OPOLSKIE STUDIA ADMINISTRACYJNO-PRAWNE XVI/1(4)
UNIWERSYTET OPOLSKI OPOLE 2018

Martyna WILBRANDT-GOTOWICZ*

Wielopostaciowość form działania administracji publicznej na przykładzie wymogu implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

Wprowadzenie

W działalności administracji publicznej akcentuje się takie cele jak: optymalizacja procedur, transparentność, efektywność oraz wydajność[1]. Ich realizacji sprzyja elastyczność form działania i dostosowanie do rodzaju wykonywanych zadań czy rozstrzyganych spraw. Szczególnym wyzwaniem na tym tle stają się sfery, w których ochrona interesu publicznego (społecznego) wymaga uwzględnienia zagadnień o wysokim stopniu złożoności technologicznej, szybkiego i adekwatnego reagowania na zagrożenia oraz ukształtowania efektywnych mechanizmów współpracy między podmiotami publicznymi i prywatnymi. Jednym z takich obszarów jest bezpieczeństwo cybernetyczne, które stało się przedmiotem regulacji w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci

* Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Wydział Prawa i Administracji, e-mail: m.gotowicz@uksw.edu.pl.

[1] Por. np. T.T. Koncewicz, *Aksjologia unijnego kodeksu proceduralnego*, Warszawa 2010, s. 267 i n.

i systemów informatycznych na terytorium Unii (dalej: dyrektywa NIS)[2]. W artykule przybliżono różnorodność form działania administracji właściwą efektywnej transpozycji tej dyrektywy do prawa polskiego. W analizie uwzględniono projekt ustawy o krajowym systemie cyberbezpieczeństwa opracowany w Ministerstwie Cyfryzacji (dalej: projekt)[3]. Przyjęto przy tym perspektywę wewnętrzną działalności podmiotów krajowego systemu cyberbezpieczeństwa, nie zaś współpracy horyzontalnej – między podmiotami z różnych państw członkowskich – czy wertykalnej – między podmiotami krajowymi a administracją unijną.

Założenia dyrektywy NIS

Podstawowym celem wskazanym w art. 1 ust. 1 dyrektywy NIS jest „osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego". Dla jego realizacji dyrektywa:

a) ustanawia obowiązki dla wszystkich państw członkowskich dotyczące przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych;

b) tworzy grupę współpracy, aby wspierać i ułatwiać strategiczne współdziałanie i wymianę informacji między państwami członkowskimi oraz rozwijać wśród nich zaufanie i pewność;

c) tworzy sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (sieć CSIRT), aby przyczyniać się do rozwijania zaufania między państwami członkowskimi oraz promować szybką i skuteczną współpracę operacyjną;

d) ustanawia wymogi dotyczące bezpieczeństwa i zgłaszania incydentów dla operatorów usług kluczowych i dostawców usług cyfrowych;

e) ustanawia obowiązki dla państw członkowskich dotyczące wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz CSIRT mających zadania związane z bezpieczeństwem sieci i systemów informatycznych[4].

W dyrektywie wielokrotnie wskazuje się na obowiązki państw członkowskich służące urzeczywistnieniu jej celów:

– identyfikację operatorów kluczowych w odniesieniu do każdego sektora i podsektora, posiadających jednostkę organizacyjną na ich terytorium (art. 5 ust. 1 dyrektywy NIS);

---

[2] Dz.Urz. UE L 194 z 19.07.2016 r., s. 1.

[3] Por. projekt z dnia 31 października 2017 r. ustawy o krajowym systemie cyberbezpieczeństwa, opublikowany na stronie internetowej Ministerstwa Cyfryzacji: https://www.gov.pl/cyfryzacja/projekt-ustawy-o-krajowym-systemie-cyberbezpieczenstwa (27.11.2017).

[4] Art. 1 ust. 2 dyrektywy NIS.

