Mirosław Karpiuk*

Computer fraud

Abstract

Computer fraud is one of the offences against property defined by the legislator. It is committed with the purpose of financial gain or with the intent of causing damage to another person. It may also be classified as cybercrime if information systems and networks are used, including where an information and communication (ICT) system is applied in connection with committing the offence. Computer fraud is also described in this paper from a statistical perspective based on data from annual reports concerning cybersecurity incidents recorded by CERT Poland.

Key words: computer fraud, cybercrime, cyberspace

* 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.

Computer fraud has been defined in Art. 287 of the Polish Penal Code (PC)[1]. As laid down in Art. 287(1) of the PC, whoever, with the purpose of financial gain or with the intent to cause damage to another person, affects the automated processing, collection or transfer of computer data, or alters, deletes or inputs new computer data, without being authorised to do so, is subject to a penalty of imprisonment for a term of between three months and five years. It is an act committed against the actual will of an authorised entity. And apart from the purpose of financial gain or the intent to cause damage to another person, it is not characterised by any other *mens rea* components[2].

The criterion expressed as „without being authorised to do so", used to distinguish between legal and unlawful acts, means the absence of any rights vested in the perpetrator to perform activities involving given computer data or records of such data. If, in a given area, there are no regulations specifying the form of authorising a person to affect, alter, delete or input data records, it should be assumed that any form of authorisation should be taken into account – including oral and implied authorisation[3]. In turn, „computer data" is defined as any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program appropriate to cause a computer system to perform a function (while a „computer system" means any device or a group of interconnected or related devices, one or more of which, according to a program, performs automatic processing of data)[4]. As per Art. 115(11) of the PC, financial gain covers benefits for oneself and another person.

The offence under Art. 287(1) of the PC is committed upon altering or otherwise interfering with devices or systems used for the collection, processing or transfer of information with the use of computer technologies, as specified in the legal provision. Thus, the resulting damage does not belong to the offence criteria[5].

1 The Act of 6 June 1997 – the Penal Code (consolidated text, Journal of Laws 2022, item 1138, as amended).

2 R. Korczyński, R. Koszut, *„Oszustwo" komputerowe*, „Prokuratura i Prawo" 2002, no. 2, p. 27.

3 G. Łabuda [in:] *Kodeks karny. Część szczególna. Komentarz*, ed. J. Giezek, Warszawa 2021, Art. 287.

4 Art. 1(a–b) of the Council of Europe Convention on Cybercrime of 23 November 2001 (Journal of Laws 2015, item 728), hereinafter „the Convention".

5 Judgement of the Appeals Court in Szczecin of 14 October 2008, II AKa 120/08, LEX no. 508308.

Acts defined as cybercrimes consist of using information systems or networks to violate any legal interests protected under penal law. It should be stressed here that it is currently difficult to specify in detail any solid rules that would allow the definition of whether a given prohibited act is cybercrime[6]. Computer fraud is an offence which may also be classified as cybercrime, as ICT systems are also used to commit such fraud, and thus a relation to cybersecurity occurs[7]. Cybercrimes are offences where the use of an ICT network plays a crucial part in their commission. Therefore, it is a narrower category than computer-related crime[8]. An ICT system being used for committing a cybercrime that involves computer fraud is defined as a set of cooperating IT hardware and software, providing the possibility to process and store,

