Beata ZYCHOWICZ

Wojskowa Akademia Techniczna, Warszawa
Wydział Cybernetyki
beata.zychowicz@wat.edu.pl

Wymagania krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych międzynarodowych NATO, UE, ESA w Siłach Zbrojnych Rzeczypospolitej Polskiej

Requirements of the national security authority regarding protection of international classified information of NATO, EU, ESA in the Armed Forces of the Republic of Poland

Abstrakt: W artykule poddano analizie wymagania krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych Organizacji Traktatu Północnoatlantyckiego (NATO), Unii Europejskiej (UE) oraz Europejskiej Agencji Kosmicznej (ESA) w Siłach Zbrojnych Rzeczypospolitej Polskiej. Systemowe podejście do badanego obszaru wymagało charakterystyki podstaw prawnych. Przedstawiono rolę i zadania krajowej władzy bezpieczeństwa jako instytucji odpowiedzialnej za nadzór i funkcjonowanie systemu ochrony informacji niejawnych międzynarodowych. Rozważano kwestie odnoszące się do szeroko rozumianej polityki bezpieczeństwa jako podstawy do posiadania możliwości przetwarzania informacji niejawnych międzynarodowych na terenie RP. W pracy udowodniono, że istotnym elementem w ochronie informacji niejawnych NATO, UE, ESA jest proceduralne przestrzeganie zasad postępowania z informacjami niejawnymi międzynarodowymi, z uwzględnieniem zastosowanych środków zabezpieczeń fizycznych, technicznych i organizacyjnych w zgodzie z przepisami prawnymi obowiązującymi w naszym kraju.
Słowa kluczowe: krajowa władza bezpieczeństwa, ochrona, informacja niejawna międzynarodowa

Abstract: The article uses empirical research methods and analyses the requirements of the national security authority in the field of protection of classified information of the North Atlantic Treaty Organization (NATO), the European Union (EU) and the European Space Agency (ESA) in the Armed Forces of the Republic of Poland. The systemic approach to the studied area required the characteristics of the legal basis. The role and tasks of the National Security Authority as an institution responsible for supervision and functioning of the system of protection of international classified information are presented. Issues related to the broadly understood security policy as the basis for having the ability to process international classified information within the territory of the Republic of Poland were considered. The paper proves that an important element in the protection of NATO, EU and ESA classified information is the procedural observance of the rules of handling international classified information, taking into account the physical, technical and organizational security measures applied in accordance with the legal regulations in force in our country.
Keywords: National Security Authority, protection, international classified information

Wprowadzenie

Współczesne systemy bezpieczeństwa są nieustannie doskonalone stosownie do zmieniających się uwarunkowań środowiska bezpieczeństwa państw, regionów oraz świata. Waga problemu dostrzegana przez społeczność międzynarodową jest najważniejszą przyczyną akceptacji potrzeby współpracy pomiędzy państwami, które dążą do zapewnienia możliwie największego poziomu bezpieczeństwa narodowego. Toteż po ocenach wieloletnich doświadczeń za zasadne uznano zastosowanie podejścia systemowego w odniesieniu do bezpieczeństwa. Można zakładać, iż u podstaw takiej oceny znalazły się wymagania szeroko rozbudowanych struktur oraz znacznych obszarów działania, które wymagają racjonalnych rozwiązań, czytelnych oraz sprawnych relacji i otwartości na zmiany. Takie wymagania stawiane są głównie przed organizacjami zapewniającymi bezpieczeństwo o zasięgu międzynarodowym. Aby w pełni realizować zadania związane z bezpieczeństwem oraz interesem kraju, powstał zintegrowany system bezpieczeństwa narodowego. Jego częścią jest system ochrony państwa, który współpracuje z systemami bezpieczeństwa sojuszników. Polski system obronności jest oparty na polskich przepisach prawnych, ale również na ustaleniach, które wynikają z traktatów i umów międzynarodowych. Aby prawidłowo wykonywać swoje zadania, system obronny musi być tak zorganizowany, by posiadał zdolność do ochrony, obrony i odstraszania[1]. W pracy przedstawiono wymagania, jakie każda jednostka organizacyjna musi spełniać, aby realizować zadania związane z dostępem do informacji niejawnych międzynarodowych NATO, UE, ESA.

Siły Zbrojne Rzeczypospolitej Polskiej służą ochronie niepodległości państwa i niepodzielności jego terytorium. Zapewniają bezpieczeństwo i nienaruszalność granic. Jako podstawowy element systemu obronnego państwa uczestniczą w realizacji polityki bezpieczeństwa i obronnej, utrzymują gotowość do realizacji trzech rodzajów misji:

- obrona państwa i przeciwstawienie się agresji w ramach zobowiązań sojuszniczych (tj. utrzymania zdolności użycia wojsk w zakresie obrony i ochrony nienaruszalności granic RP, a także w działaniach antyterrorystycznych oraz w rozwiązywaniu lokalnego lub regionalnego konfliktu zbrojnego, jak również w operacji obronnej – w kraju, jak i poza nim);
- udział w procesie stabilizacji sytuacji międzynarodowej oraz w operacjach reagowania kryzysowego i humanitarnych (tj. utrzymanie sił i zdolności do uczestniczenia w operacjach pokojowych i reagowania kryzysowego prowadzonych

[1] R. Wróblewski, H. Wyrębek (red.), *Determinanty bezpieczeństwa militarnego*, wyd. UPH w Siedlcach, Siedlce 2016, s. 16.

przez NATO, UE, jak również w innych operacjach wynikających z porozumień międzynarodowych oraz w operacjach humanitarnych prowadzonych przez organizacje międzynarodowe, rządowe i inne);

- wspieranie bezpieczeństwa wewnętrznego i pomoc społeczeństwu (poprzez m.in. ochronę przestrzeni powietrznej oraz wsparcie ochrony granicy lądowej i wód terytorialnych, prowadzenie działalności rozpoznawczej i wywiadowczej, a także: monitorowanie skażeń promieniotwórczych, chemicznych i biologicznych na terytorium kraju; oczyszczanie terenu z materiałów wybuchowych i przedmiotów niebezpiecznych pochodzenia wojskowego, prowadzenie działań poszukiwawczo-ratowniczych, pomoc władzom państwowym, administracji publicznej oraz społeczeństwu w reagowaniu na zagrożenia, którym przeciwdziałanie przekracza możliwości służb cywilnych)[2].

We współczesnych czasach coraz silniejszego znaczenia nabiera ochrona informacji, a przede wszystkim informacji niejawnych. To, że żyjemy i funkcjonujemy w erze informacyjnej, nikogo już nie dziwi. Nie jest również tajemnicą, że informacja ma ogromne znaczenie i wartość. Jest ona obszarem zainteresowania wszelkich podmiotów[3]. Jedną z charakterystycznych cech współczesnej cywilizacji jest wzrost roli i znaczenia informacji w codziennym życiu, będącym świadectwem rewolucji informatycznej i powstania społeczeństwa informacyjnego. Takiego, w którym informacja stała się produktem, a jej znajomość – bogactwem. Nabrała ona strategicznego charakteru, będąc istotnym czynnikiem rozwoju cywilizacyjnego. Wykorzystana jest do sterowania procesami społecznymi i decyduje o sile i bezpieczeństwie państwa oraz jego obywateli[4].