– przyjęcie krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych (art. 7 ust. 1);

– wyznaczenie właściwych organów krajowych ds. bezpieczeństwa sieci i systemów informatycznych czy pojedynczego punktu kontaktowego (art. 8 ust. 1 i 3), jak również Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT (art. 9 ust. 1);

– odbieranie zgłoszeń o incydentach bezpieczeństwa komputerowego (art. 10 ust. 2);

– zapewnienie, by operatorzy usług kluczowych podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są wykorzystywane przez nich sieci i systemy informatyczne (art. 14 ust. 1); podejmowali odpowiednie środki zapobiegające i minimalizujące wpływ incydentów dotyczących bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w celu świadczenia takich usług kluczowych (art. 14 ust. 2) oraz niezwłocznie zgłaszali właściwemu organowi lub CSIRT incydenty mające istotny wpływ na ciągłość świadczonych przez nich usług kluczowych (art. 14 ust. 3);

– zapewnienie, by właściwe organy miały uprawnienia i środki niezbędne do oceny wypełniania przez operatorów usług kluczowych ich obowiązków, w tym uprawnienia do wymagania przekazywania informacji niezbędnych do oceny bezpieczeństwa ich sieci i systemów informatycznych oraz dowodów skutecznej realizacji polityk w zakresie bezpieczeństwa (art. 15 ust. 1 i 2);

– zapewnienie, aby dostawcy usług cyfrowych określali i podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są wykorzystywane przez nich do świadczenia usług sieci i systemy informatyczne (art. 16 ust. 1); podejmowali środki zapobiegawcze i minimalizujące wpływ incydentów dotyczących bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w celu świadczenia usług (art. 16 ust. 2) oraz bez zbędnej zwłoki zgłaszali właściwemu organowi lub CSIRT incydenty mające istotny wpływ na ciągłość świadczonych przez nich usług (art. 16 ust. 3);

– zapewnienie, by właściwe organy podjęły działania, w razie konieczności, w drodze środków nadzorczych *ex post*, gdy otrzymają dowód, że dostawca usług cyfrowych nie spełnia wymogów określonych w art. 16 (art. 17 ust. 1);

– ustanowienie przepisów dotyczących sankcji mających zastosowanie w przypadku naruszeń krajowych przepisów przyjętych na podstawie dyrektywy NIS i podejmowanie wszystkich niezbędnych środków w celu zapewnienia ich wykonania (art. 21).

Spełnienie tych wymogów wiąże się z przyjęciem ustawy (wraz z aktami wykonawczymi) zawierającej unormowania ustrojowe, materialne i proce-

sowe[5]. W szczególności powinny one uwzględniać katalog podmiotów współtworzących krajowy system cyberbezpieczeństwa, w tym organy właściwe ds. bezpieczeństwa sieci i systemów informatycznych, wyposażone w odpowiednie kompetencje umożliwiające realizację wyznaczonych w dyrektywie standardów w zakresie cyberbezpieczeństwa[6].

Różnorodność i wieloaspektowość wymogów dyrektywy NIS powoduje, iż rozwiązania krajowe powinny być dopasowane do poszczególnych zadań, a formy działania organów odpowiednio zdywersyfikowane. Należy się opowiedzieć za oparciem regulacji w zakresie bezpieczeństwa sieci i systemów informatycznych zarówno na klasycznych władczych formach działania administracji (decyzje administracyjne), jak i innych formach (polegających np. na wymianie informacji, zapewnianiu pomocy technicznej, zaleceniach czy wezwaniach). Poniżej przeanalizowano z tego punktu widzenia wybrane zagadnienia szczegółowe: identyfikację operatorów usług kluczowych, obsługę incydentów bezpieczeństwa komputerowego, postępowanie kontrolne, środki restytucyjne oraz środki o charakterze represyjnym. Dla uproszczenia odniesiono je jedynie do operatorów usług kluczowych, pomijając dostawców usług cyfrowych i podmioty świadczące usługi w zakresie cyberbezpieczeństwa.

