IV

(Informacje)

INFORMACJE INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

EUROPEJSKA SŁUŻBA DZIAŁAŃ ZEWNĘTRZNYCH

DECYZJA WYSOKIEGO PRZEDSTAWICIELA UNII DO SPRAW ZAGRANICZNYCH I POLITYKI BEZPIECZEŃSTWA

z dnia 19 kwietnia 2013 r.

w sprawie przepisów bezpieczeństwa mających zastosowanie do Europejskiej Służby Działań Zewnętrznych

(2013/C 190/01)

WYSOKI PRZEDSTAWICIEL UNII DO SPRAW ZAGRANICZNYCH I POLITYKI BEZPIECZEŃSTWA,

uwzględniając decyzję Rady 2010/427/UE z dnia 26 lipca 2010 r. określającą organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych [1] (ESDZ),

uwzględniając opinię Komitetu, o którym mowa w art. 9 ust. 6 decyzji Wysokiego Przedstawiciela z dnia 15 czerwca 2011 r. w sprawie przepisów bezpieczeństwa mających zastosowanie do Europejskiej Służby Działań Zewnętrznych [2],

uwzględniając opinię Komitetu, o którym mowa w art. 10 ust. 1 decyzji Rady 2010/427/EU z dnia 26 lipca 2010 r. określającej organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych,

a także mając na uwadze, co następuje:

(1) W ESDZ, jako autonomicznym funkcjonalnie organie Unii Europejskiej (UE), powinny obowiązywać przepisy bezpieczeństwa, o których mowa w art. 10 ust. 1 decyzji Rady 2010/427/UE.

(2) Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (dalej zwany „Wysokim Przedstawicielem") powinien w drodze decyzji określić przepisy bezpieczeństwa mające zastosowanie do ESDZ, obejmujące wszystkie aspekty bezpieczeństwa w zakresie funkcjonowania ESDZ, aby umożliwić jej skuteczne zarządzanie ryzykiem, na jakie narażony jest personel podlegający odpowiedzialności ESDZ, jego majątek rzeczowy, informacje i osoby odwiedzające, a także aby umożliwić jej wypełnianie w tym względzie jej zadań wynikających z obowiązku dochowania należytej staranności.

(3) W szczególności personelowi podlegającemu odpowiedzialności ESDZ, majątkowi rzeczowemu ESDZ, w tym systemom teleinformatycznym, informacjom i osobom odwiedzającym należy zapewnić poziom ochrony zgodny z najlepszymi praktykami stosowanymi w Radzie, Komisji, państwach członkowskich oraz w stosownych przypadkach w organizacjach międzynarodowych.

(4) Przepisy bezpieczeństwa mające zastosowanie do ESDZ powinny przyczynić się do stworzenia w UE bardziej spójnych kompleksowych ogólnych ram ochrony informacji niejawnych UE (dalej zwanych „EUCI") w oparciu o przepisy bezpieczeństwa przyjęte przez Radę Unii Europejskiej (dalej zwaną „Radą") oraz przez Komisję Europejską i przy zachowaniu możliwie jak największej spójności z tymi przepisami.

(5) ESDZ, Rada i Komisja zobowiązują się stosować równoważne normy bezpieczeństwa w celu ochrony EUCI.

(6) Niniejsza decyzja zostaje przyjęta bez uszczerbku dla art. 15 i 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) oraz aktów prawnych służących wykonaniu tych artykułów.

(7) Konieczne jest określenie zasad organizacji bezpieczeństwa w ESDZ oraz przydzielenie zadań w zakresie bezpieczeństwa w ramach struktur ESDZ.

[1] Dz.U. L 201 z 3.8.2010, s. 30.
[2] Dz.U. C 304 z 15.10.2011, s. 5

(8) Wysoki Przedstawiciel powinien w razie potrzeby korzystać z odnośnej wiedzy fachowej w państwach członkowskich, Sekretariacie Generalnym Rady oraz Komisji Europejskiej.

(9) Wysoki Przedstawiciel powinien podjąć wszelkie niezbędne środki w celu wprowadzenia w życie niniejszych przepisów przy wsparciu państw członkowskich, Sekretariatu Generalnego Rady i Komisji Europejskiej,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Cel i zakres stosowania

W niniejszej decyzji ustanawia się przepisy bezpieczeństwa mające zastosowanie do Europejskiej Służby Działań Zewnętrznych (dalej zwane „przepisami bezpieczeństwa ESDZ").

Zgodnie z art. 10 ust. 1 decyzji Rady 2010/427/UE z dnia 26 lipca 2010 r. określającej organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych przepisy te mają zastosowanie do personelu ESDZ oraz wszystkich członków personelu w delegaturach Unii, niezależnie od ich pochodzenia i statusu administracyjnego; określają one ogólne ramy regulacyjne skutecznego zarządzania ryzykiem, na jakie narażony jest personel podlegający odpowiedzialności ESDZ, zgodnie z jego definicją w art. 2, a także lokale, majątek rzeczowy, informacje i osoby odwiedzające ESDZ.

Artykuł 2

Definicje

Do celów niniejszej decyzji stosuje się następujące definicje:

a) „personel ESDZ" oznacza urzędników i innych pracowników ESDZ, w tym pracowników służb dyplomatycznych państw członkowskich mianowanych na czas określony oraz oddelegowanych ekspertów krajowych w rozumieniu art. 6 decyzji Rady 2010/427/UE z dnia 26 lipca 2010 r. określającej organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych;

b) „personel podlegający odpowiedzialności ESDZ" oznacza personel ESDZ oraz wszystkich członków personelu w delegaturach Unii, niezależnie od ich pochodzenia i statusu administracyjnego, a także, w kontekście niniejszej decyzji, Wysokiego Przedstawiciela i w stosownych przypadkach innych członków personelu znajdujących się w siedzibie głównej ESDZ;

c) „osoby na utrzymaniu" oznaczają członków rodzin personelu podlegającego odpowiedzialności ESDZ w delegaturach Unii, zamieszkujących w tym samym gospodarstwie domowym, co dany członek personelu, zgodnie z informacją przekazaną ministerstwu spraw zagranicznych państwa przyjmującego;

d) „lokale ESDZ" oznaczają wszelkie obiekty ESDZ, w tym budynki, biura, pomieszczenia i inne miejsca, a także pomieszczenia, w których znajdują się systemy teleinformatyczne (w tym systemy obchodzące się z EUCI), w których ESDZ stale lub czasowo prowadzi działalność;

e) „interesy bezpieczeństwa ESDZ" obejmują personel podlegający odpowiedzialności ESDZ i osoby będące na ich utrzymaniu, a także lokale ESDZ, jej majątek rzeczowy, w tym systemy teleinformatyczne, oraz informacje i osoby odwiedzające;

f) „informacje niejawne UE" („EUCI") 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.

Pozostałe definicje zawarto w odpowiednich załącznikach oraz w dodatku A.

Artykuł 3

Obowiązek dochowania należytej staranności

1. Przepisy bezpieczeństwa ESDZ mają na celu realizację przez ESDZ jej zadań wynikających z obowiązku dochowania należytej staranności.

2. Obowiązek dochowania należytej staranności obejmuje podjęcie wszelkich racjonalnych kroków w zakresie wdrożenia środków bezpieczeństwa mających zapobiec dającej się racjonalnie przewidzieć szkodzie dla interesów bezpieczeństwa ESDZ.

Obejmuje to aspekty bezpieczeństwa i ochrony, w tym wynikające z wszelkiego rodzaju sytuacji nagłych lub kryzysowych.

3. Biorąc pod uwagę obowiązek dochowania należytej staranności spoczywający na państwach członkowskich, instytucjach i organach UE oraz innych stronach, których personel znajduje się w delegaturach Unii lub ich lokalach, bądź obowiązek taki spoczywający na ESDZ w sytuacji, gdy delegatury Unii korzystają z lokali wyżej wymienionych innych stron, ESDZ zawiera porozumienia administracyjne z poszczególnymi wyżej wymienionymi podmiotami, określając role, zakresy odpowiedzialności i zadania poszczególnych stron i mechanizmy współpracy.

Artykuł 4

Bezpieczeństwo fizyczne i bezpieczeństwo infrastruktury

1. W celu ochrony interesów bezpieczeństwa ESDZ wprowadza ona wszelkie właściwe środki bezpieczeństwa (o charakterze stałym lub tymczasowym), w tym w zakresie kontroli dostępu, we wszystkich lokalach ESDZ. Takie środki uwzględnia się przy projektowaniu i planowaniu nowych lokali lub przed wynajęciem lokali istniejących.

2. W państwach trzecich ESDZ wprowadza również wszelkie właściwe dodatkowe środki bezpieczeństwa o charakterze stałym lub tymczasowym w celu ochrony swoich interesów bezpieczeństwa.

W tym celu możliwe jest ze względów bezpieczeństwa nakładanie na określony czas i na określonych obszarach szczególnych obowiązków lub ograniczeń na personel podlegający odpowiedzialności ESDZ i na osoby będące na jego utrzymaniu.

3. Środki, o których mowa w ust. 1 i 2, są współmierne do oszacowanego ryzyka.

Artykuł 5

Ochrona informacji niejawnych

1. Ochrona EUCI podlega wymogom określonym w niniejszej decyzji, a w szczególności w załączniku A. Posiadacz jakichkolwiek EUCI jest odpowiedzialny za ich należytą ochronę.

2. ESDZ zapewnia, aby dostępu do informacji niejawnych udzielano wyłącznie osobom, które spełniają warunki określone w art. 5 załącznika A.

3. Warunki udzielania dostępu do EUCI pracownikom miejscowym są określane również przez Wysokiego Przedstawiciela zgodnie z zasadami ochrony EUCI określonymi w załączniku A do niniejszej decyzji.

4. Dyrekcja ds. Bezpieczeństwa ESDZ prowadzi bazę danych dotyczącą statusu wszystkich członków personelu podlegającego odpowiedzialności ESDZ oraz wykonawców ESDZ pod względem poświadczenia bezpieczeństwa.

5. W przypadku gdy państwo członkowskie wprowadza do struktur lub sieci ESDZ informacje niejawne opatrzone krajowym oznaczeniem klauzuli tajności, ESDZ obejmuje te informacje ochroną zgodnie z wymogami, które mają zastosowanie do EUCI mających klauzulę o równoważnym poziomie, zgodnie z przepisami obowiązującymi na podstawie załącznika A do niniejszej decyzji.

6. W miejscach, w których w ESDZ przechowuje się informacje o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, bądź klauzuli jej równoważnej, tworzy się strefy zabezpieczone zgodnie z przepisami obowiązującymi na podstawie załącznika A do niniejszej decyzji, a strefy te zatwierdza organ ds. bezpieczeństwa ESDZ.

7. Procedury wykonywania przez Wysokiego Przedstawiciela jego obowiązków w ramach umów lub porozumień administracyjnych dotyczących wymiany EUCI z państwami trzecimi lub organizacjami międzynarodowymi określono w załącznikach A i A VI do niniejszej decyzji.

Artykuł 6

Incydenty związane z bezpieczeństwem i sytuacje nadzwyczajne

1. W celu zapewnienia szybkiego i skutecznego reagowania na incydenty związane z bezpieczeństwem ESDZ wprowadza proces zgłaszania takich incydentów i sytuacji nadzwyczajnych, działający całą dobę we wszystkie dni tygodnia i obejmujący wszelkiego rodzaju incydenty związane z bezpieczeństwem lub sytuacje powodujące zagrożenie dla interesów bezpieczeństwa ESDZ (np. wypadki, konflikty, działania podejmowane w złych zamiarach, działania przestępcze, porwania oraz przetrzymywanie zakładników, nagłe przypadki medyczne, incydenty dotyczące systemów teleinformatycznych, ataki cybernetyczne itp.).

2. Pomiędzy główną siedzibą ESDZ, delegaturami Unii, Radą, Komisją, specjalnymi przedstawicielami UE i państwami członkowskimi tworzy się kanały łączności kryzysowej, ułatwiające postępowanie na wypadek incydentów związanych z bezpieczeństwem, dotyczących personelu, oraz służące łagodzeniu ich skutków, co obejmuje również planowanie ewentualnościowe.

3. Wspomniane postępowanie na wypadek incydentów związanych z bezpieczeństwem obejmuje między innymi:

— procedury skutecznego wspierania procesu decyzyjnego w odniesieniu do incydentu związanego z bezpieczeństwem dotyczącego personelu, w tym decyzji dotyczących wycofania lub zawieszenia misji oraz

— strategie i procedury poszukiwania i uwalniania personelu, np. w wypadku zaginięcia, porwania lub przetrzymywania zakładników, z uwzględnieniem szczegółowych zakresów odpowiedzialności państw członkowskich, instytucji UE i ESDZ w tym zakresie. W zarządzaniu tego rodzaju operacjami bierze się pod uwagę potrzebę zaangażowania szczególnych środków z uwzględnieniem zasobów, jakich mogą udostępnić państwa członkowskie.

4. ESDZ wprowadza odpowiednie uregulowania administracyjne na potrzeby zgłaszania incydentów związanych z bezpieczeństwem w delegaturach Unii. W stosownych przypadkach informuje się państwa członkowskie, Komisję, wszelkie inne odpowiednie organy oraz odpowiednie komitety ds. bezpieczeństwa.

5. Dokonuje się regularnych ćwiczeń i przeglądów procesów postępowania na wypadek incydentów.

Artykuł 7

Bezpieczeństwo systemów teleinformatycznych

1. ESDZ chroni informacje przetwarzane w systemach teleinformatycznych („CIS") przed zagrożeniami dla ich poufności, integralności, dostępności, autentyczności i niezaprzeczalności.

2. Zasady, politykę bezpieczeństwa i program bezpieczeństwa służące ochronie wszelkich CIS należących do ESDZ lub przez nią użytkowanych zatwierdza organ ESDZ ds. bezpieczeństwa, zdefiniowany w art. 12 sekcja I ust. 1.

3. Treść wyżej wspomnianych zasad, polityki i programu jest zgodna, a ich wdrażanie – ściśle skoordynowane z zasadami, polityką i programami bezpieczeństwa Rady i Komisji, a w stosownych przypadkach z polityką bezpieczeństwa stosowaną przez poszczególne państwa członkowskie.

4. Wszystkie CIS, w których przetwarza się informacje niejawne, przechodzą proces akredytacji. ESDZ stosuje system zarządzania akredytacją bezpieczeństwa w porozumieniu z Sekretariatem Generalnym Rady oraz Komisją.

5. W przypadkach gdy EUCI przetwarzane przez ESDZ podlegają ochronie przy użyciu produktów kryptograficznych, produkty te są zatwierdzane przez organ ds. zatwierdzania produktów kryptograficznych ESDZ na podstawie zalecenia Komitetu ds. Bezpieczeństwa w Radzie.

6. W zakresie, w jakim jest to niezbędne, organ ESDZ ds. bezpieczeństwa ustanawia następujące funkcje w zakresie zabezpieczania informacji:

a) organ ds. zabezpieczania informacji;

b) organ ds. TEMPEST;

c) organ ds. zatwierdzania produktów kryptograficznych;

d) organ ds. dystrybucji produktów kryptograficznych.

7. Organ ESDZ ds. bezpieczeństwa ustanawia dla każdego systemu następujące funkcje:

a) organ ds. akredytacji bezpieczeństwa;

b) organ operacyjny ds. zabezpieczania informacji.

8. Przepisy dotyczące wprowadzania w życie niniejszego artykułu w zakresie ochrony EUCI znajdują się w załącznikach A i A IV.

Artykuł 8

Naruszenia zasad bezpieczeństwa oraz nieuprawnione ujawnienie informacji niejawnych

1. Naruszenie zasad bezpieczeństwa następuje w wyniku działania określonej osoby lub zaniechania przez nią działania w sposób sprzeczny z przepisami bezpieczeństwa ustanowionymi w niniejszej decyzji lub z polityką bądź wytycznymi określającymi środki niezbędne do wdrożenia tych przepisów, zatwierdzonymi zgodnie z art. 20 ust. 1.

2. Nieuprawnione ujawnienie informacji niejawnych następuje wówczas, gdy informacje niejawne zostają w całości lub częściowo ujawnione nieupoważnionym osobom lub podmiotom.

3. Wszelkie naruszenia zasad bezpieczeństwa lub nieuprawnione ujawnienie informacji niejawnych bądź podejrzenie takiego naruszenia lub ujawnienia należy niezwłocznie zgłaszać do Dyrekcji ds. Bezpieczeństwa ESDZ, która podejmuje odpowiednie działania określone w załączniku A.

4. Każda osoba odpowiedzialna za naruszenie przepisów bezpieczeństwa określonych w niniejszej decyzji lub za nieuprawnione ujawnienie informacji niejawnych może podlegać postępowaniu dyscyplinarnemu lub sądowemu zgodnie z mającymi zastosowanie zasadami oraz przepisami ustawowymi i wykonawczymi, wymienionymi w art. 11 ust. 3 załącznika A.

Artykuł 9

Dochodzenia w przypadkach incydentów związanych z bezpieczeństwem, naruszeń zasad bezpieczeństwa i nieuprawnionego ujawnienia informacji niejawnych oraz działania naprawcze

1. Dyrekcja ds. Bezpieczeństwa ESDZ, w stosownych przypadkach przy wsparciu ekspertów z państw członkowskich lub innych instytucji UE i w razie potrzeby za zezwoleniem dyrektora ds. operacyjnych:

a) przeprowadza w stosownych przypadkach dochodzenia lub weryfikacje:

(i) w przypadkach, gdy wiadomo lub istnieją racjonalne podstawy do podejrzeń, że nastąpiła utrata lub nieuprawnione ujawnienie informacji niejawnej mającej znaczenie dla ESDZ;

(ii) w przypadku stwierdzonego lub podejrzewanego naruszenia zasad bezpieczeństwa bądź innych incydentów związanych z bezpieczeństwem lub sytuacji stwarzających zagrożenie dla interesów bezpieczeństwa ESDZ;

(b) w stosownych przypadkach podejmuje wszelkie niezbędne działania naprawcze wynikające z dochodzeń.

2. Osobom prowadzącym dochodzenia zapewnia się dostęp do wszelkich informacji niezbędnych do ich prowadzenia oraz pełne wsparcie wszelkich służb ESDZ w tym zakresie.

Osoby prowadzące dochodzenia mogą podejmować odpowiednie działania w celu zabezpieczenia materiału dowodowego w sposób proporcjonalny do wagi kwestii będącej przedmiotem dochodzenia.

3. W przypadku gdy dostęp do informacji dotyczy danych osobowych, w tym danych znajdujących się w systemach teleinformatycznych, dostępu takiego udziela się zgodnie z rozporządzeniem (WE) nr 45/2001.

4. W przypadkach gdy na potrzeby dochodzenia konieczne jest stworzenie bazy danych zawierającej dane osobowe, powiadamia się Europejskiego Inspektora Ochrony Danych zgodnie z wyżej wspomnianym rozporządzeniem.

Artykuł 10

Zarządzanie ryzykiem dla bezpieczeństwa

1. W celu określenia swoich potrzeb w zakresie zapewnienia bezpieczeństwa ESDZ w ścisłej współpracy z Dyrekcją ds. Bezpieczeństwa w Komisji oraz w stosownych przypadkach z Biurem Bezpieczeństwa w Sekretariacie Generalnym Rady opracowuje metodykę kompleksowego szacowania ryzyka dla bezpieczeństwa.

2. Zarządzanie ryzykiem dla interesów bezpieczeństwa ESDZ przebiega w ramach określonego procesu. Celem tego procesu jest ustalenie znanych rodzajów ryzyka dla bezpieczeństwa, określenie środków bezpieczeństwa mających ograniczać to ryzyko do dopuszczalnego poziomu oraz stosowanie środków zgodnie z koncepcją ochrony w głąb. Skuteczność takich środków i poziom ryzyka podlega ciągłej ocenie.

3. Role, zakresy odpowiedzialności i zadania określone w niniejszej decyzji pozostają bez uszczerbku dla odpowiedzialności każdego członka personelu podlegającego odpowiedzialności ESDZ; w szczególności personel UE przebywający na misjach w państwach trzecich musi wykazywać zdrowy rozsądek i właściwą ocenę sytuacji w zakresie własnego bezpieczeństwa oraz przestrzegać wszelkich obowiązujących przepisów, zasad, procedur i instrukcji dotyczących bezpieczeństwa.

4. ESDZ podejmuje wszelkie racjonalne środki dla zapewnienia ochrony swoich interesów bezpieczeństwa i zapobieżenia dającym się racjonalnie przewidzieć szkodom dla tych interesów.

5. Środki bezpieczeństwa w ESDZ dotyczące ochrony EUCI w całym ich cyklu życia ustala się w sposób współmierny w szczególności do ich klauzuli tajności, formy i ilości informacji lub materiału, lokalizacji i konstrukcji obiektów, w których przechowywane są EUCI, oraz zagrożenia (w tym oszacowanego na poziomie lokalnym) działaniami podejmowanymi w złych zamiarach lub działalnością przestępczą, taką jak np. działalność szpiegowska, sabotażowa lub terrorystyczna.

Artykuł 11

Świadomość w kwestiach związanych z bezpieczeństwem i szkolenie

1. Organ ESDZ ds. bezpieczeństwa zapewnia opracowanie i wdrożenie odpowiednich programów podnoszenia świadomości i szkolenia w dziedzinie bezpieczeństwa oraz dba o to, by członkowie personelu podlegającego odpowiedzialności ESDZ, a w stosownych przypadkach również osoby na ich utrzymaniu, odebrali niezbędne instrukcje i szkolenia w zakresie bezpieczeństwa, współmierne do ryzyka w ich miejscu pracy lub zamieszkania.

2. Przed uzyskaniem dostępu do EUCI, a po jego uzyskaniu – w regularnych odstępach czasu członkowie personelu informowani są o obowiązku ochrony EUCI zgodnie z przepisami określonymi w art. 5 i potwierdzają przyjęcie tego obowiązku do wiadomości.

Artykuł 12

Organizacja bezpieczeństwa w ESDZ

Sekcja 1

Przepisy ogólne

1. Organem ESDZ ds. bezpieczeństwa jest dyrektor ds. operacyjnych. Pełniąc tę funkcję, dyrektor ds. operacyjnych zapewnia, aby:

a) środki bezpieczeństwa koordynowano w miarę potrzeb z właściwymi organami państw członkowskich, Sekretariatem Generalnym Rady i Komisją oraz, w stosownych przypadkach, państwami trzecimi lub organizacjami międzynarodowymi w odniesieniu do wszelkich kwestii związanych z bezpieczeństwem, które są istotne dla działań ESDZ, w tym charakteru zagrożeń dla interesów bezpieczeństwa ESDZ oraz sposobów ochrony przed tymi zagrożeniami;

b) we wszystkich działaniach ESDZ od samego początku w pełni uwzględniano aspekty bezpieczeństwa;

c) dostęp do informacji niejawnych był udzielany wyłącznie osobom, które spełniają warunki określone w art. 5 załącznika A;

d) ustanowiono system kancelarii tajnych gwarantujący, że sposób obchodzenia się z informacjami opatrzonymi klauzulą CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą jest zgodny z niniejszą decyzją zarówno w ESDZ, jak i przy ich przekazywaniu państwom członkowskim UE, instytucjom, organom lub agencjom UE lub innym upoważnionym odbiorcom. Osobno prowadzi się rejestr wszystkich EUCI przekazanych przez ESDZ państwom trzecim i organizacjom międzynarodowym oraz wszystkich informacji niejawnych otrzymanych od tych państw i organizacji;

e) przeprowadzano inspekcje bezpieczeństwa, o których mowa w art. 15;

f) w sprawie wszelkich przypadków lub podejrzeń naruszenia zasad bezpieczeństwa bądź utraty lub nieuprawnionego ujawnienia informacji niejawnych będących w posiadaniu lub pochodzących z ESDZ przeprowadzano postępowanie wyjaśniające oraz by o pomoc w takich postępowaniach zwracano się do odpowiednich organów ds. bezpieczeństwa;

g) wprowadzono odpowiednie plany i mechanizmy postępowania na wypadek incydentów oraz służące łagodzeniu ich konsekwencji w celu zapewnienia szybkiego i skutecznego reagowania na incydenty związane z bezpieczeństwem;

h) podejmowano odpowiednie środki w razie nieprzestrzegania przez poszczególne osoby przepisów niniejszej decyzji;

i) wprowadzono odpowiednie środki fizyczne i organizacyjne w celu ochrony interesów bezpieczeństwa ESDZ.

