complex projects: how system dynamics can help, [w:] *Encyclopedia of Complexity and Systems Science*, R. Meyers (ed.), Springer Verlag, Berlin 2009;A. Jastrzębska, W. Jastrzębska, *Wykluczenie cyfrowe – przyczyny, zagrożenia i bariery jego pokonania. Studium przypadku*, „Nierówności Społeczne a Wzrost Gospodarczy" 2012, nr 25; *Wykluczenie cyfrowe w Polsce*, https://www.senat.gov.pl/gfx/senat/pl/senatopracowania/133/plik/ot-637_internet.pdf (dostęp 21.04.2019).

ORGANY WŁAŚCIWE DO SPRAW CYBERBEZPIECZEŃSTWA – zostały określone w art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie → cyberbezpieczeństwa [t. 1]. Dla poszczególnych sektorów ustawodawca przewidział osiem organów właściwych do spraw cyberbezpieczeństwa. Za sektor energetyczny odpowiada minister do spraw energii, za sektor transportu – minister do spraw transportu, natomiast za sektor transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej. Z kolei dla sektora bankowego i infrastruktury rynków finansowych za organ właściwy do spraw cyberbezpieczeństwa uznano Komisję Nadzoru Finansowego. Dla sektora ochrony zdrowia – ministra zdrowia, dla sektora zaopatrzenia w wodę pitną i jej dystrybucji – ministra gospodarki wodnej. Za sektor infrastruktury cyfrowej w zakresie cyberbezpieczeństwa są odpowiedzialni minister do spraw informatyzacji oraz minister obrony narodowej. Dla dostawców usług cyfrowych za organy właściwe do spraw bezpieczeństwa w → cyberprzestrzeni [t. 1] uznano ministra do spraw informatyzacji oraz ministra obrony narodowej.

Na wspomniane organy zostały nałożone ustawowo konkretne obowiązki, polegające m.in. na: bieżącej analizie podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej; wydawaniu decyzji o uznaniu podmiotu za operatora usługi kluczowej bądź stwierdzaniu wygaśnięcia decyzji o uznaniu podmiotu za operatora usługi kluczowej; przekazywaniu wniosków do ministra właściwego do spraw informatyzacji o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu; składaniu wniosków o zmianę danych w wykazie operatorów usług kluczowych nie później niż w terminie 6 miesięcy od zmiany tychże danych; przygotowywaniu

(we współpracy z CSIRT NASK, CSIRT GOV, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa) rekomendacji na temat działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytycznych sektorowych w sprawie zgłaszania incydentów; monitorowaniu stosowania przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych. Ponadto organy do spraw cyberbezpieczeństwa: wzywają (na wniosek CSIRT NASK, CSIRT GOV lub CSIRT MON) operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie błędów, które doprowadziły lub mogły doprowadzić do incydentu; sprawują kontrolę nad operatorami usług kluczowych i dostawcami usług cyfrowych; mają możliwość współpracowania z właściwymi organami państw członkowskich Unii Europejskiej poprzez Pojedynczy Punkt Kontaktowy; przetwarzają →informacje [t. 1] (np. dane osobowe) o świadczonych usługach kluczowych i usługach cyfrowych oraz na temat operatorów usług kluczowych lub dostawców usług cyfrowych w zakresie niezbędnym do realizacji zadań wynikających z ustawy; uczestniczą w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych zarówno w Polsce, jak i w innych państwach członkowskich Unii Europejskiej. Wspomniane zadania organy właściwe do spraw cyberbezpieczeństwa mogą zlecać (na podstawie porozumienia) do realizacji jednostkom podległym lub nadzorowanym. W takim przypadku wymagane jest określenie zasad sprawowania przez organ właściwy do spraw cyberbezpieczeństwa kontroli nad prawidłowym wykonywaniem powierzonych zadań.

Warto również wspomnieć, że organy właściwe do spraw cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy w uzasadnionych przypadkach podejmują współpracę z organami ścigania, a także z organem właściwym do spraw ochrony danych osobowych.

Organ właściwy do spraw cyberbezpieczeństwa może, bez wszczynania postępowania w sprawie uznania podmiotu za operatora usługi kluczowej, wystąpić do podmiotu, o którym mowa w załączniku nr 1 do ustawy o →krajowym systemie cyberbezpieczeństwa [t. 1], o udzielenie informacji, które zweryfikują, czy dany podmiot spełnia warunki do uznania go za operatora usługi kluczowej.

Organ właściwy do spraw bezpieczeństwa w cyberprzestrzeni ma również możliwość, bez wszczynania kontroli, wystąpić do operatora usługi

kluczowej o udzielenie informacji, które umożliwią ustalenie potrzeby przeprowadzania kontroli, a także może, bez wszczynania postępowania, wystąpić do operatora usługi kluczowej o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot przestał spełniać warunki do uznania go za operatora usługi kluczowej.

Na mocy art. 44 ust. 1 organ właściwy do spraw cyberbezpieczeństwa może ustanowić, zgodnie z odrębnymi przepisami, sektorowy zespół cyberbezpieczeństwa dla danego sektora lub podsektora. Taki zespół przyjmuje zgłoszenia o incydentach poważnych oraz wspiera w obsłudze tych incydentów, wspiera operatorów usług kluczowych, podejmuje analizę incydentów poważnych, wyszukuje powiązania pomiędzy incydentami, a także opracowuje wnioski i wydaje rekomendacje w związku z obsługą incydentu, współpracuje również z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych. W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa organ właściwy do spraw cyberbezpieczeństwa informuje operatorów usług kluczowych w danym sektorze oraz CSIRT MON, CSIRT NASK i CSIRT GOV o ustanowieniu takiego zespołu i zakresie realizowanych zadań.

Julia Anna Gawęcka

Krajowy system cyberbezpieczeństwa, https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa- (dostęp 25.03.2019); *Krajowy system cyberbezpieczeństwa*, https://www.ksoin.pl/krajowy-system-cyberbezpieczenstwa-dla-operatorow-uslug-kluczowych-szkolenie/ (dostęp 26.03.2019); M. Maj, *Pięć kluczowych wyzwań przy wdrożeniu Ustawy o krajowym systemie cyberbezpieczeństwa*, https://www.cybsecurity.org/pl/piec-kluczowych-wyzwan-przy-wdrozeniu-ustawy-o-krajowym-systemie-cyberbezpieczenstwa/ (dostęp 23.03.2019); *Organy właściwe*, https://www.gov.pl/web/cyfryzacja/organy-wlasciwe (dostęp 26.03.2019); Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r., poz. 1560.