Z E S Z Y T Y N A U K O W E UNIWERSYTETU RZESZOWSKIEGO

SERIA PRAWNICZA

ZESZYT 107/2019 PRAWO 26

DOI: 10.15584/znurprawo.2019.26.16

Krzysztof Chochowski

Państwowa Wyższa Szkoła Zawodowa w Tarnobrzegu
ORCID: 0000-0003-3198-9619

STRATEGIA CYBERBEZPIECZEŃSTWA JAKO PRZEJAW POLITYKI ADMINISTRACYJNEJ

Wprowadzenie

Dokonujący się w ogromnym tempie postęp technologiczny, zwłaszcza w sektorze IT, rozwój e-administracji i e-usług, stawia szereg nowych wyzwań przed administracją publiczną. Stąd też ogromnego znaczenia nabiera kwestia cyberbezpieczeństwa, którego zapewnieniu ma służyć tytułowa Strategia Cyberbezpieczeństwa Rzeczpospolitej Polski.

Triada nauk administracyjnych Fritza Stiera-Somlo

Podejmując rozważania dotyczące Strategii Cyberbezpieczeństwa RP jako przejawu polityki administracyjnej, już na wstępie należy odnieść się do tego, czym jest owa polityka administracyjna i czy koncepcja tzw. triady nauk administracyjnych Fritza Stiera-Somlo jest w dalszym ciągu aktualna.

Jak wskazuje J. Jeżewski, w Niemczech do nurtu nauk administracyjnych zalicza się: opisową naukę administracji, normatywno-analityczną naukę prawa administracyjnego oraz postulatywną, prospektywną naukę polityki administracyjnej. Początków tak rozumianej nauki administracji należy doszukiwać się w twórczości L. von Steina, który promował ideę silnego państwa (7 tomów *Verwaltungslehre* oraz 3 tomy *Handbuch der Verwaltungslehre*). Jego poglądy rozwinął Fritz Stier-Somlo, którego dzieło *Die Zukunft der Verwaltungswissenchaft* jest do dziś uznawane za doktrynalny fundament wspomnianej już triady nauk administracyjnych[1].

[1] A. Błaś, J. Boć, J. Jeżewski, *Administracja publiczna*, Wrocław 2004, s. 353–354.

H. Izdebski i M. Kulesza zgodnie twierdzą, że przedmiotem nauki prawa administracyjnego jest świat norm i ich wykładni, a także stosunków prawnych, natomiast nauka administracji i nauka polityki administracyjnej zajmuje się administracją rzeczywistą, a więc światem faktów społecznych i ich ocen[2]. Uczeni ci stwierdzają następnie: „Dla nauki administracji w sensie ścisłym jest to sama administracja jako taka, zachodzące w niej relacje, jej budowa i funkcjonowanie jako organizacji realizującej określone prawem zadania publiczne. Dla nauki polityki administracyjnej charakterystyczne jest inne podejście – jej przedmiotem jest kwestia optymalizacji skuteczności działalności publicznej, a więc zewnętrzna sprawność działalności administracyjnej państwa. Wartościowanie zjawisk społecznych (w tym administracyjnych) następuje tu zatem nie ze względu na samą administrację, lecz ze względu na skutki, jakie jej działalność rodzi w otoczeniu"[3].

Polityka administracyjna jest więc nauką, której przedmiotem jest przewidywanie skutków działania i wykorzystywanie możliwości działania w ramach prawa, przygotowywanie programów działania administracji oraz weryfikacja ich realizacji i ocenianie oraz wartościowanie metod i sposobów pracy, a także wysuwanie postulatów dotyczących zmian w całokształcie funkcjonowania administracji[4]. Zwięźle na temat przedmiotu polityki administracyjnej wypowiedział się J. Jeżewski, który uważa, że jest nim po prostu administrowanie[5].