W tym zakresie, w porozumieniu z wykonawczym sekretarzem generalnym, COO:

— ustala kategorię bezpieczeństwa delegatur, w porozumieniu z Komisją;

— podejmuje po konsultacji z Wysokim Przedstawicielem decyzję o ewentualnej ewakuacji delegatury, jeśli wymaga tego sytuacja pod względem bezpieczeństwa;

— podejmuje decyzję o środkach, jakie należy podjąć w stosownych przypadkach w celu ochrony osób na utrzymaniu, z uwzględnieniem uzgodnień dokonanych z instytucjami UE, o których mowa w art. 3 ust. 3;

— zatwierdza strategię przekazywania informacji kryptograficznych, w szczególności program instalacji mechanizmu i produktów kryptograficznych.

2. W wykonywaniu tych zadań dyrektor ds. operacyjnych otrzymuje wsparcie dyrektora zarządzającego ds. administracyjnych i finansowych, kierownika Dyrekcji ds. Bezpieczeństwa ESDZ oraz w stosownych przypadkach dyrektora zarządzającego ds. reagowania w sytuacjach kryzysowych i koordynatora operacyjnego.

3. Dyrektor ds. operacyjnych jako organ ESDZ ds. bezpieczeństwa może w stosownych przypadkach delegować swoje zadania w tym zakresie.

4. Każdy kierownik departamentu lub działu jest odpowiedzialny za wdrażanie zasad ochrony EUCI w podległym mu departamencie lub dziale.

Bez uszczerbku dla odpowiedzialności za powyższe zadania każdy kierownik departamentu lub działu wyznacza pracownika do pełnienia funkcji departamentalnego koordynatora ds. bezpieczeństwa, dysponującego zasobami proporcjonalnymi do ilości EUCI, z którymi obchodzi się dany departament lub dział.

Departamentalni koordynatorzy ds. bezpieczeństwa w stosownych przypadkach służą pomocą i wsparciem kierownikom departamentów lub działów, którym podlegają, w wykonywaniu zadań związanych z bezpieczeństwem, takich jak:

a) opracowywanie ewentualnych dodatkowych wymogów bezpieczeństwa odpowiednich do konkretnych potrzeb danego departamentu lub działu;

b) prowadzenie okresowych instruktaży dotyczących bezpieczeństwa dla pracowników danego departamentu lub działu;

c) zapewnianie przestrzegania w danym departamencie lub dziale zasady ograniczonego dostępu;

d) prowadzenie i aktualizowanie listy kodów i kluczy;

e) utrzymywanie procedur i środków bezpieczeństwa;

f) zgłaszanie wszelkich naruszeń zasad bezpieczeństwa i nieuprawnionych ujawnień EUCI dyrektorowi, któremu podlegają, oraz Dyrekcji ds. Bezpieczeństwa;

g) odbieranie sprawozdań od pracowników odchodzących z pracy w ESDZ;

h) regularne przedstawianie sprawozdań dotyczących kwestii bezpieczeństwa w departamencie lub dziale za pośrednictwem hierarchii;

i) utrzymywanie kontaktów z Departamentem ds. Bezpieczeństwa ESDZ na temat kwestii bezpieczeństwa.

Wszelkie działania lub kwestie mogące mieć wpływ na bezpieczeństwo należy bez zwłoki zgłaszać Departamentowi ds. Bezpieczeństwa ESDZ.

5. Każdy szef delegatury Unii jest odpowiedzialny za wdrażanie wszelkich środków w zakresie bezpieczeństwa danej delegatury.

Sekcja 2

Dyrekcja ds. Bezpieczeństwa ESDZ

1. W ESDZ powołuje się Dyrekcję ds. Bezpieczeństwa, która:

a) zajmuje się zarządzaniem, koordynacją, nadzorem i wdrażaniem w odniesieniu do wszelkich środków bezpieczeństwa w siedzibie głównej oraz we wszystkich lokalach podlegających odpowiedzialności ESDZ w UE i w państwach trzecich;

b) zapewnia spójność i zgodność wszelkich działań, które mogą wpływać na ochronę interesów bezpieczeństwa ESDZ, z niniejszą decyzją i przepisami wykonawczymi;

c) pełni funkcję głównego doradcy Wysokiego Przedstawiciela, wykonawczego sekretarza generalnego i dyrektora ds. operacyjnych we wszelkich kwestiach dotyczących bezpieczeństwa;

d) korzysta z pomocy właściwych służb państw członkowskich zgodnie z art. 10 ust. 3 decyzji Rady 2010/427/UE określającej organizację i zasady funkcjonowania ESDZ;

e) wspiera działania organu ESDZ ds. akredytacji bezpieczeństwa poprzez prowadzenie ocen bezpieczeństwa fizycznego ogólnego i lokalnego środowiska bezpieczeństwa, systemów teleinformatycznych, w których przetwarzane są EUCI, oraz lokali, które mają zostać dopuszczone do przetwarzania i przechowywania EUCI.

2. Kierownik Dyrekcji ds. Bezpieczeństwa ESDZ odpowiada za:

a) zapewnienie ogólnej ochrony interesów bezpieczeństwa ESDZ;

b) opracowywanie, przeglądy i aktualizacje przepisów bezpieczeństwa oraz koordynację środków bezpieczeństwa z właściwymi organami państw członkowskich oraz w stosownych przypadkach z właściwymi organami państw trzecich i organizacji międzynarodowych powiązanych z UE umowami lub uzgodnieniami dotyczącymi bezpieczeństwa;

c) wspieranie prac Komitetu ds. Bezpieczeństwa ESDZ, o którym mowa w art. 14 ust. 1 niniejszej decyzji;

d) utrzymywanie w stosownych przypadkach kontaktów w kwestiach bezpieczeństwa z wszelkimi partnerami lub organami niewymienionymi w lit. b);

e) ustalanie priorytetów i przedstawianie wniosków dotyczących gospodarowania środkami budżetowymi na cele bezpieczeństwa w siedzibie głównej i w delegaturach Unii.

3. Kierownik Dyrekcji ds. Bezpieczeństwa ESDZ:

a) dopilnowuje ewidencjonowania naruszeń zasad bezpieczeństwa i przypadków nieuprawnionego ujawnienia oraz wszczynania i podejmowania dochodzeń w razie konieczności;

b) odbywa zarówno regularne, jak i zwoływane w razie konieczności spotkania z dyrektorem ds. bezpieczeństwa Sekretariatu Generalnego Rady oraz dyrektorem Dyrekcji ds. Bezpieczeństwa w Komisji Europejskiej w celu omówienia kwestii stanowiących przedmiot wspólnego zainteresowania.

4. Dyrekcja ds. Bezpieczeństwa ESDZ nawiązuje kontakt i utrzymuje ścisłą współpracę z:

— departamentami ds. bezpieczeństwa w ministerstwach spraw zagranicznych państw członkowskich;

— krajowymi władzami bezpieczeństwa (KWB) i innymi właściwymi organami ds. bezpieczeństwa w państwach członkowskich w celu uzyskiwania od nich pomocy w zakresie informacji potrzebnych do oceny niebezpieczeństw i zagrożeń, jakie mogą grozić ESDZ, jej personelowi, działalności, majątkowi i zasobom oraz jej informacjom niejawnym w miejscu, w którym zwykle prowadzi ona działalność;

— właściwymi organami bezpieczeństwa państw członkowskich lub państw, na których terytorium ESDZ prowadzi działalność, we wszelkich kwestiach dotyczących ochrony jej personelu, działalności, majątku i zasobów oraz jej informacji niejawnych na terytorium tych państw;

— Biurem Bezpieczeństwa Sekretariatu Generalnego Rady oraz Dyrekcją ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji, a w stosownych przypadkach również odpowiednimi departamentami ds. bezpieczeństwa innych instytucji, organów i agencji UE;

— departamentów ds. bezpieczeństwa państw trzecich lub organizacji międzynarodowych w celu prowadzenia użytecznej koordynacji;

— krajowymi władzami bezpieczeństwa w państwach członkowskich w zakresie wszelkich kwestii dotyczących ochrony EUCI.

Sekcja 3

Delegatury Unii

1. Każdy szef delegatury Unii jest odpowiedzialny za lokalne wdrażanie wszelkich środków służących ochronie interesów bezpieczeństwa ESDZ w lokalach danej delegatury Unii i w zakresie jej kompetencji oraz za zarządzanie tymi środkami.

W porozumieniu z właściwymi organami państwa przyjmującego podejmuje on w razie konieczności wszelkie racjonalnie możliwe działania dla zapewnienia, aby wprowadzono odpowiednie środki fizyczne i organizacyjne służące osiągnięciu tego celu.

Szef delegatury opracowuje w stosownych przypadkach procedury bezpieczeństwa służące ochronie osób na utrzymaniu w rozumieniu art. 2 lit. c) z uwzględnieniem wszelkich porozumień administracyjnych, o których mowa w art. 3 ust. 3. Szef delegatury przekazuje Dyrekcji ds. Bezpieczeństwa ESDZ coroczne sprawozdania dotyczące wszelkich kwestii bezpieczeństwa będących w zakresie jego kompetencji.

W wykonywaniu tych zadań jest on wspierany przez Dyrekcję ds. Bezpieczeństwa ESDZ, personel ESDZ w delegaturze wypełniający powierzone mu zadania i funkcje oraz specjalnych pracowników ochrony rozmieszczonych tam, gdzie jest to konieczne.

2. Ponadto szef delegatury:

— ustala szczegółowe plany bezpieczeństwa i plany awaryjne na podstawie ogólnych standardowych procedur działania;

— zapewnia skuteczne działanie, przez całą dobę i wszystkie dni tygodnia, systemu zarządzania incydentami związanymi z bezpieczeństwem i sytuacjami nadzwyczajnymi w zakresie działania delegatury;

— dopilnowuje, aby wszyscy członkowie personelu pracujący w delegaturze byli objęci ubezpieczeniem zgodnie z wymogami obowiązującymi na danym obszarze;

— zapewnia, aby w szkoleniach udzielanych wszystkim członkom personelu przydzielonym do pracy w delegaturze przed ich przybyciem do delegatury lub niezwłocznie po nim uwzględniano kwestie bezpieczeństwa oraz

— zapewnia wdrożenie wszelkich zaleceń wynikających z ocen bezpieczeństwa oraz regularnie przekazuje do organu ESDZ ds. bezpieczeństwa pisemne sprawozdania dotyczące wdrożenia tych zaleceń oraz innych kwestii bezpieczeństwa.

3. Bez uszczerbku dla odpowiedzialności i rozliczalności za zapewnienie zarządzania kwestiami bezpieczeństwa oraz odporności organizacji, szef delegatury może delegować wykonanie swoich zadań w zakresie bezpieczeństwa koordynatorowi delegatury ds. bezpieczeństwa, który jest zastępcą szefa delegatury, a w wypadku kiedy nie został on powołany – innej odpowiedniej osobie.

Koordynatorowi delegatury ds. bezpieczeństwa można powierzyć w szczególności następujące działania:

— utrzymywanie kontaktów w kwestiach bezpieczeństwa z właściwymi organami państwa przyjmującego oraz odpowiednimi osobami w ambasadach i misjach dyplomatycznych państw członkowskich;

— wdrażanie odpowiednich procedur zarządzania bezpieczeństwem związanych z interesami bezpieczeństwa ESDZ, w tym z ochroną EUCI;

— udzielanie personelowi instruktaży na temat obowiązujących przepisów bezpieczeństwa oraz na temat szczególnych zagrożeń w danym państwie przyjmującym;

— składanie wniosków do Dyrekcji ds. Bezpieczeństwa ESDZ dotyczących stanowisk, które wymagają poświadczenia bezpieczeństwa osobowego oraz

— ciągłe informowanie szefa delegatury, regionalnego pełnomocnika ds. ochrony i Dyrekcji ds. Bezpieczeństwa ESDZ o incydentach lub wydarzeniach w tej dziedzinie, mających znaczenie dla ochrony interesów bezpieczeństwa ESDZ.

4. Szef delegatury może delegować zadania związane z bezpieczeństwem o charakterze administracyjnym lub technicznym kierownikowi administracyjnemu oraz innym członkom personelu delegatury.

5. Delegaturę Unii wspomaga regionalny pełnomocnik ds. ochrony. Każdy regionalny pełnomocnik ds. ochrony wykonuje niżej opisane zadania w delegaturach należących do jego geograficznego zakresu kompetencji.

W pewnych okolicznościach, jeśli wymaga tego aktualna sytuacja pod względem bezpieczeństwa, do konkretnej delegatury może zostać przypisany w pełnym wymiarze czasu osobny regionalny pełnomocnik ds. ochrony.

Regionalny pełnomocnik ds. ochrony może być zobowiązany do przeniesienia się poza swój obecny obszar kompetencji, w tym do głównej siedziby w Brukseli, lub nawet objąć stanowisko o stałej lokalizacji z uwagi na sytuację w zakresie bezpieczeństwa w danym kraju i zgodnie z wymogami Dyrekcji ds. Bezpieczeństwa ESDZ.

6. Pod względem hierarchicznym regionalni pełnomocnicy ds. ochrony podlegają bezpośrednio Dyrekcji ds. Bezpieczeństwa ESDZ, natomiast pod względem funkcjonalnym i administracyjnym – szefom poszczególnych delegatur. Wspomagają oni szefów i personel delegatur w organizowaniu i realizacji wszelkich środków fizycznych, organizacyjnych i proceduralnych dotyczących bezpieczeństwa wszystkich członków personelu delegatur niezależnie od ich pochodzenia administracyjnego.

7. Regionalni pełnomocnicy ds. ochrony służą szefom i personelowi delegatur radą i wsparciem. W stosownych przypadkach, szczególnie jeśli dany regionalny pełnomocnik ds. ochrony jest przypisany do konkretnej delegatury i wykonuje w niej obowiązki w pełnym wymiarze czasu, może on wspomagać tę delegaturę w zakresie zarządzania środkami bezpieczeństwa i wdrażania ich, w tym w przygotowywaniu umów w zakresie bezpieczeństwa oraz zarządzaniu akredytacjami i poświadczeniami.

Artykuł 13

Działania w ramach WPBiO i specjalni przedstawiciele UE

Dyrekcja ds. Bezpieczeństwa ESDZ oferuje pomoc i radę dyrektorowi Dyrekcji ds. Zarządzania Kryzysowego i Planowania, dyrektorowi generalnemu Sztabu Wojskowego UE, cywilnemu dowódcy operacji, kierującemu Komórką Planowania i Prowadzenia Operacji Cywilnych oraz dowódcom operacji wojskowych UE w zakresie aspektów bezpieczeństwa działań w ramach WPBiO, a także specjalnym przedstawicielom UE – w zakresie kwestii bezpieczeństwa związanych z pełnionymi przez nich funkcjami, w uzupełnieniu szczegółowych przepisów w tym zakresie, przewidzianych w odpowiednich politykach przyjętych przez Radę.

Artykuł 14

Komitet ds. Bezpieczeństwa ESDZ

1. Niniejszym ustanawia się Komitet ds. Bezpieczeństwa ESDZ.

Komitetowi przewodniczy dyrektor ds. operacyjnych lub wyznaczona przez niego osoba, a zbiera się on na polecenie przewodniczącego lub na wniosek jednego z członków. Dyrekcja ds. Bezpieczeństwa ESDZ wspiera przewodniczącego w wykonywaniu jego obowiązków i w razie konieczności służy wsparciem administracyjnym prac Komitetu.

2. Komitet ds. Bezpieczeństwa ESDZ składa się z przedstawicieli:

— każdego z państw członkowskich;

— Biura ds. Bezpieczeństwa Sekretariatu Generalnego Rady;

— Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji.

Delegacja państwa członkowskiego w Komitecie ds. Bezpieczeństwa ESDZ może składać się z członków:

— krajowej władzy bezpieczeństwa lub wyznaczonej władzy bezpieczeństwa;

— departamentu ds. bezpieczeństwa w ministerstwie spraw zagranicznych.

3. W przypadkach, w których przedstawiciele Komitetu uznają to za konieczne, mogą im towarzyszyć i służyć radą eksperci. Przedstawiciele innych instytucji, agencji lub organów UE mogą być zapraszani do udziału w dyskusjach dotyczących kwestii istotnych dla ich bezpieczeństwa.

4. Nie naruszając przepisów ust. 5 Komitet Bezpieczeństwa ESDZ wspiera ESDZ w formie konsultacji we wszelkich kwestiach bezpieczeństwa mających znaczenie dla działalności ESDZ oraz dla siedziby głównej i delegatur Unii.

W szczególności, nie naruszając przepisów ust. 5:

a) konsultacja z Komitetem ds. Bezpieczeństwa ESDZ jest konieczna w odniesieniu do:

   — polityk, wytycznych, pojęć lub innych dokumentów metodycznych dotyczących bezpieczeństwa, w szczególności w zakresie ochrony informacji niejawnych oraz środków, jakie należy podjąć w przypadku nieprzestrzegania przepisów bezpieczeństwa przez personel ESDZ;

   — technicznych aspektów bezpieczeństwa, które mogą mieć wpływ na decyzję Wysokiego Przedstawiciela o przedstawieniu Radzie zalecenia dotyczącego otwarcia negocjacji na temat umów o bezpieczeństwie informacji, o których mowa w art. 10 ust. 1 lit. a) załącznika A;

   — wszelkich ewentualnych zmian niniejszej decyzji;

b) konsultacja z Komitetem ds. Bezpieczeństwa ESDZ jest możliwa w stosownych przypadkach w odniesieniu do kwestii bezpieczeństwa personelu i majątku w siedzibie głównej ESDZ i w delegaturach Unii, nie naruszając przepisów art. 3 ust. 3;

c) Komitet ds. Bezpieczeństwa ESDZ powiadamia się o każdym nieuprawnionym ujawnieniu lub utracie EUCI, jakie nastąpiły w ESDZ.

5. Wszelkie zmiany zasad dotyczących ochrony EUCI określonych w niniejszej decyzji i w załączniku A wymagają jednogłośnej przychylnej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ. Taka jednogłośna przychylna opinia jest wymagana również przed:

— podjęciem negocjacji na temat porozumień administracyjnych, o których mowa w art. 10 ust. 1 lit. b) załącznika A;

— ujawnieniem informacji niejawnych w wyjątkowych okolicznościach, o których mowa w art. 9, 11 i 12 załącznika A VI;

— przyjęciem odpowiedzialności jako wytwórca informacji w okolicznościach, o których mowa w art. 10 ust. 4 zdanie ostatnie załącznika A.

W przypadku kiedy wymagana jest jednogłośna przychylna opinia, warunek ten jest spełniony, o ile żadna z delegacji państw członkowskich nie wyraża sprzeciwu w czasie obrad Komitetu.

6. Komitet ds. Bezpieczeństwa ESDZ w pełni uwzględnia polityki i wytyczne w zakresie bezpieczeństwa obowiązujące w Radzie i w Komisji.

7. Komitet ds. Bezpieczeństwa ESDZ otrzymuje wykaz corocznych inspekcji ESDZ oraz sprawozdania z inspekcji po ich zakończeniu.

8. Organizacja posiedzeń:

— Komitet ds. Bezpieczeństwa ESDZ spotyka się co najmniej dwa razy w roku. Przewodniczący może zorganizować dodatkowe posiedzenia w pełnym składzie bądź tylko z udziałem przedstawicieli krajowych władz bezpieczeństwa (KWB), wyznaczonych władz bezpieczeństwa (WWB) lub ministerstw spraw zagranicznych mających kompetencje w dziedzinie bezpieczeństwa; o zorganizowanie takich posiedzeń mogą zwrócić się też członkowie Komitetu.

— Komitet ds. Bezpieczeństwa ESDZ organizuje swoją działalność w taki sposób, aby móc przedstawiać zalecenia w konkretnych dziedzinach dotyczących bezpieczeństwa. Może on w razie potrzeby powoływać inne podgrupy eksperckie. Komitet wyznacza zakres zadań takich podgrup eksperckich i otrzymuje od nich sprawozdania z działalności.

— Dyrekcja ds. Bezpieczeństwa ESDZ odpowiada za przygotowywanie poszczególnych punktów do dyskusji. Przewodniczący sporządza wstępny porządek obrad każdego posiedzenia. Członkowie Komitetu mogą proponować dodatkowe punkty do dyskusji.

Artykuł 15

Inspekcje w zakresie bezpieczeństwa

1. Organ ESDZ ds. bezpieczeństwa zapewnia regularne przeprowadzanie w siedzibie głównej ESDZ i w delegaturach Unii inspekcji w zakresie bezpieczeństwa, których celem jest sprawdzenie, czy środki bezpieczeństwa są odpowiednie i zgodne z niniejszą decyzją. Dyrekcja ds. Bezpieczeństwa ESDZ może w stosownych przypadkach wyznaczać ekspertów, którzy będą brać udział w inspekcjach w zakresie bezpieczeństwa w agencjach i organach UE powoływanych na mocy tytułu V rozdział 2 TUE.

2. Inspekcje ESDZ w zakresie bezpieczeństwa odbywają się pod kierunkiem Dyrekcji ds. Bezpieczeństwa ESDZ, w stosownych wypadkach ze wsparciem ekspertów w dziedzinie bezpieczeństwa, reprezentujących inne instytucje UE lub państwa członkowskie, w szczególności w kontekście uzgodnień, o których mowa w art. 3 ust. 3.

3. ESDZ może w razie potrzeby korzystać z wiedzy fachowej w państwach członkowskich, Sekretariacie Generalnym Rady oraz Komisji.

W razie konieczności do udziału w inspekcji w zakresie bezpieczeństwa w delegaturze Unii mogą być zaproszeni odpowiedni eksperci w dziedzinie bezpieczeństwa pracujący w misjach państw członkowskich w państwach trzecich lub przedstawiciele departamentów zajmujących się bezpieczeństwem dyplomatycznym w państwach członkowskich.

