The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Cybersecurity and Law

2026 Nr 1(15)

DOI: 10.35467/cal/221352

Kształtowanie bezpieczeństwa informacji w systemie budowania ochrony zmieniającej się administracji publicznej

Shaping information security in the system of building the protection for the changing public administration

Paweł ROMANIUK
Uniwersytet Warmińsko-Mazurski w Olsztynie
ORCID: 0000-0002-7217-956X
E-mail: pawel.romaniuk@uwm.edu.pl

Streszczenie

W artykule zwrócono uwagę na ważną rolę informacji i jej bezpieczeństwo w systemie budowania ochrony współczesnej administracji publicznej. Znaczenie informacji, w tym przypadku także i mechanizmów ochrony takich danych, wymaga zintegrowanego podejścia. Stąd przybliżone zostaną główne segmenty i zasady zarządzania bezpieczeństwem informacji w jednostkach sektora finansów publicznych. Obowiązujące przepisy prawa, regulujące mechanizmy administrowania takimi danymi, wyznaczają przy tym odpowiednie poziomy ochrony różnych informacji, będących w posiadaniu podmiotów administracji publicznej. W artykule przybliżone zostały wybrane, z uwagi na złożony charakter poruszanego zagadnienia, te obszary, które wdrażane są przez organy administracji publicznej w obszarze kształtowania bezpieczeństwa informacji. Wskazane zostaną również warunki wzmacniania świadomości pracowników, związanych z zagrożeniami informacyjnymi i informatycznymi w administracji publicznej, wspartej odpowiednim zaangażowaniem kierownictwa jednostki.

Słowa kluczowe

administracja publiczna, informacja, bezpieczeństwo informacji, zagrożenie, ochrona

Abstract

The text highlights the use of information and its security in the public administration's public security system. The importance of information, including the application of data protection requirements, is discussed. The main segments and principles of information management in public finance sector entities are presented. Applicable regulations, administrative powers, and administrative tools define the horizontal principles for protecting various types of information held by public

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

administration bodies. The article provides a selection of those used by public administration bodies in shaping information security, with comments on the general nature of their operations. It is also necessary to ensure increased employee awareness of information and IT threats in public administration, supported by disclosure from the unit's management.

Keywords
public administration, information, information security, threat, protection.

Wprowadzenie

Podmioty administracji publicznej pełnią ważną rolę w życiu społeczno-gospodarczym społeczeństwa. Posiadają z każdym rokiem coraz więcej informacji i wypełniając swoje zadania, przetwarzają szeroki zakres informacji obywateli. To właśnie z takimi podmiotami mieszkańcy mają najczęstszy kontakt, który - wraz z naturalnym rozwojem usług e-usług - powoli zaczyna przenosić się w sferę cyfrową. Obecnie, blisko 65 tyś. instytucji sektora publicznego, posiada dostęp do szerokiego zakresu informacji, które są fundamentalne dla funkcjonowania państwa. Gromadzą one m.in. informacje dotyczące obywateli, dane o majątku publicznym, przebiegu kontroli, umowach cywilnoprawnych a także treści wielu aktów administracyjnych i orzeczeń sądowych. Ponadto instytucje publiczne, dysponujące w ramach obowiązującego prawa, dostępem do ogromnych zbiorów danych, od rejestrów państwowych po informacje przestrzenne, stają się swoistym „opiekunem" takich danych i odpowiadają za ich prawidłową ochronę. Umiejętne wykorzystanie różnych zasobów informacji (danych), pozwala nie tylko na zwiększenie przejrzystości działań władz publicznych, ale również umożliwia podejmowanie świadomych decyzji.

Współczesne zastosowanie narzędzi informatycznych do pracy, rozrywki, czy pozyskiwania informacji, stało się bardzo powszechne i nikt nie wyobraża sobie życia bez tego typu rozwiązań. Powszechność korzystania z zasobów informatycznych wskazuje, że nie zawsze poziom wiedzy, dotyczący przepływu informacji w Internecie, jest wystraczający. Także realizacja zadań przez samą administrację publiczną, również narażona jest na wiele niebezpieczeństw, często związanych z wymianą zbiorów elektronicznych danych, które powinny być właściwie chronione. Działanie takie powinno być podjęte przy aktywnym uczestnictwie wszystkich pracowników, tym bardziej, że konsekwencji związane z naruszeniem bezpieczeństwa informacji, niezwykle trudno dziś realnie oszacować.

Głównym celem pracy, z uwagi na ograniczone ramy objętościowe, jest wskazanie warunków bezpieczeństwa informacji w systemie budowania ochrony współczesnej i zmieniającej się administracji publicznej. Wśród sposobów i metod badawczych, jakimi się posłużono, znaczną rolę odegrała metoda opisowa.

