Този документ е средство за документиране и не обвързва институциите

►**B**

РЕШЕНИЕ НА СЪВЕТА

от 23 септември 2013 година

относно правилата за сигурност за защита на класифицирана информация на ЕС

(2013/488/ЕС)

(ОВ L 274, 15.10.2013 г., стр. 1)

Изменено със:

		Официален вестник		
		№	страница	дата
►**M1**	Решение 2014/233/ЕС на Съвета от 14 април 2014 година	L 125	72	26.4.2014 г.

▼B

РЕШЕНИЕ НА СЪВЕТА

от 23 септември 2013 година

относно правилата за сигурност за защита на класифицирана информация на ЕС

(2013/488/ЕС)

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 240, параграф 3 от него,

като взе предвид Решение 2009/937/ЕС на Съвета от 1 декември 2009 г. за приемане на процедурен правилник на Съвета [1], и по-специално член 24 от него,

като има предвид, че:

(1) За да се развиват дейностите на Съвета във всички области, които изискват работа с класифицирана информация, е подходящо да се създаде всеобща система за сигурност за защита на класифицирана информация, която да обхваща Съвета, неговия генерален секретариат и държавите членки.

(2) Настоящото решение следва да се прилага в случаите, когато Съветът, неговите подготвителни органи и генералният секретариат на Съвета (ГСС) работят с класифицирана информация на ЕС (КИЕС).

(3) В съответствие с националните законови и подзаконови актове и в степента, необходима за функционирането на Съвета, държавите членки следва да спазват настоящото решение при работа на техните компетентни органи, служители и изпълнители с КИЕС, така че всички да имат увереност, че на КИЕС се осигурява еднакво ниво на защита.

(4) Съветът, Комисията и Европейската служба за външна дейност (ЕСВД) са решени да прилагат равностойни стандарти за сигурност за защита на КИЕС.

(5) Съветът подчертава значението на присъединяването, когато е подходящо, на Европейския парламент и на други институции, органи, служби или агенции на Съюза към принципите, стандартите и правилата за защита на класифицирана информация, които са необходими, за да се защитят интересите на Съюза и на неговите държавите членки.

(6) Съветът следва да определи подходящата рамка за обмен на КИЕС, която се държи от Съвета, с други институции, органи, служби и агенции на Съюза, по целесъобразност в съответствие с настоящото решение и действащите междуинституционални договорености.

(7) Органите и агенциите на Съюза, създадени съгласно дял V, глава 2 от Договора за Европейския съюз (ДЕС), Европол и Евроюст следва да прилагат в рамките на вътрешната си организация основните принципи и минимални стандарти, установени в настоящото решение за защита на КИЕС, когато това е предвидено в акта за създаването им.

[1] ОВ L 325, 11.12.2009 г., стр. 35.

▼B

(8) Операциите за управление на кризи, създадени съгласно дял V, глава 2 от ДЕС, и техният персонал следва да прилагат правилата за сигурност, приети от Съвета за защита на КИЕС, когато това е предвидено в акта на Съвета за създаването им.

(9) Специалните представители на ЕС и членовете на техните екипи следва да прилагат приетите от Съвета правила за сигурност за защита на КИЕС, когато това е предвидено в съответния акт на Съвета.

(10) Настоящото решение се приема, без да се засягат членове 15 и 16 от Договора за функционирането на Европейския съюз (ДФЕС) и инструментите за изпълнението им.

(11) Настоящото решение се приема, без да се засягат съществуващите практики в държавите членки за информиране на националните им парламенти за дейностите на Съюза.

(12) С цел да се гарантира навременното прилагане на правилата за сигурност за защита на КИЕС във връзка с присъединяването на Република Хърватия към Европейския съюз, настоящото решение следва да влезе в сила в деня на публикуването му,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Цел, приложно поле и определения

1. С настоящото решение се установяват основните принципи и минимални стандарти за сигурност с оглед защитата на КИЕС.

2. Тези основни принципи и минимални стандарти се прилагат от Съвета и ГСС и се спазват от държавите членки в съответствие с техните национални законови и подзаконови актове, така че всички да имат увереност, че на КИЕС се осигурява еднакво ниво на защита.

3. За целите на настоящото решение се прилагат определенията, изложени в допълнение А.

Член 2

Определение на КИЕС, класификации за сигурност и грифове

1. „Класифицирана информация на ЕС“ (КИЕС) означава всяка информация или материал, носещи гриф за сигурност на ЕС, неразрешеното разкриване на които би могло да увреди в различна степен интересите на Европейския съюз или на една или повече от държавите членки.

2. КИЕС се класифицира на някое от следните нива:

а) TRÈS SECRET UE/EU TOP SECRET: информация и материали, неразрешеното разкриване на които би могло да увреди изключително сериозно съществените интереси на Европейския съюз или на една или повече от държавите членки.

б) SECRET UE/EU SECRET: информация и материали, неразрешеното разкриване на които би могло да увреди сериозно съществените интереси на Европейския съюз или на една или повече от държавите членки.

▼B

в) CONFIDENTIEL UE/EU CONFIDENTIAL: информация и материали, неразрешеното разкриване на които би могло да увреди съществените интереси на Европейския съюз или на една или повече от държавите членки.

г) RESTREINT UE/EU RESTRICTED: информация и материали, неразрешеното разкриване на които би се отразило неблагоприятно на интересите на Европейския съюз или на една или повече от държавите членки.

3. КИЕС носи гриф за сигурност в съответствие с параграф 2. Може да се добавят и допълнителни обозначения с цел да се посочи сферата на дейност, до която се отнася тя, да се идентифицира създателят, да се ограничи разпределението ѝ, да се ограничи ползването ѝ или да се обозначи доколко тази информация подлежи на предоставяне.

Член 3

Управление на класификацията

1. Компетентните органи правят необходимото КИЕС да бъде подходящо класифицирана, ясно обозначена като класифицирана информация и да запазва нивото си на класификация само докато това е необходимо.

2. Нивото на класификация на КИЕС не се понижава или тя не се декласифицира, както и никой от посочените в член 2, параграф 3 грифове не се изменя или премахва без предварителното писмено съгласие на създателя на информацията.

3. Съветът одобрява политика за сигурност по отношение на създаването на КИЕС, която включва практическо ръководство за класифициране.

Член 4

Защита на класифицираната информация

1. На КИЕС се осигурява защита в съответствие с настоящото решение.

2. Притежателят на какъвто и да е елемент от КИЕС носи отговорност за защитата му в съответствие с настоящото решение.

3. Когато държавите членки въвеждат в структурите или мрежите на Съюза класифицирана информация, обозначена с национален гриф за сигурност, Съветът и ГСС осигуряват защита на тази информация в съответствие с изискванията, приложими към КИЕС на съответстващото ниво, съгласно съдържащата се в допълнение Б таблица на съответствието на нивата на класификация за сигурност.

4. За даден масив от КИЕС може да се наложи защита на по-високо ниво на класификация, отколкото на отделните му компоненти.

▼B

Член 5

Управление на риска за сигурността

1. Рискът по отношение на КИЕС се управлява като процес. Този процес има за цел да се установят познатите рискове за сигурността, да се набележат мерки за сигурност с оглед свеждане на такива рискове до приемливо ниво съгласно установените в настоящото решение основни принципи и минимални стандарти и да се прилагат тези мерки в съответствие с концепцията за защита в дълбочина, както е определена в допълнение А. Ефективността на тези мерки подлежи на постоянна оценка.

2. Мерките за сигурност за защита на КИЕС за целия ѝ жизнен цикъл съответстват по-конкретно на нивото на класификацията ѝ за сигурност, формата и обема на информацията или материалите, местоположението и конструкцията на структурите, в които се намира КИЕС, както и оценката на местно ниво на риска от злонамерени и/или престъпни действия, включително шпионаж, саботаж и тероризъм.

3. Плановете за действие при извънредни ситуации отчитат необходимостта от защита на КИЕС в извънредни ситуации, за да се предотврати неразрешен достъп, разкриване или загуба на интегритета или наличността.

4. В плановете за непрекъснатост на дейността се включват мерки за предотвратяване и възстановяване с оглед да се намали въздействието на сериозни грешки или инциденти при работа с КИЕС и нейното съхранение.

Член 6

Изпълнение на настоящото решение

1. При необходимост Съветът, по препоръка на Комитета по сигурността, одобрява политиките за сигурност, които определят мерки за изпълнение на настоящото решение.

2. Комитетът по сигурността може да договори на своето ниво насоки за сигурност с оглед да се допълнят или подкрепят настоящото решение и одобрените от Съвета политики за сигурност.

Член 7

Персонална сигурност

1. Персоналната сигурност означава прилагане на мерки за гарантиране, че достъп до КИЕС се предоставя единствено на лица, които:

— е необходимо да знаят,

— са преминали проучване за надеждност за съответното ниво, когато е необходимо, и

— са информирани за отговорностите си.

2. Процедурите за проучване на персонала за надеждност имат за цел да се определи дали може да се даде разрешение за достъп до КИЕС на дадено физическо лице, като се имат предвид неговата лоялност и надеждност.

▼B

3. В ГСС всички лица, на които за изпълнение на служебните задължения е необходимо да имат достъп до или да работят с КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, преминават проучване за надеждност за съответното ниво, преди да им бъде предоставен достъп до такава КИЕС. Тези лица трябва да имат разрешение от назначаващия орган на ГСС за достъп до КИЕС до определено ниво и с определен срок.

4. Служителите на държавите членки, посочени в член 15, параграф 3, на които за изпълнение на служебните задължения може да е необходим достъп до КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, преминават проучване за надеждност за съответното ниво или са съответно надлежно оправомощени по силата на своите функции, в съответствие с националните законови и подзаконови актове, преди да им бъде предоставен достъп до такава КИЕС.

5. Преди да им бъде предоставен достъп до КИЕС и периодично след това всички лица биват информирани за задължението си да опазват КИЕС в съответствие с настоящото решение и декларират, че са запознати с тези задължения.

6. Разпоредбите за изпълнение на настоящия член се съдържат в приложение I.

Член 8

Физическа сигурност

1. Физическа сигурност означава прилагане на физически и технически защитни мерки за предотвратяване на неразрешен достъп до КИЕС.

2. Мерките за физическа сигурност са предназначени за предотвратяване на тайно или насилствено проникване на нарушител, за възпиране, препятстване и разкриване на неразрешени действия и за даване на възможност за категоризиране на персонала по отношение на достъпа до КИЕС на основата на принципа „необходимост да се знае“. Тези мерки се определят на базата на процес за управление на риска.

3. Мерки за физическа сигурност се въвеждат за всички помещения, сгради, офиси, зали и други зони, в които се работи с КИЕС или се съхранява такава, включително зони, в които се помещават комуникационни и информационни системи, съгласно определеното в член 10, параграф 2.

4. Зони, в които се съхранява КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, се определят като зони за сигурност в съответствие с приложение II и се одобряват от компетентния орган по сигурността.

5. За защита на КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо се използват единствено одобрени устройства или оборудване.

6. Разпоредбите за изпълнение на настоящия член се съдържат в приложение II.

▼B

Член 9

Управление на класифицирана информация

1. Управлението на класифицирана информация представлява прилагане на административни мерки за контрол на КИЕС през жизнения ѝ цикъл в допълнение на мерките, предвидени в членове 7, 8 и 10, като по този начин се съдейства за възпиране и разкриване на умишлено или случайно компрометиране или загуба на такава информация. Тези мерки се отнасят по-конкретно до създаването, регистрирането, копирането, писмения превод, понижаването на нивото на класификация, декласификацията, преноса и унищожаването на КИЕС.

2. Информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо се регистрира за целите на сигурността, преди да бъде разпространена и при получаването ѝ. За целта компетентните органи в ГСС и в държавите членки създават регистрационна система. Информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се регистрира в специални регистратури.

3. Службите и помещенията, в които се работи с КИЕС или се съхранява такава, подлежат на редовни проверки от компетентния орган по сигурността.

4. КИЕС се предава между различните служби и помещения извън физически защитените зони, както следва:

а) като общо правило КИЕС се предава чрез електронни средства, защитени чрез криптографски продукти, одобрени в съответствие с член 10, параграф 6;

б) когато средствата, посочени в буква а), не са използвани, КИЕС се пренася или:

i) на електронен носител (напр. USB памет, компактдиск, твърд диск), защитен чрез криптографски продукти, одобрени в съответствие с член 10, параграф 6; или

ii) във всички останали случаи — в съответствие с предписанията на компетентния орган по сигурността, съгласно съответните защитни мерки, установени в приложение III.

5. Разпоредбите за изпълнение на настоящия член се съдържат в приложения III и IV.

Член 10

Защита на КИЕС, с която се работи в комуникационни и информационни системи

1. Осигуреност на информацията (ОИ) в областта на комуникационните и информационните системи е увереността, че тези системи ще осигурят защита на информацията, с която се работи в тях, и че ще функционират, както и когато е необходимо, под контрола на легитимни ползватели. Ефективната ОИ гарантира необходимите нива на поверителност, интегритет, наличност, невъзможност за отказ и автентичност. ОИ се основава на процес за управление на риска.

▼B

2. „Комуникационна и информационна система“ (КИС) означава всяка система, даваща възможност за работа с класифицирана информация в електронна форма. Една КИС обхваща всички активи, необходими за нейното функциониране, включително инфраструктура, организация, персонал и информационни ресурси. Настоящото решение се прилага за КИС, работещи с КИЕС.

3. КИС работят с КИЕС в съответствие с концепцията за ОИ.

4. Всички КИС преминават през процес на акредитация. Целта на акредитацията е да се гарантира, че са изпълнени всички необходими мерки за сигурност и е постигнато достатъчно ниво на защита на КИЕС и на КИС в съответствие с настоящото решение. В декларацията за акредитация се определя най-високото ниво на класификация за сигурност на информацията, с което може да се работи в дадена КИС, както и съответните изисквания и условия за това.

5. С цел защита на КИС за работа с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и по-високо по начин, който да не допуска информацията да бъде компрометирана от неумишлени електромагнитни излъчвания, се прилагат мерки за сигурност на информацията („мерки за сигурност по Tempest“). Тези мерки за сигурност са съизмерими с риска от експлоатация и нивото на класификация на информацията.

6. Когато защитата на КИЕС се осигурява от криптографски продукти, такива продукти се одобряват, както следва:

а) защита на поверителността на информацията с ниво на класификация за сигурност SECRET UE/EU SECRET и по-високо се осигурява чрез криптографски продукти, одобрени от Съвета в качеството му на орган за криптографско одобрение (ОКО) по препоръка на Комитета по сигурността;

б) защита на поверителността на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или RESTREINT UE/EU RESTRICTED се осигурява чрез криптографски продукти, одобрени от генералния секретар на Съвета („генералния секретар“), действащ в качеството си на ОКО, по препоръка на Комитета по сигурността.

Без да се засяга буква б), при предаване в рамките на националните системи на държавите членки поверителността на КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или RESTREINT UE/EU RESTRICTED може да бъде защитена чрез криптографски продукти, одобрени от ОКО на държавата членка.

7. При предаване на КИЕС чрез електронни средства се използват одобрени криптографски продукти. Въпреки това изискване, при извънредни обстоятелства могат да се прилагат специфични процедури или специфични технически конфигурации, както е посочено в приложение IV.

▼B

8. Компетентните органи съответно на ГСС и на държавите членки създават следните органи по ОИ:

а) орган по ОИ (ООИ);

б) орган по Tempest (ОТ);

в) орган за криптографско одобрение (ОКО);

г) орган за разпределение на криптографски материали (ОРКМ).

9. За всяка система компетентните органи съответно на ГСС и на държавите членки създават:

а) орган по акредитиране на сигурността (ОАС);

б) оперативен орган по ОИ.

10. Разпоредбите за изпълнение на настоящия член се съдържат в приложение IV.

Член 11

Индустриална сигурност

1. Индустриална сигурност е прилагането на мерки за гарантиране на защитата на КИЕС от изпълнители или подизпълнители по време на преговори за сключване на договор и през целия жизнен цикъл на класифицирани договори. При такива договори не се допуска достъп до информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET.

2. ГСС може да възложи с договор изпълнението на задачи, включващи или налагащи достъп до КИЕС или работа с КИЕС, или нейното съхранение, на индустриални или други единици, регистрирани в държава членка или в трета държава, която е сключила споразумение или административна договореност в съответствие с член 13, параграф 2, буква а) или б).

3. ГСС в качеството си на възложител гарантира, че при възлагане на класифицирани договори на индустриални или други единици се спазват минималните стандарти за индустриална сигурност, установени в настоящото решение и посочени в договора.

4. Във всяка държава членка националният орган по сигурността (НОС), определеният орган по сигурността (ООС) или друг компетентен орган гарантира, във възможната според националните законови и подзаконови актове степен, че изпълнителите и подизпълнителите, регистрирани на нейна територия, вземат всички необходими мерки за защита на КИЕС по време на преговорите за сключване или по време на изпълнението на класифициран договор.

5. Във всяка държава членка НОС, ООС или друг компетентен орган по сигурността гарантира в съответствие с националните законови и подзаконови актове, че изпълнителите и подизпълнителите, регистрирани в съответната държава членка, които участват в класифицирани договори за изпълнение и подизпълнение, изискващи достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET в рамките на техните обекти както при изпълнение на такива договори, така и по време на преддоговорния етап, разполагат с удостоверение за сигурност на структура (УСС) на съответното ниво на класификация за сигурност.

▼B

6. На изпълнителския или подизпълнителския персонал, на който е необходим достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET за изпълнение на класифициран договор, се дава разрешение за достъп на персонала (РДП) от съответния НОС, ООС или друг компетентен орган по сигурността, в съответствие с националните законови и подзаконови актове и минималните стандарти за сигурност, установени в приложение I.

7. Разпоредбите за изпълнение на настоящия член се съдържат в приложение V.

Член 12

Обмен на КИЕС

1. Съветът определя условията, съгласно които може да обменя държана от него КИЕС с други институции, органи, служби или агенции на Съюза. Може да се въведе съответна рамка за тази цел, включително като се сключат междуинституционални споразумения или други договорености при необходимост за целта.

2. Тази рамка гарантира, че на КИЕС е осигурена защита, съответстваща на нивото ѝ на класификация и на основни принципи и минимални стандарти, които са равностойни на определените в настоящото решение.

Член 13

Обмен на класифицирана информация с трети държави и международни организации

1. Когато Съветът реши, че съществува необходимост от обмен на КИЕС с трета държава или международна организация, за тази цел се създава подходяща рамка.

2. За създаване на такава рамка и за определяне на реципрочни правила за защита на обменяната класифицирана информация:

а) Съюзът сключва с трети държави или международни организации споразумения за процедури за сигурност за обмен и защита на класифицирана информация („споразумения за сигурност на информацията“); или

б) генералният секретар може да встъпи в административни договорености от името на ГСС в съответствие с точка 17 от приложение VI, ако нивото на класификация на КИЕС, която се предоставя, като правило не надвишава RESTREINT UE/EU RESTRICTED.

3. Споразуменията за сигурност на информацията или административните договорености, посочени в параграф 2, съдържат разпоредби, които гарантират, че когато трети държави или международни организации получат КИЕС, тази информация е защитена на ниво, съответстващо на класификацията ѝ, и съобразно минимални стандарти, които са не по-малко стриктни от стандартите, установени с настоящото решение.

