E-ISSN 2544-9567
ISSN 1230-3801

Zeszyt 167 nr 5/2023, str. 149 - 159

POLSKIE PODEJŚCIE DO BEZPIECZEŃSTWA INFORMACYJNEGO

Karolina MIKUSEK, *karolina.mikusek@interia.pl,* ORCID: 0009-0006-1645-7605
Akademia Sztuki Wojennej, Wydział Bezpieczeństwa Narodowego

DOI 10.5604/01.3001.0054.3001

Streszczenie: W obecnie funkcjonującym środowisku bezpieczeństwa istnieje coraz większa potrzeba zwrócenia uwagi na aspekt informacyjny. Wraz z rozwojem nowych technologii oraz przestrzeni internetowej, przepływ informacji stanowi ważny proces wymagający odpowiedniej ochrony na każdym etapie jego trwania. Nie ulega wątpliwości, że w zależności od posiadanego potencjału naukowego oraz technologicznego każde z państw podchodzi do wspomnianej tematyki w indywidulany sposób. Niektóre kwestie pozostają ze sobą spójne ze względu na aspekt unifikacji norm i standardów, podczas gdy inne opierają się na unikalnych doświadczeniach i wypracowanych praktykach. W związku z tym przedmiotem niniejszych rozważań jest polskie podejście do bezpieczeństwa informacyjnego, ze szczególnym uwzględnieniem podstaw prawnych oraz założeń strategicznych dotyczących bezpieczeństwa informacyjnego. Odniesiono się również do kwestii podmiotów odpowiedzialnych za zapewnienie ochrony potencjału informacyjnego oraz rozwiązań umożliwiających podjęcie działań związanych z omawianą tematyką.

Słowa kluczowe: informacja, bezpieczeństwo narodowe, bezpieczeństwo informacyjne, krajowy system cyberbezpieczeństwa CSIRT, NSC

1. Wstęp

W obecnie rozwijającym się świecie coraz większego znaczenia zaczyna nabierać informacja. Sposób pojmowania omawianego zagadnienia uzależniony jest od licznych aspektów zdeterminowanych przez kategorie badawcze, umożliwiające dokonanie analizy wspomnianej kwestii. W związku z tym informacja może być postrzegana zarówno jako wartość strategiczna, determinująca planowanie i wdrażanie działań korzystnych z perspektywy państwa, jak również przetworzony zakres danych o otaczającym nas świecie. Niezależnie od interpretacji oraz charakterystyki wspomnianego pojęcia, wiele grup funkcjonujących w ramach państwa można scharakteryzować jako społeczeństwa informacyjne. Rozumiane jako grupa społeczna znajdująca się w obrębie sfery wpływów nowoczesnych mediów o różnym natężeniu oraz sile[1] utożsamia swoje szanse na rozwój poprzez pozyskanie, gromadzenie oraz przetwarzanie informacji. W ten sposób istnieje szansa na uzyskanie wiedzy na temat środowiska rozwoju danej społeczności, a także podejmowania kluczowych decyzji umożliwiających dalsze przetrwanie i zapobieganie prawdopodobnym zagrożeniom.

W związku z tym tak istotnym aspektem jest zapewnienie bezpieczeństwa oraz utrzymania podstawowych wartości związanych z informacją. Dlatego też coraz częstszą praktyką jest stosowanie pojęcia bezpieczeństwa informacyjnego w kategoriach części składowej bez-

[1] M. Golka, *Czym jest społeczeństwo informacyjne?*, [w:] „Ruch prawniczy, ekonomiczny i socjologiczny". (wyd.) , 2005, zeszyt 5, s. 257.

pieczeństwa narodowego. W ten sposób możliwe jest opracowanie praktyk związanych z odpowiednim zabezpieczeniem działań dokonywanych na informacji w odniesieniu do interesów narodowych oraz celów strategicznych kraju. Wiele państw, w tym również Rzeczpospolita Polska, podejmuje szereg starań, umożliwiających zapewnienie wspomnianych kwestii. Biorąc pod uwagę powyższe rozważania przedmiotem niniejszego artykułu jest omówienie polskiego podejścia do aspektu bezpieczeństwa informacyjnego, ze szczególnym uwzględnieniem miejsca wspomnianego zagadnienia w sferze bezpieczeństwa narodowego oraz możliwości jego charakterystyki. Głównym problem badawczym niniejszego opracowania jest następujące pytanie: W jaki sposób polskie podejście do bezpieczeństwa informacyjnego wpływa na skuteczność ochrony i obrony społeczeństwa przed zagrożeniami w infosferze? Na potrzeby prowadzenia dalszych rozważań we wskazanej tematyce sformułowano również następującą hipotezę badawczą: Autor publikacji sądzi, że zintegrowane podejście Polski do bezpieczeństwa informacyjnego, oparte na skoordynowanych działaniach rządu, a także sektora prywatnego oraz stosowania innowacyjnych rozwiązań, istotnie przyczynia się do zwiększenia odporności na zagrożenia w infosferze, poprawy świadomości bezpieczeństwa w społeczeństwie oraz skutecznej ochrony kluczowych interesów państwa.