Triady nauk administracyjnych nie sposób analizować niezależnie od siebie, dążąc do określenia optymalnego modelu administracji publicznej. Zdaniem J. Szreniawskiego, „[t]e trzy części składowe (triady nauk administracyjnych – K.Ch.) tworzą w sumie całość i wzajemnie się uzupełniają. Dostrzec jednak można, że mają odrębne metody badawcze, różnice w historycznym procesie rozwijania się i w źródłach inspiracji oraz w rezultatach poszukiwań"[6]. Podobne stanowisko zajmuje A. Błaś, który uznaje, że w polskiej nauce prawa publicznego nie znajdzie się argumentów przemawiających na rzecz tezy, iż polityka administracyjna uchyla się od regulacji zawartej w prawie powszechnie obowiązującym, że może być prowadzona obok prawa, ponad prawem czy poza jego granicami. Co więcej, to prawo jest podstawą działań objętych pojęciem polityki administracyjnej i to ono określa zasady i kryteria, a także formy i zakres prowadzenia polityki administracyjnej[7].

---

[2] H. Izdebski, M. Kulesza, *Administracja publiczna, zagadnienia ogólne,* Warszawa 2004, s. 12.

[3] *Ibidem*, s. 351.

[4] J. Szreniawski, *Wstęp do nauki administracji*, Lublin 2003, s. 9–10.

[5] J. Jeżewski, *Polityka administracyjna – przedmiot i metoda*, w: *Polityka administracyjna*, red. J. Łukasiewicz, Rzeszów 2008, s. 293.

[6] J. Szreniawski, *Wstęp do nauki*…, s. 9.

[7] A. Błaś, *Państwo prawa i polityka administracyjna*, w: *Polityka administracyjna*, red. J. Łukaszewicz, Rzeszów 2008, s. 144.

Trafnie zatem postuluje J. Izdebski, że należy utrzymać ścisłe związki pomiędzy naukami administracyjnymi, gdyż jedynie w ten sposób możliwe jest zapewnienie prawidłowej oceny zjawisk administracyjnych[8]. Dyscypliny te, jak podkreśla S. Wrzosek, zajmują się administracją publiczną, jednakże analizują ją z różnych punktów widzenia[9]. Oznacza to, że współcześnie triada nauk administracyjnych Fritza Stiera-Somlo jest w dalszym ciągu aktualna. Zaznaczyć jednak należy, iż współcześnie bazowanie wyłącznie na powyższej triadzie wydaje się być niewystarczające, albowiem zjawisko administracji publicznej ma wiele wymiarów i może być rozpatrywane z punktu widzenia różnych nauk.

Ewolucja Strategii

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej została opracowana w wyniku swoistego procesu. Zapoczątkował go opublikowany 7 lutego 2013 r. przez Komisję Europejską Wspólny komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, pierwszy dokument UE poświęcony kwestii cyberbezpieczeństwa, który miał charakter strategiczny.

Uznano w nim, że „[w] ciągu ostatnich dwóch dziesięcioleci internet oraz szerzej rozumiana cyberprzestrzeń miały olbrzymi wpływ na wszystkie aspekty funkcjonowania społeczeństwa. Nasze codzienne życie, prawa podstawowe, interakcje społeczne i gospodarka uzależnione są od sprawnie funkcjonujących technologii informacyjno-komunikacyjnych”[10]. Stwierdzono następnie, że „[a]by cyberprzestrzeń pozostała otwarta i wolna, w środowisku internetowym powinny mieć zastosowanie te same normy, zasady i wartości, które UE wspiera w świecie rzeczywistym. W cyberprzestrzeni należy zapewnić ochronę praw podstawowych, demokracji i praworządności. Nasza wolność i nasz dobrobyt w coraz większym stopniu uzależnione są od sprawnego i innowacyjnego internetu, który nadal będzie odgrywał kluczową rolę, jeżeli sektor prywatny i społeczeństwo obywatelskie będą w dalszym ciągu stymulować jego rozwój. Wolność w środowisku internetowym wymaga jednak również bezpieczeństwa i ochrony”[11].

---

[8] J. Izdebski, *Rozwój zainteresowań nauki administracji w systemie nauk administracyjnych*, „Roczniki Nauk Prawnych” 2009, t. XIX, nr 2, s. 247.

[9] S. Wrzosek, *System: administracja publiczna. Systemowe determinanty nauki administracji*, Lublin 2008, s. 31.

