STRATEGIA BEZPIECZEŃSTWA INFORMACYJNEGO

RZECZYPOSPOLITEJ POLSKIEJ

PROJEKT AKADEMICKI

STRATEGIA BEZPIECZEŃSTWA INFORMACYJNEGO RZECZYPOSPOLITEJ POLSKIEJ

PROJEKT AKADEMICKI

STRATEGIA BEZPIECZEŃSTWA INFORMACYJNEGO RZECZYPOSPOLITEJ POLSKIEJ

PROJEKT AKADEMICKI

Włodzimierz Fehler
Stanisław Topolewski
Robert Wawer
Piotr Bączek

OŚRODEK BADAŃ BEZPIECZEŃSTWA INFORMACYJNEGO
2026

WYDAWNICTWO NAUKOWE
COLLEGIUM BOBOLANUM

Tytuł: Strategia Bezpieczeństwa Informacyjnego Rzeczypospolitej Polskiej. Projekt akademicki

Skład autorski:

prof. dr hab. Włodzimierz Fehler
Ośrodek Badań Bezpieczeństwa Informacyjnego UwS
AKW Collegium Bobolanum, Warszawa
ORCID: 0000-0002-0927-4337

dr hab. prof. ucz. Stanisław Topolewski
Ośrodek Badań Bezpieczeństwa Informacyjnego UwS
ORCID: 0000-0001-8268-3754

dr inż. Robert Wawer
Ośrodek Badań Bezpieczeństwa Informacyjnego UwS
AKW Collegium Bobolanum, Warszawa
ORCID: 0000-0002-3001-5268

dr Piotr Bączek
Ośrodek Badań Bezpieczeństwa Informacyjnego UwS
Wyższa Szkoła Kształcenia Zawodowego we Wrocławiu
ORCID: 0000-0002-5432-1657

ISBN 978-83-970591-8-4 (wersja drukowana)
ISBN 978-83-970591-9-1 (wersja cyfrowa)

Spis treści

Wprowadzenie

Przygotowanie akademickiego projektu Strategii Bezpieczeństwa Informacyjnego Rzeczypospolitej Polskiej (dalej w dokumencie nazywanego Strategią) wynika z imperatywu utrzymywania i rozwijania zdolności do skutecznego zapewniania bezpieczeństwa w warunkach dynamicznych przeobrażeń infosfery, w tym postępującej cyfryzacji, rozwoju sztucznej inteligencji oraz rosnącej skali oddziaływań informacyjnych o charakterze wrogim, nieprzyjaznym, konkurencyjnym lub zaśmiecającym. Strategia przedstawia kompleksowe założenia dotyczące kształtowania bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej w wymiarze wewnętrznym, zewnętrznym i systemowym. Przyjmuje perspektywę zgodną z Konstytucją RP i standardami międzynarodowymi, a także uwzględnia interesy narodowe oraz cele strategiczne w dziedzinie bezpieczeństwa. Działania państwa na rzecz bezpieczeństwa informacyjnego muszą być: legalne, proporcjonalne, poddawane kontroli i rozliczane. W odróżnieniu od podejść redukujących bezpieczeństwo informacyjne do cyberbezpieczeństwa Strategia ujmuje infosferę jako środowisko obejmujące także: media tradycyjne, platformy społecznościowe, komunikację inter-

personalną, sferę edukacji, kulturę, procesy polityczno-społeczne, infrastrukturę informacyjną oraz zasoby informacyjne.

Jeden z najważniejszych wyróżniających składników współczesności stanowi skokowy wzrost znaczenia informacji. Jest to rezultat rewolucji informacyjnej, która doprowadziła do powstania społeczeństwa informacyjnego przeobrażającego się obecnie w szybkim tempie w społeczeństwo hiperpołączone z coraz większym wpływem sztucznej inteligencji. W konsekwencji wysokiego pozycjonowania roli informacji w różnych sferach życia zbiorowego i indywidualnego, także w dziedzinie bezpieczeństwa uwzględnia się jego transsektorowy i wieloaspektowy wymiar informacyjny. Strategia opiera się na aksjomacie, że infosfera stanowi współcześnie pole rywalizacji, w której zagrożenia informacyjne plasują się jako silnie destrukcyjne. Polska nie może wobec takiego rozwoju sytuacji pozostać bierna. Znaczenie oraz charakter środków i instrumentów używanych w działalności na rzecz bezpieczeństwa informacyjnego spowodowały, że w ramach polityki bezpieczeństwa państwa niezbędne stało się wyodrębnienie polityki bezpieczeństwa informacyjnego. Jednym z podstawowych elementów koniecznych do jej właściwej konceptualizacji oraz realizacji jest precyzyjne określenie terminologii, w tym sposobu pojmowania „bezpieczeństwa informacyjnego" oraz terminów z nim związanych. Ważnym składnikiem polityki bezpieczeństwa informacyjnego w demokratycznym państwie prawnym jest także zapewnienie bezpieczeństwa informacyjnego na poziomie jednostki.

Procesy globalizacji oraz innowacyjne technologie teleinformatyczne głęboko przeobraziły i ciągle zmieniają środowisko bez-

pieczeństwa informacyjnego różnych podmiotów – od jednostek i grup społecznych począwszy, na państwach i systemie międzynarodowym skończywszy. Jednak mimo systematycznego wzrostu znaczenia bezpieczeństwa informacyjnego nie zawsze uwzględnia się odpowiednie lokowanie tego wymiaru bezpieczeństwa w hierarchii interesów narodowych. Stosowne do wagi oraz wielowątkowości problematyki bezpieczeństwa informacyjnego jego ujmowanie w planowaniu strategicznym jest dla państwa polskiego zadaniem priorytetowym. Podejście do bezpieczeństwa informacyjnego prezentowane w polskich dokumentach strategicznych cechują sektorowość i brak holistycznego ujęcia oraz koncentrowanie się na bardzo ważnym, ale nie jedynym elemencie infosfery, jakim jest cyberprzestrzeń. Zniekształca to rzeczywistość oraz obniża jakość przygotowywanych strategii. To z kolei otwiera drogę do kreowania nieadekwatnych do potrzeb państwa, nieoptymalnych (a czasami wręcz szkodliwych) rozwiązań praktycznych. Z tych względów jednym z zasadniczych zadań dla twórców dokumentów strategicznych z zakresu bezpieczeństwa informacyjnego jest zapewnienie odpowiedniego przedstawiania jego istoty i uwarunkowań przy wykorzystaniu poprawnie ukształtowanego aparatu pojęciowego. Wypełnienie tak zidentyfikowanej luki to zadanie, które postawił przed sobą zespół autorów, przygotowujących akademicki projekt Strategii Bezpieczeństwa Informacyjnego Rzeczypospolitej Polskiej. Zadanie to zostało zrealizowane poprzez przedstawienie w aktualnym i merytorycznie poprawnym, zdaniem autorów, kształcie kwestii:

– celów strategicznych RP w sferze bezpieczeństwa informacyjnego;

– uwarunkowań bezpieczeństwa informacyjnego RP;
– założeń polityki bezpieczeństwa informacyjnego RP;
– konstrukcji i celów działania systemu bezpieczeństwa informacyjnego RP.

Należy podkreślić, że w sytuacji systematycznie poszerzającego się zakresu powiązań bezpieczeństwa informacyjnego z innymi wymiarami bezpieczeństwa dla zachowania przejrzystości struktury i zwartości treści Strategii skoncentrowano się na kwestiach zasadniczych, wyznaczających ogólne ramy obszaru bezpieczeństwa informacyjnego państwa polskiego. Projekt Strategii Bezpieczeństwa Informacyjnego RP jest efektem wysiłku badawczego zespołu naukowców reprezentujących różne podmioty akademickie, działającego w ramach Ośrodka Badań Bezpieczeństwa Informacyjnego i ma charakter autorskiej propozycji stanowiącej prolegomenę do dalszych prac badawczych nad przygotowaniem oficjalnej wersji Strategii Bezpieczeństwa Informacyjnego RP. W założeniu zarówno projekt Strategii, jak i efekty oczekiwanych w związku z jej upublicznieniem dyskusji mają służyć wszystkim, którzy na poziomie państwowym są zobligowani do troski o bezpieczeństwo informacyjne RP. Ze względu na akademicki charakter projektu jest on ważny także dla badaczy zajmujących się problematyką informacyjnego wymiaru bezpieczeństwa państwa.

Przyjmując stanowisko, że bezpieczeństwo informacyjne to stan, i ciąg stanów oraz procesy, w ramach których zapewniana jest wysoka jakość informacji, jej skuteczna ochrona przed zagrożeniami oraz swoboda wytwarzania, dostępu, gromadzenia i przepływu tej informacji połączona z wyodrębnieniem pewnych

ich kategorii, podlegających szczególnej ochronie bądź reglamentacji, trzeba pamiętać, że towarzyszy temu szereg wydarzeń i zjawisk tworzących szerokie spektrum szans, wyzwań i zagrożeń. Taki stan rzeczy wymaga ciągłego doskonalenia działań państwa w sferze bezpieczeństwa informacyjnego. Powinny być one skoncentrowane na rozpoznawaniu sytuacji w sferze bezpieczeństwa informacyjnego, prognozowaniu zmian oraz sprawowaniu nad nią kontroli w taki sposób, aby wykorzystywać szanse, ograniczać występowanie zagrożeń i łagodzić ich skutki oraz sprawnie i efektywnie podejmować wyzwania. Należy zauważyć, że takie wysiłki są podejmowane i obejmują szeroki wachlarz zagadnień. Jednak uwzględniając prognozy i współczesne realia, w tym charakter toczących się wojen oraz stosowanie na szeroką skalę dezinformacji, za konieczne dla kształtowania pożądanego poziomu bezpieczeństwa informacyjnego RP należy uznać: systematyczne monitorowanie i kształtowanie jego uwarunkowań w celu dostosowywania do nich podejmowanych działań o charakterze strategicznym oraz zdecydowane wzmocnienie systemowych rozwiązań w zakresie zarządzania tym aspektem bezpieczeństwa jako jednym z kluczowych składników bezpieczeństwa RP.

1. Ustalenia ogólne

Prowadzona przez RP polityka bezpieczeństwa informacyjnego ukierunkowana na wzmacnianie potencjału informacyjnego, zapewnienie dostępu do wysokiej jakości informacji oraz modernizację i ochronę narodowej infosfery stanowi wkład w osiąganie założonego poziomu bezpieczeństwa państwa. Fundamentalne wartości i zasady bezpieczeństwa informacyjnego RP określa Konstytucja RP. Zasady te znajdują potwierdzenie w konwencjach i układach międzynarodowych ratyfikowanych przez Polskę. Jest to istotne bowiem harmonijne połączenie działań państwa polskiego z jego sojuszniczymi i międzynarodowymi partnerami oraz aktywnością społeczeństwa zapewni kształtowanie i utrzymywanie bezpiecznego stanu narodowej infosfery. Wymaga to podejmowania spójnych działań wewnątrzpaństwowych i zewnętrznych na rzecz realizacji strategicznych priorytetów bezpieczeństwa informacyjnego RP, zorientowanych na neutralizację zagrożeń zewnętrznych i wewnętrznych oraz tworzenie warunków do osiągania narodowych celów z zakresu bezpieczeństwa informacyjnego. Nadrzędnym celem Strategii jest komplementarne powiązanie bezpieczeństwa informacyjnego z całościowo postrzeganą polityką bezpieczeństwa RP. W związ-

ku z tym zastosowano koncepcję holistycznego podejścia do infosfery z uwzględnieniem roli obywateli, przedsiębiorstw, instytucji publicznych oraz partnerów międzynarodowych i sojuszników w budowaniu odporności na zagrożenia informacyjne. Uwzględniając powyższe ustalenia:

A. Strategia jest dokumentem planowania strategicznego, określającym interesy państwowe, strategiczne priorytety, cele oraz główne kierunki działań w zakresie bezpieczeństwa informacyjnego w perspektywie długoterminowej.
B. Strategia opiera się na założeniu współzależności bezpieczeństwa informacyjnego z innymi wymiarami bezpieczeństwa RP.
C. Strategia uwzględnia znaczenie uwarunkowań międzynarodowych w tym zobowiązań wynikających z członkostwa w UE i NATO.

Realizacja Strategii opiera się na zasadach: legalizmu i praworządności, proporcjonalności, ochrony praw i wolności, minimalizacji szkód, odporności, współodpowiedzialności, i rozliczalności.

W Strategii używane są następujące podstawowe pojęcia:

1) **bezpieczeństwo informacyjne RP** – (dalej bezpieczeństwo informacyjne) to sta,n i ciąg stanów oraz procesów, w ramach których zapewniana jest wysoka jakość informacji, jej skuteczna ochrona przed zagrożeniami oraz swoboda wytwarzania, gromadzenia, przetwarzania i przepływu, a także dostępu do niej. Bezpieczeństwo informacyjne obejmuje stosowanie szczególnych reżimów ochronnych i reglamentacyjnych dla niektórych katego-

rii informacji, wyodrębnionych ze względu na zapewnienie bezpieczeństwa podmiotów, których one dotyczą.