2. Miejsce bezpieczeństwa informacyjnego w obszarze bezpieczeństwa narodowego

Dokonując rozważań na temat bezpieczeństwa informacyjnego, nie sposób nie odnieść się do miejsca, jakie wspomniane zagadnienie zajmuje w obszarze bezpieczeństwa narodowego. Jest to szczególnie ważny aspekt ze względu na rolę, jaką w obecnym świecie odgrywa informacja. Pojęcie to może być rozumiane na wiele sposobów, w zależności od kontekstu prowadzonych badań, jak również obszaru działalności człowieka. Z tego też względu informacja może być interpretowana jako[2]:

- Towar o charakterze strategicznym - wiedza jest cennym i strategicznym zasobem, nie tylko dla rządów i firm, ale także dla jednostek. W historii ci, którzy posiadali odpowiednie informacje we właściwym czasie, wygrywali bitwy i osiągali sukcesy w biznesie. Dziś wiedza jest traktowana jak inne towary, takie jak uran czy nowe technologie, które można kupić i które należy chronić.
- Część składowa procesów biznesowych - informacja jest niezbędnym elementem większości współczesnych operacji biznesowych, w tym działań dokonywanych przez organizacje rządowe. Jeśli przepływ informacji jest zakłócony lub manipulowany, może to doprowadzić do bankructwa firm i spowodować znaczne szkody dla państwa, takie jak niepokoje społeczne, zakłócenia w gospodarce narodowej i uszczerbek na jego reputacji w społeczności globalnej.
- Czynnik sterujący procesami produkcyjnymi i usługowymi - informacja odgrywa również istotną rolę w kontrolowaniu zautomatyzowanych procesów produkcyjnych i usługowych, które są krytyczne dla gospodarki i społeczeństwa. Procesy te mogą obejmować specjalistyczne narzędzia, takie jak czujniki i siłowniki, a niewłaściwe zarządzanie nimi może prowadzić do katastrof i kryzysów na poziomie lokalnym, krajowym lub międzynarodowym.
- Wartość chroniona przez prawo - aby zabezpieczyć prawa jednostek, cywilizowane kraje ustanowiły akty prawne, które chronią dane przed nieautoryzowanym dostę-

[2] K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania.* (wyd.) PWN, Warszawa 2017, wydanie II, s.15.

pem, zapewniają prawidłową obsługę, przechowywanie i przekazywanie informacji oraz ustanawiają wytyczne dotyczące gromadzenia określonych rodzajów danych.

Jak można zauważyć zakres stosowania informacji oraz jej charakterystyka jest rozbudowanym zagadnieniem. W związku z tym odpowiednie zapewnienie ochrony wspomnianej kwestii stanowi ważny element funkcjonowania państwa i jego obywateli.

Odnosząc się do obszaru bezpieczeństwa narodowego oraz rozszerzenia jego ram o kwestie związane z bezpieczeństwem informacyjnym, należy wskazać na proces zmian zachodzących w tym zakresie. Od początku funkcjonowania państw oraz społeczeństw dominowała koncepcja zakładająca prym bezpieczeństwa fizycznego nad omawianą tematyką[3]. W związku z tym początkowo stosowano podział oparty na dwóch rodzajach bezpieczeństwa: bezpieczeństwie militarnym i bezpieczeństwie cywilnym (pozamilitarnym). Pierwsza z kategorii odnosi się do aspektu reagowania oraz przeciwdziałania wszelkim zagrożeniom zewnętrznym, wymierzonym w pewność istnienia państwa. Z kolei część cywilna omawianego zagadnienia odnosi się również do oddziaływania, a także neutralizacji negatywnych sytuacji godzących w wewnętrzny aspekt funkcjonowania narodu[4]. Z czasem jednak zaczęto dostrzegać inne kategorie bezpieczeństwa, których charakterystyka oraz zakres zastosowania przyczyniały się do wsparcia dotychczasowych działań. W związku z tym możemy obecnie mówić o gospodarczych, społecznych, finansowych, ekologicznych, kulturowych oraz ideologicznych aspektach rozwoju i istnienia państwa[5]. Rozpatrywanie bezpieczeństwa informacyjnego jako części składowej bezpieczeństwa narodowego funkcjonuje od przełomu XX i XXI wieku. To właśnie za sprawą rozwoju cywilizacyjnego oraz technicznego coraz większą wartość zaczęto przypisywać informacji oraz jej wpływu na społeczeństwo[6]. Według Kazimierza Malaka bezpieczeństwo informacyjne jest jedną z kluczowych kwestii bezpieczeństwa narodowego. Wynika to z faktu, że wspomniane zagadnienie ma kluczowe znaczenie dla bezpieczeństwa, gdyż jest integralną częścią funkcjonowania różnych aspektów stosunków międzynarodowych, życia społecznego oraz kształtującego się społeczeństwa informacyjnego[7]. Co równie ważne, bezpieczeństwo narodowe jest zależne od swobodnego przepływu informacji oraz pracy systemów, które je przetwarzają.

