Paweł Romaniuk*

Kształtowanie administracyjnoprawnych warunków służących do budowy cyberbezpieczeństwa w administracji publicznej

Streszczenie

Przedmiotowy artykuł dotyczy tworzenia administracyjnoprawnych warunków do budowy właściwego systemu cyberbezpieczeństwa w administracji publicznej. Cyberbezpieczeństwo państwa staje się w obecnych uwarunkowaniach, zarówno prawnych, jak i organizacyjnych, jednym z ważniejszych celów strategicznych w obszarze bezpieczeństwa. Rosnąca z każdym rokiem liczba zagrożeń i incydentów w cyberprzestrzeni, a także stopień ich zaawansowania stanowią obecnie jeden z kluczowych problemów stawianych przed administracją publiczną w obszarze zagwarantowania niezakłóconego funkcjonowania całego państwa, gospodarki oraz społeczeństwa.

Słowa kluczowe: administracja publiczna, prawo, cyberbezpieczeństwo, prawo administracyjne, mechanizmy ochronne

* Dr hab. Paweł Romaniuk, Uniwersytet Warmińsko-Mazurski w Olsztynie, e-mail: pawel.romaniuk@uwm.edu.pl, ORCID: 0000-0002-7217-956X.

Wstęp

Współczesne odniesienie do prawnoadministracyjnych założeń, związanych z problematyką cyberbezpieczeństwa w jednostkach sektora finansów publicznych, wynika przede wszystkim z konieczności utożsamiania się tego zjawiska z przeciwdziałaniem atakom skierowanym głównej na sieci teleinformatyczne. Jednakże wydaje się, że stanowisko takie nie do końca jest zasadne, uwzględniając kontekst weryfikacji pojęcia cyberprzestrzeni i zagrożeń z nią związanych w przestrzeni publicznej.

Cyberbezpieczeństwo staje się pojęciem ściśle korelującym z zagwarantowaniem ochrony i przeciwdziałaniem wielu zagrożeniom dotykającym samą cyberprzestrzeń oraz obecności w cyberprzestrzeni wielu ważnych danych i informacji, które są w posiadaniu zarówno sektora publicznego, jak i prywatnego. Tematem niniejszego artykułu jest analiza funkcjonującego już od kilku lat systemu cyberbezpieczeństwa jako swoistego procesu budowania odporności systemów informacyjnych i informatycznych na działania naruszające poufność, integralność, dostępność oraz autentyczność przetwarzanych danych będących w posiadaniu administracji publicznej.

Bezpieczeństwo czynnikiem wspomagającym budowę systemu cyberbezpieczeństwa

Bezpieczeństwo w strukturze administracji publicznej jest jednym z najbardziej istotnych i znaczących elementów, które odpowiadają za wewnętrzne bezpieczeństwo państwa. Pojęcie to w sposób nie zawsze trafny jest łączone z porządkiem publicznym w jeden termin – bezpieczeństwo i porządek publiczny. Trzeba zaznaczyć, że porządek publiczny w niektórych swych strukturach wkomponowany jest w bezpieczeństwo publiczne, co też może wywoływać różne odczucia pojęciowe[1]. Założenia związane z systemem bezpieczeństwa są traktowane w sposób uniwersalny jako dobro wspólne społeczeństwa. Bezpieczeństwo jest postrzegane w kategorii ważnego elementu państwa, którego rolą jest gotowość do przeciwdziałania potencjalnym zagrożeniom

1 W. Fehler, *Bezpieczeństwo publiczne jako składnik wewnętrznego bezpieczeństwa państw*, „Bezpieczeństwo. Teoria i Praktyka" 2010, nr 1–2, s. 25.

i likwidowania skutków ich wystąpienia[2]. Działania te pozostają w ścisłym związku z zabiegami o bezpieczeństwo państwa, co z kolei wiąże się z troską o zapewnienie potrzeb i dóbr powszechnych.