4. Przepisy dotyczące wprowadzania w życie niniejszego artykułu w zakresie ochrony EUCI znajdują się w załączniku A III.

Artykuł 16

Wizyty oceniające

Aby stwierdzić skuteczność środków bezpieczeństwa stosowanych w państwie trzecim lub organizacji międzynarodowej w celu ochrony EUCI wymienianych na podstawie porozumienia administracyjnego, o którym mowa w art. 10 ust. 1 lit. b) załącznika A, przeprowadzane są wizyty oceniające.

Dyrekcja ds. Bezpieczeństwa ESDZ może wyznaczyć ekspertów do udziału w wizytach oceniających w państwach trzecich lub organizacjach międzynarodowych, z którymi UE zawarła umowę o bezpieczeństwie informacji, o której mowa w art. 10 ust. 1 lit. b) załącznika A.

Artykuł 17

Planowanie ciągłości działania

W ramach ogólnego planowania ciągłości działania ESDZ Dyrekcja ds. Bezpieczeństwa ESDZ wspiera dyrektora ds. operacyjnych w zarządzaniu aspektami procesów ciągłości działania ESDZ związanymi z bezpieczeństwem.

Artykuł 18

Porady dla osób podróżujących na misje poza UE

Dyrekcja ds. Bezpieczeństwa ESDZ udostępnia porady dla członków personelu podlegającego odpowiedzialności ESDZ, wyjeżdżającego na misje poza UE, z wykorzystaniem zasobów wszystkich odnośnych służb ESDZ, w szczególności SITROOM, INTCEN, departamentów geograficznych i delegatur Unii.

Na żądanie Dyrekcja ds. Bezpieczeństwa ESDZ przedstawia na podstawie wyżej wymienionych zasobów szczegółowe porady dla członków personelu podlegającego odpowiedzialności ESDZ, wyjeżdżającego na misje do państw trzecich o wysokim lub podwyższonym poziomie ryzyka.

Artykuł 19

Zdrowie i bezpieczeństwo

Przepisy bezpieczeństwa ESDZ stanowią uzupełnienie przyjętych przez Wysokiego Przedstawiciela zasad ESDZ dotyczących ochrony zdrowia i bezpieczeństwa.

Artykuł 20

Wdrożenie i przegląd

1. Organ ESDZ ds. bezpieczeństwa, w stosownych przypadkach po konsultacji z Komitetem ds. Bezpieczeństwa ESDZ, zatwierdza polityki lub wytyczne dotyczące bezpieczeństwa, określające wszelkie środki służące wdrażaniu niniejszych zasad w ESDZ, oraz zapewnia tworzenie niezbędnego potencjału obejmującego wszystkie aspekty bezpieczeństwa w ścisłej współpracy z organami państw członkowskich mającymi kompetencje w dziedzinie bezpieczeństwa oraz ze wsparciem odpowiednich służb instytucji UE.

2. Zgodnie z art. 4 ust. 5 decyzji Rady 2010/427/UE z dnia 26 lipca 2010 r. określającej organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych w razie potrzeby mogą być stosowane rozwiązania przejściowe z wykorzystaniem porozumień o gwarantowanym poziomie usług z odpowiednimi służbami Sekretariatu Generalnego Rady i Komisji.

3. Wysoki Przedstawiciel zapewnia ogólną spójność stosowania niniejszej decyzji i prowadzi przeglądy niniejszych przepisów bezpieczeństwa.

4. Przepisy bezpieczeństwa ESDZ wdraża się w ścisłej współpracy z organami państw członkowskich mającymi kompetencje w dziedzinie bezpieczeństwa, Biurem Bezpieczeństwa Sekretariatu Generalnego Rady oraz Dyrekcją ds. Bezpieczeństwa Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji.

5. ESDZ zapewnia uwzględnianie wszystkich aspektów procesu bezpieczeństwa w ramach systemu reagowania w sytuacjach kryzysowych ESDZ.

6. Wdrożenie niniejszej decyzji zapewniają dyrektor ds. operacyjnych jako organ ds. bezpieczeństwa ESDZ oraz kierownik Dyrekcji ds. Bezpieczeństwa ESDZ.

Artykuł 21

Zastąpienie poprzednich decyzji

1. Niniejsza decyzja uchyla i zastępuje decyzję Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 15 czerwca 2011 r. w sprawie przepisów bezpieczeństwa mających zastosowanie do Europejskiej Służby Działań Zewnętrznych ([1]).

2. Niniejsza decyzja uchyla decyzję Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 23 lutego 2011 r. w sprawie powołania i zadań delegowanego organu ds. bezpieczeństwa Europejskiej Służby Działań Zewnętrznych.

Artykuł 22

Przepisy końcowe

Niniejsza decyzja wchodzi w życie w dniu jej podpisania.

Zostaje ona opublikowana w *Dzienniku Urzędowym Unii Europejskiej*.

Właściwe organy ESDZ w odpowiednim terminie należycie informują wszystkich członków personelu objętych zakresem niniejszej decyzji i jej załączników o ich treści, wejściu w życie i wszelkich ewentualnych późniejszych zmianach.

Sporządzono w Brukseli dnia 19 kwietnia 2013 r.

Wysoki Przedstawiciel

C. ASHTON

([1]) Dz.U. C 304 z 15.10.2011, s. 5

ZAŁĄCZNIK A

ZASADY I NORMY OCHRONY EUCI

Artykuł 1

Cel, zakres stosowania i definicje

1. W niniejszym załączniku określa się podstawowe zasady i minimalne normy bezpieczeństwa służące ochronie EUCI.

2. Podstawowe zasady i minimalne normy mają zastosowanie do ESDZ w rozumieniu art. 1 niniejszej decyzji oraz personelu podlegającego odpowiedzialności ESDZ w rozumieniu definicji zawartej w art. 2 niniejszej decyzji.

Artykuł 2

Definicja EUCI, klauzule tajności i oznaczenia

1. „Informacje niejawne UE" (EUCI) 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.

2. EUCI otrzymują jedną z następujących klauzul tajności:

a) TRES 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;

b) SECRET UE/EU SECRET: informacje i materiały, których nieuprawnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informacje i materiały, których nieuprawnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;

d) RESTREINT UE/EU RESTRICTED: informacje i materiały, których nieuprawnione ujawnienie mogłoby być niekorzystne dla interesów Unii Europejskiej lub co najmniej jednego państwa członkowskiego.

3. EUCI nadaje się klauzulę tajności zgodnie z ust. 2. Można nadać im dodatkowe oznaczenie wskazujące na dziedzinę działalności, do której się odnoszą, na wytwórcę, ograniczenia dystrybucji, ograniczenia wykorzystania lub możliwość ujawnienia.

Artykuł 3

Oznaczanie klauzulami tajności

1. ESDZ zapewnia, by EUCI 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.

2. Obniżenie lub zniesienie klauzuli tajności nadanej EUCI bądź zmiana lub usunięcie oznaczeń, o których mowa w art. 2 ust. 3, wymagają uprzedniej pisemnej zgody wytwórcy.

3. Organ ESDZ ds. bezpieczeństwa, po konsultacji z Komitetem Bezpieczeństwa ESDZ zgodnie z art. 14 ust. 5 niniejszej decyzji, zatwierdza politykę bezpieczeństwa w zakresie wytwarzania EUCI, która obejmuje praktyczny przewodnik nadawania klauzul tajności.

Artykuł 4

Ochrona informacji niejawnych

1. EUCI podlegają ochronie zgodnie z niniejszą decyzją.

2. Posiadacz jakichkolwiek EUCI jest odpowiedzialny za ich ochronę zgodnie z niniejszą decyzją.

3. Jeżeli państwa członkowskie wprowadzają do struktur lub sieci ESDZ informacje niejawne, którym nadano krajową klauzulę tajności, ESDZ obejmują te informacje ochroną zgodnie z wymogami, które mają zastosowanie do EUCI mających równorzędną klauzulę tajności – zgodnie z tabelą odpowiedników klauzul tajności zamieszczoną w dodatku B do decyzji Rady 2011/292/WE z dnia 31 marca 2011 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE.

ESDZ ustanawia odpowiednie procedury w celu prowadzenia dokładnych rejestrów dotyczących wytwórcy:

— informacji niejawnych otrzymywanych przez ESDZ oraz

— materiałów źródłowych zawartych w informacjach niejawnych wytworzonych przez ESDZ.

O procedurach tych informuje się Komitet ds. Bezpieczeństwa ESDZ.

4. Uzasadnione może być objęcie dużych ilości lub kompilacji EUCI ochroną na poziomie właściwym dla wyższej klauzuli tajności niż klauzula, którą objęto ich części składowe.

Artykuł 5

Bezpieczeństwo osobowe w kontekście obchodzenia się z informacjami niejawnymi UE

1. Bezpieczeństwo osobowe oznacza stosowanie środków gwarantujących, że dostęp do EUCI jest przyznawany tylko osobom, które:

— spełniają zasadę ograniczonego dostępu;

— w odniesieniu do dostępu do informacji o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej – otrzymały poświadczenie bezpieczeństwa do odpowiedniego poziomu lub ze względu na pełnione przez siebie funkcje otrzymały inne odpowiednie uprawnienie zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; oraz

— zostały poinformowane o swoich obowiązkach.

2. W ramach procedur wydawania poświadczenia bezpieczeństwa osobowego (PBO) stwierdza się, czy daną osobę, ze względu na jej lojalność, wiarygodność i rzetelność, można uprawnić do dostępu do EUCI.

3. Przed uzyskaniem dostępu do EUCI, a następnie w regularnych odstępach czasu po jego uzyskaniu, wszystkie osoby informowane są o obowiązku ochrony EUCI zgodnie z niniejszą decyzją i potwierdzają na piśmie przyjęcie do wiadomości tego obowiązku.

4. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A I.

Artykuł 6

Bezpieczeństwo fizyczne informacji niejawnych UE

1. Bezpieczeństwo fizyczne oznacza stosowanie fizycznych i technicznych środków ochrony w celu powstrzymania nieuprawnionego dostępu do EUCI.

2. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie wtargnięciu osoby nieupoważnionej, w sposób niezauważony lub z użyciem siły, powstrzymanie od podjęcia nieuprawnionych działań, udaremnianie i wykrywanie takich działań oraz umożliwienie podziału personelu pod względem dostępu do EUCI zgodnie z zasadą ograniczonego dostępu. Środki te określane są na podstawie procesu zarządzania ryzykiem.

3. Środkami bezpieczeństwa fizycznego obejmuje się wszystkie lokale, budynki, biura, pomieszczenia i inne strefy, w których ma miejsce obchodzenie się z EUCI lub ich przechowywanie, w tym strefy, w których znajdują się systemy teleinformatyczne zdefiniowane w art. 8 ust. 2.

4. Strefy, w których przechowywane są EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, ustanawiane są strefami bezpieczeństwa zgodnie z załącznikiem A II; strefy takie zatwierdza organ ESDZ ds. bezpieczeństwa.

5. Do ochrony EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej wykorzystuje się wyłącznie zatwierdzony sprzęt lub zatwierdzone urządzenia.

6. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A II.

Artykuł 7

Zarządzanie informacjami niejawnymi

1. Zarządzanie informacjami niejawnymi polega na stosowaniu środków administracyjnych służących kontroli EUCI na wszystkich etapach ich cyklu życia w uzupełnieniu środków przewidzianych w art. 5, 6 i 8, co ma pomóc w powstrzymywaniu od zamierzonego lub przypadkowego nieuprawnionego ujawnienia lub utraty tych informacji, w wykrywaniu takich przypadków i usuwaniu ich skutków. Środki takie dotyczą w szczególności wytwarzania, rejestracji, kopiowania, tłumaczenia i przenoszenia EUCI, obchodzenia się z nimi, ich przechowywania i niszczenia.

2. Informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej są ze względów bezpieczeństwa rejestrowane przed dystrybucją i w momencie wpłynięcia. Właściwe organy ESDZ ustanawiają do tego celu system kancelarii tajnych. Informacje niejawne o klauzuli tajności TRES SECRET UE/EU TOP SECRET rejestruje się w wyznaczonych kancelariach tajnych.

3. Jednostki organizacyjne i lokale, w których ma miejsce obchodzenie się z EUCI lub ich przechowywanie, poddawane są regularnym inspekcjom przeprowadzanym przez organ ESDZ ds. bezpieczeństwa.

4. Poza strefami chronionymi fizycznie EUCI są przekazywane między jednostkami organizacyjnymi i lokalami w sposób następujący:

a) zgodnie z ogólną zasadą EUCI są przekazywane drogą elektroniczną chronioną przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 7 ust. 5 niniejszej decyzji oraz zgodnie z jasno zdefiniowanymi operacyjnymi procedurami bezpieczeństwa;

(b) gdy nie korzysta się ze sposobu, o którym mowa w lit. a), EUCI są przenoszone:

(i) za pomocą środków elektronicznych (jak np. pamięć USB, płyty kompaktowe, twarde dyski) chronionych przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 7 ust. 5 niniejszej decyzji; lub

(ii) we wszystkich pozostałych przypadkach – zgodnie z wytycznymi organu ESDZ ds. bezpieczeństwa wydanymi w myśl odpowiednich środków ochrony określonych w załączniku A III sekcja V.

5. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A III.

Artykuł 8

Ochrona EUCI podczas obchodzenia się z nimi w systemach teleinformatycznych

1. Zabezpieczanie informacji w ramach systemów teleinformatycznych oznacza pewność, że systemy te będą chronić informacje, z którymi będą się obchodzić, i będą działać zgodnie z przeznaczeniem i w każdej sytuacji, w której będzie to konieczne, pod kontrolą uprawnionych użytkowników. Skuteczne zabezpieczanie informacji musi gwarantować odpowiedni poziom poufności, integralności, dostępności, niezaprzeczalności i autentyczności. Zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem.

2. „System teleinformatyczny" oznacza każdy system umożliwiający obchodzenie się z informacjami w formie elektronicznej. System teleinformatyczny obejmuje wszystkie zasoby niezbędne do jego funkcjonowania, w tym infrastrukturę, organizację, personel oraz zasoby informatyczne. Niniejszy załącznik ma zastosowanie do wszelkich systemów teleinformatycznych ESDZ obchodzących się z EUCI.

3. System teleinformatyczny obchodzi się z EUCI zgodnie z koncepcją zabezpieczania informacji.

4. Wszystkie systemy teleinformatyczne obchodzące się z EUCI poddawane są procedurze akredytacji. Celem akredytacji jest upewnienie się, że zastosowano wszystkie odpowiednie środki bezpieczeństwa i że osiągnięto wystarczający poziom ochrony EUCI i systemu teleinformatycznego zgodnie z niniejszą decyzją. W świadectwie akredytacji określa się najwyższą klauzulę tajności informacji, z którymi może obchodzić się dany system teleinformatyczny, oraz odnośne warunki.

5. System teleinformatyczny obchodzący się z informacjami niejawnymi o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i wyższej jest chroniony w taki sposób, by wykluczyć nieuprawnione ujawnienie informacji z powodu niezamierzonych emisji elektromagnetycznych („środki bezpieczeństwa TEMPEST").

6. W przypadku gdy EUCI podlegają ochronie przy użyciu produktów kryptograficznych, produkty te są zatwierdzane w sposób zgodny z art. 7 ust. 5 niniejszej decyzji.

7. Podczas transmisji EUCI drogą elektroniczną stosuje się zatwierdzone produkty kryptograficzne. Niezależnie od tego wymogu w okolicznościach nadzwyczajnych mogą mieć zastosowanie szczególne procedury lub szczególne konfiguracje techniczne określone w załączniku A IV.

8. Zgodnie z art. 7 ust. 6 niniejszej decyzji ustanawia się, w zakresie, w jakim jest to niezbędne, następujące funkcje zabezpieczania informacji:

a) organ ds. zabezpieczania informacji (IAA);

b) organ ds. TEMPEST (TA);

c) organ ds. zatwierdzania produktów kryptograficznych (CAA);

d) organ ds. dystrybucji produktów kryptograficznych (CDA).

9. Zgodnie z art. 7 ust. 7 niniejszej decyzji w odniesieniu do każdego systemu ustanawia się:

a) organ ds. akredytacji bezpieczeństwa (SAA);

b) organ operacyjny ds. zabezpieczania informacji.

10. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A IV.

Artykuł 9

Bezpieczeństwo przemysłowe

1. Bezpieczeństwo przemysłowe oznacza stosowanie środków mających zapewnić ochronę EUCI przez wykonawców lub podwykonawców podczas negocjacji poprzedzających zawarcie umów i na wszystkich etapach cyklu życia umów niejawnych. Umowy takie co do zasady nie obejmują dostępu do informacji niejawnych o klauzuli tajności TRES SECRET UE/EU TOP SECRET.

2. ESDZ może na podstawie umowy powierzyć zadania obejmujące dostęp do EUCI lub wiążące się z nim bądź z obchodzeniem się z EUCI lub ich przechowywaniem przez podmioty gospodarcze lub inne, zarejestrowane w państwie członkowskim lub w państwie trzecim, z którym zawarto umowę dotyczącą bezpieczeństwa informacji lub porozumienie administracyjne, o których mowa w art. 10 ust. 1 załącznika A.

3. Jako instytucja zamawiająca ESDZ zapewnia, by w przypadku zawierania umów niejawnych z podmiotami gospodarczymi lub innymi spełnione były minimalne normy bezpieczeństwa przemysłowego określone w niniejszej decyzji i te, o których mowa w danej umowie. ESDZ zapewnia zgodność z wspomnianymi minimalnymi wymogami za pośrednictwem odpowiednich KWB lub WWB.

4. Wykonawcy lub podwykonawcy zarejestrowani w państwie członkowskim, będący stronami umów niejawnych lub niejawnych umów o podwykonawstwo, które to umowy wymagają od nich obchodzenia się z informacjami niejawnymi o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET i przechowywania ich podczas wykonywania takich umów lub na etapie poprzedzającym ich zawarcie, muszą posiadać świadectwo bezpieczeństwa przemysłowego (SBP) do odpowiedniego poziomu klauzuli tajności, wydane przez KWB, WWB lub jakikolwiek inny właściwy organ ds. bezpieczeństwa danego państwa członkowskiego.

5. Pracownicy 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, muszą posiadać poświadczenie bezpieczeństwa osobowego (PBO) wydane przez odpowiednią krajową władzę bezpieczeństwa (KWB), wyznaczoną władzę bezpieczeństwa (WWB) lub jakikolwiek inny właściwy organ bezpieczeństwa zgodnie z krajowymi przepisami ustawowymi i wykonawczymi oraz minimalnymi normami bezpieczeństwa określonymi w załączniku A I.

6. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A V.

Artykuł 10

Wymiana informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi

1. ESDZ może wymieniać EUCI z państwem trzecim lub organizacją międzynarodową wyłącznie pod warunkiem, że:

a) obowiązuje umowa o bezpieczeństwie informacji zawarta między UE a tym państwem trzecim lub organizacją międzynarodową zgodnie z art. 37 TUE i art. 218 TFUE lub

b) obowiązuje porozumienie administracyjne pomiędzy Wysokim Przedstawicielem a właściwymi organami ds. bezpieczeństwa tego państwa trzeciego lub organizacji międzynarodowej, regulujące wymianę informacji niejawnych opatrzonych klauzulą tajności co do zasady nie wyższą niż RESTREINT UE/EU RESTRICTED, zawarte zgodnie z procedurą określoną w art. 14 ust. 5 niniejszej decyzji lub

c) obowiązuje umowa ramowa lub umowa *ad hoc* w sprawie udziału zawarta między UE a tym państwem trzecim w kontekście operacji zarządzania kryzysowego WPBiO, zawarta zgodnie z art. 37 TUE i art. 218 TFUE

i spełniono warunki określone w tym instrumencie.

Wyjątki od ogólnej zasady opisanej powyżej określono w załączniku A VI sekcja V.

2. Porozumienia administracyjne, o których mowa w ust. 1 lit. b), 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.

Wymiana informacji na podstawie umów, o których mowa w ust. 1 lit. c), ogranicza się do informacji dotyczących działań WPBiO, w których uczestniczy dane państwo członkowskie na podstawie tych umów i zgodnie z ich postanowieniami.

3. Aby stwierdzić skuteczność środków bezpieczeństwa służących ochronie wymienianych EUCI organizuje się w państwach członkowskich lub organizacjach międzynarodowych wizyty oceniające, o jakich mowa w art. 16 niniejszej decyzji.

4. Decyzję o udostępnieniu EUCI, którymi dysponuje ESDZ, państwu trzeciemu lub organizacji międzynarodowej podejmuje się 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.

Dla upewnienia się, że nie ma przeciwwskazań do udostępnienia informacji, ESDZ zwraca się o pisemną zgodę do każdego podmiotu, który przekazał informację niejawną stanowiącą materiał źródłowy do EUCI wytworzonej przez ESDZ.

Jeżeli wytwórcą informacji niejawnej, o której udostępnienie wystąpiono, nie jest ESDZ, to ESDZ najpierw zwraca się o pisemną zgodę wytwórcy na jej udostępnienie.

Jeśli jednak ESDZ nie jest w stanie ustalić wytwórcy informacji, to organ ESDZ ds. bezpieczeństwa przyjmuje na siebie odpowiedzialność wytwórcy po uzyskaniu jednogłośnej przychylnej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ.

5. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A VI.

Artykuł 11

Naruszenia zasad bezpieczeństwa oraz nieuprawnione ujawnienie informacji niejawnych

1. Wszelkie naruszenia zasad bezpieczeństwa lub nieuprawnione ujawnienie informacji niejawnych lub podejrzenie takiego naruszenia lub ujawnienia należy niezwłocznie zgłaszać do Dyrekcji ds. Bezpieczeństwa ESDZ, która w stosownych przypadkach informuje Dyrekcję ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji oraz Biuro ds. Bezpieczeństwa Sekretariatu Generalnego Rady, a także państwo lub państwa członkowskie lub inne podmioty, których sprawa dotyczy.

2. Jeżeli wiadomo lub jeżeli istnieją uzasadnione przesłanki, by podejrzewać, że doszło do nieuprawnionego ujawnienia lub utraty informacji niejawnych, Dyrekcja ds. Bezpieczeństwa ESDZ informuje w stosownych przypadkach Dyrekcję ds. Bezpieczeństwa w Komisji, Biuro ds. Bezpieczeństwa w Sekretariacie Generalnym Rady lub krajową władzę bezpieczeństwa państwa lub państw członkowskich lub inne podmioty, których to dotyczy, oraz podejmuje wszelkie stosowne środki zgodnie z przepisami ustawowymi i wykonawczymi, w celu:

a) oceny potencjalnych szkód dla interesów UE lub państw członkowskich;

b) podjęcia właściwych środków w celu zapobieżenia powtórzeniu się podobnego przypadku;

c) zabezpieczenia dowodów;

d) zapewnienia zbadania tego przypadku przez personel niezwiązany bezpośrednio z danym naruszeniem w celu ustalenia przebiegu wydarzeń;

e) powiadomienia właściwych organów o skutkach danego wydarzenia i o podjętych działaniach oraz

f) poinformowania wytwórcy informacji.

3. Każdy członek personelu podlegającego odpowiedzialności ESDZ, odpowiedzialny za naruszenie przepisów bezpieczeństwa określonych w niniejszej decyzji, może podlegać postępowaniu dyscyplinarnemu zgodnie z mającymi zastosowanie zasadami i przepisami wykonawczymi.