▼B

4. Решението да се предостави на трета държава или международна организация КИЕС, създадена в Съвета, се взема от Съвета поотделно за всеки конкретен случай, в зависимост от естеството и съдържанието на тази информация, „необходимостта да се знае“ от получателя и предимствата, които това дава на Съюза. Ако исканата класифицирана информация не е създадена от Съвета, ГСС най-напред иска писмено съгласие за нейното предоставяне от създателя на информацията. Ако създателят на информацията не може да бъде установен, неговата отговорност се поема от Съвета.

5. За да се установи ефективността на съществуващите в трета държава или международна организация мерки за сигурност за защита на предоставена или обменена КИЕС, се организират посещения за оценка.

6. Разпоредбите за изпълнение на настоящия член се съдържат в приложение VI.

Член 14

Нарушения на сигурността и компрометиране на КИЕС

1. До нарушение на сигурността се стига в резултат на действие или бездействие от физическо лице, което противоречи на правилата за сигурност, установени в настоящото решение.

2. До компрометиране на КИЕС се стига, когато в резултат на нарушение на сигурността тя бъде изцяло или частично разкрита пред неоправомощени лица.

3. Всяко нарушение на сигурността или подозрение за такова нарушение се докладва незабавно на компетентния орган по сигурността.

4. Когато е известно или когато има достатъчно основания да се приеме, че КИЕС е компрометирана или изгубена, НОС или друг компетентен орган предприема всички необходими мерки съгласно съответните законови и подзаконови актове за:

а) информиране на създателя на информацията;

б) осигуряване на разследване на случая от служители, които нямат непосредствено отношение към нарушението, с оглед установяване на фактите;

в) извършване на оценка на потенциалните вреди, причинени на интересите на Съюза или на държавите членки;

г) предприемане на необходимите мерки за предотвратяване на повторно нарушение; и

д) уведомяване на съответните органи за предприетите действия.

5. На всяко лице, отговорно за нарушение на правилата за сигурност, установени в настоящото решение, могат да бъдат наложени дисциплинарни мерки в съответствие с приложимите правила и подзаконови актове. Всяко лице, отговорно за компрометиране или загуба на КИЕС, подлежи на дисциплинарно и/или съдебно производство в съответствие с приложимите закони, правила и подзаконови актове.

▼B

Член 15

Отговорност за прилагане на решението

1. Съветът предприема всички необходими мерки за гарантиране на цялостна съгласуваност при прилагане на настоящото решение.

2. Генералният секретар предприема всички необходими мерки, за да се гарантира, че при работа със или съхранение на КИЕС или друга класифицирана информация настоящото решение се прилага в използваните от Съвета обекти и в рамките на ГСС, от длъжностните лица и другите служители на ГСС, от командированите в ГСС служители, както и от външните изпълнители, наети от ГСС.

3. В съответствие с националните си законови и подзаконови актове държавите членки предприемат всички необходими мерки, за да гарантират, че при работа с КИЕС или при съхранението ѝ настоящото решение се спазва от:

а) служителите на постоянните представителства на държавите членки към Европейския съюз и от членовете на националните делегации, които присъстват на заседания на Съвета или на неговите подготвителни органи или които участват в други дейности на Съвета;

б) други служители в националните администрации на държавите членки, включително служители, командировани в тези администрации, независимо дали работят на територията на държавите членки или зад граница;

в) други лица в държавите членки, които по силата на изпълняваните от тях функции имат надлежно разрешение за достъп до КИЕС;

г) изпълнители, наети от държавите членки, независимо дали работят на територията на държавите членки или зад граница.

Член 16

Организация на сигурността в Съвета

1. В рамките на функциите си за осигуряване на цялостна съгласуваност при прилагане на настоящото решение Съветът одобрява:

а) споразуменията, посочени в член 13, параграф 2, буква а);

б) решенията, с което се разрешава или се дава съгласие за предоставяне на КИЕС, създадена или съхранявана от Съвета, на трети държави или международни организации, в съответствие с принципа на съгласие на създателя на информацията;

в) годишна програма за посещения за оценка, препоръчана от Комитета по сигурността, за посещения за оценка на службите и обектите в държавите членки, на органите, агенциите и структурите на Съюза, които прилагат настоящото решение или неговите принципи, и за посещения за оценка в трети държави и международни организации с цел да се удостовери ефективността на мерките, прилагани за защита на КИЕС; и

▼B

г) политиките за сигурност, предвидени в член 6, параграф 1.

2. Генералният секретар действа като орган на ГСС по сигурността. В това си качество генералният секретар::

а) изпълнява и прави преглед на политиката на Съвета в областта на сигурността;

б) координира с националните органи по сигурността на държавите членки всички въпроси на сигурността, свързани със защитата на класифицирана информация от значение за дейностите на Съвета;

в) предоставя на длъжностните лица на ГСС, на други служители и на командированите национални експерти разрешение за достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо — в съответствие с член 7, параграф 3;

г) когато е подходящо, разпорежда провеждане на разследване за всяко действително или подозирано компрометиране или загуба на класифицирана информация, държана или произхождаща от Съвета, и отправя към съответните органи по сигурността искане за съдействие при такива разследвания;

д) извършва периодични проверки на мерките по сигурността за защита на класифицираната информация в обектите на ГСС;

е) извършва периодични посещения за оценка на мерките по сигурността за защита на КИЕС в органите, агенциите и структурите на Съюза, които прилагат настоящото решение или неговите принципи;

ж) провежда съвместно и съгласувано със съответния НОС периодични оценки на мерките по сигурността за защита на КИЕС в службите и обектите на държавите членки;

з) прави необходимото за съответното координиране на мерките за сигурност с компетентните органи на държавите членки, отговарящи за защитата на класифицирана информация, и ако е уместно, с трети държави или международни организации, включително по отношение на естеството на заплахите за сигурността на КИЕС и средствата за защита срещу тях; и

и) влиза в административните договорености, посочени в член 13, параграф 2, буква б).

Службата на ГСС по сигурността е на разположение на генералния секретар, за да го подпомага при изпълнението на тези задачи.

3. За целите на изпълнението на член 15, параграф 3 държавите членки следва да:

а) определят НОС, вписан в допълнение В, който да отговаря за мерките по сигурността за защита на КИЕС, така че:

i) КИЕС, държана от национално ведомство, орган или агенция, публични или частни, в страната или зад граница, да бъде защитена в съответствие с настоящото решение;

ii) мерките по сигурността за защита на КИЕС да се проверяват или оценяват периодично;

▼B

iii) всички лица, работещи в националната администрация или наети от изпълнител, на които може да бъде предоставен достъп до класифицирана информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, да бъдат съответно проучени за надеждност или надлежно оправомощени по силата на изпълняваните от тях функции, съгласно националните законови и подзаконови актове;

iv) програмите за сигурност да са изградени, както е необходимо, за да се сведе до минимум рискът от компрометиране или загуба на КИЕС;

v) въпросите на сигурността, свързани с опазването на КИЕС, да се координират с други компетентни национални органи, включително с органите, посочени в настоящото решение; и

vi) да се дава отговор на съответните заявления за проверки за надеждност, по-специално от всички органи, агенции, структури и операции на Съюза, създадени съгласно дял V, глава 2 от ДЕС, от специалните представители на ЕС (СПЕС) и техните екипи, които прилагат настоящото решение или неговите принципи;

б) гарантират, че техните компетентни органи предоставят информация и експертни становища на правителствата си, а чрез тях и на Съвета, относно естеството на заплахите за сигурността на КИЕС и средствата за защита срещу тях.

Член 17

Комитет по сигурността

1. Създава се Комитет по сигурността. Той разглежда и извършва оценка на всички въпроси на сигурността в обхвата на настоящото решение и прави съответните препоръки до Съвета.

2. Комитетът по сигурността се състои от представители на НОС на държавите членки и на заседанията му присъства представител на Комисията и на ЕСВД. Комитетът се председателства от генералния секретар или от определен от него заместник. Комитетът заседава по указание на Съвета или по искане на генералния секретар или на НОС.

На заседанията могат да бъдат поканени представители на органите, агенциите и структурите на Съюза, които прилагат настоящото решение или неговите принципи, когато се обсъждат засягащи ги въпроси.

3. Комитетът по сигурността организира дейността си по такъв начин, че да може да отправя препоръки в специфични области на сигурността. В зависимост от нуждите той установява експертни подобласти по въпросите на ОИ, както и други експертни подобласти. Комитетът изготвя правила за работа в тези експертни подобласти и получава доклади от експертите за дейността им, включително, ако е уместно, и евентуални препоръки за Съвета.

▼B

Член 18

Замяна на предходни решения

1. С настоящото решение се отменя и заменя Решение 2011/292/ЕС на Съвета ([1]).

2. Цялата КИЕС, класифицирана в съответствие с Решение 2001/264/ЕО на Съвета ([2]) и с Решение 2011/292/ЕС, продължава да бъде защитена съгласно съответните разпоредби от настоящото решение.

Член 19

Влизане в сила

Настоящото решение влиза в сила в деня на публикуването му в *Официален вестник на Европейския съюз.*

([1]) Решение 2011/292/ЕС на Съвета от 31 март 2011 г. относно правилата за сигурност за защита на класифицирана информация на ЕС (ОВ L 141, 27.5.2011 г., стр. 17).

([2]) Решение 2001/264/ЕО на Съвета от 19 март 2001 г. за приемане на разпоредбите относно сигурността на Съвета (ОВ L 101, 11.4.2001 г., стр. 1).

▼B

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ I

Персонална сигурност

ПРИЛОЖЕНИЕ II

Физическа сигурност

ПРИЛОЖЕНИЕ III

Управление на класифицирана информация

ПРИЛОЖЕНИЕ IV

Защита на КИЕС, с която се работи в КИС

ПРИЛОЖЕНИЕ V

Индустриална сигурност

ПРИЛОЖЕНИЕ VI

Обмен на класифицирана информация с трети държави и международни организации

▼B

ПРИЛОЖЕНИЕ I

ПЕРСОНАЛНА СИГУРНОСТ

I. ВЪВЕДЕНИЕ

1. В настоящото приложение се съдържат разпоредбите за изпълнение на член 7. В него се установяват критерии, с които се определя дали на дадено лице, отчитайки неговата лоялност и благонадеждност, може да бъде дадено разрешение за достъп до КИЕС, както и проучвателните и административните процедури, които се следват за тази цел.

II. ПРЕДОСТАВЯНЕ НА ДОСТЪП ДО КИЕС

2. Физическо лице получава достъп до класифицирана информация, след като:

а) бъде установена неговата „необходимост да знае“;

б) бъде информирано за правилата и процедурите за сигурност за защита на КИЕС и приеме своята отговорност за защитата на тази информация; и

в) когато се отнася за информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо:

— получи РДП на съответното ниво или е съответно надлежно оправомощено по силата на изпълняваните от него функции в съответствие с националните законови и подзаконови актове, или

— когато се отнася за длъжностно лице на ГСС, друг служител или командирован национален експерт, получи разрешение за достъп до КИЕС от назначаващия орган на ГСС в съответствие с точки 16—25 до определено ниво и за определен срок.

3. Всяка държава членка и ГСС определят в рамките на своите структури длъжностите, които изискват достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо и за които по тази причина е необходимо разрешение за достъп за съответното ниво.

III. ИЗИСКВАНИЯ ЗА РАЗРЕШЕНИЕ ЗА ДОСТЪП НА ПЕРСОНАЛА

4. След получаване на надлежно разрешено искане националните органи по сигурността или други компетентни национални органи отговарят за осигуряване извършването на проучване за надеждност на свои граждани, които кандидатстват за достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо. Стандартите за проучването са в съответствие с националните законови и подзаконови актове за издаване на РДП или за предоставяне на уверение, за да може лицето да получи разрешение за достъп до КИЕС по целесъобразност.

5. В случай че съответното физическо лице пребивава на територията на друга държава членка или на трета държава, компетентните национални органи се обръщат за съдействие към компетентния орган на държавата по пребиваване в съответствие с националните законови и подзаконови актове. Държавите членки взаимно си съдействат при извършване на проучвания за надеждност в съответствие с националните законови и подзаконови актове.

6. Когато това е допустимо съгласно националните законови и подзаконови актове, националните органи по сигурността или други компетентни национални органи могат да извършат проучване на граждани на други държави, които искат достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо. Стандартите на проучването са в съответствие с националните законови и подзаконови актове.

▼B

Критерии за проучване за надеждност

7. За да получи дадено физическо лице разрешение за достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, неговата лоялност и надеждност се определят посредством проучване за надеждност. Компетентният национален орган прави обща преценка на базата на констатациите от такова проучване за надеждност. Основните критерии, използвани за целта, включват, във възможната според националните законови и подзаконови актове степен, проверка дали въпросното физическо лице:

а) е извършило или е направило опит за извършване на шпионаж, тероризъм, саботаж, държавна измяна или противодържавна дейност, съвместно с друго лице или е помогнало и подбудило друго лице към извършване им;

б) е или е било свързано с шпиони, терористи, саботьори или лица, за които има основателни причини да се подозира, че са такива или че са свързани с представители на организации или чужди държави, включително чужди разузнавателни служби, които могат да застрашат сигурността на Съюза и/или на държавите членки, освен ако подобни връзки не са били разрешени в рамките на официалните му задължения;

в) е или е било член на организация, която с насилствени, подривни или други противозаконни средства се стреми, *inter alia*, към сваляне на правителство на държава членка, промяна на конституционния ѝ ред или промяна на формата или политиките на нейното правителство;

г) е или е било поддръжник на организация, описана в буква в), или е, или е било тясно свързано с членове на такива организации;

д) умишлено е премълчало, представило невярна или подправило важна информация, по-специално свързана със сигурността, или умишлено е излъгало при попълване на въпросника за проучване на надеждността на персонала или по време на събеседването при проучването за надеждност;

е) е осъждано за извършване на престъпление или престъпления;

ж) има доказана зависимост от алкохол, използва незаконни наркотични вещества и/или злоупотребява с разрешени от закона лекарствени средства;

з) има или е имало поведение, което би могло да породи риск от уязвимост при изнудване или натиск;

и) с действия или с думи е демонстрирало неискреност, нелоялност, ненадеждност или че не заслужава доверие;

й) сериозно или многократно е нарушавало правилата за сигурност; или е правило опити да извърши или успешно е извършвало неразрешена дейност по отношение на комуникационни и информационни системи; и

к) може да бъде податливо на натиск (напр. ако има едно или повече гражданства на държави извън ЕС или е във връзка с роднини или близки сътрудници, които могат да бъдат уязвими за чужди разузнавателни служби, терористични групи или други подривни организации, или с физически лица, чиито цели могат да застрашават интересите на Съюза и/или на държавите членки в областта на сигурността).

▼B

8. Когато е уместно и в съответствие с националните законови и подзаконови актове, финансовото и медицинското състояние на лицето също могат да бъдат взети предвид при проучването за надеждност.

9. Когато е уместно и в съответствие с националните законови и подзаконови актове, поведението на съпруга(ата) и обстоятелствата, свързани с него(нея), както и тези на лицето, с което проучваното лице живее на съпружески начала, или на близък член на семейството му също могат да бъдат взети предвид по време на проучването за надеждност.

Изисквания на проучването за надеждност с оглед достъпа до КИЕС

Първоначално издаване на разрешение за достъп

10. Първоначалното разрешение за достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се основава на проучване за надеждност, което обхваща най-малко последните пет години или периода от навършване на 18-годишна възраст на лицето до настоящия момент (което от двете е по-кратко) и включва следното:

а) попълване на национален въпросник за проучване на надеждността на персонала за нивото на КИЕС, за което на лицето може да е необходим достъп; след като бъде попълнен, този въпросник се изпраща на компетентния орган по сигурността;

б) проверка на самоличността/гражданството/националността — проверяват се датата и мястото на раждане на лицето, както и неговата самоличност. Установяват се гражданството и/или националността на лицето в миналото и в настоящия момент; това включва преценка за евентуална уязвимост на натиск от чужди източници, например свързани с предходно местопребиваване или връзки в миналото; и

в) проверка на националните и местните регистри — извършва се проверка на националните регистри по сигурността и централните регистри за съдимост, когато съществуват такива, и/или други подобни правителствени и полицейски регистри. Прави се проверка в регистрите на правоприлагащите органи, които упражняват юрисдикция на мястото, където лицето е пребивавало или работило.

11. Първоначалното разрешение за достъп до информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се основава на проучване, което обхваща най-малко последните десет години или периода от навършване на 18-годишна възраст на лицето до настоящия момент (което от двете е по-кратко). Когато събеседванията се провеждат съгласно буква д), проучванията обхващат най-малко последните седем години или периода след навършване на 18-годишна възраст на лицето, което от двете е по-кратко. В допълнение на критериите, посочени в точка 7 по-горе, се проучват и изложените по-долу елементи, във възможната според националните законови и подзаконови актове степен, преди да бъде дадено разрешение за достъп до информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET; те могат да бъдат проучени и преди предоставяне на РДП с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, когато това се изисква от националните законови и подзаконови актове:

а) финансово състояние — събира се информация относно финансовото положение на физическото лице, за да се направи преценка за евентуална предразположеност към чуждестранен или вътрешен натиск поради сериозни финансови затруднения или за да се разкрие несъответствие между стандарта на живот и доходите на лицето;

▼B

б) образование — събира се информация за проверка на образованието на лицето в училища, университети и други образователни институции, посещавани след навършване на 18-годишна възраст или по време на период, определен за подходящ от водещия проучването орган;

в) трудова заетост — събира се информация относно настоящото и предходни работни места, като се прави справка в регистри по заетостта, доклади за качеството или ефективността на работата на лицето, както и с работодатели или преки ръководители;

г) военна служба — когато е приложимо, се прави проверка на прослуженото време във въоръжените сили и на вида освобождаване от военна служба; и

д) събеседвания — когато това е предвидено и е допустимо по националното право, с физическото лице се провежда събеседване или събеседвания. Провеждат се събеседвания и с лицата, които са в състояние да предоставят безпристрастна оценка на произхода, дейностите, лоялността и надеждността на лицето. Когато в съответствие с националната практика от лицето, което се проучва, се изисква да посочи лица за препоръки, с тези лица се провежда събеседване, освен в случаите, когато съществуват сериозни основания това да не се направи.

12. При нужда и в съответствие с националните законови и подзаконови актове могат да се извършат допълнителни проучвания за разработване на цялата относима информация, налична за лицето, и да се потвърди или обори неблагоприятна информация.

Подновяване на разрешение за достъп

13. След първоначалното предоставяне на разрешение за достъп и при условие че лицето е работило непрекъснато в националната администрация или в ГСС и продължава да се нуждае от достъп до КИЕС, разрешението за достъп се преразглежда с цел подновяване за периоди, които не надвишават пет години за ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET и десет години за ниво на класификация за сигурност SECRET UE/EU SECRET и CONFIDENTIEL UE/EU CONFIDENTIAL, считано от датата на уведомлението за резултатите от последното проучване за надеждност, на което те се основават. Всички проучвания за надеждност за подновяване на разрешение за достъп обхващат периода след предишното такова проучване.