[10] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52013JC0001&from=PL (28.06.2019).

[11] *Ibidem.*

Unijna wizja przedstawiona w omawianym dokumencie składa się z pięciu strategicznych priorytetów, które uwzględniają wyzwania wymienione powyżej. Zalicza się do nich:

– osiągnięcie odporności na zagrożenia cybernetyczne,
– radykalne ograniczenie cyberprzestępczości,
– opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (WPBiO),
– rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego,
– ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE.

Jak zatem widać, cyberbezpieczeństwo ma być osiągnięte na całym obszarze UE i uwzględniać nie tylko teraźniejsze, ale i przyszłe zagrożenia. Znamienne jest to, że wszelkie formy naruszenia cyberbezpieczeństwa nie ograniczają do granic UE. W analizowanym dokumencie stwierdza się jednoznacznie, że „[c]yberprzestępczość nie zna granic – globalny zasięg internetu oznacza, że egzekwując prawo, należy przyjąć skoordynowane i wspólne podejście ponadgraniczne, aby właściwie reagować na to rosnące zagrożenie”[12]. Z tego też względu odpowiedzialność za zapewnienie bezpieczeństwa cybernetycznego spoczywa na podmiotach zarówno na poziomie krajowym, jak i Unii Europejskiej.

Niejako w odpowiedzi na powyższe działania Komisji Europejskiej w 2013 r. opracowano Politykę Ochrony Cyberprzestrzeni RP, którą uznaje się za pierwszy krajowy dokument strategiczny dotyczący cyberbezpieczeństwa. Została ona przyjęta uchwałą Rady Ministrów nr 111/2013 z 25 czerwca 2013 r., a koordynację realizacji jej postanowień powierzono ministrowi właściwemu ds. informatyzacji. Podstawowym jego celem (celem strategicznym) było osiągnięcie wzmiankowanego w Strategii bezpieczeństwa cybernetycznego Unii Europejskiej akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. Natomiast do celów szczegółowych zaliczono:

– zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa,
– zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni,
– zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne,
– określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni,

[12] *Ibidem.*

– stworzenie i realizację spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych,
– stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni,
– zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni[13].

Powyższe cele Polityki są realizowane przez:
– system koordynacji przeciwdziałania i reagowania na zagrożenia i ataki na cyberprzestrzeń, w tym ataki o charakterze terrorystycznym,
– powszechne wdrożenie w jednostkach administracji rządowej, a także podmiotach niepublicznych mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń dla bezpieczeństwa cyberprzestrzeni oraz właściwemu postępowaniu w przypadku stwierdzonych incydentów,
– powszechną oraz specjalistyczną edukację społeczną w zakresie bezpieczeństwa cyberprzestrzeni RP (zwana dalej w skrócie CRP).

Polityka Ochrony Cyberprzestrzeni RP zakładała, iż zostanie stworzony trzypoziomowy Krajowy system reagowania na incydenty komputerowe w CRP. Poziom I to poziom koordynacji, którym zajmować miał się minister właściwy ds. informatyzacji. Poziom II to poziom reagowania na incydenty komputerowe. Składać się na niego miały: Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL – realizujący jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze CRP; Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych realizujące zadania w sferze militarnej. Natomiast poziom III to poziom realizacji, w skład którego wchodzić mieli administratorzy odpowiadający za poszczególne systemy teleinformatyczne funkcjonujące w cyberprzestrzeni[14].

Kolejnym krokiem na drodze do opracowanie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej jest Doktryna Cyberbezpieczeństwa RP. Dokument ten został opracowany przez Biuro Bezpieczeństwa Narodowego i zaakceptowany 12 stycznia 2015 r. przez Radę Bezpieczeństwa Narodowego, która jest organem doradczym Prezydenta RP. Podkreślić należy, że Doktryna Cyberbezpieczeństwa RP jest dokumentem o charakterze koncepcyjnym i nie ma mocy prawnej.

W *Doktrynie* za cel strategiczny uznano zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni, w tym adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza

[13] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/PO_NCSS.pdf (28.06.2019).