Należy zauważyć, że poczucie bezpieczeństwa jest wartością nadrzędną dla każdego społeczeństwa. Wielu autorów w bogatym piśmiennictwie proponuje zastąpienie określeń „pokój" i „wojna" pojęciami „bezpieczeństwo" i „zagrożenie". Charakterystyczna zamienność tych terminów bez wątpienia jest związana z procesem nieuchronnej zmiany społeczno-kulturowej[3]. Bezpieczeństwo jest również jedną z głównych potrzeb człowieka, która jest dla każdego z nas niezwykle ważna. Poczucie bezpieczeństwa musi bezwzględnie kojarzyć się z pożądanym stanem spokoju, brakiem lęku, strachu czy obaw. Z socjologicznego punktu widzenia bezpieczeństwo polega na wyznaczaniu takich systemów i ruchów społecznych, które służą zapewnieniu bezpieczeństwa i wzmagają pozycję i stan spokoju[4]. Dla każdego społeczeństwa zagadnienia związane z bezpieczeństwem są jednymi z podstawowych wymiarów traktowania o rzeczywistości społecznej, uwzględniając przy tym założenia prawne skoncentrowane na budowaniu odpowiedzialności organizacyjnej i zarządczej oraz na zapewnianiu bezpieczeństwa swoim obywatelom[5].

Dla zagwarantowania bezpieczeństwa administracji publicznej w obszarze posiadanych przez nią zasobów niezwykle ważne jest zapewnienie bezpieczeństwa e-administracji, dlatego że bezpieczeństwo wpływa na stanowienie i stosowanie prawa, w tym dokonywanie wykładni przepisów, które regulują administrowanie systemami teleinformatycznymi i środkami komunikacji elektronicznej oraz ich prawidłowe, i co najważniejsze – bezpieczne użytkowanie[6]. Przywołana zasada konfigurowania bezpieczeństwa w e-administracji jest zasadą prawa o opisowym charakterze, gdyż jej treść można wyprowadzić z wielu norm prawnych, które odnaleźć można m.in. w ustawie o informatyzacji

2 R. Gwardyński, *Racjonalizacja działań Policji na poziomie lokalnym* [w:] *Racjonalizacja zarządzania jednolitymi formacjami umundurowanymi odpowiedzialnymi za bezpieczeństwo wewnętrzne*, red. B. Wiśniewski, P. Lubiewski, T. Zwęgliński, Warszawa 2020, s. 120–121.

3 A. Giddens, *Socjologia*, Warszawa 2006, s. 382.

4 Z. Zagórski, *Socjologia bezpieczeństwa. O potrzebie nowej subdyscypliny?* [w:] *Socjologiczne aspekty bezpieczeństwa narodowego*, red. T. Leszczykiewicz, Z. Zagórski, Wrocław 1999, s. 11.

5 Z. Ludziejewski, *Bezpieczeństwo informacyjne w instytucjach gospodarczych*, „Zeszyty Naukowe WSOWL" 2013, nr 4, s. 6–7.

6 M. Błażewski, *Zasada zapewnienia bezpieczeństwa w e-administracji*, „Folia Iuridica Universitatis Wratislaviensis" 2017, t. 6, nr 1, s. 108.

działalności podmiotów realizujących zadania publiczne[7], ustawie o ochronie danych osobowych[8] i w innych ustawach oraz wielu rozporządzeniach wykonawczych. Na podstawie tej zasady, wpływającej na zapewnienie bezpieczeństwa administracji publicznej, administratorzy i wszyscy użytkownicy systemów teleinformatycznych i środków komunikacji elektronicznej powinni w szczególności wykonywać czynności o charakterze technicznym i organizacyjnym, co ma przyczyniać się do ochrony informacji publicznej czy prywatnej[9].