Każda osoba odpowiedzialna za nieuprawnione ujawnienie lub utratę informacji niejawnych podlega postępowaniu dyscyplinarnemu lub sądowemu zgodnie z mającymi zastosowanie przepisami ustawowymi, zasadami i przepisami wykonawczymi.

W stosownych przypadkach informuje się niezwłocznie Dyrekcję ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji, Biuro ds. Bezpieczeństwa w Sekretariacie Generalnym Rady lub krajową władzę bezpieczeństwa państwa lub państw członkowskich lub inne podmioty, których sprawa dotyczy.

4. Na czas trwania dochodzenia dotyczącego danego naruszenia lub nieuprawnionego ujawnienia kierownik Dyrekcji ds. Bezpieczeństwa ESDZ może zawiesić dostęp danej osoby do EUCI i do lokali ESDZ. O decyzji takiej informuje się niezwłocznie Dyrekcję ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji, Biuro ds. Bezpieczeństwa w Sekretariacie Generalnym Rady lub krajową władzę bezpieczeństwa państwa lub państw członkowskich lub inne podmioty, których sprawa dotyczy.

ZAŁĄCZNIK A I

BEZPIECZEŃSTWO OSOBOWE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 5 załącznika A. Określa się w nim w szczególności kryteria, które powinna stosować ESDZ do oceny, czy daną osobę ze względu na jej lojalność, wiarygodność i rzetelność można uprawnić do dostępu do EUCI, a także procedury sprawdzające i administracyjne, które należy stosować w tym celu.

2. „Poświadczenie bezpieczeństwa osobowego" (PBO) w zakresie dostępu do EUCI to oświadczenie właściwego organu państwa członkowskiego, wydawane po zakończeniu postępowania sprawdzającego dotyczącego bezpieczeństwa, prowadzonego przez właściwe organy państwa członkowskiego; stanowi ono poświadczenie, że dana osoba – o ile stwierdzono, że spełnia ona zasadę ograniczonego dostępu – może uzyskać dostęp do EUCI opatrzonych klauzulą tajności do określonego poziomu (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonej daty; osobę taką określa się jako „posiadającą poświadczenie bezpieczeństwa".

3. „zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego" to zaświadczenie wydane przez organ ESDZ ds. bezpieczeństwa, potwierdzające, że dana osoba posiada poświadczenie bezpieczeństwa, oraz zawierające informację o poziomie klauzuli tajności EUCI, do których dana osoba może uzyskać dostęp, terminie ważności odpowiedniego PBO oraz terminie ważności samego zaświadczenia.

4. „Uprawnienie do dostępu do EUCI" to uprawnienie wydawane zgodnie z niniejszą decyzją przez organ ESDZ ds. bezpieczeństwa po wydaniu PBO przez odpowiednie organy państwa członkowskiego, stanowiące poświadczenie, że dana osoba – o ile stwierdzono, że spełnia ona zasadę ograniczonego dostępu – może uzyskać dostęp do EUCI opatrzonych klauzulą tajności do określonego poziomu (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonego terminu; osobę taką określa się jako „posiadającą poświadczenie bezpieczeństwa".

II. PRZYZNAWANIE UPRAWNIEŃ DO DOSTĘPU DO EUCI

5. Uprawnienie do dostępu do informacji o klauzuli tajności RESTREINT UE/EU RESTRICTED nie wymaga poświadczenia bezpieczeństwa i jest przyznawane po:

   a) ustaleniu związku statutowego lub umownego danej osoby z ESDZ;

   b) stwierdzeniu, że osoba ta spełnia zasadę ograniczonego dostępu;

   c) poinformowaniu tej osoby o przepisach i procedurach bezpieczeństwa służących ochronie EUCI i uzyskaniu od niej pisemnego potwierdzenia, że jest ona świadoma swoich obowiązków w zakresie ochrony EUCI zgodnie z niniejszą decyzją.

6. Daną osobę można uprawnić do dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej wyłącznie po tym, jak:

   a) stwierdzono, że spełnia ona zasadę ograniczonego dostępu;

   b) otrzymała ona PBO do odpowiedniego poziomu lub ze względu na pełnione przez nią funkcje przyznano jej inne odpowiednie upoważnienie zgodnie z krajowymi przepisami ustawowymi i wykonawczymi oraz

   c) została ona poinformowana o przepisach i procedurach bezpieczeństwa służących ochronie EUCI i potwierdziła na piśmie, że jest świadoma swoich obowiązków w zakresie ochrony takich informacji.

7. ESDZ określa, które stanowiska w jej strukturach wymagają dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej i w związku z tym wymagają uzyskania PBO do odpowiedniego poziomu zgodnie z art. 4.

8. Członkowie personelu ESDZ składają oświadczenia, w których informują, czy posiadają obywatelstwo więcej niż jednego państwa.

Procedury związane z ubieganiem się o PBO w ESDZ

9. W przypadku personelu ESDZ organ powołujący ESDZ przekazuje wypełnioną ankietę bezpieczeństwa osobowego krajowej władzy bezpieczeństwa w państwie członkowskim, którego obywatelem jest dana osoba, z wnioskiem o przeprowadzenie postępowania sprawdzającego do poziomu EUCI, do którego dostęp będzie tej osobie niezbędny.

10. W przypadku osoby posiadającej obywatelstwo więcej niż jednego państwa wniosek o postępowanie sprawdzające kieruje się do krajowej władzy bezpieczeństwa w tym państwie, którego obywatelstwem legitymowała się dana osoba przy przyjmowaniu jej do pracy.

11. Jeżeli ESDZ uzyska istotną dla postępowania sprawdzającego informację dotyczącą osoby, która złożyła wniosek o PBO, powiadamia o tym odpowiednią KWB, działając zgodnie z odpowiednimi zasadami i przepisami wykonawczymi.

12. Po zakończeniu postępowania sprawdzającego odpowiednia KWB powiadamia Dyrekcję ds. Bezpieczeństwa ESDZ o wyniku takiego postępowania.

a) Jeżeli w wyniku postępowania sprawdzającego uzyskuje się pewność, że nie istnieją żadne niekorzystne okoliczności, które mogłyby podważać lojalność, wiarygodność i rzetelność danej osoby, organ ESDZ ds. bezpieczeństwa może wydać tej osobie uprawnienie do dostępu do EUCI do odpowiedniego poziomu i do określonego terminu.

b) ESDZ podejmuje wszelkie stosowne środki dla zapewnienia należytego wdrożenia warunków lub ograniczeń nałożonych przez KWB. Krajową władzę bezpieczeństwa informuje się o wyniku.

c) Jeżeli w wyniku postępowania sprawdzającego nie uzyskuje się takiej pewności, organ ESDZ ds. bezpieczeństwa powiadamia o tym fakcie daną osobę, a ona może się do niego zwrócić z prośbą o wysłuchanie. Organ ESDZ ds. bezpieczeństwa może zwrócić się do właściwej KWB o przedstawienie wszelkich dalszych wyjaśnień, których może ona udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli wynik zostanie potwierdzony, nie wydaje się uprawnienia do dostępu do EUCI. W takim wypadku ESDZ podejmuje wszelkie stosowne środki w celu uniemożliwienia takiej osobie wszelkiego dostępu do EUCI.

13. Postępowanie sprawdzające oraz jego wyniki, stanowiące dla ESDZ podstawę do decyzji o przyznaniu lub odmowie uprawnienia do dostępu do EUCI, podlegają odpowiednim przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim, w tym także przepisom dotyczącym środków odwoławczych. Decyzje organu ESDZ ds. bezpieczeństwa podlegają środkom odwoławczym zgodnie z Regulaminem pracowniczym urzędników Unii Europejskiej i Warunkami zatrudnienia innych pracowników Unii Europejskiej, określonymi w rozporządzeniu (EWG, Euratom, EWWiS) nr 259/68 [1] (zwanymi dalej „regulaminem pracowniczym").

14. Pewność, na podstawie której wydaje się PBO, o ile jest ono nadal ważne, odnosi się do każdego zadania powierzonego danej osobie w ESDZ, Sekretariacie Generalnym Rady lub Komisji.

15. Jeżeli okres wykonywania przez daną osobę obowiązków służbowych nie rozpocznie się w terminie 12 miesięcy od powiadomienia organu ESDZ ds. bezpieczeństwa o wyniku postępowania sprawdzającego lub jeżeli w pełnieniu obowiązków przez daną osobę występuje przerwa trwająca 12 miesięcy lub dłużej, w czasie której osoba ta nie jest zatrudniona w ESDZ, w innych instytucjach, agencjach ani organach UE ani też na żadnym stanowisku w administracji krajowej państwa członkowskiego wymagającym dostępu do informacji niejawnych, wynik postępowania sprawdzającego jest przekazywany odpowiedniej KWB w celu potwierdzenia, czy nadal pozostaje ważny i właściwy.

16. W wypadku gdy ESDZ uzyska informację o ryzyku dla bezpieczeństwa przez osobę, która posiada ważne PBO, ESDZ powiadamia o tym odpowiednią KWB, działając zgodnie z odpowiednimi zasadami i przepisami wykonawczymi. Jeżeli KWB powiadomi ESDZ o utracie pewności uzyskanej zgodnie z pkt 12 lit. a) w odniesieniu do osoby posiadającej ważne uprawnienie do dostępu do EUCI, organ ESDZ ds. bezpieczeństwa może zwrócić się o przedstawienie wszelkich dalszych wyjaśnień, których KWB może udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli niekorzystne informacje zostaną potwierdzone, ww. uprawnienie 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.

17. O każdej decyzji w sprawie cofnięcia członkowi personelu ESDZ uprawnienia do dostępu do EUCI, a także w stosownych przypadkach o przyczynach tego cofnięcia, powiadamia się daną osobę, a ona może zwrócić się do organu ESDZ ds. bezpieczeństwa 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 ESDZ ds. bezpieczeństwa podlegają środkom odwoławczym zgodnie z regulaminem pracowniczym.

18. Eksperci krajowi oddelegowani do ESDZ na stanowisko wymagające dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej przedstawiają organowi ESDZ ds. bezpieczeństwa – przed rozpoczęciem wykonywania swoich zadań – ważne PBO uprawniające do dostępu do EUCI. Wyżej opisanym procesem zarządza wysyłające państwo członkowskie.

Rejestr PBO

19. ESDZ prowadzi bazę danych dotyczącą statusu wszystkich członków personelu podlegającego odpowiedzialności ESDZ oraz personelu wykonawców ESDZ pod względem poświadczenia bezpieczeństwa. Rejestr ten zawiera informacje o poziomie klauzuli tajności EUCI, do których dana osoba może mieć dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), dacie wydania PBO i okresie jego ważności.

20. Wprowadza się odpowiednie procedury koordynacji z państwami członkowskimi oraz innymi instytucjami, agencjami i organami UE w celu zapewnienia, że ESDZ posiada zgodny z prawdą i wyczerpujący wykaz statusu wszystkich członków personelu podlegającego odpowiedzialności ESDZ oraz personelu wykonawców ESDZ pod względem poświadczenia bezpieczeństwa.

[1] Dz.U. L 56 z 4.3.1968, s. 1.

21. Organ ESDZ ds. 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), terminie ważności odpowiedniego PBO oraz terminie ważności samego zaświadczenia.

Zwolnienia z wymogu posiadania PBO

22. Osobom uprawnionym do dostępu do EUCI ze względu na pełnione przez siebie funkcje zgodnie z krajowymi przepisami ustawowymi i wykonawczymi Dyrekcja ds. Bezpieczeństwa ESDZ udziela w stosownych przypadkach instrukcji dotyczącej ich obowiązków dotyczących bezpieczeństwa w zakresie ochrony EUCI.

III. SZKOLENIA I UPOWSZECHNIANIE WIEDZY W ZAKRESIE BEZPIECZEŃSTWA

23. Wszystkie osoby mające otrzymać uprawnienie do dostępu do EUCI oświadczają uprzednio na piśmie, że zrozumiały spoczywające na nich obowiązki w zakresie ochrony EUCI i konsekwencje ewentualnego nieuprawnionego ujawnienia EUCI. ESDZ zachowuje takie pisemne oświadczenia w aktach.

24. Wszystkie osoby, które są uprawnione do dostępu do EUCI lub muszą obchodzić się z EUCI, są na początku powiadamiane o zagrożeniach bezpieczeństwa, a następnie odbierają regularne instrukcje w zakresie tych zagrożeń; osoby te muszą bezzwłocznie zgłaszać właściwym organom bezpieczeństwa wszelkie zdarzenia lub wszelką działalność, które uznają za podejrzane lub nietypowe.

25. Wszystkie osoby, które uzyskały uprawnienie do dostępu do EUCI, podlegają środkom stałego bezpieczeństwa osobowego (tj. stałej opiece) przez cały okres obchodzenia się przez nie z EUCI. Stałe bezpieczeństwo osobowe należy do zakresu odpowiedzialności:

a) osób, którym udzielono dostępu do EUCI: osoby te są osobiście odpowiedzialne za własne postępowanie w zakresie bezpieczeństwa i muszą bezzwłocznie zgłaszać właściwym organom bezpieczeństwa wszelkie zdarzenia lub wszelką działalność, które uznają za podejrzane lub nietypowe, a także wszelkie zmiany we własnej sytuacji osobistej, które mogą mieć znaczenie dla ich PBO lub uprawnienia do dostępu do EUCI;

b) bezpośredni przełożeni: odpowiadają oni za to, aby ich personel był zaznajomiony ze środkami bezpieczeństwa i własnymi obowiązkami w zakresie ochrony EUCI, a także za monitorowanie postępowania personelu w zakresie bezpieczeństwa oraz za rozwiązywanie we własnym zakresie wszelkich problemów związanych z bezpieczeństwem lub przekazywanie odpowiednim organom ds. bezpieczeństwa wszelkich negatywnych informacji, które mogą mieć znaczenie dla PBO podlegającego im personelu lub na udzielanie im uprawnienia do dostępu do EUCI;

c) osoby odpowiedzialne za bezpieczeństwo w ramach organizacji bezpieczeństwa ESDZ, o której mowa w art. 12 niniejszej decyzji: odpowiadają one za okresowe organizowanie szkoleń dla zapewnienia personelowi w ich obszarze odpowiedzialności wiedzy na temat bezpieczeństwa, kształtowanie silnej kultury bezpieczeństwa w ich obszarze odpowiedzialności, wprowadzenie środków monitorowania postępowania personelu w zakresie bezpieczeństwa oraz za zgłaszanie odpowiednim organom ds. bezpieczeństwa wszelkich negatywnych informacji, które mogą mieć znaczenie dla PBO którejkolwiek osoby;

d) ESDZ i państwa członkowskie: uruchamiają specjalne kanały przekazywania informacji, które mogą mieć znaczenie dla PBO którejkolwiek osoby lub jej uprawnienie do dostępu do EUCI.

26. 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.

IV. WYJĄTKOWE OKOLICZNOŚCI

27. W nagłych przypadkach, jeżeli jest to należycie uzasadnione interesami ESDZ, w oczekiwaniu na zakończenie pełnego postępowania sprawdzającego organ ESDZ ds. bezpieczeństwa 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 ESDZ tymczasowe uprawnienie do dostępu do EUCI, by mogli wykonać określone zadania. Pełne postępowanie sprawdzające należy przeprowadzić w najbliższym możliwym terminie. Takie tymczasowe uprawnienia zachowują ważność przez okres nieprzekraczający sześciu miesięcy i nie uprawniają do dostępu do informacji niejawnych o klauzuli tajności TRES 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 ewentualnego nieuprawnionego ujawnienia EUCI. ESDZ zachowuje takie pisemne oświadczenia w aktach.

28. Jeżeli dana osoba ma objąć stanowisko, które wymaga PBO na poziomie o jeden stopień wyższym niż aktualnie posiadany przez nią, może ona tymczasowo pełnić obowiązki związane z tym stanowiskiem, pod warunkiem że:

a) bezwzględna potrzeba dostępu do EUCI o wyższej klauzuli tajności jest uzasadniona na piśmie przez przełożonego tej osoby;

b) dostęp jest ograniczony do konkretnych EUCI, które są potrzebne do pracy na tym stanowisku;

c) osoba ta posiada ważne PBO;

d) podjęto czynności w celu uzyskania uprawnienia do dostępu do informacji na poziomie wymaganym na tym stanowisku;

e) właściwy organ dokonał sprawdzenia, które potwierdziło, że dana osoba nie naruszała poważnie ani wielokrotnie przepisów dotyczących bezpieczeństwa;

f) objęcie tego stanowiska przez daną osobę zatwierdził właściwy organ ESDZ oraz

g) zasięgnięto opinii właściwej KWB lub WWB, która wydała PBO danej osoby, i władza ta nie wyraziła sprzeciwu;

h) 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.

29. Powyższa procedura jest stosowana, by przyznać danej osobie jednorazowy dostęp do EUCI o klauzuli tajności o jeden poziom wyższej niż klauzula, do której odnosi się poświadczenie bezpieczeństwa danej osoby. Z procedury tej nie korzysta się w sposób wielokrotny.

30. 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, Wysoki Przedstawiciel, wykonawczy sekretarz generalny lub dyrektor ds. operacyjnych 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.

31. Taki nadzwyczajny dostęp do informacji niejawnych o klauzuli tajności TRES SECRET UE/EU TOP SECRET przysługuje tylko obywatelom UE, których upoważniono do dostępu do informacji niejawnych o klauzuli krajowej odpowiadającej klauzuli tajności TRES SECRET UE/EU TOP SECRET albo do informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET.

32. O przypadkach skorzystania z procedury przedstawionej w pkt 29 i 30 informuje się Komitet ds. Bezpieczeństwa ESDZ.

33. Komitet ds. Bezpieczeństwa ESDZ otrzymuje roczne sprawozdanie na temat korzystania z procedur określonych w niniejszej sekcji.

V. UDZIAŁ W POSIEDZENIACH W SIEDZIBIE GŁÓWNEJ ESDZ I W DELEGATURACH UNII

34. Osoby wyznaczone do udziału w posiedzeniach w siedzibie głównej ESDZ i w delegaturach Unii, podczas których omawiane są informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, mogą brać w nich udział tylko po potwierdzeniu statusu ich PBO. W przypadku przedstawicieli państw członkowskich i urzędników Sekretariatu Generalnego Rady oraz Komisji ich ZPBO lub inny dowód posiadania przez nich PBO przesyłany jest przez odpowiednie organy do Dyrekcji ds. Bezpieczeństwa ESDZ lub do koordynatora delegatury Unii ds. bezpieczeństwa bądź, w sytuacjach wyjątkowych, przedstawiany jest przez osobę, której dotyczy. W stosownych przypadkach można zastosować zbiorczy wykaz nazwisk, przedstawiając odpowiednie dowody posiadania PBO.

35. W przypadku cofnięcia PBO uprawniającego do dostępu do EUCI osobie, której obowiązki obejmują uczestnictwo w posiedzeniach w siedzibie głównej ESDZ i w delegaturach Unii, podczas których omawiane są informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, właściwy organ informuje o tym ESDZ.

VI. POTENCJALNY DOSTĘP DO EUCI

36. Osoby, które mają zostać zatrudnione w warunkach stwarzających potencjalny dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, muszą posiadać odpowiednie poświadczenie bezpieczeństwa lub przez cały czas towarzyszy im eskorta.

37. Kurierzy, strażnicy i eskorta muszą posiadać poświadczenie bezpieczeństwa do odpowiedniego poziomu lub są w inny sposób odpowiednio sprawdzani zgodnie z krajowymi przepisami ustawowymi i wykonawczymi oraz otrzymują regularne instruktaże dotyczące procedur bezpieczeństwa w zakresie ochrony EUCI i obowiązku ochrony informacji, które im powierzono lub do których mogą mimowolnie mieć dostęp.

ZAŁĄCZNIK A II

BEZPIECZEŃSTWO FIZYCZNE INFORMACJI NIEJAWNYCH UE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 6 załącznika A. Określa się w nim minimalne wymogi w zakresie fizycznej ochrony lokali, budynków, biur, pomieszczeń i innych stref, w których ma miejsce obchodzenie się z EUCI i ich przechowywanie, w tym stref, w których znajdują się CIS.

2. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie nieuprawnionemu dostępowi do EUCI poprzez:

   a) zapewnienie właściwego obchodzenia się z EUCI i ich przechowywania;

   b) umożliwienie podziału pracowników pod względem dostępu do EUCI zgodnie z zasadą ograniczonego dostępu i, w odpowiednich przypadkach, posiadanym przez nich poświadczeniem bezpieczeństwa;

   c) powstrzymywanie nieuprawnionych działań, ich udaremnianie i wykrywanie; oraz

   d) uniemożliwienie lub opóźnienie wtargnięcia osób nieupoważnionych w sposób niezauważony lub z użyciem siły.

II WYMOGI I ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

3. ESDZ stosuje w swoich lokalach proces zarządzania ryzykiem służący ochronie EUCI, aby zapewnić poziom ochrony fizycznej proporcjonalny do szacowanego ryzyka. W procesie zarządzania ryzykiem uwzględnia się wszystkie istotne czynniki, a w szczególności:

   a) klauzulę tajności EUCI;

   b) postać i ilość EUCI, z uwzględnieniem faktu, że duża ilość EUCI lub ich kompilacja mogą wymagać zastosowania bardziej rygorystycznych środków ochrony;

   c) otoczenie i strukturę budynków lub stref, w których znajdują się EUCI;

   d) ocenę zagrożenia w danym państwie trzecim, opracowaną przez INTCEN w szczególności na podstawie sprawozdań delegatur Unii oraz

   e) szacowane zagrożenie ze strony służb wywiadowczych, których celem jest UE lub państwa członkowskie, oraz zagrożenie sabotażem, terroryzmem, działalnością wywrotową lub inną działalnością przestępczą.

4. Stosując koncepcję ochrony w głąb, organ ESDZ ds. bezpieczeństwa określa właściwą kombinację środków bezpieczeństwa fizycznego, które należy zastosować. Mogą one obejmować jeden z poniższych środków lub większą ich liczbę:

   a) ogrodzenie: fizyczne ogrodzenie, które chroni granice strefy wymagającej ochrony;

   b) 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;

   c) 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;

   d) pracownicy ochrony: przeszkoleni, nadzorowani, a w razie konieczności posiadający poświadczenie bezpieczeństwa pracownicy ochrony mogą być zatrudniani m.in. w celu powstrzymania osób planujących niezauważone wejście na dany teren;

   e) 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 ich granicach;

   f) 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

g) wszelkie inne stosowne środki fizyczne służące powstrzymywaniu lub wykrywaniu przypadków nieuprawnionego dostępu lub zapobieganiu utracie lub uszkodzeniu EUCI.

5. Dyrekcja ds. Bezpieczeństwa ESDZ może przeprowadzać przeszukania osób wchodzących i wychodzących jako środek odstraszający przed nieuprawnionym wnoszeniem materiałów lub nieuprawnionym wynoszeniem EUCI z lokali lub budynków.

6. Jeżeli istnieje ryzyko podglądu EUCI, także przypadkowego, podejmuje się stosowne środki w celu zlikwidowania takiego ryzyka.

