IV

(Информация)

ИНФОРМАЦИЯ ОТ ИНСТИТУЦИИТЕ, ОРГАНИТЕ, СЛУЖБИТЕ И АГЕНЦИИТЕ НА ЕВРОПЕЙСКИЯ СЪЮЗ

ЕВРОПЕЙСКА СЛУЖБА ЗА ВЪНШНА ДЕЙНОСТ

РЕШЕНИЕ НА ВЪРХОВНИЯ ПРЕДСТАВИТЕЛ НА СЪЮЗА ПО ВЪПРОСИТЕ НА ВЪНШНИТЕ РАБОТИ И ПОЛИТИКАТА НА СИГУРНОСТ

от 19 април 2013 година

относно правилата за сигурност на Европейската служба за външна дейност

(2013/C 190/01)

ВЪРХОВНИЯТ ПРЕДСТАВИТЕЛ НА СЪЮЗА ПО ВЪПРОСИТЕ НА ВЪНШНИТЕ РАБОТИ И ПОЛИТИКАТА НА СИГУРНОСТ,

като взе предвид Решение 2010/427/ЕС на Съвета от 26 юли 2010 г. за определяне на организацията и функционирането на Европейската служба за външна дейност ([1]) („ЕСВД“),

като взе предвид становището на комитета, посочен в член 9, параграф 6 от решението на върховния представител от 15 юни 2011 г. относно правилата за сигурност на Европейската служба за външна дейност ([2]),

като взе предвид становището на комитета, посочен в член 10, параграф 1 от Решение 2010/427/ЕС на Съвета от 26 юли 2010 г. за определяне на организацията и функционирането на Европейската служба за външна дейност,

като има предвид, че:

(1) ЕСВД, като функционално независим орган на Европейския съюз (ЕС) следва да разполага с правила за сигурност, както е посочено в член 10, параграф 1 от Решение 2010/427/ЕС на Съвета;

(2) Върховният представител на Съюза по въпросите на външните работи и политиката на сигурност (наричан по-долу „върховният представител“ или „ВП“) следва да вземе решение относно правилата за сигурност на ЕСВД, които обхващат всички аспекти на сигурността, за да бъде ЕСВД в състояние да управлява ефективно рисковете по отношение на своя персонал, материални активи, информация и посетители и да изпълнява своите задължения за полагане на грижи в тази връзка;

(3) По-специално на персонала под отговорността на ЕСВД, материалните активи, включително комуникационни и информационни системи, информация и посетители на ЕСВД следва да се осигури такова равнище на защита, което съответства на най-добрите практики на Съвета, Комисията, държавите членки и по целесъобразност на международни организации;

(4) Правилата за сигурност на ЕСВД следва да спомогнат за установяването на по-съгласувана и всеобхватна обща рамка в Европейския съюз за защита на класифицирана информация на ЕС (наричана по-долу „КИЕС“), като се основават на и са във възможно най-голяма степен съгласувани с правилата за сигурност на Съвета на Европейския съюз (наричан по-долу „Съветът“) и разпоредбите за сигурност на Европейската комисия;

(5) ЕСВД, Съветът и Комисията са решени да прилагат равностойни стандарти за сигурност за защита на КИЕС;

(6) 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;

(7) Необходимо е да се установи организацията на сигурността в ЕСВД и разпределението на задачите, свързани със сигурността, в структурите на ЕСВД;

([1]) ОВ L 201, 03.08.2010 г., стр. 30.
([2]) ОВ C 304, 15.10.2011 г., стр. 5.

(8) Върховният представител следва да вземе предвид подходящия експертен опит в държавите членки, Генералния секретариат на Съвета и Комисията според необходимото;

(9) Върховният представител следва да предприеме всички подходящи мерки, необходими за прилагането на тези правила, с подкрепата на държавите членки, Генералния секретариат на Съвета и Комисията,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Цел и обхват

С настоящото решение се определят правилата за сигурност на Европейската служба за външна дейност (наричани по-долу „правилата за сигурност на ЕСВД“).

В съответствие с член 10, параграф 1 от Решение 2010/427/ЕС на Съвета от 26 юли 2010 г. за определяне на организацията и функционирането на Европейската служба за външна дейност, решението се прилага за персонала на ЕСВД и за целия персонал на делегациите на Съюза, независимо от техния административен статут или произход и с него се създава общата регулаторна рамка за ефективно управление на рисковете за персонала под отговорността на ЕСВД, както е посочено в член 2, за помещенията, материалните активи, информацията и посетителите на ЕСВД.

Член 2

Определения

За целите на настоящото решение се прилагат следните определения:

а) „Персонал на ЕСВД“ означава длъжностни лица и други служители на ЕСВД, включително служители от дипломатическите служби на държавите членки, назначени като срочно наети служители, командировани национални експерти, както е определено в член 6 от Решение 2010/427/ЕС на Съвета от 26 юли 2010 г. за определяне на организацията и функционирането на Европейската служба за външна дейност.

б) „Персонал под отговорността на ЕСВД“ означава персоналът на ЕСВД и целият персонал на делегациите на Съюза, независимо от техния административен статут или произход, а също така в контекста на настоящото решение — върховният представител и по целесъобразност друг персонал, работещ в помещенията на централата на ЕСВД.

в) „Лица на издръжка на персонала“ означава членовете на семействата на персонала под отговорността на ЕСВД в делегациите на Съюза, които са част от техните съответни домакинства, както е съобщено на министерството на външните работи на приемащата държава.

г) „Помещения на ЕСВД“ означава всички съоръжения на ЕСВД, включително сгради, офиси, зали и други зони, както и зони, в които се помещават комуникационни и информационни системи (включително тези, в които се работи с КИЕС), в които ЕСВД извършва постоянни или временни дейности.

д) „Интереси на ЕСВД в областта на сигурността“ означава персоналът под отговорността на ЕСВД, помещенията, лицата на издръжка, материалните активи, включително комуникационни и информационни системи, информация и посетители на ЕСВД.

е) „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.

Други определения са посочени в съответните приложения и в допълнение А.

Член 3

Задължение за полагане на грижи

1. Правилата за сигурност на ЕСВД са насочени към изпълнение на отговорностите на ЕСВД за полагане на грижи.

2. Задължението на ЕСВД за полагане на грижи включва добросъвестно предприемане на всички разумни стъпки за прилагане на мерките за сигурност с цел предотвратяване на предвидимо в разумни граници увреждане на интересите на ЕСВД в областта на сигурността.

То обхваща компоненти, свързани както със сигурността, така и с безопасността, включително тези, произтичащи от спешни ситуации или кризи, независимо от тяхното естество.

3. Като взема предвид отговорността за полагане на грижи на държавите членки, институциите или органите на ЕС и други страни с персонал в делегациите на Съюза и/или в помещения на делегациите на Съюза или отговорността, която се поема от ЕСВД, когато делегации на Съюза се разполагат в помещения на горепосочените други страни, ЕСВД сключва административни договорености с всеки от горепосочените субекти, в които се определят съответните роли и отговорности, задачи и механизми за сътрудничество.

Член 4

Физическа сигурност и сигурност на инфраструктурата

1. ЕСВД въвежда всички подходящи мерки за физическа сигурност (независимо дали постоянни или временни), включително разпоредби за контрол на достъпа за всички помещения на ЕСВД с цел защита на интересите на ЕСВД в областта на сигурността. Тези мерки се вземат предвид при проектирането и планирането на нови помещения или преди наемането на съществуващи помещения.

2. В трети държави ЕСВД също така предприема подходящи допълнителни мерки за физическа сигурност, постоянни или временни, за защита на своите интереси в областта на сигурността.

За тази цел могат да се налагат специални задължения или ограничения от съображения за сигурност на персонала под отговорността на ЕСВД и на лицата на тяхна издръжка за конкретен период и в конкретни зони.

3. Мерките, посочени в параграфи 1 и 2, съответстват на оценения риск.

Член 5

Защита на класифицирана информация

1. Защитата на КИЕС се урежда с изискванията, определени в настоящото решение, и по-специално приложение А. Притежателят на какъвто и да е елемент от КИЕС носи отговорност за защитата му по съответния начин.

2. ЕСВД гарантира, че достъп до класифицирана информация се предоставя само на лица, които отговарят на условията, определени в член 5 от приложение А.

3. Върховният представител също така определя условията, съгласно които местен нает персонал може да получи достъп до КИЕС в съответствие с правилата за защита на КИЕС, определени в приложение А към настоящото решение.

4. Дирекция „Сигурност“ на ЕСВД управлява база данни относно статуса за разрешенията за достъп до класифицирана информация на целия персонал под отговорността на ЕСВД и изпълнителите, с които ЕСВД е сключила договори.

5. Когато държавите членки въвеждат в структурите или мрежите на ЕСВД класифицирана информация, обозначена с национален гриф за сигурност, ЕСВД осигурява защита на тази информация в съответствие с изискванията, приложими към КИЕС на съответното ниво, съгласно посоченото в приложимите правила в съответствие с приложение А към настоящото решение.

6. Зони в ЕСВД, в които се съхранява информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, или с равностойно ниво на класификация за сигурност, се определят като зони за сигурност в съответствие с правилата в приложение А към настоящото решение и се одобряват от органа по сигурността на ЕСВД.

7. Процедурите за изпълнение на отговорностите на върховния представител в рамките на споразумения или административни договорености за обмен на КИЕС с трети държави или международни организации са описани в приложения А и А VI към настоящото решение.

Член 6

Свързани със сигурността инциденти и спешни случаи

1. С оглед да се гарантира навременно и ефективно реагиране на свързани със сигурността инциденти ЕСВД установява процес за докладване за такива инциденти и спешни случаи, който функционира денонощно и обхваща всички видове инциденти, свързани със сигурността, или заплахи за интересите на ЕСВД в областта на сигурността (например злополуки, конфликти, злонамерени действия, престъпни действия, отвличане на хора и вземане на заложници, спешни медицински случаи, инциденти с комуникационни и информационни системи, кибернетични атаки и др.).

2. Установяват се канали за контакти при спешни случаи между централата на ЕСВД, делегациите на Съюза, Съвета, Комисията, специалните представители на ЕС и държавите членки с цел осигуряване на подкрепа при управление на свързани със сигурността инциденти, засягащи персонала, и последиците от тях, включително планиране на действия при непредвидени ситуации.

3. Това управление на свързани със сигурността инциденти *inter alia* включва:

— процедури за ефективно подпомагане на процеса на вземане на решения във връзка със свързан със сигурността инцидент, засягащ персонала, включително решения, свързани с изтегляне на служители или прекратяване на мисия; както и

— политика и процедури за спасяване на служители — например в случай на изчезнали служители или при отвличане и вземане на заложници — като се вземат предвид конкретните отговорности на държавите членки, институциите на ЕС и ЕСВД в това отношение. Необходимостта от специфичен капацитет в рамките на управлението на такива операции в този контекст се проучва, като се вземат предвид ресурсите, които могат да се предоставят от държавите членки.

4. ЕСВД въвежда подходящи административни разпоредби за докладване на свързани със сигурността инциденти в делегациите на Съюза. По целесъобразност се информират държавите членки, Комисията и всеки друг съответен орган, както и съответните комитети по сигурността.

5. Процесите на управление на инциденти следва да подлежат на редовно провеждане на учения и преглед.

Член 7

Сигурност на комуникационните и информационните системи

1. ЕСВД защитава информацията, с която се работи в комуникационните и информационните системи („КИС“), срещу заплахи за поверителността, интегритета, наличността, автентичността и невъзможността за отказ.

2. Органът по сигурността на ЕСВД одобрява правила, политика на сигурност и програма за сигурността с цел защита на всички КИС, притежавани или обработвани от ЕСВД, както е определено в член 12, раздел I, параграф 1.

3. Правилата, политиката и програмата са съгласувани и тяхното прилагане се координира тясно с правилата, политиките и програмите на Съвета и Комисията и по целесъобразност с политиките на сигурност, прилагани от държавите членки.

