Mirosław Karpiuk
Wydział Prawa i Administracji
Uniwersytet Warmińsko-Mazurski w Olsztynie
ORCID: 0000-0001-7012-8999
miroslaw.karpiuk@uwm.edu.pl

# Monitorowanie zagrożeń cyberbezpieczeństwa oraz incydentów na poziomie krajowym przez CSIRT NASK i CSIRT GOV

**Streszczenie**

W świecie cyfrowym znaczna część aktywności jest przeniesiona do sieci. Dotyczy to zarówno sfery prywatnej, jak i publicznej. Systemy teleinformatyczne odpowiadają dzisiaj za funkcjonowanie wielu sektorów, w tym mających istotne znaczenie dla gospodarki, a także zapewnienia bezpieczeństwa państwa. Wykonywanie zadań z wykorzystaniem cyberprzestrzeni musi być bezpieczne, dlatego zarówno na organach władzy publicznej, jak i na podmiotach prywatnych (operatorach usług kluczowych, dostawcach usług cyfrowych) ciąży obowiązek ochrony odpowiednich systemów teleinformatycznych przed cyberzagrożeniami. Ważne jest też odpowiednie zabezpieczenie infrastruktury krytycznej, do której działania wykorzystywane są takie systemy.

**Słowa kluczowe**

cyberbezpieczeństwo, cyberzagrożenia, incydenty cyberbezpieczeństwa, phishing

## Wstęp

Cyfryzacja poprzez implementację zaawansowanych technologii, w tym sztucznej inteligencji, przyczynia się do automatyzacji oraz optymalizacji procesów w różnych dziedzinach, od przemysłu po usługi publiczne. Tego rodzaju zmiany mają bezpośredni wpływ nie tylko na codzienne życie obywateli, lecz

także na efektywność funkcjonowania państw. Rozwój technologii komunikacyjnych, w tym szerokopasmowego dostępu do internetu, powoduje znoszenie barier geograficznych oraz społecznych, umożliwia tym samym większą integrację na poziomie międzynarodowym[1]. Niesie on również za sobą różne zagrożenia, które wymagają stosowania nowoczesnych narzędzi.

Dokonująca się obecnie transformacja cyfrowa wymaga zaangażowania wielu podmiotów zarówno ze sfery publicznej, jak i prywatnej, w tym prowadzenia odpowiedniej polityki przez państwo, które odpowiada za jej przebieg, zwłaszcza w sferze administracyjnej. Należy też zwrócić uwagę, że procesy zachodzące podczas transformacji cyfrowej są determinowane przez uwarunkowania międzynarodowe, nie można zatem wprowadzać stosownych zmian w tym zakresie w oderwaniu od polityki międzynarodowej czy rozwiązań prawno-międzynarodowych. Nowe technologie nie są domeną jednego państwa bądź kilku państw, ich zasięg jest globalny. Oddziałują one zarówno na gospodarkę międzynarodową, jak i sektor publiczny, który też musi się liczyć z uwarunkowaniami międzynarodowymi[2]. Ponieważ cyberprzestrzeń nie ogranicza się do jednego, konkretnego państwa, ale ma charakter globalny, zatem podejście do zagrożeń w niej występujących też musi mieć taki charakter. Inaczej działania nie będą tak skuteczne, żeby zapobiegać cyberatakom czy skutecznie je zwalczać.

Zagrożenia w cyberprzestrzeni powodują coraz częściej znaczne szkody (w tym w sferze publicznej), które mogą doprowadzić nawet do ograniczenia działania lub paraliżu ważnych dla bezpieczeństwa sektorów. Ustawodawca definiuje cyberprzestrzeń jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[3]. Cyberprzestrzeń to zbiór wszystkich fizycznych i technicznych środków pozwalających na elektroniczną relację, w tym użytkowników mających dostęp do jej zasobów. Całość tych zjawisk

**1** T. Wojciechowski, *Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego*, „Ius et Securitas" 2024, nr 1, s. 84.

**2** C. Gaie, M. Karpiuk, A. Spaziani, *New Technologies in Public Administration*, ibidem, nr 2, s. 50.

**3** Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, t.j., Dz.U. 2022, poz. 2091, z późn. zm., art. 2, ust. 1b.

dzieje się w jednoczesnej przestrzeni stanowiącej nowe pole ludzkich działań, gdzie są przenoszone zachowania oraz rozwiązania stosowane w świecie realnym[4].