Podstawą prawną systemu ochrony informacji niejawnych w Polsce jest Konstytucja RP, w której, w rozdziale *Wolność i prawa osobiste*, w art. 54 ust. 1 zapisano: „Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji". Wyrażono w ten sposób wolę społeczeństwa, aby stworzony porządek prawny, szanujący wolność człowieka, respektował także jego prawa do zdobywania, przekazywania, przetwarzania czy odtwarzania informacji .

Bezpieczeństwo informacyjne, w tym ochrona informacji niejawnych, o których mowa w *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 2014 r., to jeden z najważniejszych obszarów funkcjonowania systemu bezpieczeństwa państwa. Strategiczne zadania w tym zakresie obejmują: zapewnienie bezpieczeństwa informacyjnego

[2] http://www.wojsko-polskie.pl/pl/pages/siy-zbrojne-rp-2016-04-18-j/ (14.03.2019)
[3] S. Topolewski, P. Żarkowski, *Ochrona informacji niejawnych i danych osobowych. Wymiar teoretyczny i praktyczny*, wyd. UPH w Siedlcach, Siedlce 2014, s. 47.
[4] S. Topolewski, *Ochrona informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Wyd. UPH w Siedlcach, Siedlce 2017, s. 9.

państwa poprzez zapobieganie uzyskaniu nieuprawnionego dostępu do informacji niejawnych i ich ujawnieniu; zapewnianie personalnego, technicznego i fizycznego bezpieczeństwa informacji niejawnych; akredytację systemów teleinformatycznych służących przetwarzaniu tych informacji; zapewnienie realizacji funkcji krajowej władzy bezpieczeństwa w celu umożliwienia międzynarodowej wymiany informacji niejawnych[5].

Informacje niejawne są specyficznym zasobem chronionych ze względu na interesy państwa. Specyfikę tę określa po pierwsze przedmiot ochrony, a więc informacje, których nieuprawnione ujawnienie mogłoby narazić państwo na określone szkody. Te zaś oceniane są w relacji do interesów państwa w dziedzinie bezpieczeństwa. Nietrudno zauważyć, że w dobie zmian pozycji i roli państwa, zarówno międzynarodowej, jak też jako regulatora wewnętrznych stosunków, sposób interpretacji tych interesów jest uzależniony od przyjęcia określonej perspektywy politycznej. Po drugie, specyfikę ochrony informacji niejawnych określa zakres ich przetwarzania oraz metodyka ochrony oparta na normach prawa krajowego, pozostających w relacji odpowiedzialności do względnie uniwersalnych, międzynarodowych norm zarządzania bezpieczeństwem informacji, a w warunkach polskich także norm Organizacji Traktatu Północnoatlantyckiego, które określają minimalne standardy bezpieczeństwa[6].

Uwarunkowania prawne ochrony informacji niejawnych.

Głównym aktem prawnym, określającym zasady i organizację systemu ochrony informacji niejawnych w Polsce, jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Zgodnie z treścią art. 1 ust. 1 ustawy informacje niejawne są to informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażenia, to jest zasady[7]:

- klasyfikowania informacji niejawnych;
- organizowania ochrony informacji niejawnych;
- przetwarzania informacji niejawnych;
- postępowania sprawdzającego prowadzonego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy;

[5] pkt 85, *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2014.
[6] S. Zalewski, *Informacje niejawne we współczesnym państwie*, wyd. Editions Spotkania, Warszawa 2017, s. 7.
[7] S. Topolewski, *Ochrona informacji niejawnych*…, op. cit., s. 269-270.

- postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych
- organizacji kontroli stanu zabezpieczenia informacji niejawnych;
- ochrony informacji w systemach teleinformatycznych;
- stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.

Ustawa o ochronie informacji niejawnych wprowadziła poziom zabezpieczeń informacji porównywalny do stosowanego przez państwa członkowskie NATO[8]. System ochrony informacji niejawnych obejmuje zasady przetwarzania informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi, w tym takich organizacji jak: Organizacja Traktatu Północnoatlantyckiego (NATO), Unia Europejska (UE) czy Europejska Agencja Kosmiczna (ESA).

W tabeli 1 przedstawiono porównywalne klauzule tajności dla Polski, NATO, UE, ESA oraz ich potencjalny skutek ujawnienia.

Tabela 1. Przykładowe klauzule tajności oraz ich potencjalny skutek ujawnienia

KRAJOWE	NATO	UE	ESA	POTENCJALNY SKUTEK UJAWNIENIA
ŚCIŚLE TAJNE	COSMIC TOP SECRET	TRÈS SECRET UE/ EU TOP SECRET	ESA TOP SECRET	WYJĄTKOWO POWAŻNA SZKODA
TAJNE	NATO SECRET	SECRET UE/ EU SECRET	ESA SECRET	POWAŻNA SZKODA
POUFNE	NATO CONFIDENTIAL	CONFIDENTIEL UE/ EU CONFIDENTIAL	ESA CONFIDENTIAL	SZKODA
ZASTRZEŻONE	NATO RESTRICTED	RESTREINT UE/ EU RESTRICTED	ESA RESTRICTED	RP - SZKODLIWY WPŁYW NA WYKONYWANIE ZADAŃ PRZEZ ORGANY WŁADZY LUB INNE JEDNOSTKI ORG. NATO, UE, ESA - NIEKORZYSTNE DLA INTERESÓW

Źródło: opracowanie własne

[8] Art. 1 ust. 1 Ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r.

Informacje niejawne międzynarodowe są to informacje pochodzące od podmiotów zagranicznych lub wytworzone w ich interesie, które na podstawie zobowiązań przyjętych przez Rzeczpospolitą Polską wymagają ochrony przed nieuprawnionym dostępem lub ujawnieniem na poziomie jednoznacznie wskazanym poprzez odwołanie się do klauzul tajności obowiązujących w Rzeczpospolitej Polskiej.

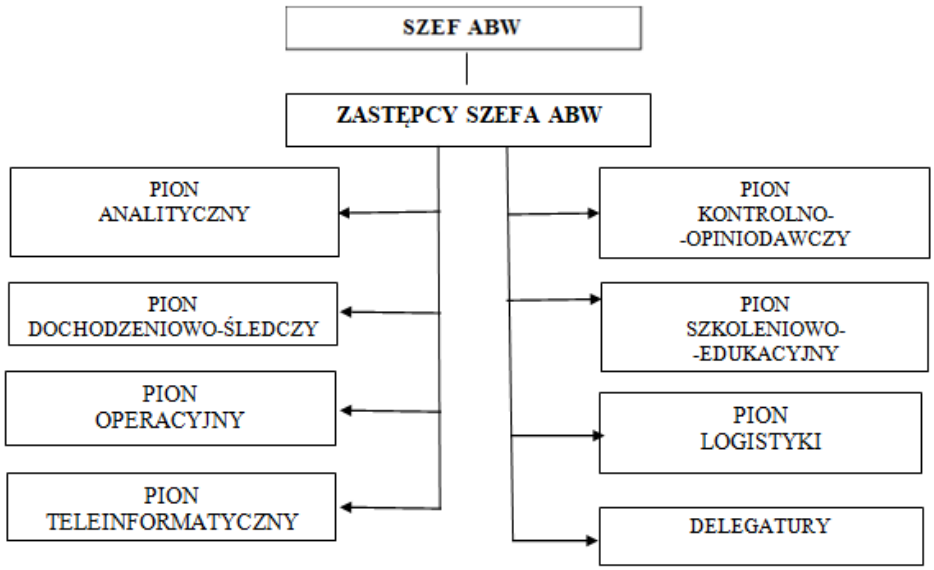
Formalnoprawne uwarunkowania organizacji i funkcjonowania Agencji Bezpieczeństwa Wewnętrznego

