CYBERBEZPIECZEŃSTWO

Zarys wykładu

redakcja naukowa Cezary Banasiński

Cezary Banasiński, Cezary Błaszczyk, Jacek M. Chmielewski
Władysław Hydzik, Dariusz Jagiełło, Filip Krzyżankiewicz
Arwid Mednis, Włodzimierz Nowak, Marcin Rojszczak
Adam Szafrański, Ryszard Szpyra, Kazimierz Waćkowski
Paweł Widawski, Joanna Worona, Zofia Zawadzka

SERIA AKADEMICKA

Wolters Kluwer

Str. 30 Cezary Banasiński (red.), *Cyberbezpieczeństwo*. Zarys wykładu

Rozdział I. Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni

Trudności w zdefiniowaniu **bezpieczeństwa** przekładają się na możliwość jednoznacznego określenia **bezpieczeństwa w cyberprzestrzeni (cyberbezpieczeństwa)**. Występują w tym wypadku dwa pojęcia niedookreślone - bezpieczeństwa i cyberprzestrzeni. W literaturze podnosi się wręcz, że skoro wątpliwe jest wyodrębnienie - z technicznego punktu widzenia - samej przestrzeni cybernetycznej, to trudno mówić o potrzebie bezpieczeństwa i możliwościach ochrony takiego hipotetycznego tworu[57]. Niemniej w literaturze, podobnie jak w aktach prawnych oraz oficjalnych dokumentach, podejmowane są próby zdefiniowania tego pojęcia.

Przykładowo **definicja bezpieczeństwa cybernetycznego** zaproponowana przez **National Initiative for Cybersecurity Careers and Studies (NICCS)** - będącą organizacją zarządzaną przez Wydział Edukacji i Świadomości Cyberbezpieczeństwa (usytuowany w Departamencie Bezpieczeństwa Wewnętrznego Urzędu Cyberbezpieczeństwa i Komunikacji Rządu Federalnego USA) - określana jest jako sytuacja gwarantująca, że „(...) systemy informacyjne lub komunikacyjne oraz informacja zawarta w nich są zabezpieczone czy chronione przed uszkodzeniem, nieautoryzowanym użyciem, modyfikacją bądź wykorzystaniem”[58]. Ta sama instytucja zaproponowała też **szeroką definicję cyberbezpieczeństwa**, jako „strategię, politykę i normy dotyczące zarówno bezpieczeństwa cyberprzestrzeni, jak i działania w niej, obejmujące z jednej strony pełen zakres czynności ukierunkowanych na redukcję zagrożeń, zmniejszenie podatności na nie i odstraszanie, międzynarodowe zaangażowanie, reagowanie na zdarzenia, zaś z drugiej - elastyczną politykę prewencyjną, uwzględniającą odpowiednie operacje w sieci komputerowej, zapewnienie informacji, działania organów ścigania, dyplomacji, wojska, służb wywiadowczych, odnoszące się do bezpieczeństwa i stabilności globalnej infrastruktury informacyjnej i komunikacyjnej”[59].

Z kolei **Międzynarodowy Związek Telekomunikacyjny w Rekomendacji ITU-T X.1205 definiuje cyberbezpieczeństwo** jako „zbiór narzędzi, polityk, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, metod zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk, zapewnień i technologii, które mogą być wykorzystywane do ochrony środowiska cybernetycznego oraz organizacja i zasoby użytkownika. Organizacja i zasoby użytkownika obejmują podłączone urządzenia komputerowe, personel, infrastrukturę, aplikacje, usługi, systemy telekomunikacyjne oraz całość przekazanych i/lub przechowywanych informacji w środowisku cybernetycznym. Cyberbezpieczeństwo dąży do zapewnienia osiągnięcia i utrzymania właściwości bezpieczeństwa organizacji i zasobów użytkownika względem odpowiednich zagrożeń bezpieczeństwa w środowisku cybernetycznym”.

---

57 D. Lisiak-Felicka, M. Szmit, Cyberbezpieczeństwo administracji..., s. 49.

58 Za Z. Chmielewski, Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich, „Studia z Polityki Publicznej" 2016/2(10), s. 108.

59 Z. Chmielewski, Polityka publiczna w zakresie..., s. 108.

31

Ogólne cele bezpieczeństwa obejmują dostępność, integralność (która może obejmować uwierzytelnianie i niezaprzeczalność) oraz poufność[60]. W istocie Zalecenie to zawiera taksonomię zagrożeń bezpieczeństwa z punktu widzenia organizacji.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 utożsamia **pojęcie cyberbezpieczeństwa** z bezpieczeństwem sieci i systemów informatycznych oraz bezpieczeństwem teleinformatycznym, traktując je jako synonimy oznaczające „odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne". Definicja ta odzwierciedla postanowienia **normy międzynarodowej ISO/IEC 27032**, w której definiuje się bezpieczeństwo w cyberprzestrzeni jako zachowanie poufności, dostępności i integralności, aczkolwiek zaznacza się, że możliwe jest uwzględnienie również innych właściwości bezpieczeństwa informacji, takich jak: „autentyczność, rozliczalność, niezaprzeczalność i niezawodność w cyberprzestrzeni". Norma ISO/IEC 27032, zawierając zbiór rekomendacji przeznaczonych dla dostawców usług internetowych, siłą rzeczy nie odnosi się natomiast do ochrony cybernetycznej (cybersafety), czyli zapobiegania skutkom negatywnych zdarzeń, które mogą wystąpić w efekcie korzystania z technik informacyjnych. Zdecydowanie szerzej podchodzi do tej kwestii **ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa**[61], która, wykorzystując normę ISO/IEC 27032, definiuje pojęcie cyberbezpieczeństwa jako „odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".

Jeszcze inaczej podchodzi do tego zagadnienia **Doktryna cyberbezpieczeństwa RP z 2015 r.**, która wyodrębnia cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni), traktując je jako proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni oraz bezpieczeństwo cyberprzestrzeni RP, rozumiane jako część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych.

---

60 https://www.ccdcoe.org/sites/default/files/documents/ITU-080418-RecomOverviewOfCS.pdf (dostęp: 20.08.2018 r.).

61 Dz.U. z 2018 r. poz. 1560.