6 M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, no. 7–8, p. 250–251.

7 For additional information about cybersecurity, refer to: M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; K. Chałubińska-Jentkiewicz, M. Nowikowska, *Ochrona informacji w cyberprzestrzeni*, Warszawa 2020; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2; M. Nowikowska, *The right to privacy in cyberspace* [in:] *Human Rights as a Guarantee of Smart, Sustainable and Inclusive Growth*, eds. I. Florek, I. Laki, Budapest 2022; M. Karpiuk, *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1; K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021; M. Karpiuk, *Cybersecurity-related responsibilities of the minister competent for computerisation*, „Cybersecurity and Law" 2022, no. 2; K. Chałubińska-Jentkiwiecz, M. Nowikowska, *Security v. Privacy – Legal Aspects*, Maribor 2021; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, ibidem, no. 1; K. Chałubińska-Jentkiewicz, *Prawne granice dezinformacji w środkach społecznego przekazu*, Toruń 2023; M. Czuryk, *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2, M. Karpiuk, *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 3; M. Karpiuk, M. Kelemen, *Cybersecurity in civil aviation in Poland and Slovakia*, „Cybersecurity and Law" 2022, no. 2; M. Karpiuk, *Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2; K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1; M. Karpiuk, *Tasks of the Minister of National Defence in the area of cybersecurity*, ibidem 2022, no. 1; A. Bencsik, M. Karpiuk, *Cybersecurity in Hungary and Poland. Military aspects*, ibidem 2023, no. 1; M. Karpiuk, *The executive agency as a legal organisational form of implementing cybersecurity tasks*, ibidem.

8 P. Lewulis, *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, no. 3, p. 26. For additional information about cybercrime and computer-related crime, refer to F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, p. 119–131; Ł. Krupa, *Money laundering and cybercrime*, „Cybersecurity and Law" 2022, no. 2, p. 163–164.

as well as send and receive, data via ICT networks with the use of an end device suitable for a given network type[9].

The essence of the types of prohibited acts classified as computer-related crime is the specific object of the perpetrator's impact, related to the electronic means of collecting, processing and transferring information, and the precise method for performing activities that are the constituents of such offences, which involves modern technologies related to collecting, processing and transferring digital data[10].

In minor cases, as stipulated in Art. 287(2) of the PC, the perpetrator of computer fraud is subject to a fine, a non-custodial sentence or imprisonment for up to one year. The decision concerning whether it is a minor case is based on the objective (*actus reus*) and subjective (*mens rea*) criteria of a prohibited act. The most central objective criteria include, in particular, the type of interest that is infringed by the offence, the perpetrator's behaviour and means of conduct, the resources used, the type and extent of damage caused or threat to an interest protected by law, the time, place, and other circumstances of committing the offence, as well as the aggrieved party's sense of loss. Regarding the subjective components, the extent of fault and the motives and objectives of the perpetrator's actions are of vital significance. The degree of social harm is the underlying criterion used to assess whether a given act may be classified as a minor case[11].

Computer fraud often threatens the financial security of banks and their customers. Given that, the compromising of electronic bank account safeguards, by obtaining electronic banking access codes that allow money transfers, following a previous change of the customer contact phone number, meets the criteria of a prohibited act under Art. 287(1) of the PC[12]. The unauthorised acquisition of bank account authentication tools and the unlawful performance of operations on the said bank account, in the form of bank transfers after

9 Art. 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of the Entities Performing Public Tasks (consolidated text, Journal of Laws 2023, item 57).

10 M. Dąbrowska-Kardas, P. Kardas [in:] *Kodeks karny. Część szczególna. Komentarz do art. 278–283*, eds. W. Wróbel, A. Zoll, Warszawa 2022, Art. 287.

11 Judgement of the Appeals Court in Wrocław of 29 September 2010, II AKa 270/10, LEX no. 621279.

12 Judgement of the Appeals Court in Warsaw of 25 May 2018, II AKa 441/17, LEX no. 2520509.

logging in, constitute the input of new computer data records. The act meets the criteria of computer fraud, as specified in Art. 287(1) of the PC[13].

As set out in Art. 287(3) of the PC, if a computer fraud has been committed against an immediate family member, the offence is prosecuted at the request of the aggrieved person. Under Art. 115(11) of the PC, an immediate family member is a spouse, ascendant, descendant, sibling, a person related by affinity in the same line and degree, a person related by adoption and their spouse, and a cohabitee[14]. As a rule, computer fraud is prosecuted *ex-officio*. If a crime has been committed against an immediate family member, the procedure changes to private prosecution pursuant to the provisions set out in Art. 287(3) of the PC[15]. In the event of offences prosecuted upon complaint, intending to determine whether the perpetrator of the offence is an immediate family member of the aggrieved person, it is vital to define not only the point of time when the crime has been committed but also the moment of the establishment of the family relationship giving rise to the status of an immediate family member, also in the course of further proceedings, provided that it precedes the final and binding conclusion of such proceedings[16].