W przypadku zarówno generowania cyberzagrożeń, jak i im przeciwdziałania należy zwrócić uwagę na sztuczną inteligencję. Z jednej strony może być ona używana jako narzędzie przeciwko społeczeństwom, stwarzające realne zagrożenia. Wrogie podmioty mogą wykorzystywać ją do prowadzenia operacji przestępczych, czyniąc je bardzo wydajnymi. Z drugiej, sztuczna inteligencja może stać się ważnym elementem obronnym, pełnić istotną funkcję analityczną, umożliwiać szybką identyfikację i zwalczanie zagrożeń[5]. Pomimo ogromnego potencjału sztucznej inteligencji i korzyści, jakie ona niesie, nie należy zapominać o zachowaniu równowagi między postępem technologicznym a ochroną prywatności i prawami człowieka. Wprowadzając ją, należy mieć na względzie aspekty etyczne i społeczne, żeby ta technologia służyła wspólnym interesom i nie naruszała podstawowych praw i wolności[6].

## Incydenty cyberbezpieczeństwa. Studium przypadku

Polski ustawodawca cyberbezpieczeństwo definiuje jako odporność systemów informacyjnych na działania, które naruszają poufność, integralność, dostępność oraz autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[7]. Według prawodawcy Unii Europejskiej cyberbezpieczeństwo oznacza działania, które są niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów, a także innych osób przed cyberzagrożeniami. Cybrzagrożenie to z kolei wszelkie potencjalne okoliczności, zdarzenia lub działania, które mogą wyrządzić szkodę, spowodować zakłócenia bądź też w inny sposób niekorzystnie wpłynąć na

**4** K. Chałubińska-Jentkiewicz, *Cyberprzestrzeń*, [w:] *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz, Warszawa 2024, s. 90.

**5** T. Gergelewicz, *Bipolarity of Artificial Intelligence – Chances and Threats*, „Ius et Securitas" 2024, nr 2, s. 91.

**6** K. Kaczmarek, M. Karpiuk, U. Soler, *The Potential Use of Artificial Intelligence in Crisis Management*, „Sicurezza, Terrorismo e Società" 2024, nr 2, s. 149.

**7** Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j., Dz.U. 2024, poz. 1077, z późn. zm., art. 2, pkt 4.

sieci i systemy informatyczne, użytkowników takich systemów oraz inne osoby[8]. Cyberbezpieczeństwo jest pojęciem związanym z zapewnieniem ochrony i przeciwdziałaniem zagrożeniom, które dotyczą samej cyberprzestrzeni, a także funkcjonowania w niej, co odnosi się do sektora zarówno publicznego, jak i prywatnego oraz ich wzajemnych relacji[9].

Incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Definicja ta wynika z art. 2 pkt 5 ustawy z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (u.k.s.c.). Incydent nie jest tożsamy z zagrożeniem cyberbezpieczeństwa, gdyż to drugie pojęcie, według art. 2 pkt 17 u.k.s.c., oznacza potencjalną przyczynę wystąpienia incydentu.

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, który działa na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (CSIRT NASK) monitoruje w Polsce incydenty cyberbezpieczeństwa. Odpowiada za ich obsługę w sieciach publicznych[10].

**8** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz. Urz. UE 2019, L 151/15, art. 2, pkt 1, 8.

**9** K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo*, [w:] *Leksykon*…, s. 63. Na temat cyberbezpieczeństwa zob. także: K. Kaczmarek, *Finland in the light of cyber threats in the context of Russia's aggression against Ukraine*, „Cybersecurity and Law" 2023, nr 1, s. 212; M. Czuryk, *The legal status of digital service providers in the national cybersecurity system*, ibidem 2024, nr 1, s. 39–46; M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity management – current state and directions of change*, „International Journal of Legal Studies" 2023, nr 2, s. 646; K. Kaczmarek, *Nordic countries in the face of digital threats*, „Cybersecurity and Law" 2024, nr 1, s. 152; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, nr 3, s. 31–43; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, nr 2, s. 57–72; K. Kaczmarek, *Vulnerability to cyber threats: a qualitative analysis from societal and institutional perspectives*, ibidem 2024, nr 2, s. 108–109; E.M. Włodyka, K. Kaczmarek, *Cyber Security of Electrical Grids – A Contribution to Research*, ibidem, nr 2, s. 262–263; M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, nr 5, s. 43–52; A. Bencsik, M. Karpiuk, *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, nr 1, s. 82–94.