4. Всички КИС, които обработват класифицирана информация, преминават през процес на акредитация. ЕСВД прилага система за управление на акредитацията за сигурност, като се консултира с Генералния секретариат на Съвета и Комисията.

5. Когато защитата на КИЕС, обработвана от ЕСВД, се осигурява с криптографски продукти, тези продукти се одобряват от органа на ЕСВД за криптографско одобрение по предложение на Комитета по сигурността на Съвета.

6. Органът по сигурността на ЕСВД, доколкото е необходимо, определя следните функции за гарантиране на информацията:

а) орган по осигуреността на информацията;

б) орган по TEMPEST;

в) орган за криптографско одобрение;

г) орган за разпределение на криптографски материали.

7. За всяка система органът по сигурността на ЕСВД определя следните функции:

а) орган по акредитиране на сигурността;

б) оперативен орган по осигуреността на информацията.

8. Разпоредбите за прилагане на настоящия член във връзка със защитата на КИЕС са посочени в приложения А и А IV.

Член 8

Нарушения на сигурността и излагане на риск на класифицирана информация

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 и/или политиките или насоките за сигурност, в които се определят необходимите мерки за тяхното прилагане, одобрени в съответствие с член 20, параграф 1.

2. До излагане на риск на КИЕС се стига, когато тя бъде изцяло или частично разкрита пред неоправомощени лица или субекти.

3. Всяко нарушение или подозрение за нарушение на сигурността и всяко излагане на риск или подозрение за излагане на риск на класифицирана информация се докладва незабавно на дирекция „Сигурност“ на ЕСВД, която предприема подходящи мерки, както е описано в приложение А.

4. На всяко лице, отговорно за нарушение на правилата за сигурност, установени в настоящото решение, или за излагане на риск на класифицирана информация, могат да бъдат наложени дисциплинарни мерки и/или да бъдат предприети мерки по съдебен път в съответствие с приложимите закони, правила и подзаконови актове, определени в член 11, параграф 3 от приложение А.

Член 9

Разследване на свързани със сигурността инциденти, нарушения и/или излагане на риск и корективни действия

1. Дирекция „Сигурност“ на ЕСВД, по целесъобразност подпомагана от експерти от държавите членки и/или от други институции на ЕС и при необходимост оправомощена от главния оперативен служител, извършва следните дейности:

а) извършва разследвания или проверки по целесъобразност:

i) когато е известно или когато има достатъчно основания да се предположи, че е била изложена на риск или изгубена класифицирана информация от значение за ЕСВД;

ii) при всяко действително или подозирано нарушение на сигурността или при други свързани със сигурността инциденти или заплахи за интересите на ЕСВД в областта на сигурността;

б) предприема необходими корективни действия в резултат на разследванията, когато и доколкото е целесъобразно.

2. Разследващите имат достъп до цялата необходима информация за провеждане на такива разследвания и получават пълна подкрепа от всички служби на ЕСВД в това отношение.

Разследващите могат да предприемат подходящи действия, за да защитят уликите по начин, който е пропорционален на сериозността на разследвания случай.

3. Когато достъпът до информация е свързан с лични данни, включително съдържащите се в комуникационните и информационните системи, този достъп е в съответствие с Регламент (ЕО) № 45/2001.

4. Когато е необходимо да се създаде база данни за разследвания, която ще съдържа лични данни, Европейският надзорен орган по защита на данните (ЕНОЗД) се уведомява в съответствие с горепосочения регламент.

Член 10

Управление на риска за сигурността

1. За да определи своите нужди, свързани с осигуряване на сигурността, ЕСВД разработва всеобхватна методология за оценка на риска за сигурността в тясно сътрудничество с дирекция „Сигурност“ на Комисията и по целесъобразност със Службата за сигурност на Генералния секретариат на Съвета.

2. Рисковете за интересите на ЕСВД в областта на сигурността се управляват като процес. Този процес е насочен към определяне на познатите рискове за сигурността, набелязване на мерки за сигурност, с които да се намалят тези рискове до приемливо равнище, и прилагане на мерки в съответствие с концепцията за защита в дълбочина. Ефективността на тези мерки и нивото на риск подлежат на постоянна оценка.

3. Посочените в настоящото решение роли, отговорности и задачи не засягат отговорността на всеки член на персонала под отговорността на ЕСВД; по-специално персоналът на ЕС на мисии в трети държави трябва да проявява благоразумие и трезва преценка по отношение на собствената си безопасност и сигурност и да спазва всички приложими правила, разпоредби, процедури и указания за сигурност.

4. ЕСВД предприема всички разумни мерки за гарантиране на защитата на своите интереси в областта на сигурността и за предотвратяване на предвидимо в разумни граници тяхно увреждане в тази връзка.

5. Мерките за сигурност в ЕСВД 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 заплахата, включително оценената заплаха на местно ниво от злонамерени и/или престъпни действия, включително шпионаж, саботаж и тероризъм.

Член 11

Обучение и повишаване на осведомеността по въпросите на сигурността

1. Органът по сигурността на ЕСВД гарантира, че се разработват и изпълняват подходящи програми за повишаване на осведомеността и програми за обучение по въпросите на сигурността, както и че членовете на персонала под отговорността на ЕСВД, а когато е целесъобразно — и лицата на тяхна издръжка, получават необходимите инструкции и обучение в съответствие с рисковете в тяхното място на работа или пребиваване.

2. Преди да им бъде предоставен достъп до КИЕС и периодично след това членовете на персонала биват информирани за задължението си да опазват КИЕС в съответствие с правилата съгласно член 5 и декларират, че са запознати с тези задължения.

Член 12

Организация на сигурността в ЕСВД

Раздел 1.

Общи разпоредби

1. Главният оперативен служител (ГОС) е органът по сигурността на ЕСВД. В това си качество ГОС гарантира по-специално, че:

а) мерките за сигурност се координират при необходимост с компетентните органи на държавите членки, Генералния секретариат на Съвета и с Комисията и, ако е уместно, с трети държави или международни организации по отношение на всички въпроси, свързани със сигурността, които са от значение за дейността на ЕСВД, включително по отношение на естеството на заплахите за интересите на ЕСВД в областта на сигурността и средствата за защита срещу тези заплахи;

б) аспектите, свързани със сигурността, са изцяло взети предвид от самото начало за всички дейности на ЕСВД;

в) достъп до класифицирана информация се предоставя само на лица, които отговарят на условията, определени в член 5 от приложение А;

г) създава се система за регистриране, с която се гарантира, че информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо се обработва в съответствие с настоящото решение в рамките на ЕСВД, когато се предоставя на държавите — членки на ЕС, институции, органи или агенции на ЕС или други оправомощени получатели. Поддържа се отделен регистър на цялата КИЕС, която се предоставя от ЕСВД на трети държави и международни организации, както и на цялата класифицирана информация, която се получава от трети държави или международни организации;

д) проверките на сигурността, посочени в член 15, се извършват;

е) за всяко действително или подозирано нарушение на сигурността се провежда разследване, включително при действително или подозирано излагане на риск или загуба на класифицирана информация, която се съхранява или е с произход от ЕСВД, и че към съответните органи за сигурност се отправя искане за съдействие при такива разследвания;

ж) за да се даде своевременен и ефективен отговор на инциденти, свързани със сигурността, се създават подходящи планове и механизми за управление на инцидентите и последиците от тях;

з) в случай на неспазване на настоящото решение от страна на физически лица се приемат подходящи мерки;

и) въвеждат се подходящи материални и организационни мерки за защита на интересите на ЕСВД в областта на сигурността.

В това отношение в консултация с изпълнителния генерален секретар ГОС извършва следните действия:

— определя категорията на сигурност на делегациите в консултация с Комисията,

— взема решение след консултация с ВП кога персоналът на делегациите следва да се евакуира, ако свързаната със сигурността ситуация налага това,

— по целесъобразност взема решение относно мерките, които следва да се предприемат за защита на лицата на издръжка на персонала, като отчита договореностите с институциите на ЕС, както е посочено в член 3, параграф 3;

— одобрява политиката за криптографска комуникация и по-специално програмата за инсталиране на криптографски продукти и механизъм.

2. Управителният директор на администрацията и финансите, ръководителят на дирекция „Сигурност“ на ЕСВД и по целесъобразност управителният директор на службата за реагиране на кризи и оперативният координатор подпомагат ГОС в изпълнението на тази задача.

3. В качеството си на орган по сигурността на ЕСВД ГОС може да делегира задачи в това отношение по целесъобразност.

4. Всеки ръководител на отдел/звено отговаря за правилата за изпълнение във връзка със защитата на КИЕС в рамките на своя отдел/звено.

Макар да остава отговорен, както е посочено по-горе, всеки ръководител на отдел/звено определя персонал, който изпълнява функциите на координатор по сигурността на отдела, чиито ресурси са пропорционални на обема КИЕС, обработвана от съответния отдел/звено.

Когато и доколкото е целесъобразно координаторите по сигурността на отделите съдействат на и подпомагат ръководителя на своя отдел/звено при изпълнението на задачи, свързани със сигурността, например:

а) разработване на допълнителни изисквания за сигурността, които са подходящи за специфичните нужди на отдела/звеното;

б) осигуряване на периодични инструкции за сигурността на членовете на съответния отдел/звено;

в) гарантиране, че принципът „необходимост да се знае“ се спазва в съответния отдел/звено;

г) поддържане на актуален списък на кодове и ключове за сигурност;

д) поддържане на процедури за сигурност и мерки за сигурност;

е) докладване за всички нарушения на сигурността и/или излагане на риск на КИЕС на своя директор и на дирекция „Сигурност“;

ж) инструктаж за опазване на тайна на персонала, който вече не е нает от ЕСВД;

з) представяне на редовни доклади съгласно своята йерархия относно въпроси, свързани със сигурността на отдела/департамента;

и) осъществяване на контакт с дирекция „Сигурност“ на ЕСВД относно въпроси, свързани със сигурността.

Всички дейности или въпроси, които могат да окажат въздействие върху сигурността, се съобщават своевременно на дирекция „Сигурност“ на ЕСВД.

5. Всеки ръководител на делегация на Съюза отговаря за изпълнение на всички мерки, свързани със сигурността на делегацията на Съюза.

Раздел 2.

Дирекция „Сигурност“ на ЕСВД

1. ЕСВД разполага с дирекция „Сигурност“. Тази дирекция:

а) управлява, координира, осъществява надзор над и/или изпълнява всички мерки за сигурност във всички помещения под отговорността на ЕСВД, в централата, в рамките на ЕС и в трети държави;

б) гарантира съгласуваност и последователност с настоящото решение и с разпоредбите за изпълнение на всяка дейност, която може да окаже въздействие върху защитата на интересите на ЕСВД в областта на сигурността;

в) е главният съветник на ВП, изпълнителния генерален секретар и ГОС по всички въпроси, свързани със сигурността;

г) се подпомага от компетентните служби на държавите членки в съответствие с член 10, параграф 3 от Решение 2010/427/ЕС на Съвета за определяне на организацията и функционирането на ЕСВД, дирекция „Сигурност“;

д) подпомага дейностите на органа по акредитиране на сигурността на ЕСВД, като извършва оценки на физическата сигурност на общата среда за сигурност (GSE) / локалната среда за сигурност (LSE) на комуникационните и информационните системи, в които се обработва КИЕС, и на помещенията, за които следва да се издадат разрешения за обработване и съхранение на КИЕС.

2. Ръководителят на дирекция „Сигурност“ на ЕСВД отговаря за:

а) гарантиране на общата защита на интересите на ЕСВД в областта на сигурността;

б) изготвяне, преглед и актуализиране на правилата за сигурност, както и координиране на мерките за сигурност с компетентните органи на държавите членки и по целесъобразност с компетентните органи на трети държави и международни организации, свързани с ЕС чрез споразумения и/или договорености за сигурност;

в) подпомагане на процедурите на Комитета по сигурността на ЕСВД, както е предвидено в член 14, параграф 1 от настоящото решение;

г) осъществяване на контакт с всички партньори или органи, различни от изброените в буква б) по-горе, относно въпроси, свързани със сигурността, когато е целесъобразно;

д) приоритизиране и изготвяне на предложения за управление на бюджета за сигурността в централата и делегациите на Съюза.