7. W przypadku nowych obiektów wymogi dotyczące bezpieczeństwa fizycznego i specyfikacje dotyczące ich stosowania określane są w ramach planowania i projektowania tych obiektów. W przypadku obiektów już istniejących wymogi dotyczące bezpieczeństwa fizycznego stosowane są w największym możliwym zakresie.

III. SPRZĘT SŁUŻĄCY DO FIZYCZNEJ OCHRONY EUCI

8. Przy zakupie sprzętu służącego do fizycznej ochrony EUCI (takiego jak zabezpieczone szafy, niszczarki, zamki do drzwi, elektroniczne systemy kontroli dostępu, SSWiN, systemy alarmowe) organ ESDZ ds. bezpieczeństwa zapewnia, by sprzęt ten spełniał zatwierdzone normy techniczne i minimalne wymogi.

9. Specyfikacje techniczne sprzętu, który ma być wykorzystywany do fizycznej ochrony EUCI, określane są w wytycznych dotyczących bezpieczeństwa, które zatwierdza Komitet ds. Bezpieczeństwa ESDZ.

10. Systemy bezpieczeństwa są poddawane regularnym inspekcjom, a sprzęt – regularnej konserwacji. Podczas konserwacji uwzględnia się wyniki inspekcji, aby zapewnić dalsze optymalne działanie sprzętu.

11. Podczas każdej inspekcji przeprowadza się ocenę skuteczności poszczególnych środków bezpieczeństwa oraz całego systemu bezpieczeństwa.

IV. STREFY CHRONIONE FIZYCZNIE

12. Ustanawia się dwa rodzaje stref chronionych fizycznie lub ich krajowych odpowiedników, służących fizycznej ochronie EUCI:

a) strefy administracyjne oraz

b) strefy bezpieczeństwa (w tym strefy technicznie zabezpieczone).

13. Organ ESDZ ds. bezpieczeństwa stwierdza, czy dana strefa spełnia wymogi potrzebne do uznania jej za strefę administracyjną, strefę bezpieczeństwa lub strefę technicznie zabezpieczoną.

14. W przypadku stref administracyjnych:

(a) wyraźnie określa się granicę umożliwiającą kontrolę osób i, jeżeli to możliwe, pojazdów;

(b) dostęp bez eskorty umożliwia się tylko osobom odpowiednio upoważnionym przez Dyrekcję ds. Bezpieczeństwa ESDZ; oraz

c) wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równorzędnej kontroli.

15. W przypadku stref bezpieczeństwa:

a) wyraźnie określa się i chroni granicę, na której wszelkie wejścia i wyjścia kontrolowane są za pomocą przepustki lub systemu rozpoznawania osób;

b) dostęp bez eskorty umożliwia się tylko osobom posiadającym poświadczenie bezpieczeństwa do odpowiedniego poziomu i wyraźnie upoważnionym do wejścia do danej strefy zgodnie z zasadą ograniczonego dostępu;

c) wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równorzędnej kontroli.

16. 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:

a) wyraźnie wskazuje się najwyższą klauzulę tajności, którą przyznano informacjom zwykle przechowywanym w tej strefie;

b) wszystkie osoby wchodzące do tej strefy muszą posiadać specjalne upoważnienie, przez cały czas towarzyszy im eskorta i muszą one posiadać odpowiednie poświadczenie bezpieczeństwa, chyba że podjęte zostały kroki służące uniemożliwieniu dostępu do EUCI;

c) urządzenia elektroniczne pozostawia się poza tą strefą.

17. Strefy bezpieczeństwa chronione przed podsłuchem uznawane są za strefy technicznie zabezpieczone. Zastosowanie mają następujące dodatkowe wymogi:

a) 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 niniejszego załącznika;

(b) wszystkie osoby wchodzące do takich stref lub materiały tam wnoszone podlegają kontroli;

c) strefy takie podlegają regularnym inspekcjom fizycznym lub technicznym zgodnie z wymogami organu ESDZ ds. bezpieczeństwa. Inspekcje takie przeprowadza się także po każdorazowym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście miało miejsce; oraz

d) w strefach takich nie mogą się znajdować niezatwierdzone linie telekomunikacyjne, niezatwierdzone telefony, inne niezatwierdzone urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny.

18. Niezależnie od pkt 17 lit. d), zanim urządzenia komunikacyjne i sprzęt elektryczny lub elektroniczny zostaną użyte w strefach, w których odbywają się posiedzenia lub prowadzone są prace związane z wykorzystaniem informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET i wyższej, a także jeżeli ocenia się, że istnieje wysokie zagrożenie dla EUCI, urządzenia i sprzęt taki zostają najpierw sprawdzone przez organ ESDZ ds. bezpieczeństwa w celu zapewnienia, aby żadne zrozumiałe informacje nie mogły zostać nieumyślnie lub nielegalnie przekazane przez taki sprzęt poza granicę strefy bezpieczeństwa.

19. Strefy bezpieczeństwa, w których nie pracują w systemie całodobowym pracownicy pełniący dyżur, są w odpowiednich przypadkach poddawane inspekcji na koniec normalnych godzin pracy i w przypadkowych odstępach czasu poza tymi godzinami, chyba że znajdują się tam SSWiN.

20. Strefy bezpieczeństwa oraz strefy technicznie zabezpieczone mogą być tworzone tymczasowo na terenie stref administracyjnych w celu zorganizowania niejawnego posiedzenia lub w jakimkolwiek innym podobnym celu.

21. Dla każdej strefy bezpieczeństwa opracowywane są procedury bezpiecznej eksploatacji określające:

a) poziom klauzuli tajności EUCI, które można wykorzystywać i przechowywać w tej strefie;

b) środki nadzoru i ochrony, które należy stosować;

c) osoby upoważnione do wejścia do strefy bez eskorty ze względu na zasadę ograniczonego dostępu i posiadane poświadczenie bezpieczeństwa;

d) w odpowiednich przypadkach procedury dotyczące eskort lub ochrony EUCI, jeżeli zezwala się na wejście do strefy innym osobom;

e) wszelkie inne odpowiednie środki i procedury.

22. W ramach stref bezpieczeństwa są budowane wzmocnione pomieszczenia. Ściany, podłogi, sufity, okna oraz drzwi wyposażone w zamki zatwierdzane są przez organ ESDZ ds. bezpieczeństwa i zapewniają ochronę równoważną zabezpieczonym szafom zatwierdzonym do celów przechowywania EUCI o tym samym poziomie klauzuli tajności.

V. FIZYCZNE ŚRODKI OCHRONY NA POTRZEBY OBCHODZENIA SIĘ Z EUCI I ICH PRZECHOWYWANIA

23. Wykorzystywanie EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED może się odbywać:

a) w strefie bezpieczeństwa;

b) w strefie administracyjnej, pod warunkiem że EUCI są chronione przed dostępem osób nieupoważnionych; lub

c) poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz przenosi EUCI zgodnie z załącznikiem A III pkt 30–42 i zobowiązał się do zastosowania środków zastępczych określonych w instrukcjach bezpieczeństwa, wydanych przez organ ESDZ ds. bezpieczeństwa, służących zapewnieniu, aby nieupoważnione osoby nie miały dostępu do EUCI.

24. EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED przechowywane są w odpowiednim do tego celu zamkniętym meblu biurowym w strefie administracyjnej lub strefie bezpieczeństwa. Mogą być one tymczasowo przechowywane poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz zobowiązał się do zastosowania środków zastępczych określonych w instrukcjach bezpieczeństwa wydanych przez organ ESDZ ds. bezpieczeństwa.

25. Wykorzystywanie EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET może się odbywać:

    a) w strefie bezpieczeństwa;

    b) w strefie administracyjnej, pod warunkiem że EUCI są chronione przed dostępem osób nieupoważnionych; lub

    c) poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz:

        (i) przenosi EUCI zgodnie z załącznikiem A III pkt 30–42;

        (ii) zobowiązał się do zastosowania środków zastępczych określonych w instrukcjach bezpieczeństwa wydanych przez organ ESDZ ds. bezpieczeństwa, służących zapewnieniu, aby nieupoważnione osoby nie miały dostępu do EUCI;

        (iii) przechowuje EUCI przez cały czas pod swoją kontrolą; oraz

        (iv) w przypadku dokumentów w formie papierowej – powiadomił o tym fakcie właściwą kancelarię tajną.

26. EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET przechowywane są w strefie bezpieczeństwa w zabezpieczonej szafie lub wzmocnionym pomieszczeniu.

27. Wykorzystywanie EUCI o klauzuli tajności TRES SECRET UE/EU TOP SECRET odbywa się w strefie bezpieczeństwa.

28. EUCI o klauzuli tajności TRES SECRET UE/EU TOP SECRET przechowywane są w strefie bezpieczeństwa w siedzibie głównej, przy spełnieniu jednego z następujących warunków:

    a) są one przechowywane w zabezpieczonej szafie zgodnej z pkt 8, z co najmniej jednym z następujących zabezpieczeń dodatkowych:

        (i) stała ochrona lub kontrola przez posiadających poświadczenie bezpieczeństwa pracowników ochrony lub pracowników pełniących dyżur;

        (ii) zatwierdzony SSWiN obsługiwany przez pracowników odpowiedzialnych za bezpieczeństwo;

        lub

    b) są one przechowywane we wzmocnionym pomieszczeniu wyposażonym w SSWiN oraz obsługiwanym przez pracowników odpowiedzialnych za bezpieczeństwo.

29. Przepisy regulujące przenoszenie EUCI poza strefy chronione fizycznie znajdują się w załączniku A III.

VI. KONTROLA KLUCZY I KODÓW WYKORZYSTYWANYCH DO OCHRONY EUCI

30. Organ ESDZ ds. bezpieczeństwa określa procedury zarządzania kluczami i kodami do biur, pomieszczeń, wzmocnionych pomieszczeń i zabezpieczonych szaf. Procedury te chronią przed nieuprawnionym dostępem do informacji.

31. Kody są powierzane do zapamiętania jak najmniejszej liczbie osób, którym ich znajomość jest niezbędna. Kody do zabezpieczonych szaf i wzmocnionych pomieszczeń, w których przechowywane są EUCI, są zmieniane:

    a) w przypadku otrzymania nowej szafy;

    b) przy każdej zmianie pracowników znających kod;

    c) w każdym przypadku, gdy następuje rzeczywiste lub domniemane nieuprawnione ujawnienie informacji;

    d) gdy zamek poddano konserwacji lub naprawie; oraz

    e) co najmniej co 12 miesięcy.

ZAŁĄCZNIK A III

ZARZĄDZANIE INFORMACJAMI NIEJAWNYMI

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 7 załącznika A. Określa się w nim środki administracyjne służące kontroli EUCI na wszystkich etapach ich cyklu życia, co ma pomóc w powstrzymywaniu od zamierzonego lub przypadkowego nieuprawnionego ujawnienia takich informacji lub ich utraty, w wykrywaniu takich przypadków i usuwaniu ich skutków.

II. ZARZĄDZANIE KLAUZULAMI TAJNOŚCI

Klauzule tajności i oznaczenia

2. Informacjom nadaje się klauzulę tajności, jeżeli należy chronić ich poufność.

3. Za określenie poziomu klauzuli tajności, zgodnie z odpowiednimi wytycznymi w zakresie nadawania klauzul, i za dystrybucję informacji odpowiada wytwórca EUCI.

4. Poziom klauzuli tajności EUCI określa się zgodnie z art. 2 ust. 2 załącznika A i poprzez odniesienie do polityki bezpieczeństwa, która ma być zatwierdzona zgodnie z art. 3 ust. 3 załącznika A.

5. Informacjom niejawnym pochodzącym z państw członkowskich, przekazywanym ESDZ, zapewnia się ten sam poziom ochrony, jak w odniesieniu do EUCI opatrzonych równorzędną klauzulą tajności. Tabela równorzędnych odpowiedników klauzul tajności znajduje się w dodatku B do decyzji Rady 2011/292/UE z dnia 31 marca 2011 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE.

6. Klauzulę tajności, w stosownych przypadkach wraz z datą lub określeniem konkretnego wydarzenia, po którym klauzulę można obniżyć lub znieść, nanosi się wyraźnie i poprawnie, niezależnie od tego, czy dana EUCI ma formę pisemną, ustną, elektroniczną czy jakąkolwiek inną.

7. Poszczególne części danego dokumentu (np. strony, punkty, sekcje, załączniki, dodatki, załączone dokumenty i uzupełnienia) mogą wymagać nadania różnych klauzul tajności i zostają odpowiednio oznaczone, także wtedy, gdy są przechowywane w formie elektronicznej.

8. W stopniu, w jakim jest to możliwe, dokumenty, których częściom nadaje się różne klauzule tajności, są sporządzane w taki sposób, aby części oznaczone różnymi klauzulami można było łatwo zidentyfikować i w razie konieczności rozdzielić.

9. Ogólna klauzula tajności dokumentu lub pliku jest co najmniej tak wysoka jak klauzula tajności tej części dokumentu, która została oznaczona najwyższą klauzulą tajności. W przypadku zebrania informacji pochodzących z różnych źródeł sprawdza się ostateczną wersję dokumentu w celu określenia jego ogólnej klauzuli tajności, gdyż może istnieć konieczność nadania mu klauzuli tajności wyższej niż klauzule jego poszczególnych części.

10. Klauzula tajności pisma lub noty zawierających załączniki ma taki poziom jak najwyższa klauzula tajności nadana tym załącznikom. Wytwórca wyraźnie wskazuje, jaki poziom klauzuli tajności ma być nadany takiemu pismu lub nocie po ich odłączeniu od załączników, stosując w tym celu odpowiednie oznaczenie, np.:

CONFIDENTIEL UE/EU CONFIDENTIAL

RESTREINT UE/EU RESTRICTED bez załącznika(-ów)

Oznakowania

11. Oprócz jednej z klauzul tajności określonych w art. 2 ust. 2 załącznika A EUCI mogą być opatrzone dodatkowymi oznaczeniami, takimi jak:

    a) dane identyfikujące wytwórcę;

    b) wszelkie oznaczenia zastrzegające, kody słowne lub akronimy określające obszar działalności, do którego odnosi się dany dokument, szczególny sposób dystrybucji dokumentu zgodnie z zasadą ograniczonego dostępu lub ograniczenia w zakresie wykorzystania;

    c) oznaczenia dotyczące możliwości udostępnienia.

12. W następstwie decyzji o udostępnieniu EUCI państwu trzeciemu lub organizacji międzynarodowej Dyrekcja ds. Bezpieczeństwa ESDZ przekazuje daną informację niejawną, która jest opatrzona oznaczeniem dotyczącym możliwości jej udostępnienia, wskazującym państwo trzecie lub organizację międzynarodową, którym ma zostać udostępniona.

13. Organ ESDZ ds. bezpieczeństwa przechowuje wykaz takich zatwierdzonych oznaczeń.

Skrócone oznaczenia klauzul tajności

14. Dla wskazania poziomu klauzuli tajności nadanej pojedynczym ustępom tekstu można stosować standardowe skrócone oznaczenia klauzul tajności. Skróty nie zastępują pełnych nazw klauzul tajności.

15. W celu wskazania poziomu klauzuli tajności sekcji lub ciągłych fragmentów tekstu krótszych niż jedna strona w dokumentach niejawnych UE można stosować następujące standardowe skróty:

TRES 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

Wytwarzanie EUCI

16. Przy wytwarzaniu dokumentu niejawnego UE:

a) każdą stronę wyraźnie oznacza się klauzulą tajności;

b) strony numeruje się;

c) na dokumencie umieszcza się numer referencyjny i temat, który nie stanowi informacji niejawnej, chyba że z jego oznaczenia wynika inaczej;

d) na dokumencie umieszcza się datę;

e) na każdej stronie dokumentów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, które mają zostać rozpowszechnione w kilku kopiach, umieszcza się numer kopii.

17. Jeżeli do EUCI nie można zastosować pkt 15, podejmowane są inne odpowiednie środki zgodnie z wytycznymi dotyczącymi bezpieczeństwa, które należy ustalić na mocy niniejszej decyzji.

Obniżanie i znoszenie klauzul tajności EUCI

18. W momencie wytwarzania EUCI wytwórca wskazuje, o ile to możliwe, a w szczególności w odniesieniu do informacji niejawnych o klauzuli tajności RESTREINT UE/EU RESTRICTED, czy klauzula tajności EUCI może zostać obniżona lub zniesiona z daną datą lub w następstwie konkretnego wydarzenia.

19. ESDZ przeprowadza regularne przeglądy EUCI znajdujących się w jej posiadaniu, by stwierdzić, czy dana klauzula tajności ma nadal zastosowanie. ESDZ tworzy system służący do przeglądu klauzul tajności nadanych zarejestrowanym EUCI, których jest wytwórcą, nie rzadziej niż co pięć lat. Taki przegląd nie jest konieczny, jeżeli wytwórca określił na samym początku czas, po upływie którego klauzula tajności nadana danym informacjom zostanie automatycznie obniżona lub zniesiona, a informacje te zostały odpowiednio oznaczone.

III. REJESTRACJA EUCI ZE WZGLĘDÓW BEZPIECZEŃSTWA

20. W siedzibie głównej ustanawia się główną kancelarię tajną. Dla każdej jednostki organizacyjnej w ESDZ, w której wykorzystuje się EUCI, ustanawia się odpowiedzialną kancelarię tajną, podlegającą głównej kancelarii tajnej, w celu zapewnienia obchodzenia się z EUCI w sposób zgodny z niniejszą decyzją. Kancelarie tajne uznaje się za strefy bezpieczeństwa zgodnie z ich definicją w załączniku A.

Każda delegatura Unii ustanawia własną kancelarię tajną na potrzeby EUCI.

Organ ESDZ ds. bezpieczeństwa wyznacza dyrektora ds. kancelarii tajnych.

21. Do celów niniejszej decyzji rejestracja ze względów bezpieczeństwa (zwana dalej „rejestracją") oznacza stosowanie procedur rejestrowania etapów cyklu życia informacji, w tym jej dystrybucji i zniszczenia. W przypadku CIS procedury rejestracji mogą być stosowane w ramach działań samego CIS.

22. Wszystkie materiały o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i wyższej rejestruje się w momencie ich wpłynięcia do jednostki organizacyjnej, co obejmuje również delegatury Unii, lub wysłania z tej jednostki. Informacje niejawne o klauzuli tajności TRES SECRET UE/EU TOP SECRET rejestruje się w wyznaczonych kancelariach tajnych.

23. Główna kancelaria tajna stanowi w głównej siedzibie ESDZ główny punkt, do którego wpływają i z którego przekazywane są informacje niejawne wymieniane z państwami trzecimi i organizacjami międzynarodowymi. Główna kancelaria tajna rejestruje wszystkie takie wymiany informacji.

24. Wysoki Przedstawiciel zatwierdza politykę bezpieczeństwa dotyczącą rejestrowania EUCI ze względów bezpieczeństwa zgodnie z art. 14 niniejszej decyzji.

Kancelarie tajne Tres secret UE/EU top secret

25. W głównej siedzibie ESDZ wyznacza się główną kancelarię tajną będącą głównym organem otrzymującym i wysyłającym informacje niejawne o klauzuli tajności TRES SECRET UE/EU TOP SECRET. W razie konieczności można wyznaczyć podległe kancelarie tajne do wykorzystywania takich informacji do celów rejestracji.

26. Takie podległe kancelarie tajne nie mogą przekazywać dokumentów o klauzuli tajności TRES SECRET UE/EU TOP SECRET bezpośrednio innym podległym kancelariom tajnym podlegającym tej samej głównej kancelarii tajnej TRES SECRET UE/EU TOP SECRET ani na zewnątrz bez wyraźnego pisemnego upoważnienia z jej strony.

IV. KOPIOWANIE I TŁUMACZENIE DOKUMENTÓW NIEJAWNYCH UE

27. Dokumenty o klauzuli tajności TRES SECRET UE/EU TOP SECRET nie mogą być kopiowane ani tłumaczone bez wcześniejszej pisemnej zgody ich wytwórcy.

28. Jeżeli wytwórca dokumentów o klauzuli tajności SECRET UE/EU SECRET i niższej nie zgłosił zastrzeżeń co do ich kopiowania lub tłumaczenia, dokumenty takie można kopiować lub tłumaczyć na zlecenie posiadacza.

29. Środki bezpieczeństwa, które stosuje się do oryginału dokumentu, mają zastosowanie do jego kopii i tłumaczeń. Kopie dokumentów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej wykonuje wyłącznie właściwa kancelaria lub podkancelaria tajna za pomocą zabezpieczonej kopiarki. Kopie muszą być rejestrowane.

V. PRZENOSZENIE EUCI

30. Przenoszenie EUCI podlega środkom ochrony określonym w pkt 31–41. Gdy EUCI przenosi się na nośnikach elektronicznych, niezależnie od przepisów art. 7 ust. 4 załącznika A, poniższe środki ochrony mogą być uzupełnione odpowiednimi technicznymi środkami zaradczymi zgodnie z wytycznymi organu ESDZ ds. bezpieczeństwa, tak aby zminimalizować ryzyko utraty lub nieuprawnionego ujawnienia informacji.

31. Organ ESDZ ds. bezpieczeństwa wydaje instrukcje dotyczące przenoszenia EUCI zgodnie z niniejszą decyzją.

W obrębie budynku lub grupy budynków stanowiącej zamkniętą całość

32. EUCI przenoszone w ramach budynku lub grupy budynków stanowiącej zamkniętą całość zakrywa się, aby nie można było zobaczyć ich treści.

33. W ramach budynku lub grupy budynków stanowiącej zamkniętą całość informacje niejawne o klauzuli tajności TRES SECRET UE/EU TOP SECRET przenoszą osoby o odpowiednim poświadczeniu bezpieczeństwa w zabezpieczonej kopercie, na której znajduje się jedynie nazwisko adresata.

Na terytorium UE

34. EUCI przenoszone między budynkami lub obiektami na terytorium UE są opakowane w sposób zabezpieczający je przed nieuprawnionym ujawnieniem.

35. Przenoszenie informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET na terytorium UE odbywa się za pomocą jednego z następujących środków:

a) za pośrednictwem, w odpowiednich przypadkach, kurierów wojskowych, rządowych lub dyplomatycznych;

b) osobiście, pod warunkiem że:

(i) EUCI przez cały czas znajdują się w posiadaniu osoby przenoszącej, chyba że są przechowywane zgodnie z wymogami określonymi w załączniku A II;

(ii) EUCI nie są po drodze otwierane ani czytane w miejscach publicznych;

(iii) osoby przenoszące posiadają poświadczenie bezpieczeństwa do odpowiedniego poziomu i zostają poinformowane o obowiązkach w zakresie bezpieczeństwa;

(iv) w razie potrzeby osobom przenoszącym wydaje się list kurierski;

c) za pośrednictwem usług pocztowych lub prywatnych służb kurierskich, pod warunkiem że:

(i) są one zatwierdzone przez odpowiednią KWB zgodnie z krajowymi przepisami ustawowymi i wykonawczymi;

(ii) stosują one odpowiednie środki ochrony zgodnie z minimalnymi wymogami, które mają być ustalone w wytycznych dotyczących bezpieczeństwa zgodnie z art. 20 ust. 1 niniejszej decyzji.

W przypadku przewozu z jednego państwa członkowskiego do drugiego przepisy lit. c) są ograniczone do informacji niejawnych o klauzuli tajności do poziomu CONFIDENTIEL UE/EU CONFIDENTIAL.

