BEZPIECZEŃSTO MIĘDZYNARODOWE

Jacek SOBCZAK
Szkoła Wyższa Psychologii Społecznej, Warszawa

OCHRONA INFORMACJI NIEJAWNYCH W SYSTEMIE PRAWNYM UNII EUROPEJSKIEJ

Problematyka odnosząca się do ochrony informacji niejawnych podjęta została w tekście Traktatu ustanawiającego Europejską Wspólnotę Gospodarczą z 1957 roku. Wzorem dla art. 223 Traktatu ustanawiającego Wspólnotę Europejską był artykuł XXI Układu Ogólnego w sprawie Taryf Celnych i Handlu z roku 1947[1]. Po zmianach artykuł ten oznaczony był w wersji skonsolidowanej, uwzględniającej zmiany wprowadzone traktatem z Nicei, jako art. 296. Traktat z Lizbony pozostawił redakcję art. 296 w dotychczasowym kształcie, natomiast zmianie uległa numeracja przepisu, który po wejściu w życie traktatu z Lizbony (Traktatu o funkcjonowaniu Unii Europejskiej) oznaczony jest jako art. 346. W początkowej wersji art. 296 TWE stanowił: „1. Postanowienia niniejszego Traktatu nie stanowią przeszkody w stosowaniu następujących reguł: a) żadne Państwo Członkowskie nie ma obowiązku dzielenia informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa; b) każde Państwo Członkowskie może podejmować środki, jakie uważa za konieczne w celu ochrony podstawowych interesów jego bezpieczeństwa, a które odnoszą się do produkcji lub handlu bronią, amunicją lub materiałami wojennymi; środki takie nie mogą negatywnie wpływać na warunki konkurencji na wspólnym rynku w odniesieniu do produktów, które nie są przeznaczone wyłącznie do celów wojskowych. 2. W ciągu pierwszego roku od wejścia w życie niniejszego Traktatu Rada stanowiąc jednomyślnie, określi listę produktów, do których mają zastosowanie postanowienia ustępu 1 litera b). 3. Rada stanowiąc jednomyślnie na wniosek Komisji może dokonać zmian na tej liście".

Treść wspomnianego przepisu została zmieniona w Traktacie amsterdamskim w ten sposób, że z art. 296 usunięto ust. 2, zastępując go zmodyfikowanym dotychczasowym ust. 3 w brzmieniu: „Rada stanowiąc jednomyślnie na wniosek Komisji, może wprowadzać zmiany do sporządzonej przez siebie 15 kwietnia 1958 roku listy produktów, do których mają zastosowanie postanowienia ustępu 1 litera b)".

Art. 296 TWE umieszczony został w części szóstej traktatu „Postanowienia ogólne i końcowe". Po zmianach wprowadzonych przez traktat z Lizbony o funkcjonowaniu Unii Europejskiej znalazł się w części siódmej, noszącej ten sam tytuł co wcześniejsza część szósta.

---

[1] K. Eikenberg, *Article 296 (ex 223) E. C. and external trade in strategic goods*, „European Law Review" 2000, Vol. 25, s. 118; S. Peers, *National Security an European Law*, „Yearbook of European Law" 1996, s. 379; M. Trybus, *The EC Treaty as an Instrument of European Defence Integration: Judicial Security of Defence and Security Exeptions*, „Common Market Law Review", Vol. 39, s. 1359.

W literaturze wskazuje się, że przepis art. 296 (art. 346 TFUE) to norma o charakterze ogólnym, której zastosowanie nie jest ograniczone do poszczególnych dziedzin prawa wspólnotowego. W zakresie swojej regulacji przepis ten wyłącza zastosowanie wszystkich postanowień traktatu, zarówno materialno-prawnych, jak i procesowych, będąc normą o charakterze wyjątkowym, a co za tym idzie podlegającą wykładni restryktywnej[2]. Art. 296 nie jest jedynym przepisem traktatu upoważniającym państwa członkowskie do podejmowania ze względów bezpieczeństwa środków niezgodnych z regulacjami traktatu oraz z normami prawa wspólnotowego[3]. Jednak art. 296 jest klauzulą derogacyjną o charakterze ogólnym, podczas gdy pozostałe przepisy zezwalają na niestosowanie norm prawa wspólnotowego w granicach wyznaczonych przez zakres konkretnej klauzuli. Pozostałe przepisy posługują się pojęciem „bezpieczeństwa publicznego", tymczasem w treści art. 296 mowa o bezpieczeństwie w znaczeniu interesu bezpieczeństwa, co definiowane jest jako „bezpieczeństwo narodowe" lub „zewnętrzne bezpieczeństwo wojskowe"[4]. Tak więc w treści art. 296 chodzi o interesy bezpieczeństwa w znaczeniu militarnym węższym, niezbędne dla zapewnienia funkcjonowania państwa. Ważne jest także i to, że do środków podejmowanych na podstawie art. 296 nie mają zastosowania przesłanki proporcjonalności obowiązujące na podstawie art. 30 TWE, lecz wystarczające jest ustalenie, że środki te nie są w sposób oczywisty nieproporcjonalne do zapewnienia bezpieczeństwa militarnego państwa członkowskiego[5]. Państwa członkowskie mogą powoływać się na treść art. 296 w czasach pokoju. Treść art. 297 TWE (art. 347 TFUE) zezwala państwom członkowskim na stosowanie niezbędnych działań w przypadku poważnych zaburzeń wewnętrznych zagrażających porządkowi publicznemu, w przypadku wojny, poważnego napięcia międzynarodowego stanowiącego groźbę wojny lub w celu wypełnienia zobowiązań przyjętych w celu utrzymania pokoju i bezpieczeństwa międzynarodowego.

W oparciu o treść art. 296 ust. 1 lit. a (art. 346 ust. 1 lit. a TFUE) państwo członkowskie może odmówić ujawnienia informacji, których przekazanie uważa za sprzeczne z podstawowymi interesami swojego bezpieczeństwa. Norma ta ma charakter ogólny, a jak zauważa się zarówno w dyrektywach, jak i w judykatach Trybunału Sprawiedliwości w Luksemburgu ochrona dostępu do informacji wrażliwych z punktu widzenia interesów państw członkowskich może być regulowana w sposób szczegółowy, także w aktach prawa pochodnego[6]. Prawo odmowy ujawnienia informacji jest wyjątkiem od

---

[2] S. Weatherhill, P. Beaumont, *EC Law*, London 1995, s. 464; *INTERPRETATIVE COMMUNICATION of the European Commission on the application of Article 296 of the Treaty in the field of defence procurement*, Brussels 7.12.2006, COM (206); par. 61, *Case T-26/01 Fiocchi Munizioni v Commission*, Judgment of 30 September 2003. Patrz także: *Opinion of Advocate General Jacobs* of 8 May 1991.

[3] Możliwość taką przewidują także art. 30, 39 ust. 3, 46, 55, 58 ust. 1 lit. b, 64 ust. 1 TWE.

[4] Wyrok 72/83 z 10 lipca 1984 r. w sprawie *Campus Oil Ltd. i inni p. Minister for Industry and Energy i inni*, „Recueil" 1984, s. 2727; tamże: opinia Rzecznika Generalnego Slynna.

[5] E. Bratanova, *Legal Limits of the National Defence Privilege in the European Union*, Bonn International Center for Conversion, Paper No. 34, s. 9.

[6] Art. 30 ust. 2, *dyrektywa 2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium Państw Członkowskich zmieniająca rozporządzenie EWG nr 1612/68 i uchylająca dyrektywy 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG,*

zasady lojalności wynikającej z treści art. 10 TWE[7]. Ocena, które informacje mają takie znaczenie, że ich ujawnienie zagrażałoby podstawowym interesom państwa członkowskiego należy do organów tego państwa. Do informacji takich należy zaliczyć informacje dotyczące składu i rozmieszczenia sił zbrojnych, ich wyposażenia, raporty służb specjalnych, wywiadowczych i kontrwywiadowczych. Jak dotychczas europejski Trybunał Sprawiedliwości nie wydał żadnego rozstrzygnięcia dotyczącego bezpośrednio wykładni art. 296 ust. 1 lit. a.

Sporna jest sprawa dopuszczalności stosowania art. 296 ust. 1 lit. a TWE (art. 346 TFUE) w odniesieniu do ochrony informacji, gdyż dostęp do informacji został objęty harmonizacją w prawie wspólnotowym. Z jednej strony niewątpliwe jest, że przyjęcie tezy, iż państwo członkowskie zachowało prawo do ochrony informacji w zakresie bezpieczeństwa z natury rzeczy musi osłabić skuteczność działań integracyjnych. Z drugiej jednak strony art. 296 ma charakter wyjątkowy i służy ochronie tak ważnych interesów jak interes bezpieczeństwa państwa członkowskiego, a więc ochrona tych interesów ma znaczenie pierwszorzędne i musi mieć pierwszeństwo przed zasadą skuteczności prawa wspólnotowego[8].

Warto dodać, że zgodnie z treścią art. 287 TWE (art. 339 TFUE) członkowie instytucji Wspólnoty, członkowie Komitetów oraz urzędnicy i inni współpracownicy wspólnoty są zobowiązani, również po zaprzestaniu pełnienia swoich funkcji, nie ujawniać informacji objętych ze względu na swój charakter tajemnicą zawodową, a zwłaszcza informacji dotyczących przedsiębiorstw i ich stosunków handlowych lub kosztów własnych. Rozwiązanie to jest tym bardziej ważne, że w myśl art. 284 TWE (art. 338 TFUE) w celu wypełnienia zadań, które są jej powierzone Komisja może zbierać wszelkie informacje i dokonywać wszelkich niezbędnych weryfikacji w granicach i na warunkach określonych przez Radę Europejską zgodnie z postanowieniami Traktatu. Państwa członkowskie, zgodnie z zasadą lojalności określoną w art. 10, mają obowiązek udzielić Komisji wszelkich niezbędnych informacji. Mogą odmówić przedstawienia tej informacji jedynie powołując się na potrzebę ochrony swoich istotnych interesów[9].

Problem bezpieczeństwa dotyczącego ochrony informacji niejawnych Unii Europejskiej podejmuje decyzja Rady z 31 marca 2011 roku w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (2011/292/UE)[10]. Ze wstępu

---

90/364/EWG, 90/365/EWG i 93/96/EWG, Dz. Urz. UE L 158/77, 30.04.2004, s. 46; *Wyrok Trybunału w Strasburgu (Wielka Izba) z 12 kwietnia 2005 w sprawie C-61/03 Komisja przeciwko zjednoczonemu Królestwu*, Dz. Urz. C 132, 28.05.2005.

[7] S. Trombetta, *La protection des intérêts nationaux de la défense quand la défense devient européenne: les evolutions de l'article 296 TCE,* „Revue de Marché Commun et de l'Union Européenne" 2005, No. 490, s. 442; W. Hummer, w: *Kommentar zum EWG Vertrag*, red. E. Garbitz, 4. Aufl, München 1990 (komentarz do art. 223–225 TEWG), s. 1.

[8] W. Sadowski, w: *Traktat ustanawiający Wspólnotę Europejską*, red. A. Wróbel, t. III, Warszawa 2010, s. 929.

[9] Wypada zauważyć, że traktat z Lizbony zmodyfikował przepisy dotyczące zasady lojalności w ten sposób, że na mocy art. 4 ust. 3 traktatu z Lizbony rozciągnięto zobowiązanie zasady lojalności na całe prawo unijne.