W celu wnioskowania na podstawie poczynionych obserwacji a także dokonanych badań, wykorzystano metodą weryfikacji. Przeprowadzone założenia wskazują, że w obszarach zmian technologicznych w administracji publicznej, wykorzystującej aktywnie narzędzia komunikacyjne i elektroniczne, nastąpił widoczny progres. Bardzo pozytywnym efektem wyników jest zwiększająca się dość dynamicznie dostępność do e-usług. Kluczowe wnioski płynące z analizy i przeprowadzonych badań, skierowane są na budowanie ochrony danych administracji publicznej, jako kluczowego elementu

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

informatyzacji. Należy również prowadzić zintensyfikowaną politykę informacyjną i edukacyjną w zakresie wzmacniania systemów bezpieczeństwa informacji.

Model bezpieczeństwa w systemie demokratycznego państwa prawa

Na początku należy zastanowić się nad problematyką bezpieczeństwa i samego pojęcia „bezpieczeństwo". W każdym demokratycznym pastwie prawnym, bezpieczeństwo należy do głównych i niezaprzeczalnych wartości, które oddziałują zarówno na prawidłowe funkcjonowanie całego państwa i jego organów, ale również na społeczeństwo, pobudzając jego właściwą egzystencję i poczucie spokoju[1]. Trzeba zaznaczyć, że poczucie bezpieczeństwa zawsze było obecne i towarzyszyło ludzkości od początku jej istnienia. Gwarantując odpowiedni poziom bezpieczeństwa, obok działalności ludzkiej, duże znaczenie przybierają również czynniki naturalne, które powiązane są z różnymi żywiołami i środowiskiem. Nie raz zdarzały się sytuacje, że wielka potęga i moc różnorodnych żywiołów natury, pokazała swoją prawdziwą „twarz", powodując niejednokrotnie katastrofy wielkich rozmiarów[2]. Pomimo tego, że nauka o bezpieczeństwie jest zdecydowanie wciąż młodą dyscypliną naukową, to trudno wymienić dziś wszystkie obecne próby zdefiniowania pojęcia bezpieczeństwa, jakie podjęto od momentu rozpoczęcia badań tego nurtu naukowego[3]. Współcześni badacze, którzy na co dzień zajmują się zagadnieniem bezpieczeństwa, przedstawiają różne jego definicje, zwracając uwagę na liczne parametry. Zapewnienie bezpieczeństwa stanowi cel działania każdego państwa, wyznaczając jego charakter oraz określoną potrzebę społeczną, która powinna być nieustannie zaspakajana, wzbudzająca przy tym poczucie spokoju i należytej ochrony[4].

Nie istnieje również legalna definicja tego pojęcia, co pokazuje, że w doktrynie różne są jego odmiany i formy oceny[5]. Samo to pojęcie, nieustannie przyczynia się do jakże istotnej polemiki naukowej oraz dyskusji teoretyków i praktyków. Można przyjąć z pełną odpowiedzialnością, że bezpieczeństwo i zapewnienie jego właściwego i akceptowanego poziomu, oznacza stan braku potencjalnego i realnego zagrożenia[6]. Należy podkreślić, 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

[1] M. Karpiuk, K. Orzeszyna, Wstęp [w:] M. Karpiuk, K. Orzeszyna (red.), Bezpieczeństwo narodowe Rzeczypospolitej Polskiej. Wybrane zagadnienia prawne, Warszawa 2014, s. 5.
[2] B. Bonisławska, Zadania administracji samorządowej w zakresie bezpieczeństwa publicznego - wybrane zagadnienia, „Teka of Political Science and International Relations" 2021, vol. 16, nr 2, s. 49.
[3] A. Furgała, Bezpieczeństwo wewnętrzne - dylematy definicyjne w kontekście zmian ewolucyjnych i rozwoju społeczno-gospodarczego państwa, „Przegląd Policyjny" 2020, nr 3(139), s. 186.
[4] M. Karpiuk, Prawne podstawy bezpieczeństwa [w:] A. Żukowski, M. Hartliński, W.T. Modzelewski, J. Więcławski (red.), Podstawowe kategorie bezpieczeństwa narodowego, Olsztyn 2015, s. 66.
[5] J. Potrzeszcz, Bezpieczeństwo i porządek publiczny w ujęciu filozofii prawa [w:] W. Lis (red.), Bezpieczeństwo państwa. Zagadnienia podstawowe, Lublin 2014, s. 15.
[6] Z. Ściborek, B. Wiśniewski, R.B. Kuc, A. Dawidczyk, Bezpieczeństwo wewnętrzne, Toruń 2015, s. 26.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

jednostki, grupy społecznej czy zbiorowości. Z kolei drugi ma charakter subiektywny i jest poczuciem bezpieczeństwa”[7]. Bezpieczeństwo w takim ujęciu staje się walorem niezwykle generalnym i dotyczy coraz to większej grupy odbiorców. W doktrynie obecne są różnorodne kategorie bezpieczeństwa, które pojawiają się w strukturach administracyjnych w zależności od prawnej sfery aktywności danego podmiotu[8].