Under Art. 294(1) of the PC, whoever commits computer fraud concerning property of a considerable value shall be subject to a penalty of imprisonment for a term of between one and ten years, provided that property of a considerable value is defined as property whose value exceeds PLN 200 000 as of the date of committing the prohibited act. Concerning computer fraud, the notion of property of a considerable value should be referred to as the amount of damage caused, which results from the structure of this legal provision[17].

13 Judgement of the Warszawa-Praga Regional Court in Warsaw of 21 July 2017, V K 217/15, LEX no. 2675229. For detailed information about the relationships between banks and their customers who have fallen victim to computer fraud, refer to P. Milik, G. Pilarski, *Cyberattacks and the bank's liability for unauthorized payment transactions in the online banking system – theory and practice*, „Cybersecurity and Law" 2023, no. 1.

14 As per Art. 115(11) of the PC, family relationships that provide the status of an immediate family member include the relationships between the party to the proceedings and their spouse, ascendant, descendant, sibling, person related by affinity in the same line and/or degree, a person related by adoption and their spouse. This list is exhaustive and may not be extended to other persons, according to the decision of the Supreme Court of 4 March 2015, IV KO 98/16, „Orzecznictwo Sądu Najwyższego Izba Karna i Wojskowa" 2015, no. 8, item 67.

15 M. Szwarczyk [in:] *Kodeks karny. Komentarz*, ed. T. Bojarski, Warszawa 2016, Art. 287.

16 Judgement of the Supreme Court of 3 March 2015, IV KO 1/15, „Orzecznictwo Sądu Najwyższego Izba Karna i Wojskowa" 2015, no. 7, item 62.

17 M. Kulik [in:] *Kodeks karny. Komentarz*, ed. M. Mozgawa, Warszawa 2015, Art. 194.

In Art. 294(1) of the PC, the legislator has established the aggravated types of certain offences against property, and it is an exhaustive list[18].

Computer fraud can be classified as cybercrime if it is committed in cyberspace. Cyberspace should be understood as a space for the processing and exchange of information created by ICT systems, including the links between them and their relations with users[19]. Today's cyberspace is a global network consisting of interconnected ICT systems built of devices that allow the automated generation, processing and exchange of information between devices and their users, acting intentionally and purposefully. Taking into account the above definition, cyberspace (constituting the sphere of everyday activities of states and their citizens where their interests are pursued) faces continuous threats, first of all from criminal offenders and criminal organisations, including terrorist groups, and secondly as a result of errors or malfunctions of individual ICT systems[20].

Incidents, including computer fraud, are recorded by the Computer Security Incident Response Team operating at the national level and managed by the Research and Academic Computer Network – National Research Institute[21] (CSIRT NASK)[22].

Incidents, defined in Art. 2(5) of the NCSA as events which have, or might have, a negative effect on cybersecurity, are notified, *inter alia*, to CSIRT NASK, which also pertains to cybercrimes, including computer fraud. Having analysed all notifications, the team records those which meet the criteria of a cybersecurity incident.

Computer fraud, comprising incidents recorded by CERT Poland (operating within the structure of NASK), accounts for a relatively large share of all such events. In 2021, 25 472 computer fraud offences were recorded. They

18 I. Zgoliński [in:] *Kodeks karny. Komentarz*, ed. V. Konarska-Wrzosek, Warszawa 2020, art. 194.

19 Art. 2(1b) of the Act of 29 August 2022 on Martial Law and the Competences of the Commander-in-Chief of the Army and the Rules of Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Journal of Laws of 2022, item 2091).

20 P. Milik, G. Pilarski, op. cit., p. 109.

21 Art. 2(3) of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws 2022, item 1863, as amended), further referred to as the NCSA.

22 To learn more about incident notifications submitted to CSIRT NASK, refer to K. Bojarski [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022, p. 168–169.

accounted for 86,4% of all incidents, which totalled 29 483. The number of phishing incidents was 22 575.