2) **bezpieczeństwo informacji** – stan, i ciąg stanów oraz procesów, w ramach których na drodze działań politycznych, prawnych i organizacyjno-technicznych zapewnia się w całym cyklu życia informacji osiąganie i utrzymywanie, z uwzględnieniem zaprogramowanych standardów jakościowych i ilościowych, na pożądanym poziomie takich fundamentalnych właściwości informacji, jak: dostępność, użyteczność, integralność, autentyczność, niezaprzeczalność, rozliczalność oraz tam, gdzie to potrzebne, także poufność czy tajność.

3) **cyberbezpieczeństwo RP** – (dalej cyberbezpieczeństwo) stan, i ciąg stanów oraz procesów, w ramach których zapewnia się i utrzymuje na pożądanym przez państwo poziomie sprawność cyfrowych systemów informacyjnych w zakresie dostarczania, gromadzenia i przetwarzania wysokiej jakości danych i informacji, a także ich odporność na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych oraz informacji lub związanych z nimi usług oferowanych przez te systemy.

4) **cyberprzestrzeń** – będące częścią infosfery środowisko komunikacji, przetwarzania i wymiany informacji oraz danych za pomocą połączonych sieci i systemów komputerowych, pozwalające użytkownikom posiadającym dostęp do jej zasobów na komunikację i nawiązywanie relacji drogą elektroniczną w czasie rzeczywistym.

5) **infosfera** – traktowane całościowo wieloskładnikowe środowisko informacyjne, w którym funkcjonują podmioty indywi-

dualne i zbiorowe (w tym państwa), obejmujące wszystkie zasoby informacji produkowanej przez ludzkość, tworzone i przechowywane na wszelkich nośnikach informacji, przetwarzane i wykorzystywane przez użytkowników za pomocą technologii cyfrowych i analogowych w trybie on-line i off-line, a także informacje przekazywane w bezpośrednich i pośrednich kontaktach interpersonalnych, wpływające na człowieka oraz kształtujące jego postawy, wiedzę i umiejętności komunikacyjne.

6) **komunikacja strategiczna** – planowane i skoordynowane działania komunikacyjne państwa służące realizacji racji stanu, budowaniu odporności na manipulację oraz spójności przekazu w sytuacjach kryzysowych. Komunikacja strategiczna obejmuje komunikację zewnętrzną (międzynarodową) i wewnętrzną (na linii administracja – społeczeństwo – instytucje).

7) **odporność informacyjna** – zdolność instytucji i społeczeństwa do rozpoznawania, odrzucania i neutralizacji szkodliwych oddziaływań informacyjnych przy zachowaniu ciągłości procesów demokratycznych oraz spójności społecznej.

8) **polityka bezpieczeństwa informacji** – uporządkowany w celowy sposób zestaw praw, norm, procedur i dobrych praktyk regulujących: pozyskiwanie, gromadzenie, przechowywanie, przetwarzanie, dystrybucję, ochronę oraz niszczenie informacji, zapewniający stosowny do potrzeb i warunków działania danego podmiotu poziom ilościowy i jakościowy tej informacji oraz tam, gdzie trzeba, właściwe rozwiązania reglamentacyjno-ochronne.

9) **polityka bezpieczeństwa informacyjnego RP** – (dalej polityka bezpieczeństwa informacyjnego) to celowa i zorganizowana działalność państwa polskiego prowadzona z udziałem pod-

miotów społecznych i prywatnych, ukierunkowana na tworzenie i utrzymywanie w jak najlepszym jakościowo i ilościowo kształcie własnych zasobów informacyjnych i mechanizmów ich użytkowania, połączona z efektywną ich ochroną przed destrukcyjnym oddziaływaniem zdarzeń losowych, podmiotów konkurencyjnych, nieprzyjaznych czy wrogich oraz usuwaniem i minimalizowaniem barier informacyjnych.

10) **potencjał informacyjny państwa** – suma zasobów informacyjnych, infrastruktury informacyjnej oraz zdolności do kreowania, ochrony i wykorzystania przewagi informacyjnej w celu zapewnienia bezpieczeństwa państwa oraz realizacji celów strategicznych w warunkach rywalizacji czy konfliktów.

11) **strategiczne priorytety bezpieczeństwa informacyjnego RP** – (dalej strategiczne priorytety) wskazane przez polskie władze państwowe kluczowe cele w dziedzinie zapewnienia bezpieczeństwa informacyjnego RP.

12) **suwerenność informacyjna państwa** – autonomiczne możliwości w zakresie kreowania regulacji oraz realizacji działań dotyczących procesów informowania, komunikowania, ochrony systemów informacyjnych i zasobów informacyjnych. Suwerenność informacyjna państwa obejmuje także zapewnienie wolności obywatelskich w sferze informacyjnej oraz zdolność struktur państwa do zwalczania zagrożeń informacyjnych. Suwerenność informacyjna jest składowym elementem ogólnej suwerenności państwa.

13) **system bezpieczeństwa informacyjnego RP** – (dalej system bezpieczeństwa informacyjnego) skoordynowany wewnętrznie zbiór elementów organizacyjnych, osobowych i ma-

teriałowych, mających za zadanie: zapewnienie na pożądanym poziomie jakościowym i ilościowym dostępu do informacji organom administracji publicznej oraz społeczeństwu, przeciwdziałanie zagrożeniom bezpieczeństwa informacyjnego w różnych formach, reagowanie na występujące zagrożenia, likwidowanie i ograniczanie barier informacyjnych, zapewnianie wymaganego poziomu ochrony informacji, które należy chronić ze względu na interesy państwa i zamieszkującego go społeczeństwa, prowadzenie sprawnej współpracy międzynarodowej w sprawach bezpieczeństwa informacyjnego oraz podejmowanie ofensywnych i defensywnych działań w odpowiedzi na różne formy agresji informacyjnej.

14) **uwarunkowania bezpieczeństwa informacyjnego państwa** – zmienne czynniki materialne i niematerialne wpływające na stan i dynamikę bezpieczeństwa informacyjnego państwa, jego charakter i przeobrażenia, architekturę systemu bezpieczeństwa oraz politykę bezpieczeństwa informacyjnego.

15) **walka informacyjna** – zorganizowane działania informacyjne, defensywne i ofensywne, prowadzone stosownie do możliwości i zamiarów stron walczących, mające na celu forsowanie i realizację określonych, posiadających sprecyzowany, ograniczony zakres celów (politycznych, wojskowych, ekonomicznych i in.) w odniesieniu do konkretnego przeciwnika lub przeciwników.

16) **wojna informacyjna** – planowana forma przemocy stosowana na szeroką skalę przez państwo (koalicję państw) w stosunku do innego podmiotu państwowego (lub podmiotów), w ramach której dąży się do korzystnego rozstrzygnięcia istniejących sporów, spełnienia wysuwanych żądań czy narzucenia rozwiązań

i zachowań na drodze prowadzonych na szeroką skalę obezwładniających działań w różnych sferach: politycznej, gospodarczej, wojskowej, społecznej, ekologicznej i in. realizowanych przy użyciu różnorodnych narzędzi informacyjnych.

17) **wolność informacyjna jednostki** – umocowane na gruncie prawa międzynarodowego i wewnętrznego zagwarantowanie każdej osobie wolnego dostępu do informacji publicznej, wolności słowa bez cenzury prewencyjnej oraz swobody zarządzania informacjami osobistymi.

18) **zagrożenia dla bezpieczeństwa informacyjnego RP** – (dalej zagrożenia dla bezpieczeństwa informacyjnego) ogół zjawisk, działań i czynników stwarzających realną i potencjalną oraz bezpośrednią lub pośrednią możliwość wyrządzenia szkód w narodowej infosferze oraz naruszenia interesów informacyjnych RP.

2. Cele strategiczne RP w sferze bezpieczeństwa informacyjnego

Wprowadzenie do politycznych koncepcji i praktycznych działań na rzecz bezpieczeństwa państwa jego informacyjnego wymiaru wiąże się z dynamicznymi przeobrażeniami infosfery, które szczególnego przyspieszenia nabrały wraz z rozwojem nowoczesnych technik i kanałów przesyłania informacji oraz powstaniem Internetu. Chociaż aspekty informacyjne zawsze były obecne w planowaniu i działaniu na rzecz bezpieczeństwa, to jednak dopiero w następstwie rozwoju społeczeństwa informacyjnego bezpieczeństwo informacyjne uzyskało status jednego z fundamentalnych składników bezpieczeństwa państwa. Biorąc pod uwagę długofalowe i kompleksowe tendencje dotyczące rozwoju sytuacji w Polsce, w jej bliższym i dalszym otoczeniu oraz na świecie, można stwierdzić, że interesy narodowe RP w sferze bezpieczeństwa informacyjnego obejmują:

- kształtowanie narodowej infosfery zgodnie z racją stanu;
- nieustanne rozwijanie potencjału informacyjnego państwa;
- umacnianie bezpiecznego funkcjonowania państwa w infosferze;

– zapewnienie zdolności do prowadzenia działań defensywnych i ofensywnych w odpowiedzi na akty agresji informacyjnej;
– rozwój narodowego ekosystemu badawczego w zakresie zastosowań sztucznej inteligencji i technologii kwantowych w obszarze bezpieczeństwa informacyjnego;
– budowanie odporności instytucji i jednostek na destrukcyjne oddziaływania wymierzone w ich zasoby informacyjne;
– kształtowanie infosfery ukierunkowane na promowanie zasad i pozytywnych wartości kluczowych dla rozwoju RP i przeciwdziałanie negatywnym zjawiskom;
– wzmacnianie kompetencji cyfrowych społeczeństwa poprzez różne formy edukacji ze szczególnym uwzględnieniem przeciwdziałania dezinformacji;
– ochronę suwerenności informacyjnej RP oraz zapewnienie realizacji konstytucyjnych praw i wolności informacyjnych obywateli;
– systematyczny rozwój informatyzacji administracji i usług publicznych;
– zapewnienie bezpieczeństwa informacyjnego przedsiębiorcom i użytkownikom platform społecznościowych;
– kształtowanie efektywnego i nowoczesnego narodowego systemu bezpieczeństwa informacyjnego;
– stałe rozwijanie dostępności do informacji spoza narodowej infosfery.

3. Uwarunkowania bezpieczeństwa informacyjnego RP

3.1. Znaczenie uwarunkowań

Uwarunkowania należy traktować jako zmienne determinanty materialne i niematerialne wpływające na stan i dynamikę bezpieczeństwa informacyjnego państwa, jego charakter i przeobrażenia oraz architekturę systemu bezpieczeństwa. Czynniki warunkujące bezpieczeństwo informacyjne ze względu na zmienny charakter wymagają ciągłej analizy. Ich transfiguracja wynikająca z procesów społecznych, zmian w układzie międzynarodowym, przemian cywilizacyjnych oraz rozwoju technologicznego powoduje, że zapewnianie bezpieczeństwa informacyjnego jest permanentnym procesem. Właściwe określenie istniejących oraz perspektywicznych determinant stanowi warunek zaprojektowania spójnego systemu bezpieczeństwa informacyjnego oraz skutecznego przeciwdziałania zagrożeniom i podejmowania pojawiających się wyzwań. Celna prognoza dotycząca przyszłych czynników warunkujących bezpieczeństwo informacyjne niesie pomoc w zapobieganiu zaistnienia niebezpieczeństw. Nieuwzględnianie lub marginalizowanie istotnych determinant może doprowadzić do sytuacji kryzysowych i groźnych dla bezpieczeń-

stwa narodowej infosfery. Dlatego warunkiem skutecznego zapewnienia bezpieczeństwa informacyjnego RP jest adaptowanie jego architektury do zmieniających się uwarunkowań. Na poziomie ogólnym uwarunkowania bezpieczeństwa informacyjnego wynikają m.in. z ustroju politycznego państwa, obowiązującego ustawodawstwa, istniejących struktur chroniących państwową i społeczną infosferę, obecnych i przyszłych zagrożeń informacyjnych, poziomu wykształcenia społeczeństwa, historii, tradycji i kultury, rozwoju gospodarczego, infrastruktury informatycznej, sytuacji geopolitycznej, stanu stosunków międzynarodowych, powiązań sojuszniczych. Na tej podstawie można wyróżnić trzy zasadnicze grupy determinant bezpieczeństwa informacyjnego RP:

- wewnętrzne;
- zewnętrzne;
- techniczno-technologiczne.

Należy podkreślić, że w zglobalizowanym świecie coraz trudniejsze jest jednoznaczne przeprowadzenie podziału na uwarunkowania wewnętrzne i zewnętrzne. Wynika to z charakteru społeczeństwa informacyjnego, w którym zanikają bariery, w tym zwłaszcza te komunikacyjne między różnymi podmiotami. W związku z tym tradycyjne granice międzypaństwowe nie mogą już zapewnić w takim stopniu jak w epoce „przedinternetowej" bezpieczeństwa narodowej infosfery.

3.2. Uwarunkowania wewnętrzne

Do zasadniczych wewnętrznych uwarunkowań bezpieczeństwa informacyjnego RP zaliczyć należy zbiór czynników: ustro-

jowo-prawnych, politycznych, społecznych, wojskowych, cywilizacyjno-kulturowych oraz organizacyjno-instytucjonalnych.