3. Bezpieczeństwo informacyjne – zarys teoretyczny

Zwracając uwagę na kontekst istoty bezpieczeństwa informacyjnego należy odnieść się do sposobu jego definiowania. W związku z tym, tak ważne jest podjęcie tematyki związanej z koniecznością rozróżnienia pojęć, które niejednokrotnie traktowane są jako tożsame. Problematyka tego zagadnienia opiera się na zrównywaniu bezpieczeństwa informacyjnego z bezpieczeństwem informacji. Jest to swojego rodzaju uproszczenie, które może generować trudności z klasyfikacją elementów, będących częścią wspominanych pojęć. Z tego względu konieczne

[3] S. Koziej, *Polityka bezpieczeństwa państwa. Cz. I. Wprowadzenie. Podstawy teoretyczne oraz Polska jako podmiot bezpieczeństwa*. https://koziej.pl/wp-content/uploads/2022/05/PBP-Cz.I-Podstawy-polityki-bezpiecze%C5%84stwa.pdf (dostęp: 17.02.2023).

[4] Tenże, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucji*, [w:] „Bezpieczeństwo Narodowe". (wyd.) Biuro Bezpieczeństwa Narodowego, 2011, nr 18, s. 18-19.

[5] K. Grzebiela, *Pojęcie i istota bezpieczeństwa informacyjnego*, [w:] „Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje", 2018, nr 30, s. 92.

[6] S. Koziej, *Polityka bezpieczeństwa państwa (...)*, op. cit.

[7] K. Malak, *Typologia bezpieczeństwa. Nowe wyzwania*, [w:] C. Szyjko (red.), „Kształtowanie bezpieczeństwa europejskiego. Wybrane problemy instytucjonalno-prawne". (wyd.) Instytut Stosunków Międzynarodowych UJK, Warszawa 2008, s. 40

jest analizowanie założeń teoretycznych obu kwestii. W publikacji *Bezpieczeństwo informacyjne. Nowe wyzwania* Krzysztof Liderman określił definicje wspomnianych zagadnień, przedstawiając jednocześnie różnice zachodzące między nimi. Według autora, bezpieczeństwo informacyjne „dotyczy podmiotu (człowieka lub organizacji, również takiej jak państwo), który może być zagrożony utratą zasobów informacyjnych lub otrzymaniem informacji złej jakości. Bezpieczeństwo informacyjne oznacza zatem uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji". Z kolei bezpieczeństwo informacji rozumiane jest jako „uzasadnione (np. analizą ryzyka i przyjętymi metodami postępowania z ryzykiem) zaufanie, że nie zostaną poniesione straty wynikające z niepożądanej zmiany, na skutek realizacji zagrożenia, wymaganych wartości istotnych kryteriów jakości informacji"[8]. Biorąc pod uwagę powyższe rozważania należy przyjąć, że bezpieczeństwo informacji stanowi podkategorię bezpieczeństwa informacyjnego. Wynika to z faktu, że pierwszorzędnym działaniem w ramach pozyskiwania określonej wiedzy jest uzyskanie informacji wysokiej jakości. Kolejnym zaś krokiem jest zapewnienie odpowiednich warunków do dokonywania zmian, a także skutecznej ochrony zasobów informacyjnych. Oprócz bezpieczeństwa informacji w skład bezpieczeństwa informacyjnego należy również zaliczyć cyberbezpieczeństwo, którego zakres obejmuje „odporności systemów informacyjnych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na cyberzagrożenia, a także zwiększenie poziomu ochrony informacji w systemach informacyjnych przez standaryzację zabezpieczeń"[9].

Odnosząc się do sposobu definiowania bezpieczeństwa informacyjnego w literaturze przedmiotowej można odnaleźć liczne charakterystyki oraz sposoby pojmowania omawianego zagadnienia. Każda z przedstawionych poniżej definicji posiada opis różnych cech, odnoszących się do indywidualnego charakteru bezpieczeństwa informacyjnego.

Tabela 1. Zbiór definicji związanych z pojęciem bezpieczeństwa informacyjnego

Opis definicyjny	Uwagi do definicji
„Stan, gdy jeden podmiot (w tym wypadku państwo) może (i czyni to) gromadzić, posiadać, a w razie potrzeby wykorzystać różnego rodzaju dane (będące swoistego gatunku informacja) do osiągnięcia określonego przez niego celu". [P. Alkowski, 2015]	Niezbędna jest dostosowanie bezpieczeństwa informacyjnego do zagadnień związanych z bezpieczeństwem narodowym, a także zapewnieniem nadzoru nad możliwością oddziaływania innych organizacji w zakresie pozyskania informacji istotnych z punktu widzenia działalności państwa.
„Zachowanie dostępu do potrzebnych źródeł informacyjnych przy zapewnieniu ochrony tych osobistych informacji i źródeł, przy których to jest konieczne z perspektywy interesów subiektu (osoby, państwa, zakładu itp.)". [M. Bieniek, S. M. Mazur, 2012]	Zagadnienia bezpieczeństwa informacyjnego powinny być analizowane na wszystkich poziomach, ze względu na fakt, że większość zjawisk i procesów w dzisiejszym świecie opierają się na informacji. W niektórych przypadkach niedostrzeganie znaczenia bezpieczeństwa informacyjnego może mieć daleko idące konsekwencje, zarówno w sferze militarnej, społecznej lub gospodarczej.
„Pożądany poziom ochrony niezbędnych zasobów informacyjnych, technologii ich tworzenia i	Bezpieczeństwo informacyjne stanowi istotny element działań podejmowanych przez państwa i organizacje za-