Identyfikacja operatorów usług kluczowych

Państwa członkowskie zobowiązane są m.in. identyfikować operatorów usług kluczowych posiadających jednostkę organizacyjną na ich terytorium[7]. Operatorem takich usług jest przy tym podmiot publiczny lub prywatny należący do jednego z rodzajów wskazanych w załączniku II dyrektywy (załączniku do ustawy[8]), który jednocześnie spełnia następujące kryteria[9]:

a) podmiot świadczy usługę kluczową (wymienioną w wykazie usług kluczowych);

b) świadczenie tej usługi kluczowej zależy od systemów informacyjnych[10];

---

[5] Zgodnie z art. 25 ust. 1 dyrektywy NIS przyjęcie i publikacja przepisów krajowych służących wykonaniu dyrektywy powinny nastąpić do 9 maja 2018 r.

[6] W tym zakresie por. np. art. 4 projektu.

[7] Por. art. 5 ust. 1 dyrektywy NIS.

[8] Por. art. 5 ust. 1 projektu.

[9] Por. art. 4 pkt 4, art. 5 ust. 2 dyrektywy NIS.

[10] Por. wprowadzone w projekcie rozróżnienie systemu informacyjnego od systemu informatycznego, które realizuje postulaty wyrażane w doktrynie, np. G. Szpor, *Europejska regulacja bezpieczeństwa sieci i systemów informacyjnych a suwerenność państwa*, [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017, s. 68.

c) incydent (każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na cyberbezpieczeństwo) miałby istotny skutek zakłócający dla świadczenia tej usługi[11].

Dla identyfikacji takich podmiotów w projekcie ustawy przyjęto formę decyzji o uznaniu za operatora usługi kluczowej. Ze statusem tym wiążą się bowiem konkretne obowiązki o charakterze administracyjnoprawnym, co przemawia za nałożeniem ich na indywidualnie określony podmiot w następstwie sformalizowanej i odznaczającej się określonymi gwarancjami procedury. Nie zdecydowano się natomiast na kwalifikację z mocy prawa do omawianej kategorii pewnych grup podmiotów spełniających wskazane kryteria.

Wykaz usług kluczowych (z podziałem na sektory i podsektory wymienione w załączniku do ustawy), czyli usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, ma zostać określony w rozporządzeniu Rady Ministrów[12]. Wątpliwości natomiast budzi forma ustalenia progów istotności skutku zakłócającego incydentu dla świadczenia poszczególnych usług, właściwych jednej z przesłanek identyfikacji operatorów usług kluczowych. Progi te mają bowiem zostać zawarte nie w akcie prawa powszechnie obowiązującego, lecz w uchwale Rady Ministrów, dla której dodatkowo przewidziano zastosowanie przepisów o ochronie informacji niejawnych[13].

Obsługa incydentów bezpieczeństwa komputerowego

Nadanie statusu operatora usługi kluczowej wiąże się m.in. z: wdrożeniem systemu zarządzania bezpieczeństwem, opracowaniem dokumentacji dotyczącej systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, przeprowadzaniem audytów bezpieczeństwa czy wyznaczeniem osoby odpowiedzialnej za cyberbezpieczeństwo[14]. Na szczególną uwagę zasługuje przy tym warunek zgłaszania i obsługi incydentów. Projektowane regulacje obejmują: podmioty przekazujące i otrzymujące informacje o incydencie, charakter incydentu podlegającego zgłoszeniu, zakres przekazywanych informacji, w tym pozwalających na ocenę transgranicznego wpływu incydentu, zasady przepływu informacji pomiędzy poszczególnymi podmiotami krajowego systemu cyberbezpieczeństwa oraz odpowiednio innych państw i podmiotów unijnych odpowiedzialnych za koordynację polityki w tym zakresie. Jest to przejaw realizacji wymogu dyrektywy, by

[11] Por. art. 5 ust. 2 projektu.

[12] Por. art. 6 projektu.

[13] Por. art. 7 projektu.

[14] Por. art. 10 i n. projektu.

państwa członkowskie zapewniały odbieranie zgłoszeń o incydentach przez właściwe organy albo CSIRT[15].