Żeby zdefiniować pojęcie „cyberbezpieczeństwo", obecne w polskiej doktrynie, należy za punkt wyjścia przyjąć, czym jest samo bezpieczeństwo. Co ważne, model bezpieczeństwa, będący elementem obecności w codziennych zjawiskach życia jednostek i społeczeństw, nie daje się jednoznacznie zdefiniować[10]. Dlatego też na kanwie takiego podejścia pojęcie to wciąż budzi wiele dyskusji i rozważań. Najprościej przyjmuje się, że bezpieczeństwo oznacza stan braku potencjalnego zagrożenia[11]. Można zauważyć, że „[...] bezpieczeństwo jest pewnym stanem obiektywnym, polegającym na braku zagrożenia, odczuwanym subiektywnie przez jednostki i grupy. Oznacza to, że bezpieczeństwo składa się z dwóch elementów, obiektywnego i subiektywnego. Pierwszy z nich, mający charakter obiektywny, jest zewnętrzny w stosunku do jednostki, grupy społecznej czy zbiorowości. Z kolei drugi ma charakter subiektywny i jest poczuciem bezpieczeństwa"[12]. Bezpieczeństwo staje się wartością niezwykle uniwersalną i dotyczy dużej liczby podmiotów. Przyjmuje się, że bezpieczeństwo ma największe znaczenie dla jednostki, określonej grupy społecznej i w konsekwencji dla całego państwa. Różne są także kategorie (rodzaje) bezpieczeństwa, wyodrębniane w zależności od sfery aktywności danego podmiotu[13].

W ujęciu potocznym bezpieczeństwo jest traktowane w szczególności jako stan, w którym każda jednostka ma poczucie właściwej pewności w sprawnie

7 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j., Dz.U. 2023, poz. 57.

8 Więcej zob. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, t.j., ibidem 2019, poz. 1781.

9 Por. B. Michalak, *Bezpieczeństwo informacji w rejestrach medycznych*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2010, z. 2, s. 144–146.

10 J. Potrzeszcz, *Bezpieczeństwo i porządek publiczny w ujęciu filozofii prawa* [w:] *Bezpieczeństwo państwa. Zagadnienia podstawowe*, red. W. Lis, Lublin 2014, s. 15.

11 Z. Ścibiorek, B. Wiśniewski, R.B. Kuc, A. Dawidczyk, *Bezpieczeństwo wewnętrzne*, Toruń 2015, s. 26.

12 H. Korzeniowska, *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, Kraków 2004, s. 9–10.

13 K. Dunaj, *Istota bezpieczeństwa państwa* [w:] *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, red. M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, Olsztyn 2016, s. 17.

funkcjonującym systemie prawnym. Stan bezpieczeństwa nie powinien być traktowany jako zmienna niezależność, gdyż przybiera on dość specyficzny charakter i jest: 1) dynamiczny i procesualny, a także ulega nieustannym zmianom pod wpływem złożonych i wieloczynnikowych zjawisk; 2) subiektywny i obiektywny, gdyż postawy społeczne wobec bezpieczeństwa tworzą się wskutek wpływu danego zjawiska na jednostkę, grupę społeczną, społeczeństwo czy prawo; 3) relatywny oraz zależny od wielu subiektywnych i obiektywnych czynników[14].

Należy podkreślić, że jedną z podstawowych funkcji państwa jest zagwarantowanie bezpieczeństwa każdemu obywatelowi. Przyjmuje się, że państwo w swojej filozofii działania jest najlepszą formą zapewnienia bezpieczeństwa[15]. Wraz z rozwojem technologicznym i cywilizacyjnym państwo – za pomocą organów administracji publicznej, pełni coraz bardziej rozległe funkcje względem swoich mieszkańców. Wśród tych funkcji fundamentalną rolę odgrywa zapewnienie bezpieczeństwa zarówno wewnętrznego, jak i zewnętrznego. W związku z tym w doktrynie można wyodrębnić takie funkcje państwa, jak: 1) zewnętrzna – polega na utrzymywaniu stosunków z innymi państwami i organizacjami międzynarodowymi; 2) wewnętrzna – nazywana też ochronną, polega na zapewnieniu bezpieczeństwa i porządku publicznego; 3) gospodarczo-organizatorska – jest ukierunkowana na prowadzeniu przez państwo odpowiedniej polityki gospodarczej; 4) socjalna – gwarantuje ludności minimum egzystencji; 5) kulturalna – zapewnia dostęp do dóbr kultury; 6) edukacyjna – polega na zapewnieniu równego dostępu do systemu edukacji; 7) ochrony zdrowia – polega na stworzeniu warunków dostępu do opieki zdrowotnej[16].