36. Materiał oznaczony klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET (np. sprzęt lub urządzenia), który nie może być przewożony środkami, o których mowa w pkt 34, transportuje się jako ładunek przez prywatne firmy przewozowe zgodnie z załącznikiem A V.

37. Przenoszenie informacji niejawnych o klauzuli tajności TRES SECRET UE/EU TOP SECRET między budynkami lub obiektami na terytorium UE odbywa się za pośrednictwem, w odpowiednich przypadkach, kurierów wojskowych, rządowych lub dyplomatycznych.

Z terytorium UE na terytorium państwa trzeciego lub pomiędzy jednostkami organizacyjnymi UE w państwach trzecich

38. EUCI przewożone z terytorium UE na terytorium państwa trzeciego lub pomiędzy jednostkami organizacyjnymi UE w państwach trzecich są opakowane w sposób zabezpieczający je przed nieuprawnionym ujawnieniem.

39. Przewóz informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET z terytorium UE na terytorium państwa trzeciego oraz przenoszenie wszelkich EUCI o klauzuli tajności do poziomu SECRET UE/EU SECRET pomiędzy jednostkami organizacyjnymi UE w państwach trzecich odbywa się za pomocą jednego z następujących środków:

a) za pośrednictwem kurierów wojskowych lub dyplomatycznych;

b) osobiście, pod warunkiem że:

(i) przesyłka opatrzona jest urzędową pieczęcią lub sposób zapakowania wskazuje na to, że jest to przesyłka urzędowa i nie powinna podlegać kontroli celnej ani kontroli bezpieczeństwa;

(ii) osoba przenosząca posiada list kurierski zawierający informacje o przesyłce i upoważniający ją do przenoszenia tej przesyłki;

(iii) EUCI przez cały czas znajdują się w posiadaniu osoby przenoszącej, chyba że są przechowywane zgodnie z wymogami określonymi w załączniku A II;

(iv) EUCI nie są po drodze otwierane ani czytane w miejscach publicznych; oraz

(v) osoby przenoszące posiadają poświadczenie bezpieczeństwa do odpowiedniego poziomu oraz informuje się je o ich obowiązkach w zakresie bezpieczeństwa.

40. Przewóz informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET udostępnionych przez UE państwu trzeciemu lub organizacji międzynarodowej odbywa się w sposób zgodny z odpowiednimi przepisami umowy o bezpieczeństwie informacji lub porozumienia administracyjnego zgodnie z art. 10 ust. 2 załącznika A.

41. Informacje niejawne o klauzuli tajności RESTREINT UE/EU RESTRICTED mogą być przewożone z terytorium UE na terytorium państwa trzeciego także za pośrednictwem usług pocztowych lub prywatnych służb kurierskich.

42. Przewóz informacji niejawnych o klauzuli tajności TRES SECRET UE/EU TOP SECRET z terytorium UE na terytorium państwa trzeciego lub pomiędzy jednostkami organizacyjnymi UE w państwach trzecich odbywa się za pośrednictwem kurierów wojskowych lub dyplomatycznych.

VI. **NISZCZENIE EUCI**

43. Dokumenty niejawne UE, które nie są już potrzebne, mogą zostać zniszczone, bez uszczerbku dla odpowiednich zasad i przepisów wykonawczych dotyczących archiwizowania.

44. Dokumenty podlegające rejestracji zgodnie z art. 7 ust. 2 załącznika A są niszczone przez odpowiedzialną kancelarię tajną na polecenie posiadacza lub właściwego organu. Rejestry i inne informacje dotyczące rejestracji są odpowiednio uaktualniane.

45. W odniesieniu do dokumentów niejawnych o klauzuli tajności SECRET UE/EU SECRET lub TRES SECRET UE/EU TOP SECRET niszczenie przebiega w obecności świadka, który posiada poświadczenie bezpieczeństwa co najmniej do poziomu klauzuli tajności niszczonego dokumentu.

46. Osoba dokonująca rejestracji oraz świadek, jeżeli jego obecność jest wymagana, podpisują protokół zniszczenia, który zostaje umieszczony w dokumentacji kancelarii tajnej. Protokoły zniszczenia dokumentów o klauzuli tajności TRES SECRET UE/EU TOP SECRET przechowuje się w kancelarii tajnej przez okres co najmniej dziesięciu lat, a dokumentów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET – przez okres co najmniej pięciu lat.

47. Dokumenty niejawne, w tym dokumenty o klauzuli tajności RESTREINT UE/EU RESTRICTED, są niszczone przy zastosowaniu metod, które spełniają odpowiednie normy UE lub normy równoważne lub które zostały zatwierdzone przez państwa członkowskie zgodnie z krajowymi normami technicznymi, tak by nie mogły zostać całkowicie ani częściowo odtworzone.

48. Niszczenie komputerowych nośników EUCI odbywa się zgodnie z pkt 36 załącznika A IV.

VII. INSPEKCJE W ZAKRESIE BEZPIECZEŃSTWA

Inspekcje ESDZ w zakresie bezpieczeństwa

49. Zgodnie z art. 15 niniejszej decyzji inspekcje ESDZ w zakresie bezpieczeństwa obejmują:

a) ogólne inspekcje w zakresie bezpieczeństwa, mające na celu ocenę ogólnego poziomu bezpieczeństwa siedziby głównej ESDZ, delegatur Unii i wszelkich lokali zależnych lub powiązanych, w szczególności w celu oceny skuteczności środków bezpieczeństwa wdrożonych dla ochrony interesów bezpieczeństwa ESDZ;

b) inspekcje w zakresie bezpieczeństwa EUCI, mające na celu ocenę, ogólnie pod kątem akredytacji, skuteczności środków podjętych w celu ochrony EUCI w siedzibie głównej ESDZ i w delegaturach Unii.

W szczególności inspekcje takie przeprowadza się m.in. aby:

(i) zapewnić przestrzeganie określonych w niniejszej decyzji wymaganych norm minimalnych w zakresie ochrony EUCI;

(ii) podkreślić znaczenie bezpieczeństwa i skutecznego zarządzania ryzykiem wewnątrz kontrolowanych podmiotów;

(iii) zalecić środki zaradcze mające złagodzić konkretne skutki, jakie może powodować utrata poufności, integralności lub dostępności informacji niejawnych; oraz

(iv) ulepszyć istniejące, opracowane przez organy bezpieczeństwa, programy szkoleń i upowszechniania wiedzy w dziedzinie bezpieczeństwa.

Przeprowadzanie inspekcji ESDZ w zakresie bezpieczeństwa i sprawozdawczość

50. Inspekcje ESDZ w zakresie bezpieczeństwa przeprowadza zespół kontrolny Dyrekcji ds. Bezpieczeństwa ESDZ, w razie potrzeby ze wsparciem ekspertów w dziedzinie bezpieczeństwa z innych instytucji UE lub państw członkowskich.

Zespół kontrolny ma dostęp do wszystkich miejsc, w których ma miejsce obchodzenie się z EUCI, w szczególności do kancelarii tajnych i punktów, w których znajdują się CIS.

51. Inspekcje ESDZ w zakresie bezpieczeństwa w delegaturach Unii można przeprowadzać w razie potrzeby ze wsparciem urzędników ds. bezpieczeństwa ambasad państw członkowskich znajdujących się w danych państwach trzecich.

52. Przed końcem każdego roku kalendarzowego organ ESDZ ds. bezpieczeństwa przyjmuje program inspekcji na następny rok.

53. W razie potrzeby organ ESDZ ds. bezpieczeństwa może zorganizować inspekcje w zakresie bezpieczeństwa, które nie zostały przewidziane w wyżej wspomnianym programie.

54. Pod koniec inspekcji w zakresie bezpieczeństwa kontrolowanemu podmiotowi przedstawiane są główne wnioski i zalecenia. Następnie zespół kontrolny sporządza sprawozdanie z inspekcji. W przypadku gdy zostały zaproponowane działania naprawcze i zalecenia, w sprawozdaniu zamieszcza się odpowiednio szczegółowe dane uzasadniające sformułowane wnioski. Sprawozdanie przekazuje się organowi ESDZ ds. bezpieczeństwa oraz kierownikowi kontrolowanego podmiotu.

Pod nadzorem Dyrekcji ds. bezpieczeństwa ESDZ opracowuje się okresowe sprawozdanie mające na celu uwypuklenie doświadczeń nabytych w wyniku inspekcji przeprowadzonych w danym okresie; sprawozdanie to podlega analizie Komitetu ds. Bezpieczeństwa ESDZ.

Przeprowadzanie inspekcji w zakresie bezpieczeństwa w agencjach i organach UE ustanowionych na mocy tytułu V rozdział 2 TUE oraz sprawozdawczość.

55. Dyrekcja ds. Bezpieczeństwa ESDZ może w stosownych przypadkach wyznaczać ekspertów, którzy będą członkami wspólnych zespołów kontrolnych przeprowadzających inspekcje w agencjach i organach UE ustanowionych na mocy tytułu V rozdział 2 TUE.

Lista kontrolna na potrzeby inspekcji ESDZ w zakresie bezpieczeństwa

56. Dyrekcja ds. Bezpieczeństwa ESDZ sporządza i uaktualnia listę kontrolną, zawierającą kwestie, które należy sprawdzić w trakcie inspekcji ESDZ w zakresie bezpieczeństwa. Wspomniana lista kontrolna przekazywana jest Komitetowi ds. Bezpieczeństwa ESDZ.

57. Informacji służących uzupełnieniu listy kontrolnej udziela, w szczególności podczas inspekcji, personel odpowiedzialny za bezpieczeństwo w jednostce, w której przeprowadzana jest inspekcja. Po wypełnieniu listy kontrolnej szczegółowymi odpowiedziami nadaje się jej klauzulę tajności w porozumieniu z kontrolowaną jednostką. Lista ta nie jest częścią raportu z inspekcji.

ZAŁĄCZNIK A IV

OCHRONA EUCI, Z KTÓRYMI OBCHODZĄ SIĘ SYSTEMY TELEINFORMATYCZNE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 8 załącznika A.

2. Następujące cechy i koncepcje zabezpieczania informacji są niezbędne dla bezpieczeństwa i prawidłowego funkcjonowania operacji dokonywanych w ramach systemów teleinformatycznych (CIS):

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

II. ZASADY ZABEZPIECZANIA INFORMACJI

3. Przedstawione poniżej przepisy stanowią podstawę bezpieczeństwa wszelkich systemów CIS, w ramach których przetwarzane są EUCI. Szczegółowe wymogi dotyczące wdrażania tych przepisów są zdefiniowane w ramach polityk bezpieczeństwa w zakresie zabezpieczania informacji oraz w wytycznych dotyczących bezpieczeństwa.

Zarządzanie ryzykiem dla bezpieczeństwa

4. Zarządzanie ryzykiem dla bezpieczeństwa stanowi integralną część projektowania, tworzenia, eksploatacji i konserwacji CIS. Zarządzanie ryzykiem (ocena, zmniejszanie, akceptacja i powiadamianie) jest prowadzone jako wielokrotny 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. Zakres stosowania CIS oraz jego zasobów jest jasno definiowany na początku procesu zarządzania ryzykiem.

5. Właściwe organy ESDZ dokonują przeglądu potencjalnych zagrożeń dla CIS i prowadzą aktualne i dokładne oceny zagrożeń, odzwierciedlające aktualne środowisko operacyjne. Stale uaktualniają swoją wiedzę na temat podatności na zagrożenia i dokonują okresowych przeglądów oceny podatności, aby dostosować się do zmieniających się technologii informatycznych (IT).

6. Celem zarządzania ryzykiem dla bezpieczeństwa jest zastosowanie zestawu środków bezpieczeństwa prowadzących do osiągnięcia zadowalającej równowagi między wymaganiami użytkownika a szczątkowym ryzykiem dla bezpieczeństwa.

7. Szczególne wymogi, skala i stopień szczegółowości określone przez właściwy organ ds. akredytacji bezpieczeństwa (SAA) do celów przyznania akredytacji CIS są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników, w tym poziomu klauzuli tajności EUCI przetwarzanych w danym CIS. Akredytacja obejmuje oficjalne oświadczenie o ryzyku szczątkowym oraz akceptację ryzyka szczątkowego przez odpowiedzialny organ.

Bezpieczeństwo w całym cyklu życia CIS

8. Zapewnianie bezpieczeństwa jest wymogiem obowiązującym w całym cyklu życia CIS, od jego uruchomienia do wycofania z użytkowania.

9. Dla każdego etapu cyklu życia CIS określana jest rola i interakcja każdego z podmiotów związanych z CIS w odniesieniu do jego bezpieczeństwa.

10. Wszystkie CIS wraz z technicznymi i innymi środkami bezpieczeństwa są podczas procedury akredytacji poddawane testom bezpieczeństwa, aby zapewnić osiągnięcie odpowiedniego stopnia zabezpieczenia wdrożonych środków bezpieczeństwa oraz sprawdzić, czy są one prawidłowo wdrożone, zintegrowane i skonfigurowane.

11. Oceny bezpieczeństwa, inspekcje i przeglądy przeprowadzane są okresowo w fazie operacyjnej oraz podczas konserwacji CIS, jak również przy pojawieniu się nadzwyczajnych okoliczności.

12. Dokumentacja bezpieczeństwa CIS ewoluuje podczas wszystkich etapów jego cyklu życia na zasadzie integralnej części procesu zmian i zarządzania konfiguracjami.

Najlepsze praktyki

13. ESDZ współpracuje z Sekretariatem Generalnym Rady i państwami członkowskimi, aby opracować najlepsze praktyki ochrony EUCI, z którymi obchodzą się CIS. Wytyczne w zakresie dobrych praktyk obejmują techniczne, fizyczne, organizacyjne i proceduralne środki bezpieczeństwa dotyczące CIS o sprawdzonej skuteczności w zapobieganiu danym zagrożeniom i podatności.

14. Ochrona EUCI przetwarzanych w ramach CIS opiera się na doświadczeniach podmiotów zaangażowanych w zabezpieczanie informacji, zarówno w UE, jak i poza nią.

15. Rozpowszechnianie, a następnie wdrażanie dobrych praktyk pomaga w osiągnięciu równoważnego poziomu zabezpieczenia różnych CIS eksploatowanych przez ESDZ i obchodzących się z EUCI.

Ochrona w głąb

16. Aby zmniejszyć ryzyko zagrażające CIS, wdraża się szereg technicznych i innych środków bezpieczeństwa o strukturze różnych poziomów ochrony. Poziomy te obejmują:

a) *powstrzymywanie:* środki bezpieczeństwa ukierunkowane na zniechęcenie osób planujących atak na CIS;

b) *zapobieganie:* środki bezpieczeństwa ukierunkowane na udaremnienie lub powstrzymanie ataku na CIS;

c) *wykrywanie:* środki bezpieczeństwa ukierunkowane na ujawnienie ataku na CIS;

d) *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

e) *usuwanie skutków:* środki bezpieczeństwa ukierunkowane na odzyskanie bezpiecznego statusu CIS.

Stopień rygorystyczności i zakres stosowania takich środków bezpieczeństwa ustalany jest na podstawie oceny ryzyka.

17. ESDZ dba o to, by była w stanie reagować na incydenty, które mogą przekraczać granice poszczególnych organizacji i państw, koordynować reakcje i dzielić się informacjami o tych incydentach i związanym z nimi ryzyku (zdolności do reagowania na sytuacje nadzwyczajne w ramach systemów komputerowych).

Zasada minimalizmu i najmniejszych uprawnień

18. Aby zapobiec niepotrzebnemu ryzyku, stosowane są wyłącznie funkcje, urządzenia i usługi służące spełnieniu wymogów operacyjnych.

19. Aby ograniczyć szkody wynikające z wypadków, błędów lub nieuprawnionego korzystania z zasobów CIS, użytkownicy CIS oraz procesy zautomatyzowane otrzymują wyłącznie taki dostęp i takie przywileje i upoważnienia, jakie są im niezbędne do wykonywania ich zadań.

20. Procedury rejestracji stosowane w razie konieczności w ramach CIS sprawdzane są jako element procedury akredytacji.

Świadomość zabezpieczania informacji

21. Świadomość ryzyka i dostępnych środków bezpieczeństwa stanowi pierwszą linię obrony bezpieczeństwa CIS. W szczególności wszyscy członkowie personelu związani z CIS na poszczególnych etapach jego cyklu życia, w tym użytkownicy, powinni:

a) zdawać sobie sprawę, że niedopatrzenia w zakresie bezpieczeństwa mogą znacznie zaszkodzić CIS i całej organizacji;

b) rozumieć potencjalne szkody, jakie mogą ponieść inne podmioty w związku z podłączeniem do systemów lub sieci i współzależnością; oraz

c) być świadomi, że osobiście ponoszą odpowiedzialność i są rozliczani za bezpieczeństwo CIS zgodnie z pełnionymi przez siebie funkcjami w tych systemach i procesach.

22. Aby zapewnić zrozumienie obowiązków związanych z bezpieczeństwem, wszyscy członkowie personelu związani z CIS, w tym wyższe kierownictwo i użytkownicy CIS, przechodzą obowiązkowe szkolenia mające na celu edukację i zdobycie wiedzy w zakresie zabezpieczania informacji.

Ocena i zatwierdzanie produktów służących bezpieczeństwu systemów informatycznych

23. Wymagany stopień zabezpieczenia, jaki zapewniają środki bezpieczeństwa, określony jako poziom zabezpieczenia, określa się zgodnie z wynikami procesu zarządzania ryzykiem i zgodnie z odpowiednimi politykami i wytycznymi dotyczącymi bezpieczeństwa.

24. Poziom zabezpieczenia sprawdzany jest przy użyciu uznanych na szczeblu międzynarodowym lub zatwierdzonych na szczeblu krajowym procesów i metod. Obejmują one przede wszystkim ocenę, kontrole i audyt.

25. Produkty kryptograficzne służące ochronie EUCI są oceniane i zatwierdzane przez krajowy organ ds. zatwierdzania produktów kryptograficznych (CAA) państwa członkowskiego.

26. Przed zaleceniem organowi ESDZ ds. zatwierdzania produktów kryptograficznych (CAA ESDZ) zgodnie z art. 7 ust. 5, wspomniane produkty kryptograficzne muszą uzyskać pozytywny wynik podczas zewnętrznej oceny dokonywanej przez wykwalifikowany organ oceny produktów kryptograficznych (AQUA) państwa członkowskiego, które nie jest zaangażowane w projektowanie ani wytwarzanie tego sprzętu. Wymagany stopień szczegółowości oceny zewnętrznej zależy od przewidywanego najwyższego poziomu klauzuli tajności EUCI, które mają być chronione za pomocą tych produktów.

27. Jeżeli uzasadniają to określone względy operacyjne, CAA ESDZ może na zalecenie Komitetu ds. Bezpieczeństwa Rady znieść wymogi wynikające z pkt 25 lub 26 i udzielić tymczasowej akceptacji na dany okres zgodnie z art. 7 ust. 5 niniejszej decyzji.

28. AQUA jest organem ds. zatwierdzania produktów kryptograficznych (CAA) państwa członkowskiego, który na podstawie kryteriów ustalonych przez Radę otrzymał akredytację, aby przeprowadzić ocenę zewnętrzną produktów kryptograficznych służących ochronie EUCI.

29. Wysoki Przedstawiciel zatwierdza politykę bezpieczeństwa dotyczącą kwalifikowania i zatwierdzania niekryptograficznych produktów służących bezpieczeństwu systemów informatycznych.

Transmisja w strefach bezpieczeństwa

30. Niezależnie od przepisów niniejszej decyzji, gdy transmisja EUCI ogranicza się do stref bezpieczeństwa, można je dystrybuować w postaci niezaszyfrowanej lub zaszyfrować je na niższym poziomie na podstawie wyników procesu zarządzania ryzykiem i z zastrzeżeniem zatwierdzenia przez SAA.

Bezpieczne połączenia międzysystemowe CIS

31. Do celów niniejszej decyzji połączenie międzysystemowe oznacza bezpośrednie połączenie co najmniej dwóch systemów informatycznych w celu wspólnego korzystania z danych i innych zasobów informacyjnych (np. łączności) w sposób jednokierunkowy lub wielokierunkowy.

32. CIS traktuje każdy system informatyczny przyłączony połączeniem międzysystemowym jako niezaufany i stosuje środki ochrony, aby kontrolować wymianę informacji niejawnych.

33. Wszystkie połączenia międzysystemowe CIS z innym systemem informatycznym podlegają następującym podstawowym wymogom:

a) właściwe organy określają i zatwierdzają wymogi biznesowe i operacyjne dla takich połączeń;

b) połączenie międzysystemowe przechodzi proces zarządzania ryzykiem i akredytacji oraz wymaga zatwierdzenia przez właściwe organy akredytacji bezpieczeństwa (SAA); oraz

c) na granicach wszystkich CIS stosowane są usługi ochrony na granicy systemów (BPS).

34. Pomiędzy CIS posiadającym akredytację a siecią niezabezpieczoną lub publiczną brak jest połączeń międzysystemowych z wyjątkiem sytuacji, w których w ramach CIS zainstalowano w tym celu zatwierdzone BPS między CIS a siecią niezabezpieczoną lub publiczną. Środki bezpieczeństwa dotyczące takich połączeń międzysystemowych są poddawane przeglądowi przez właściwy organ ds. zabezpieczania informacji (IAA) i zatwierdzane przez właściwy SAA.

Gdy sieć niezabezpieczona lub publiczna wykorzystywana jest wyłącznie jako nośnik, a dane zostały zaszyfrowane przy wykorzystaniu produktu kryptograficznego zatwierdzonego zgodnie z art. 7 ust. 5 niniejszej decyzji, takiego połączenia nie uznaje się za połączenie międzysystemowe.

35. Bezpośrednie lub kaskadowe połączenie międzysystemowe CIS posiadającego akredytację do przetwarzania informacji o klauzuli tajności TRES SECRET UE/EU TOP SECRET z siecią niezabezpieczoną lub publiczną jest zakazane.

Komputerowe nośniki informacji

36. Komputerowe nośniki informacji są niszczone zgodnie z procedurami zatwierdzonymi przez organ ESDZ ds. bezpieczeństwa.

37. Ponowne użycie komputerowych nośników informacji bądź obniżenie lub zniesienie ich klauzuli tajności odbywa się zgodnie z polityką bezpieczeństwa, którą należy ustalić na mocy art. 7 ust. 2 niniejszej decyzji.

Okoliczności nadzwyczajne

38. Niezależnie od przepisów niniejszej decyzji w okolicznościach nadzwyczajnych, takich jak zbliżający się lub trwający kryzys, konflikt, stan wojny, lub w wyjątkowych sytuacjach operacyjnych można przez ograniczony czas stosować specjalne procedury opisane poniżej.

39. EUCI można przekazywać z wykorzystaniem produktów kryptograficznych zatwierdzonych dla niższego poziomu klauzuli tajności lub w postaci niezaszyfrowanej za zgodą właściwego organu, jeżeli wszelka zwłoka spowodowałaby szkody wyraźnie większe od szkód, które mogłoby spowodować ujawnienie materiałów niejawnych, oraz jeżeli:

a) nadawca i odbiorca nie posiadają wymaganego urządzenia szyfrującego lub też nie posiadają żadnego urządzenia szyfrującego; oraz

b) dane materiały niejawne nie mogą być dostarczone na czas w inny sposób.