[8] Tamże.
[9] Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, 2019, s. 6.

wykorzystywania a także praw podmiotów działalności informatycznej oraz zapewnienie im stabilnego funkcjonowania w każdych warunkach międzynarodowych oraz społecznych". [K. Malak, 2008]	równo w wymiarze międzynarodowym, jak i narodowym.
„Transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa; proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze". [Biuro Bezpieczeństwa Narodowego, 2015]	Realizacja wspomnianych założeń możliwa jest poprzez: – Odpowiednią ochronę zasobów informacyjnych oraz przeciwdziałanie aktywności dezinformacyjnej i propagandowej podjętej przez przeciwnika. – Utrzymanie zdolności do prowadzenia działań ofensywnych wobec potencjalnych przeciwników w terenie.
„Nowa dziedzina bezpieczeństwa narodowego, łącząca w sobie szereg cząstkowych ujęć, które odnieść należy do narzędzi i procedur ochrony danych, informacji i systemów informacyjnych" [J. Kaczmarek, W. Łepkowski, B. Zdrodowski (red.), 2008]	Koncepcja bezpieczeństwa informacyjnego jest oparta na rozumieniu komputerów zarówno jako magazynu informacji, jak i narzędzia kontroli, co zostało wyjaśnione w teorii wojny informacyjnej. Wdrożenie strategii bezpieczeństwa informacji polega na integracji różnych metod i narzędzi w celu zabezpieczenia zasobów informacyjnych użytkowników. Obejmuje to m.in.: zabezpieczenie komputerów osobistych przed wirusami, ochronę parametrów danych wykorzystywanych w zarządzaniu systemami, wdrożenie środków zapobiegających atakom hackerskim i cyberterrorystycznym oraz zapewnienie ochrony prawnej zasobów i systemów.

(Źródło: opracowanie własne na podstawie: Przemysław Alkowski, 2015; M. Bieniek, S. M. Mazur, 2012; Biuro Bezpieczeństwa Narodowego, 2015; J. Kaczmarek, W. Łepkowski, B. Zdrodowski (red.), 2008.)

Biorąc pod uwagę powyższe rozważania można przyjąć, że bezpieczeństwo informacyjne to szereg działań podejmowanych przez podmioty w celu zapewnienia odpowiednich narzędzi i środków, umożliwiających osiągnięcie właściwego poziomu ochrony zasobów informacyjnych poprzez pozyskiwania oraz gromadzenie informacji.

4. Działania Rzeczpospolitej Polskiej w zapewnieniu bezpieczeństwa informacyjnego

Odnosząc się do kwestii zapewnienia bezpieczeństwa informacyjnego przez Rzeczypospolitą Polską, należy skupić się na kilku ważnych zagadnieniach, umożliwiających zgłębienie tej tematyki. W tym zakresie szczególnie ważnym aspektem są dokumenty, regulujące aspekt przedmiotu rozważań. Jednym z istotnych źródeł odnoszących się do pewnego wycinka bezpieczeństwa informacyjnego jest *Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej* z 2020 roku. W treści koncepcji można odnaleźć odniesienie do kwestii związanej z cyberbezpieczeństwem oraz sferą informacyjną. W przypadku pierwszego zagadnienia, strategia przewiduje działania zmierzające do zwiększenia odporności na zagrożenia cybernetyczne oraz poprawy bezpieczeństwa informacji w sektorze publicznym, wojskowym i prywatnym. Ważnym punktem rozważań jest również możliwość rozpowszechniania wiedzy i najlepszych praktyk, w celu wsparcia obywateli w procesie lepszej ochrony posiadanych

przez nich informacji. Wspomniane cele możliwe będą do osiągnięcia dzięki działaniom opartym na[10]:

- Poprawie odporności systemów informatycznych, wykorzystywanych w środowisku wojskowym i cywilnym, w celu skutecznego zapobiegania i reagowania na zagrożenia cybernetyczne.
- Wzmocnieniu zdolności obronnych narodu poprzez ciągłe doskonalenie systemu cyberbezpieczeństwa, w celu wspierania jego rozwoju.
- Rozwinięciu zdolności do prowadzenia wszystkich wojskowych operacji cybernetycznych.
- Stworzeniu krajowej zdolności do oceny, badania, testowania i certyfikowania usług oraz rozwiązań w zakresie bezpieczeństwa cybernetycznego.
- Edukacji urzędników państwowych i społeczności, w celu zwiększenia ich wiedzy i świadomości na temat zagrożeń i wyzwań cybernetycznych.
- Wzmocnieniu i rozszerzeniu krajowych zdolności, w tym poprzez finansowanie ze środków publicznych badań i rozwoju zaawansowanych technologii, we współpracy z uniwersytetami, instytucjami badawczymi oraz przedsiębiorstwami publicznymi i prywatnymi.