Utrzymanie stanu bezpieczeństwa w administracji publicznej wiąże się również z zapewnieniem dynamicznego, ale i kontrolowanego charakteru jego naturalnych modyfikacji. Polega to przede wszystkim na tym, że bezpieczeństwo jest związane ze zmianami zachodzącymi pod wpływem wielu złożonych i wieloczynnikowych zjawisk. Jest to spowodowane tym, że określone postawy społeczne wobec bezpieczeństwa tworzą się wskutek wpływu danego

14 J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna* [w:] *Zarządzanie bezpieczeństwem*, red. P. Tyrała, Kraków 2000, s. 166.

15 Więcej na ten temat zob. W. Kitler, *Bezpieczeństwo narodowe. Podstawowe kategorie, dylematy pojęciowe i próba systematyzacji*, „Towarzystwo Wiedzy Obronnej. Zeszyt Problemowy" 2010, nr 1, s. 19–20.

16 A. Breczko, *Cele państwa i zasadnicze kierunki jego działania* [w:] *Wprowadzenie do nauk o państwie i prawie*, red. G. Kryszeń, Białystok 2004, s. 23–24.

zjawiska na jednostkę, grupę społeczną, społeczeństwo i finalnie na państwo[17]. Na zapewnienie właściwego bezpieczeństwa mają wpływ wszystkie interakcje społeczne. Sama kultura bezpieczeństwa wyznacza, jaki jest stosunek danej społeczności do ryzyka, zagrożeń, obaw i bezpieczeństwa, a także jakie wartości w tym zakresie są uznawane za ważne i obowiązkowe.

Administracyjne założenia cyberbezpieczeństwa

Ze względu na globalny i nieustannie dynamicznie rozwijający się charakter cyberprzestrzeni należy dbać o właściwe zabezpieczenie posiadanych w niej informacji. Jest to bardzo ważne, ponieważ wszelkie działania podejmowane w przestrzeni wirtualnej charakteryzują się przede wszystkim własną specyficzną kultura zachowań jej użytkowników budujących społeczność wirtualną. Stąd można przyjąć, że zjawisko bezpieczeństwa obecne w obszarze funkcjonowania sieci teleinformatycznych stwarza warunki, które wcale nie muszą być obecne poza cyberprzestrzenią[18].

Pojęcie „cyberbezpieczeństwo" odnosi się zazwyczaj do ściśle określonego obszaru działań silnie powiązanych z zapewnieniem bezpieczeństwa informacji, bezpieczeństwa komunikacji oraz bezpieczeństwa samej sieci zapewniającej bezpieczną formę wymiany informacji i danych. Jednakże trzeba mieć na uwadze, że pojęcie to nie wyczerpuje wszystkich kwestii związanych z koniecznością zagwarantowania ochrony przed niepożądanymi i nieautoryzowanymi działaniami w cyberprzestrzeni. Funkcjonowanie internetu opiera się na obecności zarówno infrastruktury, jak i kultury jego twórców oraz coraz większej grupy użytkowników. Jest on z jednej strony narzędziem pozyskania informacji, gdzie klasyczna prostota i łatwość korelacji różnych komputerów zapewnia obecność w nim dużej liczby użytkowników. Z drugiej strony, otwartość w dostępie do danych pozwala traktować to miejsce jako niezwykle atrakcyjny obszar spędzania czasu[19]. Nikogo nie trzeba przekonywać, że dzięki internetowi można robić zakupy, można się komunikować z osobami w dowolnym miejscu na świecie, można korzystać z cyfrowych treści, obsługując np. konta bankowe. Dzięki internetowi można ostatecznie załatwiać coraz dłuższą

