Mirosław Karpiuk*

# Competence of the CSIRT NASK Team in the Field of Combating Abuse of Electronic Communications

**Abstract**

The legislator includes, within the tasks of the CSIRT NASK team, the monitoring of cybersecurity threats and incidents at the national level, as well as the estimation of risks that are related to the disclosed cybersecurity threats and incidents which have occurred, including the conduction of a dynamic risk assessment. The team's obligation is also to collect reports from recipients of short message services (SMS), regarding messages which are suspected of including content that qualifies as smishing, i.e., such text messages in which the sender impersonates another entity to induce the message recipient to behave in a specific manner, including the provision of personal data, the unfavourable disposal of property, the opening of a website, the initiation of a voice call, or the installation of software.

Key words: smishing, CSIRT NASK, cybersecurity

* Prof. Mirosław Karpiuk, PhD, Chair of Administrative Law and Security Studies, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

The CSIRT NASK (alongside other entities) is part of the national cybersecurity system. The legislator defines it as the Computer Security Incident Response Team operating at the national level and managed by the Scientific and Academic Computer Network – the National Research Institute[1]. Since the CSIRT NASK constitutes an element of the national cybersecurity system, it is required to fulfil the objective of that system, which is, according to Article 3 of the ANCS, to ensure cybersecurity at the national level, including the uninterrupted provision of key and digital services, by achieving an adequate level of security of the information systems used to provide these services and ensuring incident handling.

Therefore, its general characteristics relate to cybersecurity which is defined in Art. 2(4) of the ANCS as the resilience of information systems against operations that compromise the confidentiality, integrity, availability and authenticity of the data processed or the related services offered by these systems[2].

**1** Art. 2(3) of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws 2023, item 913 as amended), hereinafter referred to as the ANCS.

**2** Regarding cybersecurity, see also: A. Bencsik, M. Karpiuk, *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2; M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5; A. Bencsik, M. Karpiuk, *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1; U. Soler, *The World of New, Virtual Trends – Central Europe Societies Touched by Covid-19*, „European Journal of Transformation Studies" 2020, no. 8; A. Pieczywok, *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2; K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2; A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023; K. Gawkowski, *Cyberbezpieczeństwo w inteligentnym mieście*, „Cybersecurity and Law" 2023, no. 2; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3; A. Bencsik, M. Karpiuk, N. Strizzolo, *Information Society Services and Their Cybersecurity*, „Cybersecurity and Law" 2024, no. 1; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, ibidem 2021, no. 2; M. Karpiuk, M. Kelemen, *Cybersecurity in civil aviation in Poland and Slovakia*, ibidem 2022, no. 2; R. Buch, D. Ganda, P. Kalola, N. Borad, *World of Cyber Security and Cybercrime*, „Recent Trends in Programming Languages" 2017, no. 2; M. Czuryk, *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2; K. Kaczmarek, *Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022; M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1; K. Kaczmarek, *Technologia deep fake jako potencjalne narzędzie wpływania na decyzje wyborcze w państwach byłego bloku wschodniego* [in:] *Cyberbezpieczeństwo. Aspekty krajowe*

The tasks of the CSIRT NASK are stipulated in Art. 26(6) of the ANCS and include: 1) the coordination of incident handling; 2) the creation and provision of tools for voluntary cooperation and information sharing on cybersecurity threats and incidents; 3) the provision of a telephone line or Internet service for the reporting and analysis of the distribution, dissemination and transmission of child pornography through information and communication technologies; 4) the monitoring of the occurrence of smishing and development of a message template that qualifies as smishing; 5) maintaining and making available on its website a list of names and their abbreviations reserved for public entities as a superscript of the message originating from the public entity, as well as variants of these names and abbreviations which may mislead the recipient as to the origin of the message from a public entity[3].

The CSIRT NASK monitors the occurrence of smishing based on short message services (SMS) received from the recipients of these messages, and information received from telecommunications operators and other entities. According to the results of this monitoring, it creates a template for a smishing message (a message template). It also ensures the functioning of the ICT system for the provision and transmission of information on the occurrence of smishing with a message template. It acts as the controller of the data processed within this system. Through this system, the CSIRT NASK provides access to information on the occurrence of smishing, including message patterns, to the Commander of the Central Office for Combating Cybercrime[4], the President of

*i międzynarodowe*, ed. M. Karpiuk, Warszawa 2024; M. Czuryk, *The Legal Status of Digital Service Providers in the National Cybersecurity System*, „Cybersecurity and Law" 2024, no. 1; M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2; O. Evsyukova, M. Karpiuk, M. Kelemen, *Cyberthreats in Ukraine, Poland and Slovakia*, „Cybersecurity and Law" 2024, no. 1.