Dodatkowo pojęcie „bezpieczeństwo” występuje w rożnych uwarunkowaniach, konfiguracjach i znaczeniach. W literaturze przedmiotu można spotkać się z różnymi terminami, np. bezpieczeństwo publiczne, bezpieczeństwo obywateli, bezpieczeństwo państwa, czy bezpieczeństwo cyfrowe. Określenie to wskazywane jest również wielokrotnie w Konstytucji Rzeczypospolitej Polskiej[9]. Jest to o tyle ważne, że problematyka bezpieczeństwa stała się kluczowym filarem funkcjonowania państwa, które odnalazło swoje miejsce w ustawie zasadniczej[10]. W języku prawnym, także na poziome konstytucyjnym, pojawia się również określenie typu wewnętrzne lub zewnętrzne zagrożenie państwa[11]. Ciekawe stanowisko prezentuje S. Sulowski, traktujący bezpieczeństwo, jako sytuację, w której istnieje „(…) stała gotowość i działalność określonych instytucji i organów państwowych, a także prywatnych podmiotów, która ma znaczenie dla zachowania stabilności i integralności państwa”[12]. Interesującą próbę oceny bezpieczeństwa przedstawiają E. Ura i S. Pieprzny, którzy twierdzą, że głównym wyznacznikiem bezpieczeństwa, w tym bezpieczeństwa wewnętrznego jest fakt, iż jego konsekwencje widoczne są w wewnątrz państwa, przy czym „bezpieczeństwo wewnętrzne jest kategorią ogólną, zawierającą w swej treści wiele jego rodzajów bezpieczeństwa dookreślanego chronionym dobrem lub zagrożeniem, np. bezpieczeństwo ekologiczne, społeczne, pożarowe”[13].

Bezpieczeństwo informacji jako fundament zaufania do cyfrowego państwa

Wdrażanie wskazanych administracji publicznej przez ustawodawcę zadań, wymaga w obowiązującym porządku prawnym, posiadania coraz większej ilości różnych informacji. Jednak zakres przedmiotowy takich informacji, bywa także kreowany w sposób normatywny, gdzie musi być brane pod uwagę sposób i narzędzia do wykonania precyzyjnie wyznaczonego zadania. Pojawia się przy tym ocena niezwykle ważnego zagadnienia, jakim jest społeczny popyt na informację oraz możliwość dostępu do takiej informacji. Ciekawe spostrzeżenie w analizowanym temacie przedstawia K. Liderman, dla którego

[7] Zob. szerzej: H. Korzeniowska, Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji, Kraków 2004, s. 8-10.
[8] Por. K. Dunaj, Istota bezpieczeństwa państwa [w:] M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop (red.), Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne, Olsztyn 2016, s. 17-18.
[9] Konstytucyjne założenia bezpieczeństwa są zdeponowane m.in. w: art. 5, 45 ust. 2, 74 ust. 1, 146 ust. 4 pkt 7-8 Konstytucji Rzeczypospolitej Polskiej z dnia 7 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78 poz. 483 ze zm.).
[10] Patrz: J. Filaber, Pojęcie bezpieczeństwa publicznego w prawie administracyjnym (wybrane uwagi), „Wrocławskie Studia Erazmiańskie. Zeszyty Studenckie. Prace prawnicze, administratywistyczne i historyczne”, Wrocław 2009, s. 246-248.
[11] Por. S. Pieprzny, Administracja bezpieczeństwa i porządku publicznego, Rzeszów, 2014, s. 26-36.
[12] Por. S. Sulowski, W poszukiwaniu definicji bezpieczeństwa wewnętrznego, „Przegląd Bezpieczeństwa Wewnętrznego” 2009, nr 1, s. 13-14.
[13] E. Ura, S. Pieprzny, Bezpieczeństwo wewnętrzne państwa, Rzeszów 2015, s. 22.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

rozwój elektroniki, rozwój sieci teleinformacyjnych, coraz bardziej widoczna powszechność urządzeń dostępowych, powstanie sieci społecznościowych czy wykorzystywanie sieci publicznych do przesyłania informacji dla różnych systemów administracyjnych i przemysłowych powoduje, iż informacja taka staje się ważnym czynnikiem wyodrębnienia nie tylko wiedzy i władzy, ale i także działaniem, decydującym o poziomie bezpieczeństwie obywateli, organizacji czy całych państw[14].

