Konferencja

LEKSYKON CYBERBEZPIECZEŃSTWA

Warszawa, 31 lipca 2020

Sesja 2

Definicje prawne związane z krajowym systemem cyberbezpieczeństwa

Słowniki w wielopoziomowej regulacji

prof. dr hab. Grażyna Szpor

Uniwersytet Kardynała Stefana Wyszyńskiego

Wielopoziomowa regulacja cyberbezpieczeństwa

- Prawo międzynarodowe

Rezolucje Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych, które są zaleceniami adresowanymi do państw członkowskich, nie zawierającymi norm prawnie wiążących, m.in.: 45/121 z 14.12.1990 r. nr 56/121 z 19.12.2001 r., nr 58/199 z 23.12.2003 r, nr 64/211 z 21.12.2009 r.

Konwencja Rady Europy o cyberprzestępczości sporządzona 23.11.2001 r. w Budapeszcie - regionalny akt prawa międzynarodowego

- Prawo Unii Europejskiej

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

- Prawo krajowe

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Zasady techniki prawodawczej dotyczące terminologii

Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej”
§ 21. 1. W przepisach ogólnych zamieszcza się objaśnienia użytych w ustawie określeń i skrótów.

§ 146. 1. W ustawie lub innym akcie normatywnym formułuje się definicję danego określenia, jeżeli:

1) dane określenie jest wieloznaczne;

2) dane określenie jest nieostre, a jest pożądane ograniczenie jego nieostrości;

3) znaczenie danego określenia nie jest powszechnie zrozumiałe;

4) ze względu na dziedzinę regulowanych spraw istnieje potrzeba ustalenia nowego znaczenia danego określenia.

2. Jeżeli określenie wieloznaczne występuje tylko w jednym przepisie prawnym, jego definicję formułuje się tylko w przypadku, gdy wieloznaczności nie eliminuje zamieszczenie go w odpowiednim kontekście językowym.

§ 147. 1. Jeżeli w ustawie lub innym akcie normatywnym ustalono znaczenie danego określenia w drodze definicji, w obrębie tego aktu nie wolno posługiwać się tym określeniem w innym znaczeniu.

2. Jeżeli zachodzi konieczność odstąpienia od zasady wyrażonej w ust. 1, wyraźnie podaje się inne znaczenie danego określenia i ustala się jego zakres odniesienia.

[Dz.U.2016.283 t.j.]

Słownik w ustawie o krajowym systemie cyberbezpieczeństwa

Art. 2. [Definicje legalne]
Użyte w ustawie określenia oznaczają:
1)CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
2)CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;
3)CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
4)cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

Słownik w ustawie o krajowym systemie cyberbezpieczeństwa

Art. 2. [Definicje legalne] Użyte w ustawie określenia oznaczają:
5)incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
6)incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;
7)incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;
8)incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151”;
9)incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym w art. 4 pkt 7–15

Słownik w ustawie o krajowym systemie cyberbezpieczeństwa

Art. 2. [Definicje legalne]
Użyte w ustawie określenia oznaczają:
10)obsługa incydentu – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;
11)podatność – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa
12)ryzyko – kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
13)szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka;
14)system informacyjny – system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z przetwarzanymi w nim danymi w postaci elektronicznej;

Słownik w ustawie o krajowym systemie cyberbezpieczeństwa

Art. 2. [Definicje legalne]
Użyte w ustawie określenia oznaczają:
15)usługa cyfrowa – usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z 18.07.2002r. o świadczeniu usług drogą elektroniczną, wymienioną w załączniku nr 2 do ustawy;
16)usługa kluczowa – usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych;
17)zagrożenie cyberbezpieczeństwa – potencjalną przyczynę wystąpienia incydentu;
18)zarządzanie incydentem – obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;
19)zarządzanie ryzykiem – skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.

Wykładnia = interpretacja

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz. Warszawa 2019

Redakcja naukowa:
K. Czaplicki, A. Gryszczyńska, G. Szpor

Autorzy: Kamil Czaplicki, Piotr Drobek, , Agnieszka Gryszczyńska, Katarzyna Prusak-Górniak, Krzysztof Silicki, Krzysztof Świtała, Bolesław Szafrański, Grażyna Szpor, Martyna Wilbrandt-Gotowicz