W kwestiach związanych z przestrzenią informacyjną koncepcja strategiczna odnosi się przede wszystkim do konieczności gwarancji stateczności istnienia państwa i obywateli w sferze informacyjnej. Z tego względu zostaną podjęte niezbędne działania z zakresu[11]:

- Ustanowienia strategicznych warstw aktywności zarówno w warstwie wirtualnej, fizycznej oraz poznawczej. Umożliwi to ochronę architektury informacji i zmniejszenia wpływu dezinformacji.
- Określenia kompleksowych ram dla komunikacji rządowej, które obejmują przewidywanie, planowanie i realizację skoordynowanych działań komunikacyjnych przy użyciu różnych kanałów i narzędzi. Podjęcie takich działań umożliwia identyfikację i oddziaływanie na obszary bezpieczeństwa narodowego.
- Aktywnego zwalczania dezinformacji poprzez budowanie potencjału i opracowywanie procedur angażowania obywateli, społeczeństwa obywatelskiego oraz organizacji pozarządowych w mediach i sieciach społecznościowych.
- Promowania świadomości zagrożeń związanych z manipulacją informacjami poprzez edukację w zakresie bezpieczeństwa cybernetycznego w celu zmniejszenia podatności społeczeństwa na dezinformację.

Co równie ważne, w 2019 roku Rada Ministrów przyjęła *Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*. Koncepcja szczegółowo określa cele strategiczne, politykę i regulacje niezbędne do zwiększenia odporności operatorów infrastruktury krytycznej, dostawców usług cyfrowych i administracji publicznej na zagrożenia cybernetyczne, czego ostatecznym celem jest poprawa bezpieczeństwa narodowego. Strategia ma na celu zwiększenie odporności cybernetycznej i ochrony informacji w całym sektorze publicznym, wojskowym i prywatnym, przy jednoczesnym promowaniu wiedzy i najlepszych praktyk wśród obywateli. W dokumencie określono pięć celów szczegółowych, w tym rozwój krajowego systemu cyberbezpieczeństwa, zwiększenie odporności systemów informatycz-

[10] Biuro Bezpieczeństwa Narodowego, *Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej*, 2020, s. 20.
[11] Tamże, s. 21.

nych, rozbudowę krajowego potencjału w zakresie technologii cyberbezpieczeństwa, rozwój świadomości i kompetencji społeczeństwa w zakresie cyberbezpieczeństwa oraz budowę silnej pozycji międzynarodowej w dziedzinie cyberbezpieczeństwa. Cele Strategii będą osiągane poprzez różnorodne działania, w tym opracowanie Krajowych Standardów Cyberbezpieczeństwa, kontynuację inicjatyw badawczo-rozwojowych oraz realizację programów szkoleniowych i działań w zakresie współpracy międzynarodowej[12].

Wśród aktów prawnych regulujących kwestie bezpieczeństwa informacyjnego należy wskazać przykłady dokumentów, odnoszących się do tego zagadnienia. W tym zakresie ważnym aktem prawnym jest *Ustawa z dnia* 5 sierpnia *2010 r. o ochronie informacji niejawnych*. Zawarte w dokumencie przepisy mające na celu zabezpieczenie informacji, których ujawnienie bez upoważnienia mogłoby zaszkodzić Rzeczypospolitej Polskiej lub godzić w jej interesy, niezależnie od formy lub sposobu przetwarzania tych informacji. Szczególny zakres regulacji prawnych odnosi się do m.in.: procesu klasyfikowania informacji jako niejawnych, środków ich ochrony, procesu zarządzania nimi, a także organizacji kontroli w celu oceny poziomu ochrony[13]. Kolejnym ważnym dokumentem odnoszącym się do omawianej kwestii jest *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.* We wspomnianym akcie prawnym uszczegółowiono aspekty związane z ochroną danych osobowych osób fizycznych, zgodnie z zapisami *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*. Przepisy wspomnianej ustawy regulują kwestie związane m.in. z: wymaganiami i trybem powoływania inspektora ochrony danych przez podmioty publiczne, procesem akredytacji organów uprawnionych do certyfikowania ochrony i monitorowania danych osobowych, nadzorem nad przestrzeganiem przepisów o ochronie danych osobowych, a także odpowiedzialnością karną i karami administracyjnymi za naruszenie przepisów dotyczących ochrony danych osobowych[14].W kontekście aktów prawnych, odnoszących się do bezpieczeństwa informacyjnego, należy wspomnieć również o rozdziale XXXIII *Ustawy z dnia 6 czerwca 1997 r. Kodeks karny*, dotyczącym przestępstw przeciwko ochronie informacji. We wspomnianym dokumencie znajdują się zapisy odnoszące się do sposobu penalizacji wspomnianych nielegalnych działań wraz z uwzględnieniem ich typologii. Wśród wyszczególnionych w akcie prawnym przestępstw należy wyodrębnić m.in.: ujawnianie lub wykorzystanie informacji niejawnych, bezprawne uzyskanie informacji, utrudnianie zapoznania się z informacją czy też zakłócanie działania systemu komputerowego[15].