14. За подновяване на разрешение за достъп се проучват посочените в точки 10 и 11 елементи.

15. Исканията за подновяване се отправят своевременно, като се отчита времето, необходимо за проучванията за надеждност. Независимо от това, ако съответният НОС или друг компетентен национален орган е получил съответното искане за подновяване и съответния въпросник за проучване на надеждността на лицето преди изтичане на разрешение за достъп, а необходимото проучване за надеждност все още не е приключило, компетентният национален орган може, когато това е допустимо по националните законови и подзаконови актове, да удължи срока на валидност на съществуващото разрешение за достъп за период до 12 месеца. Ако при изтичането на този допълнителен 12-месечен срок проучването за надеждност все още не е завършило, на лицето се възлагат единствено задачи, за които не се изисква разрешение за достъп.

Процедури за издаване на разрешение в ГСС

16. За длъжностните лица и други служители, работещи в ГСС, органът на ГСС по сигурността изпраща попълнения въпросник за проучване на надеждността на персонала на НОС на държавата членка, чийто гражданин е лицето, с молба да се предприеме проучване за надеждност за нивото на класификация на КИЕС, до което лицето ще има нужда от достъп.

▼B

17. Когато на ГСС стане известна информация от значение за проучването за надеждност на лице, подало искане за разрешение за достъп до КИЕС, ГСС уведомява за това съответния НОС в съответствие с приложимите правила и разпоредби.

18. След приключване на проучването за надеждност съответният НОС уведомява органа по сигурността на ГСС за резултата от това проучване, като използва утвърдения от Комитета по сигурността стандартен образец за кореспонденция.

    а) Когато в резултат от проучването за надеждност се стигне до уверение, че няма неблагоприятни данни, които да поставят под въпрос лоялността и надеждността на лицето, назначаващият орган на ГСС може да предостави разрешение за достъп до КИЕС на съответното ниво за определен срок.

    б) Когато проучването за надеждност не завърши с такова уверение, назначаващият орган на ГСС уведомява съответното лице, което може да поиска да бъде изслушано от назначаващия орган. Назначаващият орган на ГСС може да поиска от компетентния НОС всякакви допълнителни пояснения, които този орган може да предостави в съответствие с националните законови и подзаконови актове. Ако крайният резултат бъде потвърден, не се предоставя разрешение за достъп до КИЕС.

19. Проучването за надеждност заедно с получените резултати се подчиняват на действащите законови и подзаконови актове на съответната държава членка в тази област, включително на актовете, отнасящи се до обжалването. Решенията на назначаващия орган на ГСС подлежат на обжалване в съответствие с Правилника за длъжностните лица на Европейския съюз и Условията за работа на другите служители на Европейския съюз, установени в Регламент (ЕИО, Евратом, ЕОВС) № 259/68 на Съвета [1] („Правилник и условия за работа“).

20. Националните експерти, командировани в ГСС на длъжност, изискваща достъп до КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, преди да поемат функциите си, представят на органа на ГСС по сигурността валидно удостоверение за разрешение за достъп на персонала (УРДП) за достъп до КИЕС, въз основа на което назначаващият орган издава разрешение за достъп до КИЕС.

21. ГСС приема разрешения за достъп до КИЕС, издадени от всяка друга институция, орган или агенция на Съюза, при условие че тези разрешения все още са валидни. Разрешението обхваща всяка задача, възложена на съответното лице в рамките на ГСС. Институцията, органът или агенцията на Съюза, в която лицето започва работа, уведомява съответния НОС за промяната на работодателя.

22. Ако лицето не започне работа в рамките на 12 месеца от съобщаването на резултата от проучването за надеждност на назначаващия орган на ГСС или когато е налице прекъсване от 12 месеца, през които то не е било на работа в ГСС или в националната администрация на държава членка, резултатът се изпраща на съответния национален орган по сигурността за потвърждаване на валидността и целесъобразността му.

23. Когато на ГСС стане известна информация, свързана с риск за сигурността, породен от лице, което разполага с разрешение за достъп до КИЕС, ГСС уведомява за това съответния НОС в съответствие с приложимите правила и разпоредби и може временно да преустанови достъпа до КИЕС или да оттегли разрешението за достъп до КИЕС.

[1] Регламент (ЕИО, Евратом, ЕОВС) № 259/68 на Съвета от 29 февруари 1968 г. за създаване на правилник за длъжностните лица и условия за работа на останалите служители на Европейските общности и за въвеждане на специални мерки, които се прилагат временно за длъжностните лица от Комисията (ОВ L 56, 4.3.1968 г., стр. 1).

▼B

24. Когато НОС уведоми ГСС, че оттегля уверение, дадено в съответствие с точка 18, буква а) за лице, разполагащо с разрешение за достъп до КИЕС, назначаващият орган на ГСС може да отправи искане за всякакъв вид пояснения, които НОС може да предостави съгласно националните законови и подзаконови актове. Ако неблагоприятната информация бъде потвърдена, разрешението се оттегля и лицето се изключва от достъп до КИЕС и от длъжности, където е възможен такъв достъп или където то може да представлява опасност за сигурността.

25. Всяко решение за отнемане или временно преустановяване на разрешение от длъжностно лице или друг служител на ГСС за достъп до КИЕС и, когато това е уместно, основанията за него се съобщават на заинтересованото лице, което може да поиска да бъде изслушано от назначаващия орган. Информацията, предоставена от НОС, се подчинява на действащите законови и подзаконови актове на съответната държава членка в тази област, включително на актовете, отнасящи се до обжалването. Решенията на назначаващия орган на ГСС подлежат на обжалване в съответствие с Правилника и Условията за работа.

Регистри на удостоверения за надеждност и разрешения за достъп

26. Всяка държава членка и съответно ГСС водят регистри на РДП и на предоставените разрешения за достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо. Като минимум регистрите съдържат информация за нивото на КИЕС, до което може да бъде даден достъп на физическото лице, датата на разрешението за достъп и срока му на валидност.

27. Компетентният орган по сигурността може да издаде УРДП, на което са означени нивото на класификация на КИЕС, до което лицето има достъп (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо), срокът на валидност на съответното РДП за достъп до КИЕС или разрешение за достъп до КИЕС и датата на изтичане на валидността на самото удостоверение.

Освобождаване от изискването за РДП

28. Достъпът до КИЕС на лица в държавите членки, които са надлежно оправомощени по силата на изпълняваните от тях функции, се определя в съответствие с националните законови и подзаконови актове; тези лица се информират за задълженията им в областта на сигурността, свързани със защитата на КИЕС.

IV. ОБУЧЕНИЕ И ПОВИШАВАНЕ НА ОСВЕДОМЕНОСТТА ПО ВЪПРОСИТЕ НА СИГУРНОСТТА

29. Всички лица, които притежават удостоверение за надеждност, декларират писмено, че са запознати със задълженията си по отношение на защитата на КИЕС и последиците от компрометиране на КИЕС. Тези писмени декларации се регистрират съответно от държавите членки и ГСС.

30. Всички лица, които имат разрешение за достъп до КИЕС или от които се изисква да работят с КИЕС, получават първоначална информация и биват впоследствие редовно информирани относно заплахите за сигурността и са длъжни незабавно да докладват на съответните органи по сигурността за всеки подход или дейност, които считат за подозрителни или необичайни.

31. Всички лица, които престават да изпълняват задължения, свързани с достъп до КИЕС, биват информирани за задълженията им да продължат да опазват КИЕС, за което при нужда подписват декларация.

V. ИЗВЪНРЕДНИ ОБСТОЯТЕЛСТВА

32. Когато това е допустимо съгласно националните законови и подзаконови актове, разрешение за достъп до национална класифицирана информация, предоставено от компетентен национален орган

▼B

на държава членка, може временно — за периода до издаване на РДП до КИЕС — да дава на национални длъжностни лица достъп до КИЕС на равностойното ниво, посочено в таблицата на съответствието в допълнение Б, когато такъв временен достъп се изисква в интерес на Съюза. Националните органи по сигурността информират Комитета по сигурността, ако националните законови и подзаконови актове не позволяват такъв временен достъп до КИЕС.

33. При неотложни случаи, когато това е надлежно оправдано от интереса на работата, и до завършване на цялостното проучване за надеждност назначаващият орган на ГСС, след консултация с НОС на държавата членка, чийто гражданин е лицето, и в зависимост от резултата от предварителната проверка за удостоверяване, че няма неблагоприятна информация, може да разреши временно на длъжностни лица и други служители на ГСС достъп до КИЕС за изпълнение на конкретни задължения. Временното разрешение важи за период, който не надвишава шест месеца и не дава право на достъп до информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET. Всички лица, които притежават временно разрешение, декларират писмено, че са запознати със задълженията си по отношение на защитата на КИЕС и последиците от компрометирането на КИЕС. ГСС регистрира тези писмени декларации.

34. Когато предстои дадено лице да бъде назначено на длъжност, изискваща разрешение за достъп, една степен по-високо от притежаваното от него, лицето може да бъде назначено временно, при условие че:

а) належащата необходимост от достъп до КИЕС на по-високо ниво бъде обоснована писмено от ръководителя на лицето;

б) достъпът е ограничен до конкретни елементи от КИЕС, свързани с длъжността;

в) лицето разполага с валидно РДП или разрешение за достъп до КИЕС;

г) са предприети действия за получаване на РДП за нивото, необходимо за тази длъжност;

д) проверките, извършени от компетентния орган, са дали удовлетворителен отговор, че лицето не е нарушавало сериозно или многократно разпоредбите по сигурността;

е) назначаването на лицето е одобрено от компетентния орган; и

ж) това изключение, включително описание на информацията, до която е предоставен достъп, бъде отразено в отговарящата регистратура или в отговарящата подчинена регистратура.

35. Посочената по-горе процедура се използва за еднократен достъп до КИЕС на ниво с една степен по-високо от това, до което лицето е получило достъп. До тази процедура не се прибягва редовно.

36. В крайно изключителни обстоятелства, като мисии във враждебна среда или в периоди на нарастващо международно напрежение, когато това се налага за предприемане на неотложни мерки, особено с цел спасяване на човешки живот, държавите членки и генералният секретар могат, по възможност в писмена форма, да предоставят достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET на лица, които не разполагат с необходимото разрешение за достъп, при условие че такова разрешение е абсолютно необходимо и липсват основателни съмнения относно лоялността и надеждността на съответното лице. Даденото разрешение се регистрира, като се описва информацията, до която е одобрен достъп.

▼B

37. При информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET извънредният достъп се ограничава до граждани на Съюза, на които е разрешен достъп до информация с национално ниво на класификация за сигурност, равностойно на TRÉS SECRET UE/EU TOP SECRET, или до информация с ниво на класификация за сигурност SECRET UE/EU SECRET.

38. Комитетът по сигурността се информира за случаите, в които се прибягва до процедурата, установена в точки 36 и 37.

39. Когато в националните законови и подзаконови актове на дадена държава членка се предвиждат по-строги правила по отношение на временни разрешения и еднократен или извънреден достъп на лица до класифицирана информация, предвидените в настоящия раздел процедури се прилагат единствено в рамките на ограниченията, посочени в съответните национални законови и подзаконови актове.

40. Комитетът по сигурността получава годишен доклад относно използването на процедурите, установени в настоящия раздел.

VI. УЧАСТИЕ В ЗАСЕДАНИЯ НА СЪВЕТА

41. При условията на точка 28 лица, на които е възложено да участват в заседания на Съвета или на неговите подготвителни органи, на които се обсъжда информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, се допускат до участие само след потвърждаване на статуса им на лица с разрешение за достъп. За участниците се изпраща УРДП или друго доказателство за разрешение за достъп от съответните органи до службата на ГСС по сигурността или, по изключение, УРД се представя лично от самия участник. Когато е приложимо, може да се използва единен списък с имена, който да предоставя съответно доказателство за разрешение за достъп.

42. Когато от съображения за сигурност бъде оттеглено РДП до КИЕС на лице, чиито задължения изискват присъствието му на заседания на Съвета или на подготвителните органи на Съвета, компетентният орган уведомява ГСС за това.

VII. ПОТЕНЦИАЛЕН ДОСТЪП ДО КИЕС

43. Куриерите, охранителите и придружителите преминават през проучване за надеждност на съответното ниво или се проучват по други начини в съответствие с националните законови и подзаконови актове, биват инструктирани относно процедурите за сигурност за защита на КИЕС и получават указания за задълженията им във връзка със защитата на поверената им КИЕС.

▼B

ПРИЛОЖЕНИЕ II

ФИЗИЧЕСКА СИГУРНОСТ

I. ВЪВЕДЕНИЕ

1. В настоящото приложение се съдържат разпоредбите за изпълнение на член 8. В него се установяват минималните изисквания за физическа защита на помещения, сгради, офиси, зали и други зони, в които се работи с КИЕС и се съхранява такава, включително на зоните, в които се помещават КИС.

2. Мерките за физическа сигурност са предназначени да предотвратяват неразрешен достъп до КИЕС, като:

а) гарантират, че работата с КИЕС и нейното съхранение се извършват по подходящ начин;

б) дават възможност за разграничаване на служителите по отношение на достъпа до КИЕС на основание „необходимост да се знае“ и евентуално според вида на разрешението им за достъп;

в) възпират, препятстват и разкриват неразрешени действия; и

г) предотвратяват или забавят тайно или насилствено проникване на нарушители.

II. ИЗИСКВАНИЯ И МЕРКИ ЗА ФИЗИЧЕСКА СИГУРНОСТ

3. Мерките за физическа сигурност се подбират въз основа на извършена от компетентните органи оценка на заплахата. ГСС и държавите членки прилагат процес на управление на риска за защита на КИЕС в техните обекти, за да гарантират, че се осигурява ниво на физическа защита, което е съизмеримо с оценката на риска. В процеса на управление на риска се вземат предвид всички необходими фактори, и по-специално:

а) нивото на класификация на КИЕС;

б) формата и обемът на КИЕС, като се отчита, че за големи количества или масиви от КИЕС може да се наложи прилагане на по-строги защитни мерки;

в) заобикалящата среда и конструкцията на сградите или зоните, в които се съхранява КИЕС; и

г) оценката на заплахата, произтичаща от действия на разузнавателни служби, насочени срещу Съюза или държавите членки, както и от саботажи, терористична, подривна или друг вид престъпна дейност.

4. Компетентният орган по сигурността, като прилага концепцията за защита в дълбочина, определя необходимото съчетание от мерки за физическа сигурност, които да се приложат. То може да включва една или повече от следните мерки:

а) бариера по периметъра: физическа бариера, която отбранява границите на зоната, изискваща защита;

б) системи против проникване (СПП): една система против проникване може да се използва за повишаване на нивото на сигурност, което дава бариерата по периметъра, или да се използва в помещения и сгради вместо или за подпомагане на служителите за охрана;

▼B

в) контрол на достъпа: контрол на достъпа може да се упражнява по отношение на отделен обект, сграда или сгради в рамките на обекта, или по отношение на зони или помещения в рамките на дадена сграда. Контролът може да бъде електронен или електромеханичен, да се извършва от служители за охрана и/или пропускателен пункт, и/или с други физически способи;

г) служители за охрана: квалифицирани служители за охрана, при съответния надзор, а при необходимост и надлежно проучени за надеждност, могат да бъдат наемани, *inter alia*, с цел възпиране на лица, планиращи тайно проникване;

д) вътрешна система за видеонаблюдение (ВСВН): ВСВН може да се използва от служителите за охрана за установяване на инциденти и сигнали, постъпили от СПП, при големи обекти или по периметъра;

е) защитно осветление: защитно осветление може да се използва за възпиране на потенциални нарушители, както и за осигуряване на необходимото осветление за ефективно наблюдение пряко от служителите за охрана или непряко, с помощта на вътрешна система за видеонаблюдение; и

ж) всякакви други подходящи физически мерки, предназначени да възпрат или открият неразрешен достъп, или да предотвратят загуба или повреждане на КИЕС.

5. Компетентните органи по сигурността могат да имат разрешение да извършват претърсвания на влизащите или излизащите, което действа като възпиращ фактор по отношение на неразрешено внасяне на материали или изнасяне на КИЕС от дадено помещение или сграда.

6. Когато съществува риск от пропуски, дори случайни, по отношение на КИЕС, се вземат необходимите мерки за неутрализиране на риска.

7. За нови структури изискванията за физическа сигурност и техните функционални спецификации се определят като част от планирането и разработката на тези структури. За съществуващи структури изискванията за физическа сигурност се осъществяват в максималната възможна степен.

III. ОБОРУДВАНЕ ЗА ФИЗИЧЕСКА ЗАЩИТА НА КИЕС

8. При придобиване на оборудване (като сейфове, машини за унищожаване на хартиени документи, ключалки за врати, електронни системи за контрол на достъпа, системи против проникване, алармени системи) за физическа защита на КИЕС компетентният орган по сигурността гарантира, че оборудването отговаря на одобрените технически стандарти и минимални изисквания.

9. Техническите спецификации на оборудването, което се използва за физическа защита на КИЕС, се посочват в насоките за сигурност, които се одобряват от Комитета по сигурността.

10. Системите за сигурност се проверяват периодично, като оборудването подлежи на редовна поддръжка. Поддръжката е съобразена с резултатите от проверките, за да се гарантира постоянно оптимално функциониране на оборудването.

11. При всяка проверка се прави преоценка на ефективността на отделните мерки и на цялата система за сигурност.

IV. ФИЗИЧЕСКИ ЗАЩИТЕНИ ЗОНИ

12. За физическа защита на КИЕС се създават два вида физически защитени зони или националните им еквиваленти:

▼B

а) административни зони; и

б) зони за сигурност (включително технически зони за сигурност).

В настоящото решение всяко позоваване на административни зони и зони за сигурност, включително технически зони за сигурност, се разбира и като позоваване на техните национални еквиваленти.

13. Компетентният орган по сигурността определя дали дадена зона отговаря на изискванията за административна зона, зона за сигурност или техническа зона за сигурност.

14. За административните зони:

а) се определя видимо очертан периметър, който да позволява проверка на лицата и при възможност — на превозните средства;

б) непридружен достъп се разрешава само на лица, надлежно оправомощени от компетентния орган; и

в) всички останали лица се придружават по всяко време или подлежат на равностойни проверки.

15. За зоните за сигурност:

а) се определя видимо очертан и защитен периметър, чрез който се контролират всички влизания и излизания чрез пропуски или система за индивидуално разпознаване;

б) достъп без придружител се предоставя само на лица, които имат разрешение за достъп и са конкретно оправомощени да влизат в зоната на основание „необходимост да се знае“; и

в) всички останали лица се придружават по всяко време или подлежат на равностойни проверки.

16. Когато влизането в зона за сигурност представлява на практика пряк достъп до класифицираната информация в нея, се прилагат следните допълнителни изисквания:

а) обозначава се ясно най-високото ниво на класификация за сигурност на информацията, която обикновено се намира в зоната;

б) необходимо е всички посетители да имат специално разрешение за влизане в зоната, те се придружават непрекъснато и са преминали през съответното проучване за надеждност, освен ако не са взети мерки да се гарантира, че достъпът до КИЕС е невъзможен.