3. Ръководителят на дирекция „Сигурност“ на ЕСВД извършва следните дейности:

а) гарантира, че нарушенията на сигурността и излагането на риск на класифицирана информация се записват и че се предприемат разследвания, където и когато е необходимо;

б) среща се редовно и при необходимост с директора по сигурността на Генералния секретариат на Съвета и директора на дирекция „Сигурност“ на Комисията, за да обсъждат области от общ интерес.

4. Дирекция „Сигурност“ на ЕСВД осъществява контакт и поддържа тясно сътрудничество със:

— отделите, които отговарят за сигурността в министерствата на външните работи на държавите членки;

— националните органи по сигурността (НОС) и/или други компетентни органи по сигурността на държавите членки, за да получи съдействие от тях по отношение на информацията, от която се нуждае, за да оцени опасностите и заплахите, пред които може да е изправена ЕСВД, нейният персонал, нейните дейности, активи и ресурси, както и класифицирана информация на нейното обичайно място на извършване на дейност;

— компетентните органи по сигурността на държавите членки или приемащите държави, на територията на които ЕСВД може да извършва дейностите си по отношение на въпроси, свързани със защитата на нейния персонал, дейности, активи и ресурси, както и класифицирана информация, докато се намира на тяхна територия;

— Службата за сигурност на Генералния секретариат на Съвета и дирекция „Сигурност“ на ГД „Човешки ресурси и сигурност“ на Комисията и по целесъобразност отделите за сигурност на другите институции, органи и агенции на ЕС;

— отделите по сигурността на трети държави или международни организации с оглед полезна координация, и

— НОС на държавите членки по отношение на въпроси, свързани със защитата на КИЕС.

Раздел 3.

Делегации на Съюза

1. Всеки ръководител на делегация на Съюза отговаря за прилагането и управлението на местно равнище на всички мерки, свързани със защитата на интересите на ЕСВД в областта на сигурността, в рамките на помещенията и компетентността на делегациите на Съюза.

При необходимост, в консултация с компетентните органи на приемащите държави, ръководителят предприема всички разумни и практични мерки, за да гарантира въвеждане на подходящи материални и организационни мерки за постигане на тази цел.

Ръководителят на делегацията по целесъобразност изготвя процедури за сигурност с цел защита на лицата на издръжка от персонала, както е определено в член 2, буква в), като взема предвид всички административни договорености, посочени в член 3, параграф 3. Ръководителят на делегацията докладва ежегодно за всички свързани със сигурността въпроси в рамките на своя мандат на ръководителя на дирекция „Сигурност“ на ЕСВД.

Ръководителят се подпомага в тези задачи от дирекция „Сигурност“ на ЕСВД, от персонала на ЕСВД в делегацията, който извършва специални задачи и функции, свързани със сигурността, и при необходимост — от специален командирован персонал по сигурността.

2. Освен това ръководителят на делегацията извършва следните дейности:

— създава подробни планове за сигурност и действия при непредвидени ситуации за делегациите въз основа на общи и стандартни оперативни процедури;

— внедрява ефективна денонощна система за управление на свързани със сигурността инциденти и спешни случаи в рамките на обхвата на операциите на делегацията;

— гарантира, че целият персонал, включен в делегацията, е застрахован съобразно условията на съответното място;

— гарантира, че сигурността е част от уводното обучение на делегацията на Съюза, през което преминават всички служители, включени в делегацията, преди и при пристигане в делегацията; както и

— гарантира изпълнение на всички препоръки, които се отправят в резултат на оценки на сигурността, и представя редовни писмени доклади за тяхното изпълнение и по други въпроси, свързани със сигурността, на органа по сигурността на ЕСВД.

3. Макар че продължава да носи отговорност и да се отчита за защитата на управлението на сигурността, както и за гарантиране на корпоративна устойчивост, ръководителят на делегацията може да делегира изпълнението на своите задачи, свързани със сигурността, на координатора по сигурността на делегацията („КСД“), като тази длъжност се изпълнява от заместник-ръководителя на делегацията или, ако не бъде назначено такова лице, от друго подходящо лице.

По-специално на КСД могат да бъдат поверени следните отговорности:

— да осъществява контакт по въпроси, свързани със сигурността, с компетентните органи на приемащата държава и съответните партньори в посолствата и дипломатическите мисии на държавите членки;

— да прилага подходящи процедури за управление на сигурността, свързани с интересите на ЕСВД в областта на сигурността, включително защитата на КИЕС;

— да инструктира персонала относно правилата за сигурност, които се прилагат спрямо него, и относно конкретните рискове в приемащата държава;

— да представя искания пред дирекция „Сигурност“ на ЕСВД относно длъжностите, които изискват разрешение за достъп на персонала (РДП), и

— да информира редовно ръководителя на делегацията, регионалния служител по сигурността (РСС) и дирекция „Сигурност“ на ЕСВД по отношение на инциденти или развития в областта, която са от значение за защитата на интересите на ЕСВД в областта на сигурността.

4. Ръководителят на делегацията може да делегира свързани със сигурността задачи от административно или техническо естество на административния ръководител и други членове на персонала на делегацията.

5. Делегацията на Съюза се подпомага от регионален служител по сигурността (РСС). РСС изпълняват задачите, определени по-долу, в делегациите в рамките на всяка от своите съответни географски области на отговорност.

При определени обстоятелства, когато това се налага от ситуацията по отношение на сигурността, за конкретна делегация може да бъде назначен специален РСС като постоянно пребиваващ служител.

От даден РСС може да бъде поискано да се премести в област извън настоящата му област на отговорност, включително централата в Брюксел, или дори да поеме длъжност, свързана с постоянно пребиваване, във връзка със съответната ситуация по отношение на сигурността в дадена държава и съгласно изискванията на дирекция „Сигурност“ на ЕСВД.

6. РСС са под прекия йерархичен контрол на дирекция „Сигурност“ на ЕСВД и под прекия функционален и административен контрол на съответния ръководител на делегация. Те подпомагат ръководителя на делегацията и персонала на делегацията при организиране и изпълнение на всички материални, организационни и процедурни мерки, свързани със сигурността на целия персонал на делегацията, независимо от техния административен произход.

7. РСС предоставят съвети и помощ на ръководителя на делегацията и на персонала на делегацията. По целесъобразност, и по-специално когато специален РСС е постоянно пребиваващ служител, той може да подпомага делегация на Съюза в управлението и прилагането на мерки за сигурност, включително в изготвянето на договори за сигурност, управлението на акредитациите и разрешенията за достъп.

Член 13

Операции по общата политика за сигурност и отбрана и специални представители на ЕС

Дирекция „Сигурност“ на ЕСВД подпомага и съветва директора на Дирекцията за управление и планиране при кризи (ДУПК), генералния директор на Военния секретариат на ЕС (ВСЕС), командващия гражданските операции, който ръководи структурата „Способности за планиране и провеждане на граждански операции“ (СППГО), и командващите военните операции на ЕС относно свързаните със сигурността аспекти на операциите по общата политика за сигурност и отбрана, както и специалните представители на ЕС относно свързаните със сигурността аспекти на техния мандат, в допълнение към специфичните съществуващи разпоредби в това отношение в съответните политики, приети от Съвета.

Член 14

Комитет по сигурността на ЕСВД

1. С настоящото решение се създава Комитет по сигурността на ЕСВД.

Той се председателства от ГОС или специално определен делегат и заседава по указания на председателя или по искане на някой от неговите членове. Дирекция „Сигурност“ на ЕСВД подпомага председателя в тази функция и при необходимост осигурява административна помощ за процедурите на комитета.

2. Съвместният комитет на ЕСВД се състои от представители на:

— всяка държава членка;

— Службата за сигурност на Генералния секретариат на Съвета;

— дирекция „Сигурност“ на Генерална дирекция „Човешки ресурси и сигурност“ на Комисията.

Делегациите на държавите членки в Комитета по сигурността на ЕСВД могат да се състоят от членове на:

— националния орган по сигурността и/или определения орган по сигурността,

— отделите, които отговарят за сигурността в министерствата на външните работи.

3. Представителите на комитета могат да бъдат придружавани и консултирани от експерти, когато това бъде счетено за необходимо. Представителите на други институции, агенции или органи на ЕС могат да бъдат канени да присъстват, когато се обсъждат въпроси от значение за тяхната сигурност.

4. Без да се засяга параграф 5 по-долу, Комитетът по сигурността на ЕСВД подпомага ЕСВД чрез консултации по всички въпроси, свързани със сигурността, които са от значение за дейностите на ЕСВД, централата и делегациите на Съюза.

По-специално, без да се засяга параграф 5 по-долу, Комитетът по сигурността на ЕСВД:

а) бива консултиран относно:

— политики за сигурност, насоки, концепции или други документи за методология, свързани със сигурността, по-специално по отношение на защитата на класифицирана информация и мерките, които следва да се предприемат в случай на неспазване на правилата за сигурност от страна на персонала на ЕСВД;

— технически аспекти на сигурността, които могат да повлияят на решението на ВП да представи препоръка на Съвета за започване на преговори по споразумения относно сигурността на информацията, както е посочено в член 10, параграф 1, буква а) от приложение А;

— изменения на настоящото решение.

б) може да бъде консултиран или информиран по целесъобразност относно въпроси, свързани със сигурността на персонала и активите в рамките на централата на ЕСВД и делегациите на Съюза, без да се засяга член 3, параграф 3;

в) бива информиран за всички случаи на изложена на риск или изгубена КИЕС, настъпили в рамките на ЕСВД.

5. Всички промени на правилата, свързани със защитата на КИЕС, които се съдържат в настоящото решение и приложение А към него, изискват единодушно положително становище от държавите членки, представени в Комитета по сигурността на ЕСВД. Такова единодушно положително становище се изисква и преди:

— да се встъпи в преговори относно административни договорености, както е посочено в член 10, параграф 1, буква б) от приложение А;

— да се предостави класифицирана информация в извънредните случаи, посочени в параграфи 9, 11 и 12 от приложение А VI;

— да се поеме отговорността на създател на информация в случаите, посочени в член 10, параграф 4, последно изречение, от приложение А.

Когато се изисква единодушно положително становище, това условие се счита за изпълнено, когато делегациите на държавите членки не изразят възражения по време на процедурата на комитета.

6. Комитетът по сигурността на ЕСВД напълно отчита политиките и насоките за сигурност, които се прилагат от Съвета и Комисията.

7. Комитетът по сигурността на ЕСВД получава списъка с годишни проверки на ЕСВД и докладите от проверките, след като бъдат финализирани.

8. Организация на заседанията:

— Комитетът по сигурността на ЕСВД заседава не по-малко от два пъти годишно. Допълнителни заседания на съвета, било то в пълната му конфигурация, в рамките на НОС/ООС или във формата за сигурност на министерствата на външните работи, могат да се организират от председателя или да бъдат поискани от членовете на комитета.

— Комитетът по сигурността на ЕСВД организира дейността си по такъв начин, че да може да отправя препоръки в специфични области на сигурността. При необходимост той може да установява и други експертни подобласти. Той изготвя мандата за тези експертни подобласти и получава доклади от тях относно техните дейности.

— Дирекция „Сигурност“ на ЕСВД носи отговорност за изготвянето на точките за обсъждане. Председателят подготвя предварителен дневен ред за всяко заседание. Членовете на комитета могат да предлагат допълнителни точки за обсъждане.