Niezwykle dynamiczny rozwój społeczeństwa informacyjnego, oparty na procesie wytwarzania, gromadzenia, przekazywania, przechowywania i w konsekwencji wykorzystania informacji – należy do fundamentalnych obowiązków, leżących po stronie szeroko rozumianej administracji publicznej. Podjęcie właściwej ścieżki zarządzania dokumentami a tym samym i informacji, wpływa bez wątpienia nie tylko na budowanie zaufania do instytucji publicznych, ale również zapewnia transparentność działań państwa, przy jednoczesnym zachowaniu ochrony danych osobowych i innych tajemnic prawnie chronionych. Zmieniające i rozwijające się w sposób naturalny społeczeństwo informacyjne, budujące gospodarkę opartą na innowacyjności i wiedzy a także dające powszechny dostęp do wielu technologii (np. e-administracja, e-bankowość), zaczęło przywiązywać, i nie bez znaczenia, coraz większą uwagę na zagadnienia bezpieczeństwa informacji w konstrukcji prawidłowo funkcjonujących instytucji publicznych[15].

Omawiane niezwykle ważne bezpieczeństwo informacji, stało się nie tylko przestrzeganą normą czy wymogiem współczesności. Zagadnienie to stanowi priorytet dla prawidłowo funkcjonującej administracji publicznej i jest również jej obowiązkiem w zakresie skutecznego i zgodnego z prawem zarządzania informacjami[16]. Przy czym, traktując wartość i znaczenie każdej informacji w społeczeństwie informacyjnym i w całym systemie administracji publicznej, jako kluczowy jej atrybut, ważnym zagadnieniem stało się formułowanie odpowiedniego systemu jej bezpieczeństwa. Proces taki ze swojej natury jest niezwykle złożony i co istotne, ustawodawca nie próbuje konstruować jednoznacznych i konkretnych rozwiązań w tym zakresie. Pokazuje konieczność podjęcia skutecznych, ukierunkowanych i adekwatnych działań, mając na względzie aktualny stan wiedzy technologicznej, który dynamicznie się zmienia, koszt wdrażania a także zakres i cele przetwarzania różnych informacji i danych, będących w posiadaniu podmiotów administracji publicznej[17].

Bezpieczeństwo informacji jest kluczowe, zarówno dla podmiotów sektora prywatnego, jak i jednostek sektora finansów publicznych. Obserwuje się nieustanne uzależnienie od sieci Internet, gdzie wszelakie informacje narażone są na coraz to większą liczbę i różnorodność niebezpieczeństw i zagrożeń cyfrowych. Ważna przy tym staje się implementacja odpowiednich środków bezpieczeństwa w celu odpowiedniego zabezpieczenia informacji przed świadomym lub nieumyślnym jej zmodyfikowaniem, zniszczeniem czy wręcz

[14] Por.: K. Liderman, Bezpieczeństwo informacyjne, Warszawa 2012, s. 11-12.

[15] Por. A. Suchorzewska, Rozdział I. Społeczeństwo w dobie rozwoju sieci teleinformatycznych 6. Współczesne zagrożenia informacyjne, [w:] A. Suchorzewska, Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem, Oficyna 2010 Lex/el.

[16] Patrz: J. Kowalewski, M. Kowalewski, Polityka bezpieczeństwa informacji w praktyce, Wrocław 2004, s. 21-23.

[17] Podobne założenia nakreśla art. 25 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE. L. z 2016 nr 119, poz. 1).

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

bezprawnym ujawnieniem[18]. Podstawowe elementy informacji związane z jej prawidłową ochroną, dotyczą kilku paramentów, do których należy w szczególności:

- poufność (tajność) informuje o poziomie ochrony, przy czym stopień ten jest tworzony przez wytwórcę lub dostawcę informacji lub użytkownika, bądź odbiorcę informacji;
- integralność oznacza, że informacje są poprawne i niczym nie zmienione, czyli kompletne i nienaruszone;
- dostępność informuje zazwyczaj o zakresie i upoważnieniu osób, które otrzymały dostęp do informacji i związanych z nią aktywów, kiedy jest to uzasadnione i niezbędne[19].