17. Зони за сигурност, защитени срещу подслушване, се определят за технически зони за сигурност. Прилагат се следните допълнителни изисквания:

а) такива зони се оборудват със системи против проникване, стоят заключени, когато не се ползват, и са под охрана, когато се ползват. Всички ключове се контролират в съответствие с раздел VI;

б) всички лица и материали, които влизат в тези зони, се подлагат на контрол;

▼B

в) зоните се проверяват редовно физически и/или технически съгласно изискванията на компетентния орган по сигурността. Такива проверки се извършват и след всяко неразрешено влизане или при подозрение за такова влизане; и

г) в такива зони няма неразрешени линии за комуникации, неразрешени телефони или други неразрешени комуникационни средства и електрическо или електронно оборудване.

18. Независимо от точка 17, буква г), преди да се използва в зони, където се провеждат заседания или се извършва дейност, включваща работа с информация с ниво на класификация за сигурност SECRET UE/EU SECRET и по-високо, и където степента на заплаха за КИЕС се оценява като висока, комуникационните средства и електрическото или електронното оборудване най-напред се проверяват от компетентния орган по сигурността, за да се гарантира, че с това оборудване не може да се предаде, неволно или неправомерно, разбираема информация отвъд периметъра на зоната за сигурност.

19. Зоните за сигурност, в които няма денонощно присъствие на дежурен персонал, се проверяват, когато това е уместно, в края на установеното работно време и на произволни интервали извън установеното работно време, освен ако не е инсталирана система против проникване.

20. Зони за сигурност и технически зони за сигурност могат да бъдат временно създадени в рамките на административна зона за целите на класифицирано заседание или други подобни цели.

21. За всяка зона за сигурност се изготвят оперативни процедури за сигурност, в които се определят:

а) нивото на КИЕС, с която може да се работи в зоната и която може да се съхранява там;

б) мерките за наблюдение и защита, които да се поддържат;

в) лицата, които имат право на непридружен достъп до зоната на основание „необходимост да се знае“ и разрешение за достъп;

г) ако е уместно, процедури за придружаване или за защита на КИЕС, когато се разрешава достъп на други лица до зоната; и

д) всякакви други подходящи мерки и процедури.

22. В рамките на зоните за сигурност се изграждат блиндирани помещения. Стените, подовете, таваните, прозорците и вратите с ключалки се одобряват от компетентния орган по сигурността и осигуряват защита, равностойна на тази на сейф от категорията, одобрена за съхранение на КИЕС със същото ниво на класификация за сигурност.

V. ФИЗИЧЕСКИ ЗАЩИТНИ МЕРКИ ЗА РАБОТА С КИЕС И НЕЙНОТО СЪХРАНЕНИЕ

23. С КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED може да се работи:

а) в зона за сигурност;

б) в административна зона, при условие че КИЕС е защитена срещу достъп от страна на неоправомощени лица; или

▼B

в) извън зона за сигурност или административна зона, при условие че притежателят пренася КИЕС в съответствие с точки 28—41 от приложение III и се е ангажирал да спазва компенсаторните мерки, установени в инструкциите за сигурност, издадени от компетентния орган по сигурността с цел да се гарантира, че КИЕС е защитена срещу достъп от страна на неоправомощени лица.

24. КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED се съхранява в подходящи заключващи се офис мебели в административна зона или в зона за сигурност. Тя може да се съхранява временно извън зона за сигурност или административна зона, при условие че притежателят се е ангажирал да спазва компенсаторните мерки, установени в инструкциите за сигурност, издадени от компетентния орган по сигурността.

25. С КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET може да се работи:

а) в зона за сигурност;

б) в административна зона, при условие че КИЕС е защитена срещу достъп от страна на неоправомощени лица; или

в) извън зона за сигурност или административна зона, при условие че притежателят:

i) пренася КИЕС в съответствие с точки 28—41 от приложение III;

ii) се е ангажирал да спазва компенсаторните мерки, установени в инструкциите за сигурност, издадени от компетентния орган по сигурността с цел да се гарантира, че КИЕС е защитена срещу достъп от страна на неоправомощени лица;

iii) непрекъснато контролира лично КИЕС; и

iv) в случай че документите са на хартиен носител, е уведомил за това съответната регистратура.

26. КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се съхранява в зона за сигурност в сейф или в блиндирано помещение.

27. С КИЕС с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се работи в зона за сигурност.

28. КИЕС с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се съхранява в зона за сигурност при някое от следните условия:

а) в сейф, съобразно точка 8, с поне една от следните допълнителни мерки за контрол:

i) постоянна защита или проверки от служители с разрешение за достъп на персонала или от дежурен персонал;

ii) одобрена система против проникване, в съчетание със служители за охрана и реагиране;

б) в блиндирани помещения, оборудвани със системи против проникване, в съчетание със служители за охрана и реагиране.

▼B

29. Правилата, уреждащи преноса на КИЕС извън физически защитените зони, се съдържат в приложение III.

VI. КОНТРОЛ НА КЛЮЧОВЕТЕ И КОМБИНАЦИИТЕ, ИЗПОЛЗВАНИ ЗА ЗАЩИТА НА КИЕС

30. Компетентният орган по сигурността определя процедурите за управление на ключовете и шифровите комбинации за офисите, помещенията, блиндираните помещения и сейфовете. Тези процедури осигуряват защита срещу неразрешен достъп.

31. Шифровите комбинации се запаметяват от възможно най-малък брой лица на основание „необходимост да се знае“. Шифровите комбинации за сейфовете и блиндираните помещения, в които се съхранява КИЕС, се променят:

а) при получаване на нов сейф;

б) винаги когато има смяна на служител, на когото е известна комбинацията;

в) в случай на компрометиране или подозрение за компрометиране на информация;

г) когато дадена ключалка е преминала през поддръжка или ремонт; и

д) най-малко на всеки 12 месеца.

▼B

ПРИЛОЖЕНИЕ III

УПРАВЛЕНИЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

I. ВЪВЕДЕНИЕ

1. В настоящото приложение се съдържат разпоредбите за изпълнение на член 9. В него се установяват административните мерки за контрол на КИЕС през жизнения ѝ цикъл с цел да се съдейства за възпиране и разкриване на умишлено или случайно компрометиране или загуба на такава информация.

II. УПРАВЛЕНИЕ НА КЛАСИФИКАЦИЯТА

Класификация и обозначения

2. Информацията се класифицира, когато е необходимо да бъде защитена от съображения за поверителност.

3. Създателят на КИЕС отговаря за определянето на нивото на класификацията за сигурност, в съответствие със съответните насоки за класификация, както и за първоначалното разпространение на информацията.

4. Нивото на класификация на КИЕС се определя в съответствие с член 2, параграф 2 и при спазване на политиката за сигурност, която се одобрява в съответствие с член 3, параграф 3.

5. Класификацията за сигурност се посочва ясно и точно, независимо дали КИЕС е на хартия, в устна, електронна или друга форма.

6. Отделни части от даден документ (т.е. страници, параграфи, раздели, приложения, допълнения, добавки и притурки) може да изискват различно ниво на класификация за сигурност, за което се поставя съответният гриф, включително когато се съхраняват в електронен вид.

7. Нивото, на което се класифицира даден документ или файл, е не по-ниско от най-високото ниво на класификация за сигурност на негов елемент. Когато се обединява информация от различни източници, се прави преглед на окончателния продукт, за да се определи цялостното ниво на класификация за сигурност, тъй като може да е необходимо той да бъде с по-високо ниво на класификация от това на съставните му части.

8. Доколкото е възможно, документите, съдържащи части с различни нива на класификация, се структурират така, че частите с различни нива на класификация да могат лесно да се идентифицират и отделят при необходимост.

9. Класификацията на писмо или записка, включващи приложения, съответства на най-високата степен на класификация на тези приложения. Създателят ясно обозначава нивото на класификация на основния документ без приложенията, като използва подходящ гриф, например:

CONFIDENTIEL UE/EU CONFIDENTIAL

Без приложение(я) RESTREINT UE/EU RESTRICTED

Обозначения

10. В допълнение към един от грифовете за сигурност, посочени в член 2, параграф 2, КИЕС може да носи допълнително обозначение, като:

а) знак за идентифициране на създателя на информацията;

б) предупредително обозначение, кодови думи или акроними, уточняващи областта, до която се отнася документът, конкретното разпределение на документа на основание „необходимост да се знае“ или ограниченията за ползването му;

в) обозначение, уточняващо условията за предоставяне; или

▼B

г) когато е приложимо, датата или конкретното събитие, след които нивото на класификация може да бъде понижено или премахнато.

Съкратено обозначаване на класификацията

11. За обозначаване на нивото на класификация на отделни параграфи от текста могат да се използват стандартни съкращения на нивата на класификация. Пълното название на грифовете за сигурност не се заменя със съкратени обозначения.

12. В класифицирани документи на ЕС за обозначаване на нивото на класификация на раздели или части от текст, по-малки от една страница, могат да се използват следните стандартни съкращения:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Създаване на КИЕС

13. При създаване на класифициран документ на ЕС:

а) върху всяка страница се отбелязва ясно нивото на класификация;

б) всяка страница се номерира;

в) върху документа се отбелязват регистрационният му номер и за какво се отнася, които сами по себе си не представляват класифицирана информация, освен ако не са обозначени като такава;

г) върху документа се поставя дата; и

д) на всяка страница на документи с ниво на класификация за сигурност SECRET UE/EU SECRET и по-високо се обозначава номерът на копието, ако документите се разпространяват в няколко екземпляра.

14. Когато не е възможно да се приложи точка 13 към КИЕС, се вземат други подходящи мерки в съответствие с насоките за сигурност, които се определят съгласно член 6, параграф 2.

Понижаване нивото на класификация и декласификация на КИЕС

15. При създаване на информацията създателят обозначава, когато е възможно, и особено за информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, дали нивото на класификация на КИЕС може да бъде понижено или класификацията може да бъде премахната на определена дата или след настъпване на определено събитие.

16. ГСС прави редовен преглед на КИЕС, с която разполага, за да установи дали нивото на класификация продължава да е приложимо. ГСС установява система за преразглеждане на нивото на класификация на КИЕС, чийто създател е той, не по-рядко от веднъж на пет години. Такъв преглед не се налага, ако от самото начало създателят е посочил, че нивото на класификация на информацията ще бъде автоматично понижено или че класификацията ще бъде премахната и че информацията носи съответното обозначение.

III. РЕГИСТРАЦИЯ НА КИЕС ЗА ЦЕЛИТЕ НА СИГУРНОСТТА

17. За всяка организационна единица в рамките на ГСС и в националните администрации на държавите членки, в която се работи с КИЕС, се определя отговаряща регистратура, за да гарантира, че с КИЕС се работи в съответствие с настоящото решение. Регистратурите се обособяват като зони за сигурност съгласно посоченото в приложение II.

▼B

18. За целите на настоящото решение регистрация за целите на сигурността („регистрация“) означава прилагането на процедури за отбелязване на жизнения цикъл на материалите, включително тяхното разпространение и унищожаване.

19. Всички материали с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и по-високо се регистрират в определени за целта регистратури при постъпването им в дадена организационна единица и при излизането им от нея.

20. Централната регистратура в ГСС поддържа регистри на цялата класифицирана информация, която се предоставя от Съвета и ГСС на трети държави и международни организации, както и за цялата класифицирана информация, която се получава от трети държави или международни организации.

21. По отношение на КИС процедурите за регистрация могат да се изпълнят като процес в рамките на самата КИС.

22. Съветът одобрява политика за сигурност при регистриране на КИЕС за целите на сигурността.

Регистратури за информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET

23. В държавите членки и в ГСС се определя регистратура, която да играе ролята на централен орган за получаване и изпращане на информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET. При необходимост могат да се определят и подчинени регистратури, в които да се работи с такава информация с цел регистрация.

24. Тези подчинени регистратури не могат да предават документи с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET пряко на други регистратури, подчинени на същата централна регистратура TRÉS SECRET UE/EU TOP SECRET, или на външни получатели без изричното писмено одобрение на последната.

IV. КОПИРАНЕ И ПРЕВОД НА КЛАСИФИЦИРАНИ ДОКУМЕНТИ НА ЕС

25. Документите с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET не се копират или превеждат без предварителното писмено съгласие на създателя.

26. Когато създателят на документи с ниво на класификация за сигурност SECRET UE/EU SECRET и по-ниско не е поставил предупредителни обозначения за тяхното копиране или превод, документите могат да бъдат копирани или превеждани по указание на притежателя.

27. Мерките за сигурност, приложими към оригиналния документ, се прилагат и за неговите копия и преводи.

V. ПРЕНОС НА КИЕС

28. Преносът на КИЕС подлежи на защитните мерки, уредени в точки 30—41. Когато КИЕС се пренася на електронен носител и независимо от разпоредбите на член 9, параграф 4, изложените по-долу защитни мерки могат да бъдат допълнени с подходящи технически контрамерки, предписани от компетентния орган по сигурността, така че да се сведе до минимум рискът тя да бъде загубена или компрометирана.

29. Компетентните органи по сигурността в ГСС и в държавите членки издават инструкции за преноса на КИЕС в съответствие с настоящото решение.

В рамките на отделна сграда или самостоятелна група от сгради

30. В рамките на отделна сграда или самостоятелна група от сгради КИЕС се покрива при пренасяне, така че да не се вижда нейното съдържание.

▼B

31. В рамките на отделна сграда или самостоятелна група от сгради информацията с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се пренася в защитен плик, на който е обозначено само името на получателя.

В рамките на Съюза

32. Когато се пренася между сгради или обекти в рамките на Съюза, КИЕС се опакова по такъв начин, че да е защитена от неразрешено разкриване.

33. Преносът на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET в рамките на Съюза се извършва по един от следните начини:

а) с военен, правителствен или дипломатически куриер, в зависимост от случая;

б) на ръка, при положение че:

i) КИЕС не напуска приносителя, освен ако не се съхранява в съответствие с изискванията, посочени в приложение II;

ii) КИЕС не се отваря по пътя, нито се чете на обществени места;

iii) лицата биват информирани за отговорностите им по отношение на сигурността; и

iv) когато е необходимо, на лицата се предоставя удостоверение за куриер;

в) пощенски услуги или платени куриерски услуги, при положение че:

i) те са одобрени от съответния НОС в съответствие с националните законови и подзаконови актове; и

ii) те прилагат подходящи защитни мерки в съответствие с минималните изисквания, които се определят в насоките за сигурност съгласно член 6, параграф 2.

В случай на пренос от една държава членка към друга разпоредбите на буква в) се ограничават до информация с ниво на класификация за сигурност до CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED може също да се пренася чрез пощенски служби или платени куриерски услуги. За преноса на такава информация не се изисква удостоверение за куриер.

35. Материали с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET (например оборудване или машини), които не могат да бъдат пренесени по посочените в точка 33 начини, се пренасят като товар от транспортни дружества в съответствие с приложение V.

36. Преносът на информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET между сгради и обекти в рамките на Съюза се извършва с военен, правителствен или дипломатически куриер, в зависимост от случая.

От територията на Съюза до територията на трета държава

37. Когато се пренася от територията на Съюза до територията на трета държава, КИЕС се опакова по такъв начин, че да е защитена от неразрешено разкриване

▼B

38. Преносът на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET от територията на Съюза до територията на трета държава се извършва по един от следните начини:

а) с военен или дипломатически куриер;

б) на ръка, при положение че:

i) върху пакета е поставен официален печат или опаковката е направена по начин, указващ, че се касае за официална пратка, която не следва да бъде подлагана на митнически проверки или проверки за сигурност;

ii) лицата са снабдени с удостоверение за куриер, в което е идентифициран пакетът и което съдържа разрешение да го пренасят;

iii) КИЕС не напуска приносителя, освен ако не се съхранява в съответствие с изискванията, посочени в приложение II;

iv) КИЕС не се отваря по пътя, нито се чете на обществени места; и

v) лицата биват информирани за отговорностите им по отношение на сигурността.

39. При пренос на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, предоставена от Съюза на трета държава или международна организация, се спазват съответните разпоредби на споразумение за сигурност на информацията или на административна договореност в съответствие с член 13, параграф 2, буква а) или б).

40. Информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED може също да се пренася чрез пощенски служби или платени куриерски услуги.

41. Преносът на информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET от територията на Съюза до територията на трета държава се извършва с военен или дипломатически куриер.

VI. УНИЩОЖАВАНЕ НА КИЕС

42. Класифицирани документи на ЕС, които вече не са необходими, могат да бъдат унищожени, при условие че не се засягат съответните правила и разпоредби за архивиране.

43. Документи, подлежащи на регистрация в съответствие с член 9, параграф 2, се унищожават от отговарящата за тях регистратурата по указание на притежателя или на компетентен орган. Регистрите и друга регистрационна информация се актуализират съответно.

44. Унищожаването на документи с ниво на класификация за сигурност SECRET UE/EU SECRET или TRÉS SECRET UE/EU TOP SECRET се извършва в присъствието на свидетел, който притежава разрешение за достъп до ниво на класификация за сигурност най-малко на нивото на документа, който се унищожава.

45. Регистраторът и свидетелят, когато се изисква присъствие на такъв, подписват удостоверение за унищожаване, което се завежда в регистратурата. Удостоверенията за унищожаване на документи с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се съхраняват в регистратурата за срок от най-малко 10 години, а на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET — за срок от най-малко пет години.

46. Класифицирани документи, включително документи с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, се унищожават по методи, отговарящи на съответните стандарти на Съюза или равностойни на тях стандарти, или по методи, одобрени

▼B

от държавите членки в съответствие с националните технически стандарти, така че да се предотврати цялостното им или частичното им възстановяване.

47. Унищожаването на компютърните средства за съхранение на КИЕС се извършва в съответствие с точка 37 от приложение IV.

48. При извънредна ситуация и наличие на непосредствен риск от нерегламентирано разкриване КИЕС се унищожава от притежателя ѝ по начин, който прави невъзможно цялостното или частичното възстановяване на информацията. Създателят на информацията и регистърът, от който е получена информацията, биват информирани за извънредната ситуация, наложила унищожаването на КИЕС.

VII. ПОСЕЩЕНИЯ ЗА ОЦЕНКА

49. Понятието „посещение за оценка“ се използва по-нататък в текста за обозначаване на всички:

а) проверки или посещения за оценка в съответствие с член 9, параграф 3 и член 16, параграф 2, букви д), е) и ж); или

б) посещения за оценка в съответствие с член 13, параграф 5,

с цел да се прецени ефективността на прилаганите мерки за защита на КИЕС.

50. Посещенията за оценка се извършват, *inter alia*, с цел:

а) да се гарантира спазването на изискваните минимални стандарти за защита на КИЕС, установени в настоящото решение;

б) да се подчертае значението на сигурността и ефективното управление на риска в рамките на проверяваните единици;

в) да се препоръчат мерки за противодействие с цел намаляване на конкретните последствия при загуба на поверителност, интегритет или наличност на класифицирана информация; и

г) да се окаже подкрепа за текущите образователни и информационни програми на органите по сигурността.

51. Преди изтичането на всяка календарна година Съветът приема програма за посещения за оценка за следващата година, както е предвидено в член 16, параграф 1, буква в). Точната дата на всяко посещение за оценка се определя по споразумение със съответния орган или агенция на Съюза, държава членка, трета държава или международна организация.