Ważną ustawą, odnoszącą się do omawianego zagadnienia, jest *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.* Akt prawny jest odpowiedzią polskich władz na *Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*. Ministerstwo Cyfryzacji stworzyło ustawę, mając na celu ustanowienie przepisów prawnych, które ułatwiłyby wdrożenie dyrektywy NIS i stwo-

[12] Ministerstwo Cyfryzacji, *Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, s. 2, 9, 12, 18, 22, 25, 27.
[13] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz. U. 2010 Nr 182 poz. 1228), art. 1, s. 1.
[14] *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz. U. 2018 poz. 1000), art. 1, s. 1-2.
[15] Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (Dz.U. z 1997 r. nr 88, poz. 553), art. 265-269c, s. 129-132.

rzenie skutecznego systemu zabezpieczenia teleinformatycznego na poziomie krajowym[16]. Dokument odnosi się do kwestii związanych z ustanowieniem oraz określeniem ról i obowiązków podmiotów zaangażowanych w krajowy system cyberbezpieczeństwa. Ważnym punktem poruszanym w akcie prawnym jest przedstawienie procedur nadzorowania i egzekwowania przestrzegania przepisów ustawy, a także określenia celów i zakresu Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej. Krajowy system cyberbezpieczeństwa składa się z różnych podmiotów, które współpracują ze sobą, aby umożliwić podjęcie szeregu skutecznych działań w odpowiedzi na zagrożenia, zapewniając możliwość skutecznego przeciwdziałania i reagowania na takie sytuacje. Wśród wyszczególnionych w ustawie jednostek należy zwrócić szczególną uwagę na Zespoły Reagowania na Incydenty Komputerowe (CSIRT)[17]. W Polsce funkcjonują trzy takie podmioty:

- CSIRT GOV - Zespołów Reagowania na Incydenty Komputerowe odpowiedzialny za koordynację procesu reagowania na incydenty komputerowe na szczeblu krajowym. Działaniami Zespołu kieruje Szef Agencji Bezpieczeństwa Wewnętrznego. Jednym z głównych zadań instytucji jest wykrywanie, zapobieganie i identyfikacja zagrożeń bezpieczeństwa, które mogą mieć wpływ na prawidłowość istnienia państwa, a także systemów teleinformatycznych, organów administracji publicznej, systemu sieci teleinformatycznej objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej[18].
- CSIRT MON - Zespołów Reagowania na Incydenty Komputerowe szczebla krajowego, działający w ramach Dowództwa Komponentu Wojsk Obrony Cybernetycznej pod kierownictwem Ministra Obrony Narodowej. Zespół odpowiada za koordynację oraz reagowanie na incydenty dla podmiotów podległych lub nadzorowanych przez Ministra Obrony Narodowej, a także dla przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym. Instytucja we współpracy z innymi zespołami realizuje szereg zadań, takich jak: monitorowanie zagrożeń i incydentów cyberbezpieczeństwa na poziomie krajowym, prowadzenie analizy ryzyka, przekazywanie informacji o incydentach i zagrożeniach podmiotom w ramach krajowego systemu cyberbezpieczeństwa, wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa, reagowanie na zgłoszone incydenty, klasyfikowanie incydentów (w tym incydentów poważnych, istotnych i krytycznych) oraz koordynowanie obsługi incydentów krytycznych[19].
- CSIRT NASK - Państwowy Instytut Badawczy znajdujący się pod nadzorem Kancelarii Prezesa Rady Ministrów. Jego głównym zadaniem jest zagwarantowanie bezpieczeństwa w Internecie, w tym reagowanie na incydenty zagrażające bezpieczeństwu polskiej sieci. Ponadto Zespół prowadzi działalność w zakresie badawczo-rozwojowym, koncentrując się na poprawie wydajności i bezpieczeństwa różnych sieci teleinformatycznych oraz systemów sieciowych[20].

[16] Ministerstwo Cyfryzacji, *Krajowy system cyberbezpieczeństwa*. https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa - (dostęp: 20.02.2023).
[17] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz. U. 2018 poz. 1560), art. 2, s. 2.
[18] CSIRT GOV, *O nas*. https://csirt.gov.pl/ (dostęp: 20.02.2023).
[19] CSIRT MON, *O nas. Zadania*. https://csirt-mon.wp.mil.pl/pl/pages/zadania-2017-01-16-4/ (dostęp: 20.02.2023).
[20] CSIRT NASK, *Kim jesteśmy*. https://www.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html (dostęp: 20.02.2023).