Член 15

Проверки на сигурността

1. Органът по сигурността на ЕСВД гарантира редовно извършване на проверки на сигурността в рамките на централата на ЕСВД и делегациите на Съюза с цел да се оцени адекватността на мерките за сигурност и да се провери дали отговарят на настоящото решение. Дирекция „Сигурност“ на ЕСВД може по целесъобразност да определи експерти за оказване на принос, които да участват в проверките на сигурността в агенциите и органите на ЕС, създадени съгласно дял V, глава 2 от Договора за ЕС.

2. Проверките на сигурността на ЕСВД се извършват под ръководството на дирекция „Сигурност“ на ЕСВД и по целесъобразност с подкрепата на експерти по сигурността, представляващи други институции на ЕС или държави членки, по-специално в контекста на договореностите, посочени в член 3, параграф 3.

3. При необходимост ЕСВД може да използва експертния опит на държавите членки, Генералния секретариат на Съвета и Комисията.

При необходимост в проверката на сигурността на делегация на Съюза могат да бъдат поканени да участват съответните експерти по сигурността, участващи в мисии на държави членки в трети държави, и/или представители на дипломатическите отдели по сигурността на държавите членки.

4. Разпоредбите за прилагане на настоящия член във връзка със защитата на КИЕС са посочени в приложение А III.

Член 16

Посещения за оценка

Организират се посещения за оценка с цел оценяване на ефективността на въведените мерки за сигурност в трета държава или международна организация във връзка със защитата на КИЕС, която се обменя съгласно административна договореност, както е посочено в член 10, параграф 1, буква б) от приложение А.

Дирекция „Сигурност“ на ЕСВД може да определи експерти за оказване на принос, които да участват в проверките на сигурността в трети държави или международни организации, с които ЕС е сключил споразумение относно сигурността на информацията, както е посочено в член 10, параграф 1, буква а) от приложение А.

Член 17

Планиране на непрекъснатост на дейностите

Дирекция „Сигурност“ на ЕСВД подпомага ГОС в управлението на свързаните със сигурността аспекти на процесите за непрекъснатост на дейностите на ЕСВД като част от общото планиране за непрекъснатост на дейностите на ЕСВД.

Член 18

Насоки при пътуване за мисии извън ЕС

Дирекция „Сигурност“ на ЕСВД гарантира наличието на насоки при пътуване по отношение на мисии на персонал под отговорността на ЕСВД извън ЕС, като се използват ресурсите на всички съответни служби на ЕСВД — по-специално SITROOM, INTCEN, географските отдели и делегациите на Съюза.

При поискване и като използва горепосочените ресурси, дирекция „Сигурност“ на ЕСВД предоставя специфични насоки при пътуване по отношение на мисии на персонал под отговорността на ЕСВД в трети държави, които се характеризират с високо ниво на риск или увеличено ниво на риск.

Член 19

Здраве и безопасност

Правилата за сигурност на ЕСВД допълват правилата на ЕСВД за защита на здравето и безопасността, приети от върховния представител.

Член 20

Изпълнение и преглед

1. По целесъобразност след консултация с Комитета по сигурността на ЕСВД органът по сигурността на ЕСВД одобрява политики или насоки за сигурност, в които се определят всички необходими мерки за прилагане на тези правила в ЕСВД и изгражда необходимия капацитет, който обхваща всички аспекти на сигурността, в тясно сътрудничество с компетентните органи по сигурността на държавите членки и с подкрепата на съответните служби на институциите на ЕС.

2. В съответствие с член 4, параграф 5 от Решение 2010/427/ЕС на Съвета от 26 юли 2010 г. за определяне на организацията и функционирането на Европейската служба за външна дейност, при необходимост могат да се използват преходни договорености посредством споразумения за нивото на обслужване със съответните служби на Генералния секретариат на Съвета и Комисията.

3. ВП гарантира обща съгласуваност при прилагането на настоящото решение и извършва преглед на тези правила за сигурност.

4. Правилата за сигурност на ЕСВД следва да се прилагат в тясно сътрудничество с компетентните органи по сигурността на държавите членки, със Службата за сигурност на Генералния секретариат на Съвета и дирекция „Сигурност“ на ГД „Човешки ресурси и сигурност“ на Комисията.

5. ЕСВД гарантира, че всички аспекти на процеса по сигурността се вземат предвид в рамките на системата на ЕСВД за реагиране при кризи.

6. ГОС, в качеството си на орган по сигурността, и ръководителят на дирекция „Сигурност“ на ЕСВД гарантират прилагането на настоящото решение.

Член 21

Замяна на предходни решения

1. С настоящото решение се отменя и заменя решението на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност от 15 юни 2011 г. относно правилата за сигурност на Европейската служба за външна дейност ([1]).

2. С настоящото решение се отменя и заменя решението на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност от 23 февруари 2011 г. за създаване и определяне на задачи на делегирания орган по сигурността на Европейската служба за външна дейност.

Член 22

Заключителни разпоредби

Настоящото решение влиза в сила от датата на подписването му.

Настоящото решение се публикува в *Официален вестник на Европейския съюз.*

Компетентните органи в ЕСВД надлежно и своевременно уведомяват всички служители, които попадат в обхвата на настоящото решение и приложенията към него, за съдържанието, влизането в сила и всички последващи изменения на същите.

Съставено в Брюксел на 19 април 2013 година.

Върховен представител

C. ASHTON

([1]) ОВ C 304, 15.10.2011 г., стр. 7.

ПРИЛОЖЕНИЕ А

ПРИНЦИПИ И СТАНДАРТИ ЗА ЗАЩИТА НА КИЕС

Член 1

Цел, приложно поле и определения

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

2. Тези основни принципи и минимални стандарти се прилагат по отношение на ЕСВД и персонала под отговорността на ЕСВД, както се посочва и определя съответно в членове 1 и 2 от настоящото решение.

Член 2

Определение на КИЕС, нива на класификация за сигурност и грифове за сигурност

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. Всяка КИЕС се класифицира на някое от следните нива:

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

в) CONFIDENTIEL UE/EU CONFIDENTIAL: информация и материали, чието неразрешено разкриване 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, чието неразрешено разкриване 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. ЕСВД гарантира, че КИЕС е подходящо класифицирана, ясно обозначена като класифицирана информация и запазва нивото си на класификация само докато това е необходимо.

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

3. След консултация с Комитета по сигурността на ЕСВД съгласно член 14, параграф 5 от настоящото решение органът по сигурността на ЕСВД одобрява политика на сигурност относно създаване 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 ЕСВД класифицирана информация, обозначена с национален гриф за сигурност, ЕСВД осигурява защита на тази информация в съответствие с изискванията, приложими към КИЕС на съответното ниво, съгласно таблицата на съответствията на нивата на класификация за сигурност, съдържаща се в допълнение Б към Решение 2011/292/ЕС на Съвета от 31 март 2011 г. относно правилата за сигурност за защита на класифицирана информация на ЕС.

ЕСВД прилага подходящи процедури за поддържане на точен регистър относно създателя на

— класифицираната информация, която ЕСВД получава; както и

— изходния материал, включен в класифицираната информация с произход от ЕСВД.

Комитетът по сигурността на ЕСВД се уведомява за тези процедури.

4. За големи количества КИЕС или масиви от КИЕС може да се наложи защита на по-високо ниво на класификация за сигурност от това на отделните компоненти.

Член 5

Сигурност, свързана с персонала, при обработка на класифицирана информация на ЕС

1. Сигурността, свързана с персонала, означава прилагане на мерки за гарантиране, че достъп до КИЕС се предоставя единствено на лица, които:

— е необходимо да знаят,

— за достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, са преминали проучване за надеждност за съответното ниво или са съответно надлежно оправомощени по силата на своите функции, в съответствие с националните законови и подзаконови актове; както 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.

3. Всички лица се информират за своите отговорности за защита на КИЕС в съответствие с настоящото решение и декларират, че са запознати с тях, преди да получат достъп до КИЕС и периодично след това.

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

Член 6

Физическа сигурност на класифицирана информация на ЕС

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 въз основа 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 8, 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 A II и се одобряват от органа по сигурността на ЕСВД.

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 A II.

Член 7

Управление на класифицирана информация

1. Управлението на класифицирана информация представлява прилагане на административни мерки за контрол на КИЕС през жизнения ѝ цикъл в допълнение към мерките, предвидени в членове 5, 6 и 8, като по този начин се съдейства за възпиране, разкриване и възстановяване на такава информация при умишлено или случайно излагане на риск или загуба. Тези мерки се отнасят по-конкретно до създаването, регистрирането, копирането, превода, преноса, работата със, съхранението 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. Компетентните органи в ЕСВД създават регистрационна система за тази цел. Информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се регистрира в специални регистри.

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

4. КИЕС се предава между 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 7, параграф 5 от настоящото решение, и съгласно ясно определени оперативни процедури за сигурност (ОПС);

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

i) на електронен носител (например USB памет, компактдиск, твърд диск), защитен чрез криптографски продукти, одобрени в съответствие с член 7, параграф 5 от настоящото решение; или

ii) във всички останали случаи — в съответствие с предписанията на органа по сигурността на ЕСВД съгласно съответните защитни мерки, установени в приложение A III, раздел V.

5. Разпоредбите за изпълнение на настоящия член се съдържат в приложение A III.

Член 8

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.

2. „Комуникационна и информационна система“ (КИС) означава всяка система, даваща възможност за работа с информация в електронна форма. Една комуникационна и информационна система обхваща всички активи, необходими за нейното функциониране, включително инфраструктура, организация, персонал и информационни ресурси. Настоящото приложение се прилага по отношение на всяка КИС на ЕСВД, която работи с КИЕС.

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

4. Всички КИС, които работят с КИЕС, 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. КИС за работа с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и по-високо са защитени по начин, който да не допуска информацията да се излага на риск от неумишлени електромагнитни излъчвания („мерки за сигурност по TEMPEST“).

6. Когато защитата на КИЕС се осигурява от криптографски продукти, такива продукти се одобряват в съответствие с член 7, параграф 5 от настоящото решение.

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 A IV.

8. В съответствие с член 7, параграф 6 от настоящото решение се създават следните функции във връзка с ОИ в необходимата степен:

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. В съответствие с член 7, параграф 7 от настоящото решение за всяка система се създава:

а) орган по акредитиране на сигурността (ОАС);

б) оперативен орган по ОИ.

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

Член 9

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 договори и през целия жизнен цикъл на класифицирани договори. Като общо правило тези договори не включват достъп до информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET.

2. ЕСВД 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 за сигурност на информацията или административна договореност в съответствие с член 10, параграф 1 от приложение A.

3. ЕСВД, 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. Той гарантира спазване на такива минимални стандарти чрез съответния НОС/ООС.

4. Изпълнители или подизпълнители, регистрирани в дадена държава членка и участващи в класифицирани договори за изпълнение или подизпълнение, съгласно които се изисква работа със и съхранение на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET в рамките на техните структури, било то при изпълнението на тези договори или по време на преговорите за сключването на договори, разполагат с удостоверение за сигурност на структура (УСС) на съответното ниво на класификация за сигурност, което се предоставя от НОС, ООС или друг компетентен орган по сигурността на съответната държава членка.

5. Изпълнителският или подизпълнителският 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, разполага с РДП, издадено от съответния национален орган по сигурността (НОС), определен орган по сигурността (ООС) или друг компетентен орган по сигурността, в съответствие с националните законови и подзаконови актове и минималните стандарти, определени в приложение A I.

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

Член 10

Обмен на класифицирана информация с трети държави и международни организации

1. ЕСВД може да извършва обмен на КИЕС с трети държави или международни организации само когато:

а) има влязло в сила споразумение за сигурност на информацията между ЕС и тази трета държава или международна организация, сключено в съответствие с член 37 от Договора за ЕС и член 218 от ДФЕС; или

б) се прилага административна договореност между ВП и компетентните органи по сигурността на тази трета държава или международна организация, касаеща обмен на информация с ниво на класификация за сигурност, което по принцип не е по-високо от RESTREINT UE/EU RESTRICTED, сключена в съответствие с процедурата съгласно член 14, параграф 5 от настоящото решение; или

в) се прилага рамково или *ad hoc* споразумение за участие между ЕС и тази трета държава в контекста на операция по управление на кризи по линия на ОПСО, сключено в съответствие с член 37 от Договора за ЕС и член 218 от ДФЕС,

и условията в този инструмент са спазени.