17 J. Szmyd, op. cit., s. 166–167.
18 K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, nr 2, s. 13.
19 T. Goban-Klas, *Cywilizacja medialna*, Warszawa 2005, s. 151.

listę spraw urzędowych oraz wykorzystywać to narzędzie do nauki czy pracy. Wpływ na zapewnienie w organach administracji publicznej właściwego poziomu bezpieczeństwa mają wszystkie interakcje społeczne. W tym obszarze sama kultura bezpieczeństwa wyznacza pożądany stosunek danej społeczności do możliwości pojawienia się nie tylko ryzyka, lecz także i potencjalnych zagrożeń, które mogą wpływać na sposób realizacji zadań publicznych.

W przypadku podejmowania różnorodnych zachowań związanych z funkcjonowaniem cyberprzestrzeni i wszelkich zjawisk w niej występujących należy mieć na względzie to, że ze względu na jej globalny charakter jest to sfera niezwykle niebezpieczna i mogąca realnie wpływać na funkcjonowanie administracji publicznej. Wszelkie działania podejmowane w przestrzeni wirtualnej charakteryzuje niezwykle indywidualna i specyficzna forma modelowania struktury zachowań jej użytkowników. Dlatego należy przyjąć, że kreowanie bezpieczeństwa w internecie w obszarze funkcjonowania sieci teleinformatycznych wymusza uwzględnienie budowy właściwych systemów ochronnych i zabezpieczających zasoby administracji publicznej. Wyodrębnienie pojęcia „cyberbezpieczeństwo" odnosi się przede wszystkim do kształtowania obszaru wszelakich działań, które silnie korelują z zapewnieniem bezpieczeństwa informacji (zawartości sieci), bezpieczeństwem komunikowania (przekazu informacji) oraz bezpieczeństwem samej sieci. Tego typu działania bez wątpienia wpływają na potrzebę budowy nieustającej ochrony przed niepożądanymi zjawiskami, które w przestrzeni internetowej (cyberprzestrzeni) są coraz bardziej wszechobecne i, niestety, stwarzające coraz większe zagrożenia[20].

Główny szkielet internetu opiera się na otwartości nie tylko samej architektury jego infrastruktury, lecz także i kultury jego twórców oraz nowych użytkowników. Klasyczna prostota i dostępność do sieci zapewnia nowe możliwości korzystania z internetu, ale sposób korzystania z sieci informatycznych nie zawsze jest właściwy[21]. Stąd założenia dotyczące identyfikacji cyberbezpieczeństwa wymagają wykorzystania wielu podobnych i pomocnych zjawisk, do których można zaliczyć np. bezpieczeństwo informacyjne czy cyberprzestępczość.

Pierwsze wspomniane pojęcie, związane z bezpieczeństwem informacyjnym, można zakwalifikować i zdefiniować jako „[…] obronę informacyjną, która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego oraz planowanego stanu rzeczy i zjawisk we własnej