3 Regarding the competence of the CSIRT NASK, see also: M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2, p. 62–63.

4 The Commander of the Central Office for Combating Cybercrime serves as the police authority subordinate to the Commander-in-Chief of the Police, and heads the Central Office for Combating Cybercrime, which forms an organisational unit of the police service for combating cybercrime, responsible for the implementation, throughout the country, of tasks in the field of identifying and combating crimes committed with the use of an IT system, an ICT system or an ICT network, as well as in the field of prevention, detection and prosecution of such offences, and for supporting the police organisational units in the identification, prevention and combating of such offences, and the detection and prosecution of their perpetrators, Art. 5d of the Police Act of 6 April 1990 (consolidated text, Journal of Laws 2024, item 145, as amended). See also: K. Pawelec, *Centralne Biuro*

the Office of Electronic Communications[5], and telecommunication operators[6], while also providing said operators with information on the occurrence of smishing with a message template. These entities, in order to exchange information on the occurrence of smishing together with message templates, must use this system. The message template is made available by the CSIRT NASK on its website no earlier than 14 days and no later than 21 days after it has been communicated to the telecommunication operator in that manner. Should it be deemed that the content of the message template does not qualify as smishing or that it is unnecessary to continue blocking the short message service (SMS), including content compliant with the message template, the CSIRT NASK shall immediately inform the relevant entities (the Commander of the Central Office of Combating Cybercrime, the President of the Office of Electronic Communications, and telecommunication operators) of this fact and post on its website information regarding the period for which the message template was in force[7]. When processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person or data concerning a person's health, sexuality or sexual orientation[8], the CSIRT NASK is obliged to conduct a risk analysis, to apply protection measures against malware and access control mechanisms, and to have procedures in place for the secure exchange of information, as required by Art. 39(2) of the ANCS.

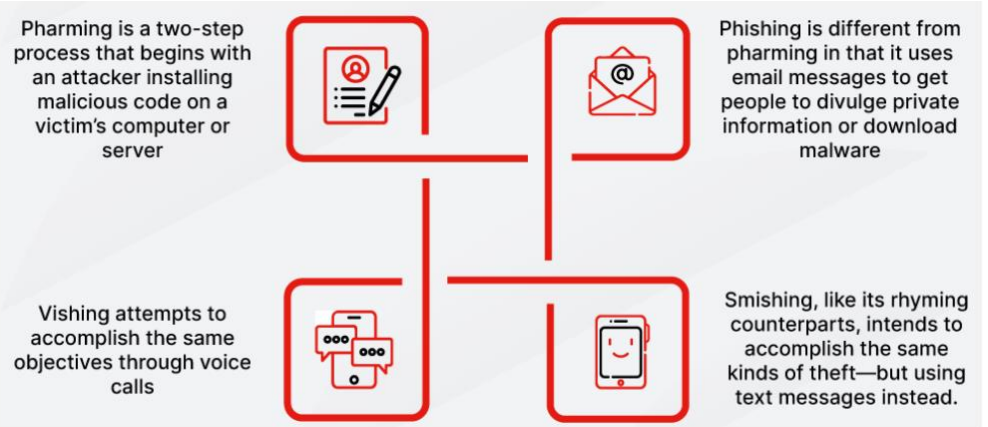
*Zwalczania Cyberprzestępczości i jego wybrane uprawnienia. Kilka refleksji*, „Cybersecurity and Law" 2022, no. 1, p. 130–141.

**5** The President of the Office of Electronic Communications is competent for matters of telecommunications and post, and acts as the regulatory authority in the field of the market for telecommunications and postal services, Art. 189(1) and Art. 190(1) of the Act of 16 July 2004 – Telecommunications Law (consolidated text, Journal of Laws 2024, item 34, as amended), hereinafter referred to as the Telecommunications Law.

**6** A telecommunication operator is an entrepreneur or another entity authorised to conduct business activities, which performs business activities consisting in the provision of telecommunication networks, accompanying services or telecommunication services, Art. 2(27) of Telecommunications Law.

**7** Art. 4 of the Act of 28 July 2023 on Combating Abuse of Electronic Communications (Journal of Laws 2023, item 1703, as amended), hereinafter referred to as the ACAEC.