**10** F. Radoniewicz, *CSIRT NASK*, [w:] *Leksykon*…, s. 49.

Tabela1. Incydenty cyberbezpieczeństwa zarejestrowane w latach 2019–2023 przez CSIRT NASK

| | |
|---|---|
| 2023 | 80 267 |
| 2022 | 39 683 |
| 2021 | 29 483 |
| 2020 | 10 420 |
| 2019 | 6 484 |

Źródło: *Raport roczny z działalności CERT Polska*, Warszawa 2024, s. 102.

W 2023 roku najczęściej występującym typem incydentów zarejestrowanych były strony phishingowe. Od lat phishing zajmuje pierwsze miejsce na liście incydentów cyberbezpieczeństwa. CSIRT NASK zarejestrował 41 423 tego typu incydenty, i stanowiły one 51,61% wszystkich obsłużonych incydentów. Najgroźniejsze kampanie phishingowe wykorzystywały wizerunek serwisu aukcyjnego Allegro – 11 161 zgłoszonych incydentów, serwisu społecznościowego Facebook – 5308 incydentów, oraz serwisu sprzedażowego OLX – 4753 przypadki. Następne w kolejności były oszustwa komputerowe – 34 304 przypadki, które stanowiły ponad 42% wszystkich zarejestrowanych incydentów. Wśród nich odnotowano fałszywe sklepy internetowe, a także oszustwa finansowe związane z podszywaniem się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy oraz instytucje. Trzecim typem incydentów, które według CSIRT NASK występowały najczęściej w 2023 roku, było szkodliwe oprogramowanie. Tego typu incydentów zarejestrowano 1650. Było to o połowę mniej niż w roku poprzednim. Ten rodzaj incydentów obejmował nie tylko infekcje oprogramowaniem ransomware, ale też kampanie spamowe, które dystrybuowały oprogramowanie Remcos i Agent Tesla[11].

CSIRT NASK obsłużył 40 incydentów, które uznano za poważne[12]. Incydent poważny, według art. 2 pkt 7 u.k.s.c., to ten, który powoduje lub może spowodować poważne obniżenie jakości bądź przerwanie ciągłości świadczenia usługi kluczowej.

W 2023 roku CSIRT NASK obsłużył 2184 incydenty, które dotyczyły podmiotów publicznych. Najczęściej rejestrowane incydenty, które uznano jako incydenty w podmiocie publicznym, miały miejsce w sektorze administracji publicznej – 1206, w sektorze oświaty i wychowania – 282, oraz w ochronie zdrowia – 231[13].

**11** *Raport roczny z działalności CERT Polska*, Warszawa 2024, s. 102.
**12** Ibidem, s. 103.
**13** Ibidem, s. 104.

Tabela 2. Najczęstsze cele phishingu w 2023 roku według CSIRT NASK

| Poz. | Cel phishingu | Liczba domen 2023 r. | Liczba domen 2022 r. |
|---|---|---|---|
| 1 | Inwestycje | 20 609 | 2 443 |
| 2 | Allegro | 11 015 | 643 |
| 3 | Baltic Pipe | 6 971 | 583 |
| 4 | Facebook | 6 638 | 7 186 |
| 5 | OLX | 4 564 | 1 656 |
| 6 | InPost | 2 770 | 6 728 |
| 7 | PGNiG | 2 764 | 309 |
| 8 | Tesla | 2 758 | 2 647 |
| 9 | Netflix | 1 495 | 1 231 |
| 10 | Webmail | 1 325 | 562 |

Źródło: *Raport…*, s. 88.