Kolejnym ważnym działaniem podjętym przez władze Rzeczypospolitej Polskiej, w zakresie bezpieczeństwa informacyjnego, jest stworzenie Narodowych Standardów Cyberbezpieczeństwa (NSC). Wspomniane zasady stanowią zbiór zaleceń dotyczących standaryzacji rozwiązań w zakresie bezpieczeństwa sieci i systemów informatycznych, które mogą być wykorzystane do efektywnego zarządzania systemami bezpieczeństwa informacji. Standardy te powstały na bazie założeń amerykańskiego Narodowego Instytutu Nauki i Technologii (NIST) i zostały dostosowane do polskiego systemu prawnego. Przepisy przeznaczone są dla podmiotów w krajowym systemie cyberbezpieczeństwa, w tym realizujących zadania publiczne, operatorów usług kluczowych oraz dostawców usług cyfrowych. NSC jako przewodnik metodyczny, oparty na praktykach amerykańskiej administracji federalnej, służy do budowy efektywnego systemu zarządzania bezpieczeństwem informacji[21].

Istotną kwestią, odnoszącą się do zapewnienia bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej, jest powołanie Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP. Wspomniane działanie zostało podjęte w oparciu o *Rozporządzenie Rady Ministrów z dnia 11 sierpnia 2022 r. w sprawie ustanowienia Pełnomocnika Rządu do spraw Bezpieczeństwa Przestrzeni Informacyjnej Rzeczypospolitej Polskiej*. W dokumencie wyszczególniono główne zadania Pełnomocnika, do których należy m.in.: organizacja działań agencji rządowych odpowiedzialnych za ujawnianie, badanie i przeciwdziałanie zagrożeniom informacyjnym dla interesów Polski. Obejmuje to identyfikację i neutralizację zagrożeń dla bezpieczeństwa informacyjnego kraju oraz reagowanie na nie. Kolejnym ważnym obowiązkiem Pełnomocnika jest prezentowanie rekomendacji dla Rady Ministrów w zakresie systemowych rozwiązań, mających na celu zwiększenie możliwości Polski do zwalczania zagrożeń informacyjnych[22].

Biorąc pod uwagę powyższe rozważania należy wskazać na szeroki zakres działań podejmowanych przez administrację rządową Rzeczypospolitej Polskiej w zakresie zapewnienia odpowiedniego bezpieczeństwa informacyjnego państwa i obywateli. W tym kontekście kluczową kwestią okazuje się opracowanie koncepcji strategicznych oraz aktów prawnych, regulujących główne cele umożliwiające zagwarantowanie omawianego zagadnienia, jak również zadania i rolę podmiotów wyspecjalizowanych do realizacji zaplanowanych inicjatyw. Istotne okazały się również Narodowe Standardy Cyberbezpieczeństwa, których zakres obejmuje wszelkie zasady wykorzystywane w ramach działalności administracji publicznej oraz podmiotów odpowiedzianych za aspekt bezpieczeństwa informacyjnego. Kolejnym ważnym aspektem było stworzenie Zespołów Reagowania na Incydenty Komputerowe, których funkcjonowanie zapewnia obsługę incydentów oraz odpowiednie reagowanie na zagrożenia cybernetyczne. Powołanie Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP umożliwia prowadzenie czynności kontrolnych, związanych z zapewnieniem bezpieczeństwa informacyjnego przez wspominane w powyższych rozważaniach podmioty.

5. Wnioski

Bezpieczeństwo informacyjne stanowi istotny element funkcjonowania państwa i jego obywateli. W obecnie funkcjonującej erze społeczności informacyjnej, możliwość dokony-

[21] Gov.pl, *Narodowe Standardy Cyberbezpieczeństwa*. https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber (dostęp: 20.02.2023).
[22] *Rozporządzenie Rady Ministrów z dnia 11 sierpnia 2022 r. w sprawie ustanowienia Pełnomocnika Rządu do spraw Bezpieczeństwa Przestrzeni Informacyjnej Rzeczypospolitej Polskie* (Poz. 1714), §2, s. 1.

wania działań związanych z pozyskiwaniem, przetwarzaniem i gromadzeniem informacji stanowi kluczowy punkt działalności człowieka. Sposób pojmowania informacji w kategoriach towaru o znaczeniu strategicznym, wartości chronionej prawnie, a także dobra umożliwiającego pozyskanie wiedzy o środowisku funkcjonowania danego podmiotu, stanowi potwierdzenie konieczności podjęcia działań z zakresu ochrony, z perspektywy zapewnienia jej odpowiedniej jakości i dostępności. W związku z przewagą potencjału informacyjnego nad potencjałem fizycznym, konieczne okazało się ujęcie bezpieczeństwa informacyjnego w strukturach bezpieczeństwa narodowego. Szanse związane z pozyskaniem dobrej jakościowo, rzetelnej informacji w szybkim czasie ułatwia państwom podejmowanie strategicznych decyzji zarówno w wymiarze wewnątrzkrajowym, jak również na arenie międzynarodowej.