Table 1. Computer fraud recorded by CERT Poland in 2021

VIII. Oszustwa komputerowe	**25 472**	**86,40%**
Nieuprawnione wykorzystanie zasobów	3	0,01%
Naruszenie praw autorskich	1	0,00%
Kradzież tożsamości, podszycie się	12	0,04%
Phishing	22 575	76,57%
Niesklasyfikowane	2 881	9,77%

The „computer fraud" item in the table includes the following types of incidents: unlawful use of resources, copyright infringement, identity theft, impersonation, phishing, not elsewhere classified.

Source: *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2021 z działalności CERT Polska*, Warszawa 2022, p. 24.

A significant share of computer fraud events which had, or might have had, a negative effect on cybersecurity, in the total number of incidents, was also reported in 2020. CERT Poland recorded a total of 10 420 incidents, including 8310 incidents of computer fraud, with phishing demonstrating the highest percentage (7622 incidents accounting for 73,15% of the total number).

Table 2. Computer fraud recorded by CERT Poland in 2020

VIII. Oszustwa komputerowe, w tym:	**8310**	**79,75%**
Nieuprawnione wykorzystanie zasobów	25	0,24%
Naruszenie praw autorskich	2	0,02%
Kradzież tożsamości, podszycie się	11	0,11%
Phishing	7622	73,15%
Niesklasyfikowane	650	6,24%

The „computer fraud" item in the table includes the following types of incidents: unlawful use of resources, copyright infringement, identity theft, impersonation, phishing, not elsewhere classified.

Source: *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2020 z działalności CERT Polska*, Warszawa 2021, p. 28.

CERT Poland recorded 6484 incidents in 2019, over half of which involved computer fraud (4086 incidents). The most popular incident type was phishing, with a share of 54,2% of all recorded incidents and 3516 phishing attacks.

Table 3. Computer fraud recorded by CERT Poland in 2019

VIII. Oszustwa komputerowe, w tym:	4086	63,0%
Nieuprawnione wykorzystanie zasobów	5	0,1%
Naruszenie praw autorskich	5	0,1%
Kradzież tożsamości, podszycie się	23	0,4%
Phishing	3516	54,2%
Niesklasyfikowane	537	8,3%

The „computer fraud" item in the table includes the following types of incidents: unlawful use of resources, copyright infringement, identity theft, impersonation, phishing, not elsewhere classified.

Source: *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2019 z działalności CERT Polska*, Warszawa 2020, p. 16.

In 2018, a total of 3739 incidents were recorded. According to the statistics maintained by CERT Poland, phishing attacks took the lead position (1655 incidents), with 1878 computer fraud offences recorded that year, accounting for over half of all incidents (50,23%).

Table 4. Computer fraud recorded by CERT Poland in 2018

Oszustwa komputerowe	**1 878**	**50,23**
Nieuprawnione wykorzystanie zasobów	1	0,03
Naruszenie praw autorskich	8	0,21
Kradzież tożsamości, podszycie się	43	1,15
Phishing	1 655	44,26
Niesklasyfikowane	171	4,57

The „computer fraud" item in the table includes the following types of incidents: unlawful use of resources, copyright infringement, identity theft, impersonation, phishing, not elsewhere classified.

Source: *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2018 z działalności CERT Polska*, Warszawa 2019, p. 12.

In 2017, CERT Poland recorded 3182 incidents, of which there were 1439 computer fraud offences, constituting 45,22% of the all incidents. While phishing was the most prevalent incident type, with 1304 such incidents recorded, accounting for 90,62% of all computer fraud.