Każda informacja może pochodzić z wielu źródeł, które nie zawsze są wiarygodne i oparte na sprawdzonych źródłach. Informacja, przebywająca niekiedy „dłuższą drogę", docierająca pod drodze do wielu odbiorców, może niestety ulegać wielu zniekształceniom, nie zawsze kontrolowanym. Może to w konsekwencji wpłynąć nie tylko na jej ważną treść, ale i również i cenną wartość informacji[20]. Jeżeli taka sytuacja miała miejsce, rozsądnym jest stworzenie odpowiedniej ochrony informacji pod względem jej poufności, dokładności i integralności. Przywoływana poufność informacji jest sytuacją dzielenia się informacją wyłącznie z tymi osobami lub grupą osób, dla których jest to niezbędne do wypełniania obowiązków, posiadających prawną legitymację do jej dostępu i wykorzystania. Dokładność jest ważnym elementem wiarygodności każdej informacji. Oznacza to, że taka informacja pochodzi z wiarygodnego i rzetelnego źródła i łączy się w sposób naturalny z jej integralnością. Integralność jest zatem swego rodzaju pewnością, iż wraz z upływem czasu, informacja nie zostanie przez różne czynniki zniekształcona lub nie utraci swojej wartości w następstwie jej nieautoryzowanej modyfikacji. Z integralnością utożsamiana jest także dostępność informacji, która może być wykorzystana w sposób całkowicie prawidłowy. Jest to także stan pewności, że dane pozostają spójne i prawdziwe w każdym momencie i są odpowiednio chronione przed przypadkowym zniekształceniem lub nieautoryzowaną zmianą[21].

Podejmowana problematyka bezpieczeństwa informacji, może być również łączona ze stanem gwarancji odpowiednich warunków zewnętrznych i wewnętrznych, w których instytucje publiczne mogą swobodnie doskonalić mechanizmy ochrony danych. Istnieją przy tym warunki konieczne do zapewnienia skutecznego i funkcjonalnego mechanizmu bezpieczeństwa informacji, do których zalicza się m.in. prawidłowo zabezpieczone strategiczne zasoby, sprawnie funkcjonujące sieci teleinformatyczne, które tworzą krytyczną infrastrukturę teleinformatyczną państwa czy zagwarantowana przez państwo

[18] A. Myśko, E. Młodzik, Bezpieczeństwo informacji - dylematy związane z realizacją obowiązku prowadzenia audytu wewnętrznego w jednostkach sektora finansów publicznych, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 833; „Finanse, Rynki Finansowe, Ubezpieczenia" 2014, nr 72, s. 109.

[19] Zob. szerzej: N. Pazio, Polityka bezpieczeństwa jako element zarządzania ryzykiem operacyjnym [w:] Zarządzanie ryzykiem działalności organizacji, J. Monkiewicz, L. Gąsiorkiewicz (red.), Warszawa, s. 176-177.

[20] Warunki formowania informacji i zarządzania bezpieczeństwem informacji prezentuje: M. Beskosty, Zarządzanie bezpieczeństwem informacji, „Studia nad Bezpieczeństwem" 2017, nr 2, s. 163-164.

[21] D. Fleszer, Wokół problematyki bezpieczeństwa informacji, „Roczniki Administracji i Prawa", nr XVIII(1), s. 188-190.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

ochrona informacji niejawnych i wszelkich innych informacji prawnie chronionych[22].

Dostrzega się, że podmioty publiczne budują platformy cyfrowe, związane z agregacją danych, kształtując w ten sposób politykę bezpieczeństwa organizacji. Polityka taka zawiera strukturę organizacyjną, która zapewnia realny podział i koordynację zadań oraz odpowiedzialność, związaną z zapewnieniem skutecznego stopnia bezpieczeństwa informacji i innych informacji prawnie chronionych. Często takie działania traktowane są jako kształtowanie bezpieczeństwa narodowego[23]. Czynności takie zmierzają do przetwarzania takich danych nie tylko metodami tradycyjnymi, ale również wykorzystując nowoczesne systemy informatyczne.