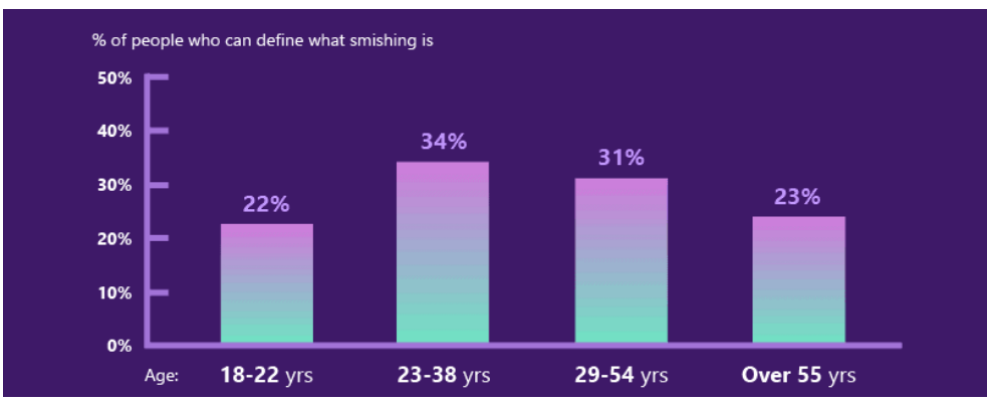
**8** Such personal data are referred to in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the European Union 2016, L 119/1).




Source: *60+ Smishing Statistics in 2024 (SMS Phishing Attacks)*, https://techreport.com/statistics/smishing-statistics/ [access: 22.02.2024].

Diagram 1. Smishing vs. other phishing tools

Smishing is defined in Art. 3(1)(2) of the ACAEC as sending a short message service (SMS) in which the sender impersonates another entity to induce the recipient of the message to behave in a certain way, in particular, to provide personal data, to make an unfavourable disposal of property, to open a website, to initiate a voice call or to install software.




Source: *60+ Smishing Statistics in 2024...*

Diagram 2. Individuals able to define smishing

The CSIRT NASK is obliged, under Art. 5(1) of the ACAEC, to collect reports from recipients of short message services (SMS) regarding messages which are suspected of including content that qualifies as smishing.

A telecommunication operator, upon receipt of information from the CSIRT NASK on the occurrence of smishing, under Art. 6 of the ACAEC, shall immediately block the short message services (SMS) including content compliant with the message template, through an ICT system allowing the automatic identification of short message services (SMS), and in the event of determining that it is no longer necessary to continue blocking the short message service (SMS) or that the content of a message template does not qualify as smishing, it shall cease such blocking if it finds that the content of the message template does not qualify as smishing content or that it is no longer necessary to continue blocking the short message services (SMS) which include content compliant with the message template.

Under Art. 7 of the ACAEC, a short message service (SMS) sender may file an objection to such a message being blocked to the President of the Office of Electronic Communications. The objection shall be formalised and should include: 1) full content of the short message service (SMS); 2) justification explaining why the content of a short message service (SMS) does not qualify as smishing; 3) indication of the number used to send a short message service (SMS); 4) data identifying the sender, including: a) full name and address – in the case of natural persons, b) name (business name) of the entity, address of its registered office, and number from the relevant register – in the case of legal persons and organisational units without legal personality, or c) name of the person authorised to represent the sender, together with his/her authorisation, if applicable. The objection shall bear a qualified electronic signature, a trusted signature or a personal signature, and it shall be submitted to the electronic delivery address of the President of the Office of Electronic Communications. The above formal requirements for an objection to be recognised as valid are mandatory. Failure to comply with any of these conditions shall result in the objection being unprocessed. To successfully initiate a short message service (SMS) blocking control procedure, the sender must draw up an objection strictly following the guidelines specified in Art. 7(2)–(3) of the ACAEC.

As stipulated in Art. 8 of the ACAEC, the President of the Office of Electronic Communications shall consider the objection within 14 days from the date of its receipt and shall immediately notify the sender of the short message service (SMS) of how the objection has been considered, and shall do so using the same means of electronic communication as were employed by the sender of the short message service (SMS) submitting the objection. The central government administration authority competent for telecommunications matters shall either: 1) acknowledge the objection if the

short message service (SMS), which contains content that conforms to the message template, does not qualify as smishing, or 2) reject the objection if the short text message service (SMS), which contains content that conforms to the message template, is recognised as smishing. Should the objection be acknowledged, the President of the Office of Electronic Communications shall order the CSIRT NASK to immediately, and no later than within 3 days from the date of acknowledging the objection, change the message template in such a way that the short message service (SMS) is not blocked. The rejection of an objection constitutes another public administration action against which a complaint may be lodged with the administrative court.

