje CW i SSB.
Więcej https://dnimorza.ot14.pzk.org.pl

Kazik SP9GFI

SPCM SP Contest Maraton

SPCM wyniki z dnia 12.06.2022 r. (częściowe): https://pzk.org.pl/download.php?action=subcat&id=106

Tomek SP3QDM

Zawody Poznańskie

W imieniu Zarządu OT-8 oraz organizatorów zapraszamy wszystkich krótkofalowców do wzięcia udziału w Zawodach Poznańskich mających na celu upamiętnienie wydarzeń czerwcowych w Poznaniu. Zawody mają miejsce co roku w 4 sobotę czerwca, w tym roku przypada to w dniu 25 czerwca, godz. 05:00-05:59 UTC. Obowiązuje 5-minutowe QRT przed i po zawodach. Pełen regulamin znajdziemy na stronie https://logsp.pzk.org.pl/?page=contest&id=1438

Zygi SP5ELA

Informatyka i telekomunikacja

Otrzymaliśmy według rozdzielnika pismo z sekretariatu DRC MC. Szanowni Państwo, zgodnie z § 36 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348), uprzejmie informuję, że w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny udostępniony został projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (RD402). Zwracam się z uprzejmą prośbą o zgłoszenie ewentualnych uwag (w tym w wersji edytowalnej) do ww. projektu w terminie 14 dni od dnia otrzymania niniejszego pisma. Uwagi 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. wg rozdzielnika Szanowni Państwo, zgodnie z § 36 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348), uprzejmie i informuję, że w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny udostępniony został projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (RD402). Zwracam się z uprzejmą prośbą o zgłoszenie ewentualnych uwag (w tym w wersji edytowalnej) do ww. projektu w terminie 14 dni od dnia otrzymania niniejszego pisma. Uwagi 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. Z poważaniem z up. Adam Andruszkiewicz Sekretarz Stanu w Kancelarii Prezesa Rady Ministrów /podpisano kwalifikowanym podpisem elektronicznym/ Otrzymują:

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

*Dokumenty związane z projektem Ustawy o zwalczaniu nadużyć w komunikacji elektronicznej znajdują się w załączniku do Komunikatu.

SILENT KEY

SP5BR SK

W dniu 20 czerwca br. zmarł Janusz Kozłowski SP5BR ex SP5DBR. Niegdyś bardzo aktywny krótkofalowiec i konstruktor specjalista od lampowych wzmacniaczy dużej mocy. Pogrzeb odbędzie się w czwartek 23.06.2022 r. o 14:30 na Cmentarzu Południowym w Warszawie.

Ryszard SP5EWY

SP4IGV SK

13 czerwca 2022 po długiej chorobie zmarł w szpitalu iławskim kol. SP4IGV Roman Dembiński. (jedyny jego znak) Bardzo aktywny członek radioklubu (kiedyś SP4KGB) SP4KVA, telegrafista. Członek PZK, oddziału 17.

Tomasz SP4GHL

QRPGuys Pacificon – transceiver QRP DSB-CW/40 m

INDEKS 332739 ISSN 1425-1701

świat radio

7-8/22

Magazyn wszystkich użytkowników eteru

KRÓTKOFALARSTWO CB RADIOTECHNIKA

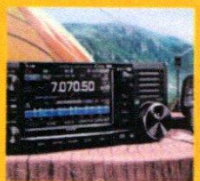
14,90 zł
w tym VAT 8%

tu przejrzysz i kupisz ten numer

wewnątrz
KRÓTKOFALOWIEC POLSKI nr 7–9 (681)/2022

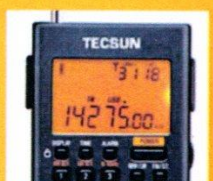
50 lat MFJ

9 771425 170029 07



Icom IC-705

Uniwersalny TRX QRP na pasma 160–6 m, 2 m i 70 cm, o bardzo dobrych parametrach odbiornika i nadajnika



Tecsun PL-368 DSP

Przenośny odbiornik globalny, o kształcie ułatwiającym obsługę jedną ręką

Yaesu FTDX101MP

Wyższej klasy TRX HF i 6 m, o mocy nadajnika 200 W, przydatny w pracy DX-owej i zawodach

10 sekund dla krótkofalarstwa

Wspólnie stwórzmy krótki film. W nie więcej niż 10 sekund dokończ przed kamerą jedno zdanie. Dlaczego warto zostać krótkofalowcem? Prześlij nagranie. My zmontujemy film, który pomoże nam wszystkim promować naszą pasję! Jest wiele powodów dla których warto! Jesteśmy ciekawi co jest najważniejsze dla Ciebie! Łączy nas pasja i miłość do radia.

Nagranie prześlij na adres sp5e@pzk.org.pl najwygodniej z pomocą wetransfer.com lub podobnych serwisów do przesyłania dużych plików. Co ważne - plik wideo bez edycji, filtrów, dodatkowych napisów. Optymalnie wersja „w poziomie", czyli tak jak widzimy obraz w kinie. Wersję pionową też zaakceptujemy i połączymy. Za każdym razem potwierdzę, że plik dotarł poprawnie. Jeśli nie otrzymasz potwierdzenia w ciągu jednego dnia to proszę o ponowny kontakt. Chcesz porozmawiać o akcji? Napisz śmiało sp5e@pzk.org.pl

Vy 73! Krzysztof SP5E

image: Flaticon.com

***Załącznik. Projekt Ustawy o zwalczaniu nadużyć w komunikacji elektronicznej.**

Projekt z 15 czerwca 2022 r.

USTAWA

z dnia …… 2022 r.

o zwalczaniu nadużyć w komunikacji elektronicznej1)

Art. 1. Ustawa określa:

1) prawa i obowiązki przedsiębiorców telekomunikacyjnych związane z zapobieganiem oraz zwalczaniem nadużyć w komunikacji elektronicznej;

2) zasady wnoszenia sprzeciwu przez nadawcę krótkiej wiadomości tekstowej (SMS), wobec uznania treści takiej wiadomości za wyczerpującą znamiona nadużycia w komunikacji elektronicznej;

3) obowiązki dostawcy poczty elektronicznej oraz podmiotu publicznego związane ze świadczeniem i korzystaniem z poczty elektronicznej w celu zapobiegania nadużyciom w komunikacji elektronicznej;

4) szczególne zasady przetwarzania informacji objętych tajemnicą telekomunikacyjną związane z zapobieganiem oraz zwalczaniem nadużyć w komunikacji elektronicznej.

Art. 2. Określenia użyte w ustawie oznaczają:

1) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, o którym mowa w art. 2 pkt 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655);

2) dostawca poczty elektronicznej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy usługę poczty elektronicznej;

3) komunikat elektroniczny – każdą informację wymienianą lub przekazywaną między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług telekomunikacyjnych lub usług komunikacji interpersonalnej niewykorzystujących numerów; nie obejmuje on informacji przekazanej jako część transmisji radiofonicznych lub telewizyjnych transmitowanych przez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania użytkownika otrzymującego informację;

4) nadużycie w komunikacji elektronicznej – świadczenie usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści;

---

1) Niniejszą ustawą zmienia się ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

5) operator – operatora, o którym mowa w art. 2 pkt 27 lit. b ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. 2021 r. poz. 576 oraz z 2022 r. poz. 501);

6) podmiot publiczny – podmiot, o którym mowa w art. 4 pkt 7–15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

7) przedsiębiorca telekomunikacyjny – przedsiębiorcę, o którym mowa w art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

8) poczta elektroniczna – usługę komunikacji interpersonalnej niewykorzystującą numerów, która umożliwia przekazywanie komunikatu elektronicznego z wykorzystaniem standardu SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), lub IMAP4 (Internet Message Access Protocol);