[14] *Ibidem.*

teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych, w szczególności wchodzących w skład sektorów: finansowego, energetycznego i ochrony zdrowia[15]. Powyższy cel strategiczny ma zostać osiągnięty przez realizację zadań prowadzących do osiągania celów o charakterze operacyjnym i preparacyjnym. Do głównych celów operacyjnych zaliczono:

– ocenę warunków cyberbezpieczeństwa, w tym rozpoznawanie zagrożeń, szacowanie ryzyk i identyfikację szans,
– zapobieganie (przeciwdziałanie) zagrożeniom, redukowanie ryzyk i wykorzystywanie szans,
– obronę i ochronę własnych systemów i zgromadzonych w nich zasobów,
– zwalczanie (dezorganizowanie, zakłócanie i niszczenie) źródeł zagrożeń (aktywna obrona oraz działania ofensywne),
– po ewentualnym ataku – odtwarzanie sprawności i funkcjonalności systemów tworzących cyberprzestrzeń[16].

By osiągnąć powyższe cele operacyjne, potrzebne jest, w wymiarze preparacyjnym, zbudowanie, utrzymywanie i systematyczne doskonalenie (rozwój) zintegrowanego, zarządzanego (koordynowanego) ponadresortowo systemu cyberbezpieczeństwa RP obejmującego:

– podsystem kierowania – zdolny do organizowania i koordynowania działań podmiotów rządowych i pozarządowych realizujących zadania w zakresie cyberbezpieczeństwa,
– podsystemy operacyjne i wsparcia – zdolne do samodzielnego prowadzenia defensywnych (ochronnych i obronnych) oraz ofensywnych cyberoperacji, a także udzielania i przyjmowania wsparcia w ramach działań sojuszniczych[17].

Kolejnym dokumentem dotyczącym polityki cyberbezpieczeństwa są Krajowe Ramy Polityki Cyberbezpieczeństwa. Ramy te stanowią zbiór założeń, których głównym celem jest zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli, którzy korzystają z usług cyfrowych. Dokument ten został przyjęty 9 maja 2017 r. uchwałą Rady Ministrów nr 52/2017 i zastąpił Politykę Ochrony Cyberprzestrzeni RP.

Do celów szczegółowych zalicza się:

– osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa,
– wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom,

[15] https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf (28.06.2019).
[16] *Ibidem.*
[17] *Ibidem.*

– zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni,
– zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa[18].

Koordynatorem wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji.

Następnym dokumentem wpływającym na treść Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej jest komunikat Komisji Europejskiej z 13 września 2017 r., który jest aktualizacją Strategii Cyberbezpieczeństwa UE. Podniesiono w nim potrzebę zwrócenia większej uwagi na kwestię wspólnej odpowiedzi państw członkowskich na międzynarodowe incydenty oraz współpracę sektora cywilnego z militarnym.

Reforma Strategii Cyberbezpieczeństwa UE opiera się na trzech filarach. Pierwszym z nich jest budowanie odporności UE na ataki cybernetyczne. Zakłada on:
– wzmocnienie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA),
– rozwój w kierunku jednolitego rynku bezpieczeństwa cybernetycznego,
– wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS),
– odporność dzięki szybkiemu reagowaniu w sytuacji kryzysowej,
– stworzenie sieci ośrodków kompetencji w dziedzinie bezpieczeństwa cybernetycznego oraz Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego,
– budowanie silnej unijnej bazy umiejętności cybernetycznych,
– propagowanie cyberhigieny i świadomości zagrożeń[19].

Drugim filarem jest kształtowanie skutecznej unijnej prewencji cybernetycznej. W jej skład ma wchodzić:
– identyfikacja podmiotów działających w złych intencjach,
– doskonalenie reagowania przez organy ściągania,
– publiczno-prywatna współpraca w zwalczaniu cyberprzestępczości,
– doskonalenie reagowania politycznego,
– kształtowanie prewencji w zakresie bezpieczeństwa cybernetycznego za pomocą potencjału obronnego państw członkowskich[20].

Trzecim i zdaje się najważniejszym filarem jest wzmocnienie współpracy międzynarodowej w dziedzinie bezpieczeństwa cybernetycznego. W jego ramach znajdować ma się:

---

[18] https://cyberpolicy.nask.pl/wp-content/uploads/2017/05/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf (28.06.2019).