[10] Dz. Urz. UE L 2011, nr 141, s. 17. Decyzja ta uchyliła i zastąpiła decyzję Rady z 19 marca 2001 roku w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa, Dz. Urz. UE L 2001, nr 101,

do tej decyzji wynika, że tworząc ją Rada Unii Europejskiej zmierzała do utworzenia kompleksowego systemu bezpieczeństwa, służącego ochronie informacji niejawnych, który obejmie Radę i jej Sekretariat Generalny oraz państwa członkowskie. Decyzja ta, jak stwierdzono, winna mieć zastosowanie do przypadków, gdy Rada i jej organy przygotowawcze oraz Sekretarz Generalny wykorzystują informacje niejawne Unii Europejskiej. Zauważono także, że zgodnie z krajowymi przepisami ustawodawczymi i wykonawczymi w zakresie, jaki jest niezbędny do funkcjonowania Rady w przypadkach, gdy właściwe organy, pracownicy lub wykonawcy z państw członkowskich wykorzystują informacje niejawne UE (zwane w treści decyzji EUCI) państwa członkowskie powinny przestrzegać postanowień decyzji Rady z 31 marca 2011 r., tak aby każda ze stron mogła mieć pewność, że zagwarantowany został równoważny poziom ochrony EUCI. Zadeklarowano przy tym w preambule, że zarówno Rada, jak i Komisja zdecydowane są stosować równoważne normy bezpieczeństwa w celu ochrony informacji niejawnych UE, podkreślając znaczenie włączania się w odpowiednich przypadkach Parlamentu Europejskiego i innych instytucji, agencji, organów lub biur UE w przestrzeganie zasad, norm i przepisów dotyczących ochrony informacji niejawnych, które są niezbędne do ochrony interesów Unii i jej państw członkowskich. Wskazano także, że agencje i organy Unii Europejskiej utworzone na mocy tytułu V rozdziału 2 Traktatu o Unii Europejskiej, a także Europol i Eurojust mają obowiązek stosować w ramach swoich struktur wewnętrznych podstawowe zasady i minimalne normy określone we wspomnianej decyzji w celu ochrony EUCI.

W treści decyzji określono podstawowe zasady i minimalne normy bezpieczeństwa służące ochronie EUCI. Stwierdzono przy tym, że mają one zastosowanie do Rady i Sekretariatu Generalnego, a winny być przestrzegane także przez Państwa Członkowskie zgodnie z ich krajowymi przepisami ustawodawczymi i wykonawczymi tak, aby każda ze stron mogła mieć pewność, że zagwarantowany został równoważny poziom ochrony. Warto zauważyć, że w treści decyzji zdefiniowano zarówno pojęcie informacji niejawnych EUCI, jak i klauzule tajności i zasady ich oznaczenia. Decyzja w dodatku A przynosi także 51 szczegółowych definicji, pojęć, które winny mieć zastosowanie do jej treści. Pod pojęciem „informacji niejawnych UE" (EUCI) decyzja chce rozumieć wszelkie informacje lub materiały objęte klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby w różnym stopniu wyrządzić szkodę interesom Unii Europejskiej

---

s. 1 z późn. zm. (załącznik do wspomnianej decyzji, zawierający przepisy Rady Unii Europejskiej dotyczące bezpieczeństwa został zmieniony przez art. 1 i 2 decyzji Rady z 20 grudnia 2005 roku nr 2005/952/WE (Dz. Urz. UE L 2005, nr 346, s. 18). Wydając decyzję działano między innymi w oparciu o treść art. 207 ust. 3 Traktatu ustanawiającego Wspólnotę Europejską (TWE) oraz decyzję Rady 2000/396/WE, EWWiS, Euratom z 5 czerwca 2000 roku przyjmującą regulamin Rady, w szczególności zaś mając na względzie art. 24. Dodać należy, że decyzja ta zastąpiła: decyzję Rady 98/319/WE z 27 kwietnia 1988 roku (Dz. Urz. L 140, 12.05.1998, s. 12), odnoszącą się do procedur, według których urzędnikom oraz pracownikom Sekretariatu Generalnego Rady można umożliwić dostęp do informacji niejawnych posiadanych przez Radę; decyzję Sekretarza Generalnego/Wysokiego Przedstawiciela z 27 lipca 2000 roku (Dz. Urz. C 239, 23.08.2000, s. 1) w sprawie środków ochrony niejawnych informacji stosowanych w odniesieniu do Sekretariatu Generalnego Rady (4); decyzję 433/97 Sekretarza Generalnego Rady z 27 maja 1997 roku w sprawie procedury postępowania sprawdzającego urzędników odpowiedzialnych za funkcjonowanie sieci Cortesy.

lub interesom przynajmniej jednego Państwa Członkowskiego. Przewidziano, że EUCI winny otrzymać jedną z czterech klauzul tajności, a mianowicie:

- 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.

Zawarowano jednocześnie, że EUCI można nadać dodatkowe oznaczenie wskazujące na dziedzinę działalności, do której się odnoszoną, na wytwórcę, ograniczenia dystrybucji, ograniczenia wykorzystania lub możliwości ujawnienia. Wyraźnie stwierdzono przy tym, że właściwe organy winny zapewnić, aby EUCI nadawano odpowiednie klauzule tajności i aby informacje takie były wyraźnie oznaczone jako informacje niejawne, a także by były one objęte danym poziomem klauzuli tajności nie dłużej, niż to jest konieczne. Do obniżenia lub zniesienia klauzul tajności nadanych EUCI, a także do zmiany lub usunięcia oznaczeń potrzebna jest uprzednia pisemna zgodna wytwórcy. Jednocześnie wyraźnie zaznaczono, że Rada zatwierdza politykę bezpieczeństwa w zakresie wytwarzania EUCI, „która obejmuje praktyczny przewodnik nadawania klauzul tajności". W treści decyzji zajęto się także organizacją bezpieczeństwa w Radzie (art. 15 decyzji), ustanawiając Komitet ds. Bezpieczeństwa, który winien analizować i oceniać wszelkie kwestie bezpieczeństwa, wchodzące w zakres stosowania decyzji z 31 marca 2011 roku oraz przedstawiać Radzie odpowiednie zalecenia. Komitet ten winien składać się z przedstawicieli Krajowych Władz Bezpieczeństwa (KWB) państw członkowskich, a w jego obradach winien uczestniczyć przedstawiciel Komisji i Europejskiej Służby Działań Zewnętrznych[11]. Przewodniczy obradom Komitetu Sekretarz

[11] Służbę tę powołuje lakoniczny w swej treści art. 27 ust. 3 Traktatu o Unii Europejskiej (tekst skonsolidowany Dz. Urz. UE 2010 C/13), w którym stwierdzono, że wykonywaniu swego mandatu Wysoki przedstawiciel Unii Europejskiej ds. zagranicznych i polityki bezpieczeństwa, który przewodniczy Radzie ds. Zagranicznych jest wspomagany przez Europejską Służbę Działań Zewnętrznych, która współpracuje ze służbami dyplomatycznymi Państw Członkowskich i składa się z urzędników właściwych służb Sekretariatu Generalnego, Rady i Komisji, jak również z personelu delegowanego przez krajowe służby dyplomatyczne. Organizacje i zasady funkcjonowania tej służby określa decyzja Rady wydana na wniosek wysokiego przedstawiciela, po konsultacji z Parlamentem Europejskim i po uzyskaniu zgody Komisji. Koncepcja utworzenia Europejskiej Służby Działań Zewnętrznych łączy się z podjęciem przez Unię Europejską wspólnej polityki zagranicznej i bezpieczeństwa. Narodziła się ona w procesie stopniowej konstytucjonalizacji Unii Europejskiej. Celem powołania tej służby była próba nadania większej spójności unijnej polityce zagranicznej oraz dążenie do zniesienia napięć między wspólnotową polityką zewnętrzną, na którą składają się głównie handel, pomoc rozwojowa i relacje z krajami ubiegającymi się o członkostwo w Unii Europejskiej lub pozostającymi w jej bliskim sąsiedztwie, a międzyrządową wspólną polityką zagraniczną i bezpieczeństwem. Zob.:

Generalny lub wyznaczona przez niego osoba. Komitet ten zbiera się na polecenie Rady lub na wniosek Sekretarza Generalnego bądź Krajowej Władzy Bezpieczeństwa. Do uczestnictwa w obradach Komitetu mogą być zaproszeni przedstawiciele agencji i organów Unii Europejskiej, utworzonych na mocy tytułu V, rozdział 2 TUE, jak również Europolu i Eurojustu, jeżeli omawiane są kwestie, które ich dotyczą. Komitet ds. Bezpieczeństwa organizuje swą działalność w taki sposób, aby móc przedstawiać zalecenia w konkretnych dziedzinach dotyczących bezpieczeństwa. Z mocy decyzji ma on obowiązek powołać podgrupę ekspercką, zajmującą się kwestiami zabezpieczenia informacji oraz inne podgrupy eksperckie w zależności od okoliczności. Wyznacza przy tym zakres zadań takich podgrup i otrzymuje od nich sprawozdania z działalności, a także w zależności od sytuacji zalecenia dla Rady.

Organem bezpieczeństwa Sekretariatu Generalnego Rady jest Sekretarz Generalny Rady. Obowiązki jego z tego tytułu określa art. 15 ust. 2 decyzji z 31 marca 2011 roku w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE[12]. W wypełnianiu obowiązków przez Sekretarza pomaga mu z mocy art. 17 ust. 2 Biuro ds. Bezpieczeństwa, które upoważnione zostało w myśl załącznika III do prowadzenia inspekcji agencji i organów UE utworzonych na mocy tytułu V rozdziału 2 TUE, jak również Europolu i Eurojustu. W dużej mierze zdaje się ono dublować kompetencje Dyrekcji ds. bezpieczeństwa Komisji Europejskiej, która zresztą w myśl pkt 54 załącznika III „Zarządzanie informacjami niejawnymi" może brać udział w inspekcji

---

O. Osica, R. Trzaskowski, współprac. J. Popielawska, *Europejska Służba Działań Zewnętrznych. Implikacje dla instytucji i stosunków zewnętrznych Unii Europejskiej*, „Nowa Europa. Przegląd Natoliński" 2009, nr 2, s. 5–58. Kwestie przepisów bezpieczeństwa odnoszących się do Europejskiej Służby Działań Zewnętrznych reguluje decyzja Wysokiego Przedstawiciela Unii ds. Zagranicznych i Polityki Bezpieczeństwa z 15 czerwca 2011 roku w sprawie przepisów bezpieczeństwa mających zastosowanie do Europejskiej Służby Działań Zewnętrznych 2011/C 304/05, Dz. Urz. UE C 2011, nr 304, s. 7.

[12] Pełniąc tę funkcję, Sekretarz Generalny: wdraża politykę bezpieczeństwa opracowaną przez Radę i dokonuje jej przeglądu; koordynuje z KWB państw członkowskich wszystkie kwestie bezpieczeństwa dotyczące ochrony informacji niejawnych mających związek z działaniami Rady; wydaje PBO UE urzędnikom i innym pracownikom SGR, zgodnie z art. 7 ust. 3, przed uzyskaniem przez nich dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej; w razie potrzeby zaleca wyjaśnienie każdego zaistniałego lub domniemanego przypadku narażenia na szwank bezpieczeństwa informacji niejawnych znajdujących się w posiadaniu Rady lub wytworzonych przez Radę lub utraty takich informacji oraz zwraca się do właściwych organów bezpieczeństwa o pomoc w takim postępowaniu wyjaśniającym; przeprowadza okresowe inspekcje zabezpieczeń służących ochronie informacji niejawnych w obiektach SGR; przeprowadza okresowe inspekcje zabezpieczeń służących ochronie EUCI w agencjach i organach UE utworzonych na mocy tytułu V rozdział 2 TUE, w Europolu i Eurojuście, jak również podczas operacji zarządzania kryzysowego prowadzonych na mocy tytułu V rozdział 2 TUE oraz zabezpieczeń stosowanych przez specjalnych przedstawicieli UE (SPUE) i członków ich zespołów; przeprowadza, wspólnie i w porozumieniu z zainteresowanymi KWB, okresowe inspekcje zabezpieczeń służących ochronie EUCI w jednostkach organizacyjnych i obiektach w państwach członkowskich; koordynuje środki bezpieczeństwa z właściwymi organami państw członkowskich odpowiedzialnymi za ochronę informacji niejawnych oraz, w stosownych przypadkach, z państwami trzecimi lub organizacjami międzynarodowymi, w tym w zakresie charakteru zagrożeń dla bezpieczeństwa EUCI oraz środków ochrony przed tymi zagrożeniami; zawiera porozumienia administracyjne, o których mowa w art. 12 ust. 2 lit. b); oraz przeprowadza wstępne i okresowe wizyty oceniające w państwach trzecich lub w organizacjach międzynarodowych w celu sprawdzenia skuteczności środków wprowadzonych, by chronić EUCI przekazane im jednostronnie lub w ramach wymiany.

agencji i organów UE, jeśli tylko prowadzi regularną wymianę EUCI z podległą inspekcji agencją bądź organem. Po przeprowadzeniu inspekcji pod nadzorem Biura ds. Bezpieczeństwa Sekretariatu Generalnego sporządzany ma być raport z inspekcji.