9) połączenie głosowe – połączenie ustanowione za pomocą publicznie dostępnej usługi komunikacji interpersonalnej, pozwalające na dwukierunkową komunikację głosową;

10) sieć telekomunikacyjna – sieć o której mowa w art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

11) tajemnica telekomunikacyjna – tajemnicę, o której mowa w art. 159 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

12) usługa komunikacji interpersonalnej – usługę umożliwiającą bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci telekomunikacyjnej między skończoną liczbą osób, gdzie osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, z wyłączeniem usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej;

13) usługa komunikacji interpersonalnej niewykorzystująca numerów – usługę komunikacji interpersonalnej, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji;

14) usługa telekomunikacyjna – usługę, o której mowa w art. 2 pkt 48 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

15) użytkownik – podmiot, o którym mowa w art. 2 pkt 49 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

16) użytkownik końcowy – podmiot, o którym mowa w art. 2 pkt 50 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Art. 3. 1. Zakazane są nadużycia w komunikacji elektronicznej, w szczególności dotyczące:

1) inicjowania wysyłania lub odbierania komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe (sztuczny ruch);

2) wysyłania krótkich wiadomości tekstowych (SMS), w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem, przekierowania na stronę internetową, żądania kontaktu telefonicznego lub instalacji oprogramowania (smishing);

3) nieuprawnionego posłużenia się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing).

2. Przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie.

Art. 4. 1. CSIRT NASK na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS) monitoruje występowanie smishingu.

2. CSIRT NASK na podstawie monitorowania, o którym mowa w ust. 1, tworzy wzorzec wiadomości wyczerpującej znamiona smishingu.

3. CSIRT NASK przekazuje informację o wystąpieniu smishingu, za pomocą systemu teleinformatycznego, Komendantowi Głównemu Policji, Prezesowi Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE" i przedsiębiorcom telekomunikacyjnym, wraz ze wzorcem wiadomości wyczerpującej znamiona smishingu.

4. Wzorzec wiadomości, o którym mowa w ust. 2, CSIRT NASK udostępnia na swojej stronie internetowej, w terminie 14 dni nie później jednak niż w terminie 21 dni od dnia jego przekazania przedsiębiorcy telekomunikacyjnemu w sposób, o którym mowa w ust. 3.

5. CSIRT NASK, w przypadku gdy uzna, że treść zawarta we wzorcu wiadomości nie stanowi smishingu lub niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS) zgodnie z wzorcem wiadomości niezwłocznie informuje o tym podmioty, o których mowa w ust. 3.

6. Przedsiębiorca telekomunikacyjny po otrzymaniu informacji, o której mowa w ust. 3 lub 5, jest obowiązany do:

1) niezwłocznego blokowania krótkich wiadomości tekstowych (SMS) zawierających treści zawarte we wzorcu wiadomości, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację krótkich wiadomości tekstowych (SMS);

2) zaprzestania blokowania krótkich wiadomości tekstowych (SMS) w przypadku uzyskania informacji, że treść zawarta we wzorcu wiadomości nie nosi znamion smishingu lub niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS) zawierających treści wskazane we wzorcu wiadomości.

Art. 5. 1. Nadawca krótkiej wiadomości tekstowej (SMS) może wnieść do Prezesa UKE sprzeciw wobec uznania treści takiej wiadomości za wyczerpującą znamiona smishingu.

2. Sprzeciw zawiera:

1) uzasadnienie wyjaśniające dlaczego treść krótkiej wiadomości tekstowej (SMS) nie wyczerpuje znamion smishingu;

2) wskazanie numeru wykorzystanego do nadania krótkiej wiadomości tekstowej (SMS).

3. Sprzeciw opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się do Prezesa UKE, za pomocą środków komunikacji elektronicznej.

4. Sprzeciw niespełniający wymagań, o których mowa w ust. 2 lub 3, pozostawia się bez rozpoznania.

Art. 6. 1. Prezes UKE:

1) rozpatruje sprzeciw, w terminie 14 dni od dnia jego otrzymania, oraz

2) niezwłocznie informuje nadawcę krótkiej wiadomości tekstowej (SMS) o sposobie rozpatrzenia sprzeciwu za pomocą środków komunikacji elektronicznej, których użył nadawca krótkiej wiadomości tekstowej (SMS) składając sprzeciw.

2. W przypadku uwzględnienia sprzeciwu przez Prezesa UKE, CSIRT NASK przekazuje informację o której mowa w art. 4 ust. 5, podmiotom, o których mowa w art. 4 ust. 3.

Art. 7. Przedsiębiorca telekomunikacyjny może blokować krótkie wiadomości tekstowe (SMS) zawierające treści wyczerpujące znamiona smishingu, inne niż zawarte we wzorcu wiadomości, o którym mowa w art. 4 ust. 3, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację takich krótkich wiadomości tekstowych (SMS).

Art. 8. W celu zapobiegania i zwalczania CLI spoofing przedsiębiorca telekomunikacyjny blokuje połączenie głosowe albo ukrywa identyfikację numeru wywołującego dla użytkownika końcowego.

Art. 9. 1. Prezes UKE, prowadzi jawny wykaz numerów telefonów służących wyłącznie do odbierania połączeń głosowych, i udostępnia go w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

2. Prezes UKE dokonuje wpisu do wykazu, o którym mowa w ust. 1, na wniosek:

1) jednostki sektora finansów publicznych, o której mowa w art. 9 z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. 2021 r. poz. 305, z późn. zm.2)),

2) banku

– w zakresie wykorzystywanych przez te podmioty numerów.

3. Prezes UKE na wniosek przedsiębiorcy telekomunikacyjnego dokonuje wpisu do wykazu, o którym mowa w ust. 1, wyłącznie numerów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby biura obsługi klientów lub infolinii.

4. Wniosek, o którym mowa w ust. 2 i 3, zawiera wskazanie podmiotu, od którego pochodzi oraz numeru, który ma służyć wyłącznie do odbierania połączeń głosowych.

5. W przypadku gdy wniosek, o którym mowa w ust. 2 i 3, nie zawiera informacji, o których mowa w ust. 4, Prezes UKE wzywa podmiot do ich uzupełnienia w terminie 7 dni od dnia otrzymania wezwania pod rygorem pozostawienia wniosku bez rozpoznania.

6. Prezes UKE dokonuje wpisu numeru do wykazu, o którym mowa w ust. 1, w terminie 5 dni od dnia otrzymania wniosku.

---

2) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 1236, 1535, 1773, 1927, 1981, 2054 i 2270 oraz z 2022 r. poz. 583, 655 i 1079.

7. Wpis do wykazu, o którym mowa w ust. 1, jest czynnością materialno-techniczną.

8. Prezes UKE odmawia wpisu do wykazu, o którym mowa w ust. 1, w drodze decyzji, jeżeli wniosek został złożony przez podmiot nieuprawniony lub dotyczy on numeru niewykorzystywanego przez ten podmiot.

9. Podmiot, który złożył wniosek, o którym mowa w ust. 2 i 3, może w każdym czasie go wycofać. W takim przypadku Prezes UKE niezwłocznie, jednak nie później niż w terminie 5 dni od dnia złożenia wniosku o wycofanie numeru z wykazu, wykreśla numer z wykazu, o którym mowa w ust. 1.

10. Wniosek, którym mowa w ust. 2 i 3, oraz wniosek o wycofanie numeru z wykazu opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnosi się do Prezesa UKE za pomocą środków komunikacji elektronicznej.

11. Wniosek niespełniający wymagań, o których mowa w ust. 10, pozostawia się bez rozpoznania.

12. Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych blokuje połączenia inicjowane z wykorzystaniem numeru wpisanego do wykazu.