Uwarunkowania ustrojowo-prawne odnoszą się do ustroju państwa polskiego oraz jego systemu prawnego dotyczącego infosfery. Determinują one prawa i obowiązki obywateli, kompetencje organów państwa oraz dopuszczalne granice aktywności władz. W Rzeczypospolitej Polskiej podstawą w tym zakresie są normy prawne powszechnie obowiązujące zawarte w konstytucji, ustawach, aktach wykonawczych, niekiedy również w przepisach resortowych. Określony w Konstytucji RP ustrój demokratyczny warunkuje pluralizm polityczny oraz gwarantuje prawa i wolności obywatelskie, w tym również w sferze informacyjnej. Ustawa zasadnicza zapewnia każdej osobie wolność wyrażania poglądów, uzyskiwania i rozpowszechniania informacji, w tym również tych dotyczących działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Te swobody obywatelskie w dostępie do informacji mogą zostać ograniczone i zablokowane tylko w szczególnych sytuacjach, gdy jest to konieczne dla zapewnienia bezpieczeństwa, porządku publicznego, ochrony środowiska, zdrowia i moralności publicznej. Przesłankami wyłączenia jawności jest również ochrona wolności i praw innych osób oraz ważnego interesu gospodarczego państwa. Normy konstytucyjne wyznaczają ogólne ramy prawne systemu bezpieczeństwa informacyjnego. Kolejnym czynnikiem prawnym warunkującym bezpieczeństwo informacyjne są przepisy zawarte w ustawach. Przede wszystkim są to: ustawa o dostępie do informacji publicznej, ustawa prawo prasowe, ustawa o radiofonii i telewizji, ustawa o ochronie informacji niejawnych, ustawa o krajowym

systemie cyberbezpieczeństwa, ustawa o ochronie danych osobowych, ustawa kodeks karny. Ważne są również przepisy ustaw zawierające regulacje dotyczące prawnie chronionych tajemnic zawodowych. Normy prawne tworzą ustrój informacyjny państwa, którego poszczególne elementy ze względu na dynamikę procesów legislacyjnych są ciągle modyfikowane. Proces kształtowania ustroju informacyjnego państwa musi gwarantować prawa obywatelskie do swobodnego uzyskiwania i rozpowszechniania informacji, ale również uwzględniać pojawiające się nowe zagrożenia, wyzwana i ryzyka, w tym: polaryzację informacyjną i degradację jakości debaty publicznej, deficyt kompetencji w obszarze sztucznej inteligencji i analityki danych w administracji, nabywanie odpowiedniej znajomości technik i technologii informacyjnych, rosnącą ekspozycję dzieci i seniorów na manipulację. W związku tym jako priorytet należy traktować dbałość o właściwe tempo dostosowywania ustawodawstwa do zmieniających się zagrożeń i technologii informacyjnych.

Polityczne uwarunkowania bezpieczeństwa informacyjnego kształtowane są w wyniku działalności indywidualnych oraz zbiorowych podmiotów funkcjonujących w ramach systemu politycznego. W tej grupie szczególny wpływ na wspomniane uwarunkowania wywierają partie polityczne tworzące większość rządową, jak i te będące w opozycji, grupy lobbystyczne, środowiska opiniotwórcze, politycy o dużym społecznym autorytecie. Wymienione podmioty życia politycznego RP formułują własne przekazy informacyjne. W ten sposób próbują pozyskiwać zwolenników, przedstawiać i uzasadniać swoje decyzje, propagować własne programy, wpływać na opinię publiczną, tworzyć ko-

rzystną dla siebie atmosferę społeczną. Zdarza się, że w tym celu wspomniane podmioty przekazują treści zmanipulowane i nieprawdziwe. Silnie spolaryzowana scena polityczna sprzyja takim negatywnym zachowaniom. Ich konsekwencją jest zainfekowanie sfery informacyjnej fake newsami, utrudnienia w docieraniu do wiarygodnych informacji, pogłębiający się chaos informacyjny, dezorientacja społeczeństwa oraz jego podział i separacja w „bańkach informacyjnych". Silna polaryzacja tworzy dogodne warunki do wywierania wpływu ze strony zagranicznych podmiotów na narodową infosferę. Dzięki temu mogą one skutecznie prowadzić kampanie dezinformacyjne skierowane przeciwko strukturom państwa, obowiązującym rozwiązaniom systemowym, podejmowanym decyzjom oraz konkretnym osobom. Ich efektem jest blokowanie merytorycznej debaty publicznej, dezintegracja społeczeństwa i jego podział na zwalczające się grupy zdolne do kontaktów jedynie w ramach własnej „banki informacyjnej". Rozwiązaniem tej sytuacji jest podjęcie wielopoziomowych działań przez struktury państwowe, partie polityczne, ośrodki akademickie, organizacje pozarządowe, think tanki, autorytety społeczne. Celem tych inicjatyw powinno być przyjęcie „kodeksu dobrych praktyk antydezinformacyjnych" dotyczących przestrzegania przez uczestników debat publicznych zasad rzetelności w sferze informacyjnej, wprowadzenie programów edukacyjnych w zakresie zagrożeń informacyjnych oraz korzystania ze współczesnych mediów, uchwalenie przepisów uniemożliwiających intencjonalne rozpowszechnianie treści dezinformacyjnych, podjęcie przez instytucje państwowe efektywnych działań dotyczących zablokowania prowadzenia przez zagraniczne podmioty wrogich operacji wpływu.

Społeczne uwarunkowania bezpieczeństwa informacyjnego obejmują cechy wspólne społeczeństwa oraz jego poszczególnych odłamów i ich umiejętności, a także tendencje w zakresie korzystania z infosfery. Szczególnie ważne determinanty z tego obszaru uwarunkowań dotyczą społecznej odporności na manipulacje informacyjne, fałszywe treści, działania dezinformacyjne, wrogie działania obcych państw w sferze informacyjnej, w tym również wywiadowcze. Społeczna odporność na pojawiające się zagrożenia informacyjne jest wciąż niedocenianym czynnikiem kształtującym poziom informacyjnego bezpieczeństwa państwa. Szczególnie istotne w tym kontekście są: świadomość informacyjna i kompetencje cyfrowe. Społeczeństwo wyposażone w odpowiednią wiedzę, umiejętności psychologiczne i informacyjne oraz zasady etyczne jest bardziej odporne na negatywne oddziaływania. Podatność na dezinformację, zagraniczne operacje wpływu, wrogą działalność jest większa w społeczeństwie spolaryzowanym, które łatwo ulega podziałom. Dlatego ważnym elementem kreowania polityki bezpieczeństwa informacyjnego państwa są programy edukacyjne dotyczące właściwego odbioru treści informacyjnych oraz rozpoznawania fałszywych przekazów i manipulacji w tej sferze. Ich uzupełnieniem powinna być działalność ośrodków akademickich i naukowych w zakresie badania pojawiających się zagrożeń informacyjnych, wykorzystywania w celu ich zwalczania nowoczesnych technologii i innowacyjnych metod oraz kształcenia państwowych i społecznych elit w dziedzinie bezpieczeństwa informacyjnego. Jako istotne dla tego obszaru działań należy uznać ograniczanie barier biurokratycznych dla nowatorskich przedsięwzięć z zakresu bezpieczeństwa infor-

macyjnego oraz odpowiednie wsparcie dla realizujących je osób i ośrodków.

Wojskowe uwarunkowania bezpieczeństwa informacyjnego to czynniki informacyjne wpływające na system militarny państwa, zarówno w ujęciu aktywnym, jak i pasywnym. Podstawą sprawności i efektywności systemu militarnego jest działalność oparta na informacjach, które są rzetelne, przydatne, dokładne, użyteczne, kompletne, niezawodne i aktualne. Informacje dotyczące militarnych aspektów bezpieczeństwa państwa muszą być dostarczone we właściwym terminie oraz bezpiecznymi kanałami uniemożliwiającymi obcą ingerencję w ich treść. Zbiór informacji dotyczący przygotowań i zasobów militarnych państwa należy traktować jako jego zasób strategiczny. Musi on być odpowiednio zabezpieczony różnymi metodami: prawnymi, osobowymi, fizycznymi, technologicznymi i in. Warunek ten dotyczy zarówno pokojowego i stabilnego funkcjonowania państwa, jak i okoliczności, kiedy znajdzie się ono w sytuacji kryzysowej lub zagrożenia wojennego.

System militarny państwa powinien uzyskiwać informacje o niebezpieczeństwach różnego typu, nie tylko o zagrożeniach militarnych. Współcześnie agresja militarna jest często poprzedzana działaniami niekonwencjonalnymi, np. w postaci presji ekonomicznej, eksportu przestępczości zorganizowanej, akcji terrorystycznych i dywersyjnych. W tym katalogu zagrożeń należy również uwzględnić operacje wywiadowcze, informacyjne, psychologiczne, propagandowe, dezinformacyjne. Ich celem może być zarówno uzyskanie strategicznych informacji, jak i wpływanie na decyzje władz, zainfekowanie społeczeństwa dezin-

formującymi przekazami, wytworzenie w atakowanym państwie atmosfery nieufności czy dokonanie zmiany społecznych postaw. Rozwój działań militarnych, w których prowadzenie walki informacyjnej to jeden z podstawowych instrumentów, spowodował, że wroga ingerencja informacyjna może być ukierunkowana zarówno na wybraną sferę życia publicznego, jak i sprofilowana na konkretną grupę społeczną, która następnie stanie się nośnikiem komunikatów dezintegrujących szersze społeczności. Brak w systemie bezpieczeństwa informacyjnego struktur, które odpowiadają za przeciwdziałanie tego typu atakom lub ich słabość, naraża państwo na poważne zagrożenia informacyjne. Dlatego istotnym czynnikiem kształtowania bezpieczeństwa państwa jest sprawny system bezpieczeństwa informacyjnego odpowiednio powiązany i współpracujący z systemem militarnym, który w swoich strukturach musi posiadać także specjalistyczne narzędzia informacyjne, za pomocą których uzyskuje, przetwarza, analizuje, dystrybuuje i wykorzystuje informacje dotyczące wojskowego wymiaru bezpieczeństwa państwa.

Cywilizacyjno-kulturowe uwarunkowania bezpieczeństwa informacyjnego wiążą się z przynależnością do określonego typu cywilizacji, historią państwa i narodu, jego kulturą, tradycją, systemem religijnym, procesami kształtowania świadomości narodowej oraz struktur państwowych. Wszystkie te czynniki wpływają nie tylko na tożsamość społeczeństwa, poczucie przynależności grupowej, wzajemne więzi i relacje międzyludzkie, ale determinują także zasady postępowania w sytuacjach zagrożeń, metody obrony państwa oraz kształt i charakter struktur państwowych, w tym również tych odpowiedzialnych za bezpieczeństwo infor-

macyjne. Uwzględnianie uwarunkowań cywilizacyjno-kulturowych stanowi ważny element procesu kreowania bezpieczeństwa informacyjnego państwa. Duchowe podstawy życia zbiorowego są często niedocenianym elementem wpływającym na sferę informacyjną. Wskazując na cywilizacyjno-kulturowe determinanty uwarunkowań bezpieczeństwa informacyjnego RP, nie można zapominać o europejskim systemie wartości ukształtowanym przez zachodnie chrześcijaństwo, rzymskie prawo oraz grecką filozofię. Jedną z tych wartości jest dążenie do prawdy. W dalszym ciągu jest ono dla wielu ludzi i wspólnot wyznacznikiem działalności i ważnym celem. Istotnym elementem dziedzictwa duchowego każdego narodu jest historia, która dostarcza wiedzy o jego korzeniach, rozwoju, w tym także o zwycięstwach i klęskach z przeszłości. Poznanie i rzetelna analiza wydarzeń historycznych pomagają unikać powielania błędów oraz przewidywać i oceniać potencjalne zagrożenia. Doświadczenia historyczne pokazują, że zaniechanie rozwoju własnego systemu bezpieczeństwa może być źródłem upadku państwa. Jak ważne są uwarunkowania cywilizacyjno-kulturowe dla sfery bezpieczeństwa informacyjnego widać na przykładzie zmagań Polaków o zachowanie dziedzictwa niematerialnego, w tym ojczystego języka i kultury. Ataki ukierunkowane na dokonanie erozji świadomości charakterystycznej dla narodu są poważnym zagrożeniem dla jego istnienia. Brak odpowiedniego zakorzenienia w przeszłości może przyczynić się do zerwania więzi społecznych, a w dalszej perspektywie do upadku wspólnoty narodowej i osłabienia spajającego ją państwa. Pielęgnowanie niematerialnego dziedzictwa, które pozwoliło polskiemu narodowi przetrwać okresy zniewolenia, represji, prób fizycz-

nej eliminacji, oraz przekazywanie historycznych doświadczeń muszą być uwzględnione w procesie budowy społecznej odporności na zagrożenia informacyjne. Twórcze wykorzystywanie dziedzictwa cywilizacyjno-kulturowego jest istotnym czynnikiem kształtowania dobrze funkcjonującego systemu bezpieczeństwa informacyjnego państwa. Chwalebne doświadczenia historyczne, atrakcyjna kultura, sukcesy naukowe mogą stać się również elementem tzw. miękkiej siły w polityce bezpieczeństwa.