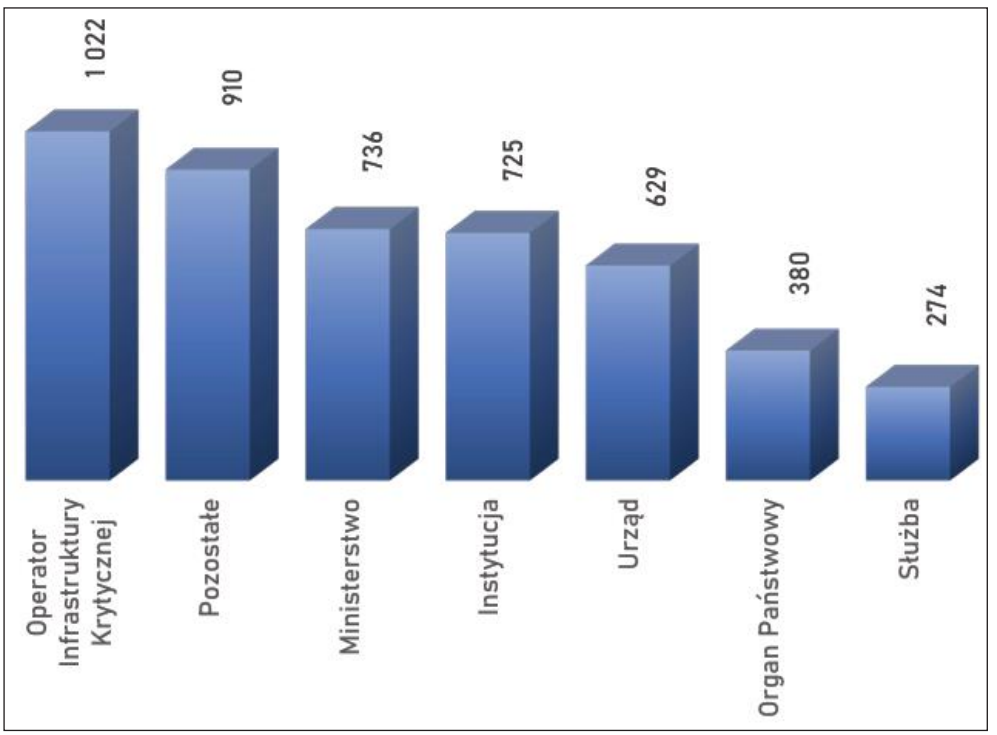
Incydent w podmiocie publicznym, według art. 2 pkt 9 u.k.s.c., to ten, który powoduje bądź też może spowodować obniżenie jakości lub przerwanie wykonania zadania publicznego przez podmiot publiczny.

Tabela 3. Incydenty cyberbezpieczeństwa zarejestrowane w 2023 roku przez CSIRT NASK z podziałem na sektory gospodarki

| Sektor gospodarki | Liczba incydentów | Procent wszystkich |
|---|---|---|
| Handel hurtowy i detaliczny | 19 253 | 23,99 |
| Infrastruktura rynków finansowych | 18 943 | 23,61 |
| Media | 10 191 | 12,70 |
| Energetyka | 9 196 | 11,46 |
| Poczta i usługi kurierskie | 5 319 | 6,63 |
| Infrastruktura cyfrowa | 5 101 | 6,35 |
| Bankowość | 2 481 | 3,09 |
| Produkcja | 2 353 | 2,93 |
| Administracja publiczna | 2 234 | 2,78 |
| Osoby fizyczne | 2 105 | 2,62 |
| Usługi inne | 902 | 1,12 |
| Transport | 492 | 0,61 |
| Inne | 451 | 0,56 |
| Ochrona zdrowia | 405 | 0,50 |
| Oświata i wychowanie | 354 | 0,44 |
| Hotele, restauracje, catering | 153 | 0,19 |

Źródło: *Raport…*, s. 102.

W Polsce zespołem reagowania na incydenty bezpieczeństwa komputerowego, prowadzonym przez Szefa Agencji Bezpieczeństwa Wewnętrznego, jest CSIRT GOV. Jest to zespół koordynujący obsługę incydentów, które są zgłaszane przez podmioty należące do administracji rządowej, Narodowy Bank Polski, Bank Gospodarstwa Krajowego. CSIRT GOV odpowiada za rozpoznawanie, zapobieganie oraz wykrywanie zagrożeń godzących w bezpieczeństwo systemów teleinformatycznych należących do organów administracji publicznej lub systemów i sieci teleinformatycznych, które wchodzą w skład infrastruktury krytycznej[14].