Art. 10. 1. Operatorzy mogą zawrzeć z Prezesem UKE porozumienie określające środki organizacyjne i techniczne, które będą stosowali przy realizacji obowiązków, o których mowa w art. 8.

2. Zawarcie porozumienia i jego prawidłowe wykonywanie stanowi spełnienie przez strony porozumienia obowiązku podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie w zakresie o którym mowa w art. 3 ust. 1 pkt 3.

3. Operator prawidłowo wykonujący porozumienie, o którym mowa w ust. 1, nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będącej skutkiem wprowadzonych środków technicznych i organizacyjnych, o których mowa w ust. 1.

4. Prezes UKE kontroluje prawidłowość stosowania środków organizacyjnych i technicznych określonych w porozumieniu, o którym mowa w ust. 2. Przepisy ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne dotyczące kontroli stosuje się.

Art. 11. 1. W celu ochrony użytkowników internetu przed stronami internetowymi wyłudzającymi dane, w tym dane osobowe oraz doprowadzającymi użytkowników internetu do niekorzystnego rozporządzenia ich majątkiem, może zostać zawarte porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu oraz uniemożliwienia dostępu do tych stron.

2. W celu ochrony użytkowników internetu przed CLI spoofing, elementem porozumienia, o którym mowa w ust. 1, może być jawna lista ostrzeżeń dotyczących domen internetowych, które służą do nieuprawnionego wykorzystania numeru lub identyfikatora użytkownika wywołującego połączenie głosowe oraz uniemożliwienia dostępu do tych stron.

3. CSIRT NASK opracowuje, prowadzi i utrzymuje jawną listę ostrzeżeń dotyczącą domen internetowych, o których mowa w ust. 1 i 2. Lista ostrzeżeń jest udostępniana na stronie internetowej CSIRT NASK.

4. Stronami porozumienia są:

1) Prezes UKE;

2) minister właściwy do spraw informatyzacji;

3) Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, oraz

4) przedsiębiorca telekomunikacyjny lub przedsiębiorcy telekomunikacyjni.

5. Porozumienie określa co najmniej zasady współpracy między stronami, w tym zasady zgłaszania domen internetowych, wpisania oraz usuwania ich z listy ostrzeżeń, o której mowa w ust. 1.

6. Przedsiębiorca telekomunikacyjny może uniemożliwić użytkownikom internetu dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę, o której mowa w ust. 1.

Art. 12. 1. Dostawca poczty elektronicznej:

1) dla co najmniej 500 000 użytkowników,

2) dla podmiotu publicznego, lub

3) obsługujący co najmniej 500 000 aktywnych kont pocztowych

– ma obowiązek stosowania mechanizmu SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail).

2. Podmiot publiczny jest obowiązany do korzystania z poczty elektronicznej wykorzystującej mechanizmy, o których mowa w ust. 1.

3. Prezes UKE może przeprowadzić kontrolę:

1) wykonywania obowiązku, o którym mowa w ust. 1, przez dostawcę poczty elektronicznej oraz

2) wykonywania obowiązku, o którym mowa w ust. 2, przez podmiot publiczny.

4. Przepisy ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne dotyczące kontroli stosuje się.

Art. 13. 1. Przedsiębiorca telekomunikacyjny jest obowiązany do rejestracji danych o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją:

1) obowiązku, o którym mowa w art. 4 ust. 6,

2) uprawnienia, o którym mowa w art. 7

– w zakresie umożliwiającym rozpatrzenie reklamacji, o której mowa w art. 106 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

2. Przedsiębiorca telekomunikacyjny przechowuje dane, o których mowa w ust. 1, co najmniej przez okres 12 miesięcy, a w przypadku wniesienia reklamacji – przez okres niezbędny do rozstrzygnięcia sporu.

Art. 14. 1. Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, z wyłączeniem komunikatu elektronicznego, w celu identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej, z uwzględnieniem ust. 2.

2. Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać również komunikat elektroniczny w celu identyfikacji, zapobiegania i zwalczania smishingu.

3. Przedsiębiorca telekomunikacyjny może przetwarzać:

1) treści krótkich wiadomości tekstowych (SMS), oraz

2) dane o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją obowiązku, o którym mowa w art. 4 ust. 6 lub uprawnienia, o którym mowa w art. 7

– w celu realizacji obowiązku, o którym mowa w art. 3 ust. 2, art. 4 ust. 6 i art. 8 oraz realizacji uprawnienia, o którym mowa w art. 7, a także na cele związane z dochodzeniem roszczeń. Przetwarzanie to dopuszczalne jest tylko do końca okresu, w którym możliwe jest dochodzenie roszczeń.

4. Do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych, przepisu art. 14 i 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) nie stosuje się w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego.

Art. 15. 1. Kto dokonuje nadużyć w komunikacji elektronicznej, o których mowa w art. 3 ust. 1 pkt 1, 2 lub 3, podlega karze pieniężnej.

2. Na przedsiębiorcę telekomunikacyjnego, który nie wypełnia obowiązków, o których mowa w:

1) art. 4 ust. 6,

2) art. 8,

3) art. 9 ust. 12

– może zostać nałożona kara pieniężna.

3. Na dostawcę poczty elektronicznej, który nie wypełnia obowiązków, o których mowa w art. 12 ust. 1, może zostać nałożona kara pieniężna.

4. Kary, o których mowa w ust. 1–3, nakłada Prezes UKE w drodze decyzji. Do kar nakładanych na podstawie ust. 1–3 stosuje się odpowiednio przepisy art. 209 ust. 1a–3 oraz art. 210 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

5. Prezes UKE może, w drodze decyzji, nałożyć karę pieniężną na kierownika podmiotu publicznego, jeżeli nie został wykonany obowiązek, o którym mowa w art. 11 ust. 2. Kara pieniężna nakładana jest w wysokości do jednokrotności przeciętnego wynagrodzenia w gospodarce narodowej, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego, w ostatnim komunikacie, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2022 r. poz. 504).

6. Wpływy z tytułu kar pieniężnych, o których mowa w ust. 1-3, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 1 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych

zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2021 r. poz. 2333 oraz z 2022 r. poz. 655).

Art. 16. 1. Kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody dopuszcza się:

1) inicjowania wysyłania lub odbierania komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe,

2) wysyłania krótkich wiadomości tekstowych (SMS), w których podszywa się pod inny podmiot, w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem, przekierowania na stronę www, żądania kontaktu telefonicznego lub instalacji oprogramowania,

3) nieuprawnionego posłużenia się przy wywoływaniu połączenia głosowego informacją adresową wskazującą na inną osobę lub jednostkę organizacyjną, służącego podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych lub instalacji oprogramowania

– podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

3. Jeżeli działanie, o którym mowa w ust. 1 pkt 1–3, popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Art. 17. Prezes UKE przedstawia sejmowej komisji właściwej w sprawach nowych technologii roczne sprawozdanie z wykonywania swoich obowiązków i uprawnień określonych w niniejszej ustawie. Sprawozdanie składa się do dnia 31 marca za rok poprzedni.

Art. 18. W ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 2333 oraz z 2022 r. poz. 655) w art. 2 w ust. 4 po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) wpływy z kar pieniężnych, o których mowa w art. 15 ustawy z dnia … o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. …);”.

Art. 19. 1. CSIRT NASK uruchomi system, o którym mowa w art. 4 ust. 3, i poinformuje ministra właściwego do spraw informatyzacji, w terminie nie później niż w 3 miesięcy od dnia wejścia w życie ustawy.

2. Minister właściwy do spraw informatyzacji niezwłocznie po otrzymaniu informacji, o której mowa w ust. 1, udostępnia, w Biuletynie Informacji Publicznej, informację o uruchomieniu systemu, o którym mowa w art. 4 ust. 3.