Organizacyjno-instytucjonalne uwarunkowania bezpieczeństwa informacyjnego to czynniki związane z organizacją jawnej i niejawnej działalności podmiotów funkcjonujących w polskiej infosferze lub kształtujących jej charakter. Mają one lub mogą mieć wpływ na treści informacyjne przekazywane w mediach, kształtowanie opinii publicznej, podejmowane przez władze decyzje, zmiany polityczne, uchwalane normy prawne itp. Podmiotami tymi są zarówno organy i instytucje państwa zbierające, gromadzące, przetwarzające, analizujące, rozpowszechniające informacje, regulujące infosferę, jak i instytucje prywatne, takie jak organizacje pozarządowe, fundacje, stowarzyszenia twórców, think tanki, ośrodki badawcze, uczelnie niepubliczne czy skomercjalizowane mass media. W sferze organizacyjno-instytucjonalnej istotna jest kwestia przejrzystości działania i odpowiedzialności instytucji publicznych w obszarze usług informacyjnych. Do czynników organizacyjno-instytucjonalnych należy zaliczyć również organy, instytucje, służby specjalne obcych państw, które dążą do uzyskania wpływu na polską infosferę oraz dostępu do jej elementów. Dotyczy to zarówno jej segmentu jawnego i ogólnodostępnego, jak i niejawnego zawierającego chronione zasoby informacyjne państwa.

Niekontrolowane oddziaływanie obcych podmiotów może w wyniku wywołania zagrożeń informacyjnych doprowadzić do szeregu negatywnych konsekwencji. W skrajnych sytuacjach może dojść nawet do dezintegracji społeczeństwa, zahamowania rozwoju, naruszenia stabilności państwa oraz podważenia jego suwerenności. Możliwości blokowania negatywnych wpływów zagranicznych podmiotów informacyjnych zależą od istniejącego systemu prawnego, skuteczności instytucji państwa, świadomości społeczeństwa oraz determinacji władz. Słabości organizacyjne, niedostateczny poziom systemowej współpracy, brak skuteczności wspomnianych elementów mogą powodować istotne deficyty w zakresie efektywnego działania na rzecz bezpieczeństwa informacyjnego państwa. Sprawia to, że uwarunkowania organizacyjno-instytucjonalne stanowią znaczący i jednocześnie bardzo wrażliwy czynnik w kształtowaniu tego wymiaru bezpieczeństwa.

3.3. Uwarunkowania zewnętrzne

Zewnętrzne uwarunkowania bezpieczeństwa informacyjnego tworzą zjawiska, wydarzenia, działania jednostek i podmiotów zbiorowych, procesy społeczno-polityczne, zmiany cywilizacyjne oraz byty niematerialne występujące w otoczeniu zewnętrznym państwa, które oddziałują lub mogą oddziaływać na jego bezpieczeństwo informacyjne. Zewnętrzne (zagraniczne) oddziaływania mogą mieć charakter neutralny, pozytywny lub negatywny. Pozytywne oddziaływania informacyjne z zagranicy przejawiają się np. w wymianie strategicznych informacji czy międzypaństwowej współpracy dotyczącej projektów ze sfery

bezpieczeństwa informacyjnego. Z kolei negatywne oddziaływania informacyjne przybierają różne formy. Jest to uzależnione od wielu czynników, m.in. celu takich operacji, podmiotu realizującego te działania oraz tego, kto ma być ofiarą negatywnego oddziaływania. W związku z tym można wyróżnić negatywne oddziaływania informacyjne z zagranicy o charakterze wywiadowczym, politycznym, terrorystycznym, kryminalnym, psychologicznym czy kulturowym. Zagraniczne podmioty mogą oddziaływać poprzez szpiegostwo polityczne i gospodarcze, operacje dezinformacyjne i propagandowe, celowe ujawnianie i publikowanie tajemnic oraz strategicznych informacji państwowych, wywieranie wpływu na nastroje społeczne, procesy polityczne (w tym na procesy wyborcze) i decyzje władz, działalność kryminalną w sferze informacyjnej, włamywanie się do zasobów informacyjnych i ich kradzież, technologiczny sabotaż sieci teleinformatycznych w celach politycznych lub uzyskania korzyści materialnych. Konsekwencjami negatywnego oddziaływania informacyjnego mogą być nietrafne decyzje wyborcze, błędne decyzje dotyczące polityki wewnętrznej i zagranicznej, inwestycji gospodarczych, rozwiązań społecznych, ochrony informacji i zasobów strategicznych, rozwoju sił zbrojnych.

Do istotnych składników uwarunkowań zewnętrznych bezpieczeństwa informacyjnego należą uwarunkowania geostrategiczne. Położenie geostrategiczne państwa polskiego wpływa nie tylko na jego ogólny poziom bezpieczeństwa, występujące zagrożenia militarne, energetyczne, finansowe czy ekologiczne, ale również na stan bezpieczeństwa informacyjnego. Skala, formy, intensywność, charakter zagranicznych oddziaływań infor-

macyjnych zależą również od sytuacji międzynarodowej, w tym od relacji z poszczególnymi państwami z bliższego i dalszego otoczenia. System bezpieczeństwa informacyjnego państwa musi uwzględniać występujące w związku z tym szanse, wyzwania, ryzyka i zagrożenia. Współcześnie działania informacyjne są ważnym instrumentem funkcjonowania na arenie międzynarodowej. Globalny system informacyjny sprzyja kształtowaniu określonych postaw i opinii w odniesieniu do poszczególnych państw. Dzięki precyzyjnym operacjom dezinformacyjnym i propagandowym opartym na nowoczesnych technologiach możliwe jest np. dyskredytowanie wybranego podmiotu państwowego na forum międzynarodowym. Zagraniczne podmioty realizują to w praktyce poprzez tworzenie nieprzychylnej atmosfery i rozpowszechnianie dezawuujących treści dotyczących struktur dyskredytowanego państwa, krytykowanie jego polityki, osłabianie pozycji międzynarodowej, wspieranie interesów obcych podmiotów, wywoływanie wewnętrznych konfliktów etnicznych, religijnych, społecznych, gospodarczych, ekologicznych itp. Środkiem służącym do minimalizowania tych zagrożeń może być aktywna polityka zagraniczna w sferze informacyjnej, kształtowanie pozytywnego wizerunku państwa, działania lobbystyczne, wzmocnienie przekazów informacyjnych w instytucjach sojuszniczych, tworzenie koalicji „wspólnych spraw" i nawiązywanie współpracy informacyjnej z innymi państwami w celu przeciwdziałania zagrożeniom w infosferze.

W związku z powyższymi uwarunkowaniami państwo polskie musi posiadać zdolności do analizowania zamiarów innych państw, poznawania ich długofalowych celów oraz kierunków po-

lityk zagranicznych, rozpoznawać pojawiające się zagrożenia oraz starać się przewidywać rozwój wydarzeń w regionie, potencjalnie niebezpieczne sytuacje, możliwe eskalacje napięć i zmieniające się okoliczności. Działania takie służą zapewnieniu suwerenności informacyjnej, która jest istotnym atrybutem umożliwiającym realizację narodowych celów z zakresu bezpieczeństwa informacyjnego, w tym skutecznej ochrony infosfery, niezależnie od zachowań innych państw. W sferze zewnętrznej należy wyróżnić również traktatowe uwarunkowania bezpieczeństwa informacyjnego. Ich podstawę stanowią zobowiązania wynikające z zawartych umów, porozumień i traktatów międzynarodowych. Są to determinanty informacyjne dotyczące relacji RP z innymi państwami, organizacjami i instytucjami międzynarodowymi, partnerami zagranicznymi i sojusznikami. Uwarunkowania traktatowe wyznaczają prawa i obowiązki poszczególnych stron umów zawartych w sferze informacyjnej. Na ich podstawie państwo polskie może żądać ochrony swoich informacji, ścigać przestępstwa informacyjne, wspierać informacyjnie sojuszników oraz uzyskiwać od nich potrzebne informacje, w tym również wywiadowcze. Członkostwo Polski w organizacjach międzynarodowych, w tym zwłaszcza UE i NATO, stanowi element wzmacniający bezpieczeństwo informacyjne.

Rozpatrując zagadnienie zewnętrznych czynników wpływających na stan bezpieczeństwa informacyjnego państwa polskiego, należy również uwzględnić uwarunkowania ustrojowo-polityczne, organizacyjno-instytucjonalne, polityczne, społeczne, wojskowe, cywilizacyjno-kulturowe oraz techniczno-technologiczne odnoszące się do charakterystyki i właściwości podmiotów zagranicznych oddziałujących w bezpośredni lub pośredni sposób na państwo polskie.

3.4. Uwarunkowania techniczno-technologiczne

Szybko zachodzące zmiany techniczno-technologiczne przeobrażające współczesny świat oraz stanowiącą jego szczególną część – infosferę – powodują konieczność wyróżnienia specyficznej grupy determinant bezpieczeństwa informacyjnego. Są nimi uwarunkowania techniczno-technologiczne. Obejmują one całokształt rozwiązań sprzętowych, programowych oraz infrastrukturalnych odnoszących się do systemów teleinformatycznych, urządzeń mobilnych, infrastruktury sieciowej oraz innych urządzeń wykorzystywanych w procesach informacyjnych. Uwarunkowania te postrzegać trzeba także przez pryzmat możliwości, jakie stwarzają dla bezpieczeństwa narodowej infosfery oraz rozwoju możliwości państwa w tym zakresie prace badawcze oraz polityka wdrożeń i transferu zagranicznych rozwiązań.

Przeobrażenia cywilizacyjne i powstanie społeczeństwa informacyjnego spowodowały, że systemy teleinformatyczne oraz cyfryzacja infosfery stały się nieodzowne w działalności państwa i decydują o jego sprawnym funkcjonowaniu. Towarzyszy temu nieustanny rozwój zagrożeń w infosferze (zwłaszcza w jej cyfrowym segmencie). Infosfera i współtworząca ją cyberprzestrzeń w coraz większym zakresie stają się areną walk informacyjnych z udziałem różnych podmiotów, zarówno państwowych, jak i niepaństwowych. Nowe rozwiązania techniczno-technologiczne, w tym systemy sztucznej inteligencji, są wykorzystywane do pobudzania agresywnych zachowań społecznych, prowadzenia operacji wywiadowczo-dezinformacyjnych, informacyjnych działań w sferze militarnej oraz dokonywania przestępstw. Zagrożenia

te są obecne we wszystkich sferach życia publicznego i mogą zagrażać stabilności państwa, a w przypadku braku skutecznego przeciwdziałania również podstawom jego istnienia. Niezbędne jest zatem wykorzystywanie najnowszych zdobyczy techniki i technologii do blokowania i zwalczania wspomnianych zagrożeń. W tym kontekście szczególnie pilnym zadaniem jest rozbudowa cyfrowych segmentów architektury bezpieczeństwa informacyjnego odpornych na ewoluujące zagrożenia i skutecznie im przeciwdziałających. Stosowanie rozwiązań opartych na szerokopasmowych sieciach łączności, Internecie Rzeczy, chmurze obliczeniowej, technologii kwantowej, nanotechnologii i sztucznej inteligencji stwarza nowe możliwości rozwojowe polskiej infosfery, generuje jednak również nieznane wcześniej zagrożenia. Istotnym wyzwaniem dla państwa polskiego w kontekście charakteryzowanych uwarunkowań jest włączenie się w wyścig technologiczny dający możliwość wyjścia z roli wyłącznie użytkownika i dołączenie do tych państw, które dostarczają rozwiązania i tworzą międzynarodowe standardy z zakresu cyfrowego wymiaru bezpieczeństwa informacyjnego. Budowanie tego bezpieczeństwa oraz tworzenie rozwiązań, które mają je zapewnić, jest procesem wymagającym spełnienia wielu warunków. Należy do nich zaliczyć konieczność prowadzenia prac badawczych w obszarze technologii informacyjnych, wdrażanie nowych (rodzimych i importowanych) zaawansowanych rozwiązań, właściwe pod kątem technicznym użytkowanie systemów zapewniających bezpieczeństwo informacji. Dla osiągnięcia wysokiej skuteczności takich działań niezbędne jest posiadanie kompetentnych kadr. Konieczne jest zatem kształcenie i pozyskiwanie specjalistów dbających o bez-

pieczeństwo narodowej infosfery. Czynnikiem warunkującym przygotowywanie kadr jest posiadanie akademickich ośrodków naukowych i placówek badawczo-rozwojowych. Prowadzenie kształcenia specjalistów, badania i opracowywanie nowych technologii stwarzają dla dziedziny bezpieczeństwa informacyjnego szereg wymiernych korzyści instytucjonalno-organizacyjnych, finansowych i prestiżowych. W ten sposób można pozyskać także nowoczesne rozwiązania zapewniające bezpieczeństwo państwa w innych niż informacyjna sferach. Pozytywnym efektem intensywnego rozwoju i dostępu do osiągnięć nowoczesnej techniki i technologii w sferze informacyjnej może być uzyskanie przewagi nad rywalami.