Извършване на посещенията за оценка

52. Посещенията за оценка се извършват с цел проверка на съответните правила, разпоредби и процедури на посетената организационна единица и проверки за установяване дали практиките на тази единица съответстват на основните принципи и на минималните стандарти, установени в настоящото решение и в разпоредбите, уреждащи обмена на класифицирана информация с тази единица.

53. Посещенията за оценка се извършват на два етапа. Преди самото посещение се провежда подготвително заседание, при необходимост с участието на съответната единица. След това подготвително заседание екипът за оценка изготвя подробна програма за посещението за оценка, която обхваща всички области на сигурността и е съгласувана с посочената единица. Екипът за посещението за оценка следва да получи достъп до всички помещения, в които се работи с КИЕС, и по-специално до регистратурите и точките за достъп до КИС.

54. Посещенията за оценка в националните администрации на държавите членки, в трети държави и международни организации се извършват при пълно сътрудничество от страна на служителите на посетената структура, трета държава или международна организация.

▼B

55. Посещенията за оценка в органи, агенции и структури на Съюза, които прилагат настоящото решение или неговите принципи, се извършват със съдействието на експерти от НОС на държавата членка, на чиято територия са разположени органът или агенцията.

56. При извършване на посещения за оценка в органи, агенции и структури на Съюза, които прилагат настоящото решение или неговите принципи, и в трети държави и международни организации може да бъде отправено искане за съдействие и участие на експерти от националния орган по сигурността, в съответствие с подробни договорености, по които Комитетът по сигурността постига съгласие.

Доклади

57. При приключване на посещението за оценка основните заключения и препоръки се представят на посетената структура. Впоследствие се изготвя доклад за посещението за оценка. Когато се предлагат коригиращи действия и се отправят препоръки, в доклада се включват достатъчно подробности в подкрепа на достигнатите заключения. Докладът се изпраща на съответния орган на посетената структура.

58. При посещения за оценка, извършени в националните администрации на държавите членки:

а) проектът на доклада за посещението за оценка се изпраща на съответния национален орган по сигурността, за да се удостовери фактическата му точност, както и че не съдържа информация с ниво на класификация за сигурност, по-високо от RESTREINT UE/EU RESTRICTED; и

б) докладите за оценка се изпращат до Комитета по сигурността, освен ако съответният НОС на държавата членка не поиска те да не се разпространяват. Докладът получава ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED.

Под ръководството на органа по сигурността на ГСС (службата по сигурността на ГСС) се изготвят редовно доклади, в които се посочват изводите от посещенията за оценка, извършени в държавите членки през даден период и разгледани от Комитета по сигурността.

59. При посещения за оценка в трети държави и в международни организации докладът се изпраща на Комитета по сигурността. Докладът получава ниво на сигурност най-малко RESTREINT UE/EU RESTRICTED. Всички коригиращи мерки се проверяват чрез последващо посещение и се докладват на Комитета по сигурността.

60. При посещения за оценка в органи, агенции и структури на Съюза, които прилагат настоящото решение или неговите принципи, докладът за посещението за оценка се изпраща на Комитета по сигурността. Проектът на доклада за посещението за оценка се изпраща на съответната агенция или орган, за да се удостовери фактическата му точност, както и че не съдържа информация с ниво на класификация за сигурност, по-високо от RESTREINT UE/EU RESTRICTED. Всички коригиращи мерки се проверяват чрез последващо посещение и се докладват на Комитета по сигурността.

61. Органът на ГСС по сигурността извършва редовни проверки на организационните единици в ГСС за целите, посочени в точка 50.

Контролен списък

62. Органът по сигурността на ГСС (службата по сигурността на ГСС) изготвя и актуализира контролен списък, който се попълва по време на посещението за оценка. Контролният списък се изпраща на Комитета по сигурността.

63. Предоставя се необходимата за попълване на контролния списък информация, особено по време на посещението от службите за управление на сигурността на проверяваната единица. След като бъдат дадени подробни отговори на въпросите от контролния списък, той се класифицира по споразумение с проверяваната структура. Той не представлява част от доклада за проверката.

▼B

ПРИЛОЖЕНИЕ IV

ЗАЩИТА НА КИЕС, С КОЯТО СЕ РАБОТИ В КИС

I. ВЪВЕДЕНИЕ

1. В настоящото приложение се съдържат разпоредбите за изпълнение на член 10.

2. Следните понятия и характеристики на ОИ имат основно значение за сигурността и правилното протичане на операциите в КИС:

Автентичност:	гаранцията, че информацията е истинска и произтича от bona fide източници.
Достъпност:	характеристиката на информацията да е достъпна и използваема при поискване от оправомощена единица.
Поверителност:	характеристиката, че информацията не е разкрита на неоправомощени лица, единици или процеси.
Интегритет:	характеристиката, че информацията и активите са запазили точността и пълнотата си.
Невъзможност за отказ:	способността да се докаже, че дадено действие или събитие действително е настъпило, така че това действие или събитие да не може впоследствие да бъде отречено.

II. ПРИНЦИПИ НА ОСИГУРЕНОСТТА НА ИНФОРМАЦИЯТА

3. Установените по-долу разпоредби съставляват основните параметри за сигурността на всяка КИС, в която се работи с класифицирана информация на ЕС. Подробните изисквания за изпълнение на тези разпоредби се определят в политиките и насоките за сигурност относно осигуреността на информацията.

Управление на риска за сигурността

4. Управлението на риска за сигурността е неразделна част от определянето, разработването, функционирането и поддръжката на КИС. Управлението на риска (оценка, третиране, приемане и съобщаване) се осъществява съвместно, като повтарящ се процес, от представители на собствениците на системата, органите по проекта, оперативните органи и органите за одобрение на сигурността чрез използване на доказан, прозрачен и напълно разбираем процес на оценка на риска. Обхватът на КИС и нейните активи се определят ясно в началото на процеса на оценка на риска.

5. Компетентните органи правят преглед на потенциалните заплахи за КИС и поддържат актуализирани и точни оценки на заплахите, които отразяват състоянието на оперативната среда към дадения момент. Те постоянно актуализират своите познания по въпросите, свързани с уязвимите места, и периодично правят преглед на оценката на уязвимостта в отговор на променящата се информационно-технологична среда.

6. Целта на третирането на риска за сигурността е да се приложи съвкупност от мерки за сигурност, които да доведат до задоволителен баланс между изискванията на ползвателите, разходите и остатъчния риск за сигурността.

7. Специфичните изисквания, мащаб и степен на задълбоченост, определени от съответния ОАС за акредитация на КИС, съответстват на оценката на риска, като се вземат предвид всички релевантни фактори, включително нивото на класификация на КИЕС, с която се работи в КИС. Акредитацията включва формална декларация за остатъчен риск и приемане на остатъчния риск от отговорния орган.

▼B

Сигурност през жизнения цикъл на КИС

8. Гарантирането на сигурността е изискване, което важи през целия жизнен цикъл на КИС, от решението за нейното създаване до извеждането ѝ от експлоатация.

9. Ролята на участниците в КИС и взаимодействието между тях по отношение на сигурността на системата се определят за всеки етап от жизнения цикъл.

10. Всяка КИС, включително техническите и нетехническите мерки за нейната сигурност, се подлага на изпитване за сигурност по време на процеса на акредитация, за да се гарантира, че е постигнато необходимото ниво на осигуреност и да се удостовери, че тези мерки са правилно приложени, интегрирани и конфигурирани.

11. Оценки на сигурността, проверки и прегледи се извършват периодично по време на функционирането и поддръжката на КИС, както и при възникване на извънредни обстоятелства.

12. Документацията по сигурността на КИС се развива по време на жизнения цикъл на системата като неразделна част от процеса за управление на промените и на конфигурацията.

Най-добри практики

13. ГСС и държавите членки си сътрудничат за разработване на най-добри практики за защита на КИЕС, с която се работи в КИС. Насоките за най-добри практики съдържат технически, физически, организационни и процедурни мерки за сигурност на КИС с доказана ефективност за противодействие на определени заплахи и уязвими места.

14. Защитата на КИЕС, с която се работи в КИС, се усъвършенства въз основа на изводите, направени от организационните единици, ангажирани с осигуреността на информацията в рамките на Съюза и извън него.

15. Разпространението и последващото прилагане на най-добри практики допринася за постигане на равностойно ниво на осигуреност на използваните от ГСС и държавите членки различни видове КИС, които работят с КИЕС.

Защита в дълбочина

16. С оглед намаляване на риска за КИС се прилага съвкупност от технически и нетехнически мерки за сигурност, организирани под формата на многослойна защита. Те включват:

    а) *възпиране:* мерки за сигурност, имащи за цел възпиране на евентуален противник, който планира атака срещу КИС;

    б) *превенция:* мерки за сигурност, имащи за цел възпрепятстване или блокиране на атаки срещу КИС;

    в) *разкриване:* мерки за сигурност, имащи за цел откриване на извършена атака срещу КИС;

    г) *устойчивост:* мерки за сигурност, имащи за цел ограничаване на въздействието на извършена атака в рамките на минимално количество информация или активи на КИС и предотвратяване на понататъшни вреди; и

    д) *възстановяване:* мерки за сигурност, имащи за цел възстановяване на сигурната среда за работа на КИС.

    Степента на стриктност на тези мерки за сигурност се определя въз основа на оценка на риска.

17. НОС или друг компетентен национален орган отговаря за:

    а) прилагането на способности за киберотбрана за отговор при заплахи, които е възможно да надхвърлят организационните и националните граници; и

▼B

б) координирането на реакциите и обмена на информацията за тези заплахи, инциденти и свързаните с тях рискове (компютърни способности за спешно реагиране).

Принцип на минималност и най-малко привилегии

18. С цел да се избегне ненужно излагане на риск, в отговор на оперативните изисквания се прилагат само основни функционални възможности, съоръжения и услуги.

19. На ползвателите и автоматизираните процеси на КИС се дава само такъв достъп, привилегии или разрешения, които са необходими за изпълнение на задачите им, с оглед ограничаване на вредите в резултат от инциденти, грешки или неразрешено използване на ресурси на КИС.

20. При необходимост изпълняваните от КИС процедури за регистрация се проверяват в рамките на процеса на акредитация.

Повишаване на осведомеността по въпросите на осигуреността на информацията

21. Познаването на риска и на наличните мерки за сигурност представлява първата линия на защита на сигурността на КИС. По-конкретно всички служители, които имат отношение към жизнения цикъл на КИС, включително ползвателите, разбират:

а) че пропуските в сигурността могат да нанесат значителни вреди на комуникационните и информационните системи;

б) потенциалната вреда за други системи, която може да бъде предизвикана от взаимната свързаност и взаимната зависимост; и

в) индивидуалната си отговорност за сигурността на КИС в зависимост от конкретната си роля в рамките на системите и процесите.

22. Обучението и повишаването на осведомеността по въпросите на ОИ са задължителни за всички участващи служители, включително висшите служители и ползвателите на КИС, с цел да се гарантира, че те осъзнават своите отговорности по отношение на сигурността.

Оценка и одобрение на информационно-технологични продукти за сигурност

23. Необходимата степен на доверие в мерките за сигурност, определена като степен на осигуреност, се определя в съответствие с резултатите от процеса на управление на риска, съобразно съответните политики и насоки за сигурност.

24. Степента на осигуреност се удостоверява чрез международно признати или национално одобрени процеси и методологии. Тук се включват преди всичко оценката, контролът и одитът.

25. Криптографските продукти за защита на КИЕС се оценяват и одобряват от националния орган за криптографско одобрение на държавата членка.

26. Преди да бъдат препоръчани за одобрение от Съвета или от генералния секретар в съответствие с член 10, параграф 6, такива криптографски продукти преминават успешно втора оценка от страна на достатъчно квалифициран и компетентен орган (ДККО) на държава членка, която не участва в проектирането или производството на оборудването. Изискваната степен на задълбоченост при оценката от втори орган зависи от предвиденото максимално ниво на класификация за сигурност на КИЕС, която да бъде защитена с тези продукти. Съветът одобрява политика за сигурност по отношение на оценката и одобрението на криптографски продукти.

27. Когато за това има специфични оперативни основания, Съветът или съответно генералният секретар може, по препоръка на Комитета по сигурността, да отмени изискванията по точка 25 или 26 от настоящото приложение и да предостави временно одобрение за определен период, в съответствие с процедурата, изложена в член 10, параграф 6.

▼B

28. По препоръка на Комитета по сигурността Съветът може да приеме процеса по оценка, избор и одобрение на криптографски продукти, проведен в трета държава или международна организация, и следователно да обяви тези криптографски продукти за одобрени за защита на КИЕС, предоставена на въпросната трета държава или международна организация.

29. ДККО е органът на държавата членка за криптографско одобрение, който на базата на определени от Съвета критерии е получил акредитация да извършва втората оценка на криптографски продукти за защита на КИЕС.

30. Съветът одобрява политика за сигурност при квалифицирането и одобряването на некриптографски информационно-технологични продукти за сигурност.

Предаване в рамките на зони за сигурност или административни зони

31. Независимо от разпоредбите на настоящото решение, когато предаването на КИЕС е ограничено в рамките на зони за сигурност или административни зони, може да се прибегне до некриптирано предаване или криптиране на по-ниско ниво въз основа на резултатите от процеса на управление на риска и с одобрението на ОАС.

Сигурност на взаимната свързаност на КИС

32. За целите на настоящото решение взаимна свързаност означава пряка връзка между две или повече информационно-технологични системи с цел обмен на данни и други информационни ресурси (напр. комуникация) в еднопосочен или многопосочен план.

33. КИС третира всички взаимосвързани информационно-технологични системи като ненадеждни и прилага защитни мерки за контрол на обмена на класифицирана информация.

34. По отношение на всички взаимни връзки на КИС с друга информационно-технологична система се спазват следните основни изисквания:

а) изискванията на дейността или оперативните изисквания за такива взаимни връзки се декларират и одобряват от компетентните органи;

б) взаимната връзка преминава през процес на управление на риска и акредитация и се нуждае от одобрението на компетентните ОАС; и

в) по периметъра на всички КИС се инсталират мерки за защита на периметъра.

35. Не се допуска взаимна свързаност между акредитирана КИС и незащитена или обществена мрежа, освен в случаите, когато КИС разполага с одобрени мерки за защита на периметъра, инсталирани за тази цел между КИС и незащитената или обществената мрежа. Мерките за сигурност при такива взаимни връзки се разглеждат от компетентния по въпросите на осигуреността на информацията орган и се одобряват от компетентния ОАС.

Когато незащитената или обществената мрежа се използва единствено като преносител и данните са криптирани чрез криптографски продукт, одобрен в съответствие с член 10, такава връзка не се счита за взаимна свързаност.

36. Забранява се пряка или каскадна взаимна свързаност между КИС, акредитирана да работи с информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET, и незащитена или обществена мрежа.

Компютърни средства за съхранение

37. Компютърните средства за съхранение се унищожават в съответствие с процедури, одобрени от компетентния орган по сигурността.

▼B

38. Повторното използване, понижаването на нивото на класификация или декласификацията на компютърните средства за съхранение се извършва в съответствие с насоки за сигурност, които се определят съгласно член 6, параграф 2.

Извънредни обстоятелства

39. Независимо от разпоредбите на настоящото решение описаните по-долу специални процедури могат да се прилагат в извънредни ситуации, например по време на предстояща или настояща криза, конфликт, състояние на война или при извънредни оперативни обстоятелства.

40. КИЕС може да се предава, като се използват криптографски продукти, одобрени за по-ниско ниво на класификация за сигурност, или без да се криптира, със съгласието на компетентния орган, в случай че евентуално забавяне би причинило очевидно по-голяма вреда от тази, произтичаща от разкриване на класифицирания материал, и ако:

а) изпращачът и получателят не притежават необходимите уреди за криптиране или не притежават никакви уреди за криптиране; и

б) класифицираният материал не може да бъде изпратен своевременно с други средства.

41. Класифицираната информация, предавана при описаните в точка 39 обстоятелства, няма грифове за сигурност или обозначения, които да я отличават от некласифицирана информация или от информация, която може да бъде защитена с наличен криптографски продукт. Получателите се уведомяват незабавно за нивото на класификация с други средства.

42. След случаи на прилагане на точка 39 се изготвя доклад до компетентния орган и до Комитета по сигурността.

III. ФУНКЦИИ И ОРГАНИ, СВЪРЗАНИ С ОСИГУРЕНОСТТА НА ИНФОРМАЦИЯТА

43. В държавите членки и в ГСС се установяват следните функции във връзка с ОИ. Тези функции не изискват самостоятелни организационни единици. Единиците имат самостоятелни мандати. Функциите обаче и съпътстващите ги отговорности могат да бъдат комбинирани или интегрирани в една и съща организационна единица или да бъдат разделени в различни организационни единици, при условие че се избягват вътрешни конфликти на интереси или задачи.

Орган по осигуреността на информацията

44. ООИ отговаря за:

а) разработване на политики и насоки за сигурност за ОИ и наблюдение на тяхната ефективност и целесъобразност;

б) опазване и администриране на техническата информация, свързана с криптографските продукти;

в) гарантиране, че избраните за защита на КИЕС мерки за ОИ съответстват на политиките, уреждащи тяхната пригодност и избор;

г) гарантиране, че криптографските продукти се подбират в съответствие с политиките, уреждащи тяхната пригодност и избор;

д) координиране на обучението и повишаване на осведомеността относно ОИ;

е) консултиране с доставчика на системата, участниците в областта на сигурността и представители на ползвателите по отношение на политиките и насоките за сигурност за ОИ; и

ж) гарантиране на наличието на подходящ експертен ресурс в състава на Комитета по сигурността, отговарящ за въпросите на ОИ.

▼B

Орган по Tempest

45. Органът по Tempest (ОТ) отговаря за осигуряване на съответствие на КИС с политиките и насоките по Tempest. Той одобрява контрамерки по Tempest за инсталации и продукти за защита на КИЕС до определено ниво на класификация за сигурност в съответната оперативна среда.

Орган за криптографско одобрение

46. Органът за криптографско одобрение (ОКО) отговаря за осигуряване на съответствие на криптографските продукти с националната криптографска политика или криптографската политика на Съвета. Този орган одобрява криптографски продукти за защита на КИЕС до определено ниво на класификация за сигурност в съответната оперативна среда. По отношение на държавите членки органът за криптографско одобрение отговаря също така за оценката на криптографските продукти.

Орган за разпределение на криптографски материали

47. Органът за разпределение на криптографски материали (ОРКМ) отговаря за:

а) управление и отчитане на криптографски материали на ЕС;

б) осигуряване прилагането на подходящи процедури и за създаване на необходимите канали за отчитане, защитена работа, съхранение и разпределение на всички криптографски материали на ЕС; и

в) осигуряване предаването на криптографски материали на ЕС на или от лицата или службите, които ги използват.