3. Komendant Główny Policji, Prezes UKE i przedsiębiorcy telekomunikacyjni obowiązani są do podłączenia się do systemu, o którym mowa w art. 4 ust. 3, w terminie 3 miesięcy od dnia udostępnienia przez ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej na swojej stronie podmiotowej informacji o uruchomieniu tego systemu.

Art. 20. Kary pieniężnej:

1) o której mowa w art. 15 ust. 2 pkt 1, nie nakłada się przed upływem 6 miesięcy od dnia wejścia w życie ustawy;

2) o której mowa w art. 15 ust. 2 pkt 2, nie nakłada się przed upływem 12 miesięcy od dnia wejścia w życie ustawy.

Art. 21. Przedsiębiorcy telekomunikacyjni są obowiązani do wdrożenia rozwiązań umożliwiających podejmowanie proporcjonalnych działań mających na celu zapobieganie i zwalczanie nadużyć w komunikacji elektronicznej, o których mowa w:

1) art. 3 ust. 1 pkt 1 i 2 – w terminie 6 miesięcy od dnia wejścia w życie ustawy;

2) art. 3 ust. 1 pkt 3 – w terminie 12 miesięcy od dnia wejścia w życie ustawy.

Art. 22. 1. Z dniem wejścia w życie ustawy porozumienie o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej, zawarte w dniu 23 marca 2020 r., staje się porozumieniem, o którym mowa w art. 11 ust. 1.

2. Z dniem wejścia w życie ustawy lista ostrzeżeń dotycząca domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu, prowadzona przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy na podstawie zawartego w dniu 23 marca 2020 r. porozumienia o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej, staje się listą, o której mowa w art. 11 ust. 3.

3. Postanowienia porozumienia, o którym mowa w ust. 1, ograniczające stosowanie porozumienia do stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej stają się bezskuteczne z dniem wejścia w życie ustawy.

Art. 23. Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

ZA ZGODNOŚĆ POD WZGLĘDEM PRAWNYM,

LEGISLACYJNYM I REDAKCYJNYM

Anna Markowska

Zastępca Dyrektora

Departamentu Regulacji Cyfrowych

Kancelarii Prezesa Rady Ministrów

/podpisano elektronicznie/

Uzasadnienie

Komunikacja elektroniczna stanowi narzędzie powszechnie wykorzystywane w życiu codziennym przez współczesne społeczeństwo informacyjne. Z usług dostarczanych przez przedsiębiorców telekomunikacyjnych codziennie korzysta wiele milionów osób. Usługi te są również coraz szerzej i w sposób bardziej wyszukany wykorzystywane przez przestępców w celu wyrządzenia szkód po stronie przedsiębiorców telekomunikacyjnych, użytkowników końcowych lub osiągnięcie nienależnych korzyści.

W ostatnich miesiącach nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych3. Przestępcy, stosując specjalne bramki internetowe VoIP podszywali się pod numer zaufanych instytucji czy osoby publiczne i dzwonili z rzekomo prawdziwego numeru. W ten sposób próbowali nakłonić odbiorców do niekorzystnego działania czy w niektórych przypadkach nawet próbowali ich zastraszyć. Oszuści wykorzystywali w ten sposób słabości sieci telekomunikacyjnych, które powodują, że operatorzy sieci mobilnych często nie są w stanie zweryfikować, czy połączenie w ramach którego jest prezentowany numer faktycznie pochodzi z karty SIM, która jest zarejestrowana dla danego numeru. Zjawisko to występuje pod nazwą CLI spoofing.

Innym zagrożeniem dla użytkowników są fałszywe krótkie wiadomości tekstowe SMS. Oszuści podszywając się pod zaufane instytucje próbują nakłonić nieświadome ofiary do ujawnienia danych osobowych, informacji o karcie kredytowej czy zainfekować urządzenie poprzez kliknięcie w link w wiadomości. Zjawisko to występuje pod nazwą smishingu.

W tej sytuacji konieczne jest wprowadzenia odpowiednich przepisów dotyczących zwalczania nadużyć w komunikacji elektronicznej. Proponowane rozwiązania mają służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania nadużyciom w komunikacji elektronicznej przez przedsiębiorców telekomunikacyjnych, a w dalszej perspektywie pozwolą w większym stopniu niż obecnie ograniczyć skalę nadużyć i chronić bezpieczeństwo użytkowników. Kwestia zwalczania nadużyć nie jest regulowana w Europejskim Kodeksie Łączności Elektronicznej oraz nie była dotychczas regulowana w ustawie - Prawo telekomunikacyjne.

Uzasadnienie poszczególnych przepisów materialnych

Art. 1

Przepis art. 1 ustawy określa zakres przedmiotowy ustawy. Przede wszystkim nowe przepisy zawierają prawa i obowiązki przedsiębiorców telekomunikacyjnych związane z zapobieganiem oraz zwalczaniem nadużyć w komunikacji elektronicznej. Określone zostały również zasady wnoszenia sprzeciwu przez nadawcę krótkiej wiadomości tekstowej (SMS), wobec uznania treści krótkiej

3 Raport roczny z działalności CERT Polska Krajobraz bezpieczeństwa polskiego Internetu 2021, s. 81,

https://cert.pl/uploads/docs/Raport_CP_2021.pdf.

wiadomości tekstowej (SMS) za wyczerpującą znamiona nadużycia w komunikacji elektronicznej, obowiązki dostawcy poczty elektronicznej oraz podmiotu publicznego związane ze świadczeniem i korzystaniem z poczty elektronicznej w celu zapobiegania nadużyciom w komunikacji elektronicznej, a także szczególne zasady przetwarzania informacji objętych tajemnicą telekomunikacyjną związane z zapobieganiem oraz zwalczaniem nadużyć w komunikacji elektronicznej.

Art. 2

Art. 2 zawiera słowniczek ustawowy. Wskazano w nim 16 definicji. Do najważniejszych definicji należy definicja CSIRT NASK. Projekt odwołuje się tutaj do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2020 r. poz. 1369, z późn. zm.). Zgodnie z art. 2 pkt 3 tej ustawy jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.

Kolejną istotną definicją jest definicja komunikatu elektronicznego. Zgodnie z projektowaną definicją komunikatem elektronicznym jest każda informacja wymieniana lub przekazywana między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług komunikacji elektronicznej; nie obejmuje on informacji przekazanej jako część transmisji radiofonicznych lub telewizyjnych transmitowanych poprzez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania abonenta lub użytkownika otrzymującego informację. Definicja ta w zasadniczej mierze powtarza treść definicji komunikatu zawartej w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. 2021 r. poz. 576, z późn. zm.). Rozszerza przy tym to pojęcie o informacje przekazywane za pośrednictwem publicznie dostępnych usług komunikacji elektronicznej, a nie jak dotychczas jedynie publicznie dostępnych usług telekomunikacyjnych.

Kluczową definicją jest także definicja nadużycia w komunikacji elektronicznej. Jest to świadczenie lub korzystanie z usługi telekomunikacyjnej lub urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, którego celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści.

Przy szeregu definicji projekt odwołuje się do ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (np. definicja przedsiębiorcy telekomunikacyjnego, operatora, usługi telekomunikacyjnej). Odesłanie do tego aktu prawnego ma na celu zapewnienie spójności definicji w systemie prawa. Podkreślić należy, że ustawa - Prawo telekomunikacyjne jest obecnie głównym aktem prawnym dla dziedziny telekomunikacji.

Definicja podmiotu publicznego odwołuje się z kolei do zbioru podmiotów wskazanych w art. 7–art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Należy przy tym podkreślić, że jest to definicja wyłącznie na potrzeby niniejszej ustawy.