Dla zapewnienia bezpieczeństwa informacyjnego państwa konieczne jest również stosowanie nowoczesnych technik i technologii do ochrony istniejących systemów teleinformatycznych oraz prowadzenie systematycznej modernizacji tych systemów, zapewniającej odporność na nowe zagrożenia. Nowoczesne technologie zmieniają także metody zabezpieczania przed zagrożeniami informacyjnymi. Zadania w tym zakresie z powodzeniem mogą już realizować urządzenia kompatybilne z systemami sztucznej inteligencji oraz Internetem Rzeczy. Wprowadzanie do użytkowania nowoczesnych krajowych technologii to jeden z ważnych czynników budowania suwerenności informacyjnej. Oznacza to, że w projektowaniu prorozwojowych działań państwa muszą zostać uwzględniane rozwiązania techniczno-technologiczne, które ze względu na znaczenie sfery bezpieczeństwa informacyjnego, nieustanny rozwój możliwości podmiotów wrogich i nieprzyjaznych muszą mieć narodową proweniencję.

4. Polityka bezpieczeństwa informacyjnego RP

4.1. Założenia ogólne

Fundament polityki bezpieczeństwa informacyjnego państwa polskiego tworzą przedsięwzięcia koncepcyjne i praktyczne, realizowane przez różne podmioty państwowe i niepaństwowe. Wszystkie one działają zgodnie z porządkiem ustrojowym pod kierownictwem kompetentnych organów państwa. Ich aktywność skupiona jest na kreowaniu takich warunków funkcjonowania infosfery, aby redukować powstawanie zagrożeń, kształtować warunki sprzyjające jej harmonijnemu rozwojowi oraz projektować i wprowadzać w życie rozwiązania pozwalające skutecznie reagować w sytuacjach niekorzystnych i niebezpiecznych z punktu widzenia bezpieczeństwa informacyjnego RP.

W procesie konceptualizacji i realizacji polityki bezpieczeństwa informacyjnego Rzeczypospolita Polska musi uwzględniać zarówno aktualny, jak i perspektywiczny stan środowiska bezpieczeństwa, w tym brać pod uwagę zróżnicowane interesy i warunki funkcjonowania innych państw oraz wewnętrznych podmiotów politycznych, społecznych czy gospodarczych. Ośrodki

władzy państwowej, kierując się racją stanu, muszą w ramach polityki bezpieczeństwa informacyjnego ściśle ze sobą współpracować, zapobiegać konfliktom oraz rozwiązywać te z nich, które się materializują. Polityka bezpieczeństwa informacyjnego jest obszarem aktywności państwa, który ze względu na swoje fundamentalne znaczenie dla jego egzystencji i rozwoju wymaga szczególnej rozwagi oraz odpowiedzialnego działania wszystkich tworzących oraz realizujących ją podmiotów.

Polityka bezpieczeństwa informacyjnego obejmuje powiązane i przenikające się, ale zachowujące swoją specyfikę dwie grupy planów i działań. Jedna skierowana jest na otoczenie państwa, druga na jego wnętrze. Jest to rezultat istnienia dwóch powiązanych ze sobą wymiarów bezpieczeństwa państwa: wewnętrznego oraz zewnętrznego (międzynarodowego). Działania mające na celu zapewnienie bezpieczeństwa informacyjnego są przedsięwzięciami skomplikowanymi. Wynika to ze złożonej natury informacji oraz charakteru współczesnej infosfery. Powoduje to, że mimo rozległych doświadczeń praktycznych i stosowania nowoczesnych rozwiązań technicznych zapobieganie i zwalczanie zagrożeń oraz skuteczne podejmowanie wyzwań w odniesieniu do informacyjnego wymiaru bezpieczeństwa państwa jest zadaniem złożonym. Należy wskazać również na istnienie szeregu barier informacyjnych, które trzeba pokonać, konstruując i realizując politykę bezpieczeństwa informacyjnego. Biorąc pod uwagę przedstawione uwarunkowania, przyjęto, że polityka bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej to celowa i zorganizowana działalność prowadzona pod auspicjami organów państwa z udziałem podmiotów społecznych i prywatnych, ukierunko-

wana na tworzenie i utrzymywanie w jak najlepszym jakościowo i ilościowo kształcie narodowych zasobów informacyjnych i mechanizmów ich użytkowania, połączona z efektywną ochroną przed destrukcyjnym oddziaływaniem zdarzeń losowych, podmiotów konkurencyjnych, nieprzyjaznych czy wrogich oraz redukcją barier informacyjnych. Polityka bezpieczeństwa informacyjnego jest realizowana przy użyciu zróżnicowanych narzędzi. W szczególności są to instrumenty: prawne i regulacyjne, organizacyjne, ekonomiczne, edukacyjne, techniczno-technologiczne.

W ramach polityki bezpieczeństwa informacyjnego państwo polskie dąży do wykorzystania szans niesionych przez dynamiczny rozwój infosfery ze szczególnym uwzględnieniem jej cyfrowych elementów, oddalania zagrożeń, minimalizowania ich i przejmowania nad nimi kontroli, zmniejszania niedogodności związanych z istnieniem barier informacyjnych, skutecznego zarządzania ryzykiem informacyjnym. Jest to podstawowy nurt aktywności na rzecz kreowania bezpiecznej narodowej infosfery. Nie zawsze jednak ze względu na skomplikowane mechanizmy konstrukcji i funkcjonowania infosfery działania te mogą być w pełni efektywne. Powoduje to, że sfera bezpieczeństwa informacyjnego bywa niestabilna i podatna na różnego rodzaju turbulencje. Mające szczególnie zmienny charakter uwarunkowania bezpieczeństwa informacyjnego powodują, że jednym z najważniejszych elementów działań w obrębie polityki bezpieczeństwa informacyjnego musi być prowadzenie ciągłego monitoringu i diagnozowania jego stanu. Bardzo ważne jest również systematyczne rozbudowywanie i doskonalenie środków oraz instrumentów służących do osiągania zaplanowanego poziomu bezpieczeń-

stwa informacyjnego. Nie należy to do zadań łatwych, ponieważ w wielu przypadkach występuje duża rozbieżność interesów i realizowanych celów w sferze tego bezpieczeństwa na poziomie poszczególnych państw, co rodzi sytuacje konfliktowe z ograniczonym polem do osiągania kompromisów. Ponadto należy dostrzec silny wpływ:

- szybko zachodzących zmian technicznych i technologicznych w infosferze;
- inwazyjnych, konfrontacyjnych lub wrogich działań niektórych państw;
- ekspansywnej, nastawionej na zyski postawy globalnych korporacji informacyjnych;
- zmiennych jakościowo i ilościowo zagrożeń dla bezpieczeństwa informacyjnego.

Należy podkreślić, że polityka bezpieczeństwa informacyjnego RP musi obejmować ograniczanie negatywnych oddziaływań pochodzących ze strony innych państw, szeroko rozumianego środowiska międzynarodowego i wewnętrznego oraz zapewnienie wewnętrznej stabilności i harmonii informacyjnej, m.in. poprzez ochronę i rozbudowę tych zasobów informacyjnych, które mają największą wartość dla państwa polskiego. Zdarzają się jednak sytuacje, w których skala i rodzaj zagrożeń informacyjnych oraz wyzwań uniemożliwia lub znacznie ogranicza skuteczność działań mających na celu uzyskanie i utrzymanie pożądanego poziomu bezpieczeństwa informacyjnego. Możliwość zaistnienia tego rodzaju okoliczności obliguje do poszukiwania koncepcji postępowania najbardziej przydatnych w takich kryzysowych

warunkach. Nie da się ich wypracować bez uwzględnienia aktualnego i perspektywicznego stanu infosfery. Nie może to nastąpić także w oderwaniu od ogólnych uwarunkowań bezpieczeństwa państwa polskiego i budowanej na tym podłożu całościowej polityki bezpieczeństwa. W warunkach funkcjonowania globalnego społeczeństwa informacyjnego konstruowanie oraz realizowanie polityki bezpieczeństwa informacyjnego musi obejmować działania unilateralne oraz prowadzone we współpracy z innymi podmiotami państwowymi i pozapaństwowymi. Narzuca to konieczność zawierania porozumień, równoważenia interesów oraz kooperacji. Zmienny charakter sfery bezpieczeństwa informacyjnego wymaga również odpowiedniego reagowania na zachodzące lub przewidywane przeobrażenia środowiska bezpieczeństwa tak w ujęciu ogólnym, jak i sektorowym. Musi to następować zarówno w trybie bieżącego nadzoru oraz kontroli, jak i w formie okresowych pogłębionych przeglądów skuteczności polityki bezpieczeństwa informacyjnego i sprawności systemu tego bezpieczeństwa z zastosowaniem adekwatnych do uzyskanych wyników działań korygujących.

Odpowiednie przygotowanie założeń polityki bezpieczeństwa informacyjnego i tworzenie jak najlepszych warunków do wprowadzania jej w życie wymaga uwzględnienia elementów obiektywnych dotyczących realnych i potencjalnych zagrożeń, wyzwań i barier oraz elementów subiektywnych związanych z ich percepcją. Kreowanie oraz realizowanie polityki bezpieczeństwa informacyjnego musi łączyć w sposób zrównoważony rozwiązania z zakresu szerokiego (pozytywnego) postrzegania tego wymiaru bezpieczeństwa opartego na kształtowaniu bezpiecznych

warunków funkcjonowania infosfery poprzez ograniczanie możliwości powstawania zagrożeń i skuteczne podejmowanie wyzwań z metodami podejścia wąskiego (negatywnego), skoncentrowanego na przygotowaniach do obrony przed zagrożeniami. W związku z tym założenia polityki bezpieczeństwa informacyjnego RP muszą uwzględniać takie środki, instrumenty i metody oddziaływania na infosferę (w aspekcie zewnętrznym i wewnętrznym), które będą sprzyjały efektywnemu i stabilnemu funkcjonowaniu państwa polskiego w wymiarze informacyjnym oraz zapewniały możliwość osiągania i utrzymywania pożądanych stanów omawianego bezpieczeństwa. Polityka bezpieczeństwa informacyjnego to ciągle zyskujący na znaczeniu element budowania i utrzymywania na wysokim poziomie bezpieczeństwa RP. Jedną z fundamentalnych korzyści z właściwej konceptualizacji i skutecznej realizacji tej polityki jest kształtowanie wysokiej jakości infosfery narodowej.

W ramach polityki bezpieczeństwa informacyjnego Rzeczypospolita Polska dąży przede wszystkim do:

- rozpoznawania i oddalania zagrożeń informacyjnych;
- minimalizowania skutków zagrożeń, których nie uda się uniknąć;
- tworzenia potencjału (organizacyjnego, materialnego, personalnego) umożliwiającego blokowanie zagrożeń oraz skuteczne reagowanie na zagrożenia zaistniałe;
- podejmowania wyzwań związanych z bezpieczeństwem informacyjnym;
- zapewnienia właściwego przepływu informacji w ramach procesów decyzyjnych w państwie.

Polityka ta obejmuje przedsięwzięcia na rzecz:

– zapewnienia bezpieczeństwa informacyjnego podmiotów zbiorowych i indywidualnych;
– pozytywnego kształtowania perspektywicznych uwarunkowań bezpieczeństwa informacyjnego RP;
– zwiększania skuteczności instytucji działających w sferze bezpieczeństwa informacyjnego;
– budowania szerokiego konsensusu wewnętrznego i zewnętrznego (międzynarodowego) w sprawach bezpieczeństwa informacyjnego.

W ramach polityki bezpieczeństwa informacyjnego Rzeczypospolita Polska wytycza strategiczne cele i tworzy warunki organizacyjne do prowadzenia działań bieżących oraz średnio- i długookresowych na rzecz kształtowania pożądanych stanów bezpieczeństwa informacyjnego.

Strategiczne cele polityki bezpieczeństwa informacyjnego RP to:

– zapewnienie bezpiecznego funkcjonowania RP w infosferze ze szczególnym uwzględnieniem bezpieczeństwa informacyjnego struktur państwowych, sektora prywatnego i społeczeństwa obywatelskiego;
– sprawowanie kontroli nad sytuacją we własnej infosferze oraz ochrona interesów narodowych w jej zewnętrznym otoczeniu realizowane poprzez:
  - utrzymywanie i demonstrowanie gotowości do przeciwdziałania zagrożeniom informacyjnym;
  - ciągłe rozpoznawanie, analizowanie i ocenianie zagrożeń informacyjnych;

– obrona strategicznych zasobów informacyjnych państwa poprzez:
  - reagowanie na zagrożenia oraz podejmowanie działań defensywnych i ofensywnych w ramach działań prewencyjnych oraz walk informacyjnych;
  - kształtowanie świadomości społecznej w zakresie celów polityki bezpieczeństwa informacyjnego państwa oraz interesów narodowych w tym zakresie;
  - badanie polityk bezpieczeństwa informacyjnego oraz systemów bezpieczeństwa informacyjnego przeciwników i wykorzystywanie zdobywanej tą drogą wiedzy;
– utrzymywanie wysokiej sprawności narodowego systemu bezpieczeństwa informacyjnego poprzez:
  - zapewnienie zdolności podsystemu kierowania do organizowania i koordynowania działań podmiotów rządowych i pozarządowych realizujących zadania w zakresie bezpieczeństwa informacyjnego;
  - odpowiednie ustrukturalizowanie i wyposażenie podsystemów wykonawczych oraz wyznaczenie im właściwych zadań.