Kluczowym aspektem, dotyczącym omawianego zagadnienia, jest uściślenie jego zakresu definicyjnego. Szczególnie ważne jest rozróżnienie bezpieczeństwa informacyjnego od bezpieczeństwa informacji. Pomimo zbieżności w brzmieniu oraz odniesienia do informacji, oba pojęcia determinują zupełnie inny aspekt tejże kwestii. Tematyka poruszana w niniejszym artykule odnosi się do procesu pozyskiwania oraz gromadzenia informacji, która musi spełniać określone wcześniej założenia. Z tego względu bezpieczeństwo informacyjne stanowią wszelkie działania, techniki oraz sposoby ułatwiające ochronę zasobów informacyjnych w trakcie trwania wspomnianych czynności, w celu zapewnienia jej jakości. W przypadku bezpieczeństwa informacji możemy mówić o dalszych działaniach, podejmowanych w celu ochrony informacji przed zagrożeniami związanymi z dokonywaniem na niej modyfikacji.

Ze względu na istotę bezpieczeństwa informacyjnego, w odniesieniu do zapewnienia istnienia oraz stabilnego rozwoju państwa, Rzeczpospolita Polska podejmuje szereg działań umożliwiających realizację zaplanowanych aktywności, związanych ze wspomnianym zagadnieniem. W tym zakresie należy wspomnieć o licznych aktach prawnych i koncepcjach strategicznych, w których bezpieczeństwo informacyjne, ale również funkcjonujące w jego ramach bezpieczeństwo informacji i cyberbezpieczeństwo mają swoje odzwierciedlenie. Co równie ważne określenie zasad oraz roli poszczególnych podmiotów, w ramach krajowego systemu cyberbezpieczeństwa, stanowi dopełnienie podejmowanych w tym zakresie starań.

Bibliografia

[1] Alkowski P., *Bezpieczeństwo informacyjne – zarys wybranych aspektów w kontekście problemu bezpieczeństwa państwa,* [w:] Guzik-Makaruk E. M., Pływaczewski E. W. (red.), „Współczesne oblicza bezpieczeństwa". (wyd.) Temida 2, Białystok 2015.

[2] Bieniek M., Mazur S .M. (red.), *Wstęp do studiów bezpieczeństwa*. (wyd.) Ladislav Hofreiter & Krakowska Akademia im. Andrzeja Frycza Modrzejewskiego, Kraków 2012.

[3] Biuro Bezpieczeństwa Narodowego, *Doktryna bezpieczeństwa informacyjnego RP. Projekt,* 2015.

[4] Biuro Bezpieczeństwa Narodowego, *Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej*, 2020.

[5] Golka M., *Czym jest społeczeństwo informacyjne?*, [w:] „Ruch prawniczy, ekonomiczny i socjologiczny". (wyd.) , 2005, zeszyt 5.

[6] Grzebiela K., *Pojęcie i istota bezpieczeństwa informacyjnego*, [w:] „Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje", 2018, nr 30.

[7] Kaczmarek J., Łepkowski W., Zdrodowski B. (red.), *Słowniku terminów z zakresu bezpieczeństwa narodowego*. (wyd.) Akademia Oborny Narodowej, wydanie szóste, Warszawa 2008.

[8] Koziej S, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucji*, [w:] „Bezpieczeństwo Narodowe". (wyd.) Biuro Bezpieczeństwa Narodowego, 2011, nr 18.
[9] Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*. (wyd.) PWN, Warszawa 2017, wydanie II.
[10] Malak K., *Typologia bezpieczeństwa. Nowe wyzwania*, [w:] C. Szyjko (red.), „Kształtowanie bezpieczeństwa europejskiego. Wybrane problemy instytucjonalno-prawne". (wyd.) Instytut Stosunków Międzynarodowych UJK, Warszawa 2008.
[11] Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, 2019.
[12] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz. U. 2010 Nr 182 poz. 1228).
[13] *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz. U. 2018 poz. 1000).
[14] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz. U. 2018 poz. 1560).
[15] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny* (Dz.U. z 1997 r. nr 88, poz. 553).

Netografia

[1] CSIRT GOV, *O nas*. https://csirt.gov.pl/ (dostęp: 20.02.2023).

[2] CSIRT MON, *O nas*. Zadania. https://csirt-mon.wp.mil.pl/pl/pages/zadania-2017-01-16-4/ (dostęp: 20.02.2023).

[3] CSIRT NASK, *Kim jesteśmy?* https://www.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html (dostęp: 20.02.2023).

[4] Gov.pl, *Narodowe Standardy Cyberbezpieczeństwa*. https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber (dostęp: 20.02.2023).

[5] Koziej S., *Polityka bezpieczeństwa państwa. Cz. I. Wprowadzenie. Podstawy teoretyczne oraz Polska jako podmiot bezpieczeństwa*. https://koziej.pl/wp-content/uploads/2022/05/PBP-Cz.I-Podstawy-polityki-bezpiecze%C5%84stwa.pdf (dostęp: 17.02.2023).

[6] Ministerstwo Cyfryzacji, *Krajowy system cyberbezpieczeństwa*. https://www.gov.pl/web/ cyfryzacja /krajowy -system-cyberbezpieczenstwa- (dostęp: 20.02.2023).