Definicja poczty elektronicznej wskazuje, że jest to usługa komunikacji interpersonalnej niewykorzystującej numerów, która umożliwia przekazywanie komunikatu elektronicznego, z wykorzystaniem standardu SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), lub IMAP4 (Internet Message Access Protocol).

Przy definicji usługi komunikacji interpersonalnej niewykorzystującej numerów wskazano, że jest to usługa, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji oraz umożliwia bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci telekomunikacyjnej między skończoną liczbą osób, gdzie

osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, z wyłączeniem usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej.

Art. 3

W art. 3 wprowadzona została generalna reguła stanowiąca, że nadużycia w komunikacji elektronicznej są zakazane. Ustawa wprowadza otwarty katalog nadużyć w komunikacji elektronicznej, ponieważ wobec postępu technologicznego nie jest możliwe zidentyfikowanie wszystkich form nadużyć. Dookreślono natomiast trzy szczególne (podstawowe) formy nadużyć w komunikacji elektronicznej. Są to:

sztuczny ruch – jest to inicjowanie wysyłania lub odbieranie komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe;

Smishing – jest to wysyłanie krótkich wiadomości tekstowych (SMS), w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem, przekierowania na stronę www, żądania kontaktu telefonicznego lub instalacji oprogramowania;

CLI spoofing – jest to nieuprawnione posłużenie się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania. Jako przykład CLI spoofing można wskazać nieuprawnione wykorzystywanie numeracji jako informacji adresowej w postaci numeru telefonu lub identyfikatora użytkownika inicjującego połączenie, do wykorzystywania której podmiot nie ma uprawnień.

Użycie w projekcie wyrażeń obcojęzycznych jest uzasadnione, ponieważ nie mają one dokładnego odpowiednika w języku polskim.

Ustęp drugi nakłada na przedsiębiorcę telekomunikacyjnego ogólny obowiązek podejmowania proporcjonalnych działań mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. Istotne jest, że mają to być działania proporcjonalne, gdyż wśród przedsiębiorców telekomunikacyjnych znajdują się zarówno duzi przedsiębiorcy dostarczający sieci mobilne, jak i mali i średni przedsiębiorcy. Działania podejmowane przez te podmioty będą więc zależne od wielkości podmiotu, posiadanej infrastruktury czy charakteru świadczonych usług. Przykładowo jako jeden ze środków można wskazać monitorowanie usług telekomunikacyjnych w celu wykrywania przypadków CLI spoofingu.

Art. 4

Projekt zakłada, aby monitorowaniem występowania smishingu zajmował się zespół CSIRT NASK. Po wykryciu smishingu zespół ten informowałby, za pomocą systemu teleinformatycznego, przedsiębiorców telekomunikacyjnych o takim nadużyciu. W systemie przekazywany byłby wzór wiadomości smishingowej. Przedsiębiorca po otrzymaniu takiej informacji blokowałby SMS zgodne ze wzorem przekazanym przez CSIRT NASK. Jednocześnie projektodawca przewidział sytuację, gdy wiadomość uznana za smishing jednak nim nie jest (tzw. false positive). Może być też tak, że nie jest

celowe dalsze blokowanie takich wiadomości. W tej sytuacji CSIRT NASK poinformuje o false positive, a przedsiębiorca przestanie blokować takie wiadomości.

Do systemu teleinformatycznego, przekazującego wzorce wiadomości smishingowej będą również podłączeni:

Komendant Główny Policji – z uwagi na to, że Policja zajmuje się zwalczaniem przestępczości, a nadużycia w komunikacji elektronicznej bardzo często mogą wyczerpywać znamiona przestępstw,

Prezes Urzędu Komunikacji Elektronicznej – z uwagi jego zadania przy ww. procedurze odwoławczej.

Art. 5

Projekt przewiduje procedurę odwoławczą dla nadawcy wiadomości uznanej za wyczerpującą znamiona nadużycia w komunikacji elektronicznej. Nadawca będzie mógł zgłosić sprzeciw do Prezesa UKE. Prezes UKE będzie obowiązany rozpatrzyć sprzeciw co do zasady w terminie 14 dni od dnia jego otrzymania.

Art. 6

Przepis zawiera obowiązki Prezesa UKE oraz CSIRT związane z procedurą odwoławczą dla nadawcy wiadomości uznanej za wyczerpującą znamiona nadużycia w komunikacji elektronicznej.

Art. 7

Art. 7 dotyczy sytuacji, w której przedsiębiorca zidentyfikował wiadomość tekstową, zawierającą treści wyczerpujące znamiona smishingu, które jednak nie zostały wskazane we wzorcu wiadomości przekazanym przez CSIRT NASK. Przepis uprawnia przedsiębiorcę telekomunikacyjnego do zablokowania takiej wiadomości za pomocą systemu teleinformatycznego umożliwiającego identyfikację takich wiadomości.

Art. 8

Przepis nakłada obowiązek na przedsiębiorcę telekomunikacyjnego zablokowania połączenia głosowego albo ukrycia identyfikacji numeru wywołującego dla użytkownika końcowego w przypadku wystąpienia CLI spoofing. Obowiązek ten należy odczytywać łącznie z art. 3 ust. 2 projektu ustawy, zgodnie z którym przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie.

Art. 9

Niektórzy oszuści podszywają się pod jednostki sektora finansów publicznych czy innych przedsiębiorców wykorzystując numery infolinii tych podmiotów. Numery te nie są wykorzystywane do wykonywania połączeń do konsumentów czy obywateli. Jednakże nieświadomy użytkownik końcowy widząc numer takiego podmiotu może mieć wrażenie, że rzeczywiście ktoś dzwoni do niego m.in. z urzędu lub z banku. Oszuści uzyskują wtedy zaufanie ofiary i są w stanie nakłonić do niekorzystnego dla niej działania.

Dlatego przepis art. 9 zawiera obowiązek dla Prezesa Urzędu Komunikacji Elektronicznej do prowadzenia jawnego wykazu numerów, które służą wyłącznie do odbierania połączeń głosowych. Rozwiązanie to ograniczy możliwość podszywania się oszustów pod numery infolinii urzędów czy innych podmiotów. Wykaz będzie prowadzony w systemie teleinformatycznym Prezesa UKE i

udostępniany na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Komunikacji Elektronicznej.

Wniosek o wpis do wykazu numeru będzie mógł być złożony przez jednostki sektora finansów publicznych, banki, jak również w przypadku numerów telefonów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby biura obsługi klientów lub infolinii. Wniosek będzie zawierał wskazanie podmiotu, od którego pochodzi oraz numeru, który ma służyć wyłącznie do odbierania połączeń głosowych. Projekt wprowadza obowiązkową elektronizację tych wniosków – powinny być opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. Wniosek, który nie spełni tych wymogów, będzie pozostawiony bez rozpoznania. Wpis do wykazu będzie miał charakter czynności materialno-technicznej. Dokonany będzie w terminie 5 dni od dnia otrzymania wniosku. Prezes UKE będzie mógł odmówić wpisu, jeżeli wniosek zostanie złożony przez podmiot nieuprawniony. Odmowa nastąpi w drodze decyzji. Wprowadza się również możliwość wycofania wniosku przez podmiot, który go złożył.

Co najważniejsze, skutek wpisu numeru do wykazu aktualizuje obowiązek po stronie przedsiębiorcy telekomunikacyjnego świadczący usługę połączeń głosowych do blokowania połączenia inicjowane z wykorzystaniem numeru wpisanego do wykazu.