Agencja Bezpieczeństwa Wewnętrznego jest służbą właściwą w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Status, obowiązki i uprawnienia ABW określa Ustawa z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; realizuje działania analityczno-informacyjne, operacyjno-rozpoznawcze i procesowe, a także uczestniczy w procedurach opiniodawczych oraz prowadzi czynności w ramach systemu ochrony informacji niejawnych. Na rys. 2 przedstawiono uproszczony schemat organizacyjny.

Prawidłowe funkcjonowanie sytemu ochrony informacji niejawnych nadzoruje Szef Agencji Bezpieczeństwa Wewnętrznego, pełniący funkcję Krajowej Władzy Bezpieczeństwa określoną w przepisach międzynarodowych funkcją National Security Authority. Do jego głównych zadań należy:

- wdrożenie standardów bezpieczeństwa NATO, UE i ESA;
- zapewnienie właściwego poziomu ochrony informacji niejawnych NATO, UE i ESA;
- nadzorowanie systemu ochrony informacji niejawnych w stosunkach RP z innymi państwami lub organizacjami międzynarodowymi;
- współpraca ze strukturami bezpieczeństwa NATO, UE i ESA oraz krajowych władz bezpieczeństwa państw członkowskich.

W celu realizacji funkcji KWB, a w szczególności w celu zapewnienia prawidłowości ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami i organizacjami międzynarodowymi, zapewnienia jednolitości systemu ochrony informacji niejawnych międzynarodowych i jego zgodności z przepisami międzynarodowymi, zapewnienia wsparcia merytorycznego dla wszystkich jednostek organizacyjnych przetwarzających informacje niejawne międzynarodowe w postaci sprawdzonych i skutecznych metod oraz procedur zapewniających ich ochronę, Szef ABW, w dniu 31 grudnia 2010 r. podpisał *Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi.*



Źródło: na podstawie, https://docplayer.pl/3448390-Agencja-bezpieczenstwa-wewnetrznego-raport-z-dzialalnosci-agencji-bezpieczenstwa-wewnetrznego-w-2014-r.html

Rysunek 1. Uproszczony schemat organizacyjny ABW

Do ważniejszych zadań ABW należy:

- rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz w jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję RP, jej niepodległość i nienaruszalność terytorium, a także w system obronny;
- rozpoznawanie, zapobieganie oraz wykrywanie przestępstw, a w szczególności identyfikacja szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa;
- identyfikacja działań naruszających podstawy ekonomiczne i bezpieczeństwo państwa, w tym identyfikacja działalności korupcyjnej osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz.U. z 2017 r. poz. 1393);
- monitorowanie i kontrolowanie procesów produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa; rozpoznawanie, wykrywanie i zapobieganie nielegalnemu wytwarzaniu, posiadaniu

i obrotowi bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi w obrocie międzynarodowym;

- rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej;
- realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji Krajowej Władzy Bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych;
- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego;
- podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych[9].

W ramach współpracy międzynarodowej Polska zapewnia jednolity stopień bezpieczeństwa informacji niejawnych, które są wymieniane z zagranicznymi partnerami. Wymóg ten gwarantują umowy dwustronne oraz regulacje organizacji międzynarodowych, których RP jest członkiem.

Szef ABW, pełniąc funkcję krajowej władzy bezpieczeństwa w stosunkach międzynarodowych, odpowiada za wdrażanie uzgodnionych zasad i środków ochrony informacji niejawnych. W sferze wojskowej funkcję w tym zakresie Szef ABW realizuje za pośrednictwem Szefa SKW jako National Distribution Authority[10].

Współdziałanie w obszarze udzielania Szefowi ABW przez Szefa SKW informacji niezbędnych do pełnienia funkcji krajowej władzy bezpieczeństwa obejmuje:

- informowanie o prowadzonych procedurach i procesach określonych w przepisach dotyczących ochrony informacji niejawnych międzynarodowych;

[9] Art. 5 ust. 1 Ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu z dnia 24 maja 2002 r.

[10] https://docplayer.pl/3448390-Agencja-bezpieczenstwa-wewnetrznego-raport-z-dzialalnosci-agencji-bezpieczenstwa-wewnetrznego-w-2014-r.html (19.02.2019).

- przekazywanie informacji dotyczących organizacji i stanu systemu ochrony informacji niejawnych międzynarodowych oraz działań planowanych i podejmowanych w celu zapewnienia prawidłowości jego funkcjonowania;
- informowanie o wpływie oraz prowadzeniu korespondencji, której treść posiada istotne znaczenie dla zapewnienia prawidłowego nadzoru nad systemem ochrony informacji niejawnych międzynarodowych;
- bezzwłoczne informowanie o istotnych incydentach bezpieczeństwa teleinformatycznego, w systemach teleinformatycznych, w których przetwarzane są informacje niejawne międzynarodowe, w tym o incydentach mających znamiona ataku cyberterrorystycznego;
- przekazywanie danych koniecznych do wypełniania zadań informacyjnych, ewidencyjnych i analitycznych;
- udostępnianie sprawozdań, raportów, notatek lub innych dokumentów o tym charakterze w zakresie, w jakim zawierają wyniki czynności nadzorczych, wyjaśniających i innych opisujących stan systemu ochrony informacji niejawnych międzynarodowych;
- relacjonują udział w pracach zespołów, grup, komitetów i innych spotkań poświęconych ochronie informacji niejawnych międzynarodowych[11].

Szef ABW sprawuje nadzór nad systemem ochrony informacji niejawnych, rozumiany jako upoważnienie do określenia kierunków polskiej polityki bezpieczeństwa w zakresie ochrony informacji niejawnych międzynarodowych, wytycznych w sprawie wdrażania tej polityki, stwierdzania, czy zastosowane środki ochrony informacji niejawnych międzynarodowych spełniają wymagane dla nich kryteria oraz występowania w tych sprawach przed właściwymi organami organizacji międzynarodowych.

Bezpieczeństwo informacji niejawnych NATO

Wymiana informacji niejawnych pomiędzy RP a NATO unormowana jest w Umowie między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzonej w Brukseli dnia 6 marca 1997 r. (Dz.U. z 2000 r. nr 64, poz. 740) oraz Umową między Stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych, sporządzoną w Paryżu dnia 18 czerwca 1964 r. (Dz.U. z 2011 r. nr 143, poz. 1594). Odpowiedzialnym za zastosowanie przez NATO postanowień

[11] Pkt 62 *Wytycznych w sprawie postępowania z informacjami niejawnymi międzynarodowym* z dnia 31.12.2010 r.

umowy jest Sekretarz Generalny. Umowa w żaden sposób nie zabrania stronom zawierania innych umów w sprawie wymiany informacji niejawnych.