Изключенията към общото правило по-горе са описани в приложение A VI, раздел V.

2. Административните договорености, посочени в параграф 1, буква б), 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.

Информацията, която се обменя въз основа на споразуменията, посочени в параграф 1, буква в), е ограничена до информация относно операции по линия на ОПСО, в които участва въпросната трета държава въз основа на тези споразумения и съгласно съдържащите се в тях разпоредби.

3. Организират се посещения за оценка в трети държави или международни организации, както е описано в член 16 от настоящото решение, с цел да се установи ефективността на мерките за сигурност за защита на КИЕС, която се обменя.

4. Решението да се предостави на трета държава или международна организация КИЕС, съхранявана от ЕСВД, се взема 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 ЕС.

ЕСВД иска писмено съгласие от всяка единица, която е предоставила класифицирана информация като изходен материал за КИЕС, създадена от ЕСВД, за да установи дали няма възражения за предоставянето на тази информация.

Ако класифицираната информация, чието предоставяне се иска, не е създадена от ЕСВД, ЕСВД най-напред иска писмено съгласие за нейното предоставяне от създателя на информацията.

Ако обаче ЕСВД не може да установи създателя на информацията, органът по сигурността на ЕСВД поема отговорността на създателя след като получи единодушно положително становище от държавите членки, представени в Комитета по сигурността на ЕСВД.

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

Член 11

Нарушаване на сигурността и излагане на риск на класифицирана информация

1. Всяко нарушение или подозрение за нарушение на сигурността и всяко излагане на риск или подозрение за излагане на риск на класифицирана информация се докладва незабавно на дирекция „Сигурност“ на ЕСВД, която по целесъобразност уведомява дирекция „Сигурност“ на ГД „Човешки ресурси и сигурност“ на Комисията и Службата за сигурност на Генералния секретариат на Съвета, съответната държава членка или държави членки или други засегнати единици.

2. Когато е известно или е налице разумно основание за съмнение, че класифицирана информация е бил изложена на риск или изгубена, дирекция „Сигурност“ на ЕСВД по целесъобразност уведомява дирекция „Сигурност“ на Комисията, Службата за сигурност на Генералния секретариат на Съвета или НОС на съответната държава членка или държави членки или други засегнати единици и предприема всички необходими мерки съгласно съответните законови и подзаконови актове с цел:

а) извършване на оценка на потенциалните вреди, причинени на интересите на ЕС или на държавите членки;

б) предприемане на необходимите мерки за предотвратяване на повторно нарушение;

в) запазване на доказателствата;

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

д) уведомяване на съответните органи за последствията от събитието и предприетите действия; както и

е) информиране на създателя на информацията.

3. Всеки член на персонала под отговорността на ЕСВД, който е отговорен за нарушение на правилата за сигурност, определени в настоящото решение, може да подлежи на дисциплинарни действия в съответствие с приложимите правила и подзаконови актове.

Всяко лице, отговорно за излагането на риск или загубата на класифицирана информация, подлежи на дисциплинарни мерки и/или действия по съдебен път в съответствие с приложимите закони, правила и подзаконови актове.

По целесъобразност незабавно се информира дирекция „Сигурност“ на ГД „Човешки ресурси и сигурност“ на Комисията, Службата за сигурност на Генералния секретариат на Съвета или НОС на съответната държава членка или държави членки или други засегнати единици.

4. Докато се провежда разследване на нарушението и/или излагането на риск на класифицирана информация, ръководителят на дирекция „Сигурност“ на ЕСВД може временно да отмени правото на достъп на дадено лице до КИЕС и до помещенията на ЕСВД. Дирекция „Сигурност“ на ГД „Човешки ресурси и сигурност“ на Комисията, Службата за сигурност на Генералния секретариат на Съвета или НОС на съответната държава членка или държави членки или други засегнати единици незабавно се информират за това решение.

ПРИЛОЖЕНИЕ A I

СИГУРНОСТ, СВЪРЗАНА С ПЕРСОНАЛА

I. **ВЪВЕДЕНИЕ**

1. В настоящото приложение се определят разпоредби за прилагането на член 5 от приложение А. В него се установяват по-специално критериите, прилагани от ЕСВД, с които се определя дали на дадено физическо лице, отчитайки неговата лоялност и надеждност, може да бъде дадено разрешение за достъп до КИЕС, както и проучвателните и административните процедури, които да се следват за тази цел.

2. „Разрешение за достъп на персонала“ (РДП) до КИЕС означава изявление на компетентен 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) с определен срок, при условие че бъде установена „необходимост да се знае“; така описаното лице се смята за „лице с разрешение за достъп“.

3. „Удостоверение за разрешение за достъп на персонала“ (УРДП) означава удостоверение, издадено от органа по сигурността на ЕСВД, с което се удостоверява, че дадено лице е преминало през проучване за надеждност и се посочва нивото на КИЕС, до което лицето може да получи достъп, срокът на валидност на съответното РДП и датата на изтичане на валидността на самото удостоверение.

4. „Разрешение за достъп до КИЕС“ означава разрешение от органа по сигурността на ЕСВД, дадено в съответствие с настоящото решение след издаване на РДП от компетентните органи на държава членка и с което се удостоверява, че дадено лице може да получи достъп до КИЕС на определено ниво (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо) с определен срок, при условие че бъде установена „необходимост да се знае“; така описаното лице се смята за „лице с разрешение за достъп“.

II. **ДАВАНЕ НА РАЗРЕШЕНИЕ ЗА ДОСТЪП ДО КИЕС**

5. Достъпът до информация с ниво на класификация RESTREINT UE/EU RESTRICTED не изисква проучване за надеждност и се предоставя след като:

   а) бъдат определени законоустановените или договорните отношения на физическото лице с ЕСВД,

   б) бъде установена неговата „необходимост да се знае“,

   в) бъде информирано за правилата и процедурите за сигурност за защита на КИЕС и декларира писмено, че е запознато със своята отговорност за защитата КИЕС в съответствие с настоящото решение.

6. Физическо лице получава разрешение за достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, след като:

   а) бъде установена неговата „необходимост да знае“;

   б) 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; както и

   в) бъде информирано за правилата и процедурите за сигурност за защита на КИЕС и декларира писмено, че е запознато със своята отговорност за защитата на такава информация.

7. ЕСВД определя длъжностите в своите структури, които изискват достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, и в съответствие с това изисква РДП до необходимото ниво, както е определено в член 4 по-горе.

8. Служителите на ЕСВД обявяват дали са граждани на повече от една държава.

Процедури за отправяне на искане за РДП в ЕСВД

9. За персонала на ЕСВД назначаващият орган на ЕСВД 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.

10. Когато дадено лице е гражданин на повече от една държава, молбата се подава до НОС на държавата, за гражданин на която се е определило лицето при наемането си.

11. Когато на ЕСВД стане известна информация от значение за проучването за надеждност на лице, подало искане за РДП, ЕСВД уведомява за това съответния НОС в съответствие с приложимите правила и разпоредби.

12. След приключване на проучването за надеждност съответният НОС уведомява дирекция „Сигурност“ на ЕСВД за резултата от проучването.

а) Когато в резултат на проучването за надеждност се стигне до уверение, че няма известни неблагоприятни данни, които да поставят под въпрос лоялността и надеждността на лицето, органът по сигурността на ЕСВД може да предостави разрешение на съответното лице за достъп до КИЕС на съответното ниво за определен срок.

б) ЕСВД предприема всички необходими мерки, за да гарантира, че условията или ограниченията, наложени от НОС, надлежно се спазват. НОС се уведомява за резултата.

в) Когато проучването за надеждност не завърши с такова уверение, органът по сигурността на ЕСВД уведомява съответното лице, което може да поиска да бъде изслушано от органа по сигурността на ЕСВД. Органът по сигурността на ЕСВД може да поиска от компетентния НОС всякакви допълнителни пояснения, които този орган може да предостави в съответствие с националните законови и подзаконови актове. Ако резултатът бъде потвърден, не се предоставя разрешение за достъп до КИЕС. В такъв случай ЕСВД предприема всички необходими мерки, за да гарантира, че заявителят не получава достъп до КИЕС.

13. Проучването за надеждност и получените резултати, въз основа на които ЕСВД издава своето решение дали да предостави разрешение за достъп до КИЕС, подлежат на съответните законови и подзаконови актове в сила в съответната държава членка, включително по отношение на обжалването. Решенията на органа по сигурността на ЕСВД 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 [1] (наричан по-долу „Правилник за длъжностните лица“).

14. Уверението, на което се основава РДП, при положение че остава валидно, обхваща всички задачи за изпълнение от съответното лице в рамките на ЕСВД, Генералния секретариат на Съвета или Комисията.

15. Ако лицето не започне работа в рамките на 12 месеца от съобщаването на резултата от проучването за надеждност на органа по сигурността на ЕСВД или когато е налице прекъсване от 12 месеца или повече, през които то не е било на работа в ЕСВД, в други институции, агенции или органи на ЕС или в националната администрация на държава членка на длъжност, която изисква достъп до класифицирана информация, резултатът от проучването се изпраща на съответния НОС за потвърждаване на валидността и целесъобразността му.

16. Когато на ЕСВД стане известна информация, че физическо лице, притежател на валидно РДП, представлява риск за сигурността, ЕСВД уведомява за това съответния НОС в съответствие с приложимите правила и разпоредби. Когато НОС уведоми ЕСВД, че оттегля уверение, дадено в съответствие с точка 12, буква а) за лице, притежател на валидно разрешение за достъп до КИЕС, органът по сигурността на ЕСВД може да отправи искане за всякакъв вид пояснения, които НОС може да предостави съгласно националните законови и подзаконови актове. Ако неблагоприятната информация бъде потвърдена, горепосоченото разрешение 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.

17. Всяко решение за отнемане на разрешение за достъп до КИЕС от длъжностно лице или ЕСВД и, когато това е уместно, основанията за него се съобщават на заинтересованото лице, което може да поиска да бъде изслушано от органа по сигурността на ЕСВД. Информацията, предоставена от НОС, се подчинява на действащите законови и подзаконови актове на съответната държава членка, включително на актовете, отнасящи се до обжалването. Решенията на органа по сигурността на ЕСВД подлежат на обжалване в съответствие с Правилника за длъжностните лица.

18. Националните експерти, командировани в ЕСВД на длъжност, изискваща достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, представят валидно РДП за достъп до КИЕС на съответното ниво пред органа по сигурността на ЕСВД преди да приемат назначението. Горепосоченият процес се управлява от изпращащата държава членка.

Регистри на РДП

19. ЕСВД поддържа база данни относно статуса на разрешение за достъп на целия персонал под отговорността на ЕСВД и персонала на изпълнителите на ЕСВД. Тези регистри съдържат информация за нивото на КИЕС, до което се дава достъп на физическото лице (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо), датата на предоставяне на РДП и срока му на валидност.

20. Въвеждат се подходящи процедури за координация с държавите членки и другите институции, агенции и органи на ЕС, за да се гарантира, че ЕСВД разполага с точен и цялостен регистър на статуса на разрешение за достъп на целия персонал под отговорността на ЕСВД и персонала на изпълнителите на ЕСВД.

[1] ОВ L 56, 4.3.1968 г., стр. 1.

21. Органът по сигурността на ЕСВД може да издава удостоверение за разрешение за достъп на персонала (УРДП), в което се посочва нивото на КИЕС, до което лицето може да получи достъп (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо), срокът на валидност на съответното РДП и датата на изтичане на валидността на самото удостоверение.

Освобождаване от изискването за РДП

22. Лицата, които са надлежно оправомощени да осъществяват достъп до КИЕС по силата на изпълняваните от тях функции в съответствие с националните законови и подзаконови актове, по целесъобразност се информират за задълженията си за защитата на КИЕС от дирекция „Сигурност“ на ЕСВД.