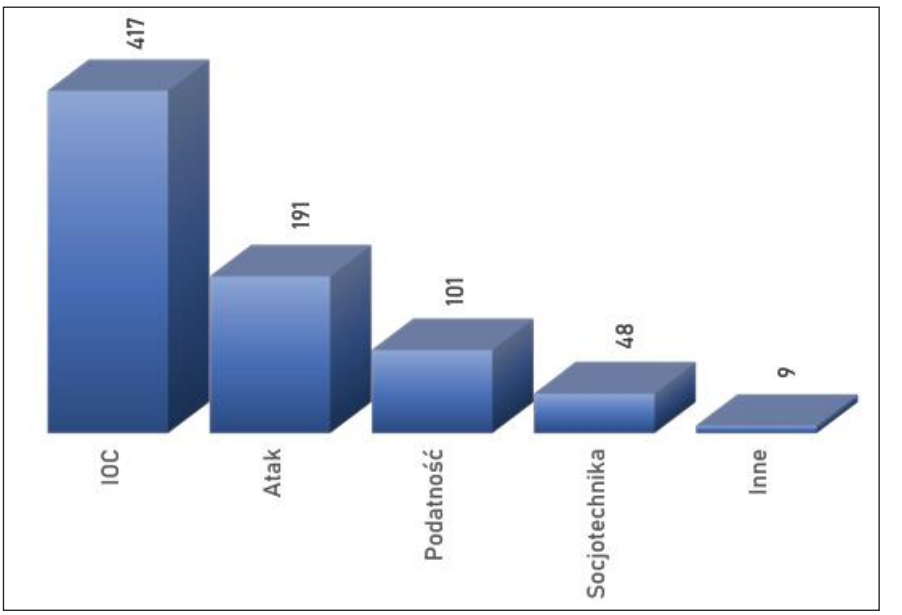



Źródło: *Raport*…, s. 13.

Wykres 1. Liczba incydentów zgłoszonych do CSIRT GOV w 2023 roku z podziałem na sektory

**14** F. Radoniewicz, *CSIRT GOV*, [w:] *Leksykon*…, s. 47.

W art. 26 ust. 3 pkt 1 i 4 u.k.s.c. prawodawca wyraźnie wskazuje, że do zadań zespołów CSIRT, w tym CSIRT GOV, należy monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym, a także wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Zadania te CSIRT GOV wykonuje m.in. przez wydawanie ostrzeżeń.




Źródło: *Raport*…, s. 15.

Wykres 2. Ostrzeżenia wydane przez CSIRT GOV z podziałem na kategorie

Wydawanie przez CSIRT GOV ostrzeżeń dotyczących incydentów cyberbezpieczeństwa ma charakter prewencyjny. Ma na celu ograniczać ich występowanie, a także edukować osoby korzystające z internetu z zachowania zasad cyberhigieny.

## Zakończenie

W związku z szybko postępującą transformacją cyfrową oraz siecią wzajemnych połączeń w społeczeństwie, w tym w zakresie wymiany transgranicznej, sieci i systemy informatyczne stały się podstawowym elementem codziennego życia. Doprowadziło to do ewolucji krajobrazu cyberzagrożeń, ale i przyniosło nowe wyzwania wymagające dostosowanych, skoordynowanych, a także

innowacyjnych reakcji we wszystkich państwach członkowskich Unii Europejskiej. Liczba, zasięg, zaawansowanie, a także częstotliwość oraz wpływ incydentów cyberbezpieczeństwa stają się coraz większe, a przy tym poważnie zagrażają funkcjonowaniu sieci i systemów informatycznych. W efekcie mogą one utrudniać prowadzenie działalności gospodarczej na rynku wewnętrznym, powodować straty finansowe, podważać zaufanie użytkowników, a także powodować poważne szkody dla gospodarki i społeczeństwa. W związku z powyższym gotowość oraz skuteczność w sferze cyberbezpieczeństwa są coraz ważniejsze dla prawidłowego funkcjonowania rynku wewnętrznego. W wielu sektorach krytycznych cyberbezpieczeństwo należy do podstawowych czynników umożliwiających udany przebieg transformacji cyfrowej oraz pełne wykorzystanie zarówno ekonomicznych, jak i społecznych korzyści wynikających z cyfryzacji[15].