Przepisy bezpieczeństwa NATO uregulowane są w dokumencie C-M(2002)49 z dnia 17 czerwca 2002 r. Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego oraz dyrektywach wykonawczych:

AC/35-D/2000 – Dyrektywa Bezpieczeństwa Osobowego,
AC/35-D/2001 – Dyrektywa Bezpieczeństwa Fizycznego,
AC/35-D/2002 – Dyrektywa Bezpieczeństwa Obiegu Informacji,
AC/35-D/2003 – Dyrektywa Bezpieczeństwa Przemysłowego,
AC/35-D/2004 – Dyrektywa podstawowa INFOSEC,
AC/35-D/2005 – Dyrektywa zarządzania INFOSEC w systemach teleinformatycznych (CIS)[12].

Standardy natowskie zawierają podstawowe zasady:

- zagwarantowanie jednolitego stopnia ochrony informacji niejawnych wymienianych pomiędzy stronami;
- zasada ograniczonego dostępu;
- obligatoryjne zarządzanie ryzykiem dla instytucji NATO;
- wspólny zestaw środków bezpieczeństwa;
- procedura reakcji na stwierdzone nieprawidłowości;
- przekazywanie informacji niejawnych w ramach NATO;
- kontrola wytwórcy nad informacjami przekazanymi;
- udostępnianie informacji poza NATO tym państwom, które zapewniają odpowiedni poziom ochrony.

Informacja niejawna w NATO oznacza informację lub materiał, który został oznaczony, wymagający ochrony przed nieupoważnionym ujawnieniem. Bezpieczeństwo obiegu informacji obejmuje stosowanie ogólnych środków ochrony i procedur w celu zapobiegania, wykrywania i likwidowania negatywnych skutków utraty lub narażenia na szwank bezpieczeństwa informacji[13].

Klauzule tajności w NATO:

- COSMIC TOP SECRET (odpowiednik polski: ŚCIŚLE TAJNE);
- NATO SECRET (odpowiednik polski: TAJNE);
- NATO CONFIDENTIAL (odpowiednik polski: POUFNE);

[12] B. Iwaszko, *Ochrona informacji niejawnych w praktyce*, wyd. PRESSCOM, Wrocław 2012, s. 193.
[13] S. Zalewski, *Informacje niejawne*…, op. cit., s. 37-38.

– NATO RESTRICTED (odpowiednik polski: ZASTRZEŻONE)[14].

Warunkiem koniecznym dopuszczenia do dostępu do informacji niejawnych międzynarodowych NATO jest posiadanie poświadczenia bezpieczeństwa wydanego przez ABW lub SKW, zgodnie z właściwością ustawową.

Dla informacji niejawnych krajowych, NATO, UE i ESA tworzy się odrębne systemy ochrony przewidziane dla każdego rodzaju informacji niejawnych.

Podstawowe zasady i minimalne normy bezpieczeństwa służące ochronie informacji niejawnych Unii Europejskiej (UE)

Przepisy bezpieczeństwa Unii Europejskiej uregulowane są w Decyzji Rady Unii Europejskiej (2001/264/EC) z dnia 19 marca 2001 r. oraz Decyzji Komisji Europejskiej (2001/844/EC) z dnia 29 listopada 2001 r.

W Radzie Unii Europejskiej, jako głównym organie posiadającym inicjatywę legislacyjną UE, za bezpieczeństwo informacji odpowiadają:

- Sekretarz Generalny/Wysoki Przedstawiciel ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa (WPZiB);
- Komitet Rady ds. Bezpieczeństwa;
- Biuro ds. Bezpieczeństwa Sekretariatu Generalnego Rady;
- zdecentralizowane agencje UE.

Podstawowe zasady i minimalne normy bezpieczeństwa mają zastosowanie do Rady i Sekretariatu Generalnego Rady oraz przestrzegane są przez państwa członkowskie zgodnie z ich krajowymi przepisami ustawowymi i wykonawczymi, tak aby każda ze stron mogła mieć pewność, że zagwarantowany został równoważny poziom ochrony informacji niejawnych UE. Organ ds. zabezpieczania informacji odpowiada za:

- opracowywanie polityki bezpieczeństwa i wytycznych dotyczących bezpieczeństwa w zakresie zabezpieczania informacji oraz za monitorowanie ich skuteczności i adekwatności;
- zabezpieczanie informacji technicznych związanych z produktami kryptograficznymi i zarządzanie tymi informacjami;
- zapewnianie, by środki zabezpieczania informacji wybrane do ochrony informacji niejawnych Unii Europejskiej były zgodne z odpowiednimi politykami dotyczącymi kryteriów ich przydatności i wyboru;

[14] https://bip.abw.gov.pl/bip/informacje-niejawne-1/ochrona-informacji (12.03.2019).

- zapewnianie, by wybór produktów kryptograficznych następował zgodnie z politykami dotyczącymi kryteriów ich przydatności i wyboru;
- koordynowanie szkoleń i upowszechnianie wiedzy na temat zabezpieczania informacji;
- konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w związku z polityką bezpieczeństwa i wytycznymi dotyczącymi bezpieczeństwa w zakresie zabezpieczania informacji;
- zapewnianie odpowiedniej wiedzy fachowej na temat zabezpieczania informacji w podgrupie eksperckiej Komitetu ds. Bezpieczeństwa.

Z decyzji wynika, że Sekretarz Generalny Rady jest zobowiązany do podjęcia odpowiednich środków w celu zapewnienia tego, aby przepisy bezpieczeństwa Rady były przestrzegane w toku pracy z informacjami klasyfikowanymi Unii Europejskiej w ramach Sekretariatu Generalnego Rady przez urzędników i jego innych pracowników, zewnętrznych kontrahentów oraz osoby delegowane do pracy w Sekretariacie Generalnym Rady, a także w obiektach i zdecentralizowanych agencjach UE. Państwa członkowskie są zobowiązane do podjęcia odpowiednich środków, zgodnie z rozwiązaniami krajowymi, w celu zapewnienia tego, aby przepisy bezpieczeństwa Rady były przestrzegane w toku pracy z informacjami klasyfikowanymi UE w ramach ich służb i obiektów.

Zarządzanie informacjami niejawnymi polega na stosowaniu środków administracyjnych służących kontroli informacji niejawnych UE na wszystkich etapach ich cyklu życia, co pomaga w powstrzymywaniu od zamierzonego lub przypadkowego narażenia na szwank bezpieczeństwa tych informacji lub ich utraty i w wykrywaniu takich przypadków. Środki takie dotyczą w szczególności wytwarzania, rejestracji, kopiowania, tłumaczenia, obniżania klauzuli tajności i znoszenia tej klauzuli, przemieszczania i niszczenia informacji niejawnych. W państwach członkowskich wyznacza się kancelarię tajną, będącą głównym organem otrzymującym i przesyłającym informacje niejawne.