[19] http://europa.eu/rapid/press-release_IP-17-3193_pl.htm (28.06.2019).

[20] *Ibidem.*

– bezpieczeństwo cybernetyczne w stosunkach zewnętrznych,
– budowanie zdolności w obszarze bezpieczeństwa cybernetycznego,
– współpraca UE–NATO[21].

Ostatnim dokumentem jest przedstawiony 18 stycznia 2018 r. przez Ministra Cyfryzacji plan działań dotyczący Krajowych Ram Polityki Cyberbezpieczeństwa. Dokument ten ma charakter planistyczny i przedstawia:
– kierunki interwencji organów administracji rządowej do 2022 r.,
– wykaz zadań służący osiągnięciu celów Krajowych Ram Polityki Cyberbezpieczeństwa,
– wykaz działań w ramach określonych zadań,
– zasady finansowania działań,
– zagadnienia monitorowania i sprawozdawczości.

Został on sporządzony, by zsynchronizować działania różnych podmiotów i organów uczestniczących w ochronie cyberprzestrzeni RP.

Dynamiczny rozwój sektora IT, e-administracji i e-usług skutkuje poszerzaniem się cyberprzestrzeni i odnajdywaniem się w niej coraz większej liczby różnych podmiotów. Siłą rzeczy w przestrzeni tej mogą mieć miejsce zjawiska patologiczne, w tym przestępstwa. Wymaga to stosownej odpowiedzi władz publicznych, które winny stworzyć mechanizmy, procedury oraz struktury, za pośrednictwem których zapewnione będzie bezpieczne i harmonijne korzystanie ze wspomnianych zdobyczy cywilizacyjnych.

Na podstawie powyższych uwag można zauważyć, iż kwestia cyberbezpieczeństwa z każdym rokiem nabiera coraz większego znaczenia. Dostrzega się to zarówno na poziomie UE, jak i krajowym, czego wyrazem są ww. dokumenty. Stanowią one przejaw polityki administracyjnej, a częstokroć są swoistym pomostem do tworzenia regulacji prawnych zaliczanych do prawa administracyjnego.

Ustawa o krajowym systemie cyberbezpieczeństwa a Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Pomiędzy strategią cyberbezpieczeństwa jako przejawem polityki a prawem administracyjnym istnieje ścisły związek, czego dowodem jest ustawa o krajowym systemie cyberbezpieczeństwa (zwana dalej w skrócie u.k.s.c.)[22]. Ustawa ta w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady

[21] *Ibidem.*

[22] Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r., poz. 1560.

(UE) 2016/1148 z 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, s. 1).

Strategii cyberbezpieczeństwa poświęcono rozdział 13 ustawy, tj. przepisy zawarte w art. 68–72, a także art. 90.

Na mocy art. 68 u.k.s.c. Rada Ministrów jest zobligowana, by przyjąć w drodze uchwały wspomnianą strategię. Uchwała, o której mowa, nie mając charakteru powszechnie obowiązującego, wiąże jednostki organizacyjnie podporządkowane Radzie Ministrów.

Jak wskazuje G. Szpor: „Strategia cyberbezpieczeństwa według ustawy o polityce rozwoju należy do kategorii «innych strategii rozwoju». Muszą one być spójne ze średniookresową strategią rozwoju kraju i określać w szczególności: diagnozę sytuacji w odniesieniu do zakresu objętego programowaniem strategicznym, prognozę trendów rozwojowych w okresie objętym strategią, określenie celów rozwoju, w tym kierunków interwencji wraz z pożądanymi wskaźnikami realizacji, systemy realizacji i ramy finansowe. Mogą też zawierać inne elementy, jeżeli wynika to ze zobowiązań międzynarodowych”[23].

Strategia cyberbezpieczństwa w myśl art. 69 ust. 1 u.k.s.c. określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. W szczególności winna ona uwzględniać:

– cele i priorytety w zakresie cyberbezpieczeństwa,
– podmioty zaangażowane we wdrażanie i realizację strategii,
– środki służące realizacji celów strategii,
– określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym,
– podejście do oceny ryzyka,
– działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa,
– działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa.