Polityki bezpieczeństwa przewidujące środki służące wprowadzeniu w życie decyzji Rady z 31 marca 2011 roku zatwierdza Rada na zlecenie Komitetu Bezpieczeństwa. W decyzji stwierdzono, że czyni to wówczas „jeżeli to konieczne" (art. 6 ust. 1 decyzji z 31 marca 2011 roku). To ostatnie stwierdzenie wydaje się być niezwykle ogólnikowe i w praktyce może powodować wiele wątpliwości. Komitet Bezpieczeństwa może na swoim poziomie uzgodnić wytyczne dotyczące bezpieczeństwa, które będą uzupełniać lub wspierać decyzję 2011/292/UE i wszelkie polityki bezpieczeństwa zatwierdzone przez Radę. W praktyce uprawnienie to może oznaczać jednak zbyt dalekie przesunięcie kompetencji pozwalających na regulację tych żywotnych kwestii i prowadzić do rozwiązań restrykcyjnych, niekoniecznie zgodnych z tymi zamiarami Rady, które legły u podstaw przyjęcia omawianej decyzji.

W myśl art. 4 decyzji Rady z 31 marca 2011 roku EUCI są chronione zgodnie z treścią decyzji, a posiadacz jakichkolwiek informacji niejawnych odpowiedzialny jest za ich ochronę zgodnie z decyzją. Przez „posiadacza" należy, w myśl dodatku A do decyzji, rozumieć osobę posiadającą odpowiednie uprawnienia i spełniającą zasadę ograniczonego dostępu, znajdującą się w posiadaniu EUCI i w związku z tym odpowiedzialną za ich ochronę. W treści decyzji zauważono, że jeżeli państwa członkowskie wprowadzają do struktur lub sieci Unii Europejskiej informacje niejawne, którym nadano krajową klauzulę tajności, wówczas Rada i Sekretarz Generalny Rady obejmują te informacje ochroną zgodnie z wymogami, które mają zastosowanie do EUCI mających równorzędną klauzulę tajności[13].

W decyzji uregulowano kwestię zarządzania ryzykiem dla bezpieczeństwa[14]. Zarządzanie ryzykiem naruszenia informacji niejawnych UE przebiega w ramach określonego procesu. Jest on ukierunkowany na określenie rodzajów ryzyka naruszenia zasad bezpieczeństwa, środków bezpieczeństwa służących zmniejszeniu tego ryzyka do akceptowalnego poziomu zgodnie z podstawowymi zasadami i minimalnymi normami bezpieczeństwa przedstawionymi w tekście decyzji oraz na zastosowanie tych środków zgodnie z koncepcją „ochrony w głąb"[15]. Skuteczność takich środków jest stale poddawana ocenie. Środki bezpieczeństwa służące ochronie EUCI „na wszystkich etapach ich cyklów życia" są proporcjonalne, w szczególności do ich klauzuli tajności, formy, ilości informacji lub materiałów, lokalizacji i konstrukcji obiektów, w których się znajdują oraz oceny zagrożenia wystąpieniem w tym miejscu działań „realizowanych

---

[13] Tabela odpowiedników klauzul tajności została zawarta w dodatku B do decyzji. W decyzji stwierdzono, że uzasadnione może być objęcie dużych ilości lub kompilacji EUCI ochroną na poziomie właściwym dla wyższej klauzuli tajności (art. 4 ust. 4 decyzji z 31 marca 2011 roku).

[14] Przez „ryzyko" decyzja w dodatku A rozumie prawdopodobieństwo, że dane zagrożenie „wykorzysta wewnętrzną i zewnętrzną podatność danej organizacji lub jakiegokolwiek systemu, z którego korzysta i tym samym spowoduje szkody dla tej organizacji i jej materialnych lub niematerialnych zasobów". W myśl definicji zawartej w dodatku A decyzji ryzyko mierzone jest jako połączenie prawdopodobieństwa wystąpienia zagrożeń oraz ich skutków.

[15] „Ochrona w głąb" w myśl dodatku A decyzji oznacza stosowanie pakietu środków bezpieczeństwa o różnych poziomach ochrony.

w złych zamiarach" lub działalności przestępczej, takiej jak: szpiegowska, sabotażowa lub terrorystyczna. Plany awaryjne uwzględniają potrzebę ochrony informacji niejawnych UE podczas wystąpienia sytuacji nadzwyczajnych w celu zapobieżenia nieuprawnionemu dostępowi do informacji, ich ujawnieniu lub utracie ich integralności lub dostępności. Natomiast w planach ciągłości działania zamieszczane są środki zapobiegawcze i naprawcze służące zminimalizowaniu skutków poważnych niedopatrzeń lub incydentów związanych z wykorzystaniem EUCI oraz ich przechowywaniem[16].

Decyzja reguluje problem bezpieczeństwa osobowego, fizycznego, zarządzania informacjami niejawnymi, ochronę EUCI przetwarzanych w systemach teleinformatycznych, bezpieczeństwa przemysłowego, wymianę informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi, wreszcie naruszenie i narażenia na szwank bezpieczeństwa EUCI i odpowiedzialność za wprowadzenie decyzji w życie. Pod pojęciem „bezpieczeństwa osobowego" decyzja rozumie stosowanie środków gwarantujących, że dostęp do EUCI jest przyznawany tylko osobom, które: spełniają zasadę ograniczonego dostępu, w odpowiednich przypadkach zostały sprawdzone oraz poinformowane o swoich obowiązkach. Procedury postępowań sprawdzających mają na celu stwierdzenie czy daną osobę ze względu na jej lojalność, wiarygodność i rzetelność można uprawnić do dostępu do informacji UE[17]. Procedura prowadzenia postępowań sprawdzających dotycząca pracowników i innych urzędników Sekretariatu Generalnego Rady została uregulowana w załączniku I do decyzji[18]. Zarówno Sekretariat

---

[16] W myśl dodatku A decyzji wykorzystywanie EUCI oznacza wszelkie możliwe działania, którym mogą podlegać EUCI „na wszystkich etapach ich cyklu życia". Pojęcie to obejmuje wytwarzanie tych informacji, ich przetwarzanie, przewożenie, obniżenie klauzuli tajności oraz niszczenie. W przypadku systemu teleinformatycznego przetwarzającego EUCI obejmuje ono także gromadzenie informacji, ich przedstawianie, transmisję i przechowywanie.

[17] W myśl art. 7 ust. 3 decyzji wszystkie osoby pracujące w Sekretariacie Generalnym, których obowiązki mogą wymagać dostępu do informacji niejawnych UE o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej są przed uzyskaniem dostępu do takich informacji odpowiednio sprawdzane.

[18] Osoba takowa winna spełniać zasadę ograniczonego dostępu. Musi posiadać poświadczenie bezpieczeństwa osobowego PBO do odpowiedniego poziomu lub ze względu na pełnione przez nią funkcje winna mieć przyznane inne odpowiednie upoważnienie zgodne z przepisami krajowymi ustawodawczymi. Ponadto osoba taka winna być poinformowana o zasadach i procedurach bezpieczeństwa służących ochronie EUCI i musi potwierdzić, że zapoznała się ze swoimi obowiązkami w zakresie ochrony takich informacji. Należy dodać, że decyzja w dodatku A wyróżnia dwa rodzaje poświadczenia bezpieczeństwa osobowego PBO. Po pierwsze poświadczenie bezpieczeństwa osobowego UE, które oznacza upoważnienie dokonane przez organ powołujący Sekretariat Generalny Rady, zgodnie z niniejszą decyzją po przeprowadzeniu przez właściwe organy państwa członkowskiego postępowania sprawdzającego, w którym to upoważnieniu poświadcza się, że danej osobie można w określonym terminie udzielać dostępu do EUCI do określonego poziomu klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej pod warunkiem, że stwierdzono, iż osoba ta spełnia zasadę ograniczonego dostępu. O takiej osobie w myśl dodatku A do decyzji można mówić, że została odpowiednio sprawdzona. Po drugie decyzja w dodatku A wyróżnia krajowe poświadczenie bezpieczeństwa osobowego, pod którym rozumie poświadczenie właściwego organu państwa członkowskiego, wydawane po przeprowadzaniu przez właściwe organy państwa członkowskiego postępowania sprawdzającego, w którym to poświadczeniu stwierdza się, że danej osobie można w określonym terminie udzielać dostępu do EUCI do określonego poziomu klauzuli tajności pod warunkiem, że stwierdzono, iż spełnia ona zasadę ograniczonego dostępu. Taka osoba także uważana jest za „odpowiednio sprawdzoną".

Generalny Rady, jak i każde z Państw Członkowskich określają, jakie stanowiska w ich strukturach wymagają dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej i w związku z tym wymagają poświadczenia bezpieczeństwa osobowego do odpowiedniego poziomu. Po otrzymaniu odpowiedniego wniosku krajowe władze bezpieczeństwa lub inne właściwe organy krajowe są odpowiedzialne za zapewnienie by przeprowadzono postępowanie sprawdzające w odniesieniu do tych obywateli ich państwa, którym niezbędny jest dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej. Normy postępowania sprawdzającego mają być zgodne z przepisami krajowymi zarówno rangi ustawowej, jak i wykonawczymi[19]. W celu wydania określonej osobie poświadczenia bezpieczeństwa osobowego upoważniającego ją do dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL sprawdza się jej lojalność, wiarygodność i rzetelność przeprowadzając postępowanie sprawdzające i na podstawie jego wyników właściwy organ krajowy dokonuje ogólnej oceny. Pojedyncza, niekorzystna informacja otrzymana w wyniku postępowania nie musi jednak skutkować odmową wydania poświadczenia. Załącznik I do decyzji precyzuje, jakie kryteria winny być stosowane, aby umożliwić sprawdzenie czy określona osoba winna uzyskać poświadczenie bezpieczeństwa osobowego[20].

---

[19] W sytuacji, gdy miejsce pobytu sprawdzanej osoby znajduje się na terytorium innego Państwa Członkowskiego lub państwa trzeciego właściwe organy krajowe zwracają się o pomoc do odpowiedniego państwa pobytu, przy czym państwa członkowskie mają obowiązek wspierać się w prowadzeniu postępowań sprawdzających zgodnie z ustanowionymi przepisami. Jeżeli krajowe przepisy ustawowe i wykonawcze dopuszczają taką możliwość krajowe władze bezpieczeństwa lub inne właściwe organy krajowe mogą przeprowadzać postępowania sprawdzające w odniesieniu do osób niebędących obywatelami ich państwa, którym niezbędny jest dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej.