4.2. Wymiar wewnętrzny

We współczesnych uwarunkowaniach bezpieczeństwo i rozwój społeczno-gospodarczy Polski pozostają zależne od szybkiego i nieskrępowanego dostępu do wysokiej jakości informacji oraz jej wykorzystywania w zarządzaniu, produkcji, usługach oraz sek-

torze publicznym, w tym także tej jego części, która bezpośrednio zajmuje się sprawami bezpieczeństwa. Dynamiczny rozwój infosfery, w szczególności zaś jej składowej części, jaką jest cyberprzestrzeń, powoduje, że liczba zagrożeń informacyjnych ciągle wzrasta. Obok już znanych pojawiają się nowe ich rodzaje. Zagrożenia te oddziałują na codzienne funkcjonowanie i bezpieczeństwo instytucji publicznych, przedsiębiorstw oraz społeczeństwa, zwłaszcza na jego najmłodszych i najstarszych członków.

Państwo polskie jest zdeterminowane, aby podejmować działania, które systemowo zwiększać będą poziom bezpieczeństwa informacyjnego oraz ograniczać ryzyka związane z negatywnymi zjawiskami w infosferze. W szczególności dążyć będzie do budowania odporności na zagrożenia dla kluczowych z punktu widzenia działalności politycznej, społecznej, gospodarczej, administracyjnej oraz potrzeb bezpieczeństwa państwa zasobów i usług informacyjnych. Projekt Strategii uwzględnia istniejący porządek prawny oraz stan i oczekiwania związane z kształtem, kierunkami rozwoju infosfery państwa, a także współtworzących ją zasobów informacyjnych wraz z systemami ich przechowywania, przetwarzania i dystrybucji. Należy podkreślić, że opracowanie oraz przyjęcie Strategii Bezpieczeństwa Informacyjnego wymagają zapewnienia jej spójności ze strategią bezpieczeństwa oraz polityką bezpieczeństwa RP. Ze względu na coraz większe znaczenie bezpieczeństwa informacyjnego dla innych wymiarów bezpieczeństwa państwa polskiego należy ono do konstytutywnych składników bezpieczeństwa wewnętrznego. Podstawowy zestaw celów polityki bezpieczeństwa informacyjnego w wymiarze wewnętrznym to:

– zapewnienie dostępu do aktualnej i rzetelnej informacji;
– utrzymywanie nowoczesnej i odpornej na zagrożenia infrastruktury informacyjnej;
– skuteczna ochrona informacji wymagających stosowania reżimów ochronnych;
– wzmacnianie odporności infrastruktury informacyjnej oraz przygotowanie procedur reagowania na sytuacje kryzysowe;
– budowanie pozytywnego wizerunku państwa w wewnętrznej infosferze;
– przygotowywanie oraz wcielanie w życie programów poprawy bezpieczeństwa informacyjnego w poszczególnych dziedzinach funkcjonowania państwa;
– zwiększanie poziomu odporności państwa na zagrożenia informacyjne ze szczególnym uwzględnieniem ochrony przed manipulacją i dezinformacją oraz zagrożeniami w cyberprzestrzeni;
– wzmacnianie informacyjnego potencjału państwa poprzez zwiększanie nakładów na badania naukowe oraz prace rozwojowe ze szczególnym uwzględnieniem sztucznej inteligencji oraz technologii kwantowych i satelitarnych.

Osiąganie powyższych celów jest zadaniem realizowanym przez różne podmioty działające pod kierownictwem organów władzy publicznej. Odpowiednio do przypisanych zadań podmioty te powinny być wyposażane w niezbędne kompetencje oraz środki służące do wcielania w życie założeń polityki bezpieczeństwa informacyjnego.

Ponieważ zapewnienie bezpieczeństwa oraz pomyślny rozwój RP są zależne od stanu bezpieczeństwa informacyjnego, państwo polskie musi, w ramach kierunków działań ujętych w Strategii, systematycznie wzmacniać i rozwijać narodowy system bezpieczeństwa informacyjnego. Przedsięwzięcia w tym zakresie powinny obejmować: systemowe rozwiązania organizacyjne, finansowe, operacyjne, technologiczne, prawne, kształtowanie postaw społecznych oraz prowadzenie badań naukowych i prac rozwojowych. Podejmowane działania muszą przebiegać z poszanowaniem praw i wolności obywateli oraz w atmosferze gwarantowanego zaufania do administracji rządowej. Kluczowe znaczenie ma w tym kontekście rozwijanie narodowej wspólnoty informacyjnej integrującej działania różnych instytucji publicznych i niepublicznych. Intensywnych działań wymaga także budowanie odporności społecznej na dezinformację i operacje wpływu. Istota i znaczenie polityki bezpieczeństwa informacyjnego powodują, że głównym jej kreatorem musi być państwo. Tylko ono bowiem jest w stanie uruchomić odpowiedni zestaw środków i instrumentów, przy pomocy których w sposób uwzględniający potrzeby sfery publicznej i prywatnej można zapewnić to, co w bezpieczeństwie informacyjnym najistotniejsze: dostęp do informacji odpowiedniej jakości i w potrzebnej ilości, swobodny jej przepływ, ochronę na właściwym poziomie tych informacji, które powinny być taką ochroną objęte, a także skuteczne zapobieganie i przeciwdziałanie zagrożeniom dla bezpieczeństwa informacyjnego oraz usuwanie i niwelowanie barier informacyjnych. Dominacja państwa w polityce bezpieczeństwa informacyjnego nie oznacza marginalizacji podmiotów pozapaństwowych, które na bazie założeń tej polityki

powinny aktywnie realizować działania na rzecz rozwijania zdolności do przeciwdziałania zagrożeniom informacyjnym, jak również aktywnego ich zwalczania.

4.3. Wymiar międzynarodowy

Globalny charakter i rozliczne powiązania współczesnej infosfery powodują, że polska polityka bezpieczeństwa informacyjnego należy do tej sfery aktywności państwa, która wymaga szczególnie dobrze zaprojektowanych i starannie realizowanych działań ukierunkowanych na otoczenie międzynarodowe z uwzględnieniem jego stanu oraz perspektywy zmian. Trzeba w tym kontekście dostrzec wzrastającą skalę nielegalnych i wrogich działań prowadzonych przez różne podmioty w cyberprzestrzeni (od indywidualnych i zorganizowanych przestępców po grupy powiązane z nieprzyjaznymi państwami lub działające w ramach ich instytucji).

W obliczu rosnącej skali tych nowych, ale również starych zagrożeń, takich jak dezinformacja, szpiegostwo czy kradzież informacji ze względu na ich transgraniczny charakter, współpraca w ramach organizacji międzynarodowych oraz w formatach dwustronnych i wielostronnych, w tym z najbliższymi sojusznikami i partnerami, ma znaczenie szczególne. Należy podkreślić, że procesy zachodzące w zewnętrznej części infosfery RP charakteryzują się:

- narastaniem skali, zasięgu, różnorodności oraz złożoności szkodliwych i wrogich działań informacyjnych;
- systematycznie wzrastającym natężeniem cyberataków na systemy informacyjne i infrastrukturę informatyczną;

– powiązaniem szkodliwych i wrogich działań wobec polskiej infosfery z oddziaływaniem na infosferę innych państw UE i NATO.

Najważniejsze czynniki przyczyniające się do diametralnego przeobrażania się zewnętrznej infosfery to:

– eskalacja zagrożeń informacyjnych związanych z digitalizacją, rozwojem usług cyfrowych i nowych technologii mających wpływ na wszystkie obszary funkcjonowania społeczeństw, gospodarek i systemów bezpieczeństwa państw;
– powstawanie poważnych kryzysów oraz konflikty zbrojne i wojny, które wywołują szereg negatywnych wielosektorowych i transgranicznych skutków;
– pojawianie się kryzysów społecznych w państwach Europy Zachodniej związanych ze zmianą struktury społecznej na skutek intensywnych ruchów migracyjnych;
– wzrost globalnego oddziaływania korporacji międzynarodowych oraz państw z aspiracjami mocarstwowymi.

W takich uwarunkowaniach międzynarodowych zapewnienie bezpieczeństwa informacyjnego RP musi uwzględniać:

– wspieranie bezpieczeństwa informacyjnego i stabilności infosfery na poziomie międzynarodowym i europejskim;
– zwiększanie możliwości oraz znaczenia państwa polskiego w zakresie zapewniania bezpieczeństwa informacyjnego w wymiarze międzynarodowym;
– kształtowanie jak najlepszego stanu bezpieczeństwa informacyjnego w relacjach sojuszniczych;

– wypracowywanie i realizowanie międzynarodowych rozwiązań systemowych ukierunkowanych na ograniczanie rozprzestrzeniania się zagrożeń bezpieczeństwa informacyjnego;
– wcielanie w życie skutecznych metod działania na rzecz realizacji przyjętej strategicznej koncepcji bezpieczeństwa informacyjnego z uwzględnieniem interesów zewnętrznych RP;
– zwiększanie sprawności działania instytucji systemu bezpieczeństwa informacyjnego RP w wymiarze międzynarodowym;
– budowanie międzynarodowego konsensusu oraz platform współpracy w sprawach wzmacniania odporności na zagrożenia dla bezpieczeństwa informacyjnego.

W obszarze międzynarodowym działania na rzecz bezpieczeństwa informacyjnego bazować muszą na: wzajemnie korzystnej współpracy i interoperacyjności uwzględniającej członkostwo w UE i NATO, promowaniu i ochronie otwartej, wolnej, stabilnej i bezpiecznej infosfery, respektowaniu praw człowieka i jego godności, przestrzeganiu podstawowych wolności, zasad demokracji i praworządności.

5. System bezpieczeństwa informacyjnego RP

5.1. Ogólny kształt i cele systemu

Polska podobnie jak większość współczesnych państw w celu osiągania i utrzymywania pożądanego poziomu bezpieczeństwa informacyjnego tworzy i wykorzystuje instrumenty w postaci aktów prawnych, rozwiązań organizacyjno-instytucjonalnych oraz używa zasobów materialnych i osobowych. Całość tych składników powinna być odpowiednio skonfigurowana i skupiona w ramach systemu bezpieczeństwa informacyjnego. Zważywszy na fakt, że bezpieczeństwo informacyjne podobnie jak inne wymiary bezpieczeństwa ma dychotomiczną naturę stanu i procesu, system taki nie może być konstrukcją sztywną i zamkniętą. Architektura systemu bezpieczeństwa informacyjnego powinna zapewnić jego elastyczność, modułowość oraz kompatybilność i dobrą koordynację działań z innymi subsystemami systemu bezpieczeństwa państwa. System taki musi być także zdolny do kooperacji międzynarodowej, zwłaszcza w ramach UE i NATO. Biorąc pod uwagę transsektorowość bezpieczeństwa informacyjnego oraz konieczność zrównoważonego rozwoju państwa, system bezpie-

czeństwa informacyjnego należy ukształtować w sposób, który zagwarantuje jego skuteczność i nie będzie zawierał rozwiązań godzących w możliwości rozwojowe państwa oraz konstytucyjne prawa i wolności obywateli.

Konstrukcja systemu bezpieczeństwa informacyjnego musi uwzględniać aktualne i perspektywiczne uwarunkowania tego bezpieczeństwa, jego miejsce w polityce bezpieczeństwa i strategii bezpieczeństwa RP, a także ewentualność działania w warunkach kryzysów i stanów nadzwyczajnych. Ogólna struktura systemu bezpieczeństwa informacyjnego powinna obejmować:

– Subsystem kierowania odpowiedzialny za: współtworzenie podstaw polityki bezpieczeństwa informacyjnego, kształtowanie strategii, analizowanie ryzyk strategicznych, procesy decyzyjne oraz nadzór i kontrolę nad podporządkowanymi subsystemami wykonawczymi, a także koordynację współdziałania w ramach systemu bezpieczeństwa państwa, ocenę rodzaju i poziomu pojawiających się zagrożeń informacyjnych i decydowanie o wdrażaniu związanych z tym procedur. To również subsystem, który opracowuje i nadzoruje regularne ćwiczenia i testy subsystemów wykonawczych.

– Subsystemy wykonawcze zapewniające zdolności operacyjne w zakresie: komunikacji strategicznej, ochrony i obrony narodowej infosfery, detekcji i reagowania na negatywne zjawiska informacyjne, odtwarzania w przypadkach uszkodzeń i zniszczeń oraz budowania odporności na zagrożenia informacyjne.