Należy pamiętać że każda nowa technologia stanowi nie tylko ułatwienie, lecz także niesie za sobą zagrożenia. Współcześnie, w dobie kulturowych przemian społecznych, napływu najnowszych technologii oraz wszechobecnej sieci, bez internetu bardzo trudno byłoby funkcjonować. Należy podkreślić, że brak ostrożności w korzystaniu z niego powoduje ryzyko cyberataku, cyberprzemocy, wykorzystania wizerunku czy też phishingu. Zainfekowana sieć może wyłączyć z użytku serwery i podłączone do nich komputery. Dostępność internetu to zachęta dla przestępców do szpiegostwa przemysłowego czy wykradania danych. Atrakcyjność wirtualnego świata powoduje, że bardzo dużym problemem jest uzależnienie od internetu, które skutkuje rozpadem więzi społecznych, chorobami, a także dysfunkcją społeczną[16].

Niektóre systemy teleinformatyczne odpowiadają za stabilność państwa i jego gospodarki, dlatego muszą być należycie chronione[17]. Ochrona ta powinna zabezpieczać przed nieuprawnioną ingerencją ograniczającą ich funkcjonowanie, ponieważ może poważnie zagrażać bezpieczeństwu państwa,

**15** Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz. Urz. UE 2022, L 333/80, motyw 3.

**16** B. Grabowski, *Cyfrowe zagrożenia – zarys problemu*, „Ius et Securitas" 2024, nr 1, s. 103.

**17** A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, s. 89–90.

a także powodować duże szkody w gospodarce. Szczególna ochrona powinna obejmować systemy, które odpowiadają za funkcjonowanie infrastruktury krytycznej zabezpieczającej podstawowe sektory decydujące o stabilności państwa.

## Bibliografia


Bencsik A., Karpiuk M., *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, nr 1.

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

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo*, [w:] *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz , Warszawa 2024.

Chałubińska-Jentkiewicz K., *Cyberprzestrzeń*, [w:] *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz, Warszawa 2024.

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, nr 5.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, nr 3.

Czuryk M., *The legal status of digital service providers in the national cybersecurity system*, „Cybersecurity and Law" 2024, nr 1.

Gaie C., Karpiuk M., Spaziani A., *New Technologies in Public Administration*, „Ius et Securitas" 2024, nr 2.

Gergelewicz T., *Bipolarity of Artificial Intelligence – Chances and Threats*, „Ius et Securitas" 2024, nr 2.

Grabowski B., *Cyfrowe zagrożenia – zarys problemu*, „Ius et Securitas" 2024, nr 1.

Kaczmarek K., *Finland in the light of cyber threats in the context of Russia's aggression against Ukraine*, „Cybersecurity and Law" 2023, nr 1.

Kaczmarek K., Karpiuk M., Soler U., *The Potential Use of Artificial Intelligence in Crisis Management*, „Sicurezza, Terrorismo e Società" 2024, nr 2.

Kaczmarek K., *Nordic countries in the face of digital threats*, „Cybersecurity and Law" 2024, nr 1.

Kaczmarek K., *Vulnerability to cyber threats: a qualitative analysis from societal and institutional perspectives*, „Cybersecurity and Law" 2024, nr 2.

Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity management – current state and directions of change*, „International Journal of Legal Studies" 2023, nr 2.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, nr 2.

Radoniewicz F., *CSIRT GOV*, [w:] *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz, Warszawa 2024.

Radoniewicz F., *CSIRT NASK*, [w:] *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz, Warszawa 2024.
Włodyka E.M., Kaczmarek K., *Cyber Security of Electrical Grids – A Contribution to Research*, „Cybersecurity and Law" 2024, nr 2.
Wojciechowski T., *Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego*, „Ius et Securitas" 2024, nr 1.

## Monitoring Cybersecurity Threats and Incidents at the National Level by CSIRT NASK and CSIRT GOV

**Abstract**

In the digital world, a significant part of the activity is transferred to the network. This applies to both the private and public spheres. Today, IT systems are responsible for the functioning of many sectors, including those that are of significant importance to the economy and ensuring state security. Performing tasks using cyberspace must be safe, which is why both public authorities and private entities (operators of key services, digital service providers) are obliged to protect the appropriate IT systems from cyber threats. It is also important to properly secure the critical infrastructure for which such systems are used.

**Keywords**

cybersecurity, cyber threats, cybersecurity incidents, phishing