20 K. Chałubińska-Jentkiewicz, op. cit., s. 13.
21 Ibidem.

przestrzeni funkcjonowania, a także utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych"[22]. Bezpieczeństwo informacji to nie tylko zabezpieczenia fizyczne i techniczne zasobów informatycznych. Bezpieczeństwo informacji to przede wszystkim dążenie do zapewnienia i utrzymania poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności informacji i systemów, w których są one przetwarzane. To także odpowiednio przeszkolony i świadomy zagrożeń personel. To nie tylko odpowiednio zdefiniowane umowy z dostawcami, lecz także i sformalizowane plany ciągłego działania i procedury postępowania. Bezpieczeństwo to proces, i jak każdy proces wymaga nieustannego i świadomego doskonalenia[23]. Bezpieczeństwem informacyjnym jest także każde działanie mające na celu zabezpieczenie zasobów informacyjnych, które są gromadzone, przetwarzane, przekazywane i przechowywane w pamięci komputerów, w sieci teleinformatycznej czy na serwerach. Na podstawie takich ustaleń oprócz konieczności zapewnienia bezpieczeństwa informacyjnego w administracji publicznej zrodziło się pojęcie przywołanego już cyberbezpieczeństwa. Zgodnie z tą koncepcją cyberbezpieczeństwo można identyfikować jako wszelkie działania, procesy, procedury, a także regulacje prawne, które są wdrażane przez odpowiednie w tym obszarze podmioty. Ich zadaniem jest zapewnienie optymalnej integralności zgromadzonych, przechowywanych, przekazywanych i przetwarzanych zasobów informacyjnych i zagwarantowanie właściwej ich ochrony przed niepożądanym, nieautoryzowanym, nieuprawnionym ujawnieniem, przetworzeniem lub zniszczeniem[24]. Przywołane powyżej wyjaśnienie wskazuje, że definicja bezpieczeństwa informacji jest zawężona do kwestii ochrony informacji. Musi ona być również skierowana do wielu innych zagrożeń, które wcale nie muszą być bezpośrednio powiązane z jakimkolwiek nielegalnym wykorzystaniem informacji czy jego zarządzaniem. Zagrożenia te mogą obejmować niejednokrotnie działania o charakterze przestępczym, które są w stanie wykorzystać w sposób niewłaściwy narzędzia informatyczne lub samą informację.

22 Więcej zob. L. Ciborowski, *Walka informacyjna*, Toruń 1999, s. 186.

23 M. Kaliski, A. Kierkowska, G. Tomaszewski, *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa* [w:] *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, red. J. Kaczmarek, M. Kwieciński, Toruń 2010, s. 34.

24 P. Potejko, *Bezpieczeństwo informacyjne* [w:] *Bezpieczeństwo państwa. Wybrane problemy*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Warszawa 2009, s. 194.

Z kolei drugim zjawiskiem obecnym w przestrzeni publicznej, które wypracowało katalog czynów zabronionych, jest cyberprzestępczość[25]. Jest to swoisty rodzaj przestępczości, gdzie głównym narzędziem lub wykorzystywanym przedmiotem przestępstwa jest w tym przypadku komputer. Jest to zjawisko coraz bardziej obecne w codziennym życiu, w sytuacji wzmożonego wykorzystywania urządzeń teleinformatycznych korzystających z sieci internetowej. Cyberprzestępstwo to czyn zabroniony, który jest popełniony w cyberprzestrzeni. W obszarze czynów przestępczych cyberatak jest świadomym i celowym utrudnianiem prawidłowego funkcjonowania cyberprzestrzeni. Wykorzystując nowe rozwiązania technologiczne, umożliwia ominięcie lub niejednokrotnie ograniczenie zdolności sprzętowych i programowych przyjętych w jednostce mechanizmów kontroli. Cyberprzestępczość to nie tylko działanie polegające na podszywaniu się pod inne osoby w celu osiągnięcia jakichkolwiek korzyści, lecz także coraz częstsze ataki na sieci informatyczne. Działanie te są podejmowane w celu zniekształcenia, uniemożliwienia wykorzystania lub zniszczenia informacji, która może być przechowywana w komputerze lub w sieci[26].

W literaturze przedmiotu cyberprzestrzeń traktowana jest jako „[…] zależny od czasu zestaw wzajemnie połączonych systemów informatycznych oraz ludzkich użytkowników, którzy wchodzą z tymi systemami w interakcję"[27]. Według rządowego dokumentu pt. „Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej" cyberprzestrzenią jest sposób przetwarzania i wymiany informacji, tworzony przez systemy teleinformatyczne, które zapewniają przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne[28]. W dokumencie tym sformułowano cel strategiczny – osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. Podobnie jak w przyjętej „Strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej", w omawianym dokumencie jest opisywane zapewnienie akceptowanego stanu bezpieczeństwa w sieciach teleinformatycznych.

Nie ulega wątpliwości, że głównym elementem wpływającym realnie na cyberprzestrzeń są przede wszystkim zasoby materialne systemu teleinformatycznego. System ten to zespół współpracujących ze sobą urządzeń

25 Więcej zob. K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 351–353.

26 K. Chałubińska-Jentkiewicz, op. cit., s. 15.

27 Więcej zob. R. Ottis, P. Lorents, *Cyberspace: Definition and Implications* [w:] *Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8–9 April*, Reading 2010, s. 267–270.