Podmioty publiczne tworzące krajowy system cyberbezpieczeństwa w zakresie obsługi incydentów dotyczących bezpieczeństwa komputerowego będą stosowały szereg działań organizatorskich, informacyjnych czy analitycznych. Szczególną rolę w tym zakresie pełnią: CSIRT NASK, CSIRT GOV oraz CSIRT MON[16]. Dotyczy to jednak także organów właściwych dla poszczególnych sektorów, które mają m.in. przygotowywać we współpracy z CSIRT NASK, CSIRT GOV i CSIRT MON rekomendacje do działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów[17]. Rolą ministra właściwego do spraw informatyzacji jest natomiast m.in.: monitorowanie zagrożeń cyberbezpieczeństwa oraz wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej, prowadzenie polityki informacyjnej, opracowywanie rocznych sprawozdań, w tym dotyczących incydentów poważnych i istotnych, oraz zapewnienie funkcjonowania systemu teleinformatycznego, np. do zgłaszania i obsługi incydentów[18].

Postępowanie kontrolne

Zgodnie z art. 15 dyrektywy NIS państwa członkowskie zobowiązane są zapewnić, by właściwe organy miały uprawnienia i środki niezbędne do oceny wypełniania przez operatorów usług kluczowych ich obowiązków. Oznacza to, iż prawodawstwo krajowe powinno uwzględniać przepisy dotyczące kontroli i nadzoru nad wykonywaniem obowiązków w zakresie cyberbezpieczeństwa związanych ze statusem operatora usługi kluczowej. W projekcie ustawy kompetencje w tym zakresie powierzono organom właściwym do wydawania decyzji o uznaniu za operatora usługi kluczowej[19]. Uprawnione one zostały: do prowadzenia kontroli m.in. w zakresie wykonywania przez operatorów usług kluczowych wynikających z ustawy obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów związanych ze świadczonymi usługami kluczowymi; do zobowiązywania do usunięcia nieprawidłowości ustalonych w wyniku kontroli; jak również do nakładania kar pieniężnych[20].

[15] Por. art. 10 ust. 2 dyrektywy NIS.

[16] Por. art. 28 i n. projektu.

[17] Por. art. 39 ust. 1 pkt 4 projektu.

[18] Por. art. 41 i 42 projektu.

[19] Por. art. 47 ust. 1 pkt 2 projektu.

[20] Por. 47 ust. 2 projektu.

W zaproponowanym projekcie ustawy określono (w odniesieniu do kontroli wobec przedsiębiorców): uprawnienia osób prowadzących kontrole, obowiązki podmiotów kontrolowanych, sposób prowadzenia kontroli i dokonywania ustaleń oraz sporządzanie protokołu kontroli[21]. Odesłano również do stosowania wobec podmiotów będących przedsiębiorcami przepisów rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej[22] (z wyłączeniem art. 79). Tym samym zróżnicowano ich pozycję prawną z podmiotami publicznymi (niebędącymi przedsiębiorcami), względem których w projekcie zawarto jedynie odesłanie do przepisów ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[23] określających zasady i tryb przeprowadzania kontroli[24].

Środki restytucyjne

Z punktu widzenia efektywności systemu cyberbezpieczeństwa szczególnie istotne jest, by właściwe organy nie były uprawnione jedynie do kontroli realizacji obowiązków operatorów usług kluczowych, ale również do stosowania środków nadzorczych, których podstawowym celem jest uzyskanie stanu zgodnego z prawem. W artykule 15 ust. 3 dyrektywy NIS mowa jest w szczególności o wydawaniu przez właściwy organ operatorom usług kluczowych wiążących poleceń wprowadzenia środków zaradczych w odniesieniu do stwierdzonych uchybień. W związku z powyższym właściwe organy powinny być wyposażone w odpowiednie kompetencje. Umieszczanie jedynie uwag co do stwierdzonych uchybień w protokole z kontroli, bez możliwości zastosowania środków o charakterze wiążącym, może być negatywnie oceniane z punktu widzenia efektywności implementacji.