Warto zauważyć, że polityka bezpieczeństwa informacji w podmiotach administracji publicznej jest systemem zarządzania, który dotyczy administrowania, zarówno systemami informatycznymi, ale również i całą organizacją. Zapewnienie bezpieczeństwa informacji, szczególnie w okresie wszechobecnej dezinformacji, widoczne jest najczęściej poprzez jasne komunikowanie przez zarządzających i przedstawienie obowiązujących zasad w zakresie budowania właściwego poziomu bezpieczeństwa. Procedury bezpieczeństwa formalizowane są za pomocą przyjmowanych aktów normatywnych, zarządzeń lub decyzji. Postawa ta ma na celu ujednolicenie działań obronnych i ochronnych, co pozwala na sprawną realizację zadań publicznych zgodnie z obowiązującymi przepisami prawa. Ponadto wdrażanie sformalizowanych zasad, w tym polityki bezpieczeństwa informacji, jest kluczowe dla ochrony danych osobowych, tajemnicy służbowej oraz zapewnienia ciągłości działania urzędów. Nie można zapominać, że procedury takie powinny być wynikiem analizy ryzyka, dopasowane do specyfiki danej jednostki publicznej, a nie stanowić jedynie zbiór uniwersalnych szablonów. Zatem kluczowym elementem formalnych procedur, jest nie tylko ich ustanowienie, ale także regularna aktualizacja, monitorowanie oraz wzmacnianie świadomości i szkolenie pracowników w zakresie ich stosowania[24]. Ma to o tyle ważne znaczenie dla całego systemu administracji publicznej, gdyż odpowiedzialne zarządzanie informacją i jej bezpieczeństwem, prowadzone za pomocą przyjętych rekomendacji i procedur, w sposób oczekiwany, wpływać może również na budowę właściwej kultury organizacyjnej[25].

Na zakończenie tych krótkich rozważań w obszarze bezpieczeństwa informacji, warto wspomnieć o towarzyszącej temu działaniu gwarancji bezpieczeństwa. Z procesem tym wiąże się silna potrzeba zapewnienia cyberbezpieczeństwa w systemie funkcjonujących podmiotów administracji publicznej. Z każdym dniem coraz więcej działań podejmowanych jest w przestrzeni cyfrowej. Przestrzeń tę wyróżnia dość charakterystyczna i zmienna kultura zachowań jej użytkowników, zwiększająca wirtualną społeczność. Z punktu widzenia interesów instytucji publicznych, należy dbać o zapewnienie odpowiedniego poziomu kontroli nad obszarem funkcjonujących w nich sieci teleinformatycznych. Systemy te każdego roku zarządzają coraz większą ilością

[22] Zob. szerzej: E. Nowak, M. Nowak, Zarys teorii bezpieczeństwa narodowego, Warszawa 2011, s. 103.

[23] Zob.: L. Grosicki, Zakres przedmiotowy bezpieczeństwa wewnętrznego państwa [w:] K. Grosicka, L. Grosicki, P. Grosicki (red.), Organizacja i kierowanie instytucjami bezpieczeństwa wewnętrznego państwa, Pułtusk-Warszawa 2013, s. 18.19.

[24] Por. M. Błażewski, Zasada zapewnienia bezpieczeństwa w e-administracji, „Folia Iuridica Universitatis Wratislaviensis" 2017, vol. 6 (1), 107-113

[25] T. Kifner, Polityka bezpieczeństwa i ochrony informacji, Gliwice 2013, s. 14.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

danych i informacji, które w sytuacji ich nieuprawnionego udostepnienia, jeżeli są informacjami prawnie chronionymi, mogłoby narazić takie podmioty na różnego rodzaju straty. Mogłaby to być np. utrata zaufania publicznego, destabilizacja działania organu administracji publicznej oraz odpowiedzialność karna lub dyscyplinarna pracowników za ujawnienie tajemnicy ustawowo chronionej.

Tematyka coraz częściej omawianego i niezbędnego do prowadzenia w administracji publicznej cyberbezpieczeństwa - „(…) odnosić się może do ściśle określonego obszaru działa związanych z bezpieczeństwem informacji (zawartości sieci), bezpieczeństwem komunikowania (przekazu) oraz bezpieczeństwem samej sieci umożliwiających komunikowanie, jednak nie wyczerpuje wszystkich kwestii związanych z potrzebami ochrony przed niepożądanymi działaniami w cyberprzestrzeni”[26]. Cyberbezpieczeństwo jest również procesem, gwarantującym bezpieczne funkcjonowanie w cyberprzestrzeni instytucji publicznej jako całości, jego wszystkich struktur, osób fizycznych, prawnych a także pozostałych podmiotów oraz zasobów informacyjnych, będących w globalnej cyberprzestrzeni[27]. Cyberbezpieczeństwo jest również bezpieczeństwem sieci i systemów teleinformatycznych, szczególnie traktowane jako odporność systemów teleinformatycznych na działania naruszające w szczególności: dostępność, integralność, autentyczność lub poufność przechowywania, przekazywania, przetwarzania danych lub związanych z nimi usług cyfrowych[28]. Ważnym również z punktu widzenia budowy systemu cyberbezpieczeństwa, jest znowelizowana niedawno ustawa o krajowym systemie cyberbezpieczeństwa[29].