Орган по акредитиране на сигурността

48. За всяка система ОАС отговоря за:

а) гарантиране, че КИС спазва съответните политики и насоки за сигурност, предоставяне на декларация за одобрение на КИС за работа с КИЕС до определено ниво на класификация за сигурност в съответната оперативна среда, като посочва реда и условията на акредитацията, както и критериите, по които се изисква повторно одобрение;

б) установяване на процес за акредитация на сигурността в съответствие с разработените политики, като ясно посочва условията за одобрение на подчинената му КИС;

в) определяне на стратегия за акредитация на сигурността, посочваща степента на задълбоченост при процеса на акредитация, която да съответства на необходимото равнище на осигуреност;

г) преглед и одобряване на документация, свързана със сигурността, включително правилник за управление на риска и за остатъчен риск, правилник за специфичните за системата изисквания за сигурност (ПССИС), документация за удостоверяване на изпълнението на мерките за сигурност и оперативните процедури за сигурност (ОПС), както и гарантиране на съответствието на тази документация с правилата и политиките на Съвета в областта на сигурността;

д) проверка на прилагането на мерките за сигурност по отношение на КИС чрез предприемане или спонсориране на оценки, проверки или прегледи по сигурността;

е) определяне на изискванията за сигурност (например нива на разрешение за достъп на персонала) за чувствителни от гледна точка на КИС длъжности;

ж) потвърждаване на избора на одобрени криптографски и продукти по Tempest, използвани за гарантиране на сигурността на КИС;

▼B

з) одобряване или, когато е уместно — участие в съвместно одобряване на взаимната свързаност на дадена КИС с други КИС; и

и) даване на консултации на доставчика на системата, участниците в областта на сигурността и представители на ползвателите относно управлението на риска за сигурността, по-конкретно на остатъчния риск, както и относно реда и условията на декларацията за одобрение.

49. ОАС на ГСС отговаря за акредитацията на всички КИС, които функционират в сферата на компетентност на ГСС.

50. Съответният ОАС на държава членка отговаря за акредитацията на КИС и техните компоненти, които функционират в сферата на компетентност на тази държава членка.

51. Съвместен съвет по акредитиране на сигурността (САС) отговаря за акредитацията на КИС, попадащи в сферата на компетентност както на ОАС на ГСС, така и на ОАС на държавите членки. Той е съставен от по един представител на ОАС на всяка държава членка и на заседанията му присъства представител на ОАС на Комисията. Канят се и други организационни единици, които имат електронна свързаност с дадена КИС, когато се обсъждат въпроси във връзка с тази система.

САС се председателства от представител на ОАС на ГСС. Той действа с консенсус на представителите на ОАС на институциите, държавите членки и други организационни единици, които имат електронна свързаност с дадената КИС. САС изготвя периодични доклади за дейността си до Комитета по сигурността и го уведомява за всички декларации за акредитация.

Оперативен орган по осигуреността на информацията

52. За всяка система оперативният орган по ОИ отговаря за:

а) разработване на документация по сигурността в съответствие с политиките и насоките за сигурност, по-конкретно с ПССИС, включително правилника за остатъчен риск, ОПС и криптографския план в рамките на процеса на акредитация на КИС;

б) участие в избора и изпитването на специфичните за системата мерки, уреди и софтуер за техническа сигурност с цел контрол на прилагането им и гарантиране, че те са инсталирани, конфигурирани и поддържани съгласно съответната документация по сигурността;

в) участие при подбора на мерките и устройствата за сигурност по Tempest, ако това се изисква от ПССИС, и гарантиране, че същите са безопасно инсталирани и поддържани в сътрудничество с органа по Tempest;

г) наблюдение на изпълнението и прилагането на ОПС, като при нужда може да възлага на собственика на системата отговорности, свързани с оперативната сигурност;

д) управление и работа с криптографски продукти, осигуряване на грижливото съхранение на криптографски и контролирани елементи, като при необходимост осигурява генерирането на криптографски променливи;

е) провеждане на аналитични прегледи и изпитвания на сигурността, по-специално за съставяне на съответните доклади за риска съгласно изискванията на ОАС;

ж) предоставяне на специфично за КИС обучение за целите на ОИ; и

з) въвеждане и прилагане на специфични за КИС мерки за сигурност.

▼B

ПРИЛОЖЕНИЕ V

ИНДУСТРИАЛНА СИГУРНОСТ

I. ВЪВЕДЕНИЕ

1. В настоящото приложение се съдържат разпоредбите за изпълнение на член 11. В него се излагат общите разпоредби по сигурността, приложими към индустриалните или други единици по време на преговорите за сключване на договор и през жизнения цикъл на класифицираните договори, възложени от ГСС.

2. Съветът одобрява насоки в областта на индустриалната сигурност, задаващи по-специално подробни изисквания за удостоверенията за сигурност на структура, приложенията относно аспектите на сигурността (ПАС), посещенията, предаването и преноса на КИЕС.

II. ЕЛЕМЕНТИ НА СИГУРНОСТТА В КЛАСИФИЦИРАНИ ДОГОВОРИ

Ръководство за класифициране за целите на сигурността

3. Преди да обяви търг за възлагане на класифициран договор или да възложи такъв договор, ГСС, в качеството си на възложител, определя класификацията за сигурност на информацията, която се предоставя на участниците в търга и на изпълнителите, както и класификацията за сигурност на информацията, която се създава от изпълнителя. За тази цел ГСС изготвя ръководство за класифициране за целите на сигурността (РКЦС), което да се ползва при изпълнението на договора.

4. При определяне на нивото на класификация за сигурност на различните елементи на класифицирания договор се прилагат следните принципи:

а) при изготвяне на ръководството за класифициране за целите на сигурността ГСС взема предвид всички релевантни аспекти на сигурността, включително нивото на класификация за сигурност, определено за информацията, която е предоставена и одобрена за ползване при изпълнението на договора от създателя на информацията;

б) общото ниво на класификация за сигурност на договора не може да бъде по-ниско от най-високото ниво на класификация за сигурност на който и да е от неговите елементи; и

в) при нужда ГСС влиза във връзка с националните органи по сигурността/определените органи по сигурността на държавите членки или друг заинтересован компетентен орган по сигурността, в случай на промени на нивото на класификация на информацията, създадена от изпълнителите или предоставена им при изпълнението на договора, както и при извършване на по-нататъшни промени в ръководството за класифициране за целите на сигурността.

Приложение относно аспектите на сигурността (ПАС)

5. Свързаните с договора изисквания за сигурност се описват в ПАС. Когато това е уместно, ПАС включва ръководството за класифициране за целите на сигурността и представлява неразделна част от класифицирания договор за изпълнение или подизпълнение.

6. В ПАС се съдържат разпоредби, изискващи от изпълнителя и/или подизпълнителя да спазва минималните стандарти, установени в настоящото решение. Неспазването на тези минимални стандарти може да представлява достатъчно основание за прекратяване на договора.

Инструкции за сигурност на програмата/проекта (ИСП)

7. В зависимост от обхвата на програмите или проектите, включващи достъп до, работа със или съхранение на КИЕС, определеният за управление на програмата или проекта орган възложител може да изготви специфични ИСП. ИСП изискват одобрение от страна на

▼B

националните органи по сигурността/определените органи по сигурността на държавите членки или друг компетентен орган по сигурността, участващ в ИСП, и могат да съдържат допълнителни изисквания за сигурност.

III. УДОСТОВЕРЕНИЕ ЗА СИГУРНОСТ НА СТРУКТУРА

8. Удостоверение за сигурност на структура се издава от националния орган по сигурността/определения орган по сигурността или друг компетентен орган по сигурността на държавата членка, за да удостовери в съответствие с националните законови и подзаконови актове, че индустриална или друга единица може да осигури в рамките на структурите си защита на КИЕС на съответното ниво на класификация за сигурност (CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET). Това удостоверение се представя на ГСС в качеството му на възложител, преди на изпълнителя или подизпълнителя, или на потенциалния изпълнител или подизпълнител да бъде предоставен или даден достъп до КИЕС.

9. Когато издава удостоверение за сигурност на структура, съответният национален орган по сигурността или определеният орган по сигурността извършва най-малко следното:

а) прави оценка на интегритета на индустриалната или друга единица;

б) прави оценка на собствеността, контрола или потенциала за странично влияние, които могат да се считат за риск за сигурността;

в) проверява дали индустриалната или друга единица е инсталирала система за сигурност в рамките на структурата, която обхваща всички подходящи мерки за сигурност, необходими за защитата на информация или материал с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, в съответствие с изискванията, установени в настоящото решение;

г) проверява дали статусът, от гледна точка на сигурността, на висшите служители, собствениците и служителите, от които се изисква да имат достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, е установен съгласно изискванията на настоящото решение; и

д) проверява дали индустриалната или друга единица е назначила служител по сигурността на структурата, който отговаря пред ръководството за прилагане на задълженията в областта на сигурността в рамките на съответната единица.

10. Когато е уместно, ГСС, в качеството си на възложител, уведомява съответния национален орган по сигурността/определения орган по сигурността или друг компетентен орган по сигурността, че на предварителния етап или за изпълнение на договора се изисква удостоверение за сигурност на структура. Удостоверение за сигурност на структура или разрешение за достъп на персонала се изисква на предварителния етап, ако в процеса на представяне на оферта трябва да се предостави КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET.

11. Органът възложител не възлага класифициран договор на предпочитан участник в търга, преди да е получил потвърждение от националния орган по сигурността/определения орган по сигурността или друг компетентен орган по сигурността на държавата членка, в която е регистриран съответният изпълнител или подизпълнител, че е издадено съответното удостоверение за сигурност на структура, ако такова е необходимо.

12. Националният орган по сигурността/определеният орган по сигурността или друг компетентен орган по сигурността, издал удостоверението за сигурност на структура, уведомява ГСС, в качеството му на възложител, за всички промени, засягащи удостоверението за

▼B

сигурност на структура. При договори за подизпълнение се уведомяват съответно националният орган по сигурността/определеният орган по сигурността или друг компетентен орган по сигурността.

13. Отнемането на удостоверението за сигурност на структура от съответния национален орган по сигурността/определения орган по сигурността или друг компетентен орган по сигурността представлява достатъчно основание за ГСС, в качеството му на възложител, да прекрати класифициран договор или да изключи участник от търга.

IV. КЛАСИФИЦИРАНИ ДОГОВОРИ ЗА ИЗПЪЛНЕНИЕ И ПОДИЗПЪЛНЕНИЕ

14. Когато КИЕС се предоставя на участник в търга на преддоговорния етап, поканата за представяне на оферта съдържа разпоредба, задължаваща участника в търга, който не е представил оферта или не е избран, да върне всички класифицирани документи в рамките на определен период от време.

15. След възлагането на класифициран договор за изпълнение или подизпълнение ГСС, в качеството си на възложител, уведомява националния орган по сигурността/определения орган по сигурността или друг компетентен орган по сигурността на изпълнителя или подизпълнителя за разпоредбите за сигурност на класифицирания договор.

16. При прекратяване на такива договори ГСС, в качеството си на възложител (и/или националният орган по сигурността/определеният орган по сигурността или съответно друг компетентен орган по сигурността при договори за подизпълнение), уведомява своевременно националния орган по сигурността/определения орган по сигурността или съответно друг компетентен орган по сигурността на държавата членка, в която е регистриран изпълнителят или подизпълнителят.

17. Като общо правило при прекратяване на класифицирания договор за изпълнение или подизпълнение от изпълнителя или подизпълнителя се изисква да върне на възложителя всяка държана от него КИЕС.

18. Конкретните разпоредби за разпореждане с КИЕС по време на изпълнението на договора или при неговото прекратяване се посочват в приложението относно аспектите на сигурността.

19. В случаите когато на изпълнител или подизпълнител е разрешено да задържи КИЕС след прекратяване на договора, той продължава да спазва установените в настоящото решение минимални стандарти и да осигурява защита на поверителността на КИЕС.

20. Условията, при които изпълнителят може да възлага договора за подизпълнение, се определят в условията за търга и в договора.

21. За да предостави за подизпълнение части от класифициран договор, изпълнителят получава разрешение от ГСС в качеството му на възложител. Договор за подизпълнение не може да бъде възлаган на индустриални или други единици, регистрирани в държава извън ЕС, която не е сключила споразумение за сигурност на информацията със Съюза.

22. Изпълнителят носи отговорност за осигуряване на спазването на установените в настоящото решение минимални стандарти за сигурност по време на извършването на всички подизпълнителски дейности и не предоставя КИЕС на подизпълнителя без предварителното писмено съгласие на възложителя.

23. По отношение на КИЕС, която е създадена от изпълнител или подизпълнител или с която те работят, правата на създател се упражняват от възложителя.

▼B

V. ПОСЕЩЕНИЯ ВЪВ ВРЪЗКА С КЛАСИФИЦИРАНИ ДОГОВОРИ

24. Когато за изпълнение на класифициран договор на служители на ГСС, на изпълнители и подизпълнители е необходимо да получат на взаимна основа достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET в помещенията си, се уреждат посещения, като се поддържа връзка с националните органи по сигурността/определените органи по сигурността или друг съответен компетентен орган по сигурността. В контекста на конкретни проекти обаче националните органи по сигурността/определените органи по сигурността могат да постигнат също така съгласие по процедура, при която такива посещения да могат да се организират пряко.

25. Всички посетители разполагат със съответното РДП и отговарят на изискването за „необходимост да се знае“ за получаване на достъп до КИЕС, свързана с договора на ГСС.

26. На посетителите се дава достъп единствено до КИЕС, свързана с целите на посещението.

VI. ПРЕДАВАНЕ И ПРЕНОС НА КИЕС

27. По отношение на предаването на КИЕС чрез електронни средства се прилагат съответните разпоредби на член 10 и приложение IV.

28. По отношение на преноса на КИЕС се прилагат съответните разпоредби на приложение III в съответствие с националните законови и подзаконови актове.

29. При определяне на мерките за сигурност при транспортиране на класифицирани материали като товар се прилагат следните принципи:

а) сигурността се осигурява на всеки етап по време на транспорта от пункта на произход до крайното местоназначение;

б) степента на защита, предоставена за дадена пратка, се определя от най-високото ниво на класификация за сигурност на материала, който се съдържа в нея;

в) за предоставящите транспорта компании се получава удостоверение за сигурност на структура на съответното ниво. В такива случаи персоналът, обработващ пратката, е преминал през проучване за надеждност в съответствие с приложение I;

г) преди трансграничен пренос на материали, класифицирани като CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, изпращачът изготвя план за пренос, който се одобрява от националния орган по сигурността/определения орган по сигурността или друг съответен компетентен орган по сигурността;

д) пътуванията, доколкото това е възможно, се извършват от пункт до пункт и толкова бързо, колкото позволяват обстоятелствата; и

е) винаги когато това е възможно, маршрутите следва да преминават само през държави членки. Маршрути през държави, които не са членки на ЕС, следва да се използват единствено когато са разрешени от националните органи по сигурността/определените органи по сигурността или други компетентни органи по сигурността на държавите както на изпращача, така и на получателя.

VII. ПРЕДАВАНЕ НА КИЕС НА ИЗПЪЛНИТЕЛИ, РАЗПОЛОЖЕНИ В ТРЕТИ ДЪРЖАВИ

30. Предаването на КИЕС на изпълнители и подизпълнители, разположени в трети държави, се извършва в съответствие с мерките за сигурност, договорени между ГСС, в качеството му на възложител, и националния орган по сигурността/определения орган по сигурността на съответната трета държава, в която е регистриран изпълнителят.

▼B

VIII. ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ RESTREINT UE/EU RESTRICTED

31. Като поддържа връзка съответно с националния орган по сигурността/определения орган по сигурността на държавата членка, ГСС, в качеството си на възложител, има право да извършва проверки на структурите на изпълнителя/подизпълнителя на основание на договорните разпоредби с цел да се увери, че са осъществени необходимите мерки за сигурност за защита на КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, както се изисква съгласно сключения договор.

32. В необходимата по националните законови и подзаконови актове степен националните органи по сигурността/определените органи по сигурността или други компетентни органи по сигурността биват уведомявани от ГСС в качеството му на орган възложител относно договори за изпълнение и подизпълнение, съдържащи информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED.

33. Не се изисква удостоверение за сигурност на структура, нито разрешение за достъп за изпълнители или подизпълнители и техния персонал за договори, възлагани от ГСС, които съдържат информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED.

34. ГСС, в качеството си на възложител, разглежда отговорите на поканите за представяне на оферти за договори, изискващи достъп до информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, независимо от изискванията за удостоверения за сигурност на структура или разрешения за достъп на персонала, които съществуват съгласно националните законови и подзаконови актове.

35. Условията, при които изпълнителят може да възлага изпълнението на договор за подизпълнение, са в съответствие с точка 21.

36. Когато даден договор включва работа с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED в рамките на КИС, с която оперира изпълнител, ГСС, в качеството си на възложител, гарантира включването в договора за изпълнение или подизпълнение на необходимите технически и административни изисквания за акредитация на въпросната КИС, съизмерими с оценката на риска, като се вземат предвид всички свързани с въпроса фактори. Обхватът на акредитацията на такава КИС се договаря между възложителя и съответния национален орган по сигурността/определен орган по сигурността.

▼B

ПРИЛОЖЕНИЕ VI

ОБМЕН НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ С ТРЕТИ ДЪРЖАВИ И МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

I. ВЪВЕДЕНИЕ

1. В настоящото приложение се съдържат разпоредбите за изпълнение на член 13.

II. РАМКИ ЗА УРЕЖДАНЕ НА ОБМЕНА НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

2. Когато Съветът е установил, че съществува дългосрочна необходимост от обмен на класифицирана информация:

— се сключва споразумение за сигурност на информацията, или

— се подписва административна договореност

в съответствие с член 13, параграф 2 и раздели III и IV и въз основа на препоръка от Комитета по сигурността.

3. В случаите, когато КИЕС, създадена за целите на операция по линия на ОПСО, трябва да се предостави на трети държави или международни организации, участващи в такава операция, и когато не съществува никоя от посочените в точка 2 рамки, обменът на КИЕС с участващата трета държава или международна организация се урежда, в съответствие с раздел V, чрез:

— рамково споразумение за участие,

— *ad hoc* споразумение за участие, или

— при отсъствие на двете посочени по-горе споразумения — чрез *ad hoc* административна договореност.

4. При отсъствие на посочената в точки 2 и 3 рамка и в случаите, когато се взема решение за извънредно *ad hoc* предоставяне на КИЕС на трета държава или международна организация съгласно раздел VI, от съответната трета държава или международна организация се изискват писмени уверения с оглед да се гарантира, че тя осигурява защита на предоставената ѝ КИЕС в съответствие с основните принципи и минималните стандарти, определени в настоящото решение.

III. СПОРАЗУМЕНИЯ ЗА СИГУРНОСТ НА ИНФОРМАЦИЯТА

5. Споразуменията за сигурност на информацията установяват основните принципи и минималните стандарти, които регулират обмена на класифицирана информация между Съюза и дадена трета държава или международна организация.

6. В тези споразумения се предвиждат договорености за техническото изпълнение, които се постигат между компетентните органи по сигурността на съответните институции и органи на Съюза и компетентния орган по сигурността на въпросната трета държава или международна организация. Тези договорености отчитат нивото на защита, предоставено от прилаганите в съответната трета държава или международна организация разпоредби, структури и процедури за сигурност. Те се одобряват от Комитета по сигурността.

7. КИЕС не се обменя с електронни средства по линия на споразумение за сигурност на информацията, освен ако това не е изрично предвидено в споразумението или в съответните договорености за техническото изпълнение.