The complaint to the administrative court should include: 1) identification of the contested decision, order, another act or activity; 2) identification of the authority whose action, inaction or protracted conduct constitutes the object of the complaint; and 3) identification of the infringement of a right or legal interest. Furthermore, it should meet the requirements of a pleading in court proceedings and, therefore, it should contain: 1) identification of the court to which it is addressed, name of the parties, their legal representatives and proxies; 2) designation of the type of a complaint; 3) substance of the application or statement; 4) signature of the party or its legal representative or proxy; 5) listing of attachments; 6) indication of the place of residence or, failing that, of the address for service, or of the registered office and addresses of the parties, their legal representatives and proxies; 7) personal identification numbers (PESEL) of the party lodging the complaint, who is a natural person, and of his/her legal representative, if they are required to have it or have it without being obliged to do so; 8) number in the National Court Register or, in absence thereof, business identification number (REGON) or number in any other relevant register or record, or the tax identification number of the party lodging the complaint, other than a natural person, who is not required to be entered in the relevant register or record, where it is obliged to do so; and 9) designation of the subject matter[9].

The CSIRT NASK, under Art. 10(1) of the ACAEC, shall maintain and make available on its website a list of names and their abbreviations reserved for public entities as a superscript (identifier of a short message service – SMS)

**9** Art. 46 and 57 of the Act of 30 August 2002 – Law on Proceedings before Administrative Courts (consolidated text, Journal of Laws 2023, item 1634 as amended). See also H. Knysiak-Sudyka, *Skarga i skarga kasacyjna w postępowaniu sądowoadministracyjnym. Komentarz. Orzecznictwo*, Warszawa 2021, Art. 57.

of a message originating from that public entity, as well as variants of those names and abbreviations which may mislead the recipient as to the origin of the message from the public entity[10].

Smishing shall be penalised, the sanction for this type of criminal act being envisaged in Art. 30 of the ACAEC. Whoever, in order to gain a material or personal benefit or cause damage to another person, sends a short message service (SMS), a multimedia message (MMS) or a message via other interpersonal communication services, in which they impersonate another entity to induce the recipient of the message to provide personal data, to make unfavourable disposal of property, to open a website, to initiate a voice connection, to install software, or to transfer computer passwords, access codes or other data allowing unauthorised access to information stored in a computer system, a data communication system or a data communication network, shall be subject to deprivation of liberty for a term of between 3 months and 5 years. In a minor case, the offender shall be subject to a fine, restriction of liberty or imprisonment for up to one year. If such an act is committed to the detriment of a close relative, prosecution shall occur at the victim's request.

As stipulated in Art. 20 of the ACAEC, to protect Internet users from websites that illegally obtain data, including personal data, and lead Internet users to unfavourable disposal of their property, an agreement may be concluded between the President of the Office of Electronic Communications, the minister competent for informatisation, the CSIRT NASK and telecommunication operators on maintaining a warning list and preventing access to such websites. Should this agreement be concluded, the CSIRT NASK shall be the entity responsible for maintaining the warning list. Internet domains whose primary objectives are to mislead Internet users or to illegally obtain their data and lead them to unfavourable disposal of their property are included in the warning list. Such Internet domains may be reported to the

**10** Included in the range of public entities are those listed in Art. 4(7)–(15) of the ANCS, i.e., 1) selected public finance sector entities; 2) research institutes; 3) Narodowy Bank Polski [National Bank of Poland]; 4) Bank Gospodarstwa Krajowego; 5) the Office of Technical Inspection; 6) the Polish Air Navigation Services Agency; 7) the Polish Centre for Accreditation; 8) the National Environmental Protection and Water Management Fund, as well as provincial environmental protection and water management funds; 9) commercial companies performing public utility tasks. See also: F. Radoniewicz [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 56–65.

CSIRT NASK by anyone. The CSIRT NASK, based on such a notification or on its own initiative, shall include the Internet domain in the warning list.