Art. 10

Wprowadza możliwość zawarcia przez operatorów telekomunikacyjnych porozumienia z Prezesem UKE, w którym będą określone środki organizacyjne i techniczne, stosowane przez tych przedsiębiorców przy blokowaniu połączenia lub ukrywaniu identyfikacji numeru wywołującego dla użytkownika końcowego, w przypadku gdy połączenie wyczerpuje znamiona CLI spoofingu. Projekt przesądza, że poprzez zawarcie tego porozumienia oraz jego prawidłowe wykonywanie operatorzy spełnią obowiązek podejmowania proporcjonalnych działań mających na celu zapobieganie CLI spoofing. Proponowane rozwiązanie ma na celu ułatwić operatorom telekomunikacyjnym skuteczne wykonywanie tych obowiązków oraz zapewnić im pewność regulacyjną. Wprowadza się wyłączenie odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej tych operatorów, którzy prawidłowo wykonują ww. porozumienie.

Kontrolę prawidłowości stosowania przez operatorów telekomunikacyjnych środków organizacyjnych i technicznych określonych porozumieniem będzie sprawował Prezes UKE.

Art. 11

Przepis art. 11 konstytuuje możliwość zawarcia przez: Prezesa Urzędu Komunikacji Elektronicznej, ministra właściwego do spraw informatyzacji, Naukową i Akademicką Sieć Komputerowa – Państwowy Instytut Badawczy, oraz przedsiębiorcę lub przedsiębiorców telekomunikacyjnych, porozumienia w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu. Obecnie funkcjonuje podobne porozumienie, które umożliwia w okresach stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego prowadzenie przez NASK-PIB jawnej listy ostrzeżeń. Porozumienie to spełniło swoją rolę w okresie pandemii CoVID-19, chroniąc użytkowników internetu przed utratą danych i środków. Zasadne jest umożliwienie, aby również poza okresami stanów nadzwyczajnych czy tymi związanymi zepidemią mogło obowiązywać podobne porozumienie.

Art. 12

Proponuje nałożenie na dostawców poczty elektronicznej:

dla co najmniej 500 000 użytkowników,

obsługujących 500 000 aktywnych kont pocztowych

dla podmiotów publicznych

dodatkowych obowiązków z zakresu bezpieczeństwa poczty elektronicznej.

Dostawcy ci będą mieli obowiązek stosować jeden z poniższych mechanizmów uwierzytelnienia poczty elektronicznej:

DMARC - Domain-based Message Authentication Reporting and Conformance4,

DKIM - DomainKeys Identified Mail5 oraz

SPF - Sender Policy Framework6.

Ponadto na podmiot publiczny zostanie nałożony obowiązek korzystania z poczty elektronicznej wykorzystującej jeden z powyższych mechanizmów.

Kontrolę realizacji ww. obowiązków przez dostawców poczty elektronicznej jak i podmiotów publicznych będzie sprawować Prezes Urzędu Komunikacji Elektronicznej.

Art. 13

Art. 13 nakłada na przedsiębiorców telekomunikacyjnych obowiązek rejestracji danych o niewykonanych usługach w związku z blokowaniem krótkich wiadomości tekstowych, wskazując jednocześnie przez jaki okres dane mają być przechowywane, w szczególności na potrzeby postępowania reklamacyjnego.

Art. 14

W art. 14 ust. 1 projektu wskazano jakie uprawnienia przysługują przedsiębiorcom telekomunikacyjnym w zakresie przetwarzania i wzajemnego udostępniania informacji, w tym informacji objętych tajemnicą telekomunikacyjną, z wyłączeniem komunikatu elektronicznego, w celu identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej. W ust. 2 wymienione zostały informacje, do przetwarzania których przedsiębiorca telekomunikacyjny jest uprawniony wraz ze wskazaniem celu przetwarzania oraz okresu, do kiedy przetwarzanie danych jest dopuszczalne – jako moment graniczny wskazując koniec terminu, w którym możliwe jest dochodzenie roszczeń. Ust. 3 projektowanego przepisu zawiera wyłączenie stosowania art. 14 i 15

4 M. Kucherawy, E. Zwicky, Domain-based Message Authentication, Reporting, and Conformance (DMARC), Request for Comments, RFC 7489, Internet Engineering Task Force, 2015. https://datatracker.ietf.org/doc/html/rfc7489.

5 M. Kucherawy, D. Crocker, T. Hansen, DomainKeys Identified Mail (DKIM) Signatures, Request for Comments, RFC 6376, Internet Engineering Task Force, 2011. https://datatracker.ietf.org/doc/html/rfc6376.

6 S. Kitterman, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, Request for Comments, RFC 7208, Internet Engineering Task Force, 2014. https://datatracker.ietf.org/doc/html/rfc7208.

rozporządzenia 2016/679 w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego.

Art. 15

Art. 15 zawiera przepisy związane z administracyjnymi karami pieniężnymi.

Obligatoryjnie administracyjnej karze pieniężnej będą podlegały podmioty dokonujące nadużyć w komunikacji elektronicznej, wskazane wprost w poszczególnych punktach art. 3 ust. 1.

Fakultatywnej administracyjnej karze pieniężnej będą podlegali:

przedsiębiorca telekomunikacyjny, który nie wypełnia obowiązków wskazanych w art. w art. 4 ust. 6, art. 8 ust. 2 i art. 9 ust. 12,

dostawca poczty elektronicznej który nie wypełnia obowiązków wskazanych w art. 12 ust. 1.

Kara będzie mogła być również nałożona na kierownika podmiotu publicznego, jeżeli nie został wykonany obowiązek, o którym mowa w art. 11 ust. 2.

Proponuje się, aby wpływy z tych kar stanowiły przychód Funduszu Cyberbezpieczeństwa o którym mowa w art. 1 pkt 1 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz.U. z 2021 r. poz. 2333, z późn. zm.). Z tego też powodu w art. 15 proponuje się zmianę tej ustawę stosownie modyfikując przepis o przychodach tego Funduszu.

Art. 16

Przepis art. 16 penalizuje trzy wskazane nadużycia w komunikacji elektronicznej – tworzenie sztucznego ruchu, wysyłania smishingu lub dokonywania działań o charakterze CLI spoofingu w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osoby szkody. Sprawca takiego działania będzie podlegał karze pozbawienia wolności od 3 miesięcy do 5 lat. W przypadku mniejszej wagi sprawca będzie podlegał grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Jeżeli działania te popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Art. 17

Przepis art. 17 nakłada na Prezesa UKE obowiązek przedstawienia sejmowej komisji właściwej w sprawach nowych technologii półrocznego sprawozdania z wykonywania zadań określonych w ustawie.

Art. 18

Przepis art. 18 wprowadza zmiany w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Zmiana polega na dodaniu do przychodów Funduszu Cyberbezpieczeństwa wpływów z kar pieniężnych nakładanych na podstawie art. 15 niniejszej ustawy.

Art. 19

W art. 19 ustanowiono obowiązki związane z uruchomieniem i wdrożeniem przez CSIRT NASK systemu teleinformatycznego do przekazywania informacji o wzorcach wiadomości zawierających smishing. Zgodnie z ust. 3 projektowanego przepisu, Komendant Główny Policji, Prezes UKE i

przedsiębiorcy telekomunikacyjny będą obowiązani do dostosowania i podłączenia swoich systemów teleinformatycznych do wskazanego systemu w terminie 3 miesięcy od dnia zamieszczenia przez ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej informacji o jego uruchomieniu.

Art. 20

Przepis ma charakter intertempolarny i przewiduje czas niezbędny dla przedsiębiorców telekomunikacyjnych do wdrożenia rozwiązań umożliwiających podejmowanie proporcjonalnych działań mających na celu zapobieganie i zwalczanie nadużyć w komunikacji elektronicznej w postaci sztucznego ruchu, smishingu i CLI spoofingu, bez ryzyka nałożenia w tym czasie kary przez Prezesa UKE. Jest to rozwiązanie spójne z kolejnym przepisem.