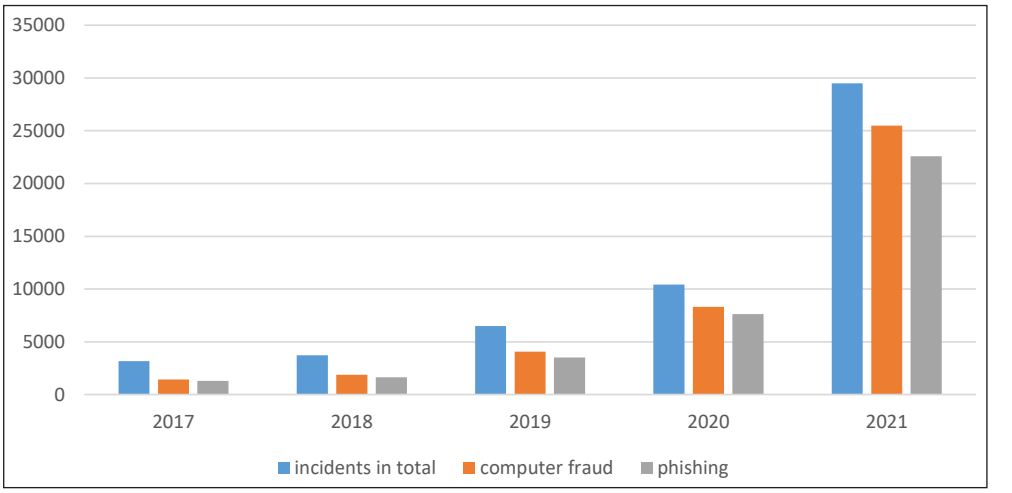
Table 5. Computer fraud recorded by CERT Poland in 2017

Oszustwa komputerowe	**1439**	**45,22**
Nieuprawnione wykorzystanie zasobów	5	0,16
Naruszenie praw autorskich	34	1,07
Kradzież tożsamości, podszycie się	10	0,31
Phishing	1304	40,98
Niesklasyfikowane	86	2,7

The „computer fraud" item in the table includes the following types of incidents: unlawful use of resources, copyright infringement, identity theft, impersonation, phishing, not elsewhere classified.

Source: *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2017 z działalności CERT Polska*, Warszawa 2018, p. 14.

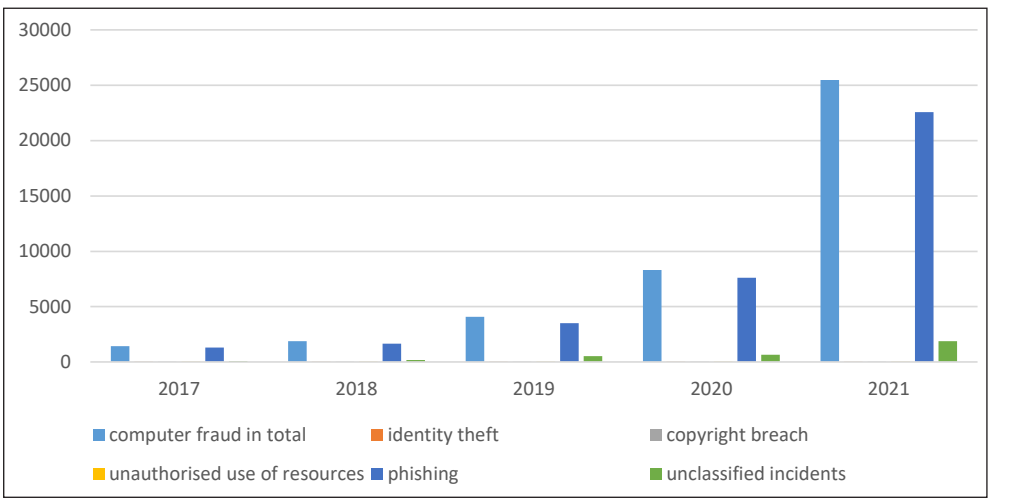
The reference period was characterised by a steady upward trend regarding the total number of incidents recorded by CERT Poland and the frequency of computer fraud. There were 3182 incidents recorded in 2017; 3739 incidents in 2018; 6484 incidents in 2019, and 10 420 incidents in 2020, following which the number increased to 29 483 in 2021, nearly twice as many as in the preceding year. The data for 2022 have not been made available yet. The statistics regarding computer fraud are as follows: 2017 – 1436 cases; 2018 – 1878 cases; 2019 – 4086 cases; 2020 – 8310 cases, and 2021 – 25 472 cases. There were 1 304 phishing incidents in 2017, and 1655 in 2018. While in 2019, this type of incident was mentioned in 3516 notifications and was recorded 7622 times in 2020, and the total number of phishing attacks recorded in 2021 was 22 572.