[20] Wskazano w ustawie, że konieczne jest ustalenie czy osoba ta: popełniła lub usiłowała popełnić akt szpiegostwa, terroryzmu, sabotażu, zdrady lub buntu, współdziałała z inną osobą w celu popełnienia takiego aktu, pomagała innej osobie w jego popełnieniu lub nakłaniała inne osoby do popełnienia takiego aktu; współdziała lub współdziałała ze szpiegami, terrorystami, sabotażystami lub osobami, co do których istnieje uzasadnione podejrzenie, że nimi są, lub z przedstawicielami organizacji lub obcych państw, w tym obcych służb wywiadowczych, które mogą stanowić zagrożenie dla bezpieczeństwa UE lub państw członkowskich, chyba że udzielono zezwolenia na takie współdziałanie w ramach obowiązków służbowych; jest lub była członkiem organizacji, która za pomocą aktów przemocy, działalności wywrotowej lub innych nielegalnych środków dąży m.in. do obalenia rządu państwa członkowskiego, zmiany porządku konstytucyjnego państwa członkowskiego lub zmiany formy lub polityki jego rządu; jest lub była stronnikiem jakiejkolwiek z takich organizacji lub blisko współdziałała z członkami takich organizacji; świadomie zataiła, fałszywie przedstawiła lub sfałszowała istotne informacje, szczególnie informacje związane z bezpieczeństwem, lub świadomie skłamała przy wypełnianiu ankiety bezpieczeństwa osobowego lub podczas rozmowy przeprowadzanej w ramach postępowania sprawdzającego; została skazana za popełnienie przestępstwa lub przestępstw; kiedykolwiek była uzależniona od alkoholu, zażywała nielegalne środki odurzające lub nadużywała legalnych środków odurzających; zachowuje się lub zachowywała w sposób mogący stwarzać ryzyko podatności na szantaż lub presję; w czynach lub słowach wykazała się nieuczciwością, nielojalnością, brakiem rzetelności lub wiarygodności; poważnie lub wielokrotnie naruszyła przepisy dotyczące bezpieczeństwa lub usiłowała dokonać albo dokonała czynności, do których nie była uprawniona, w odniesieniu do systemów teleinformatycznych; może podlegać presji (np. poprzez posiadanie jednego lub więcej obywatelstw państw niebędących członkiem UE lub presji krewnych lub bliskich współpracowników, którzy mogą być podatni na wpływy obcych służb wywiadowczych,

W załączniku I decyzji sformułowano także wymogi dotyczące postępowania sprawdzającego na potrzeby dostępu do Sieci EUCI. Stwierdzono, że pierwsze poświadczenie bezpieczeństwa osobowego upoważniające do dostępu do informacji niejawnych o klauzulach: CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET wydawane jest po przeprowadzeniu postępowania sprawdzającego, obejmującego okres ostatnich pięciu lat lub okres od ukończenia 18. roku życia do chwili obecnej, w zależności od tego, który z tych okresów jest krótszy. Określono też co obejmują tego rodzaju sprawdzenia[21].

Pierwsze poświadczenie bezpieczeństwa osobowego upoważniające do dostępu do informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET wydawane jest po przeprowadzeniu postępowania sprawdzającego obejmującego co najmniej okres ostatnich dziesięciu lat lub okres od ukończenia 18. roku życia do chwili obecnej, w zależności od tego, który z tych okresów jest krótszy. Jeżeli w procedurze tej przeprowadzane są rozmowy, postępowanie sprawdzające obejmuje co najmniej okres ostatnich siedmiu lat lub okres od ukończenia 18. roku życia do chwili obecnej, w zależności od tego, który okres jest krótszy. Poza kryteriami oznaczonymi jako główne kryteria przed wydaniem PBO upoważniającego do dostępu do informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET należy wyjaśnić – w zakresie, w jakim umożliwiają to krajowe przepisy ustawowe i wykonawcze także inne okoliczności[22].

---

grup terrorystycznych lub innych wywrotowych organizacji lub osób mogących zagrażać interesom bezpieczeństwa UE lub państw członkowskich). W decyzji podkreślono także, że w odpowiednich przypadkach oraz zgodnie z krajowymi przepisami ustawowymi i wykonawczymi podczas przeprowadzania postępowania sprawdzającego za istotną można uznać także sytuację finansową i zdrowotną danej osoby, a także charakter, zachowanie i sytuację jej współmałżonka, partnera życiowego lub członka bliskiej rodziny.

[21] Wskazano, że należy do niego wypełnienie krajowej ankiety bezpieczeństwa osobowego do odpowiedniego poziomu EUCI, do których dostęp może być niezbędny danej osobie; wypełniona ankieta przekazywana jest właściwemu organowi bezpieczeństwa; sprawdzenie tożsamości/obywatelstwa/narodowości, w ramach czego potwierdza się datę i miejsce urodzenia danej osoby i sprawdza się jej tożsamość. Ustala się przeszłe i obecne obywatelstwo lub narodowość danej osoby; obejmuje to ocenę podatności na presję wywieraną przez osoby z zagranicy, na przykład w związku z poprzednim miejscem pobytu lub przeszłymi powiązaniami; oraz sprawdzenie rejestrów krajowych i lokalnych, w ramach którego sprawdzane są krajowe rejestry bezpieczeństwa i centralne rejestry karne, o ile te ostatnie istnieją, lub inne porównywalne rejestry rządowe i policyjne. Sprawdza się rejestry organów ścigania sprawujących jurysdykcję w miejscach, w których dana osoba miała miejsce pobytu lub była zatrudniona.

[22] Do okoliczności tych należą: status finansowy – poszukuje się informacji dotyczących sytuacji finansowej danej osoby, aby ocenić stopień jej podatności na presję osób z kraju lub z zagranicy z powodu poważnych trudności finansowych lub aby ujawnić wszelkie przychody z nieznanych źródeł; wykształcenie – poszukuje się informacji służących weryfikacji wykształcenia danej osoby w szkołach, szkołach wyższych lub innych placówkach edukacyjnych, do których uczęszczała ona od ukończenia 18. roku życia lub w okresie, który organ prowadzący postępowanie sprawdzające uzna za odpowiedni; zatrudnienie – poszukuje się informacji dotyczących obecnego i poprzedniego zatrudnienia, przy wykorzystaniu takich źródeł jak historia zatrudnienia, sprawozdania dotyczące wyników lub wydajności pracy oraz opinie pracodawców lub przełożonych; służba wojskowa – w stosownych przypadkach weryfikowany jest stosunek danej osoby do służby wojskowej oraz powód zwolnienia ze służby. Z osobą taką, jeśli przepisy krajowe przewidują i dopuszczają taką możliwość, przeprowadza się rozmowę lub rozmowy. Rozmowy przeprowadza się również z innymi osobami, które są

W decyzji przewidziano także zasady przedłużenia ważności poświadczenia bezpieczeństwa osobowego wskazując, że po wydaniu pierwszego PBO oraz pod warunkiem, że w zatrudnieniu danej osoby w administracji krajowej lub w SGR nie wystąpiły przerwy, a dostęp do EUCI jest jej stale potrzebny, przedłużenie ważności PBO tej osoby rozpatrywane jest w odstępach czasu nie przekraczających pięciu lat w przypadku poświadczenia do klauzuli tajności TRÈS SECRET UE/EU TOP SECRET oraz dziesięciu lat w przypadku poświadczeń do klauzul tajności SECRET UE/EU SECRET i CONFIDENTIEL UE/EU CONFIDENTIAL, licząc od daty powiadomienia o wyniku ostatniego postępowania sprawdzającego, na podstawie którego zostały wydane te poświadczenia. Wszelkie postępowania sprawdzające dotyczące przedłużenia ważności PBO obejmują okres od poprzedniego postępowania. Wnioski o przedłużenie ważności składane być winne z odpowiednim wyprzedzeniem, z uwzględnieniem czasu wymaganego do przeprowadzenia postępowań sprawdzających. Jeżeli jednak odpowiednia KWB lub inny właściwy organ krajowy otrzymały odpowiedni wniosek o przedłużenie ważności oraz właściwą ankietę bezpieczeństwa osobowego, zanim PBO utraciło ważność, a niezbędne postępowanie sprawdzające nie zostało jeszcze zakończone, właściwy organ krajowy może przedłużyć ważność obowiązującego PBO o okres nieprzekraczający 12 miesięcy, jeżeli dopuszczają to krajowe przepisy ustawowe i wykonawcze. Jeżeli na koniec tego 12-miesięcznego okresu nadal nie zakończono postępowania sprawdzającego, danej osobie przyznaje się obowiązki, które nie wymagają posiadania PBO. W przypadku urzędników i innych pracowników SGR organ bezpieczeństwa SGR przekazuje wypełnioną ankietę bezpieczeństwa osobowego KWB państwa członkowskiego, którego obywatelem jest dana osoba, z wnioskiem o przeprowadzenie postępowania sprawdzającego do poziomu EUCI, do którego dostęp będzie tej osobie niezbędny. Po zakończeniu postępowania sprawdzającego odpowiednia krajowa władza bezpieczeństwa powiadamia organ bezpieczeństwa Sekretariatu Generalnego Rady o wyniku takiego postępowania[23].

Postępowanie sprawdzające oraz jego wyniki podlegają odpowiednim przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim,

---

w stanie przedstawić obiektywną ocenę dotyczącą pochodzenia, działalności, lojalności, wiarygodności i rzetelności osoby sprawdzanej. W przypadku, gdy krajowa praktyka przewiduje przedstawianie referencji przez osobę sprawdzaną, przeprowadza się rozmowę z osobami, które dostarczyły tych referencji, chyba że istnieją uzasadnione powody, żeby tego nie czynić. Jeżeli jest to konieczne i zgodne z krajowymi przepisami ustawodawczymi i wykonawczymi, można przeprowadzić dodatkowe wyjaśnienia w celu rozwinięcia wszelkich dostępnych istotnych informacji dotyczących danej osoby oraz w celu potwierdzenia lub wykazania fałszywości informacji działających na niekorzyść osoby sprawdzanej. Por.: pkt 12–13 załącznika I do decyzji Rady z 31 marca 2011 roku.

[23] Jeżeli w wyniku postępowania sprawdzającego uzyskuje się pewność, że nie istnieją żadne niekorzystne okoliczności, które mogłyby podważać lojalność, wiarygodność i rzetelność danej osoby, organ powołujący SGR może wydać tej osobie PBO UE oraz upoważnić ją do dostępu do EUCI do odpowiedniego poziomu i do określonej daty. Jeżeli w wyniku postępowania sprawdzającego nie uzyskuje się takiej pewności, organ powołujący SGR powiadamia o tym fakcie daną osobę, a ona może się do niego zwrócić z prośbą o wysłuchanie. Organ powołujący może zwrócić się do właściwej KWB o przedstawienie wszelkich dalszych wyjaśnień, których organ ten może udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli wynik zostanie potwierdzony, nie wydaje się PBO UE. Por.: pkt 19 załącznika I.

w tym także przepisom dotyczącym środków odwoławczych. Decyzje organu powołującego SGR podlegają środkom odwoławczym zgodnie z regulaminem pracowniczym urzędników Unii Europejskiej[24] i Warunkami zatrudnienia innych pracowników Unii Europejskiej[25], określonymi w rozporządzeniu (EWG, Euratom, EWWiS) nr 259/68[26]. Poświadczenie bezpieczeństwa osobowego odnosi się do każdego zadania powierzonego danej osobie w Sekretariacie Generalnym Rady lub Komisji[27]. Państwa Członkowskie i Sekretariat Generalny Rady mają obowiązek przechowywania wykazów krajowych poświadczenia bezpieczeństwa osobowego i poświadczenia bezpieczeństwa osobowego UE. Wykazy te mają zawierać informacje o poziomie klauzuli tajności EUCI oraz dacie wydania takiego poświadczenia i okresie jego ważności[28]. W decyzji przewidziano także okoliczności zwolnienia z posiadania poświadczenia bezpieczeństwa osobowego ze względu na pełnione funkcje w państwach członkowskich zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Osoby takie należy jednak poinformować o spoczywających na nich obowiązkach dotyczących bezpieczeństwa polegających na ochronie informacji niejawnych UE. Zresztą wszystkie osoby, którym wydano poświadczenie bezpieczeństwa, oświadczają na piśmie, że zrozumiały spoczy-

---

[24] Regulamin pracowniczy urzędników Unii Europejskiej, Dz. Urz. UE L 68, nr 56 1/1.