III. ОБУЧЕНИЕ И ПОВИШАВАНЕ НА ОСВЕДОМЕНОСТТА ПО ВЪПРОСИТЕ НА СИГУРНОСТТА

23. Преди да получат разрешение за достъп до КИЕС всички лица декларират писмено, че са запознати със задълженията си по отношение на защитата на КИЕС и последиците от излагането на риск на КИЕС. ЕСВД регистрира тези писмени декларации.

24. 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.

25. Всички лица, на които е предоставен достъп до КИЕС, подлежат на текущи мерки за сигурност, свързана с персонала, (т.е. последващи мерки) за времето, в което работят с КИЕС. Текущата сигурност, свързана с персонала, е отговорност на:

а) Лица, на които е предоставен достъп до КИЕС: тези лица носят лична отговорност за своето поведение във връзка със сигурността и трябва да докладват незабавно на съответните органи по сигурността за всеки подход или дейност, които считат за подозрителни или необичайни, и за всички промени по своите персонални обстоятелства, които могат да окажат въздействие върху тяхното РДП или разрешение за достъп до КИЕС.

б) Преки ръководители: те носят отговорност да гарантират, че техният персонал е наясно с мерките за сигурност и отговорностите за защита на КИЕС, извършват мониторинг на поведението на техния персонал във връзка със сигурността и решават всички проблеми, свързани със сигурността, или съобщават на съответните органи по сигурността всяка неблагоприятна информация, която може да окаже въздействие върху РДП или разрешенията за достъп до КИЕС на техния персонал.

в) Служители по сигурността на организацията за сигурност на ЕСВД, както е определено в член 12 от настоящото решение: те носят отговорност за информиране на служителите с цел повишаване на осведомеността по въпросите на сигурността с оглед да се гарантира, че целият персонал в тяхната област на дейност периодично бива информиран, за насърчаване на стабилна култура на сигурност в тяхната област на отговорност, за въвеждане на мерки за мониторинг на поведението на персонала във връзка със сигурността и за докладване на съответните органи по сигурността за всяка неблагоприятна информация, която може да окаже въздействие върху РДП на дадено лице.

г) ЕСВД и държавите членки: те изграждат необходими канали за съобщаване на информация, която може да окаже въздействие върху РДП или разрешение за достъп до КИЕС на физически лица.

26. Всички лица, които престават да изпълняват задължения, свързани с достъп до КИЕС, биват информирани за задълженията им да продължат да опазват КИЕС и по целесъобразност декларират писмено, че са запознати със своите задължения.

IV. ИЗВЪНРЕДНИ ОБСТОЯТЕЛСТВА

27. При неотложни случаи, когато това е надлежно оправдано от интересите на ЕСВД, и до завършване на цялостното проучване за надеждност органът по сигурността на ЕСВД, 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 ЕСВД достъп до КИЕС за изпълнение на конкретни задължения. Възможно най-скоро се извършва пълно проучване за надеждност. 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 излагането на риск на КИЕС. ЕСВД регистрира тези писмени декларации.

28. Когато предстои дадено лице да бъде назначено на длъжност, изискваща РДП на ниво, 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;

г) предприети са действия за получаване на разрешение за нивото на достъп, 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 на ЕСВД; както и

ж) съответният НОС/ООС, който е издал РДП на лицето, е бил консултиран и не е получено възражение;

з) това изключение, включително описание на информацията, до която е предоставен достъп, бъде отразено в регистъра или в съответния подчинен регистър.

29. 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.

30. 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, ВП, изпълнителният генерален секретар или главният оперативен служител 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 РДП, 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.

31. При информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET извънредният достъп се ограничава до граждани на ЕС, 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.

32. Комитетът по сигурността на ЕСВД се информира за случаите, в които се прибягва до процедурата, установена в точки 29 и 30.

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

V. ПРИСЪСТВИЕ НА ЗАСЕДАНИЯ В ЦЕНТРАЛАТА НА ЕСВД И ДЕЛЕГАЦИИТЕ НА СЪЮЗА.

34. Лица, на които е възложено да участват в заседания в централата на ЕСВД или делегациите на Съюза, 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 РДП. За представителите на държавите членки, длъжностни лица от ГСС и Комисията се изпраща УРДП или друго доказателство за РДП от съответните органи до дирекция „Сигурност“ на ЕСВД, координатора на сигурността на делегацията на Съюза 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 РДП.

35. Когато бъде оттеглено РДП за достъп до КИЕС на лице, чиито задължения изискват присъствието му на заседания в централата на ЕСВД или делегациите на Съюза, на които се обсъжда информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, компетентният орган уведомява ЕСВД за това.

VI. ПОТЕНЦИАЛЕН ДОСТЪП ДО КИЕС

36. Когато предстои дадени лица да бъдат наети на работа при обстоятелства, при които те могат потенциално да имат достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, те преминават през съответното проучване за надеждност или биват придружавани непрекъснато.

37. 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 редовно инструктирани относно процедурите за сигурност за защита на КИЕС и получават указания за задълженията им във връзка със защитата на информацията, която им е поверена или до която неволно имат достъп.

ПРИЛОЖЕНИЕ А II

ФИЗИЧЕСКА СИГУРНОСТ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

I. ВЪВЕДЕНИЕ

1. В настоящото приложение се съдържат разпоредбите за изпълнение на член 6 от приложение А. 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; както и

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

II. ИЗИСКВАНИЯ И МЕРКИ ЗА ФИЗИЧЕСКА СИГУРНОСТ

3. ЕСВД прилага процес на управление на риска за защита на КИЕС в своите помещения, за да гарантира, 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;

   г) оценка на заплахата за трета държава, извършена от Центъра за операции при здравни кризи, разузнавателните средства на Центъра на ЕС за анализ на информация (INTCEN) въз основа по-специално на доклади на делегациите на Съюза, и

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

4. Органът по сигурността на ЕСВД, 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): СПП 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;

   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 се упражнява чрез електронни или електромеханични средства, да се извършва от служители за охрана и/или пропускателен пункт или с други физически способи;

   г) служители за охрана: обучени 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; както и

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

5. Дирекция „Сигурност“ на ЕСВД може да извършва претърсвания на влизащите или излизащите, което действа като възпиращ фактор по отношение на неразрешено внасяне на материали или неразрешено 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 дизайна 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 органът по сигурността на ЕСВД гарантира, че оборудването отговаря на одобрените технически стандарти и минимални изисквания.

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

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:

а) административни зони и

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

13. Органът по сигурността на ЕСВД 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) достъп без придружител се разрешава само на лица, надлежно оправомощени от дирекция „Сигурност“ на ЕСВД; както 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 разрешава само на лица, които са преминали през проучване за надеждност за съответното ниво и са конкретно оправомощени да влизат в зоната на основание „необходимост да се знае“;

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;

в) електронните устройства се оставят извън зоната.

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 от настоящото приложение;

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

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

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 органа по сигурността на ЕСВД 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

в) извън зона за сигурност или административна зона, при условие че притежателят пренася КИЕС в съответствие с точки 30—42 от приложение A III и се е ангажирал да спазва компенсаторните мерки, установени в инструкциите за сигурност, издадени от органа по сигурността на ЕСВД 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 органа по сигурността на ЕСВД.

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 30—42 от приложение А III;

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

iii) непрекъснато контролира лично КИЕС; както и

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

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 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 в централата в съответствие с едно от следните условия:

а) в сейф, който отговаря на точка 8, с една или повече 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;

или

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

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

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

30. Органът по сигурността на ЕСВД 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 излагане на риск или подозрение за излагане на риск на информация;

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

д) най-малко на всеки 12 месеца.

ПРИЛОЖЕНИЕ A III

УПРАВЛЕНИЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

I. ВЪВЕДЕНИЕ

1. В настоящото приложение се съдържат разпоредбите за изпълнение на член 7 от приложение А. 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 излагане на риск или загуба на такава информация, както и за последващото ѝ възстановяване.

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 разпространението на информацията.

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

5. Класифицирана информация на държавите членки, която се обменя с ЕСВД, получава същото ниво на защита като КИЕС с равностойно ниво на класификация. В допълнение Б към Решение 2011/292/ЕС на Съвета от 31 март 2011 г. относно правилата за сигурност за защита на класифицирана информация на ЕС се съдържа таблица на съответствията.

6. Класификацията за сигурност и по целесъобразност датата или конкретното събитие, след които нивото на класификация може да бъде понижено или премахнато, се посочват ясно и правилно независимо дали КИЕС е на хартиен носител, в устна, електронна или друга форма.

7. 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.

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. 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.

10. 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

11. В допълнение към един от грифовете за сигурност, посочени в член 2, параграф 2 от приложение А, 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.

12. След решение за предоставяне на КИЕС на трета държава или международна организация дирекция „Сигурност“ на ЕСВД изпраща съответната класифицирана информация с обозначение, че подлежи на предоставяне, в което се посочва третата държава или международната организация, на която се предоставя.

13. Органът по сигурността на ЕСВД приема списък с разрешени обозначения.

Съкратено обозначаване на класификацията

14. 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.

15. 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

16. 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 референтен номер и за какво се отнася, които сами по себе си не представляват класифицирана информация, освен ако са обозначени като такава;

г) върху документа се поставя дата;

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

17. Когато не е възможно да се приложи точка 15 към КИЕС, се вземат други подходящи мерки в съответствие с насоките за сигурност, които се определят съгласно настоящото решение.

Понижаване нивото на класификация и декласификация на КИЕС

18. 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.

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

III. РЕГИСТРАЦИЯ НА КИЕС ЗА ЦЕЛИТЕ НА СИГУРНОСТТА

20. В централата се създава централен регистър. За всяка организационна единица в рамките на ЕСВД, която работи с КИЕС, се създава съответен регистър, подчинен на централния регистър, за да се гарантира, че КИЕС се обработва в съответствие с настоящото решение. Регистрите се обособяват като зони за сигурност съгласно посоченото в приложение А.

Всяка делегация на Съюза създава свой собствен регистър на КИЕС.

Органът по сигурността на ЕСВД определя завеждащ регистъра служител за тези регистри.

21. За целите на настоящото решение регистрация за целите на сигурността (наричана по-долу „регистрация“) означава прилагането на процедури за отбелязване на жизнения цикъл на информацията, включително нейното разпространение и унищожаване. По отношение на КИС процедурите за регистрация могат да се изпълнят като процес в рамките на самата КИС.

22. Всички материали с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и по-високо се регистрират при постъпването им в дадена организационна единица и при излизането им от нея, включително делегациите на Съюза. Информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се регистрира в специални регистри.

23. Централният регистър, разположен в централата на ЕСВД, е основната входна и изходна точка за обмен на класифицирана информация с трети държави и международни организации. В него се поддържа регистър на всички случаи на обмен.

24. ВП одобрява политика на сигурност относно регистрацията на КИЕС за цели, свързани със сигурността, в съответствие с член 14 от настоящото решение.

Регистри за информация с ниво на класификация за сигурност trés secret UE/EU top secret

25. В централата на ЕСВД се определя централен регистър, който 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 регистри, в които да се работи с такава информация с цел регистрация.

26. Тези подчинени регистри не могат да предават документи с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET пряко на други регистри, подчинени на същия централен регистър за информация с класификация за сигурност TRÉS SECRET UE/EU TOP SECRET, или на външни получатели без изричното писмено одобрение на последния.

IV. КОПИРАНЕ И ПРЕВОД НА КЛАСИФИЦИРАНИ ДОКУМЕНТИ НА ЕС

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

28. 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.

29. Мерките за сигурност, приложими към оригиналния документ, се прилагат и за неговите копия и преводи. Копия на информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо се създават само от съответния регистър/подрегистър на защитена копирна машина. Копията трябва да се регистрират.