Podsumowanie

Zapewnienie i utrzymanie właściwego poziomu bezpieczeństwa informacji w instytucjach publicznych, jest nie tylko normą, ale również i obowiązkiem. Podmioty te są nieustannie narażane na możliwość popełnienia wobec nich różnych ataków cybernetycznych, wycieków danych a także nieautoryzowanego dostępu do wrażliwych informacji, co może prowadzić do poważnych konsekwencji dla samych instytucji, w których dane są przetwarzane. Ponadto, kształtowanie bezpieczeństwa informacji w systemie budowania ochrony współczesnej administracji publicznej jest niezwykle istotnym zagadnieniem w kontekście dynamicznie rozwijającej się cyfryzacji oraz wzrastającej liczby zagrożeń związanych z cyberprzestępczością. Współczesne państwo opiera swoje funkcjonowanie na systemach informacyjnych, które przechowują,

[26] K. Chałubińska-Jentkiewicz, Cyberbezpieczeństwo - zagadnienia definicyjne, „Cybersecurity and Law” 2019, nr 2, s. 13.

[27] Ważną uwagę nad cyberbezpieczeństwem prezentuje: C. Banasiński, Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni [w:] C. Banasiński (red.), Cyberbezpieczeństwo. Zarys wykładu, Warszawa 2018, s. 31.

[28] Warunki odporności systemów teleinformatycznych przedstawia: A. Brzostek, Cyberbezpieczeństwo w administracji publicznej - zagadnienia prawne, „Zeszyty Prawnicze”, 2023, nr 23, s. 97.

[29] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 ze zm.). Ustawa ta dotyczy bezpieczeństwa informacji i obejmuje przede wszystkim zarządzanie ryzykiem, ochronę systemów informacyjnych, raportowania incydentów oraz wdrażania procedur organizacyjno-technicznych przez kluczowe podmioty. Jej celem jest zapewnienie poufności, integralności, dostępności i autentyczności danych przetwarzanych w systemach informacyjnych a także wskazuje metody sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

przetwarzają i udostępniają dane o charakterze publicznym. Zapewnienie odpowiedniego poziomu bezpieczeństwa tych informacji ma kluczowe znaczenie zarówno dla ochrony prywatności obywateli, jak i dla sprawnego funkcjonowania administracji publicznej.

Należy także nieustannie przypominać o ważnych założeniach *de lege ferenda* w zakresie polityki bezpieczeństwa. Zasadnym staje się opracowanie kompleksowej polityki bezpieczeństwa informacji oraz systematycznej oceny ryzyka, aby w miarę szybko identyfikować i minimalizować potencjalne zagrożenia. Pomocnym narzędziem w administracji publicznej są regularne audyty bezpieczeństwa informacji, które pomagają dostosować te polityki do zmieniającego się środowiska zagrożeń. Ważnym czynnikiem wzmacniania system ochrony informacji, jest również budowanie świadomości użytkowników. Pracownicy administracji publicznej powinni uczestniczyć w regularnych szkoleniach na temat zagrożeń, takich jak m.in. *phishing*, *malware* czy zasady przechowywania i udostępniania informacji, aby minimalizować ryzyko błędów ludzkich. Nie można przy tym zapominać o konieczności zabezpieczenia danych wrażliwych, które powinny być odpowiednio szyfrowane, zarówno podczas przechowywania, jak i przesyłania. Ponadto, dostęp do tych informacji, powinien być ściśle kontrolowany i ograniczony tylko do uprawnionych osób. Ważnym jest także testowanie i monitorowanie systemów informatycznych. To właśnie przeprowadzanie regularnych testów penetracyjnych oraz monitoring takich systemów, ma na celu wykrywanie ewentualnych luk w zabezpieczeniach i nieautoryzowanych próbach dostępu, gdzie wczesne wykrycie może zapobiec poważnym incydentom bezpieczeństwa. Nieustannie rozwijając zatem metody ochrony informacji, wzmacnia się jednocześnie poziom zaufania społecznego do instytucji publicznych, które w coraz większym zakresie administrują i zarządzają różnymi informacjami i danymi a także monitorują cyberzagrożenia w czasie rzeczywistym, wymuszając rygorystyczną kontrolę dostępu oraz gwarantują zgodność z przepisami i wymogami bezpieczeństwa krajowego.

Bibliografia

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 7 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78 poz. 483 ze zm.).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 ze zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE. L. z 2016 nr 119, poz. 1).