28 *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013, s. 5.

informatycznych i oprogramowania do przetwarzania, przechowywania, wysyłania i odbierania danych za pomocą sieci telekomunikacyjnej. Według Cezarego Banasińskiego siecią telekomunikacyjną są wszelkie urządzenia przekierowujące systemy transmisyjne, a także nieaktywne elementy sieci[29]. W tym przypadku nie można utożsamiać przestrzeni cybernetycznej jedynie z siecią internet, gdyż przestrzeń ta jest bardzo rozległa i obejmuje swoim zasięgiem nie tylko sieci telekomunikacyjne, lecz także komputerowe. Można zatem wskazać, że cyberprzestrzeń to wszystkie systemy informatyczne, które wspólnie tworzą globalną sieć.

Wskazując współczesny model kształtowania administracyjnoprawnych warunków do budowy cyberbezpieczeństwa w administracji publicznej, jest zasadne wskazanie wybranych założeń ustawy z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa[30]. Zgodnie z art. 2 pkt 4 rzeczonej ustawy cyberbezpieczeństwem jest odporność systemów informacyjnych na działania, które naruszają poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Istniejący obowiązek ciążący na operatorze usługi kluczowej w organie administracji publicznej zobowiązuje go do wdrażania systemu zarządzania bezpieczeństwem w systemie informacyjnym, wykorzystywanym do świadczenia usługi kluczowej (usługa mająca kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej). Zadania te w szczególności obejmują m.in.: 1) prowadzenie systematycznego szacowania ryzyka wystąpienia potencjalnego incydentu oraz zarządzanie takim ryzykiem; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych; 3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego; 4) zarządzanie incydentami; 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego; 6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa[31].

W takim ujęciu operator usługi kluczowej jest zobowiązany do zapewnienia przeprowadzenia, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu

29 C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. idem, Warszawa 2018, s. 25.

30 Zob. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j., Dz.U. 2022, poz. 1863, z późn. zm.

31 Ibidem, art. 8.

informacyjnego. Audytor jest zobligowany do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzanym audytem bezpieczeństwa systemu informacyjnego, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych. Na podstawie zebranych dokumentów i dowodów uzyskanych w trakcie przeprowadzonych czynności audytowych audytor sporządza pisemne sprawozdanie z przeprowadzonego audytu z ustaleniami i ewentualnymi rekomendacjami, które to sprawozdanie następnie przekazuje operatorowi usługi kluczowej wraz z całą dokumentacją z przeprowadzonego audytu. Operator usługi kluczowej, u którego w danym roku w stosunku do systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej został przeprowadzony przez osoby spełniające warunki określone w art. 15 ust. 2 pkt 2 ustawy o krajowym systemie cyberbezpieczeństwa audyt wewnętrzny w zakresie bezpieczeństwa informacji[32], nie ma obowiązku przeprowadzania audytu przez 2 lata.

Zakończenie

Omawiane w tekście wybrane jedynie administracyjnoprawne warunki tworzenia cyberbezpieczeństwa w administracji publicznej odnoszą się do odporności i technicznej nieugiętości systemów informatycznych. Ma to związek z coraz częstszymi działaniami, które naruszają w dużej mierze poufność, integralność, dostępność, jednolitość czy autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Pamiętać przy tym należy, że na budowę bezpieczeństwa sieci teleinformatycznych czy strukturę cyberbezpieczeństwa w systemach administracyjnych składa się zapewnienie właściwej ochrony zasobów. W obszar tych działań wchodzi ochrona, np.: treści cyfrowych, sieci teleinformatycznych, urządzeń czy ochrona transmisji treści za pomocą samej sieci. Jest to dlatego ważne, że bez względu na to, czy niebezpieczeństwo dotyczy informatycznych systemów zarządzanych przez sektor publiczny czy prywatny, jest konieczne budowanie właściwej świadomości użytkowników potencjalnych zagrożeń i niebezpieczeństw z tego wynikających, żeby móc we właściwy sposób przygotować się do odpowiedniej reakcji i ochrony posiadanych zasobów.