Informacje niejawne UE oznaczają wszelkie informacje lub materiały objęte klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby w różnym stopniu wyrządzić szkodę interesom Unii Europejskiej lub interesom co najmniej jednego państwa członkowskiego. Informacje niejawne Unii Europejskiej otrzymują jedną z następujących klauzul tajności:

– TRÈS SECRET UE/EU TOP SECRET:
  informacje i materiały, których nieuprawnione ujawnienie mogłoby wyrządzić wyjątkowo poważną szkodę podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;

– SECRET UE/EU SECRET:
  informacje i materiały, których nieuprawnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;
– CONFIDENTIEL UE/EU CONFIDENTIAL:
  informacje i materiały, których nieuprawnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;
– RESTREINT UE/EU RESTRICTED:
  informacje i materiały, których nieuprawnione ujawnienie mogłoby być niekorzystne dla interesów Unii Europejskiej lub co najmniej jednego państwa członkowskiego.

Skrócone oznaczenia klauzul tajności:

– TRÈS SECRET UE/EU TOP SECRET, TS-UE/EU-TS ;
– SECRET UE/EU SECRET, S-UE/EU-S;
– CONFIDENTIEL UE/EU CONFIDENTIAL, C-UE/EU-C;
– RESTREINT UE/EU RESTRICTED, R-UE/EU-R.

Właściwe organy zapewniają, by informacjom niejawnym UE nadawano odpowiednie klauzule tajności, by informacje takie były wyraźnie oznaczone jako informacje niejawne, a także by były one objęte danym poziomem klauzuli tajności nie dłużej niż jest to konieczne.

Bezpieczeństwo osobowe oznacza stosowanie środków zapewniających, aby dostęp do informacji niejawnych UE był przyznawany tylko osobom, które:

- spełniają zasadę ograniczonego dostępu,
- w stosownych przypadkach zostały odpowiednio sprawdzone do celów dostępu do informacji o odpowiedniej klauzuli tajności,
- zostały poinformowane o swoich obowiązkach.

Procedury prowadzenia postępowań sprawdzających mają na celu stwierdzenie, czy daną osobę, ze względu na jej lojalność, wiarygodność i rzetelność, można uprawnić do dostępu do informacji niejawnych UE.

Bezpieczeństwo fizyczne oznacza stosowanie fizycznych i technicznych środków ochrony, aby zapobiec nieuprawnionemu dostępowi do informacji niejawnych UE. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie wtargnięciu osoby nieupoważnionej, w sposób niezauważony lub z użyciem siły, powstrzymanie od podjęcia nieuprawnionych działań, udaremnienie ich i wykrycie oraz umożliwienie podziału pracowników pod względem dostępu do informacji niejawnych UE zgodnie z zasadą

ograniczonego dostępu. Środkami bezpieczeństwa fizycznego objęte są wszystkie obiekty, budynki, biura, pomieszczenia i inne strefy, w których są wykorzystywane lub przechowywane informacje niejawne UE, w tym strefy, w których znajdują się systemy teleinformatyczne. Określone środki bezpieczeństwa fizycznego dobiera się na podstawie oceny zagrożenia przeprowadzonej przez właściwe organy. Państwa członkowskie stosują w swoich obiektach proces zarządzania ryzykiem, służący ochronie informacji niejawnych, aby zapewnić poziom ochrony fizycznej proporcjonalny do szacowanego ryzyka. Proces zarządzania ryzykiem uwzględnia wszelkie istotne czynniki, a w szczególności:

- klauzulę tajności informacji niejawnych;
- postać i ilość informacji niejawnych, z uwzględnieniem faktu, że duża ilość informacji niejawnych lub ich kompilacja mogą wymagać zastosowania bardziej rygorystycznych środków ochrony;
- otoczenie i strukturę budynków lub stref, w których znajdują się informacje niejawne;
- szacowane zagrożenie ze strony służb wywiadowczych, których celem jest Unia lub państwa członkowskie, oraz zagrożenie sabotażem, terroryzmem, działalnością wywrotową lub inną działalnością przestępczą.

Organ bezpieczeństwa określa właściwą kombinację środków bezpieczeństwa fizycznego. Mogą one obejmować jeden z poniższych środków lub większą ich liczbę:

- ogrodzenie: fizyczne ogrodzenie, które chroni granice strefy wymagającej ochrony;
- systemy sygnalizacji włamania i napadu: może być stosowany w celu podwyższenia poziomu bezpieczeństwa, który daje ogrodzenie, a w pomieszczeniach i budynkach w celu zastąpienia lub wsparcia pracowników ochrony;
- kontrola dostępu: kontrola dostępu może obejmować teren, budynek lub budynki znajdujące się na danym terenie lub też strefy lub pomieszczenia wewnątrz budynku. Kontrolę można prowadzić za pomocą środków elektronicznych, środków elektromechanicznych, za pośrednictwem pracowników ochrony lub pracowników recepcji lub za pomocą wszelkich innych środków fizycznych;
- pracownicy ochrony: przeszkoleni, nadzorowani, a w razie konieczności odpowiednio sprawdzeni pracownicy ochrony mogą być zatrudniani, między innymi w celu powstrzymania osób planujących niezauważone wejście na dany teren;

- telewizja przemysłowa: może być stosowana przez pracowników ochrony w celu sprawdzania incydentów i sygnałów alarmowych pochodzących z systemu sygnalizacji włamania i napadu na rozległych terenach lub na ogrodzeniach;
- oświetlenie ochronne: oświetlenie ochronne może być stosowane w celu powstrzymania potencjalnych osób nieupoważnionych, a ponadto w celu zapewnienia oświetlenia koniecznego do prowadzenia skutecznego nadzoru bezpośrednio przez pracowników ochrony lub pośrednio za pomocą systemu telewizji przemysłowej.

Stosując koncepcję *ochrony w głąb*, oznaczającą stosowanie pakietu środków bezpieczeństwa o różnych poziomach ochrony, ustanawia się dwa rodzaje stref chronionych fizycznie:

- strefy administracyjne;
- strefy bezpieczeństwa (w tym strefy technicznie zabezpieczone).

Zabezpieczanie informacji w ramach systemów teleinformatycznych oznacza pewność, że systemy te będą chronić informacje, które są w nich przetwarzane, i będą działać zgodnie z przeznaczeniem, w razie potrzeby pod kontrolą uprawnionych użytkowników. Skuteczne zabezpieczanie informacji gwarantuje odpowiedni poziom poufności, integralności, dostępności, niezaprzeczalności i autentyczności. Zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem, które stanowi integralną część definiowania, rozwijania, obsługiwania i konserwacji systemów teleinformatycznych. Zarządzanie ryzykiem (ocena, zmniejszanie, akceptacja i powiadamianie) prowadzone jest jako interaktywny proces wspólnie przez przedstawicieli właścicieli systemu, organy odpowiedzialne za projekt, organy operacyjne oraz organy zatwierdzające bezpieczeństwo, w ramach sprawdzonego, przejrzystego i w pełni zrozumiałego procesu oceny ryzyka.