The holder of a legal title to an Internet domain included in the warning list shall be entitled to apply for a supervisory measure as to the legitimacy of its inclusion in the list. Under Art. 21 of the ACAEC, it may file an objection to an Internet domain being included in the warning list to the President of the Office of Electronic Communications. Such an objection shall include: 1) indication of the Internet domain to which it relates; 2) justification explaining why the inclusion of the Internet domain in the warning list should not be justified; 3) data identifying the holder of the legal title to the Internet domain: (a) full name and address – in the case of natural persons, b) name (business name) of the entity, address of its registered office, and number in the relevant register – in the case of legal persons and organisational units without legal personality, or (c) full name of the person authorised to represent the holder of the domain name, together with his/her authorisation, if applicable. The objection shall bear a qualified electronic signature, a trusted signature or a personal signature, and it shall be submitted to the electronic delivery address of the President of the Office of Electronic Communications. Failure to comply with any of these conditions shall result in the objection being unprocessed.

The President of the Office of Electronic Communications, as provided for in Art. 22 of the ACAEC, shall consider an objection to the inclusion of an Internet domain in the warning list within 14 days from the date of its receipt, and shall immediately inform the objector of how the objection has been considered using the same means of electronic communications as were employed by the objector. The President of the Office of Electronic Communications shall either acknowledge the objection if the Internet domain does not serve to illegally obtain data or to lead to unfavourable disposal of property of Internet users, or reject the objection if the Internet domain is used to illegally obtain data or to lead to unfavourable disposal of property of Internet users. If the objection is acknowledged, the President of the Office of Electronic Communications shall order the CSIRT NASK to remove the Internet domain from the warning list immediately, and no later than within 3 days from the date that objection is considered. The rejection of an objection shall be another public administration measure against which a complaint may be lodged with the administrative court.

## Bibliography


Bencsik A., Karpiuk M., *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1.

Bencsik A., Karpiuk M., *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2.

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Maribor 2023.

Bencsik A., Karpiuk M., Strizzolo N., *Information Society Services and Their Cybersecurity*, „Cybersecurity and Law" 2024, no. 1.

Buch R., Ganda D., Kalola P., Borad N., *World of Cyber Security and Cybercrime*, „Recent Trends in Programming Languages" 2017, no. 2.

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5.

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3.

Czuryk M., *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.

Czuryk M., *The Legal Status of Digital Service Providers in the National Cybersecurity System*, „Cybersecurity and Law" 2024, no. 1.

Evsyukova O., Karpiuk M., Kelemen M., *Cyberthreats in Ukraine, Poland and Slovakia*, „Cybersecurity and Law" 2024, no. 1.

Gawkowski K., *Cyberbezpieczeństwo w inteligentnym mieście*, „Cybersecurity and Law" 2023, no. 2.

Kaczmarek K., *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2.

Kaczmarek K., *Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Kaczmarek K., *Technologia deep fake jako potencjalne narzędzie wpływania na decyzje wyborcze w państwach byłego bloku wschodniego* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. M. Karpiuk, Warszawa 2024.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.

Karpiuk M., Kelemen M., *Cybersecurity in civil aviation in Poland and Slovakia*, „Cybersecurity and Law" 2022, no. 2.

Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2.

Knysiak-Sudyka H., *Skarga i skarga kasacyjna w postępowaniu sądowoadministracyjnym. Komentarz. Orzecznictwo*, Warszawa 2021.

Pawelec K., *Centralne Biuro Zwalczania Cyberprzestępczości i jego wybrane uprawnienia. Kilka refleksji*, „Cybersecurity and Law" 2022, no. 1.

Pieczywok A., *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2.

Radoniewicz F. [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

*60+ Smishing Statistics in 2024 (SMS Phishing Attacks)*, https://techreport.com/statistics/smishing-statistics/ [access: 22.02.2024].
Soler U., *The World of New, Virtual Trends – Central Europe Societies Touched by Covid-19*, „European Journal of Transformation Studies" 2020, no. 8.

## Właściwość zespołu CSIRT NASK w zakresie zwalczania nadużyć w komunikacji elektronicznej

**Streszczenie**

Prawodawca do zadań zespołu CSIRT NASK zalicza m.in. monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym, a także szacowanie ryzyka, które jest związane z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka. Ma on również obowiązek przyjmowania od odbiorców krótkich wiadomości tekstowych (SMS) zgłoszenia dotyczącego wiadomości, co do których istnieje podejrzenie, że ich treść wyczerpuje znamiona smishingu, zatem takiej wiadomości tekstowej, w której nadawca podszywa się pod inny podmiot, żeby nakłonić odbiorcę tej wiadomości do określonego zachowania, w tym do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego czy też instalacji oprogramowania.

**Słowa kluczowe:** smishing, CSIRT NASK, cyberbezpieczeństwo