32 Powyższe ustalenia wynikają z art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j., Dz.U. 2023, poz. 57).

Bibliografia

Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2018.

Błażewski M., *Zasada zapewnienia bezpieczeństwa w e-administracji*, „Folia Iuridica Universitatis Wratislaviensis" 2017, t. 6, nr 1.

Breczko A., *Cele państwa i zasadnicze kierunki jego działania* [w:] *Wprowadzenie do nauk o państwie i prawie*, red. G. Kryszeń, Białystok 2004.

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, nr 2.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

Ciborowski L., *Walka informacyjna*, Toruń 1999.

Dunaj K., *Istota bezpieczeństwa państwa* [w:] *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, red. M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, Olsztyn 2016.

Fehler W., *Bezpieczeństwo publiczne jako składnik wewnętrznego bezpieczeństwa państw*, „Bezpieczeństwo, Teoria i Praktyka", 2010, nr 1–2.

Giddens A., *Socjologia*, Warszawa 2006.

Goban-Klas T., *Cywilizacja medialna*, Warszawa 2005.

Gwardyński R., *Racjonalizacja działań Policji na poziomie lokalnym* [w:] *Racjonalizacja zarządzania jednolitymi formacjami umundurowanymi odpowiedzialnymi za bezpieczeństwo wewnętrzne*, red. B. Wiśniewski, P. Lubiewski, T. Zwęgliński, Warszawa 2020.

Kaliski M., Kierkowska A., Tomaszewski G., *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa* [w:] *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, red. J. Kaczmarek, M. Kwieciński, Toruń 2010.

Kitler W., *Bezpieczeństwo narodowe. Podstawowe kategorie, dylematy pojęciowe i próba systematyzacji*, „Towarzystwo Wiedzy Obronnej. Zeszyt Problemowy" 2010, nr 1.

Korzeniowska H., *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, Kraków 2004.

Ludziejewski Z., *Bezpieczeństwo informacyjne w instytucjach gospodarczych*, „Zeszyty Naukowe WSOWL" 2013, nr 4.

Michalak B., *Bezpieczeństwo informacji w rejestrach medycznych*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2010, z. 2.

Ottis R., Lorents P., *Cyberspace: Definition and Implications* [w:] *Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8–9 April*, Reading 2010.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013.

Potejko P., *Bezpieczeństwo informacyjne* [w:] *Bezpieczeństwo państwa. Wybrane problemy*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Warszawa 2009.

Potrzeszcz J., *Bezpieczeństwo i porządek publiczny w ujęciu filozofii prawa* [w:] *Bezpieczeństwo państwa. Zagadnienia podstawowe*, red. W. Lis, Lublin 2014.

Szmyd J., *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna* [w:] *Zarządzanie bezpieczeństwem*, red. P. Tyrała, Kraków 2000.

Ścibiorek Z., Wiśniewski B., Kuc R.B., Dawidczyk A., *Bezpieczeństwo wewnętrzne*, Toruń 2015.

Zagórski Z., *Socjologia bezpieczeństwa. O potrzebie nowej subdyscypliny?* [w:] *Socjologiczne aspekty bezpieczeństwa narodowego*, red. T. Leszczykiewicz, Z. Zagórski, Wrocław 1999.

Shaping the administrative and legal conditions for building cybersecurity in public administration

Summary

The article in question concerns the creation of administrative and legal conditions for building an appropriate cybersecurity system in public administration. Under the current legal and organizational conditions, state cyber security is becoming one of the most important strategic goals in the area of security. The number of threats and incidents in cyberspace, as well as the degree of their advancement, growing every year, is now one of the key problems faced by public administration in the area of ensuring the uninterrupted functioning of the entire state, economy and society.

Key words: public administration, law, cybersecurity, administrative law, protection mechanisms