8. Когато Съветът сключва споразумение за сигурност на информацията, всяка от страните определя регистратура, която служи като главна входяща и изходяща точка за обмен на класифицирана информация.

▼B

9. За оценка на ефективността на разпоредбите, структурите и процедурите за сигурност в съответната трета държава или международна организация се провеждат посещения за оценка по взаимно споразумение със съответната трета държава или международна организация. Такива посещения за оценка се провеждат съгласно съответните разпоредби на приложение III и при провеждането им се извършва оценка на:

   а) регулаторната рамка, приложима към защитата на класифицирана информация;

   б) специфични елементи на политиката за сигурност и начина, по който сигурността е организирана в третата държава или международната организация, които могат да окажат въздействие върху нивото на класифицираната информация, която може да бъде обменяна;

   в) въведените мерки и процедури за сигурност; и

   г) процедурите за разрешаване на достъп до нивото на КИЕС, която се предоставя.

10. Екипът, извършващ посещението за оценка от името на Съюза, прави преценка дали разпоредбите и процедурите за сигурност във въпросната трета държава или международна организация са на необходимото равнище за защита на КИЕС с определено ниво на класификация за сигурност.

11. Констатациите от такива посещения се оформят в доклад, въз основа на който Комитетът по сигурността определя максималното ниво на КИЕС, която може да бъде обменяна на хартиен носител, и съответно с електронни средства, с въпросната трета страна, както и други специфични условия, уреждащи обмена на информация с тази страна.

12. Полагат се всички усилия за извършване на посещение за пълна оценка на сигурността във въпросната трета държава или международна организация, преди Комитетът по сигурността да одобри договореностите за изпълнение, за да се установят естеството и ефективността на въведените системи за сигурност. Когато обаче това е невъзможно, службата на ГСС по сигурността предоставя на Комитета по сигурността възможно най-изчерпателен доклад, изготвен въз основа на информацията, с която разполага, с който го информира за приложимите разпоредби относно сигурността и за начина, по който е организирана сигурността във въпросната трета държава или международна организация.

13. Преди КИЕС да бъде реално предоставена на въпросната трета държава или международна организация, докладът за посещението за оценка или при липса на такъв — докладът, посочен в точка 12, се изпраща на Комитета по сигурността, който го преценява като удовлетворителен.

14. Компетентните органи по сигурността на институциите и органите на Съюза съобщават на третата държава или международната организация датата, от която Съюзът ще е в състояние да предостави КИЕС по линия на споразумението, както и максималното ниво на класификация на КИЕС, която може да бъде обменяна на хартиен носител или чрез електронни средства.

15. При необходимост се провеждат последващи посещения за оценка, особено ако:

   а) е налице необходимост да се повиши нивото на класификация на подлежащата на предоставяне КИЕС;

   б) Съюзът е бил уведомен за съществени промени в уредбата на третата държава или международната организация относно сигурността, които могат да имат последици върху защитата на КИЕС; или

   в) е настъпил сериозен инцидент, свързан с нерегламентирано разкриване на КИЕС.

▼B

16. След като споразумението за сигурност на информацията влезе в сила и започне обменът на класифицирана информация със съответната трета държава или международна организация, Комитетът по сигурността може да вземе решение за промяна на максималното ниво на класификация на КИЕС, която може да бъде обменяна на хартиен носител или с електронни средства, по-специално с оглед на евентуални последващи посещения за оценка.

IV. АДМИНИСТРАТИВНИ ДОГОВОРЕНОСТИ

17. Когато е налице дългосрочна необходимост от обмен на информация с ниво на класификация за сигурност като общо правило не по-високо от RESTREINT UE/EU RESTRICTED с трета държава или международна организация и когато Комитетът по сигурността е установил, че въпросната договаряща страна не разполага с достатъчно развита система за сигурност, за да е възможно тя да встъпи в споразумение за сигурност на информацията, генералният секретар може, след одобрение от страна на Съвета, да встъпи, от името на ГСС, в административна договореност със съответните органи на въпросната трета държава или международна организация.

18. Когато по неотложни оперативни причини е необходимо бързо да се създаде рамка за обмен на класифицирана информация, Съветът по изключение може да реши, че за обмен на информация с по-високо ниво на класификация за сигурност може да се постигне административна договореност.

19. Административните договорености като правило се осъществяват под формата на размяна на писма.

20. Преди КИЕС да бъде реално предоставена на въпросната трета държава или международна организация, се извършва посещение за оценка съгласно точка 9 и съответният доклад или, при липса на такъв — докладът, посочен в точка 12, се изпраща на Комитета по сигурността, който го преценява като удовлетворителен.

21. КИЕС не се обменя чрез електронни средства по линия на административна договореност, освен в случаите, когато това е изрично предвидено в тази договореност.

V. ОБМЕН НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ В КОНТЕКСТА НА ОПЕРАЦИИ ПО ЛИНИЯ НА ОПСО

22. Участието на трети държави или международни организации в операции по линия на ОПСО се регулира от рамкови споразумения за участие. Тези споразумения съдържат разпоредби относно предоставянето на КИЕС, създадена за целите на операциите по линия на ОПСО, на участващите в тях трети държави или международни организации. Най-високото ниво на класификация за сигурност, на което може да бъде обменяна КИЕС, е RESTREINT UE/EU RESTRICTED за граждански операции по линия на ОПСО и CONFIDENTIEL UE/EU CONFIDENTIAL за военни операции по линия на ОПСО, освен ако в решението за създаване на дадена операция по линия на ОПСО не е предвидено друго.

23. В ad hoc споразумения за участие, сключени по повод на конкретна операция по линия на ОПСО, се включват разпоредби относно предоставянето на КИЕС, създадена за целите на операцията, на участващата в нея трета държава или международна организация. Най-високото ниво на класификация за сигурност, на което може да бъде обменяна КИЕС, е RESTREINT UE/EU RESTRICTED за граждански операции по линия на ОПСО и CONFIDENTIEL UE/EU CONFIDENTIAL за военни операции по линия на ОПСО, освен ако в решението за създаване на дадена операция по линия на ОПСО не е предвидено друго.

▼B

24. При липса на споразумение за сигурност на информацията и предстоящо сключване на споразумение за участие предоставянето на КИЕС, създадена за целите на операцията, на трета държава или международна организация, която участва в операцията, се регламентира от административна договореност, сключвана от върховния представител или по силата на решение за *ad hoc* предоставяне съгласно раздел VI. КИЕС се обменя по линия на подобна договореност единствено доколкото плановете за участие на третата държава или международната организация продължават да са валидни. Най-високото ниво на класификация за сигурност, на което може да бъде обменяна КИЕС, е RESTREINT UE/EU RESTRICTED за граждански операции по линия на ОПСО и CONFIDENTIEL UE/EU CONFIDENTIAL за военни операции по линия на ОПСО, освен ако в решението за създаване на дадена операция по линия на ОПСО не е предвидено друго.

25. Разпоредбите относно класифицираната информация, които се включват в рамковите споразумения за участие, *ad hoc* споразуменията за участие и *ad hoc* административните договорености, посочени в точки 22—24, предвиждат въпросната трета държава или международна организация да гарантира, че нейният личен състав, командирован за участие в дадена операция, осигурява защита на КИЕС в съответствие с правилата за сигурност на Съвета и допълнителните насоки, издадени от компетентните органи, включително от командната верига на операцията.

26. Ако впоследствие между Съюза и участващата трета държава или международна организация бъде сключено споразумение за сигурност на информацията, споразумението за сигурност на информацията заменя разпоредбите относно обмена на класифицирана информация, установени в рамково споразумение за участие, *ad hoc* споразумение за участие или *ad hoc* административна договореност, що се отнася до обмена на КИЕС и работата с нея.

27. По силата на рамково споразумение за участие, *ad hoc* споразумение за участие или *ad hoc* административна договореност с трета държава или международна организация не се разрешава обмен на КИЕС чрез електронни средства, освен ако това не е изрично предвидено във въпросното споразумение или договореност.

28. КИЕС, създадена за целите на операция по линия на ОПСО, може да бъде разкрита на членове на личния състав, командирован за участие в съответната операция от трети държави или международни организации в съответствие с точки 22—27. Когато на такива членове на личния състав се разрешава достъп до КИЕС в помещенията или в КИС на операция по линия на ОПСО, се прилагат мерки (включително регистриране на разкритата КИЕС) за намаляване на риска от загуба или компрометиране на информация. Тези мерки се определят в съответните документи за планиране или осъществяване на мисията.

29. При липса на споразумение за сигурност на информацията предаването на КИЕС в случай на конкретна и непосредствена оперативна необходимост на приемащата държава, на чиято територия се провежда операцията по линия на ОПСО, може да се регламентира от административна договореност, сключвана от върховния представител. Такава възможност се предвижда в решението за създаване на съответната операция по линия на ОПСО. Предоставената при тези обстоятелства КИЕС се ограничава до информацията, създадена за целите на операцията по линия на ОПСО, и е с ниво на класификация за сигурност, не по-високо от RESTREINT UE/EU RESTRICTED, освен ако в решението за създаване на операцията по линия на ОПСО не е предвидено по-високо ниво на класификация за сигурност. По силата на такава административна договореност от приемащата държава се изисква да осигури защита на КИЕС съобразно минимални стандарти, които са не по-малко стриктни от установените в настоящото решение.

▼B

30. При липса на споразумение за сигурност на информацията предоставянето на КИЕС на имащи отношение трети държави или международни организации, които не са сред участващите в операция по линия на ОПСО, може да се регламентира от административна договореност, сключвана от върховния представител. Ако е целесъобразно, тази възможност и условията, с които тя е обвързана, се посочват в решението за създаване на операцията по линия на ОПСО. Предоставената при тези обстоятелства КИЕС се ограничава до информацията, създадена за целите на операцията по линия на ОПСО и е с ниво на класификация за сигурност, не по-високо от RESTREINT UE/EU RESTRICTED, освен ако в решението за създаване на операцията по линия на ОПСО не е предвидено по-високо ниво на класификация за сигурност. По силата на такава административна договореност от въпросната трета държава или международната организация се изисква да осигури защита на КИЕС съобразно минимални стандарти, които са не по-малко стриктни от установените в настоящото решение.

31. Не се изискват договорености за изпълнение или посещения за оценка, преди да бъдат приложени разпоредбите за предоставяне на КИЕС в контекста на точки 22, 23 и 24.

VI. ИЗВЪНРЕДНО AD HOC ПРЕДОСТАВЯНЕ НА КИЕС

32. Когато не е създадена рамка в съответствие с раздели III—V и когато Съветът или някой от подготвителните му органи преценят, че е налице извънредна необходимост от предоставяне на КИЕС на трета държава или международна организация, ГСС:

а) доколкото е възможно, прави проверка заедно с органите по сигурността на съответната трета държава или международна организация дали нейните разпоредби, структури и процедури за сигурност гарантират, че предоставената ѝ КИЕС ще бъде защитена съобразно стандарти, които са не по-малко стриктни от установените в настоящото решение; и

б) приканва Комитета по сигурността, въз основа на наличната информация, да издаде препоръка относно надеждността на разпоредбите, структурите и процедурите за сигурност на третата държава или международната организация, на която се предоставя КИЕС.

33. Ако Комитетът по сигурността издаде препоръка в полза на предоставянето на КИЕС, въпросът се отнася до Комитета на постоянните представители (Корепер), който взема решение за предоставяне на информацията.

34. Ако в препоръката на Комитета по сигурността не се подкрепя предоставянето на КИЕС:

а) за въпроси от областта на ОВППС/ОПСО, Комитетът по политика и сигурност обсъжда въпроса и формулира препоръка за решение на Корепер;

б) за всички останали въпроси Корепер обсъжда въпроса и приема решение.

35. Когато се счете за целесъобразно и с предварителното писмено съгласие на създателя, Корепер може да реши класифицираната информация да бъде предоставена само частично или само ако предварително бъде понижено или премахнато нивото на класификацията ѝ, или да реши информацията, която се предоставя, да бъде изготвена без позоваване на източника или на първоначалното ниво на класификация за сигурност на ЕС.

36. След решение за предоставяне на КИЕС ГСС изпраща съответния документ с обозначение, че подлежи на предоставяне, в което се посочва третата държава или международната организация, на която се предоставя. Преди или при самото предоставяне на КИЕС въпросната трета страна писмено потвърждава, че поема задължение за защита на получената от нея КИЕС в съответствие с основните принципи и минималните стандарти, установени в настоящото решение.

▼B

VII. ПРАВОМОЩИЕ ЗА ПРЕДОСТАВЯНЕ НА КИЕС НА ТРЕТИ ДЪРЖАВИ ИЛИ МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

37. Когато съществува рамка в съответствие с точка 2 за обмен на класифицирана информация с трета държава или международна организация, Съветът взема решение да оправомощи генералния секретар, в съответствие с принципа на съгласие на създателя на информацията, за предоставяне на КИЕС на въпросната трета държава или международна организация. Генералният секретар може да делегира такова правомощие на висши служители на ГСС.

38. При наличие на споразумение за сигурност на информацията в съответствие с точка 2, първо тире Съветът може да вземе решение за упълномощаване на върховния представител да предостави на съответната трета държава или международна организация КИЕС, създадена от Съвета в областта на Общата външна политика и политика на сигурност, след получаване на съгласието на създателя на всеки материал, използван в информацията. Върховният представител може да делегира това правомощие на висши служители на ЕСВД или на специални представители на ЕС.

39. При наличие на рамка в съответствие с точка 2 или точка 3 за обмен на класифицирана информация с трета държава или международна организация върховният представител се оправомощава да предоставя КИЕС съгласно решението за създаване на съответната операция по линия на ОПСО и принципа на съгласие на създателя на информацията. Върховният представител може да делегира това правомощие на висши служители на ЕСВД, на командващи операции, сили или мисии на ЕС или на ръководителите на мисии на ЕС.

▼**B**

Допълнения

Допълнение А

Определения

Допълнение Б

Съответствия на нивата на класификация за сигурност

Допълнение В

Списък на националните органи по сигурността

Допълнение Г

Списък на съкращенията

▼B

Допълнение A

ОПРЕДЕЛЕНИЯ

За целите на настоящото решение се прилагат следните определения:

„Акредитация“ означава процес, който води до официално произнасяне на органа по акредитиране на сигурността (ОАС) в уверение на това, че дадена система е одобрена да функционира на определено ниво на класификация за сигурност, при определен режим на сигурност в своята операционна среда и при приемливо ниво на риск, въз основа на предпоставката, че е осъществен одобрен комплекс от технически, физически, организационни и процедурни мерки за сигурност.

„Актив“ е всичко, което представлява ценност за дадена организация, нейните бизнес операции и тяхната непрекъснатост, включително информационните ресурси в подкрепа на мисията на организацията.

„Разрешение за достъп до КИЕС“ означава решение на назначаващия орган на ГСС, взето въз основа на уверение, предоставено от компетентен орган на държава членка, че дадено длъжностно лице на ГСС, друг служител или командирован национален експерт може да получи достъп до КИЕС на определено ниво (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо) до конкретна дата, при условие че бъде установена „необходимост да се знае“ за това лице и то е преминало през съответен инструктаж за своите отговорности.

„Жизнен цикъл на КИС“ означава целия период на съществуване на КИС, който включва нейното създаване, концепция, планиране, анализ на изискванията, разработка, развитие, изпитване, въвеждане, функциониране, поддръжка и извеждане от експлоатация.

„Класифициран договор“ означава договор, по който ГСС е страна, сключен с изпълнител за доставка на стоки, извършване на строително-ремонтни дейности или предоставяне на услуги, изпълнението на който изисква или включва достъп до КИЕС или създаване на КИЕС.

„Класифициран договор за подизпълнение“ означава договор, сключен от изпълнител на ГСС с друг изпълнител (т.е. подизпълнител) за доставка на стоки, извършване на строително-ремонтни дейности или предоставяне на услуги, изпълнението на който изисква или включва достъп до КИЕС или създаване на КИЕС.

„Комуникационна и информационна система“ (КИС) — вж. член 10, параграф 2.

„Изпълнител“ означава физическо или юридическо лице, което е правоспособно да сключва договори.

„Криптографски (крипто) материал“ означава криптографски алгоритми, криптографски хардуерни и софтуерни модули и продукти, включително данни за прилагането им и свързаната с това документация и материали, служещи за заключване/отключване на информацията.

„Криптографски продукт“ означава продукт, чието основно и водещо предназначение е предоставянето на услуги за сигурност (поверителност, интегритет, наличност, автентичност, невъзможност за отказ) посредством един или повече криптографски механизми.

▼B

„Операция по линия на ОПСО“ означава военна или гражданска операция по управление на кризи съгласно дял V, глава 2 от ДЕС.

„Декласификация“ означава премахване на всякаква класификация за сигурност.

„Защита в дълбочина“ означава прилагане на съвкупност от мерки за сигурност, организирани под формата на многослойна защита.

„Определен орган по сигурността“ (ООС) означава орган, отговорен пред националния орган по сигурността (НОС) на държава членка, който отговаря за информиране на индустриални или други единици за националната политика по всички въпроси на индустриалната сигурност и за предоставяне на указания и съдействие при нейното изпълнение. Функциите на определен орган по сигурността се изпълняват от НОС или от друг компетентен орган.

„Документ“ означава всяка записана информация, независимо от нейната физическа форма или характеристики.

„Понижаване нивото на класификация“ означава понижаване на нивото на класификацията за сигурност.

„Класифицирана информация на ЕС“ (КИЕС) — вж. член 2, параграф 1.

„Удостоверение за сигурност на структура“ (УСС) означава административно определяне от национален орган по сигурността или определен орган по сигурността, че дадена структура може да осигури адекватна защита на КИЕС на определено ниво на класификация за сигурност.

„Работа с КИЕС“ означава всички възможни действия, на които може да бъде подложена КИЕС през жизнения ѝ цикъл. Това включва нейното създаване, обработка и пренос, понижаването на нивото на класификацията ѝ, декласификацията ѝ и нейното унищожаване. По отношение на КИС това включва и нейното събиране, излагане, предаване и съхранение.

„Притежател“ означава надлежно оправомощено лице с добре установена „необходимост да се знае“, което притежава дадена КИЕС и носи съответно отговорност за нейната защита.“

„Индустриална или друга единица“ означава единица, която участва в процеса на снабдяване със стоки, извършване на строително-ремонтни дейности или предоставяне на услуги; това може да бъде единица от сферата на промишлеността, търговията, услугите, научноизследователската дейност, образованието или развойната дейност или самостоятелно заето лице.

„Индустриална сигурност“ — вж. член 11, параграф 1.

„Осигуреност на информацията“ — вж. член 10, параграф 1.

„Взаимна свързаност“ — вж. приложение IV, точка 32.

„Управление на класифицирана информация“ — вж. член 9, параграф 1.

▼B

„Материал“ означава документ, носител на данни или машина, или оборудване, които са вече създадени или са в процес на създаване.

„Създател“ означава институция, орган или агенция на Съюза, както и държава членка, трета държава или международна организация, под чието ръководство е създадена и/или въведена в структурите на Съюза класифицирана информация.

„Физическа сигурност“ — вж. член 7, параграф 1.

„Разрешение за достъп на персонала“ (РДП) означава изявление на компетентния орган на държава членка, което се прави след приключване на проучване за надеждност, извършено от компетентните органи на държавата членка, с което се удостоверява, че дадено лице може да получи достъп до КИЕС на определено ниво (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо) до конкретна дата.