Poniżej przedstawiono cechy i koncepcje zabezpieczania informacji niezbędne dla bezpieczeństwa i prawidłowego funkcjonowania operacji dokonywanych w ramach systemów teleinformatycznych.

Tabela 2. Cechy i koncepcje zabezpieczania informacji

Poufność	Integralność	Dostępność	Niezaprzeczalność	Autentyczność
cecha polegająca na tym, że informacje nie są ujawniane nieupoważnionym osobom, podmiotom ani do celów nieuprawnionego przetwarzania	cecha polegająca na zachowywaniu dokładności i kompletności informacji i zasobów	cecha polegająca na tym, że informacje są dostępne i gotowe do wykorzystania na wniosek uprawnionego podmiotu	możliwość udowodnienia, że działanie lub wydarzenie miało miejsce, aby następnie nie można było zaprzeczyć wystąpieniu tego działania lub wydarzenia	gwarancja, że informacje są prawdziwe i pochodzą z rzetelnych źródeł

Źródło: Decyzja Rady z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (2013/488/UE)

W celu zmniejszenia ryzyka zagrażającego w systemach teleinformatycznych, wdrażany jest pakiet technicznych i innych środków bezpieczeństwa o strukturze różnych poziomów *ochrony w głąb*, poziomy te obejmują:

- **powstrzymywanie:** środki bezpieczeństwa ukierunkowane na zniechęcenie osób planujących atak;
- **zapobieganie:** środki bezpieczeństwa ukierunkowane na udaremnienie lub powstrzymanie ataku;
- **wykrywanie:** środki bezpieczeństwa ukierunkowane na ujawnienie ataku;
- **odporność:** środki bezpieczeństwa ukierunkowane na ograniczenie skutków ataku, tak by dotknęły one jak najmniejszą ilość informacji lub zasobów systemów teleinformatycznych, oraz na zapobieżenie dalszym szkodom;
- **usuwanie skutków:** środki bezpieczeństwa ukierunkowane na odzyskanie bezpiecznego statusu systemów teleinformatycznych.

Stopień rygorystyczności środków bezpieczeństwa ustalany jest na podstawie oceny ryzyka. Zgodnie ze *Strategią Cyberbezpieczeństwa RP na lata 2017-2020* współpraca międzynarodowa na poziomie operacyjno-technicznym realizowana będzie między innymi w ramach Sieci CSIRT na poziomie Unii Europejskiej, na innych forach wymiany informacji i dokonywania analiz sytuacji bezpieczeństwa IT danego sektora, poprzez inne międzynarodowe sieci współpracy typu FIRST czy TF-CSIRT, platformy wymiany informacji typu MISP oraz w ramach współpracy dwu- i wielostronnej. W tym kontekście szczególne znaczenie będzie miało wypracowanie wspólnych procedur działania

w ramach UE i NATO. Współpraca na tym poziomie będzie służyła nie tylko skutecznemu przeciwdziałaniu zagrożeniom w cyberprzestrzeni, ale przyczyni się do wymiany doświadczeń pomiędzy personelem technicznym w ramach wspólnych przedsięwzięć. Będzie również okazją do promowania polskich rozwiązań technologicznych i polskiej kadry eksperckiej[15].

Bezpieczeństwo przemysłowe oznacza stosowanie środków mających zapewnić ochronę informacjom niejawnym przez wykonawców lub podwykonawców podczas negocjacji poprzedzających zawarcie umów i na wszystkich etapach cyklu życia umów niejawnych. Świadectwo Bezpieczeństwa Przemysłowego wydawane jest przez Krajową Władzę Bezpieczeństwa lub jakikolwiek inny właściwy organ bezpieczeństwa państwa członkowskiego w celu zaświadczenia, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, że dany podmiot prowadzący działalność gospodarczą lub inną jest w stanie zapewnić w swoich obiektach ochronę informacji niejawnych UE odpowiadającą określonemu poziomowi klauzuli tajności[16].

Bezpieczeństwo informacji niejawnych Europejskiej Agencji Kosmicznej (ESA)

Wielkość zasobów ludzkich, technicznych i finansowych wymaganych do działań w przestrzeni kosmicznej jest taka, że zasoby te wykraczają poza granice możliwości któregokolwiek pojedynczego państwa europejskiego. Uchwała przyjęta przez Europejską Konwencję Kosmiczną w dniu 31 lipca 1973 r., podczas której zdecydowano, że nowa organizacja, zwana Europejską Agencją Kosmiczną, zostanie utworzona z Europejskiej Organizacji Badań Kosmosu i Europejskiej Organizacji Rozwoju i Budowy Kosmicznych Systemów Wynoszących, celem jej działania jest zintegrowanie programów kosmicznych państw europejskich w jeden wspólny program europejski. Dąży do wzmacniania współpracy europejskiej wyłącznie dla celów pokojowych, w badaniach i technologiach kosmicznych oraz ich zastosowaniach w kosmosie, z zamiarem ich wykorzystywania dla celów naukowych oraz dla operacyjnych systemów użytkowych[17].

[15]https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09 (14.03.2019).
[16] *Decyzja Rady z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE* (2013/488/UE).
[17] Umowa pomiędzy Rządem Rzeczypospolitej Polskiej a Europejską Agencją Kosmiczną w sprawie przystąpienia Polski do Konwencji o utworzeniu Europejskiej Agencji Kosmicznej i związane z tym warunki, podpisana w Warszawie dnia 31 lipca 2012 r.

Przepisy bezpieczeństwa Europejskiej Agencji Kosmicznej uregulowane są w dokumencie ESA/REG/004 z dnia 18 stycznia 2012 r. Każde państwo członkowskie ESA wdraża normy bezpieczeństwa, tak aby zapewnić wspólny stopień ochrony informacji niejawnych, w związku z tym jest ono za nie odpowiedzialne.

Rada Europejskiej Agencji Kosmicznej jest odpowiedzialna za:

- podejmowanie decyzji we wszystkich kwestiach związanych z bezpieczeństwem, w szczególności w zakresie odpowiedniej polityki bezpieczeństwa w ramach ESA oraz w odniesieniu do wymiany informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi;
- podejmowanie decyzji o zawarciu umowy o bezpieczeństwie w sprawie wymiany informacji niejawnych z państwami trzecimi lub organizacjami międzynarodowymi;
- zatwierdzanie porozumień i protokołów ustaleń w sprawie bezpieczeństwa dotyczących wymiany informacji niejawnych z państwami trzecimi lub organizacjami międzynarodowymi;
- zatwierdzanie środków wynikających z rocznych sprawozdań z inspekcji ESA oraz ze sprawozdań państw trzecich i organizacji międzynarodowych;
- zatwierdzanie wzoru ogólnej instrukcji bezpieczeństwa programu mającej zastosowanie do każdego przyszłego programu ESA wymagającego ochrony informacji niejawnych;
- zatwierdzanie przepisów wykonawczych programu mających zastosowanie do programów ESA wymagających ochrony informacji niejawnych;