40. Informacje niejawne przekazywane w okolicznościach przedstawionych w pkt 39 nie są opatrzone żadnymi oznaczeniami ani wskazaniami odróżniającymi je od informacji jawnych lub informacji, które mogą być chronione przy pomocy dostępnego urządzenia szyfrującego. Odbiorcy są za pomocą innych środków bezzwłocznie powiadamiani o poziomie klauzuli tajności.

41. W przypadku stosowania przepisów pkt 39 należy następnie sporządzić sprawozdanie dla Dyrekcji ds. Bezpieczeństwa ESDZ i za jej pośrednictwem przekazać je Komitetowi ds. Bezpieczeństwa ESDZ. W sprawozdaniu określa się przynajmniej nadawcę, odbiorcę oraz wytwórcę każdej EUCI.

III. FUNKCJE I ORGANY ZABEZPIECZANIA INFORMACJI

42. W ESDZ ustanawia się następujące funkcje w zakresie zabezpieczania informacji. Funkcje te nie muszą być skupione w tych samych jednostkach organizacyjnych. Są one objęte oddzielnymi mandatami. Funkcje te, oraz związana z nimi odpowiedzialność, mogą być jednak połączone lub zintegrowane w tej samej jednostce organizacyjnej lub też podzielone na różne jednostki organizacyjne, z zastrzeżeniem uniknięcia wewnętrznych konfliktów interesów lub zadań.

Organ ds. zabezpieczania informacji (IAA)

43. Organ ds. zabezpieczania informacji (IAA) odpowiada za:

a) opracowywanie polityki bezpieczeństwa i wytycznych dotyczących bezpieczeństwa w zakresie zabezpieczania informacji oraz za monitorowanie ich skuteczności i adekwatności;

b) zabezpieczanie informacji technicznych związanych z produktami kryptograficznymi i zarządzanie tymi informacjami;

c) zapewnianie, by środki zabezpieczania informacji wybrane do ochrony EUCI były zgodne z odpowiednimi politykami dotyczącymi kryteriów ich przydatności i wyboru;

d) zapewnianie, by wybór produktów kryptograficznych następował zgodnie z politykami dotyczącymi kryteriów ich przydatności i wyboru;

e) koordynowanie szkoleń i upowszechniania wiedzy na temat zabezpieczania informacji;

f) konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w odniesieniu do polityki bezpieczeństwa i wytycznych dotyczących bezpieczeństwa w zakresie zabezpieczania informacji; oraz

g) zapewnianie odpowiedniej wiedzy fachowej na temat zabezpieczania informacji w podgrupie eksperckiej Komitetu ds. Bezpieczeństwa ESDZ.

Organ ds. TEMPEST

44. 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.

Organ ds. zatwierdzania produktów kryptograficznych (CAA)

45. CAA odpowiada za zapewnienie zgodności produktów kryptograficznych z odpowiednią polityką kryptograficzną. Wydaje on zgodę na to, by dany produkt kryptograficzny w swoim środowisku operacyjnym chronił EUCI do określonego poziomu klauzuli tajności.

Organ ds. dystrybucji produktów kryptograficznych (CDA)

46. CDA odpowiada za:

a) zarządzanie materiałami kryptograficznymi UE i ich ewidencjonowanie;

b) zapewnianie stosowania odpowiednich procedur i stworzenia kanałów umożliwiających ewidencjonowanie wszystkich materiałów kryptograficznych UE, bezpieczne obchodzenie się z nimi, ich przechowywanie i rozpowszechnianie; oraz

c) zapewnianie przekazywania materiałów kryptograficznych UE między osobami lub służbami korzystającymi z tych materiałów.

Organ ds. akredytacji bezpieczeństwa (SAA)

47. SAA jest w każdym systemie odpowiedzialny za:

a) 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, przy spełnieniu których konieczne jest ponowne zatwierdzenie;

(b) stworzenie procesu akredytacji bezpieczeństwa, zgodnie z odpowiednimi politykami, z wyraźnie określonymi warunkami zatwierdzenia CIS pod nadzorem tego organu;

c) określanie strategii akredytacji bezpieczeństwa, określającej stopień szczegółowości procedury akredytacji proporcjonalny do wymaganego poziomu zabezpieczenia;

(d) 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 ESDZ;

e) sprawdzanie wdrażania środków bezpieczeństwa w odniesieniu do CIS przez dokonywanie ocen, inspekcji lub przeglądów bezpieczeństwa czy też wspieranie takich działań;

f) określanie wymogów bezpieczeństwa (np. poziomów poświadczeń bezpieczeństwa personelu) w przypadku stanowisk o szczególnie wrażliwym charakterze w odniesieniu do CIS;

g) zatwierdzanie wyboru produktów kryptograficznych i produktów klasy TEMPEST wykorzystywanych do zapewnienia bezpieczeństwa CIS;

h) zatwierdzanie lub w odpowiednich przypadkach uczestniczenie we wspólnym zatwierdzaniu międzysystemowego połączenia CIS z innymi CIS; oraz

i) 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 poświadczenia zatwierdzenia.

48. SAA ESDZ jest odpowiedzialny za przyznawanie akredytacji wszystkim CIS działającym w zakresie działalności ESDZ.

Rada ds. Akredytacji w zakresie Bezpieczeństwa (SAB)

49. Wspólna Rada ds. Akredytacji w zakresie Bezpieczeństwa (SAB) jest odpowiedzialna za przyznawanie akredytacji CIS działającym w zakresie właściwości SAA ESDZ, 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 Sekretariatu Generalnego Rady oraz Komisji. Inne podmioty posiadające połączenia z danym CIS są zapraszane do uczestnictwa w obradach, gdy omawiany jest ten system.

Obradom SAB przewodniczy przedstawiciel SAA ESDZ. 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 ESDZ oraz informuje Komitet o wszystkich świadectwach akredytacji.

Operacyjny organ ds. zabezpieczania informacji

50. Operacyjny organ ds. zabezpieczania informacji odpowiada w każdym systemie za:

a) opracowanie dokumentacji bezpieczeństwa zgodnie z politykami bezpieczeństwa i wytycznymi dotyczącymi bezpieczeństwa, zwłaszcza oświadczenia o szczególnych wymaganiach bezpieczeństwa systemu (**SSRS**), w tym oświadczenia o ryzyku szczątkowym, procedur bezpiecznej eksploatacji systemu (**SecOP**) i planu kryptograficznego w ramach procesu akredytacji CIS;

b) uczestnictwo w wyborze i testowaniu technicznych 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;

c) 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;

d) monitorowanie wdrażania i stosowania SecOP, a w odpowiednich przypadkach zlecanie właścicielowi systemu operacyjnych obowiązków w zakresie bezpieczeństwa;

(e) zarządzanie produktami kryptograficznymi i ich wykorzystywanie, zapewnianie nadzoru nad obiektami kryptograficznymi i kontrolowanymi oraz, jeżeli jest to wymagane, zapewnienie wytwarzania zmiennych kryptograficznych;

f) przeprowadzanie przeglądów i testów analizy bezpieczeństwa, w szczególności w celu sporządzenia odpowiednich sprawozdań o ryzyku, zgodnie z wymogami SAA;

g) zapewnianie szkolenia w zakresie zabezpieczania informacji w odniesieniu do poszczególnych CIS;

h) wdrażanie środków bezpieczeństwa w odniesieniu do poszczególnych CIS i stosowanie tych środków.

ZAŁĄCZNIK A V

BEZPIECZEŃSTWO PRZEMYSŁOWE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 9 załącznika A. Ustanawia się w nim ogólne przepisy w zakresie bezpieczeństwa mające zastosowanie do podmiotów gospodarczych lub innych podczas negocjacji poprzedzających zawarcie umowy oraz na wszystkich etapach cyklu życia umów niejawnych zawartych przez ESDZ.

2. Wysoki Przedstawiciel zatwierdza politykę bezpieczeństwa przemysłowego, określającą w szczególności szczegółowe wymogi w odniesieniu do świadectw bezpieczeństwa przemysłowego (SBP), dokumentów określających aspekty bezpieczeństwa (DOAB), wizyt, transmisji i przenoszenia EUCI.

II. ELEMENTY DOTYCZĄCE BEZPIECZEŃSTWA W UMOWIE NIEJAWNEJ

Przewodnik nadawania klauzul (PNK)

3. Przed zamieszczeniem ogłoszenia o przetargu lub zawarciem umowy niejawnej ESDZ jako instytucja zamawiająca określa klauzulę tajności wszelkich informacji, które należy dostarczyć oferentom i wykonawcom, jak również klauzulę tajności wszelkich informacji, które mają być wytworzone przez wykonawcę. W tym celu ESDZ opracowuje PNK, który należy stosować podczas wykonywania umów.

4. Do określania klauzuli tajności różnych elementów umowy niejawnej zastosowanie mają następujące zasady:

   a) podczas opracowywania PNK ESDZ uwzględnia wszystkie odpowiednie aspekty bezpieczeństwa, w tym klauzulę tajności nadaną informacjom, które ich wytwórca przekazał i których wykorzystanie do celów umowy zatwierdził;

   b) ogólna klauzula tajności umowy nie może być niższa od najwyższej klauzuli tajności któregokolwiek z jej elementów; oraz

   c) w odpowiednich przypadkach ESDZ działa w porozumieniu z KWB/WWB państw członkowskich lub jakimkolwiek innym właściwym organem bezpieczeństwa na wypadek jakichkolwiek zmian klauzul tajności informacji wytworzonych przez wykonawców lub przekazanych im podczas wykonywania umowy oraz w przypadku wprowadzania jakichkolwiek późniejszych zmian do PNK.

Dokument określający aspekty bezpieczeństwa (DOAB)

5. Wymogi bezpieczeństwa dotyczące poszczególnych umów opisane są w DOAB. DOAB w odpowiednich przypadkach zawiera PNK i stanowi integralną część umowy niejawnej lub niejawnej umowy o podwykonawstwo.

6. DOAB zawiera przepisy zobowiązujące wykonawcę lub podwykonawcę do przestrzegania minimalnych norm określonych w niniejszej decyzji. Nieprzestrzeganie tych minimalnych norm może stanowić wystarczający powód do rozwiązania umowy.

Instrukcje bezpieczeństwa programu/projektu (IBP)

7. W zależności od zakresu programów lub projektów obejmujących dostęp do EUCI, obchodzenie się z nimi lub ich przechowywanie, instytucja zarządzająca wyznaczona do zarządzania danym programem lub projektem może sporządzić specjalne instrukcje bezpieczeństwa programu/projektu (IBP). IBP wymagają zatwierdzenia przez KWB/WWB państw członkowskich lub jakikolwiek inny właściwy organ bezpieczeństwa uczestniczący w programie/projekcie i mogą zawierać dodatkowe wymogi bezpieczeństwa.

III. ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO (SBP)

8. Dyrekcja ds. Bezpieczeństwa ESDZ zwraca się do KWB lub WWB lub innego właściwego organu bezpieczeństwa danego państwa członkowskiego o wydanie SBP w celu zaświadczenia, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, że dany podmiot gospodarczy lub inny jest w stanie zapewnić w swoich obiektach ochronę EUCI odpowiadającą określonemu poziomowi klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET). Do czasu przekazania SBP do ESDZ żadnemu rzeczywistemu ani potencjalnemu wykonawcy ani podwykonawcy nie udziela się ani nie umożliwia się dostępu do EUCI.

9. W stosownych przypadkach ESDZ jako instytucja zamawiająca powiadamia odpowiednią KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa o tym, że na etapie poprzedzającym zawarcie umowy lub do wykonywania umowy wymagane jest SBP. SBP lub PBO są wymagane na etapie poprzedzającym zawarcie umowy, jeżeli podczas składania ofert mają być dostarczone EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET.

10. ESDZ jako instytucja zamawiająca nie zawiera umowy niejawnej z wybranym oferentem, zanim nie otrzyma od KWB/WWB lub jakiegokolwiek innego właściwego organu bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest dany wykonawca lub podwykonawca, potwierdzenia, że wydane zostało, jeśli istnieje taki wymóg, odpowiednie SBP.

11. ESDZ jako instytucja zamawiająca zwraca się do KWB/WWB lub jakiegokolwiek innego właściwego organu bezpieczeństwa, który wydał SBP, o przekazywanie ESDZ wszelkich niekorzystnych informacji dotyczących SBP. W przypadku umowy o podwykonawstwo informuje się o tym odpowiednio KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa.

12. Cofnięcie SBP przez odpowiednią KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa stanowią dla ESDZ jako instytucji zamawiającej wystarczający powód do rozwiązania umowy niejawnej lub wykluczenia oferenta z postępowania.

IV. POŚWIADCZENIA BEZPIECZEŃSTWA OSOBOWEGO (PBO) DLA PRACOWNIKÓW WYKONAWCY

13. Wszyscy pracownicy wykonawców, którym niezbędny jest dostęp do EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, muszą przed uzyskaniem dostępu do tych informacji uzyskać odpowiednie poświadczenie bezpieczeństwa i spełniać zasadę ograniczonego dostępu. Dostęp do EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED nie wymaga PBO, ale wymaga spełnienia zasady ograniczonego dostępu.

14. Wnioski o PBO dla pracowników wykonawcy składa się do KWB/WWB odpowiedzialnej za dany podmiot.

15. ESDZ informuje wykonawców, którzy zamierzają zatrudnić obywatela państwa trzeciego na stanowisku wymagającym dostępu do EUCI, że za ustalenie zgodnie z niniejszą decyzją, czy tej osobie można udzielić dostępu do takich informacji, odpowiada KWB/WWB państwa członkowskiego, w którym znajduje się siedziba podmiotu zatrudniającego; do jej obowiązków należy również potwierdzenie, że przed udzieleniem takiego dostępu uzyskano zgodę wytwórcy informacji.

V. UMOWY NIEJAWNE I NIEJAWNE UMOWY O PODWYKONAWSTWO

16. Jeżeli EUCI przekazywane są oferentowi na etapie poprzedzającym zawarcie umowy, ogłoszenie o przetargu zawiera przepis zobowiązujący oferenta, który nie złoży oferty lub który nie zostanie wybrany, do zwrotu wszystkich dokumentów niejawnych w określonym terminie.

17. Po zawarciu umowy niejawnej lub niejawnej umowy o podwykonawstwo ESDZ jako instytucja zamawiająca powiadamia KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa wykonawcy lub podwykonawcy o zawartych w tej umowie przepisach bezpieczeństwa.

18. W przypadku rozwiązania lub wygaśnięcia takich umów ESDZ jako instytucja zamawiająca (lub – w przypadku umowy o podwykonawstwo – KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa, w zależności od przypadku) niezwłocznie powiadamia o tym fakcie KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest wykonawca lub podwykonawca.

19. Co do zasady, od wykonawcy lub podwykonawcy wymaga się zwrotu do instytucji zamawiającej wszelkich posiadanych przez niego EUCI po rozwiązaniu lub wygaśnięciu umowy niejawnej lub niejawnej umowy o podwykonawstwo.

20. Szczegółowe przepisy dotyczące pozbywania się EUCI podczas wykonywania umowy lub po jej rozwiązaniu bądź wygaśnięciu określa się w DOAB.

21. Jeżeli wykonawca lub podwykonawca są upoważnieni do zachowania EUCI po rozwiązaniu lub wygaśnięciu umowy, nadal przestrzegają oni minimalnych norm zawartych w niniejszej decyzji i nadal chronią poufność EUCI.

22. Warunki, na których wykonawca może zlecić podwykonawstwo, są określone w ogłoszeniu o przetargu oraz w umowie.

23. Przed zleceniem podwykonawstwa części umowy niejawnej wykonawca uzyskuje zgodę ESDZ jako instytucji zamawiającej. Nie można zawrzeć umowy o podwykonawstwo z podmiotami gospodarczymi lub innymi zarejestrowanymi w państwie, które nie jest państwem członkowskim UE i nie zawarło z UE umowy o bezpieczeństwie informacji.

24. Wykonawca odpowiada za zapewnienie zgodności wszystkich podejmowanych czynności podwykonawczych z minimalnymi normami określonymi w niniejszej decyzji i nie dostarcza EUCI podwykonawcy bez uprzedniej pisemnej zgody instytucji zamawiającej.

25. W odniesieniu do EUCI wytworzonych przez wykonawcę lub podwykonawcę lub z którymi obchodzi się wykonawca lub podwykonawca, prawa przysługujące wytwórcy są wykonywane przez instytucję zamawiającą.

VI. **WIZYTY ZWIĄZANE Z UMOWAMI NIEJAWNYMI**

26. Jeżeli ESDZ, wykonawcy lub podwykonawcy niezbędny jest do celów wykonania umowy niejawnej dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET w obiektach innej z wymienionych stron, organizuje się wizyty w porozumieniu z KWB/WWB lub jakimkolwiek innym właściwym organem bezpieczeństwa. Pozostaje to bez uszczerbku dla uprawnienia KWB/WWB do uzgodnienia, w kontekście konkretnych projektów, procedury umożliwiającej bezpośrednie organizowanie wizyt.

27. W odniesieniu do dostępu do EUCI związanych z umową zawartą przez ESDZ wszystkie osoby wizytujące muszą posiadać odpowiednie PBO i podlegają zasadzie ograniczonego dostępu.

28. Osobom wizytującym umożliwia się dostęp wyłącznie do EUCI związanych z celem wizyty.

VII. **TRANSMISJA I PRZENOSZENIE EUCI**

29. Do transmisji EUCI drogą elektroniczną zastosowanie mają odpowiednie przepisy art. 8 załącznika A oraz załącznika A IV.

30. Do przenoszenia EUCI zastosowanie mają odpowiednie przepisy załącznika A III zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.

31. Podczas transportu materiału niejawnego jako ładunku do określania zabezpieczeń stosuje się następujące zasady:

a) bezpieczeństwo zapewnia się na wszystkich etapach przewozu, począwszy od miejsca wyjazdu do ostatecznego miejsca przeznaczenia;

b) stopień ochrony, którym objęto przesyłkę, określany jest według najwyższej klauzuli tajności materiału zawartego w przesyłce;

c) firmy dokonujące przewozu muszą uzyskać SBP na stosownym poziomie, jeśli przewóz wymaga również przechowywania informacji niejawnych w obiektach wykonawcy. W każdym przypadku pracownicy obchodzący się z przesyłką muszą posiadać odpowiednie poświadczenie bezpieczeństwa zgodnie z załącznikiem A I;

d) przed wszelkim transgranicznym przemieszczeniem materiałów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET nadawca sporządza plan przewozu, który jest zatwierdzany przez ESDZ, w stosownych przypadkach w porozumieniu z KWB/WWB nadawcy i odbiorcy lub jakimkolwiek innym właściwym organem bezpieczeństwa;

e) przejazdy odbywają się w miarę możliwości bezpośrednio między dwoma punktami i w najkrótszym czasie, na jaki pozwalają okoliczności;

f) jeżeli jest to możliwe, trasy powinny przebiegać wyłącznie przez terytoria państw członkowskich. Transport trasami przebiegającymi przez terytoria państw innych niż państwa członkowskie powinien się odbywać wyłącznie pod warunkiem zatwierdzenia przez ESDZ lub jakikolwiek inny właściwy organ bezpieczeństwa zarówno państwa nadawcy, jak i państwa odbiorcy.

VIII. **PRZEKAZYWANIE EUCI WYKONAWCOM ZNAJDUJĄCYM SIĘ W PAŃSTWACH TRZECICH**

32. EUCI są przekazywane wykonawcom i podwykonawcom znajdującym się w państwach trzecich, które zawarły z UE ważną umowę dotyczącą bezpieczeństwa, zgodnie ze środkami bezpieczeństwa uzgodnionymi przez ESDZ, jako instytucję zamawiającą, z KWB/WWB państwa trzeciego, w którym zarejestrowany jest wykonawca.

IX. **WYKORZYSTYWANIE I PRZECHOWYWANIE INFORMACJI NIEJAWNYCH O KLAUZULI TAJNOŚCI RESTREINT UE/EU RESTRICTED**

33. ESDZ jako instytucja zamawiająca, w stosownych przypadkach w porozumieniu z KWB/WWB w państwie członkowskim, jest upoważniona na podstawie przepisów umownych do przeprowadzania wizyt w obiektach wykonawców/podwykonawców w celu sprawdzenia, czy wprowadzone zostały odpowiednie środki bezpieczeństwa służące ochronie EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED zgodnie z wymogami umowy.

34. W zakresie zgodnym z wymogami krajowych przepisów ustawowych i wykonawczych ESDZ jako instytucja zamawiająca powiadamia KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa o umowach niejawnych lub niejawnych umowach o podwykonawstwo zawierających informacje niejawne o klauzuli tajności RESTREINT UE/EU RESTRICTED.

35. W przypadku umów zawartych przez ESDZ zawierających informacje niejawne o klauzuli tajności RESTREINT UE/EU RESTRICTED od wykonawców, podwykonawców ani ich personelu nie wymaga się posiadania SBP ani PBO.

36. ESDZ jako instytucja zamawiająca analizuje odpowiedzi na zaproszenia do składania ofert w przypadku umów, które wymagają dostępu do informacji niejawnych o klauzuli tajności RESTREINT UE/EU RESTRICTED, niezależnie od wszelkich ewentualnych wymogów związanych z SBP lub PBO określonych w krajowych przepisach ustawowych i wykonawczych.

37. Warunki, na których wykonawca może zlecić podwykonawstwo, są zgodne z pkt 22–24.

38. Jeżeli umowa obejmuje obchodzenie się z informacjami niejawnymi o klauzuli tajności RESTREINT UE/EU RESTRICTED w ramach CIS, który eksploatuje wykonawca, ESDZ jako instytucja zamawiająca zapewnia, aby umowa ta lub jakakolwiek umowa o podwykonawstwo określała niezbędne wymogi techniczne i administracyjne dotyczące akredytacji CIS, które są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników. Zakres akredytacji dla takiego CIS jest uzgadniany między instytucją zamawiającą a odpowiednią KWB/WWB.

ZAŁĄCZNIK A VI

WYMIANA INFORMACJI NIEJAWNYCH Z PAŃSTWAMI TRZECIMI I ORGANIZACJAMI MIĘDZYNARODOWYMI

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 10 załącznika A.

II. RAMY REGULUJĄCE WYMIANĘ INFORMACJI NIEJAWNYCH

2. ESDZ może wymieniać EUCI z państwami trzecimi lub organizacjami międzynarodowymi zgodnie z art. 10 ust. 1 załącznika A.