[25] Warunki zatrudnienia innych pracowników Unii Europejskiej, Dz. Urz. UE L 68, nr 56 1/2.

[26] Dz. Urz. UE L 56, 4.03.1968.

[27] Jeżeli okres wykonywania przez daną osobę obowiązków służbowych nie rozpocznie się w terminie 12 miesięcy od powiadomienia organu powołującego SGR o wyniku postępowania sprawdzającego lub jeżeli w pełnieniu obowiązków przez daną osobę występuje 12-miesięczna przerwa, w czasie której osoba ta nie jest zatrudniona w SGR ani na żadnym stanowisku w administracji krajowej państwa członkowskiego, wynik postępowania sprawdzającego jest przekazywany odpowiedniej KWB w celu potwierdzenia, czy nadal pozostaje ważny i właściwy. Jeżeli SGR znajdzie się w posiadaniu informacji o ryzyku naruszenia zasad bezpieczeństwa przez osobę, która posiada ważne PBO UE, powiadamia o tym odpowiednią KWB, działając zgodnie z odpowiednimi zasadami i przepisami wykonawczymi. Jeżeli KWB powiadomi SGR o utracie pewności uzyskanej zgodnie z pkt 19 lit. a) w odniesieniu do osoby posiadającej ważne PBO UE, organ powołujący SGR może zwrócić się do KWB o przedstawienie wszelkich dalszych wyjaśnień, których organ ten może udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli niekorzystne informacje zostaną potwierdzone, PBO UE zostaje cofnięte, a osobie takiej odbiera się prawo dostępu do EUCI i odsuwa się ją od stanowisk, na których taki dostęp jest możliwy lub na których osoba ta mogłaby zagrażać bezpieczeństwu. O każdej decyzji w sprawie cofnięcia PBO UE przyznanego urzędnikowi lub innemu pracownikowi SGR i, w odpowiednich przypadkach, o przyczynach tego cofnięcia powiadamia się daną osobę, a ona może zwrócić się do organu powołującego z prośbą o wysłuchanie. Informacje przedstawione przez KWB podlegają odpowiednim przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim, w tym także przepisom dotyczącym środków odwoławczych. Decyzje organu powołującego SGR podlegają środkom odwoławczym zgodnie z regulaminem pracowniczym i warunkami zatrudnienia. Eksperci krajowi oddelegowani do SGR na stanowisko wymagające PBO UE przedstawiają organowi bezpieczeństwa SGR – przed rozpoczęciem wykonywania swoich zadań – ważne krajowe PBO uprawniające do dostępu do EUCI. Por.: pkt 22–25 załącznika I decyzji z 31 marca 2011 roku.

[28] Właściwy organ bezpieczeństwa może wydać zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego (ZPBO) zawierające informacje o poziomie klauzuli tajności EUCI, do których dana osoba może mieć dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), okresie ważności odpowiedniego krajowego PBO umożliwiającego dostęp do EUCI lub PBO UE oraz dacie ważności samego zaświadczenia. Por.: pkt 27 załącznika I decyzji z 31 marca 2011 roku.

wające na nich obowiązki w zakresie ochrony EUCI i konsekwencje narażenia na szwank bezpieczeństwa EUCI. Wykaz pisemnych oświadczeń przechowywany jest, odpowiednio, przez państwo członkowskie i przez SGR. Wszystkie osoby, które są upoważnione do dostępu do EUCI lub muszą wykorzystywać te informacje, na początku powiadamiane są o zagrożeniach bezpieczeństwa, a następnie regularnie szkolone w zakresie tych zagrożeń. Osoby te muszą bezzwłocznie zgłaszać właściwym organom bezpieczeństwa wszelkie zdarzenia lub wszelką działalność, które uznają za podejrzane lub nietypowe. Wszystkie osoby, które przestają wykonywać obowiązki wymagające dostępu do EUCI, powiadamiane są o obowiązku stałej ochrony EUCI; w odpowiednich przypadkach świadomość tego obowiązku potwierdzają one na piśmie[29]. W szczególnie wyjątkowych okolicznościach, takich jak misje prowadzone we wrogim środowisku lub w okresie rosnącego napięcia międzynarodowego, i gdy wymagają tego środki nadzwyczajne, w szczególności w celu ratowania życia ludzkiego, państwa członkowskie i Sekretarz Generalny mogą udzielić, w miarę możliwości na piśmie, dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET osobom, które nie posiadają wymaganego PBO pod warunkiem, że takie zezwolenie jest absolutnie niezbędne i nie ma żadnych uzasadnionych wątpliwości co do lojalności, wiarygodności i rzetelności danej osoby. Zachowuje się dokumentację takiego zezwolenia zawierającą opis informacji, do których dostęp zatwierdzono.

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, a także powstrzymanie od podjęcia nieuprawnionych działań, udaremnienie ich i wykrycie oraz umożliwienie podziału pracowników pod względem dostępu do informacji niejawnych zgodnie

---

[29] W nagłych przypadkach, jeżeli jest to należycie uzasadnione interesami jednostki organizacyjnej, w oczekiwaniu na zakończenie pełnego postępowania sprawdzającego organ powołujący SGR może, po konsultacji z KWB państwa członkowskiego, którego obywatelem jest dana osoba, oraz z zastrzeżeniem, że wynik wstępnego sprawdzenia nie wykazał niekorzystnych informacji, wydać urzędnikom i innym pracownikom SGR tymczasowe upoważnienie do dostępu do EUCI, by mogli wykonać określone zadania. Takie tymczasowe upoważnienia zachowują ważność przez okres nieprzekraczający sześciu miesięcy i nie uprawniają do dostępu do informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET. Wszystkie osoby, którym przyznano tymczasowe upoważnienie, oświadczają na piśmie, że zrozumiały spoczywające na nich obowiązki w zakresie ochrony EUCI i konsekwencje narażenia na szwank bezpieczeństwa EUCI. Wykaz takich pisemnych oświadczeń przechowywany jest przez SGR. Jeżeli dana osoba ma objąć stanowisko, które wymaga PBO na poziomie o jeden wyższym niż aktualnie posiadany przez nią, może ona tymczasowo pełnić obowiązki związane z tym stanowiskiem pod warunkiem, że: bezwzględna potrzeba dostępu do EUCI o wyższej klauzuli tajności jest uzasadniona na piśmie przez przełożonego tej osoby; dostęp jest ograniczony do konkretnych EUCI, które są potrzebne do pracy na tym stanowisku; osoba ta posiada ważne krajowe PBO lub PBO UE; podjęto czynności w celu uzyskania upoważnienia do dostępu do informacji na poziomie wymaganym na tym stanowisku; właściwy organ dokonał sprawdzenia, które potwierdziło, że dana osoba nie naruszała poważnie ani wielokrotnie przepisów dotyczących bezpieczeństwa; objęcie tego stanowiska przez daną osobę zatwierdził właściwy organ; oraz dokumentacja dotycząca przyznania dostępu w drodze wyjątku, wraz z opisem informacji, do których zatwierdzono dostęp, przechowywana jest w odpowiedzialnej kancelarii tajnej lub podległej kancelarii tajnej.

z zasadą ograniczonego dostępu. Środki te określane są na podstawie procesu zarządzania ryzykiem. Środkami bezpieczeństwa fizycznego obejmuje się 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[30]. Środki bezpieczeństwa fizycznego dobiera się na podstawie oceny zagrożenia przeprowadzonej przez właściwe organy. SGR i państwa członkowskie stosują w swoich obiektach proces zarządzania ryzykiem służący ochronie EUCI, aby zapewnić poziom ochrony fizycznej proporcjonalny do szacowanego ryzyka[31]. W załączniku do decyzji ustanowiono dwa rodzaje stref chronionych fizycznie lub ich krajowych odpowiedników służących fizycznej ochronie EUCI, a mianowicie: strefy administracyjne oraz strefy bezpieczeństwa, w tym strefy technicznie zabezpieczone. Właściwy organ bezpieczeństwa stwierdza czy dana strefa spełnia wymogi potrzebne do uznania jej za strefę administracyjną lub strefę bezpieczeństwa, względnie strefę technicznie zabezpieczoną[32]. W załączniku do decyzji zawarowano przy tym, że sfery bezpieczeństwa

---

[30] Strefy, w których przechowywane są EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, ustanawiane są strefami bezpieczeństwa zgodnie z załącznikiem II; strefy takie zatwierdza właściwy organ bezpieczeństwa. Do ochrony EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej stosuje się wyłącznie zatwierdzony sprzęt lub zatwierdzone urządzenia. Por.: art. 8 ust. 4 i 5 decyzji z 31 marca 2011 roku.

[31] Stosując środki bezpieczeństwa fizycznego należy w szczególności uwzględniać klauzulę tajności EUCI; postać i ilość EUCI, z uwzględnieniem faktu, że duża ilość EUCI lub ich kompilacja mogą wymagać zastosowania bardziej rygorystycznych środków ochrony; otoczenie i strukturę budynków lub stref, w których znajdują się EUCI; oraz szacowane zagrożenie ze strony służb wywiadowczych, których celem jest UE lub państwa członkowskie, oraz zagrożenie sabotażem, terroryzmem, działalnością wywrotową lub inną działalnością przestępczą. Stosując koncepcję ochrony w głąb, właściwy organ bezpieczeństwa określa właściwą kombinację środków bezpieczeństwa fizycznego, które należy zastosować. 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 (SSWiN): SSWiN można stosować 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 (CCTV): CCTV może być stosowana przez pracowników ochrony w celu sprawdzania incydentów i sygnałów alarmowych pochodzących z SSWiN 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 CCTV; oraz wszelkie inne stosowne środki fizyczne służące powstrzymywaniu lub wykrywaniu przypadków nieuprawnionego dostępu lub zapobieganiu utracie EUCI lub narażeniu na szwank ich bezpieczeństwa. Przewidziano także w ustawie możliwość przeszukania osób wchodzących i wychodzących przez właściwy organ, co – jak stwierdzono – ma stanowić środek odstraszający przed nieuprawnionym wnoszeniem materiałów lub nieuprawnionym wynoszeniem EUCI z obiektów lub budynków. Zob.: pkt 3 załącznika II do decyzji z 31 marca 2011 roku.

[32] W załączniku II do decyzji z 31 marca 2011 roku stwierdzono, że w przypadku stref administracyjnych: wyraźnie określa się granicę umożliwiającą kontrolę osób i, jeżeli to możliwe, pojazdów;

oraz sfery technicznie zabezpieczone mogą być tworzone tymczasowo na terenie stref administracyjnych w celu zorganizowania niejawnego posiedzenia lub w jakimkolwiek innym podobnym celu. Jednocześnie ustalono, że dla każdej sfery bezpieczeństwa należy opracować procedury bezpiecznej eksploatacji[33]. W załączniku II stwierdzono, że wykorzystywanie EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED może się odbywać: w strefie bezpieczeństwa; w strefie administracyjnej pod warunkiem, że EUCI są chronione przed dostępem osób nieupoważnionych; lub poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz przewozi EUCI i zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez właściwy organ bezpieczeństwa służących zapewnieniu, aby nieupoważnione osoby nie miały dostępu do EUCI. EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED przechowywane są w odpowiednim do tego celu zamkniętym meblu biurowym w strefie administracyjnej lub strefie bezpieczeństwa.