Zgodnie z umową o bezpieczeństwie Europejskiej Agencji Kosmicznej oraz w celu zapewnienia wspólnych procedur ochrony informacji niejawnych, przepisy dotyczące bezpieczeństwa ustanawiają podstawowe zasady i minimalne normy bezpieczeństwa, które mają zastosowanie przez Europejską Agencję Kosmiczną oraz przez państwa członkowskie, zgodnie z ich odpowiednimi przepisami ustawowymi i wykonawczymi, o ile zapewniają one równoważny poziom ochrony. Ochrona informacji niejawnych odpowiada następującym celom:

- zabezpieczenie informacji przed naruszeniem bezpieczeństwa i narażeniem na szwank ich bezpieczeństwa;
- zabezpieczenie instalacji przechowujących takie informacje przed nieuprawnionym dostępem, sabotażem i umyślnym złośliwym uszkodzeniem;
- ochrona takich informacji przetwarzanych w systemach łączności oraz związanych z nimi sieciach przed zagrożeniami dla ich integralności i dostępności;

- w przypadku sytuacji nadzwyczajnej, ocena wyrządzonych szkód, ograniczenie ich skutków i przyjęcie niezbędnych środków zaradczych;
- wdrożenie odpowiednich środków bezpieczeństwa w ramach działalności przemysłowej ESA, obejmuje także negocjacje wstępne, negocjacje i umieszczanie umów niejawnych ESA;
- określenie wymogów dotyczących wymiany takich informacji z państwami trzecimi i organizacjami międzynarodowymi w drodze umów o bezpieczeństwie i protokołów ustaleń;
- identyfikacja zagrożeń oraz plany i działania łagodzące w ESA są zarządzane jako proces. Proces ten ma na celu dokonanie oceny zagrożenia, określenie znanych zagrożeń dla bezpieczeństwa, zdefiniowanie środków bezpieczeństwa w celu zmniejszenia lub złagodzenia zagrożeń.

Środki bezpieczeństwa stosuje się do wszystkich osób mających dostęp do informacji niejawnych, nośników informacji niejawnych oraz wszystkich pomieszczeń i instalacji krytycznych zawierających takie informacje. Mają na celu wykrywanie działań osób, które mogłyby zagrozić bezpieczeństwu informacji niejawnych, oraz zapewnienie poufności, integralności, dostępności, autentyczności i niezaprzeczalności wszystkich informacji niejawnych.

Informacje niejawne oznaczają wszelkie informacje, dokumenty lub materiały oznaczone klauzulą tajności, które zostały wygenerowane i przedłożone w jakiejkolwiek formie przez ESA państwu członkowskiemu lub przez państwo członkowskie, celu wsparcia programu, projektu lub umowy, których nieuprawnione ujawnienie mogłoby zaszkodzić interesom ESA.

Informacje są klasyfikowane, jeżeli wymagają ochrony w odniesieniu do ich poufności. Klauzula jest wyraźnie i prawidłowo wskazana i jest utrzymywana jedynie tak długo, jak długo informacje wymagają ochrony.

Informacje niejawne ESA są określane i oznaczane zgodnie z następującymi poziomami:

- ESA TOP SECRET: ta klauzula jest stosowana wyłącznie do informacji i materiałów, których nieuprawnione ujawnienie mogłoby spowodować wyjątkowo poważne szkody dla podstawowych interesów ESA i/lub jednego lub więcej państw członkowskich;
- ESA SECRET: ta klauzula jest stosowana wyłącznie do informacji i materiałów, których nieuprawnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom ESA i/lub co najmniej jednego z jej państw członkowskich;

- ESA CONFIDENTIAL: ta klauzula jest stosowana do informacji i materiałów, których nieuprawnione ujawnienie mogłoby zaszkodzić podstawowym interesom ESA i/lub co najmniej jednego z jej państw członkowskich;
- ESA RESTRICTED: ta klasyfikacja jest stosowana do informacji i materiałów, których nieuprawnione ujawnienie mogłoby być niekorzystne dla interesów ESA i/lub jednego lub więcej państw członkowskich.

Klauzula tajności jest nadawana informacjom zgodnie ze stopniem ochrony wymaganym w celu zapobieżenia nieuprawnionemu ujawnieniu. System klasyfikacji bezpieczeństwa jest instrumentem wprowadzania w życie tych zasad. System klasyfikacji powinien stanowić ramy dla planowania i organizacji środków zaradczych przeciwko niezamierzonemu uwolnieniu, jak również szpiegostwu, sabotażowi, terroryzmowi i innym zagrożeniom.

Bezpieczeństwo fizyczne to stosowanie fizycznych i technicznych środków ochrony w celu zapobieżenia i opóźnienia nieuprawnionego dostępu do informacji niejawnych. Właściwe organy bezpieczeństwa, stosując dogłębnie koncepcję obrony, określają odpowiednie połączenie środków bezpieczeństwa fizycznego. Wszystkie pomieszczenia, strefy, budynki, biura, łączności i informacji, w których przechowywane lub przetwarzane są informacje niejawne, są chronione za pomocą odpowiednich środków bezpieczeństwa. Środki bezpieczeństwa fizycznego wybiera się na podstawie oceny zagrożenia przeprowadzonej przez właściwe organy bezpieczeństwa. Proces zarządzania ryzykiem stosuje się do fizycznej ochrony informacji niejawnych. Proces zarządzania ryzykiem uwzględnia w szczególności wszystkie istotne czynniki:

- poziom klauzuli tajności informacji niejawnych;
- ilość i formę posiadanych informacji;
- otaczające środowisko i strukturę budynków lub obszarów, w których znajdują się informacje niejawne;
- ocenione zagrożenie ze strony służb wywiadowczych, które są celem działań ESA lub państw członkowskich ESA, a także zagrożenie sabotażem, terroryzmem lub inną działalnością przestępczą.

Stosowane środki bezpieczeństwa fizycznego mają na celu zapobieganie nieupoważnionemu dostępowi do informacji niejawnych lub opóźnianie takiego dostępu przez osoby nieupoważnione:

- uniemożliwienie wymuszonego wejścia intruza;
- odstraszanie, utrudnianie i wykrywanie niedozwolonych działań;

- uniemożliwienie dostępu do informacji niejawnych tym członkom personelu ESA lub ekspertom, osobom pracującym dla organów krajowych lub dla państw trzecich, które nie mają dostępu do informacji niejawnej.