V. ПРЕНОС НА КИЕС

30. Преносът на КИЕС подлежи на защитните мерки, уредени в точки 31—41. Когато КИЕС се пренася на електронен носител и независимо от разпоредбите на член 7, параграф 4 от приложение А, изложените по-долу защитни мерки могат да бъдат допълнени с подходящи технически контрамерки, предписани от органа по сигурността на ЕСВД, така че да се сведе до минимум рискът тя да бъде загубена или изложена на риск.

31. Органът по сигурността на ЕСВД издава инструкции относно преноса на КИЕС в съответствие с настоящото решение.

В рамките на отделна сграда или самостоятелна група от сгради

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

33. 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, от съответно проучени за надеждност лица.

В рамките на ЕС

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

35. Преносът на информация с ниво на класификация за сигурност до SECRET UE/EU SECRET в рамките на ЕС 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 се съхранява в съответствие с изискванията, посочени в приложение А II;

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

iii) лицата са преминали през проучване за надеждност за съответното ниво и са информирани за своите задължения във връзка със сигурността;

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;

ii) те прилагат подходящи защитни мерки в съответствие с минималните изисквания, които се определят в насоките за сигурност съгласно член 20, параграф 1 от настоящото решение.

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.

36. 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 пренасяни по посочените в точка 34 начини, се пренасят като товар от транспортни дружества в съответствие с приложение A V.

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

От територията на ЕС до територията на трета държава или между институции на ЕС в трети държави

38. Когато се пренася от територията на ЕС до територията на трета държава или между институции на ЕС в трети държави, КИЕС се опакова по такъв начин, че да е защитена от неразрешено разкриване.

39. Преносът на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET от територията на ЕС до територията на трета държава и преносът на КИЕС с ниво на класификация за сигурност до SECRET UE/EU SECRET между институции на ЕС в трети държави 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 се съхранява в съответствие с изискванията, посочени в приложение A II;

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

v) лицата са преминали през проучване за надеждност за съответното ниво и са информирани за своите задължения във връзка със сигурността.

40. При пренос на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, предоставена от ЕС на трета държава или международна организация, се спазват съответните разпоредби на споразумение за сигурност на информацията или на административна договореност в съответствие с член 10, параграф 2 от приложение A.

41. Информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED може също да се пренася от територията на ЕС до територията на трета държава чрез пощенски служби или платени куриерски услуги.

42. Преносът на информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET от територията на ЕС до територията на трета държава или между институции на ЕС в трети държави се извършва с военен или дипломатически куриер.

VI. **УНИЩОЖАВАНЕ НА КИЕС**

43. 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.

44. Документи, подлежащи на регистрация в съответствие с член 7, параграф 2 от приложение А, се унищожават от отговарящия за тях регистър по указание на притежателя или на компетентен орган. Регистрите и друга регистрационна информация се актуализират съответно.

45. 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.

46. Регистраторът и свидетелят, когато се изисква присъствие на такъв, подписват удостоверение за унищожаване, което се завежда в регистъра. Удостоверенията за унищожаване на документи с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се съхраняват в регистъра за срок от най-малко десет 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.

47. Класифицирани документи, включително документи с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, се унищожават по методи, отговарящи на съответните стандарти на ЕС или равностойни на тях стандарти, или по методи, одобрени от държавите членки в съответствие с националните технически стандарти, така че да се предотврати цялостното им или частичното им възстановяване.

48. Унищожаването на компютърните средства за съхранение на КИЕС се извършва в съответствие с точка 36 от приложение А IV.

VII. **ПРОВЕРКИ ЗА СИГУРНОСТ**

Проверки на сигурността на ЕСВД

49. В съответствие с член 15 от настоящото решение проверките на сигурността на ЕСВД обхващат:

а) общи проверки на сигурността, чиято цел е да се оцени общото ниво на сигурността на централата на ЕСВД, делегациите на Съюза и всички зависими или свързани помещения, по-специално с оглед да се оцени ефективността на мерките за сигурност, които се прилагат за защита на интересите на ЕСВД в областта на сигурността;

б) проверки на сигурността на КИЕС, чиято цел е да се оцени, обикновено с цел акредитация, ефективността на мерките, които се прилагат за защита на КИЕС в централата на ЕСВД и делегациите на Съюза.

По-специално тези проверки се извършват *inter alia* с цел:

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

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

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

iv) да се окаже подкрепа за текущите програми на органите по сигурността, насочени към обучение и повишаване на осведомеността по въпросите на сигурността.

Провеждане на и докладване за проверки на сигурността на ЕСВД

50. Проверките на сигурността на ЕСВД се провеждат от екип за проверка от дирекция „Сигурност“ на ЕСВД и с подкрепата на експерти по сигурността от други институции на ЕС или държавите членки, ако е необходимо.

Екипът за проверка получава достъп до всички помещения, в които се работи с КИЕС, и по-специално до регистрите и точките за достъп до КИС.

51. Когато е необходимо, проверките на сигурността на ЕСВД в делегациите на Съюза могат да се извършват с подкрепата на служителите по сигурността на посолствата на държавите членки, разположени в трети държави.

52. Преди края на всяка календарна година органът по сигурността на ЕСВД приема програма за проверки на сигурността за ЕСВД за следващата година.

53. Когато е необходимо, органът по сигурността на ЕСВД може да организира проверки на сигурността, които не са предвидени в горепосочената програма.

54. При приключване на проверката на сигурността основните заключения и препоръки се представят на проверяваната единица. След това екипът за проверка изготвя доклад за проверката. Когато се предлагат коригиращи действия и се отправят препоръки, в доклада се включват достатъчно подробности в подкрепа на достигнатите заключения. Докладът се представя на органа по сигурността на ЕСВД и на ръководителя на проверяваната единица.

Под ръководството на дирекция „Сигурност“ на ЕСВД се изготвят редовно доклади, в които се посочват изводите от проверките, извършени през даден период и разгледани от Комитета по сигурността на ЕСВД.

Провеждане на и докладване за проверки на сигурността в агенции и органи на ЕС, създадени съгласно дял V, глава 2 от Договора за ЕС

55. По целесъобразност дирекция „Сигурност“ на ЕСВД може да определи експерти за оказване на принос, които да участват в съвместни екипи за проверка на ЕС, извършващи проверки в агенции и органи на ЕС, създадени съгласно дял V, глава 2 от Договора за ЕС.

Контролен списък за проверки на сигурността на ЕСВД

56. Дирекция „Сигурност“ на ЕСВД изготвя и актуализира контролен списък за проверка на сигурността, съдържащ въпроси, които да се установят по време на проверката на сигурността на ЕСВД. Контролният списък се изпраща на Комитета по сигурността на ЕСВД.

57. Предоставя се необходимата за попълване на контролния списък информация, особено по време на проверка 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 единица Той не представлява част от доклада за проверката.

ПРИЛОЖЕНИЕ A IV

ЗАЩИТА НА КИЕС, С КОЯТО СЕ РАБОТИ В КИС

I. **ВЪВЕДЕНИЕ**

1. В настоящото приложение се съдържат разпоредбите за изпълнение на член 8 от приложение А.

2. Следните понятия и характеристики на осигуреност на информацията (ОИ) имат основно значение за сигурността и правилното протичане на операциите в комуникационните и информационните системи (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 КИЕС. Подробните изисквания за изпълнение на тези разпоредби се определят в политиките и насоките за сигурност за ОИ.

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

7. Специфичните изисквания, мащаб и степен на задълбоченост, определени от съответния орган по акредитиране на сигурността (ОАС) за акредитация на КИС, съответстват на оценката на риска, като се вземат предвид всички уместни 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.

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 на предприетите мерки за сигурност 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. ЕСВД си сътрудничи с ГСС, Комисията и държавите членки 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 ЕС и извън него.

15. Разпространението и последващото прилагане на най-добри практики допринася за постигане на равностойно ниво на осигуреност на използваните от ЕСВД 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) *Детекция:* 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 по-нататъшни вреди; както и

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

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

17. Компетентните органи на ЕСВД гарантират, че могат да реагират на инциденти, които е възможно да надхвърлят организационните и националните граници, като координират ответните реакции и обменят информация за тези инциденти и свързаните с тях рискове (компютърни способности за реагиране при извънредни обстоятелства).

Принцип на минималност и най-малко привилегии

18. С цел да се избегне ненужно излагане на риск, се използват само функционалните възможности, устройства и услуги, с които се изпълняват оперативните изисквания.

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 КИС и цялата организация;

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

в) индивидуалната си отговорност и отчетност за сигурността на КИС в зависимост от своята 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 и 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 (НОКО) на държавата членка.

26. Преди да бъдат препоръчани за одобрение от НОКО на ЕСВД в съответствие с член 7, параграф 5 от настоящото решение, 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.

27. Когато за това има специфични оперативни основания, НОКО на ЕСВД може, по препоръка на Комитета по сигурността на Съвета, да отмени изискванията по точка 25 или 26 и да предостави временно одобрение за определен период в съответствие с член 7, параграф 5 от настоящото решение.

28. 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.

29. Върховният представител одобрява политика за сигурност при квалифицирането и одобряването на некриптографски информационно-технологични продукти за сигурност.

Предаване в рамките на зони за сигурност

30. Независимо от разпоредбите на настоящото решение, когато предаването на КИЕС е ограничено в рамките на зони за сигурност, може да се прибегне до некриптирано разпространение 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

31. 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 (например комуникация) в еднопосочен или многопосочен план.

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

33. 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; както и

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

34. Не се допуска взаимна свързаност между акредитирана КИС и незащитена или обществена мрежа, освен в случаите, когато КИС разполага с одобрени МЗП, 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 (ООИ) 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 7, параграф 5 от настоящото решение, такава връзка не се счита за взаимна свързаност.

35. 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

36. Компютърните средства за съхранение се унищожават в съответствие с процедури, одобрени от органа по сигурността на ЕСВД.

37. Повторното използване, понижаването на нивото на класификация или декласификацията на компютърните средства за съхранение се извършва в съответствие с политика за сигурност, която се определя съгласно член 7, параграф 2 от настоящото решение.

Извънредни обстоятелства

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

39. 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; както и

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

40. 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.

41. След случаи на прилагане на точка 39 се изготвя доклад до дирекция „Сигурност“ на ЕСВД и от нея до Комитета по сигурността на ЕСВД. В този доклад като минимум се посочва изпращачът, получателят и създателят на всеки елемент на КИЕС.

III. ФУНКЦИИ И ОРГАНИ, СВЪРЗАНИ С ОСИГУРЕНОСТТА НА ИНФОРМАЦИЯТА

42. В ЕСВД се установяват следните функции във връзка с ОИ. Тези функции не изискват самостоятелни организационни единици. Единиците имат самостоятелни мандати. При все това функциите и съпътстващите ги отговорности могат да бъдат комбинирани или интегрирани в една и съща организационна единица или разделени в различни организационни единици, при условие че се избягват вътрешни конфликти на интереси или задачи.

Орган по осигуреността на информацията (ООИ)

43. 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 отговарят на съответните политики, 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; както и

ж) гарантиране на наличието на подходящ експертен ресурс в експертната подобласт на Комитета по сигурността на ЕСВД по въпросите на ОИ.

Орган по TEMPEST

44. 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 своята оперативна среда.

Орган за криптографско одобрение (ОКО)

45. ОКО отговаря за осигуряване на съответствие на криптографските продукти със съответната криптографска политика. Този орган одобрява криптографски продукти за защита на КИЕС до определено ниво на класификация за сигурност в своята оперативна среда.

Орган за разпределение на криптографски материали (ОРКМ)

46. ОРКМ отговаря за:

а) управление и отчитане на криптографски материали на ЕС;

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

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

Орган по акредитиране на сигурността (ОАС)

47. 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 своята 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 съгласно съответните 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 (наричани по-долу „ПССИС“), документация за удостоверяване на изпълнението на мерките за сигурност и оперативните процедури за сигурност (наричани по-долу „ОПС“), както и гарантиране на съответствието на тази документация с правилата и политиките на ЕСВД 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 продукти и продукти по TEMPEST, използвани за гарантиране на сигурността на КИС;

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

48. ОАС на ЕСВД отговаря за акредитацията на всички КИС, които функционират в сферата на компетентност на ЕСВД.