Literatura

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

Beskosty M., Zarządzanie bezpieczeństwem informacji, „Studia nad Bezpieczeństwem", 2017, nr 2.

Błażewski M., Zasada zapewnienia bezpieczeństwa w e-administracji, „Folia Iuridica Universitatis Wratislaviensis" 2017, vol. 6(1).

Bonisławska B., Zadania administracji samorządowej w zakresie bezpieczeństwa publicznego - wybrane zagadnienia, „Teka of Political Science and International Relations" 2021, vol. 16, nr 2.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Brzostek A., Cyberbezpieczeństwo w administracji publicznej - zagadnienia prawne, „Zeszyty Prawnicze” 2023, nr 23.
Chałubińska-Jentkiewicz K., Cyberbezpieczeństwo - zagadnienia definicyjne, „Cybersecurity and Law”, 2019, nr 2.
Dunaj K., Istota bezpieczeństwa państwa [w:] M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop (red.), Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne, Olsztyn 2016.
Dzierżyńska-Mielczarek J., Rynek mediów w Polsce, Warszawa 2018.
Filaber J., Pojęcie bezpieczeństwa publicznego w prawie administracyjnym (wybrane uwagi), „Wrocławskie Studia Erazmiańskie. Zeszyty Studenckie. Prace prawnicze, administratywistyczne i historyczne” Wrocław 2009.
Fleszer D., Wokół problematyki bezpieczeństwa informacji, „Roczniki Administracji i Prawa”, nr XVIII(1).
Furgała A., Bezpieczeństwo wewnętrzne - dylematy definicyjne w kontekście zmian ewolucyjnych i rozwoju społeczno-gospodarczego państwa, „Przegląd Policyjny”, 2020, nr 3(139).
Grosicki L., Zakres przedmiotowy bezpieczeństwa wewnętrznego państwa [w:] K.Grosicka, L. Grosicki, P. Grosicki (red.) Organizacja i kierowanie instytucjami bezpieczeństwa wewnętrznego państwa, Pułtusk-Warszawa 2013.
Karpiuk M., Prawne podstawy bezpieczeństwa [w:] Żukowski, M. Hartliński, W.T. Modzelewski, J. Więcławski (red.), Podstawowe kategorie bezpieczeństwa narodowego, Olsztyn 2015.
Karpiuk M., Orzeszyna K., Wstęp [w:] M. Karpiuk, K. Orzeszyna (red.), Bezpieczeństwo narodowe Rzeczypospolitej Polskiej. Wybrane zagadnienia prawne, Warszawa 2014.
Kifner T., Polityka bezpieczeństwa i ochrony informacji, Gliwice 2013.
Korzeniowska H., Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji, Kraków 2004.
Kowalewski J., Kowalewski M., Polityka bezpieczeństwa informacji w praktyce, Wrocław 2004.
Liderman K., Bezpieczeństwo informacyjne, Warszawa 2012.
Myśko A., Młodzik E., Bezpieczeństwo informacji - dylematy związane z realizacją obowiązku prowadzenia audytu wewnętrznego w jednostkach sektora finansów publicznych, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 833; „Finanse, Rynki Finansowe, Ubezpieczenia” 2014, nr 72.
Nowak E., Nowak M., Zarys teorii bezpieczeństwa narodowego, Warszawa 2011.
Pieprzny S., Administracja bezpieczeństwa i porządku publicznego, Rzeszów,2014.
Potrzeszcz J., Bezpieczeństwo i porządek publiczny w ujęciu filozofii prawa [w:] W. Lis (red.) Bezpieczeństwo państwa. Zagadnienia podstawowe, Lublin 2014.
Safjan M., Ochrona danych osobowych – granice autonomii i informacji [w:] M. Wyrzykowski (red.), Ochrona danych osobowych, Warszawa 1999.
Suchorzewska A., Rozdział I. Społeczeństwo w dobie rozwoju sieci teleinformatycznych 6. Współczesne zagrożenia informacyjne [w:] A. Suchorzewska, Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem, Warszawa 2010.
Sulowski S., W poszukiwaniu definicji bezpieczeństwa wewnętrznego, „Przegląd Bezpieczeństwa Wewnętrznego” 2009, nr 1.
Ściborek Z., Wiśniewski B., Kuc R. B., Dawidczyk A., Bezpieczeństwo wewnętrzne, Toruń 2015.
Ura E., Pieprzny S., Bezpieczeństwo wewnętrzne państwa, Rzeszów 2015.
Wojnicka E., Prawo do wizerunku w ustawodawstwie polskim, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego” 1990, nr 56.