Zgodnie z art. 54 projektu ustawy o krajowym systemie cyberbezpieczeństwa, jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ właściwy (lub minister właściwy do spraw informatyzacji) uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości. Podmiot kontrolowany powinien przy tym, w wyznaczonym terminie, poinformować o sposobie wykonania zaleceń lub przyczynie ich niewykonania. Konstrukcja zaleceń pokontrolnych może jednak budzić w zaproponowanym kształcie szereg wątpliwości. Zalecenia ze swej istoty nie mają bowiem charakteru wiążącego, art. 54 nie jest natomiast spójny z art. 47 ust. 2 pkt 2 projektu, odnoszącym się do zobowiązywania do usunięcia

[21] Por. art. 49–53 projektu.

[22] Dz.U. z 2016 r., poz. 1829 z późn. zm.

[23] T.j. Dz.U. z 2011 r. Nr 185, poz. 1092.

[24] Por. art. 48 projektu.

nieprawidłowości ustalonych w wyniku kontroli. Niejasne jest, czy zalecenia pokontrolne byłyby częścią protokołu kontroli (wówczas można by było względem nich wnieść zastrzeżenia), czy będą zawierane w odrębnym piśmie i wówczas nie podlegałyby kontroli administracyjnej[25]. Dla formułowania nakazu zastosowania środków zaradczych służących usunięciu niezgodności z prawem nie zdecydowano się przy tym na formę decyzji administracyjnej, unikając sformalizowanej procedury administracyjnej[26]. Innym rozwiązaniem służącym wprowadzaniu środków restytucyjnych mogłoby być wzywanie przez właściwe organy do usunięcia naruszenia prawa (przywrócenia stanu zgodnego z prawem) pod rygorem zastosowania sankcji administracyjnej.

Środki represyjne

Klasyczne procedury jurysdykcyjne uznano natomiast za właściwe do nakładania sankcji z tytułu naruszenia przez operatorów usług kluczowych obowiązków wynikających z przepisów implementujących dyrektywę NIS. Sankcje te, zgodnie z dyrektywą, powinny być „skuteczne, proporcjonalne i odstraszające"[27]. W projekcie ustawy o krajowym systemie cyberbezpieczeństwa zawarto katalog naruszeń oraz maksymalne wysokości kar pieniężnych nakładanych w drodze decyzji (np. do 100 000 zł za niewdrożenie systemu zarządzania bezpieczeństwem[28]). Za uporczywe naruszanie przepisów ustawy powodujące: 1) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi; 2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych – organ właściwy będzie mógł natomiast nałożyć karę w wysokości do 200 000 zł[29].

Pozytywnie należy ocenić brak szerszej regulacji środków represyjnych w projekcie ustawy o krajowym systemie cyberbezpieczeństwa i odesłanie w sprawach nakładania lub wymierzania administracyjnej kary pienięż-

[25] Co najwyżej kontroli sądowoadministracyjnej – jako inne akty lub czynności z zakresu administracji publicznej dotyczące uprawnień lub obowiązków wynikających z przepisów prawa zgodnie z art. 3 par. 2 pkt 4 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, Dz.U. z 2017 r., poz. 1369 z późn. zm.

[26] W projekcie zaproponowano również inne niż zalecenia pokontrolne środki o charakterze restytucyjnym, w postaci wiążących poleceń wprowadzenia środków zaradczych w następstwie analizy wyników audytu (por. art. 16 ust. 6) oraz wiążących poleceń wprowadzenia środków zaradczych w odniesieniu do stwierdzonych nieprawidłowości, o których mowa w art. 39 ust. 2 projektu.

[27] Art. 21 dyrektywy NIS.

[28] Por. art. 57 ust. 1 i 2 projektu.

[29] Por. art. 57 ust. 3 projektu.

nej lub udzielania ulg w jej wykonaniu do stosowania przepisów działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[30], co zapobiega atomizacji regulacji w tym przedmiocie.