Takie ukształtowanie systemu wynika z uwarunkowań bezpieczeństwa informacyjnego RP, zgromadzonych doświadczeń i funkcjonujących rozwiązań w zakresie zapewniania tego bez-

pieczeństwa. Szczególne miejsce wśród uwarunkowań zajmują agresywne działania informacyjne ze strony państw obcych. Ze względu na sojusznicze więzy Rzeczypospolitej Polskiej uwzględnić należy w ich ramach także wrogą działalność informacyjną wobec państw UE i NATO. Zagrożenia informacyjne, w tym nasilająca się presja dezinformacyjna, generują również szereg ryzyk dla wewnętrznego bezpieczeństwa RP. Powoduje to wzrost znaczenia komunikacji strategicznej, dostępu państwowych gremiów decyzyjnych oraz społeczeństwa do rzetelnej i aktualnej informacji oraz ochrony bezpieczeństwa zasobów informacyjnych na różnych poziomach. Jednym z kluczowych warunków zapewnienia bezpieczeństwa informacyjnego państwa polskiego jest dysponowanie bezpiecznymi i nowoczesnymi sieciami teleinformatycznymi, zdolnymi do sprawnego obsługiwania różnych użytkowników. Rozwój systemów bazujących na nowoczesnych technologiach stwarza w tym obszarze nowe możliwości, ale generuje także zagrożenia. Poważnym wyzwaniem jest kwestia zapewnienia bezpieczeństwa infrastruktury informacyjnej w kontekście jej zależności od produkcji energii elektrycznej. Zagwarantowanie bezpieczeństwa energetycznego jest warunkiem koniecznym dla zapewnienia bezpieczeństwa informacyjnego.

W obszarze bezpieczeństwa informacji niejawnych i tajemnic prawnie chronionych ciągłym wyzwaniem, którego rangę dodatkowo wzmacnia duża aktywność wywiadowcza nieprzyjaznych państw, jest zapewnienie wysokiej skuteczności i efektywności instrumentów nadzoru i kontroli nad tą sferą bezpieczeństwa informacyjnego. Uzasadnione staje się także rozwijanie możliwości ochronnych opartych na nowoczesnych rozwiązaniach technicz-

no-technologicznych oraz kryptograficznych. Zagrożenie dla bezpieczeństwa w obszarze informacyjnym stanowi nadmiarowość informacji, która może wywoływać wieloskalowe negatywne zjawiska szumu i smogu informacyjnego. Istotnym wyzwaniem w kontekście zapewnienia wysokiego poziomu bezpieczeństwa informacyjnego jest zagwarantowanie wolności informacyjnej obywateli jako jednego z kluczowych elementów bezpieczeństwa demokratycznego państwa.

Dążąc do utworzenia zintegrowanego systemu bezpieczeństwa informacyjnego, Polska musi zadbać o odpowiedni zakres powiązań tego systemu w ramach UE i NATO m.in. poprzez utworzenie tematycznych platform współdziałania. W działaniach podejmowanych przez państwo polskie na rzecz zapewnienia bezpieczeństwa informacyjnego widoczna jest ich sektorowość i deficyt rozwiązań ogólnosystemowych. Stan taki nie sprzyja adekwatnemu i szybkiemu reagowaniu na pojawiające się wyzwania i zagrożenia. Odpowiednie do współczesnych i perspektywicznych potrzeb ukształtowanie struktury systemu bezpieczeństwa informacyjnego oraz dobra konfiguracja jego funkcji i celów to konieczne działania, które zwiększą bezpieczeństwo Polski zarówno w sferze informacyjnej, jak i pozostałych wymiarach bezpieczeństwa. Utworzenie nowoczesnego zintegrowanego systemu bezpieczeństwa informacyjnego wymaga przeprowadzenia dobrze zaplanowanych przedsięwzięć legislacyjno-organizacyjnych i szkoleniowo-edukacyjnych oraz wydzielenia koniecznych środków i instrumentów przyporządkowanych temu systemowi. Wskazane cele i uwarunkowania definiują zadania systemu obejmujące:

– pozyskiwanie, wytwarzanie, przetwarzanie, przechowywanie oraz sprawne dystrybuowanie wysokiej jakości informacji zgodnie z potrzebami państwa;
– chronienie informacji, które zostały sklasyfikowane jako wymagające różnych form reglamentacji dostępu i ochrony;
– rozpoznawanie, zapobieganie i zwalczanie zagrożeń dla bezpieczeństwa informacyjnego w wymiarze zewnętrznym i wewnętrznym oraz zbiorowym i jednostkowym;
– zagwarantowanie bezpiecznego funkcjonowania informacyjnej infrastruktury państwa;
– zapewnienie suwerenności narodowej infosfery oraz efektywnej współpracy w dziedzinie bezpieczeństwa informacyjnego z otoczeniem międzynarodowym.

Do stworzenia systemu bezpieczeństwa informacyjnego na bazie odpowiednio skonfigurowanej ze strategicznymi celami i interesami narodowymi polityki bezpieczeństwa państwa należy wykorzystać istniejące już rozwiązania prawne i organizacyjne. Czynnikiem wzmacniającym potencjał i uwzględnionym w konstrukcji systemu stać się powinna także ścisła współpraca z partnerami z UE i NATO.

5.2. Subsystem kierowania

Aby zapewnić prawidłową konstrukcję oraz funkcjonowanie subsystemu kierowania, należy sformatować go jako zbiór powiązanych ze sobą elementów działających w celu zapewnienia ciągłości podejmowania działań władczych i kontrolnych

dla utrzymania bezpieczeństwa informacyjnego oraz właściwej współpracy z innymi subsystemami systemu bezpieczeństwa państwa. Podsystem kierowania musi być trwale i hierarchicznie powiązany z podsystemami wykonawczymi systemu bezpieczeństwa informacyjnego RP, tak aby zapewnić:

- stały nadzór i kontrolę nad podejmowanymi działaniami;
- ciągłość i skuteczność realizacji przedsięwzięć zapewniających bezpieczeństwo informacyjne zarówno w okresach względnej stabilności, jak i w sytuacjach pojawienia się zagrożeń destabilizujących sytuację w państwie;
- realizację zadań związanych z monitorowaniem źródeł, rodzajów, kierunków i skali zagrożeń informacyjnych;
- zdolność do przewidywania zagrożeń dla bezpieczeństwa informacyjnego na terytorium Rzeczypospolitej Polskiej i poza jej granicami, zapobiegania im oraz usuwania ich skutków;
- kierowanie ofensywnymi i defensywnymi działaniami w ramach walk informacyjnych;
- gotowość systemu do działań na wypadek wojny i zagrożenia wojennego z uwzględnieniem perspektywy wojny informacyjnej.

Dla zapewnienia właściwego funkcjonowania subsystemu niezbędne jest wyodrębnienie odpowiednich modułów kierowniczych i zarządczych na poziomie:

- rządowym;
- resortowym;

– jednostek podziału terytorialno-administracyjnego (województwo, gmina, powiat).

Konieczne jest także powołanie Narodowego Centrum Bezpieczeństwa Informacyjnego – organu wyposażonego w kompetencje i zasoby do sprawowania roli centrum zarządzania bezpieczeństwem informacyjnym państwa.

5.3. Subsystemy wykonawcze

Subsystemy wykonawcze systemu bezpieczeństwa informacyjnego państwa odpowiadają za realizację przyjętych w polityce oraz strategii bezpieczeństwa informacyjnego RP kierunków działań bieżących i perspektywicznych oraz zadań płynących z subsystemu kierowania. Biorąc pod uwagę potrzeby, doświadczenia oraz istniejące rozwiązania, można stwierdzić, że uzasadnione jest ukształtowanie następujących subsystemów wykonawczych systemu bezpieczeństwa informacyjnego:

– cyberbezpieczeństwa;
– wywiadowczo-kontrwywiadowczego;
– ochrony informacji niejawnych i tajemnic prawnie chronionych;
– komunikacji strategicznej i informacji publicznej;
– ochrony danych osobowych.

Subsystem cyberbezpieczeństwa

Systematyczne poszerzanie zakresu cyfryzacji różnych form działalności, w tym także funkcjonowania systemów i sieci tele-

informatycznych oraz usług świadczonych drogą elektroniczną zarówno w domenie publicznej, jak i prywatnej implikuje połączenie w jednym systemie problematyki cyberbezpieczeństwa i bezpieczeństwa teleinformatycznego. W takim kształcie za podstawową funkcję subsystemu cyberbezpieczeństwa należy uznać zapewnienie odporności systemów teleinformatycznych na działania naruszające: poufność, integralność, dostępność, autentyczność przetwarzanych danych i informacji oraz bezpieczeństwo usług oferowanych przez te systemy. Ważne jest także zagwarantowanie transferu informacji w każdej sytuacji.

Subsystem cyberbezpieczeństwa w ramach realizacji przypisanych mu zadań odpowiada za:

- dostępność, integralność i poufność danych oraz informacji przetwarzanych w systemach teleinformatycznych;
- wprowadzanie rozwiązań pozwalających na skuteczną ochronę praw i wolności informacyjnych jednostki przy zapewnieniu efektywnego wykonywania innych zadań na rzecz bezpieczeństwa informacyjnego państwa;
- zapobieganie próbom destrukcyjnego oddziaływania na infrastrukturę teleinformatyczną poprzez redukcję jej podatności;
- minimalizowanie skutków ataków na systemy teleinformatyczne oraz przywracanie w krótkim czasie pełnej ich funkcjonalności;
- ochronę systemów teleinformatycznych przed uzyskiwaniem do nich dostępu przez podmioty do tego niepowołane;

– bezpieczne funkcjonowanie systemów teleinformatycznych w sytuacjach kryzysowych oraz zagrożenia wojennego;
– warunki do budowy i eksploatacji narodowego systemu łączności satelitarnej;
– zwiększanie zdolności w zakresie kryptologii i wytwarzania urządzeń teleinformatycznych wyposażonych w moduły kryptograficzne produkowane w Polsce.

Za właściwe ukształtowanie strukturalne i funkcjonalne subsystemu cyberbezpieczeństwa powinien odpowiadać przede wszystkim minister właściwy do spraw informatyzacji we współpracy z ministrem właściwym do spraw obrony narodowej oraz zaangażowane w budowę cyfrowego wymiaru bezpieczeństwa informacyjnego RP instytucje: Urząd Komunikacji Elektronicznej, Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK) oraz Centralne Biuro Zwalczania Cyberprzestępczości (CZBC).

Subsystem wywiadowczo-kontrwywiadowczy

Ma on wieloaspektowe znaczenie dla ochrony bezpieczeństwa wewnętrznego i zewnętrznego, praw obywateli oraz porządku konstytucyjnego państwa. Niezwykle istotne w tym kontekście jest zapewnienie efektywnej cywilnej i demokratycznej kontroli nad jego działalnością w celu zapobiegania niewłaściwemu używaniu jego możliwości. Podstawowa funkcja tego subsystemu polega na uzyskiwaniu, gromadzeniu, analizowaniu, przetwarzaniu i przekazywaniu właściwym organom państwa informacji waż-

nych z punktu widzenia interesów narodowych, w tym informacji o realnych i potencjalnych zagrożeniach dla bezpieczeństwa. Działalność tego subsystemu obejmuje także kontrwywiadowczą ochronę państwa oraz wykonywanie innych specjalistycznych zadań na rzecz pozostałych subsystemów bezpieczeństwa informacyjnego. Komponent kontrwywiadowczy subsystemu jest zaangażowany w ochronę informacji niejawnych, zapewnianie bezpieczeństwa teleinformatycznego oraz koordynację i prowadzenie współpracy w roli krajowej władzy bezpieczeństwa z podmiotami zagranicznymi. W ramach tworzenia nowego kształtu subsystemu należy:

- silniej zintegrować wojskowe służby wywiadowczo-kontrwywiadowcze z resortem obrony narodowej;
- wzmocnić możliwości kontrwywiadowczej osłony organów państwowych i krytycznej infrastruktury teleinformatycznej, adekwatnie do nasilającej się aktywności wrogich podmiotów;
- rozwinąć zdolności do działań na rzecz wczesnej identyfikacji zagrożeń w infosferze;
- priorytetowo potraktować kwestię jakości i stabilności personelu agencji i służb subsystemu oraz wdrażanie najnowszych rozwiązań technicznych;
- ustanowić standardy związane z czynnościami operacyjno-rozpoznawczymi w odniesieniu do uprawnionych agencji i służb subsystemu;
- stworzyć platformę współdziałania w ramach państwowej wspólnoty informacyjnej z innymi służbami i formacjami sektora bezpieczeństwa państwa;

– ustanowić umiejscowiony na wzór NIK poza strukturami rządowymi państwowy urząd nadzorczo-kontrolny z ustawowymi uprawnieniami do kontroli i oceny merytorycznej działalności służb wywiadowczo-kontrwywiadowczych.

Elementy strukturalne subsystemu powinny być oparte na dostosowanych kompetencyjnie oraz organizacyjnie do nowych potrzeb i zadań takich podmiotów, jak Agencja Wywiadu, Służba Wywiadu Wojskowego, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego. Minister koordynator do spraw służb specjalnych powinien uzyskać status stałego, a nie fakultatywnie powoływanego członka rządu, a także mieć przypisane obowiązki i kompetencje organizatora subsystemu wywiadowczo-kontrwywiadowczego oraz dysponować odpowiednim urzędem ministerialnym.