W celu wsparcia Wysokiego Przedstawiciela w wykonywaniu jego obowiązków określonych w art. 218 TFUE:

a) odpowiedni departament geograficzny lub tematyczny ESDZ w porozumieniu z Dyrekcją ds. Bezpieczeństwa ESDZ w stosownych przypadkach stwierdza potrzebę długoterminowej wymiany EUCI z danym państwem trzecim lub organizacją międzynarodową;

b) Dyrekcja ds. Bezpieczeństwa ESDZ w porozumieniu z właściwym departamentem geograficznym ESDZ w stosownych przypadkach przedstawia Wysokiemu Przedstawicielowi projekty tekstów, które mają zostać przedstawione Radzie jako wnioski na podstawie art. 218 ust. 3, 5 i 6 TFUE;

c) Dyrekcja ds. Bezpieczeństwa ESDZ wspiera Wysokiego Przedstawiciela w prowadzeniu negocjacji w koordynacji z właściwymi służbami Komisji i Sekretariatu Generalnego Rady;.

d) w odniesieniu do umów lub uzgodnień z państwami trzecimi dotyczących ich uczestnictwa w operacjach zarządzania kryzysowego WPBiO, o których mowa w art. 10 ust. 1 lit. c) załącznika A, Dyrekcja ds. Zarządzania Kryzysowego i Planowania ESDZ w porozumieniu z właściwymi służbami ESDZ w stosownych przypadkach przedstawia Wysokiemu Przedstawicielowi projekty tekstów, które mają zostać przedstawione Radzie jako wnioski na podstawie art. 218 ust. 3, 5 i 6 TFUE i wspiera Wysokiego Przedstawiciela w prowadzeniu negocjacji w koordynacji z właściwymi służbami ESDZ i Sekretariatu Generalnego Rady.

3. W przypadkach, w których umowy o bezpieczeństwie informacji przewidują dokonywanie technicznych uzgodnień wykonawczych pomiędzy Dyrekcją ds. Bezpieczeństwa ESDZ (w koordynacji z Dyrekcją ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji oraz Biurem Bezpieczeństwa w Sekretariacie Generalnym Rady) a właściwym organem bezpieczeństwa w danym państwie trzecim lub organizacji międzynarodowej, w uzgodnieniach takich uwzględnia się poziom ochrony przewidziany w przepisach, strukturach i procedurach dotyczących bezpieczeństwa istniejących w danym państwie trzecim lub danej organizacji międzynarodowej.

4. Jeżeli istnieje długoterminowa potrzeba wymiany przez ESDZ z państwem trzecim lub organizacją międzynarodową informacji niejawnych o klauzuli tajności nie wyższej niż RESTREINT UE/EU RESTRICTED i jeżeli ustalono, że dana strona nie dysponuje systemem bezpieczeństwa wystarczająco rozwiniętym, aby być w stanie zawrzeć umowę o bezpieczeństwie informacji, Wysoki Przedstawiciel może, po uzyskaniu jednomyślnej przychylnej opinii Komitetu ds. Bezpieczeństwa ESDZ wyrażonej zgodnie z art. 14 ust. 5 niniejszej decyzji, zawrzeć porozumienie administracyjne z właściwymi organami bezpieczeństwa danego państwa trzeciego lub organizacji międzynarodowej.

5. Nie wymienia się z państwem trzecim ani organizacją międzynarodową żadnych EUCI drogą elektroniczną, o ile nie zostało to wyraźnie przewidziane w umowie o bezpieczeństwie informacji lub porozumieniu administracyjnym.

6. W ramach porozumienia administracyjnego o wymianie informacji niejawnych ESDZ i dane państwo trzecie lub organizacja międzynarodowa wyznaczają, każde we własnym zakresie, kancelarię tajną, do której – jako głównego punktu – będą wpływać i z której będą przekazywane informacje niejawne podlegające wymianie. W przypadku ESDZ będzie to główna kancelaria tajna ESDZ.

7. Porozumienia administracyjne co do zasady przyjmują postać wymiany listów.

III WIZYTY OCENIAJĄCE

8. Wizyty oceniające, o których mowa w art. 16 niniejszej decyzji, przeprowadza się w porozumieniu z danym państwem trzecim lub organizacją międzynarodową i służą one ocenie:

a) ram prawnych mających zastosowanie do ochrony informacji niejawnych;

b) wszelkich cech charakterystycznych przepisów ustawowych i wykonawczych, polityk i procedur danego państwa trzeciego lub organizacji międzynarodowej w zakresie bezpieczeństwa, które mogą mieć wpływ na to, jaką najwyższą klauzulę tajności mogą mieć wymieniane informacje niejawne;

c) stosowanych w danym czasie środków i procedur bezpieczeństwa dotyczących ochrony informacji niejawnych; oraz

d) procedur udzielania poświadczeń bezpieczeństwa odpowiadających klauzuli tajności EUCI, które mają być udostępniane.

9. Nie dokonuje się wymiany EUCI przed przeprowadzeniem wizyty oceniającej i ustaleniem poziomu, na jakim dane strony mogą wymieniać informacje niejawne, na podstawie równoważności poziomu ochrony przypisanego tym informacjom.

Jeśli przed wizytą oceniającą Wysoki Przedstawiciel uzyska wiedzę na temat jakichkolwiek wyjątkowych lub pilnych powodów, dla których konieczna jest wymiana informacji niejawnych, wówczas ESDZ:

a) zwraca się najpierw o pisemną zgodę wytwórcy informacji w celu ustalenia, że nie ma przeciwwskazań dla udostępnienia informacji;

b) zwraca się do organu ESDZ ds. bezpieczeństwa, który może postanowić o udostępnieniu informacji pod warunkiem uzyskania jednogłośnej przychylnej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ.

Jeśli ESDZ nie jest w stanie ustalić wytwórcy informacji, to organ ESDZ ds. bezpieczeństwa przyjmuje na siebie odpowiedzialność wytwórcy po uzyskaniu jednogłośnej przychylnej opinii Komitetu ds. Bezpieczeństwa ESDZ.

IV. UPOWAŻNIENIE DO UDOSTĘPNIANIA EUCI PAŃSTWOM TRZECIM LUB ORGANIZACJOM MIĘDZYNARODOWYM

10. W przypadku gdy zgodnie z art. 10 ust. 1 załącznika A istnieją ramy wymiany informacji niejawnych z państwem trzecim lub organizacją międzynarodową, decyzję o udostępnieniu EUCI przez ESDZ państwu trzeciemu lub organizacji międzynarodowej podejmuje organ ESDZ ds. bezpieczeństwa, który może delegować udzielanie takiego upoważnienia urzędnikom ESDZ wysokiego szczebla bądź innym podlegającym mu osobom.

11. Jeżeli ESDZ nie jest wytwórcą informacji niejawnej, która ma zostać udostępniona, ani wytwórcą materiału źródłowego, który może ona zawierać, to ESDZ najpierw zwraca się o pisemną zgodę wytwórcy w celu ustalenia, że nie ma przeciwwskazań dla udostępnienia tej informacji. Jeśli ESDZ nie jest w stanie ustalić wytwórcy informacji, to organ ESDZ ds. bezpieczeństwa przyjmuje na siebie odpowiedzialność wytwórcy po uzyskaniu jednogłośnej przychylnej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ.

V. WYJĄTKOWE UDOSTĘPNIANIE EUCI AD HOC

12. W przypadku braku ram, o których mowa w art. 10 ust. 1 załącznika A, i jeśli interes UE lub co najmniej jednego z jej państw członkowskich wymaga udostępnienia EUCI z przyczyn politycznych, operacyjnych lub z innych pilnych powodów, w drodze wyjątku można udostępnić EUCI państwu trzeciemu lub organizacji międzynarodowej po podjęciu opisanych poniżej działań.

Dyrekcja ds. Bezpieczeństwa ESDZ, po zapewnieniu spełnienia warunków określonych w pkt 11:

a) w miarę możliwości sprawdza z organami bezpieczeństwa w danym państwie trzecim lub danej organizacji międzynarodowej, czy ich przepisy, struktury i procedury dotyczące bezpieczeństwa gwarantują ochronę udostępnianych EUCI zgodnie z normami nie mniej rygorystycznymi niż normy określone w niniejszej decyzji;

b) zwraca się do Komitetu ds. Bezpieczeństwa, by na podstawie dostępnych informacji wydał opinię dotyczącą zaufania, jakie można mieć do przepisów, struktur i procedur dotyczących bezpieczeństwa w państwie trzecim lub organizacji międzynarodowej, którym mają zostać udostępnione EUCI;

c) zwraca się do organu ESDZ ds. bezpieczeństwa, który może postanowić o udostępnieniu informacji pod warunkiem uzyskania jednogłośnej przychylnej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ.

13. W przypadku braku ram, o których mowa w art. 10 ust. 1 załącznika A, dana strona trzecia zobowiązuje się na piśmie do odpowiedniej ochrony EUCI.

DODATEK A

DEFINICJE

Na potrzeby niniejszej decyzji stosuje się następujące definicje:

„akredytacja" oznacza proces prowadzący do formalnego stwierdzenia przez organ ds. akredytacji bezpieczeństwa (SAA), że określony system jest zatwierdzony do celów działania na zdefiniowanym poziomie klauzuli tajności, w konkretnym trybie bezpiecznej pracy systemu w swoim środowisku operacyjnym oraz na poziomie ryzyka możliwym do zaakceptowania, przy założeniu, że wdrożono zatwierdzony zestaw technicznych, fizycznych, organizacyjnych i proceduralnych środków bezpieczeństwa;

„zasoby" lub „majątek" oznacza wszystko, co ma wartość dla organizacji, jej działalności i ciągłości, w tym zasoby informacyjne wspierające misję organizacji;

„uprawnienie do dostępu do EUCI" oznacza uprawnienie wydawane zgodnie z niniejszą decyzją przez organ ESDZ ds. bezpieczeństwa po wydaniu PBO przez odpowiednie organy państwa członkowskiego, stanowiące poświadczenie, że dana osoba – o ile stwierdzono, że spełnia ona zasadę ograniczonego dostępu – może uzyskać dostęp do EUCI opatrzonych klauzulą tajności do określonego poziomu (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonego terminu (zob. art. 2 załącznika A I);

„naruszenie" oznacza działanie określonej osoby lub zaniechanie przez nią działania w sposób sprzeczny z zasadami bezpieczeństwa ustanowionymi w niniejszej decyzji lub z polityką bądź wytycznymi dotyczącymi bezpieczeństwa, określającymi środki niezbędne do ich wdrożenia;

„cykl życia CIS" oznacza cały okres istnienia CIS, który obejmuje powstanie pomysłu, opracowanie koncepcji, zaplanowanie, analizę wymogów, zaprojektowanie, utworzenie, testowanie, wdrożenie, działanie, konserwację i wycofanie z działania;

„umowa niejawna" oznacza umowę zawieraną przez ESDZ z wykonawcą na dostawę towarów, wykonanie robót lub świadczenie usług, której wykonanie wymaga dostępu do EUCI lub wytwarzania takich informacji bądź wiąże się z dostępem do nich lub ich wytwarzaniem;

„niejawna umowa o podwykonawstwo" oznacza umowę zawieraną przez wykonawcę ESDZ z innym wykonawcą (tj. podwykonawcą) na dostawę towarów, wykonanie robót lub świadczenie usług, której wykonanie wymaga dostępu do EUCI lub wytwarzania takich informacji bądź wiąże się z dostępem do nich lub ich wytwarzaniem;

„system teleinformatyczny" (CIS) oznacza każdy system umożliwiający obchodzenie się z informacjami w formie elektronicznej. System teleinformatyczny obejmuje wszystkie zasoby niezbędne do jego funkcjonowania, w tym infrastrukturę, organizację, personel oraz zasoby informatyczne (zob. art. 8 ust. 2 załącznika A);

„nieuprawnione ujawnienie EUCI" oznacza ujawnienie EUCI w całości lub częściowo nieupoważnionym osobom lub podmiotom (zob. art. 8 ust. 2);

„wykonawca" oznacza osobę fizyczną lub prawną posiadającą zdolność prawną do zawierania umów;

„produkty kryptograficzne" oznaczają algorytmy kryptograficzne, sprzęt i oprogramowanie kryptograficzne, a także produkty zawierające szczegóły stosowania i związaną z nim dokumentację oraz klucze;

„operacja WPBiO" oznacza wojskową lub cywilną operację zarządzania kryzysowego prowadzoną na mocy tytułu V rozdział 2 TUE;

„zniesienie klauzuli tajności" oznacza zniesienie wszelkiej klauzuli tajności;

„ochrona w głąb" oznacza stosowanie szeregu środków bezpieczeństwa o strukturze różnych poziomów ochrony;

„wyznaczona władza bezpieczeństwa" (WWB) oznacza instytucję odpowiedzialną wobec krajowej władzy bezpieczeństwa (KWB) w państwie członkowskim, odpowiadającą za przekazywanie podmiotom gospodarczym lub innym informacji dotyczących krajowej polityki we wszelkich kwestiach związanych z bezpieczeństwem przemysłowym oraz za udzielanie wskazówek i pomocy w jej realizacji. Zadania WWB może wykonywać KWB lub dowolny inny właściwy organ;

„dokument" oznacza wszelką zapisaną informację, niezależnie od jej postaci fizycznej lub cech;

„obniżenie klauzuli tajności" oznacza obniżenie poziomu klauzuli tajności;

„informacje niejawne UE" (EUCI) 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 (zob. art. 2 lit. f));

„świadectwo bezpieczeństwa przemysłowego" oznacza stwierdzenie przez KWB lub WWB w wyniku procedur administracyjnych, że z punktu widzenia bezpieczeństwa dany obiekt jest w stanie zapewnić odpowiednią ochronę EUCI opatrzonych określoną klauzulą tajności, a personel tego obiektu, któremu niezbędny jest dostęp do EUCI, posiada odpowiednie poświadczenie bezpieczeństwa i odebrał instruktaż dotyczący odpowiednich wymogów bezpieczeństwa niezbędnych do uzyskania dostępu do EUCI i do ochrony EUCI;

„obchodzenie się" z EUCI oznacza wszelkie możliwe działania, jakim mogą być poddawane EUCI w całym cyklu ich życia. Pojęcie to obejmuje wytwarzanie, przetwarzanie i przenoszenie EUCI, obniżanie lub znoszenie ich klauzul tajności oraz ich zniszczenie. W odniesieniu do CIS pojęcie to obejmuje również gromadzenie, wyświetlanie, przesyłanie i przechowywanie EUCI;

„posiadacz" oznacza odpowiednio uprawnioną osobę, spełniającą zasadę ograniczonego dostępu, w której posiadaniu znajduje się EUCI i która w związku z tym odpowiada za jej ochronę;

„podmiot gospodarczy lub inny" oznacza podmiot zaangażowany w dostawę towarów, wykonanie robót lub świadczenie usług; może to być podmiot przemysłowy, gospodarczy, usługowy, naukowy, badawczy, edukacyjny lub rozwojowy bądź osoba prowadząca działalność gospodarczą;

„bezpieczeństwo przemysłowe" oznacza stosowanie środków mających zapewnić ochronę EUCI przez wykonawców lub podwykonawców podczas negocjacji poprzedzających zawarcie umów i na wszystkich etapach cyklu życia umów niejawnych (zob. art. 9 ust. 1 załącznika A);

„zabezpieczanie informacji" w ramach systemów teleinformatycznych oznacza pewność, że systemy te będą chronić informacje, z którymi się obchodzą, i będą działać zgodnie z potrzebami i w każdej sytuacji, w której będzie to potrzebne, pod kontrolą uprawnionych użytkowników. Skuteczne zabezpieczanie informacji gwarantuje odpowiedni poziom poufności, integralności, dostępności, niezaprzeczalności i autentyczności. Zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem (zob. art. 8 ust. 1 załącznika A);

„połączenie międzysystemowe" oznacza, do celów niniejszej decyzji, bezpośrednie połączenie co najmniej dwóch systemów informatycznych w celu wspólnego korzystania z danych i innych zasobów informacyjnych (np. łączności) w sposób jednokierunkowy lub wielokierunkowy (zob. załącznik A IV, pkt 31);

„zarządzanie informacjami niejawnymi" polega na stosowaniu środków administracyjnych służących kontroli EUCI na wszystkich etapach ich cyklu życia w uzupełnieniu środków przewidzianych w art. 5, 6 i 8, co ma pomóc w powstrzymywaniu od zamierzonego lub przypadkowego nieuprawnionego ujawnienia tych informacji lub ich utraty, w wykrywaniu takich przypadków i usuwaniu ich skutków. Środki takie dotyczą w szczególności wytwarzania, rejestracji, kopiowania, tłumaczenia i przenoszenia EUCI, obchodzenia się z nimi, ich przechowywania i niszczenia (zob. art. 7 ust. 1 załącznika A);

„materiały" oznaczają jakikolwiek dokument lub dowolne urządzenia lub sprzęt, już wytworzone lub będące w trakcie wytwarzania;

„wytwórca" oznacza instytucję, agencję lub organ UE, państwo członkowskie, państwo trzecie lub organizację międzynarodową, w ramach właściwości której wytworzono informacje niejawne lub wprowadzono je do struktur UE;

„bezpieczeństwo osobowe" oznacza stosowanie środków gwarantujących, że dostęp do EUCI jest przyznawany tylko osobom, które:

— spełniają zasadę ograniczonego dostępu,

— w odniesieniu do dostępu do informacji o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej – otrzymały poświadczenie bezpieczeństwa do odpowiedniego poziomu lub ze względu na pełnione przez siebie funkcje otrzymały inne odpowiednie uprawnienie zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; oraz

— zostały poinformowane o swojej odpowiedzialności

(zob. art. 5 ust. 1 załącznika A);

„poświadczenie bezpieczeństwa osobowego" (PBO) w zakresie dostępu do EUCI oznacza oświadczenie właściwego organu państwa członkowskiego, wydawane po zakończeniu postępowania sprawdzającego prowadzonego przez właściwe organy państwa członkowskiego; stanowi ono poświadczenie, że dana osoba – o ile stwierdzono, że spełnia ona zasadę ograniczonego dostępu – może uzyskać dostęp do EUCI opatrzonych klauzulą tajności do określonego poziomu (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonej daty; osobę taką określa się jako posiadającą „poświadczenie bezpieczeństwa".

„zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego" oznacza zaświadczenie wydane przez właściwy organ, potwierdzające, że dana osoba posiada poświadczenie bezpieczeństwa, oraz zawierające informację o poziomie klauzuli tajności EUCI, do których dana osoba może uzyskać dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższym), dacie ważności odpowiedniego PBO oraz dacie ważności samego zaświadczenia;

„bezpieczeństwo fizyczne" oznacza stosowanie fizycznych i technicznych środków ochrony w celu powstrzymania nieuprawnionego dostępu do EUCI (zob. art. 6 załącznika A);

„instrukcje bezpieczeństwa programu/projektu (IBP)" oznaczają wykaz procedur bezpieczeństwa stosowanych do określonego programu/projektu w celu ujednolicenia procedur bezpieczeństwa. Instrukcje mogą być zmieniane podczas trwania programu/projektu;

„rejestracja" oznacza stosowanie procedur rejestrowania etapów cyklu życia informacji, w tym jej dystrybucji i zniszczenia (zob. pkt 21 załącznika A III);

„ryzyko szczątkowe" oznacza ryzyko, które pozostaje po wdrożeniu środków bezpieczeństwa, z uwagi na to, że nie przeciwdziała się wszystkim zagrożeniom i że nie każdą podatność można wyeliminować;

„ryzyko" oznacza prawdopodobieństwo, że dane zagrożenie wykorzysta wewnętrzną i zewnętrzną podatność danej organizacji lub jakiegokolwiek systemu przez nią używanego i przez to spowoduje szkody dla tej organizacji i jej zasobów materialnych lub niematerialnych. Ryzyko mierzone jest jako połączenie prawdopodobieństwa wystąpienia zagrożeń oraz ich skutków;

„akceptacja ryzyka" jest decyzją o zaakceptowaniu dalszego występowania określonego ryzyka szczątkowego po zmniejszeniu ryzyka;

„ocena ryzyka" polega na określaniu zagrożeń i podatności oraz przeprowadzeniu odpowiedniej analizy ryzyka, tj. analizy prawdopodobieństwa i skutków;

„powiadamianie o ryzyku" polega na upowszechnianiu wiedzy o ryzyku wśród społeczności korzystających z CIS, na informowaniu o takim ryzyku organów zatwierdzających i na składaniu sprawozdań z nich organom operacyjnym;

„proces zarządzania ryzykiem" oznacza cały proces określania, kontrolowania i minimalizacji niepewnych zdarzeń, które mogą wpłynąć na bezpieczeństwo danej organizacji lub jakiegokolwiek systemu przez nią używanego. Obejmuje on wszystkie działania związane z ryzykiem, w tym ocenę, zmniejszanie, akceptację i powiadamianie;

„zmniejszanie ryzyka" polega na łagodzeniu, usuwaniu lub redukowaniu ryzyka (przy pomocy odpowiedniego połączenia środków technicznych, fizycznych, organizacyjnych lub proceduralnych) lub jego przenoszeniu lub monitorowaniu;

„dokument określający aspekty bezpieczeństwa" (DOAB) oznacza zbiór specjalnych warunków umownych, wydany przez instytucję zamawiającą, stanowiący integralną część każdej umowy niejawnej obejmującej dostęp do EUCI lub ich wytwarzanie, określający wymogi bezpieczeństwa lub wskazujący te elementy umowy, których bezpieczeństwo wymaga ochrony (zob. sekcja II załącznika A V);

„przewodnik nadawania klauzul" (PNK) oznacza dokument opisujący niejawne elementy programu lub umowy i określający mające zastosowanie poziomy klauzul tajności. PNK może być rozszerzany podczas trwania programu lub umowy, a klauzule tajności dla części informacji mogą być zmieniane lub obniżane; jeżeli PNK jest opracowany, to powinien być częścią SAL (zob. sekcja II załącznika A V);

„postępowanie sprawdzające" oznacza procedury sprawdzające przeprowadzane przez właściwy organ państwa członkowskiego zgodnie z jego przepisami ustawowymi i wykonawczymi w celu uzyskania pewności, że nie istnieją żadne znane niekorzystne okoliczności, które mogłyby stanowić przeszkodę w wydaniu danej osobie krajowego PBO lub PBO UE do dostępu do EUCI do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej);

„procedury bezpiecznej eksploatacji systemu" (SecOP) oznaczają opis sposobu wdrożenia polityki bezpieczeństwa, który należy przyjąć, procedur operacyjnych, których należy przestrzegać, oraz obowiązków personelu;

„oświadczenie o szczególnych wymaganiach bezpieczeństwa" (SSRS) oznacza wiążący zestaw zasad bezpieczeństwa, których należy przestrzegać, oraz szczegółowych wymogów bezpieczeństwa, które należy wdrożyć, stanowiący podstawę procesu certyfikacji i akredytacji CIS;

„TEMPEST" oznacza sprawdzanie, analizę i kontrolę emisji elektromagnetycznych umożliwiających przechwycenie danych oraz środki służące tłumieniu takich emisji;

„zagrożenie" oznacza potencjalną przyczynę niepożądanego incydentu, który może skutkować szkodą dla organizacji lub jakiegokolwiek systemu przez nią używanego; zagrożenia takie mogą być przypadkowe lub zamierzone (rozmyślne) i obejmują elementy zagrażające, potencjalne cele i metody ataku;

„podatność" oznacza każdego rodzaju słaby punkt, który może zostać wykorzystany przez jedno zagrożenie lub większą ich liczbę. Podatność może być zaniechaniem lub może odnosić się do słabego punktu środków kontroli, jeżeli chodzi o ich solidność, wszechstronność lub spójność; może mieć charakter techniczny, proceduralny, fizyczny, organizacyjny lub operacyjny.