Podsumowanie

Efektywna implementacja postanowień dyrektywy NIS wymaga wdrożenia systemu współpracy pomiędzy podmiotami tworzącymi krajowy system cyberbezpieczeństwa, a także między tymi podmiotami a podmiotami z innych państw (współpraca horyzontalna) bądź instytucjami, organami i jednostkami organizacyjnymi Unii Europejskiej (współpraca wertykalna). W odniesieniu do badanego aspektu wewnętrznego należy opowiedzieć się za przyjęciem systemu regulacji o charakterze hybrydowym, tj. takiego, który oparty jest zarówno na klasycznych władczych formach działania administracji (decyzje administracyjne), jak i innych formach (związanych z wymianą informacji, wydawaniem zaleceń, stosowaniem wezwań czy zapewnieniem pomocy technicznej), w tym o charakterze niewładczym.

Wskazana wielopostaciowość form działania administracji w zakresie cyberbezpieczeństwa odpowiada propagowanej w doktrynie koncepcji otwarcia administracji publicznej na idee właściwe dobremu zarządzaniu – *good governance*. Wiąże się ona z koncepcją *new public management*, która koncentruje się wokół optymalizacji procedur, ich transparentności, efektywności i wydajności[31], z przejmowaniem przez sektor publiczny pewnych ugruntowanych już doświadczeń sektora prywatnego (np. w zakresie obsługi incydentów bezpieczeństwa komputerowego). Taki model zarządzania publicznego nie stanowi jednolitego standardu, lecz charakteryzowany jest jako zbiór pomysłów, wariacji na dany temat czy zespół idei[32] i powinien być uwzględniany także w dziedzinie polityki cyberbezpieczeństwa. Dotyczy bowiem tworzenia standardów administrowania, które mają na celu zapewnienie wysokiej jakości świadczonych usług[33].

Zróżnicowanie form działania administracji w sprawach cyberbezpieczeństwa powinno być przy tym postrzegane jako przejaw kształtowania

---

[30] Dz.U. z 2017 r., poz. 1257. Por. art. 59 projektu.

[31] Zob. T.T. Koncewicz, *op. cit.*, s. 267 i n.

[32] *A group of ideas, variations on a theme or a luster of ideas*. K. Sahlin-Anderson, *National, international and transnational constructions of New Public Management*, [w:] *New Public Management – the transformation of ideas and practise*, eds. T. Christensen, P. Lægreid, Aldershot 2003, s. 51, za: A. Modrzejewski, J. Kulikowska-Kulesza, *Od wolnego rynku do monopolizacji usług New Public Management w zarządzaniu odpadami komunalnymi*, [w:] *Dziesięć lat polskich doświadczeń w Unii Europejskiej. Problemy prawnoadministracyjne*, red. J. Sługocki, t. 1, Wrocław 2014, s. 782.

[33] Zob. G. Krawiec, *Europejskie prawo administracyjne*, Warszawa 2009, s. 23.

się mechanizmów zaliczanych przez Javiera Barnesa do tzw. procedur administracyjnych trzeciej generacji, obok klasycznych procedur opartych na władzy dyskrecjonalnej i indywidualnych, władczych rozstrzygnięciach (I generacja), jak i procedur związanych z wydawaniem decyzji generalnych (II generacja)[34].

Przy uwzględnieniu powyższych postulatów modernizacji podejścia do procedur administracyjnych zadaniem ustawodawcy staje się umiejętne wyważenie różnych instrumentów i form działania. Procedury o charakterze klasycznym związane z wydawaniem decyzji charakteryzują się: szerokim wachlarzem gwarancji przyznawanych stronom postępowania, wymogami związanymi z obiektywną oceną stanu faktycznego i prawnego, rozstrzygnięciem w formie władczej, które podlega środkom zaskarżenia w postępowaniu administracyjnym i sądowoadministracyjnym. Niewątpliwie jednak procedury jurysdykcyjne mogą być mało przydatne w sytuacji konieczności szybkiego reagowania na zagrożenia dla świadczenia usług o kluczowym dla społeczeństwa lub gospodarki charakterze. Skuteczne przeciwdziałanie incydentom bezpieczeństwa komputerowego wymaga zatem również wdrażania sprawnych systemów wymiany informacji, przekazywania zaleceń, pomocy technicznej czy wzywania pod groźbą zastosowania sankcji administracyjnej do realizacji wynikających z mocy prawa obowiązków dotyczących cyberbezpieczeństwa.