Organ bezpieczeństwa, stosując dogłębnie koncepcję obrony, określa odpowiednie połączenie środków bezpieczeństwa fizycznego, które wdraża się na podstawie odpowiedniej oceny ryzyka. Mogą one obejmować jeden lub więcej z elementów:

- **bariera obwodowa**: fizyczna bariera, która broni granicy obszaru wymagającego ochrony;
- **systemy wykrywania włamań:** mogące być stosowane w celu podniesienia poziomu bezpieczeństwa oferowanego przez barierę obwodową lub w pomieszczeniach i budynkach w miejsce pracowników ochrony lub w celu wspierania ich;
- **kontrola dostępu:** kontrola dostępu może być przeprowadzana na terenie obiektu, w budynku lub budynkach na terenie obiektu lub na obszarach lub w pomieszczeniach wewnątrz budynku. Kontrola może być sprawowana za pomocą środków elektronicznych lub elektromechanicznych, przez pracowników ochrony i recepcjonistów lub za pomocą innych środków fizycznych;
- **personel ochrony:** można zatrudnić przeszkolony, nadzorowany oraz, w razie potrzeby, odpowiednio sprawdzony personel ochrony, między innymi w celu powstrzymania osób planujących wtargnięcie;
- **telewizja przemysłowa**: z telewizji przemysłowej mogą korzystać pracownicy ochrony w celu weryfikacji incydentów ze strony osób nieupoważnionych lub nieposiadających niezbędnej wiedzy oraz alarmów w systemach sygnalizacji włamania i napadu w dużych obiektach lub na obwodzie;
- **oświetlenie bezpieczeństwa:** oświetlenie bezpieczeństwa może być stosowane w celu odstraszenia potencjalnego intruza, jak również w celu zapewnienia oświetlenia niezbędnego do skutecznego nadzoru bezpośrednio przez personel ochrony lub pośrednio poprzez system telewizji przemysłowej;
- wszelkie inne odpowiednie środki fizyczne mające na celu powstrzymanie lub wykrycie nieupoważnionego dostępu lub zapobieżenie lub opóźnienie narażenia na szwank bezpieczeństwa informacji niejawnych.

W przypadku gdy informacje niejawne są narażone na ryzyko wyjawienia przez osoby nieupoważnione lub osoby nieposiadające potrzeby niezbędnej wiedzy, podejmuje się odpowiednie środki w celu przeciwdziałania ryzyku[18].

Zakończenie

Wejście do Organizacji Paktu Północnoatlantyckiego wydatnie poprawiło bezpieczeństwo Polski. W 20. rocznicę akcesji do Sojuszu Północnoatlantyckiego, bez wątpienia można stwierdzić, że nasz kraj zbudował silną pozycję w NATO. Od czasu wstąpienia Polski do NATO na terytorium kraju zorganizowano następujące struktury: NC NE (Wielonarodowy Korpus Północ-Wschód w Szczecinie) – 1999, JFTC Centrum Szkolenia Sił Połączonych NATO w Bydgoszczy) – 2004, 3NSB (3 Batalion Łączności NATO w Bydgoszczy) – 2010, MP COE (Centrum Eksperckie Policji Wojskowej NATO w Bydgoszczy) – 2013, NFIU (Jednostka Integracji Sił NATO w Bydgoszczy) – 2015, CI COE (Centrum Eksperckie Kontrwywiadu NATO w Krakowie) – 2017, MND NE (Wielonarodowa Dywizja Północ-Wschód w Elblągu) – 2017. W Polsce odbywają się największe i najważniejsze ćwiczenia Sojuszu, takie jak *Noble Jump 2015*, *Brilliant Jump 2016* czy wcześniej *Steadfast Jazz 2013*. Organizowana przez Polaków w cyklu dwuletnim *Anakonda* uzyskała status największego w regionie międzynarodowego ćwiczenia wojsk sojuszniczych i partnerskich. Siły Zbrojne RP poprzez uczestnictwo w operacjach, misjach i ćwiczeniach sojuszniczych osiągnęły pełną interoperacyjność[19], a właściwe zapewnienie ochrony informacji, w tym niejawnych, pozwoliło na skuteczne realizowanie przedsięwzięć międzynarodowych.

Uznanie informacji za kluczowy element stanowi immanentną cechę współczesnych konfliktów, w których informacja jest wykorzystywana zarówno jako broń, jak i traktowana jako cel[20].

Pozyskanie informacji, które mają wpływ na bezpieczeństwo danego państwa, czyli jego niepodległość, suwerenność oraz pozycję na arenie międzynarodowej, przez nieuprawnione osoby, może mieć daleko idące konsekwencje. Dlatego, by zachować stabilność państwa i dawać poczucie bezpieczeństwa obywatelom, najważniejszym zadaniem i obowiązkiem rządu jest ich ochrona. Może ją zapewnić sprawnie funkcjonu-

[18] Regulations of the European Space Agency Security Regulations ESA/REG/004 Paris, 18 January 2012 r.
[19] https://www.gov.pl/web/obrona-narodowa/20-lat-polski-w-nato (14.03.2019).
[20] P. Sienkiewicz, M. Marszalek, H. Świeboda, *Metodologia badań bezpieczeństwa narodowego*, t. IV, AON, Warszawa 2012, s. 184.

jący system, który będzie gwarantował ograniczenia w dostępie do informacji niejawnych, właściwe ich przetwarzanie, a także wykorzystanie odpowiednich i wystarczających środków bezpieczeństwa fizycznego, technicznego, teleinformatycznego i prawnego. Z tego też względu system ten wymaga na poziomie państwa precyzyjnie określonych zasad i norm mających umocowanie w prawie, określającym zasady tworzenia informacji niejawnych, sposób ich ochrony oraz sankcje, jakie mogą zostać zastosowane w przypadku niestosowania się do tych zasad[21].

Bibliografia

Decyzja Rady z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (2013/488/UE).

http://www.wojsko-polskie.pl/pl/pages/siy-zbrojne-rp-2016-04-18-j/ (14.03.2019).

https://bip.abw.gov.pl/bip/informacje-niejawne-1/ochrona-informacji (12.03.2019).

https://docplayer.pl/3448390-Agencja-bezpieczenstwa-wewnetrznego-raport-z-dzialalnosci-agencji-bezpieczenstwa-wewnetrznego-w-2014-r.html (19.02.2019).

https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09 (14.03.2019).

https://www.gov.pl/web/obrona-narodowa/20-lat-polski-w-nato (14.03.2019).

Iwaszko B., *Ochrona informacji niejawnych w praktyce*, wyd. Presscom, Wrocław 2012.

Regulations of the European Space Agency Security Regulations ESA/REG/004 Paris, 18 January 2012.

Sienkiewicz P., Marszałek M., Świeboda H., *Metodologia badań bezpieczeństwa narodowego*, t. IV, wyd. Akademia Obrony Narodowej, Warszawa 2012.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014.

Topolewski S., *Ochrona informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej*, wyd. Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2017.

Topolewski S., Żarkowski P., *Ochrona informacji niejawnych i danych osobowych. Wymiar teoretyczny i praktyczny*, wyd. Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2014.

Umowa pomiędzy Rządem Rzeczypospolitej Polskiej a Europejską Agencją Kosmiczną w sprawie przystąpienia Polski do Konwencji o utworzeniu Europejskiej Agencji Kosmicznej i związane z tym warunki, podpisana w Warszawie dnia 31 lipca 2012 r.

Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu z dnia 24 maja 2002 r. (Dz.U. 2002 nr 74 poz. 676, z późn. zm.).

Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz.U. 2010 nr 182 poz. 1228, z późn. zm.).

[21] S. Topolewski, *Ochrona informacji niejawnych*…, op. cit., s. 349.

Wróblewski R., Wyrębek H. (red.), *Determinanty bezpieczeństwa militarnego*, wyd. Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2016.

Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowym z dnia 31.12.2010 r.

Zalewski S., *Informacje niejawne we współczesnym państwie*, wyd. Editions Spotkania, Warszawa 2017.