Source: Author, based on annual reports issued by CERT Poland between 2017 and 2021.

Fig. 1. Computer fraud (including phishing) recorded by CERT Poland between 2017 and 2021

In its reports, CERT Poland lists the following incident types classified as computer fraud: unauthorised use of resources, copyright breach, identity theft, phishing, and unclassified incidents. Phishing accounts for the highest number of computer fraud offences (phishing is the most frequently occurring incident among all incidents recorded).



Source: Author, based on annual reports issued by CERT Poland between 2017 and 2021.

Fig. 2. Types of computer fraud recorded by CERT Poland between 2017 and 2021

Computer fraud is an offence against property, committed with the purpose of financial gain or with the intent to cause damage to another person. It may assume the form of cybercrime if an ICT system has been used throughout its commission, in which case it poses a cybersecurity threat. The threat results from the interference with the automated processing, collection or transfer of computer data or the alteration, deletion or input of new computer data records.

International legislators define computer fraud, committed intentionally and without right, as causing another person to lose their property by 1) any input, alteration, deletion or suppression of computer data, 2) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or another person. Given the above, it can be stated that, in Art. 8 of the Convention, emphasis is placed on both computer data and computer systems.

Bibliography

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

Chałubińska-Jentkiewicz K., *Prawne granice dezinformacji w środkach społecznego przekazu*, Toruń 2023.

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.

Chałubińska-Jentkiewicz K., Nowikowska M., *Ochrona informacji w cyberprzestrzeni*, Warszawa 2020.

Chałubińska-Jentkiwiecz K., Nowikowska M., *Security v. Privacy – Legal Aspects*, Maribor 2021.

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

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.

Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.

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

Karpiuk M., *Cybersecurity-related responsibilities of the minister competent for computerisation*, „Cybersecurity and Law" 2022, no. 2.

Karpiuk M., *Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2.

Karpiuk M., *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.

Karpiuk M., *The executive agency as a legal organisational form of implementing cybersecurity tasks*, „Cybersecurity and Law" 2023, no. 1.

Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 3.
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.
Kodeks karny. Część szczególna. Komentarz do art. 278–283, eds. W. Wróbel, A. Zoll, Warszawa 2022.
Kodeks karny. Część szczególna. Komentarz, ed. J. Giezek, Warszawa 2021.
Kodeks karny. Komentarz, ed. M. Mozgawa, Warszawa 2015.
Kodeks karny. Komentarz, ed. T. Bojarski, Warszawa 2016.
Kodeks karny. Komentarz, ed. V. Konarska-Wrzosek, Warszawa 2020.
Korczyński R., Koszut R., *„Oszustwo" komputerowe*, „Prokuratura i Prawo" 2002, no. 2.
Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2021 z działalności CERT Polska, Warszawa 2022.
Krupa Ł., *Money laundering and cybercrime*, „Cybersecurity and Law" 2022, no. 2.
Lewulis P., *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, no. 3.
Milik P., Pilarski G., *Cyberattacks and the bank's liability for unauthorized payment transactions in the online banking system – theory and practice*, „Cybersecurity and Law" 2023, no. 1.
Nowikowska M., *The right to privacy in cyberspace* [in:] *Human Rights as a Guarantee of Smart, Sustainable and Inclusive Growth*, eds. I. Florek, I. Laki, Budapest 2022.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, no. 7–8.
Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, eds. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022.

Oszustwo komputerowe

Streszczenie

Jednym z określonych przez ustawodawcę przestępstw przeciwko mieniu jest przestępstwo oszustwa komputerowego. Popełniane jest ono w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody. Może być ono również zakwalifikowane jako cyberprzestępstwo, w przypadku posługiwania się systemami i sieciami informatycznymi, w tym wówczas, gdy podczas jego popełnienia dojdzie do wykorzystania systemu teleinformatycznego. Przestępstwo oszustwa komputerowego jest przedstawione również w ujęciu statystycznym, na podstawie danych z raportów rocznych dotyczących incydentów cyberbezpieczeństwa zarejestrowanych przez CERT Polska.

Słowa kluczowe: oszustwo komputerowe, cyberprzestępstwo, cyberprzestrzeń