---

dostęp bez eskorty umożliwia się tylko osobom, które są odpowiednio upoważnione przez właściwy organ; oraz wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równorzędnej kontroli. W przypadku stref bezpieczeństwa: wyraźnie określa się i chroni granicę, na której wszelkie wejścia i wyjścia kontrolowane są za pomocą przepustki lub systemu rozpoznawania osób; dostęp bez eskorty umożliwia się tylko osobom odpowiednio sprawdzonym i wyraźnie upoważnionym do wejścia do danej strefy zgodnie z zasadą ograniczonego dostępu; wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równorzędnej kontroli. Jeżeli wejście do strefy bezpieczeństwa jest w praktyce równoznaczne z bezpośrednim dostępem do informacji niejawnych znajdujących się w tej strefie, zastosowanie mają następujące dodatkowe wymogi: wyraźnie wskazuje się najwyższą klauzulę tajności, którą przyznano informacjom zwykle przechowywanym w tej strefie; wszystkie osoby wchodzące do tej strefy muszą posiadać specjalne upoważnienie do wejścia do tej strefy, przez cały czas towarzyszyć im musi eskorta i muszą być odpowiednio sprawdzone, chyba że podjęte zostały kroki służące zapewnieniu, aby nie był możliwy dostęp do EUCI. Strefy bezpieczeństwa chronione przed podsłuchem uznawane są za strefy technicznie zabezpieczone. Zastosowanie mają następujące dodatkowe wymogi: strefy takie wyposażone są w SSWiN, są zamknięte na klucz, gdy nikt w nich nie przebywa, i chronione, gdy ktoś w nich przebywa. Wszystkie klucze podlegają kontroli zgodnie z sekcją VI; wszystkie osoby wchodzące do takich stref lub materiały tam wnoszone podlegają kontroli; strefy takie podlegają regularnym inspekcjom fizycznym lub technicznym zgodnie z wymogami właściwego organu bezpieczeństwa. Inspekcje takie przeprowadza się także po każdorazowym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście miało miejsce; oraz w strefach takich nie mogą się znajdować niezatwierdzone linie komunikacyjne, niezatwierdzone telefony, inne niezatwierdzone urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny. W ramach stref bezpieczeństwa są budowane wzmocnione pomieszczenia. Ściany, podłogi, sufity, okna i wyposażone w zamek drzwi zatwierdzane są przez właściwy organ bezpieczeństwa i zapewniają ochronę równoważną zabezpieczonym szafom zatwierdzonym do celów przechowywania EUCI o tym samym poziomie klauzuli tajności. Por.: pkt 14–17 i 22 załącznika II do decyzji z 31 marca 2011roku.

[33] Winny one określić: poziom klauzuli tajności EUCI, które można wykorzystywać i przechowywać w tej strefie; środki nadzoru i ochrony, które należy stosować; osoby upoważnione do wejścia do strefy bez eskorty ze względu na zasadę ograniczonego dostępu i posiadane poświadczenie bezpieczeństwa; w odpowiednich przypadkach, procedury dotyczące eskort lub ochrony EUCI, jeżeli zezwala się na wejście do strefy innym osobom; wszelkie inne odpowiednie środki i procedury. W ramach sfer bezpieczeństwa winny być budowane wzmocnione pomieszczenia. W dość kazuistycznym w swej treści załączniku II podkreślono, że ściany, podłogi, sufity, okna i wyposażone w zamek drzwi winny być zatwierdzane przez właściwy organ bezpieczeństwa i zapewniać ochronę równoważną zabezpieczonym szafom, zatwierdzonym do przechowywania europejskich informacji niejawnych. Por.: pkt 21 i 22 załącznika II decyzji z 31 marca 2011 roku.

Mogą być one tymczasowo przechowywane poza strefą bezpieczeństwa lub strefą administracyjną pod warunkiem, że posiadacz zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez właściwy organ bezpieczeństwa. EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET przechowywane są w strefie bezpieczeństwa w zabezpieczonej szafie lub wzmocnionym pomieszczeniu[34]. Wykorzystywanie EUCI o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET odbywa się w strefie bezpieczeństwa[35]. W załączniku szczegółowo opisano także zasady kontroli kluczy i kodów wykorzystywanych do ochrony sieci EUCI[36].

W treści art. 9 decyzji uregulowano problem zarządzania informacjami niejawnymi wskazując, że polega ono na stosowaniu środków administracyjnych służących kontroli EUCI na wszystkich etapach ich cyklu życia w uzupełnieniu środków przewidzianych w art. 7, 8 i 10, co ma pomóc w powstrzymywaniu od zamierzonego lub przypadkowego narażenia na szwank bezpieczeństwa tych informacji lub ich utraty, w wykrywaniu takich przypadków i usuwaniu ich skutków. Środki takie dotyczą w szczególności wytwarzania, rejestracji, kopiowania, tłumaczenia, przewożenia i niszczenia EUCI. Informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej są ze względów bezpieczeństwa rejestrowane przed dystrybucją i w momencie wpłynięcia. Właściwe organy SGR i państw członkowskich ustanawiają do tego celu system kancelarii tajnych. Informacje niejawne o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET rejestruje się w wyznaczonych kancelariach tajnych. Jednostki organizacyjne i obiekty, w których są wykorzystywane lub przechowywane EUCI, poddawane są regularnym inspekcjom przeprowadzanym przez właściwy organ bezpieczeństwa. Poza strefami chronionymi fizycznie EUCI są przekazywane między jednostkami organizacyjnymi i obiektami w sposób następujący:

---

[34] Wykorzystywanie EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET może się odbywać: w strefie bezpieczeństwa; w strefie administracyjnej pod warunkiem, że EUCI są chronione przed dostępem osób nieupoważnionych; lub poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz: przewozi EUCI zgodnie z zasadami wynikającymi z załącznika; zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez właściwy organ bezpieczeństwa służących zapewnieniu, aby nieupoważnione osoby nie miały dostępu do EUCI; przechowuje EUCI przez cały czas pod swoją kontrolą; oraz w przypadku dokumentów w formie papierowej – powiadomił o tym fakcie właściwą kancelarię tajną. Por.: pkt 25 załącznika II decyzji z 31 marca 2011 roku.

[35] EUCI o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET przechowywane są w strefie bezpieczeństwa, przy spełnieniu jednego z następujących warunków: są one przechowywane w zabezpieczonej szafie, wyposażonej w co najmniej jedno z następujących zabezpieczeń dodatkowych: stała ochrona lub kontrola przez odpowiednio sprawdzonych pracowników ochrony lub pracowników pełniących dyżur; zatwierdzony SSWiN obsługiwany przez pracowników ochrony odpowiedzialnych za bezpieczeństwo; lub są one przechowywane we wzmocnionym pomieszczeniu wyposażonym w SSWiN oraz obsługiwanym przez pracowników ochrony odpowiedzialnych za bezpieczeństwo. Por.: pkt 28 załącznika II decyzji z 31 marca 2011 roku.

[36] Kody są zapamiętywane przez jak najmniejszą liczbę osób, którym ich znajomość jest niezbędna. Kody do zabezpieczonych szaf i wzmocnionych pomieszczeń, w których przechowywane są EUCI, są zmieniane: przy każdej zmianie pracowników znających kod; w każdym przypadku, gdy następuje rzeczywiste lub domniemane narażenie na szwank bezpieczeństwa informacji; gdy zamek poddano konserwacji lub naprawie; oraz co najmniej co 12 miesięcy. Por.: pkt 31 załącznika II decyzji z 31 marca 2011 roku.

z reguły EUCI są przekazywane drogą elektroniczną chronioną przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 10 ust. 6 decyzji. EUCI są przekazywane: za pomocą środków elektronicznych (jak np. pamięć USB, płyty kompaktowe, twarde dyski) – chronionych przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 10 ust. 6 decyzji; albo we wszystkich pozostałych przypadkach, zgodnie z wytycznymi właściwego organu bezpieczeństwa. Szczegółowe kwestie odnoszące się do zarządzania informacjami niejawnymi uregulowano w załączniku III do decyzji[37].

W treści bardzo szczegółowego art. 10 decyzji uregulowano sprawy ochrony EUCI przetwarzanych w systemach teleinformatycznych. „System teleinformatyczny" (CIS) oznacza w myśl tego przepisu system umożliwiający przetwarzanie informacji w formie elektronicznej. Zabezpieczanie informacji w ramach systemów teleinformatycznych ma stworzyć sytuację, w której systemy te będą chronić informacje, które są przez nie przetwarzane, i będą działać zgodnie z przeznaczeniem, w razie potrzeby pod kontrolą uprawnionych użytkowników. Skuteczne zabezpieczanie informacji winno zagwarantować odpowiedni poziom poufności, integralności, dostępności, niezaprzeczalności i autentyczności. Zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem. Systemy teleinformatyczne przetwarzają informacje niejawne UE zgodnie z koncepcją zabezpieczenia informacji. Wszystkie CIS poddawane są procedurze akredytacji. Celem akredytacji jest upewnienie się, że zastosowano wszystkie odpowiednie środki bezpieczeństwa i że osiągnięto wystarczający poziom ochrony EUCI i CIS zgodnie z niniejszą decyzją. W świadectwie akredytacji określa się najwyższą klauzulę tajności informacji, które mogą być przetwarzane w ramach danego CIS, oraz odpowiednie warunki. CIS przetwarzające informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i wyższej są chronione w taki sposób, by bezpieczeństwo informacji nie mogło zostać narażone na szwank z powodu niezamierzonych emisji elektromagnetycznych („środki bezpieczeństwa TEMPEST"). Jeżeli EUCI podlegają ochronie przy użyciu produktów kryptograficznych, produkty te są zatwierdzane w sposób następujący: poufność informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET i wyższej podlega ochronie przy użyciu produktów kryptograficznych zatwierdzonych – na podstawie zalecenia Komitetu ds. Bezpieczeństwa – przez Radę działającą jako organ ds. zatwierdzania produktów kryptograficznych (CAA); poufność

---

[37] Załącznik III składa się z 62 punktów i zawiera kazuistyczne przepisy dotyczące wprowadzenia w życie art. 9 decyzji. Określa on środki administracyjne służące kontroli EUCI na wszystkich etapach ich cyklu życia, co ma pomóc w powstrzymywaniu od zamierzonego lub przypadkowego narażenia na szwank bezpieczeństwa takich informacji lub ich utraty, w wykrywaniu takich przypadków i usuwaniu ich skutków. W treści załącznika uregulowano kwestie dotyczące klauzul tajności i dodatkowych oznaczeń, zasady wytwarzania EUCI, obniżanie i znoszenie klauzul tajności, sprawy odnoszące się do kopiowania i tłumaczenia dokumentów niejawnych, przewożenia EUCI w obrębie budynku, na terytorium Unii Europejskiej, z terytorium Unii na terytorium państwa trzeciego, a także sprawy inspekcji i wizyt oceniających. Warto w tym miejscu zauważyć, że przy wytwarzaniu dokumentu niejawnego, w myśl pkt 13 załącznika III: każdą stronę wyraźnie oznacza się klauzulą tajności; strony numeruje się; na dokumencie umieszcza się numer referencyjny i temat, który nie stanowi informacji niejawnej chyba, że z jego oznaczenia wynika inaczej; na dokumencie umieszcza się datę; na każdej stronie dokumentów o klauzuli tajności SECRET UE/EU SECRET lub wyższej, które mają zostać rozpowszechnione w kilku kopiach, umieszcza się numer kopii.

informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub RESTREINT UE/EU RESTRICTED podlega ochronie przy użyciu produktów kryptograficznych zatwierdzonych – na podstawie zalecenia Komitetu ds. Bezpieczeństwa – przez Sekretarza Generalnego Rady działającego jako CAA. Niezależnie od tego w obrębie krajowych systemów państw członkowskich poufność EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub RESTREINT UE/EU RESTRICTED może być chroniona przy użyciu produktów kryptograficznych zatwierdzonych przez CAA danego państwa członkowskiego. Podczas transmisji EUCI drogą elektroniczną stosuje się zatwierdzone produkty kryptograficzne. Niezależnie od tego wymogu w wyjątkowych okolicznościach mogą mieć zastosowanie szczególne procedury lub szczególne konfiguracje techniczne[38]. W myśl art. 10 ust. 8 właściwe organy Sekretariatu Generalnego Rady i państw członkowskich zostały zobowiązane do ustanowienia odpowiednich organów zajmujących się zabezpieczeniem informacji, a mianowicie: organu ds. zabezpieczenia informacji (IAA)[39]; organu ds. środków bezpieczeństwa TEMPEST (TA)[40]; organu ds. zatwierdzania produktów kryptograficznych (CAA)[41]

---

[38] Sprawy te uregulowano w załączniku IV decyzji, poświęconemu ochronie EUCI przetwarzanych w CIS. W jego treści, składającej się z 51 punktów, uregulowano sprawy zasad zabezpieczenia informacji, zarządzanie ryzykiem dla bezpieczeństwa, problem transmisji w sferze bezpieczeństwa, bezpiecznych połączeń międzysystemowych, komputerowych nośników informacji, funkcjonowanie organów do spraw zabezpieczenia informacji, zatwierdzania produktów kryptograficznych, sprawę dystrybucji takich produktów, akredytacji bezpieczeństwa oraz funkcjonowanie operacyjnych organów ds. zabezpieczenia informacji. Godzi się wskazać, że definiując tzw. ochronę wgłąb postanowiono wdrożyć pakiet technicznych i innych środków bezpieczeństwa o strukturze różnych poziomów ochrony. Poziomy te obejmują: powstrzymywanie: środki bezpieczeństwa ukierunkowane na zniechęcenie osób planujących atak na CIS; zapobieganie: środki bezpieczeństwa ukierunkowane na udaremnienie lub powstrzymanie ataku na CIS; wykrywanie: środki bezpieczeństwa ukierunkowane na ujawnienie ataku na CIS; odporność: środki bezpieczeństwa ukierunkowane na ograniczenie skutków ataku, tak by dotknęły one jak najmniejszą ilość informacji lub zasobów CIS, oraz na zapobieżenie dalszym szkodom; oraz usuwanie skutków: środki bezpieczeństwa ukierunkowane na odzyskanie bezpiecznego statusu CIS. Por.: pkt 16 załącznika IV decyzji z 31 marca 2011 roku.

[39] Organ ds. zabezpieczania informacji (IAA) 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 EUCI były zgodne z odpowiednimi politykami dotyczącymi kryteriów ich przydatności i wyboru; 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; oraz zapewnianie odpowiedniej wiedzy fachowej na temat zabezpieczania informacji w podgrupie eksperckiej Komitetu ds. Bezpieczeństwa. Por.: pkt 43 załącznika IV decyzji z 31 marca 2011 roku.

[40] Organ ds. TEMPEST (TA) odpowiada za zapewnienie zgodności CIS z politykami i wytycznymi TEMPEST. Zatwierdza on środki zaradcze TEMPEST dla instalacji i produktów służące temu, by w środowisku operacyjnym chronić EUCI do określonego poziomu klauzuli tajności. Por.: pkt 44 załącznika IV decyzji z 31 marca 2011 roku.

[41] Organ ds. zatwierdzania produktów kryptograficznych (CAA) odpowiada za zapewnienie zgodności produktów kryptograficznych z krajową polityką kryptograficzną lub polityką kryptograficzną Rady. Wydaje on zgodę na to, by dany produkt kryptograficzny w swoim środowisku operacyj-

i organów ds. dystrybucji produktów kryptograficznych (CDA)[42]. Ponadto zaś w odniesieniu do każdego systemu organ ds. akredytacji bezpieczeństwa (SAA)[43] i organ operacyjny ds. zabezpieczenia informacji[44].

---

nym chronił EUCI do określonego poziomu klauzuli tajności. Jeżeli chodzi o państwa członkowskie, CAA jest dodatkowo odpowiedzialny za ocenę produktów kryptograficznych. Por.: pkt 45 załącznika IV decyzji z 31 marca 2011 roku.

[42] Organ ds. dystrybucji produktów kryptograficznych (CDA) odpowiada za: zarządzanie materiałami kryptograficznymi UE i przyjęcie za nie odpowiedzialności; zapewnianie stosowania odpowiednich procedur i stworzenia kanałów umożliwiających przyjmowanie odpowiedzialności za wszystkie materiały kryptograficzne UE, ich bezpieczne wykorzystywanie, przechowywanie i rozpowszechnianie; oraz zapewnianie przekazywania materiałów kryptograficznych UE między osobami lub służbami korzystającymi z tych materiałów. Por.: pkt 46 załącznika IV decyzji z 31 marca 2011 roku.

[43] SAA jest w każdym systemie odpowiedzialny za: zapewnianie zgodności CIS z odpowiednimi politykami bezpieczeństwa i wytycznymi dotyczącymi bezpieczeństwa, dostarczając poświadczenie zatwierdzenia CIS do celów przetwarzania EUCI do określonego poziomu klauzuli tajności w jego środowisku operacyjnym; w poświadczeniu określa się warunki akredytacji oraz kryteria, które muszą być spełnione, by konieczne było ponowne zatwierdzenie; stworzenie procesu akredytacji bezpieczeństwa, zgodnie z odpowiednimi politykami, z wyraźnie określonymi warunkami zatwierdzenia CIS pod nadzorem tego organu; określanie strategii akredytacji bezpieczeństwa przez ustalenie stopnia szczegółowości procedury akredytacji proporcjonalnego do wymaganego poziomu zabezpieczenia; analizowanie i zatwierdzanie dokumentacji związanej z bezpieczeństwem, w tym oświadczeń o zarządzaniu ryzykiem i o ryzyku szczątkowym, oświadczeń o szczególnych wymaganiach bezpieczeństwa systemu (zwanych dalej „SSRS"), dokumentacji związanej z weryfikacją zapewnienia bezpieczeństwa oraz procedur bezpiecznej eksploatacji systemu (zwanych dalej „SecOP"), jak również zapewnianie zgodności tej dokumentacji z polityką i przepisami bezpieczeństwa Rady; sprawdzanie wdrażania środków bezpieczeństwa w odniesieniu do CIS przez dokonywanie ocen, inspekcji lub przeglądów bezpieczeństwa czy też wspieranie takich działań; określanie wymogów bezpieczeństwa (np. poziomów sprawdzania pracowników) w przypadku stanowisk o szczególnie wrażliwym charakterze w odniesieniu do CIS; zatwierdzanie wyboru produktów kryptograficznych i produktów klasy TEMPEST wykorzystywanych do zapewnienia bezpieczeństwa CIS; zatwierdzanie lub w odpowiednich przypadkach uczestniczenie we wspólnym zatwierdzaniu międzysystemowego połączenia CIS z innymi CIS; oraz konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w związku z zarządzaniem ryzykiem dla bezpieczeństwa, w szczególności ryzykiem szczątkowym, jak również z warunkami i okolicznościami poświadczenia zatwierdzenia. Organ ds. akredytacji bezpieczeństwa SGR jest odpowiedzialny za przyznawanie akredytacji wszystkim CIS działającym pod nadzorem SGR. Odpowiedni SAA państwa członkowskiego jest odpowiedzialny za przyznawanie akredytacji CIS oraz jego częściom składowym działającym pod nadzorem danego państwa członkowskiego. Wspólna rada ds. akredytacji bezpieczeństwa (SAB) jest odpowiedzialna za przyznawanie akredytacji CIS działającym pod nadzorem zarówno organu ds. akredytacji bezpieczeństwa SGR, jak i SAA państw członkowskich. W skład tej rady wchodzi po jednym przedstawicielu SAA z każdego państwa członkowskiego, a w jej obradach uczestniczy przedstawiciel SAA z Komisji. Inne podmioty posiadające połączenia z danym CIS są zapraszane do uczestnictwa w obradach, gdy omawiany jest ten system.

Obradom SAB przewodniczy przedstawiciel organu ds. akredytacji bezpieczeństwa SGR. SAB podejmuje decyzje na zasadzie konsensusu przedstawicieli SAA z instytucji, państw członkowskich i innych podmiotów posiadających połączenia z danym CIS. SAB sporządza okresowe sprawozdania ze swojej działalności i przedstawia je Komitetowi ds. Bezpieczeństwa oraz informuje komitet o wszystkich świadectwach akredytacji. Por.: pkt. 47–50 załącznika IV decyzji z 31 marca 2011 roku.

[44] Operacyjny organ ds. zabezpieczania informacji odpowiada w każdym systemie za: opracowanie dokumentacji bezpieczeństwa zgodnie z politykami bezpieczeństwa i wytycznymi dotyczącymi bezpieczeństwa, zwłaszcza SSRS, w tym oświadczenia o ryzyku szczątkowym, SecOP i planu kryptograficznego w ramach procesu akredytacji CIS; uczestnictwo w wyborze i testowaniu technicznych

Decyzja dotyczy także bezpieczeństwa przemysłowego, które ma zapewnić ochronę EUCI przez wykonawców lub podwykonawców podczas negocjacji poprzedzających zawarcie umów i na wszystkich etapach cyklu życia umów niejawnych. Umowy takie nie obejmują dostępu do informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET. Stwierdzono, że Sekretariat Generalny Rady może na podstawie umowy powierzyć zadania obejmujące EUCI lub wiążące się z dostępem do tych informacji, ich wykorzystywaniem lub przechowywaniem przez podmioty prowadzące działalność gospodarczą lub inną, zarejestrowane w państwie członkowskim lub w państwie trzecim, które zawarło umowę lub porozumienie administracyjne w trybie przewidzianym przez decyzję (zgodnie z art. 12 ust. 2 lit. a lub b). Jako instytucja zamawiająca Sekretariat Generalny Rady ma obowiązek zapewnić, by w przypadku zawierania umów niejawnych z podmiotami prowadzącymi działalność gospodarczą lub inną spełnione były minimalne normy bezpieczeństwa przemysłowego określone w niniejszej decyzji i te, o których mowa w danej umowie. Krajowa władza bezpieczeństwa (KWB), wyznaczona władza bezpieczeństwa (WWB) lub jakikolwiek inny właściwy organ bezpieczeństwa każdego państwa członkowskiego zapewniają – w zakresie, jaki umożliwiają to krajowe przepisy ustawowe i wykonawcze – by wykonawcy i podwykonawcy zarejestrowani na ich terytorium stosowali wszelkie odpowiednie środki mające chronić EUCI podczas negocjacji poprzedzających zawarcie umowy i podczas wykonywania umowy niejawnej. KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa każdego państwa członkowskiego mają obowiązek zapewnić, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, by wykonawcy lub podwykonawcy zarejestrowani w tym państwie członkowskim, będący stronami umów niejawnych lub niejawnych umów o podwykonawstwo i którym niezbędny jest dostęp w ich obiektach do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET podczas wykonywania takich umów lub na etapie poprzedzającym ich zawarcie, posiadali świadectwo bezpieczeństwa przemysłowego (SBP) do odpowiedniego poziomu klauzuli tajności. Odpowiednia KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa wydaje pracownikom wykonawcy lub podwykonawcy, którym przy wykonywaniu umowy niejawnej niezbędny jest dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, poświadczenie bezpie-

środków bezpieczeństwa, urządzeń i oprogramowania dla poszczególnych systemów, nadzorowanie ich wdrażania i zapewnianie, by były one w bezpieczny sposób instalowane, konfigurowane i konserwowane zgodnie z odpowiednią dokumentacją bezpieczeństwa; uczestnictwo w wyborze środków bezpieczeństwa i urządzeń klasy TEMPEST, jeżeli jest to wymagane na podstawie SSRS, i zapewnianie, by były one w bezpieczny sposób instalowane i konserwowane we współpracy z TA; monitorowanie wdrażania i stosowania SecOP, a w odpowiednich przypadkach zlecanie właścicielowi systemu operacyjnego obowiązków w zakresie bezpieczeństwa; zarządzanie produktami kryptograficznymi i ich wykorzystywanie, zapewnianie nadzoru nad obiektami kryptograficznymi i kontrolowanymi oraz, jeżeli jest to wymagane, zapewnienie wytwarzania zmiennych kryptograficznych; przeprowadzanie przeglądów i testów analizy bezpieczeństwa, w szczególności w celu sporządzenia odpowiednich sprawozdań o ryzyku, zgodnie z wymogami SAA; zapewnianie szkolenia w zakresie zabezpieczania informacji w odniesieniu do poszczególnych CIS; wdrażanie środków bezpieczeństwa w odniesieniu do poszczególnych CIS i stosowanie tych środków. Por.: pkt 51 załącznika IV decyzji z 31 marca 2011 roku.

czeństwa osobowego (PBO) zgodnie z krajowymi przepisami ustawowymi i wykonawczymi oraz minimalnymi normami bezpieczeństwa określonymi w załączniku I decyzji[45].