„Удостоверение за разрешение за достъп на персонала“ (УРДП) означава удостоверение, издадено от компетентен орган, с което се удостоверява, че дадено лице е преминало проучване за надеждност и притежава валидно удостоверение за разрешение за достъп или издадено от назначаващия орган разрешение за достъп до КИЕС, в което се посочва нивото на класификация на КИЕС, до което лицето може да има достъп (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо), датата, до която е валидно съответното РДП, и датата, на която изтича валидността на самото удостоверение.

„Физическа сигурност“ — вж. член 8, параграф 1.

„Инструкции за сигурност на програмата/проекта (ИСП) означава списък от процедури за сигурност, които се прилагат за конкретна програма или проект с цел стандартизиране на процедурите за сигурност. Инструкциите могат да бъдат преработени, докато трае осъществяването на програмата/проекта.

„Регистрация“ — вж. приложение III, точка 18.

„Остатъчен риск“ означава риска, който продължава да съществува след прилагане на мерките за сигурност, при положение че не може да се противодейства на всички заплахи и че не всички видове уязвимост могат да бъдат премахнати.

„Риск“ означава възможността дадена заплаха да използва вътрешните или външни видове уязвимост на дадена организация или на някоя от системите, които тази организация използва, и по този начин да нанесе вреди на организацията и на нейните материални или нематериални активи. Рискът се измерва като съчетание от вероятността от осъществяване на заплахи и тяхното въздействие.

— „Приемане на риска“ означава решение за приемане на продължаващото съществуване на остатъчен риск след третиране на риска.

— „Оценка на риска“ — състои се от установяване на заплахите и видовете уязвимост и от анализ на свързаните с тях рискове, т.е. анализ на вероятността и въздействието.

— „Съобщаване за риска“ — изразява се в повишаване на осведомеността за рисковете сред общностите от ползватели на КИС, информиране за такива рискове на органите, които дават одобрение, и докладване за тях на оперативните органи.

▼B

— „Третиране на риска“ — изразява се в смекчаване, отстраняване, намаляване (чрез подходяща комбинация от технически, физически, организационни или процедурни мерки), прехвърляне или наблюдение на риска.

„Приложение относно аспектите на сигурността“ (ПАС) означава съвкупност от специални договорни условия, изготвени от възложителя, които представляват неразделна част от всеки класифициран договор, включващ достъп до КИЕС или създаване на такава информация, и в които се определят изискванията за сигурност или елементите на договора, изискващи защита на сигурността.

„Ръководство за класифициране за целите на сигурността“ (РКЦС) означава документ, който описва елементите на програма или договор, които са класифицирани, като определя приложимите нива на класификация за сигурност. РКЦС може да бъде допълвано през целия период на времетраене на програмата или договора, като нивото на класификация на елементите на информацията може да бъде променено или понижено; РКЦС, в случай че такова съществува, е част от ПАС.

„Проучване за надеждност“ означава процедури за проучване, извършвани от компетентния орган на държава членка в съответствие с нейните национални законови и подзаконови актове с цел да се получи уверение, че няма известна неблагоприятна информация, която да попречи на дадено лице да бъде издадено национално РДП или разрешение за достъп до КИЕС на определено ниво на класификация за сигурност (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо).

„Режим на сигурност“ означава определяне на условията, при които функционира дадена КИС, въз основа на нивото на класификация на информацията, с която се работи, и нивата на достъп, одобренията за официален достъп и „необходимостта да се знае“ от ползвателите на системата. Съществуват четири режима на работа с класифицирана информация или при предаване на такава: режим с общ достъп (dedicated mode), режим с общо ниво (system-high mode), сегментиран режим (compartmented mode) и режим с много нива (multilevel mode):

— „режим с общ достъп“ означава режим на работа, при който всички лица, които имат достъп до КИС, имат разрешение за достъп до информацията с най-високо ниво на класификация за сигурност, с която се работи в КИС, и имат обща „необходимост да се знае“ по отношение на цялата информация, с която се работи в КИС,

— „режим с общо ниво“ означава режим на работа, при който всички лица, които имат достъп до КИС, имат разрешение за достъп до информацията с най-високо ниво на класификация за сигурност, с която се работи в КИС, но не всички лица с достъп до КИС имат обща „необходимост да се знае“ по отношение на информацията, с която се работи в КИС; одобрение за достъп до информация може да бъде дадено от физическо лице,

— „сегментиран режим“ означава режим на работа, при който всички лица, които имат достъп до КИС, имат разрешение за достъп до информацията с най-високо ниво на класификация за сигурност, с която се работи в КИС, но не всички лица с достъп до КИС разполагат с официално разрешение за достъп до цялата информация, с която се работи в КИС; официално разрешение означава официално централно управление на контрола на достъпа, за разлика от решение по усмотрение на отделно лице да бъде даден достъп,

▼B

— „режим с много нива“ означава режим на работа, при който не всички лица, които имат достъп до КИС, имат разрешение за достъп до информацията с най-високо ниво на класификация за сигурност, с която се работи в КИС, и не всички лица с достъп до КИС имат обща „необходимост да се знае“ по отношение информацията, с която се работи в КИС.

„Процес на управление на риска за сигурността“ означава целия процес на идентифициране, контрол и свеждане до минимум на неопределени събития, които могат да засегнат сигурността на дадена организация или на която и да е от използваните от нея системи. Този процес обхваща всички дейности, свързани с риска, включително оценка, третиране, приемане и съобщаване.

„Tempest“ означава разследване, проучване и контрол на компрометиращи електромагнитни излъчвания и мерките за тяхното отстраняване.

„Заплаха“ означава потенциална причина за нежелан инцидент, който може да доведе до вредни последици за дадена организация или за която и да е от използваните от нея системи; такива заплахи могат да бъдат инцидентни или умишлени (злонамерени) и имат характерни елементи на заплаха, потенциални цели и методи за нападение.

„Уязвимост“ означава слабост от каквото и да било естество, която може да бъде използвана от една или повече заплахи. Уязвимостта може да бъде пропуск или да бъде свързана със слабости в режима на контрол, свързани с неговата строгост, всеобхватност или съгласуваност, и може да има технически, процедурен, физически, организационен или оперативен характер.

▼M1

Допълнение Б

СЪОТВЕТСТВИЯ НА НИВАТА НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ

ЕС	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Белгия	Très Secret (Loi 11.12.1998 г.) Zeer Geheim (Wet 11.12.1998 г.)	Secret (Loi 11.12.1998 г.) Geheim (Wet 11.12.1998 г.)	Confidentiel (Loi 11.12.1998 г.) Vertrouwelijk (Wet 11.12.1998 г.)	(вж. бележка [1]) по-долу)
България	Строго секретно	Секретно	Поверително	За служебно ползване
Чешка република	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Дания	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Германия	STRENG GEHEIM	GEHEIM	VS [2]— VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Естония	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ирландия	Top Secret	Secret	Confidential	Restricted
Гърция	Άκρως Απόρρητο съкр.: (ΑΑΠ)	Απόρρητο съкр.: (ΑΠ)	Εμπιστευτικό съкр.: (ΕΜ)	Περιορισμένης Χρήσης съкр.: (ΠΧ)
Испания	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Франция	Très Secret Défense	Secret Défense	Confidentiel Défense	(вж. бележка [3]) по-долу)
Хърватия	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Италия	Segretissimo	Segreto	Riservatissimo	Riservato
Кипър	Άκρως Απόρρητο съкр.: (ΑΑΠ)	Απόρρητο съкр.: (ΑΠ)	Εμπιστευτικό съкр.: (ΕΜ)	Περιορισμένης Χρήσης съкр.: (ΠΧ)
Латвия	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Литва	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo

([1]) Diffusion Restreinte/Beperkte Verspreiding не се счита за ниво на класификация за сигурност в Белгия. Белгия работи със и защитава информация с ниво на класификация за сигурност „RESTREINT UE/EU RESTRICTED“ по начин, който е не по-малко стриктен от стандартите и процедурите, описани в правилата за сигурност на Съвета на Европейския съюз.

([2]) Германия: VS = Verschlusssache.

([3]) Франция не използва ниво на класификация за сигурност „RESTREINT“ в националната си система. Франция работи със и защитава информация с ниво на класификация за сигурност „RESTREINT UE/EU RESTRICTED“ по начин, който е не по-малко стриктен от стандартите и процедурите, описани в правилата за сигурност на Съвета на Европейския съюз.

▼M1

Люксембург | Très Secret Lux | Secret Lux | Confidentiel Lux | Restreint Lux |

Унгария | Szigorúan titkos! | Titkos! | Bizalmas! | Korlátozott terjesztésű! |

Малта | L-Ogħla Segretezza | Sigriet | Kunfidenzjali | Ristrett |

Top Secret | Secret | Confidential | Restricted ([1])

Нидерландия | Stg. ZEER GEHEIM | Stg. GEHEIM | Stg. CONFIDENTIEEL | Dep. VERTROUWELIJK |

Австрия | Streng Geheim | Geheim | Vertraulich | Eingeschränkt |

Полша | Ściśle tajne | Tajne | Poufne | Zastrzeżone |

Португалия | Muito Secreto | Secreto | Confidencial | Reservado |

Румъния | Strict secret de importanţă deosebită | Strict secret | Secret | Secret de serviciu |

Словения | STROGO TAJNO | TAJNO | ZAUPNO | INTERNO

Словакия | Prísne tajné | Tajné | Dôverné | Vyhradené |

Финландия | ERITTÄIN SALAINEN YTTERST HEMLIG | SALAINEN HEMLIG | LUOTTAMUKSELLINEN KONFIDENTIELL | KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG |

Швеция ([2]) | HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET | HEMLIG/SECRET HEMLIG | HEMLIG/CONFIDENTIAL HEMLIG | HEMLIG/RESTRICTED HEMLIG |

Обединено кралство | UK TOP SECRET| UK SECRET| (вж. бележка ([3]) по-долу)| UK OFFICIAL-SENSITIVE

([1]) За Малта могат да се използват равнозначно малтийските и английските означения.

([2]) Швеция: нивата на класификация за сигурност на горния ред се използват от органите в областта на отбраната, а на долния ред — от други органи.

([3]) Обединеното кралство вече не използва в националната си система ниво на класификация за сигурност „UK CONFIDENTIAL“. Обединеното кралство работи със и защитава класифицирана информация с ниво „CONFIDENTIEL UE/EU CONFIDENTIAL“ в съответствие с изискванията за сигурност за защита на ниво „UK SECRET“.

▼B

Допълнение B

СПИСЪК НА НАЦИОНАЛНИТЕ ОРГАНИ ПО СИГУРНОСТТА (НОС)

БЕЛГИЯ
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles

Tel. Secretariat: +32 25014542
Fax: +32 25014596
E-mail: nvo-ans@diplobel.fed.be

БЪЛГАРИЯ
Държавна комисия по сигурността на информацията/State Commission on Information Security
90 Cherkovna Str./ул. Черковна № 90
1505 Sofia/София 1505

Tel.: +359 29333600
Fax: +359 29873750
E-mail: dksi@government.bg
Website: www.dksi.bg

ЧЕШКАТА РЕПУБЛИКА
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

Tel.: +420 257283335
Fax: +420 257283110
E-mail: czech.nsa@nbu.cz
Website: www.nbu.cz

ДАНИЯ
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tel.: +45 33148888
Fax: +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø

Tel.: +45 33325566
Fax: +45 33931320

ЕСТОНИЯ
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tel.: +372 717 0019, +372 7170117
Fax: +372 7170213
E-mail: nsa@mod.gov.ee

ИРЛАНДИЯ
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2

Tel.: +353 14780822
Fax: +353 14082959

ГЪРЦИЯ
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλ.: +30 2106572045 (ώρες γραφείου)
+30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279
+30 2106577612

Hellenic National Defence General Staff
(HNDGS)
Counter Intelligence and Security Directorate
(NSA)
227-231 HOLARGOS
STG 1020 ATHENS

Tel.: +30 2106572045
+30 2106572009
Fax: +30 2106536279
+30 2106577612

ИСПАНИЯ
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Tel.: +34 913725000
Fax: +34 913725808
E-mail: nsa-sp@areatec.com

▼B

ГЕРМАНИЯ Bundesministerium des Innern Referat ÖS III 3 Alt-Moabit 101 D D-11014 Berlin Tel.: +49 30186810 Fax: +49 30186811441 E-mail: oesIII3@bmi.bund.de	**ФРАНЦИЯ** Secrétariat général de la défense et de la sécurité nationale Sous-direction Protection du secret (SGDSN/PSD) 51 Boulevard de la Tour-Maubourg 75700 Paris 07 SP Tel.: +33 171758177 Fax: +33 171758200
ХЪРВАТИЯ Ured Vijeća za nacionalnu sigurnost Croatian NSA Jurjevska 34 10000 Zagreb Croatia Tel.: +385 14681222 Fax: +385 14686049 www.uvns.hr	**ЛЮКСЕМБУРГ** Autorité nationale de Sécurité Boîte postale 2379 1023 Luxembourg Tel.: +352 24782210 central +352 24782253 direct Fax: +352 24782243
ИТАЛИЯ Presidenza del Consiglio dei Ministri D.I.S. - U.C.Se. Via di Santa Susanna, 15 00187 Roma Tel.: +39 0661174266 Fax: +39 064885273	**УНГАРИЯ** Nemzeti Biztonsági Felügyelet (National Security Authority of Hungary) H-1024 Budapest, Szilágyi Erzsébet fasor 11/B Tel.: +36 (1) 7952303 Fax: +36 (1) 7950344 Пощенски адрес: H-1357 Budapest, PO Box 2 E-mail: nbf@nbf.hu Website: www.nbf.hu
КИПЪР ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ Εθνική Αρχή Ασφάλειας (ΕΑΑ) Υπουργείο Άμυνας Λεωφόρος Εμμανουήλ Ροΐδη 4 1432 Λευκωσία, Κύπρος Τηλέφωνα: +357 22807569, +357 22807643, +357 22807764 Τηλεομοιότυπο: +357 22302351 Ministry of Defence Minister's Military Staff National Security Authority (NSA) 4 Emanuel Roidi street 1432 Nicosia Tel.: +357 22807569, +357 22807643, +357 22807764 Fax: +357 22302351 E-mail: cynsa@mod.gov.cy	**МАЛТА** Ministry for Home Affairs and National Security P.O. Box 146 MT-Valletta Tel.: +356 21249844 Fax: +356 25695321
ЛАТВИЯ National Security Authority Constitution Protection Bureau of the Republic of Latvia P.O.Box 286 LV-1001 Riga Tel.: +371 67025418 Fax: +371 67025454 E-mail: ndi@sab.gov.lv	**НИДЕРЛАНДИЯ** Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Postbus 20010 2500 EA Den Haag Tel.: +31 703204400 Fax: +31 703200733 Ministerie van Defensie Beveiligingsautoriteit Postbus 20701 2500 ES Den Haag Tel.: +31 703187060 Fax: +31 703187522

▼B

ЛИТВА Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority) Gedimino 40/1 LT-01110 Vilnius Tel.: +370 706 66701, +370 706 66702 Fax: +370 706 66700 E-mail: nsa@vsd.lt	**АВСТРИЯ** Informationssicherheitskommission Bundeskanzleramt Ballhausplatz 2 1014 Wien Tel.: +43 1531152594 Fax: +43 1531152615 E-mail: ISK@bka.gv.at
ПОЛША Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Tel.: +48 225857360 Fax: +48 225858509 E-mail: nsa@abw.gov.pl Website: www.abw.gov.pl	**СЛОВАКИЯ** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 850 07 Bratislava Tel.: +421 268692314 Fax: +421 263824005 Website: www.nbusr.sk
ПОРТУГАЛИЯ Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Tel.: +351 213031710 Fax: +351 213031711	**ФИНЛАНДИЯ** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Tel. +358 16055890 Fax: +358 916055140 E-mail: NSA@formin.fi
РУМЪНИЯ Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS National Registry Office for Classified Information) Str. Mureș nr. 4, sector 1 012275 București Tel.: +40 212245830 Fax: +40 212240714 E-mail: nsa.romania@nsa.ro Website: www.orniss.ro	**ШВЕЦИЯ** Utrikesdepartementet (Ministry for Foreign Affairs) UD-RS S-103 39 Stockholm Tel.: +46 84051000 Fax: +46 87231176 E-mail: ud-nsa@foreign.ministry.se
СЛОВЕНИЯ Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Tel.: +386 14781390 Fax: +386 14781399 E-mail: gp.uvtp@gov.si	**ОБЕДИНЕНОТО КРАЛСТВО** UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1A 2AS Tel. 1: +44 2072765645 Tel. 2: +44 2072765497 Fax: +44 2072765651 E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

▼B

Допълнение Г

СПИСЪК НА СЪКРАЩЕНИЯТА

Акроним	Значение
AQUA	Appropriately Qualified Authority (достатъчно квалифициран и компетентен орган)
BPS	Boundary Protection Services (мерки за защита на периметъра)
CAA	Crypto Approval Authority (орган за криптографско одобрение)
CCTV	Closed Circuit Television (вътрешна система за видеонаблюдение)
CDA	Crypto Distribution Authority (орган за разпределение на криптографски материали)
CFSP	Common Foreign and Security Policy (Обща външна политика и политика на сигурност — ОВПСС)
CIS	Communication and Information Systems handling EUCI (комуникационни и информационни системи, работещи с КИЕС)
Корепер	Committee of Permanent Representatives (Комитет на постоянните представители — Корепер)
CSDP	Common Security and Defence Policy (обща политика на ЕС за сигурност и отбрана — ОПСО)
DSA	Designated Security Authority (определен орган по сигурността)
ECSD	European Commission Security Directorate (Дирекция по сигурността на Европейската комисия)
EUCI	EU Classified Information (класифицирана информация на ЕС — КИЕС)
EUSR	EU Special Representative (специален представител на ЕС — СПЕС)
FSC	Facility Security Clearance (удостоверение за сигурност на съоръжение)
GSC	General Secretariat of the Council (Генерален секретариат на Съвета — ГСС)
IA	Information Assurance (осигуреност на информацията)
IAA	Information Assurance Authority (орган по осигуреността на информацията
IDS	Intrusion Detection System (алармена система против проникване)
IT	Information Technology (информационни технологии — ИТ)
NSA	National Security Authority (национален орган по сигурността — НОС)
PSC	Personnel Security Clearance (разрешение за достъп на персонала — РДП)
PSCC	Personnel Security Clearance Certificate (удостоверение за разрешение за достъп — УРД)
PSI	Programme/Project Security Instructions (инструкции за сигурност на програмата/проекта — ИСП)
SAA	Security Accreditation Authority (орган по акредитиране на сигурността)
SAB	Security Accreditation Board (Съвет по акредитиране на сигурността — САС)
SAL	Security Aspects Letter (приложение относно аспектите на сигурността — ПАС)
SecOPs	Security Operating Procedures (оперативни процедури за сигурност — ОПС)
SCG	Security Classification Guide (ръководство за класификация за сигурност)
SSRS	System-Specific Security Requirement Statement (декларация за специфичните изисквания за сигурност на системата)
TA	TEMPEST Authority (орган по Tempest)