Subsystem ochrony informacji niejawnych i tajemnic prawnie chronionych

Ochrona informacji niejawnych oraz tajemnic prawnie chronionych to jeden z najbardziej wrażliwych obszarów funkcjonowania systemu bezpieczeństwa informacyjnego. Wynika to z roli, jaką odgrywają one w różnych sferach życia państwa. Podstawowa funkcja subsystemu to zapobieganie uzyskiwaniu nieuprawnionego dostępu do informacji niejawnych i tajemnic prawnie chronionych oraz ich ujawnianiu. W ramach swoich zadań subsystem odpowiada za:

– zapewnianie personalnego, technicznego i fizycznego bezpieczeństwa informacji niejawnych oraz tajemnic prawnie chronionych;

– prowadzenie akredytacji systemów teleinformatycznych służących do przechowywania, przekazywania i przetwarzania informacji niejawnych oraz tajemnic prawnie chronionych;
– zapewnienie uprawnionym podmiotom warunków do realizacji zadań w roli krajowej władzy bezpieczeństwa;
– zapewnienie bezpieczeństwa tajemnic prawnie chronionych;
– zagwarantowanie przestrzegania tajemnic kształtujących bezpieczeństwo jednostki, które tworzy m.in. prawo do prywatności, ochrona wolności wypowiedzi czy tajemnica komunikowania się;
– zapewnienie przestrzegania tajemnic jako fundamentalnego składnika: wolności mediów informacyjnych, gwarancji uczciwych procesów sądowych, czynności urzędowych w ramach funkcjonowania zawodów zaufania publicznego oraz realizacji praw wyborczych.

Ważnym zadaniem tego subsystemu jest także formułowanie wymagań prawnych, proceduralnych, fizycznych i technicznych dotyczących przechowywania, przetwarzania i wymiany informacji niejawnych oraz innych tajemnic prawnie chronionych w taki sposób, aby skutecznie zapobiegać pojawiającym się zagrożeniom. W tym kontekście istotne znaczenie mają rozwój i implementacja narodowych rozwiązań z zakresu kryptografii.

System ochrony informacji niejawnych i tajemnic prawnie chronionych powinien zostać ukształtowany zgodnie z nowymi potrzebami, opierając się na dotychczas działających w sferze

ochrony informacji w podmiotach: ABW, SKW, kierownikach jednostek organizacyjnych, pełnomocnikach ochrony informacji niejawnych. Do systemu powinny zostać włączone odpowiednio ukształtowane ogniwa nadzorujące podmioty, które z mocy prawa zobowiązane są do ochrony informacji stanowiących tajemnice zawodowe.

Subsystem komunikacji strategicznej i informacji publicznej

Funkcjonowanie infosfery państwa zarówno w wymiarze wewnętrznym, jak i zewnętrznym wymaga prowadzenia dobrej komunikacji strategicznej, która powinna być powiązana z zapewnieniem odpowiedniego dostępu społeczeństwa do informacji publicznej. Należy podkreślić, że transparentność i rzetelność są elementami bezpieczeństwa, a nie wyłącznie polityki informacyjnej. Implikuje to połączenie w ramach wspólnego subsystemu problematyki komunikacji strategicznej oraz dostarczania informacji o charakterze publicznym z uwzględnieniem starych i nowych zagrożeń i wyzwań w tym zakresie. Komunikacja strategiczna musi być oparta na skoordynowanych działaniach informacyjnych oraz wizerunkowych wspierających realizację celów polityki państwa oraz budujących jego pozycję i wiarygodność. Informacje wytworzone przez władze publiczne i osoby pełniące funkcje publiczne oraz inne podmioty wykonujące funkcje publiczne lub gospodarujące mieniem publicznym, jak również informacje odnoszące się do wspomnianych władz, osób i innych podmiotów, niezależnie od tego, przez kogo zostały wytworzone,

powinny być publicznie dostępne z zastrzeżeniem odmowy dostępu w sytuacjach określonych prawem. Podstawowa funkcja subsystemu to budowanie bezpieczeństwa narodowej infosfery na drodze dystrybucji wysokiej jakości informacji dotyczącej działalności państwa i jego instytucji w wewnętrznej i zewnętrznej warstwie narodowej infosfery. W ramach swoich zadań subsystem powinien odpowiadać za:

- informacyjne wspieranie realizacji celów państwa, w tym priorytetów polityki bezpieczeństwa;
- kreowanie pozytywnego obrazu państwa na arenie wewnętrznej i międzynarodowej;
- odpowiedzialne zarządzanie informacją w sytuacjach kryzysowych;
- zapewnienie transparentności działania władz publicznych;
- przeciwdziałanie dezinformacji.

W przyporządkowanym obszarze funkcjonalnym subsystem powinien operować, wykorzystując różne kanały: analitykę, edukację, media publiczne, komunikację społeczną.

Ze względu na utrzymującą się presję dezinformacyjną jej zwalczaniu i przeciwdziałaniu trzeba poświęcić szczególną uwagę, ustanawiając specjalistyczne rozwiązania instytucjonalne i podejmując intensywne działania edukacyjne.

Ramy organizacyjne subsystemu przy wykorzystaniu dotychczas funkcjonujących instytucji i regulacji muszą uwzględnić:

- wdrożenie jednolitego systemu komunikacji strategicznej służącego do prognozowania, planowania i realizowania spójnych działań komunikacyjnych;

– budowę zaplecza instytucjonalnego do zwalczania i przeciwdziałania dezinformacji;
– stworzenie zdolności i procedur współpracy administracji publicznej oraz instytucji bezpieczeństwa państwa z mediami informacyjnymi;
– budowanie i pogłębianie świadomości społecznej w zakresie odpowiedniego reagowania na pojawiające się zagrożenia we współpracy z mediami informacyjnymi oraz społecznościowymi przy zaangażowaniu organizacji pozarządowych.

W wymiarze instytucjonalnym należy:
– utworzyć centralny rządowy ośrodek odpowiedzialny za komunikację strategiczną;
– usprawnić działalność i podnieść merytoryczną jakość funkcjonowania rzeczników prasowych urzędów administracji publicznej i urzędów centralnych;
– nadać odpowiedni do współczesnych potrzeb z zakresu bezpieczeństwa informacyjnego kształt organizacyjno-kompetencyjny Krajowej Radzie Radiofonii i Telewizji.

Subsystem ochrony danych osobowych

Ze względu na posługiwanie się w różnych sferach życia publicznego na coraz szerszą skalę danymi osobowymi niezbędne jest zapewnienie bezpieczeństwa tego obszaru infosfery za pomocą odpowiednio zorganizowanego subsystemu. Jego podstawowa funkcja to zapewnienie ustanawiania i zachowywania wysokich

standardów ochrony danych osobowych obywateli, dotyczących różnych sfer życia. Zadania tego subsystemu powinny być skoncentrowane na:

- zagwarantowaniu pełnego poszanowania praw obywateli w zakresie ochrony danych ich dotyczących;
- reagowaniu na wszelkie przypadki naruszeń prawa i dobrych praktyk w zakresie ochrony danych osobowych;
- stosowaniu najnowocześniejszych technicznych środków bezpieczeństwa, zapewniających skuteczną ochronę danych osobowych;
- zapewnieniu zgodności z prawem europejskim rozwiązań w zakresie przechowywania danych telekomunikacyjnych;
- zapewnieniu realnej kontroli obywateli nad danymi ich dotyczącymi;
- szczególnej ochronie danych osób małoletnich;
- tworzeniu standardów ochrony danych osobowych w kontekście rozwoju zastosowań sztucznej inteligencji;
- prowadzeniu systematycznej oceny ryzyka w zakresie ochrony danych osobowych;
- inspirowaniu i wspieraniu merytorycznym szkoleń dotyczących ochrony danych osobowych na różnych poziomach.

W strukturze systemu należy odpowiednio umocować: Prezesa Urzędu Ochrony Danych Osobowych, inspektorów ochrony danych, administratorów danych osobowych, podmioty przetwarzające, administratorów systemów informatycznych, osoby

upoważnione do przetwarzania danych osobowych, właścicieli procesu przetwarzania danych osobowych.

Kluczowa dla systemu jest obecność silnego i niezależnego centralnego organu ochrony danych osobowych egzekwującego obowiązujące przepisy prawne, wykorzystującego do tego celu podległy mu urząd. Działania tego organu powinny być wzmocnione w zakresie kompetencji kontrolnych przez powołanie jego delegatur regionalnych oraz wprowadzenie cyklicznych obowiązkowych audytów ochrony danych w sektorach wysokiego ryzyka (ochrona zdrowia, edukacja, finanse, usługi publiczne). W działalność subsystemu powinny być włączone także wyspecjalizowane, mające odpowiedni dorobek organizacje społeczne, które pełniłyby funkcję adwokatów interesu publicznego. System ochrony danych osobowych należy ukształtować i utrzymywać jako kompleksowy zestaw struktur organizacyjnych, procedur i technologii zgodnych z regulacjami UE, zdolny do pełnego zabezpieczenia danych osobowych przed nieuprawnionym dostępem, utratą lub kradzieżą. Subsystem powinien zapewnić wdrażanie środków technicznych i organizacyjnych, gwarantujących poufność i rozliczalność danych osobowych stosownie do pojawiających się możliwości i konieczności odpowiadania na nowe wyzwania i zagrożenia.

System bezpieczeństwa informacyjnego jako całość oraz jego poszczególne podsystemy w celu skutecznego wypełniania swoich funkcji oprócz odpowiednio ukształtowanej struktury organizacyjnej musi dysponować zestawem zasobów oraz instrumentów. Konstrukcja systemu bezpieczeństwa informacyjnego powinna uwzględniać nadanie mu zdolności do prowadzenia działań o róż-

nej skali i charakterze. Musi on mieć możliwości mobilizacyjne oraz organizacyjno-prawne, które pozwolą na sprawne przechodzenie z funkcjonowania w warunkach stabilnych na tryb działań właściwy dla stanów kryzysowych czy nadzwyczajnych.

Zakończenie

Środowisko bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej jest dynamiczne, wielowymiarowe, ma też określone podatności na negatywne oddziaływania zewnętrzne i wewnętrzne. Wyznacza to w istotny sposób kierunki myślenia strategicznego, wektory polityki bezpieczeństwa informacyjnego oraz zasady i cele rekonstrukcji systemu bezpieczeństwa informacyjnego z podkreśleniem konieczności jego trwałego umiejscowienia jako jednego z subsystemów wykonawczych systemu bezpieczeństwa RP.

Przedstawiony projekt Strategii Bezpieczeństwa Informacyjnego Rzeczypospolitej Polskiej powstał w wyniku dostrzeżenia luki w systemie dokumentów strategicznych z zakresu bezpieczeństwa. Jego celem jest stworzenie podstawy do wzmocnienia zdolności państwa polskiego w zakresie przeciwdziałania zagrożeniom i podejmowania wyzwań wynikających z obecnego oraz perspektywicznego kształtu uwarunkowań bezpieczeństwa informacyjnego.

Strategia w sposób kompleksowy określa zakres i kierunki kształtowania bezpieczeństwa informacyjnego RP, uwzględniając podmiotowe i przedmiotowe aspekty bezpieczeństwa. Interesy narodowe oraz cele strategiczne w dziedzinie bezpieczeństwa

informacyjnego zostały sformułowane w zgodzie z pryncypiami ustrojowymi określonymi w Konstytucji Rzeczypospolitej Polskiej oraz polską racją stanu. Strategia uwzględnia konteksty związane z członkostwem Polski w UE i NATO. Zawarte w projekcie Strategii syntetyczne i ogólne propozycje działań powinny znaleźć rozwinięcie i odzwierciedlenie w innych dokumentach strategicznych dotyczących bezpieczeństwa RP.

Całościowe ujmowanie wielu dziedzin i obszarów funkcjonowania państwa związanych z różnymi aspektami bezpieczeństwa informacyjnego wymaga stosowania adekwatnych do współczesnych potrzeb i nacechowanych precyzją definicji oraz charakterystyk podstawowych pojęć i jednakowego ich rozumienia. Jest to niezbędne, aby uniknąć interpretacyjnych błędów, mogących generować sprzeczności w teorii i praktyce strategicznej.

Projekt Strategii łączy ugruntowane oraz te mające nowatorski charakter ustalenia naukowe z doświadczeniami praktycznymi, z których wynika konieczność posługiwania się Strategią Bezpieczeństwa Informacyjnego jako specjalistycznym dokumentem strategicznym opartym na teoretycznej i praktycznej komplementarności bezpieczeństwa informacyjnego z innymi wymiarami bezpieczeństwa państwa. Treści Strategii pokazują, że bezpieczeństwo informacyjne – wraz z jego ciągle zyskującym na znaczeniu wymiarem cyfrowym – jest jednym z najbardziej wrażliwych obszarów bezpieczeństwa RP. Jego transsektorowy charakter wpływający na efektywność funkcjonowania systemu bezpieczeństwa państwa rodzi konieczność nadania systemowi bezpieczeństwa informacyjnego odpowiedniego do potrzeb kształtu oraz stosownej rangi w ramach systemu bezpieczeństwa państwa. Strategia

podkreśla, że działania na rzecz bezpieczeństwa informacyjnego muszą być podejmowane z uwzględnieniem przestrzegania praw człowieka i obywatela, w tym poszanowania prawa do wolności informacyjnej jednostki oraz ochrony jej prywatności.


OBB
Ośrodek Badań
Bezpieczeństwa
Informacyjnego


WYDAWNICTWO NAUKOWE
COLLEGIUM BOBOLANUM