Strategia ta ustalana jest na okres pięcioletni, przy czym dopuszcza się możliwość wprowadzenia w niej zmian w okresie obowiązywania[24]. Jej projekt opracowuje minister właściwy do spraw informatyzacji we współpracy z pełnomocnikiem, innymi ministrami i właściwymi kierownikami urzędów centralnych.

[23] G. Szpor, *Art. 68*, w: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, https://sip.lex.pl/#/commentary/587786722/584162 (29.06.2019).

[24] Artykuł 69 ust. 3 u.k.s.c.

Ponadto w pracach nad projektem może uczestniczyć przedstawiciel Prezydenta Rzeczypospolitej Polskiej[25].

Trafnie stwierdza więc G. Szpor: „Zapewnienie bezpieczeństwa informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów teleinformatycznych, użytkowników cyberprzestrzeni, organów władzy publicznej, a także wyspecjalizowanych podmiotów zajmujących się bezpieczeństwem teleinformatycznym w sferze operacyjnej. Jest to tym istotniejsze, iż Polska jest ściśle powiązana z innymi państwami poprzez współpracę międzynarodową w ramach takich organizacji, jak UE, NATO, ONZ czy OBWE. Współpraca ta odgrywa istotną rolę w walce z rosnącą liczbą incydentów powodowanych nielegalnymi działaniami w cyberprzestrzeni, prowadzącymi do strat materialnych i wizerunkowych"[26].

Przyjęta strategia cyberbezpieczeństwa poddawana jest przeglądowi co 2 lata. Przeglądu dokonuje minister właściwy do spraw informatyzacji we współpracy z pełnomocnikiem, innymi ministrami i właściwymi kierownikami urzędów centralnych[27]. Przegląd podejmowany jest w celu oceny aktualności strategii w odniesieniu do występujących zmiennych.

Ustawodawca w art. 90 u.k.s.c. jednoznacznie wskazuje maksymalny termin do przyjęcia strategii cyberbezpieczeństwa. Strategia ma być przyjęta do 31 października 2019 r.

Na podstawie art. 72 u.k.s.c. minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej strategię w terminie 3 miesięcy od dnia jej przyjęcia przez Radę Ministrów. Jest to zgodne z art. 7 ust. 3 dyrektywy NIS[28].

Ustawa o krajowym systemie cyberbezpieczeństwa to element prawa administracyjnego, a zatem istotna składowa triady nauk administracyjnych, o której pisał Fritz Stier-Somlo. Obliguje ona RM do opracowania i przyjęcia strategii cyberbezpieczeństwa oraz przekazania jej Komisji Europejskiej. Jak zatem widać, kwestia cyberbezpieczeństwa ma nie tylko wymiar krajowy, ale i europejski.

Strategia cyberbezpieczeństwa, określając cel główny i cele szczegółowe, priorytety w zakresie cyberbezpieczeństwa, podmioty zaangażowane w jej wrażanie i realizację, a także środki służące realizacji jej celów, stanowi istotny przejaw polityki administracyjnej państwa ukierunkowanej na zapewnienie szeroko pojmowanego bezpieczeństwa.

---

[25] Artykuł 70 u.k.s.c..

[26] G. Szpor, *Art. 70*, w: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, https://sip.lex.pl/#/commentary/587786724/584164 (29.06.2019).

[27] Artykuł 71 u.k.s.c.

[28] M.B. Wilbrandt-Gotowicz, *Art. 90*, w: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, https://sip.lex.pl/#/commentary/587786746/584186 (11.04.2019).

Podsumowanie

Dokonujący się intensywnie rozwój nowych technologii teleinformatycznych i pojawienie się nowej, nieznanej uprzednio administracji publicznej przestrzeni, którą jest cyberprzestrzeń, wymusiło na władzy publicznej zajęcie się kwestią cyberbezpieczeństwa. Jednakże, by podejmowane działania były efektywne i racjonalne, konieczne stało się opracowanie stosownych planów, które finalnie złożyły się na strategię cyberbezpieczeństwa RP. Obecnie za jej nośnik uchodzą Krajowe Ramy Polityki Cyberbezpieczeństwa. Ramy te należy uznać za wyraz polityki administracyjnej, czy szerzej: polityki państwa w sferze bezpieczeństwa publicznego.