Podjęto także w art. 12 decyzji sprawę wymiany informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi stanowiąc, że jeżeli Rada stwierdza, że zachodzi konieczność wymiany EUCI z państwem trzecim lub organizacją międzynarodową, powinna ustanowić odpowiednie ramy takiej wymiany. W tym celu Rada zawiera umowy dotyczące procedur bezpieczeństwa na potrzeby wymiany i ochrony informacji niejawnych (zwane dalej „umowami o bezpieczeństwie informacji"). Sekretarz Generalny może natomiast zawierać porozumienia administracyjne, o ile poziom klauzuli tajności nadanej EUCI, które mają zostać udostępnione, nie jest – co do zasady – wyższy niż RESTREINT UE/EU RESTRICTED[46]. Umowy o bezpieczeństwie informacji lub porozumienia administracyjne zawierają postanowienia mające służyć temu, by w przypadku, gdy państwa trzecie lub organizacje międzynarodowe otrzymają EUCI, informacje te były chronione w sposób odpowiadający ich klauzuli tajności i zgodny z minimalnymi normami, które nie mogą być mniej rygorystyczne niż normy określone w niniejszej decyzji. Decyzja o udostępnieniu państwu trzeciemu lub organizacji międzynarodowej EUCI wytworzonych w Radzie podejmowana jest przez Radę po rozpatrzeniu każdego przypadku z osobna, w zależności od charakteru i treści takich informacji, od tego, czy odbiorca spełnia zasadę ograniczonego dostępu, i od tego, w jakim stopniu jest to korzystne dla UE. Jeżeli wytwórcą informacji niejawnych, o których udostępnienie wystąpiono, nie jest Rada, Sekretariat Generalny Rady najpierw zwraca się o pisemną zgodę wytwórcy na ich udostępnienie. W przypadku, gdy nie można ustalić, kto jest wytwórcą, Rada przejmuje jego odpowiedzialność. W celu stwierdzenia skuteczności środków bezpieczeństwa stosowanych w państwie trzecim lub organizacji międzynarodowej w celu ochrony EUCI, które zostały im przekazane jednostronnie lub w ramach wymiany, należy przeprowadzić wizyty oceniające (kontrole)[47].

---

[45] Kwestie odnoszące się do bezpieczeństwa przemysłowego uregulowano w liczącym 36 punktów załączniku V decyzji, który ustanawia ogólne przepisy w zakresie bezpieczeństwa mające zastosowanie do podmiotów prowadzących działalność gospodarczą lub inną podczas negocjacji poprzedzających zawarcie umowy oraz na wszystkich etapach cyklu życia umów niejawnych zawartych przez SGR. Wyraźnie wskazano jednak, że politykę bezpieczeństwa przemysłowego zatwierdza Rada, określając w szczególności wymogi w odniesieniu do SBP, dokumentu określającego aspekty bezpieczeństwa (DOAB), wizyt, transmisji i przewożenia EUCI. W treści załącznika uregulowano elementy dotyczące bezpieczeństwa w umowie niejawnej, w tym nadawanie klauzul (PNK), problem dokumentów określających aspekty bezpieczeństwa (DOAB), instrukcję bezpieczeństwa programu/projektu (IBP), sprawę świadectw bezpieczeństwa przemysłowego (SBP), kwestie umów niejawnych i niejawnych umów o podwykonawstwo, wizyty (kontrole) związane z umowami niejawnymi, zagadnienie transmisji i przewożenia EUCI, a także wykorzystywanie i przechowywanie informacji niejawnych.

[46] Kwestię tę reguluje pkt 17 załącznika VI decyzji, odnoszącego się do wymiany informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi.

[47] W załączniku VI decyzji uregulowano m.in. problem umów o bezpieczeństwie informacji, porozumień administracyjnych, kwestię wymiany informacji niejawnych oraz sprawę wyjątkowego udostępniania EUCI *ad hoc*.

W tekście decyzji zajęto się także problemem naruszenia i narażenia na szwank bezpieczeństwa informacji niejawnych (art. 13 decyzji). Wskazano, że naruszenie zasad bezpieczeństwa następuje w wyniku działania określonej osoby lub zaniechania przez nią działania w sposób sprzeczny z zasadami bezpieczeństwa ustanowionymi w niniejszej decyzji. Narażenie na szwank bezpieczeństwa EUCI ma natomiast miejsce, gdy w wyniku naruszenia zasad bezpieczeństwa takie informacje w całości lub w części zostają ujawnione osobom nieupoważnionym. Postanowiono, że o wszelkich podejrzeniach lub przypadkach naruszenia zasad bezpieczeństwa powiadamia się niezwłocznie właściwy organ bezpieczeństwa. Jeżeli wiadomo lub jeżeli istnieją uzasadnione przesłanki, by przypuszczać, że bezpieczeństwo EUCI zostało narażone na szwank lub że informacje takie zostały utracone, właściwy organ bezpieczeństwa podejmuje – zgodnie z odpowiednimi przepisami ustawowymi i wykonawczymi – wszelkie stosowne działania służące: poinformowaniu wytwórcy informacji; zapewnieniu zbadania tego przypadku przez personel niezwiązany bezpośrednio z tym naruszeniem w celu ustalenia przebiegu wydarzeń; ocenie potencjalnych szkód dla interesów UE lub państw członkowskich; podjęciu właściwych środków w celu zapobieżenia powtórzeniu się podobnego przypadku; oraz powiadomieniu właściwych organów o podjętych działaniach. Zauważono, że każda osoba odpowiedzialna za naruszenie przepisów dotyczących bezpieczeństwa określonych w niniejszej decyzji może podlegać postępowaniu dyscyplinarnemu zgodnie z mającymi zastosowanie zasadami i przepisami wykonawczymi. Każda osoba odpowiedzialna za narażenie na szwank bezpieczeństwa EUCI lub za ich utratę podlega postępowaniu dyscyplinarnemu lub sądowemu, zgodnie z mającymi zastosowanie przepisami ustawowymi, zasadami i przepisami wykonawczymi.

Decyzja Rady z 31 marca 2011 roku uwzględnia doświadczenia zdobyte przez Unię Europejską w trakcie obowiązywania decyzji 2001/264[48]. Jakkolwiek rozwiązania obecnie obowiązującej decyzji wydają się bardziej syntetyczne niż jej poprzedniczki, to jednak i ona razi biurokratyczną kazuistyką, charakterystyczną zresztą dla rozwiązań prawnych, odnoszących się szczególnie do problematyki bezpieczeństwa, zarówno międzynarodowych, jak i europejskich. Warto zauważyć, że przed wydaniem wspomnianej decyzji, 30 kwietnia 2007 roku została podpisana umowa między Unią Europejską a USA w sprawie bezpieczeństwa informacji niejawnych[49] oraz porozumienie wykonawcze do tej umowy w sprawie bezpieczeństwa między biurem ds. bezpieczeństwa Sekretariatu Generalnego Rady, dyrekcją bezpieczeństwa Komisji Europejskiej a Departamentem Stanu USA w celu ochrony informacji niejawnych wymienianych między UE a Stanami Zjednoczonymi. Decyzja z 31 marca 2011 roku w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE 2011/292/UE wyraźnie wychodzi, przynajmniej w treści art. 12, naprzeciw rozwiązaniom tej umowy.

---

[48] Treść decyzji Rady z 2001 roku, która poprzedziła decyzję 2011/292/UE, omawia: S. Hoc, *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych. Wybrane zagadnienia*, Opole 2006, s. 162–168.

[49] Dz. Urz. UE L 2007, nr 115, s. 30.

Rozważenia wymaga czy i na ile wspomniana decyzja winna skutkować nowelizacją ustawy z 5 sierpnia 2010 roku o ochronie informacji niejawnych[50]. Przy tej okazji wypada zwrócić uwagę na rozporządzenie Prezesa Rady Ministrów w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Agencji Kontrwywiadu Wojskowego w zakresie wykonywania krajowej władzy bezpieczeństwa[51], a więc organu, o jakim mowa w decyzji Rady z 31 marca 2011 roku. Przy okazji wypada przywołać rozporządzenie Prezesa Rady Ministrów z 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego[52].

STRESZCZENIE

W tekście poddano analizie zasady ochrony informacji niejawnych w prawie Unii Europejskiej rozważając treść art. 296 TWE (obecnie art. 346 TFUE) oraz decyzję Rady z 31 marca 2011 roku w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE. Rozważono kwestie odnoszące się do klauzul tajności, zarządzania ryzykiem dla bezpieczeństwa, problem bezpieczeństwa osobowego, fizycznego, zarządzania informacjami niejawnymi, ochrony informacji niejawnych w systemach teleinformatycznych, bezpieczeństwa przemysłowego, wymiany informacji z państwami trzecimi, wreszcie – naruszenia i narażenia na szwank informacji niejawnych UE. Zajęto się także sprawą organizacji bezpieczeństwa w Radzie i funkcjonowaniem Komitetu ds. Bezpieczeństwa. W końcowej części zwrócono uwagę na związek wspomnianej decyzji z innymi aktami normatywnymi.

PROTECTION OF CLASSIFIED INFORMATION IN THE LEGAL SYSTEM OF THE EUROPEAN UNION

ABSTRACT

The paper discusses the principles of protection of classified information in EU law by means of an analysis of Article 1 of the Treaty establishing the European Community, and the Council decision of 31 March 2011 on the security rules for protecting EU classified information. Issues considered involve the clauses on classified information, risk management for security, the issue of personal and physical security, classified information management, protection of classified information in ICT systems, industrial security, information exchange with third countries, and finally – the breach and compromise of EU classified information. The final part emphasizes the connection between the above-mentioned decision and other normative acts.

---

[50] Dz. U. 2010, Nr 182, poz. 1228. Jest rzeczą dziwną i niezmiernie ciekawą, że w uzasadnieniu projektu ustawy (Sejm RP VI kadencji) nie odwołano się do treści obowiązującej wówczas decyzji 2001/264/WE stwierdzając, wbrew oczywistym faktom, że „przedmiot projektowanej regulacji nie jest objęty prawem Unii Europejskiej". Bardzo źle to świadczy o znajomości prawa europejskiego przez odpowiedzialnych urzędników.

[51] Dz. U. 2011, Nr 220, poz. 1302. Funkcję szefa krajowej rady bezpieczeństwa pełni szef ABW, a jej zadania wobec podmiotów sfery wojskowej mają być wykonywane za pośrednictwem szefa służby kontrwywiadu wojskowego.

[52] Dz. U. 2011, Nr 159, poz. 948. W treści tego rozporządzenia brak nawiązań do art. 10 decyzji Rady z 31 marca 2011 r.