Bibliografia

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.Urz. UE L 194 z 19.07.2016 r.

Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, Dz.U. z 2017 r., poz. 1257.

Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, Dz.U. z 2017 r., poz. 1369 z późn. zm.

Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, Dz.U. z 2016 r., poz. 1829 z późn. zm.

Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, t.j. Dz.U. z 2011 r. Nr 185, poz. 1092.

Projekt z dnia 31 października 2017 r. ustawy o krajowym systemie cyberbezpieczeństwa, opublikowany na stronie internetowej Ministerstwa Cyfryzacji: https://www.gov.pl/cyfryzacja/projekt-ustawy-o-krajowym-systemie-cyberbezpieczenstwa (27.11.2017).

[34] J. Barnes, Transforming administrative procedure. Towards a third generation of administrative procedures, Workshop on Comparative Administrative Law, Yale Law School, May 7–9, 2009, s. 4, https://www.law.yale.edu/system/files/area/conference/compadmin/compadmin16_barnes_towards.pdf (27.11.2017). Por. M. Wilbrandt-Gotowicz, *Zintegrowane z prawem Unii Europejskiej postępowania administracyjne*, Warszawa 2017, s. 48.

Opracowania

Barnes J., Transforming administrative procedure. Towards a third generation of administrative procedures, Workshop on Comparative Administrative Law, Yale Law School, May 7–9, 2009, https://www.law.yale.edu/system/files/area/conference/compadmin/compadmin16_barnes_towards.pdf (27.11.2017).

Koncewicz T.T., *Aksjologia unijnego kodeksu proceduralnego*, Warszawa 2010.

Krawiec G., *Europejskie prawo administracyjne*, Warszawa 2009.

Modrzejewski A., Kulikowska-Kulesza J., *Od wolnego rynku do monopolizacji usług New Public Management w zarządzaniu odpadami komunalnymi*, [w:] *Dziesięć lat polskich doświadczeń w Unii Europejskiej. Problemy prawnoadministracyjne*, red. J. Sługocki, t. 1, Wrocław 2014.

Sahlin-Anderson K., *National, international and transnational constructions of New Public Management*, [w:] *New Public Management – the transformation of ideas and practise*, eds. T. Christensen, P. Lægreid, Aldershot 2003.

Szpor G., *Europejska regulacja bezpieczeństwa sieci i systemów informacyjnych a suwerenność państwa*, [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017.

Wilbrandt-Gotowicz M., *Zintegrowane z prawem Unii Europejskiej postępowania administracyjne*, Warszawa 2017.

NUMEROUS FORMS OF ACTIONS OF PUBLIC ADMINISTRATION AUTHORITIES AS ILLUSTRATED BY THE REQUIREMENT TO IMPLEMENT DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 6 JULY 2016 CONCERNING MEASURES FOR A HIGH COMMON LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS ACROSS THE UNION

Abstract: The article describes numerous forms of actions of public administration authorities, characteristic of the execution of requirements stemming from Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. In particular, it addresses the issues, such as: identifying operators of essential services, dealing with computer security incidents, control activities, restitutive measures and punitive measures. It has been demonstrated that, as regards cybersecurity, from the perspective of the requirements of effective implementation of the NIS Directive and good governance assumptions, it is appropriate to adopt hybrid forms of actions of administration authorities, based both on classic sovereign forms of actions of administration authorities (administrative decisions issued in cases regarding the recognition of an operator of an essential service, in cases concerning administrative pecuniary sanctions), as well as on other forms of actions (related to the exchange of information, issuance of recommendations, use of notices or providing technical support).

Keywords: CYBERSECURITY, NIS DIRECTIVE, OPERATORS OF ESSENTIAL SERVICES, NETWORK AND INFORMATION SYSTEMS, COMPUTER SECURITY INCIDENTS