Art. 21

W art. 21 określone zostały obowiązki przedsiębiorców telekomunikacyjnych dotyczące wdrożenia rozwiązań umożliwiających podejmowanie proporcjonalnych działań mających na celu zapobieganie i zwalczanie nadużyć w komunikacji elektronicznej wymienionych w art. 3 ust. 1 pkt 1, 2 i 3 – odpowiednio w terminie 6 i 12 miesięcy od dnia wejścia w życie projektowanej ustawy.

Art. 22

Jest to przepis dostosowujący, który uznaje Porozumienie o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub Stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej7 za porozumienie, o którym mowa w art. 11 ust.1. Również lista ostrzeżeń8 prowadzona przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy na podstawie ww. porozumienie powinna być prawnie uznana za listę, o której mowa w art. 11 ust. 3.

Pozostałe informacje

Ustawa wejdzie w życie po upływie 30 dni od dnia ogłoszenia.

Wpływ projektu ustawy na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców został omówiony w ocenie skutków regulacji.

Projekt nie będzie miał wpływu na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

Projektowana ustawa nie wymaga przedstawiania organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt nie zawiera przepisów technicznych, tym samym nie podlega procedurze notyfikacji.

7 https://www.uke.gov.pl/akt/uke-przystapil-do-porozumienia-chroniacego-abonentow,300.html.

8 https://cert.pl/posts/2020/03/ostrzezenia_phishing/

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 został udostępniony w Biuletynie Informacji Publicznej. Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348) projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Nazwa projektu Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej 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 Kancelarii Prezesa Rady Ministrów 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 15.06.2022 Źródło: Inicjatywa własna Nr w wykazie prac UD402
OCENA SKUTKÓW REGULACJI	
Jaki problem jest rozwiązywany?	
Komunikacja elektroniczna stanowi narzędzie powszechnie wykorzystywane w życiu codziennym przez współczesne społeczeństwo informacyjne. Z usług dostarczanych przez przedsiębiorców telekomunikacyjnych codziennie korzysta wiele milionów osób. Usługi te są również coraz szerzej i w sposób bardziej wyszukany wykorzystywane przez przestępców w celu wyrządzenia szkód po stronie przedsiębiorców telekomunikacyjnych, użytkowników końcowych lub osiągnięcie nienależnych korzyści. W ostatnich miesiącach nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych9. Przestępcy, stosując specjalne bramki internetowe VoIP podszywali się pod numer zaufanych instytucji czy osoby publiczne i dzwonili z rzekomo prawdziwego numeru. W ten sposób próbowali nakłonić odbiorców do niekorzystnego działania czy w niektórych przypadkach nawet próbowali ich zastraszyć. Oszuści wykorzystywali w ten sposób słabości sieci telekomunikacyjnych, które powodują, że operatorzy sieci	

9 Raport roczny z działalności CERT Polska Krajobraz bezpieczeństwa polskiego Internetu 2021 str 81

https://cert.pl/uploads/docs/Raport_CP_2021.pdf

mobilnych często nie są w stanie zweryfikować, czy połączenie w ramach którego jest prezentowany numer faktycznie pochodzi z karty SIM, która jest zarejestrowana dla danego numeru. Zjawisko to występuje pod nazwą CLI spoofing.

Innym zagrożeniem dla użytkowników są fałszywe krótkie wiadomości tekstowe SMS. Oszuści podszywając się pod zaufane instytucje próbują nakłonić nieświadome ofiary do ujawnienia danych osobowych, informacji o karcie kredytowej czy zainfekować urządzenie poprzez kliknięcie w link w wiadomości. Zjawisko to występuje pod nazwą smishingu.

W tej sytuacji konieczne jest wprowadzenia odpowiednich przepisów dotyczących zwalczania nadużyć w komunikacji elektronicznej. Proponowane rozwiązania mają służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania nadużyciom w komunikacji elektronicznej przez przedsiębiorców telekomunikacyjnych, a w dalszej perspektywie pozwolą w większym stopniu niż obecnie ograniczyć skalę nadużyć i chronić bezpieczeństwo użytkowników.

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

Na przedsiębiorców telekomunikacyjnych zostaną nałożone obowiązki i uprawnienia związane z zwalczaniem nadużyć telekomunikacyjnych.

Przedsiębiorcy telekomunikacyjnie będą obowiązani, w szczególności do:

podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu przeciwdziałać nadużyciom w komunikacji elektronicznej;

blokowania krótkich wiadomości tekstowych, które zawierają treści o charakterze smishingu zgodne ze wzorcem wiadomości przekazanym przez CSIRT NASK;

blokowania połączeń głosowych, które mają na celu podszywanie się pod inną osobę lub instytucję.

Prezes Urzędu Komunikacji Elektronicznej będzie prowadził wykaz numerów służących wyłącznie do odbierania połączeń głosowych.

Zespół CSIRT NASK będzie monitorował występowanie smishingu i przekazywał przedsiębiorcom telekomunikacyjnym wzorce wiadomości wskazujące na wystąpienie smishingu.

Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników, 500 000 aktywnych kont lub podmiotów publicznych będą obowiązani stosować mechanizm uwierzytelnienia poczty elektronicznej.

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

W Wielkiej Brytanii OFCOM prowadzi listę numerów, z których nie są inicjowane połączenia. Są to numery m. in. instytucji publicznych np. infolinie dla obywateli.

W Stanach Zjednoczonych przedsiębiorcy zostali zobowiązani na podstawie Telephone Robocall Abuse Criminal Enforcement and Deterrence Act oraz decyzji Federal Communication Commision do stosowania rozwiązania STIR/SHAKEN, które umożliwia uwierzytelnienie informacji adresowej połączenia10.			
Podmioty, na które oddziałuje projekt			
Grupa	Wielkość	Źródło danych	Oddziaływanie
CSIRT NASK	1	Informacja ogólnodostępna	Zespół CSIRT NASK będzie monitorował nadużycia w komunikacji elektronicznej oraz uruchomi system teleinformatyczny przekazujący wzorce wiadomości zawierające treści o charakterze smishingu.
Dostawcy poczty elektronicznej	brak danych		Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników, 500 000 aktywnych kont lub podmiotów publicznych będą obowiązani stosować mechanizm uwierzytelnienia poczty elektronicznej.
Komendant Główny Policji	1	Informacja ogólnodostępna	Obowiązek podłączenia się do systemu teleinformatycznego przekazującego wzorce wiadomości zawierające treści o charakterze smishingu.
Minister właściwy do spraw informatyzacji	1	Informacja ogólnodostępna	Minister właściwy do spraw informatyzacji będzie obowiązany zamieścić w Biuletynie Informacji Publicznej informację o uruchomieniu przez CSIRT NASK systemu teleinformatycznego przekazującego wzorce wiadomości zawierające treści o charakterze smishingu.
Prezes Urzędu Komunikacji Elektronicznej	1	Informacja ogólnodostępna	Obowiązek podłączenia się do systemu teleinformatycznego przekazującego wzorce wiadomości zawierające treści o charakterze nadużycia w komunikacji elektronicznej. Prezes UKE otrzyma również kompetencję do rozpatrywania sprzeciwu na zablokowanie komunikatu. Prezes UKE będzie również nakładał administracyjne kary pieniężne na przedsiębiorców telekomunikacyjnych za niestosowanie się do przepisów ustawy. Uzyska możliwość zawarcia z operatorami telekomunikacyjnymi porozumienia

10 https://www.fcc.gov/document/mandating-stirshaken-combat-spoofed-robocalls-0

			określającego środki organizacyjne i techniczne stosowanych przy przeciwdziałania CLI spoofing.
Przedsiębiorcy telekomunikacyjni	4017	Rejestr przedsiębiorców telekomunikacyjnych	Na przedsiębiorców telekomunikacyjnych zostaną nałożone obowiązki i uprawnienia związane z zwalczaniem nadużyć w komunikacji elektronicznej.

Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W ramach 14 - dniowych konsultacji i opiniowania projekt zostanie skierowany do zaopiniowania przez:

American Chamber of Commerce in Poland;

Busines Centre Club;

Federacja Konsumentów;

Fundacja Bezpieczna Przestrzeń;

Fundacja im. Kazimierza Pułaskiego;

Fundacja im. Stefana Batorego;

Fundacja Instytut Mikromakro;

Fundacja Moje Państwo;

Fundacja MY Pacjenci;

Fundacja Nowoczesna Polska;

Fundacja Panoptykon;

Fundacja Projekt: Polska;

Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego UW;

Izba Gospodarki Elektronicznej;

Klaster #CyberMadeInPoland;

Konfederacja Lewiatan;

Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;

Krajowa Izba Gospodarcza;

Krajowa Izba Gospodarki Cyfrowej;

Krajowa Izba Gospodarki Morskiej;

Krajowa Izba Komunikacji Ethernetowej;

Krajowa Izba Rozliczeniowa S.A.;

Krajowe Stowarzyszenie Ochrony Informacji Niejawnych;

Naczelna Organizacja Techniczna;

Naczelna Rada Zrzeszeń Handlu i Usług;

Ogólnopolskie Porozumienie Organizacji Radioamatorskich;

PKP TELKOL sp. z o.o.;

Polska Federacja Szpitali;

Polska Izba Handlu;

Polska Izba Informatyki i Telekomunikacji;

Polska Izba Komunikacji Elektronicznej;

Polska Izba Producentów Urządzeń i Usług na Rzecz Kolei;

Polska Izba Radiodyfuzji Cyfrowej;

Polska Organizacja Handlu i Dystrybucji;

Polska Organizacja Niebankowych Instytucji Płatności;

Polska Rada Biznesu;

Polska Wytwórnia Papierów Wartościowych;

Polski Związek Krótkofalowców;

Polski Związek Pracodawców Przemysłu Farmaceutycznego;

Polskie Centrum Badań i Certyfikacji S.A.;

Polskie Górnictwo Naftowe i Gazownictwo;

Polskie Koleje Państwowe S.A.;

Polskie Stowarzyszenie Marketingu SMB;

Polskie Towarzystwo Informatyczne;

Polskie Związek Przemysłu Motoryzacyjnego;

SABI – stowarzyszenie inspektorów ochrony danych;

Sieć Obywatelska Watchdog Polska;

Stowarzyszenie „Archiwizjoner”;

Stowarzyszenie Inżynierów Telekomunikacji;

Stowarzyszenie ISACA;

Towarzystwo Gospodarcze Polskie Elektrownie;

Związek Banków Polskich;

Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego – ZIPSEE Cyfrowa Polska;

Związek Pracodawców Branży Internetowej IAB Polska;

Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM;

Związek Pracodawców Mediów Publicznych;

Związek Przedsiębiorców i Pracodawców;

Związek Telewizji Kablowych w Polsce – Izba Gospodarcza.

Prezesa Urzędu Komunikacji Elektronicznej;

Prezesa Urzędu Ochrony Danych Osobowych;

Prezesa Urzędu Ochrony Konkurencji i Konsumentów.

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 (M.P. z 2022 r. poz. 348) projekt ustawy został udostępniony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

Wpływ na sektor finansów publicznych

(ceny stałe z …… 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												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora

	finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

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 …… r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
	(dodaj/usuń)							
W ujęciu niepieniężnym	duże przedsiębiorstwa	Przedsiębiorcy telekomunikacyjni będą obowiązani do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczaniu. Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników, 500 000 aktywnych kont lub podmiotów publicznych będą obowiązani stosować mechanizm uwierzytelnienia poczty elektronicznej.						
	sektor mikro-, małych i średnich przedsiębiorstw	Mikro, mali i średni przedsiębiorcy telekomunikacyjni będą obowiązani do podejmowania proporcjonalnych technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie.						

	rodzina, obywatele oraz gospodarstwa domowe	Projekt ustawy przełoży się na zwiększenie bezpieczeństwa usług komunikacji elektronicznej świadczonych dla obywateli. Utrudni przestępcom podszywanie się pod inne osoby i oszukiwanie obywateli.
	(dodaj/usuń)	
Niemierzalne	(dodaj/usuń)	
	(dodaj/usuń)	

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

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:

Ustawa wprowadza następujące obowiązki na przedsiębiorców telekomunikacyjnych:

podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie;

podłączenie się do systemu teleinformatycznego przekazującego wzorce wiadomości o charakterze smishingu;

niezwłoczne blokowanie krótkich wiadomości tekstowych zawierających treści zawarte we wzorcu wiadomości;

blokowanie lub ukrycie identyfikacji numeru wywołującego dla użytkownika końcowego w przypadku wystąpienia CLI spoofingu;

rejestracja danych o usługach telekomunikacyjnych, które nie zostały wykonane z uwagi na blokowanie krótkich wiadomości tekstowych.

Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników, 500 000 aktywnych kont lub podmiotów publicznych będą obowiązani stosować mechanizmy uwierzytelnienia poczty elektronicznej.

Wpływ na rynek pracy

Projekt może wygenerować potrzebę zatrudnienia przez niektórych przedsiębiorców telekomunikacyjnych specjalistów do obsługi systemów wykrywania i zwalczania nadużyć w komunikacji elektronicznej.

Wpływ na pozostałe obszary

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

Omówienie wpływu	Projekt spowoduje powstanie: nowego systemu teleinformatycznego służącego do wymiany informacji o wzorcach wiadomości o charakterze smishingu; wykazu numerów służących wyłącznie do odbierania połączeń głosowych. Ustawa wprowadza administracyjne kary za niedostosowanie się do obowiązków wynikających z jej przepisów. Skargi na decyzje administracyjne o nałożeniu kary będą rozpatrywane przez sądy administracyjne. Trudno jest oszacować ile może być nałożonych kar, a co za tym idzie nie jest możliwe oszacowanie liczby postępowań sądowoadministracyjnych wszczętych na podstawie skarg na te decyzje.

Planowane wykonanie przepisów aktu prawnego

Ustawa wejdzie w życie po upływie 30 dni od dnia ogłoszenia. W terminie 3 miesięcy od dnia wejścia w życie ustawy zespół CSIRT NASK uruchomi system teleinformatyczny służący do przekazywania wzorców wiadomości o charakterze smishingu i poinformuje o tym ministra właściwego do spraw informatyzacji. Minister z kolei niezwłocznie po otrzymaniu informacji z CSIRT NASK zamieści informację o uruchomieniu tego systemu w Biuletynie Informacji Publicznej. Po opublikowaniu tej informacji Komendant Główny Policji, Prezes Urzędu Komunikacji Elektronicznej oraz przedsiębiorcy telekomunikacyjni będą obowiązani podłączyć się do tego systemu w terminie 3 miesięcy.

Przedsiębiorcy telekomunikacyjni będą obowiązani podjąć proporcjonalne środki techniczne i organizacyjne mające na celu zapobieganie i zwalczanie: smishingu – w terminie 6 miesięcy od dnia wejścia w życie ustawy oraz CLI spoofingu – w terminie 12 miesięcy od dnia wejścia w życie ustawy.
W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?
Ewaluacja efektów projektu nastąpi po roku. Zostaną zastosowane następujące mierniki: liczba numerów wpisanych do wykazu numerów służących wyłącznie do odbierania połączeń głosowych, liczba wzorców wiadomości o charakterze smishingu przekazanych przez CSIRT NASK do przedsiębiorców telekomunikacyjnych.
Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
Brak