Wprowadzenie do rodzimego systemu prawnego ustawy o krajowym systemie cyberbezpieczeństwa uwypukla znaczenie polityki administracyjnej w tym zakresie, a co za tym idzie, również stosownej strategii. Wprost widać tu związek pomiędzy prawem administracyjnym i polityką administracyjną odnośnie do cyberbezpieczeństwa, choć zaznaczyć należy, iż także nauka administracji, podobnie jak i inne dyscypliny naukowe, może mieć tu zastosowanie. Oznacza to, że klasyczna triada nauk administracyjnych Fritza Stiera-Somlo nie straciła na ważności, choć warto ją uzupełniać i twórczo rozwijać o zdobycze innych nauk. To interdyscyplinarne i wielowątkowe spojrzenie na administrację publiczną w kontekście cyberprzestrzeni i cyberbezpieczeństwa może wzbogacić i udoskonalić przyjmowane rozwiązania, tak w wymiarze teoretycznym, jak i praktycznym, co pozytywnie przełoży się na poziom bezpieczeństwa w cyberprzestrzeni.

Bibliografia

Błaś A., Boć J., Jeżewski J., *Administracja publiczna*, Wrocław 2004.

Błaś A., *Państwo prawa i polityka administracyjna*, w: *Polityka administracyjna*, red. J. Łukaszewicz, Rzeszów 2008.

Izdebski H., M. Kulesza, *Administracja publiczna, zagadnienia ogólne,* Warszawa 2004.

Izdebski J., *Rozwój zainteresowań nauki administracji w systemie nauk administracyjnych*, „Roczniki Nauk Prawnych" 2009, t. XIX, nr 2.

Jeżewski J., *Polityka administracyjna – przedmiot i metoda*, w: *Polityka administracyjna*, red. J. Łukasiewicz, Rzeszów 2008.

Szpor G., *Art. 68*, w: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, https://sip.lex.pl/#/commentary/587786722/584162 (29.06.2019).

Szpor G., *Art. 70*, w: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, https://sip.lex.pl/#/commentary/587786724/584164 (29.06.2019).

Szreniawski J., *Wstęp do nauki administracji*, Lublin 2003.

Wilbrandt-Gotowicz M.B., *Art. 90*, w: *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, https://sip.lex.pl/#/commentary/587786746/584186 (11.04.2019).

Wrzosek S., *System: administracja publiczna. Systemowe determinanty nauki administracji*, Lublin 2008.

Streszczenie

Nie budzi wątpliwości, że polityka administracyjna jest związana z polityką państwa, którego jednym z podstawowych celów jest zapewnienie podmiotom podlegającym jego władzy bezpieczeństwa – w tym bezpieczeństwa w cyberprzestrzeni. Niniejszy artykuł prezentuje rozważania dotyczące strategii cyberbezpieczeństwa RP jako przejawu polityki administracyjnej państwa. Wskazano w nim proces dochodzenia powstania tejże strategii, a także związek pomiędzy ustawa o krajowym systemie cyberbezpieczeństwa jako składową prawa administracyjnego a wspomnianą strategią jako elementem polityki administracyjnej.

Słowa kluczowe: polityka administracyjna, cyberbezpieczeństwo, strategia cyberbezpieczeństwa

CYBER-SECURITY STRATEGY AS A MANIFESTATION OF ADMINISTRATIVE POLICY

Summary

There is no doubt that the administrative policy is related to the policy of the state, whose one of the primary goals is to ensure that entities subject to its security authority – including security in cyberspace. This article presents considerations regarding the cybersecurity strategy of the Republic of Poland as a manifestation of the state's administrative policy. It indicates the process of seeking the creation of this strategy, as well as the relationship between the law on the national cyber security system as a component of administrative law and the aforementioned strategy as an element of administrative policy.

Keywords: administrative policy, cyber security, cyber security strategy