Съвет по акредитиране на сигурността (САС)

49. Съвместният съвет по акредитиране на сигурността (САС) отговаря за акредитацията на КИС, попадащи в сферата на компетентност както на ОАС на ЕСВД, 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 ГСС и 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 ЕСВД. Той действа с консенсус на представителите на ОАС на институциите, държавите членки и други единици, които имат електронна свързаност с дадената КИС. САС изготвя периодични доклади за дейността си до Комитета по сигурността на ЕСВД и го уведомява за всички декларации за акредитация.

Оперативен орган по осигуреността на информацията

50. 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 Правилника за специфичните за системата изисквания за сигурност (**ПССИС**), включително правилника за остатъчния риск, оперативните процедури за сигурност (**ОПС**) и криптографския план в рамките на процеса на акредитация на КИС;

б) участие в избора и изпитването на специфичните за системата мерки, устройства и софтуер за техническа сигурност, с цел контрол на прилагането им и гарантиране, че те са безопасно 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 и също така 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;

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

ПРИЛОЖЕНИЕ A V

ИНДУСТРИАЛНА СИГУРНОСТ

I. ВЪВЕДЕНИЕ

1. В настоящото приложение се съдържат разпоредбите за изпълнение на член 9 от приложение А. 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 ЕСВД.

2. Върховният представител одобрява политика в областта на индустриалната сигурност, очертаваща по-специално подробни изисквания за удостоверенията за сигурност на структура (УСС), 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 (РКЦС)

3. Преди да обяви търг за възлагане на класифициран договор или да възложи такъв договор, ЕСВД, 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 ЕСВД 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 РКЦС ЕСВД взема предвид всички уместни 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; както и

   в) при нужда ЕСВД влиза във връзка с НОС/ООС 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 РКЦС.

Приложение относно аспектите на сигурността (ПАС)

5. Свързаните с договора изисквания за сигурност се описват в ПАС. Когато това е уместно, ПАС включва РКЦС 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 възложител може да изготви специфични инструкции за сигурност на програмата/проекта (ИСП). ИСП изискват одобрение от страна на НОС/ООС на държавите членки или друг компетентен орган по сигурността, участващ в програмата/проекта, и могат да съдържат допълнителни изисквания за сигурност.

III. УДОСТОВЕРЕНИЕ ЗА СИГУРНОСТ НА СТРУКТУРА (УСС)

8. Дирекция „Сигурност“ на ЕСВД отправя искане до НОС, ООС или друг компетентен орган по сигурността на съответната държава членка за издаване на УСС, 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). На изпълнителя, подизпълнителя или на потенциалния изпълнител или подизпълнител не се предоставя достъп до КИЕС до момента, в който на ЕСВД бъде представено доказателство за УСС.

9. Когато е уместно, ЕСВД, в качеството си на възложител, уведомява съответния НОС/ООС или друг компетентен орган по сигурността, че на предварителния етап или за изпълнение на договора се изисква УСС. УСС или РДП 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.

10. В качеството си на възложител ЕСВД не възлага класифициран договор на предпочитан участник в търга, преди да е получил потвърждение от НОС/ООС или друг компетентен орган по сигурността на държавата членка, в която е регистриран съответният изпълнител или подизпълнител, че е издадено съответното УСС, ако такова е необходимо.

11. В качеството си на възложител ЕСВД отправя искане до НОС/ООС или друг компетентен орган по сигурността, който е издал УСС, да го уведоми за всяка неблагоприятна информация, засягаща УСС. При договори за подизпълнение се уведомяват съответно НОС/ООС или друг компетентен орган по сигурността.

12. Отнемането на УСС от съответния НОС/ООС или друг компетентен орган по сигурността представлява достатъчно основание за ЕСВД, в качеството му на възложител, да прекрати класифициран договор или да изключи участник от търга.

IV. РАЗРЕШЕНИЯ ЗА ДОСТЪП НА ПЕРСОНАЛА (РДП) ЗА ПЕРСОНАЛА НА ИЗПЪЛНИТЕЛИТЕ

13. Всички наети от изпълнителите служители, които се нуждаят от достъп до КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, преминават през подходящо проучване за надеждност и получават достъп до информация на основата на принципа „необходимост да се знае“. Макар че не се изисква РДП за достъп до КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, за такъв достъп се прилага принципът „необходимост да се знае“.

14. Заявления за РДП за персонала на изпълнителя се отправят към НОС/ООС, който е отговорен за тази единица.

15. ЕСВД изтъква пред изпълнителите, които желаят да наемат гражданин на трета държава на длъжност, изискваща достъп до КИЕС, че НОС/ООС на държавата членка, в която е разположена и учредена наемащата единица, е отговорен да определи дали на това лице може да се предостави достъп до такава информация в съответствие с настоящото решение и да потвърди, че преди предоставянето на такъв достъп трябва да се получи съгласието на създателя на информацията.

V. КЛАСИФИЦИРАНИ ДОГОВОРИ ЗА ИЗПЪЛНЕНИЕ И ПОДИЗПЪЛНЕНИЕ

16. 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.

17. След възлагането на класифициран договор за изпълнение или подизпълнение ЕСВД, в качеството си на възложител, уведомява НОС/ООС или друг компетентен орган по сигурността на изпълнителя или подизпълнителя за разпоредбите за сигурност на класифицирания договор.

18. При прекратяване или изтичане на такива договори ЕСВД, в качеството си на възложител (и/или НОС/ООС или съответно друг компетентен орган по сигурността при договори за подизпълнение), уведомява своевременно НОС/ООС или друг компетентен орган по сигурността на държавата членка, в която е регистриран изпълнителят или подизпълнителят.

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

20. Конкретните разпоредби за разпореждане с КИЕС по време на изпълнението на договора или при неговото прекратяване или изтичане се посочват в ПАС.

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

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

23. Преди да предостави за подизпълнение части от класифициран договор, изпълнителят получава разрешение от ЕСВД 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 с ЕС.

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

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

VI. ПОСЕЩЕНИЯ ВЪВ ВРЪЗКА С КЛАСИФИЦИРАНИ ДОГОВОРИ

26. Когато за изпълнение на класифициран договор на ЕСВД, 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 НОС/ООС или друг съответен компетентен орган по сигурността. Това не засяга прерогативите на НОС/ООС в контекста на конкретни проекти да одобряват процедури, съгласно които такива посещения могат да се организират пряко.

27. 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 ЕСВД.

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

VII. ПРЕДАВАНЕ И ПРЕНОС НА КИЕС

29. По отношение на предаването на КИЕС чрез електронни средства се прилагат съответните разпоредби на член 8 от приложение А и приложение А IV.

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

31. 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 издава УСС на съответното ниво, ако това предполага също така, че класифицирана информация се съхранява в структури на изпълнителите. Във всеки случай персоналът, обработващ пратката, е преминал през проучване за надеждност в съответствие с приложение А 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 ЕСВД, по целесъобразност в контакт с НОС/ООС както на изпращача, така и на получателя 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;

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 ЕСВД или друг компетентен орган по сигурността на държавите както на изпращача, така и на получателя.

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

32. Предаването на КИЕС на изпълнители и подизпълнители, разположени в трети държави с валидно споразумение за сигурност с ЕС, се извършва в съответствие с мерките за сигурност, договорени между ЕСВД, в качеството му на възложител, и НОС/ООС на съответната трета държава, в която е регистриран изпълнителят.

IX. РАБОТА СЪС И СЪХРАНЕНИЕ НА ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ RESTREINT UE/EU RESTRICTED

33. Като поддържа връзка съответно с НОС/ООС на държавата членка, ЕСВД, в качеството си на възложител, има право да извършва посещения 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.

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

35. Не се изисква УСС, нито РДП за изпълнители или подизпълнители и техния персонал за договори, възлагани от ЕСВД, които съдържат информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED.

36. ЕСВД, 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 УСС или РДП, които съществуват съгласно националните законови и подзаконови актове.

37. Условията, при които изпълнителят може да възлага изпълнението на договор на подизпълнител, са в съответствие с точки 22—24.

38. 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, ЕСВД, 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 НОС/ООС.

ПРИЛОЖЕНИЕ A VI

ОБМЕН НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ С ТРЕТИ ДЪРЖАВИ И МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

I. **ВЪВЕДЕНИЕ**

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

II. **РАМКИ ЗА УРЕЖДАНЕ НА ОБМЕНА НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ**

2. ЕСВД може да обменя КИЕС с трети държави или международни организации в съответствие с член 10, параграф 1 от приложение А.

С оглед да се подпомогне ВП в изпълнението на отговорностите, определени в член 218 от ДФЕС:

а) съответният географски или тематичен отдел на ЕСВД, в консултация с дирекция „Сигурност“ на ЕСВД, по целесъобразност определя необходимостта от обмен на КИЕС в дългосрочен план със съответната трета държава или международна организация;

б) дирекция „Сигурност“ на ЕСВД, в консултация със съответния географски отдел на ЕСВД, по целесъобразност представя на ВП проектите на текстове, които следва да се предложат на Съвета съгласно член 218, параграфи 3, 5 и 6 от ДФЕС;

в) дирекция „Сигурност“ на ЕСВД подпомага ВП при провеждането на преговори в координация със съответните служби на Комисията и Генералния секретариат на Съвета;

г) във връзка със споразуменията или договореностите с трети държави за участието им в операции по управление на кризи по линия на ОПСО, както е посочено в член 10, параграф 1, буква в) от приложение А, дирекцията за управление и планиране при кризи на ЕСВД, в консултация със съответните служби на ЕСВД, по целесъобразност представя на ВП проектите на текстове, които следва да се предложат на Съвета съгласно член 218, параграфи 3, 5 и 6 от ДФЕС, и подпомага ВП при провеждането на преговори в координация със съответните служби на ЕСВД и Генералния секретариат на Съвета.

3. Когато в споразуменията за сигурност на информацията се предвиждат технически договорености за изпълнение, които се договарят между дирекция „Сигурност“ на ЕСВД — в координация с дирекция „Сигурност“ на ГД „Човешки ресурси и сигурност“ на Комисията и Службата за сигурност на Генералния секретариат на Съвета — и компетентния орган по сигурността на съответната трета държава или международна организация, в тези договорености се отчита нивото на защита, предвидено във въведените разпоредби, структури и процедури за сигурност в съответната трета държава или международна организация.

4. Когато за ЕСВД съществува дългосрочна нужда от обмен на информация с ниво на класификация, не по-високо от RESTREINT UE/EU RESTRICTED, с трета държава или международна организация и когато е установено, че въпросната страна не разполага с достатъчно развита система за сигурност, за да е възможно да сключи споразумение за сигурност на информацията, ВП може след получаване на единодушно положително становище от Комитета по сигурността на ЕСВД в съответствие с член 14, параграф 5 от настоящото решение да сключи административна договореност с компетентните органи по сигурността на въпросната трета държава или международна организация.

5. КИЕС не се обменя по електронен път с трета държава или международна организация, освен ако това изрично е предвидено в споразумението за сигурност на информацията или административната договореност.

6. В съответствие с административна договореност за обмен на класифицирана информация ЕСВД и третата държава или международната организация определят регистър като основна входна и изходна точка за обмен на класифицирана информация. За ЕСВД това е централният регистър на ЕСВД.

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

III. **ПОСЕЩЕНИЯ ЗА ОЦЕНКА**

8. Посещенията за оценка, посочени в член 16 от настоящото решение, се провеждат по взаимно споразумение със съответната трета държава или международна организация и се извършва оценка на:

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

б) специфични елементи на свързаните със сигурността законови и подзаконови актове, политики или процедури на третата държава или международната организация, които могат да окажат въздействие върху максималното ниво на класифицираната информация, която може да се обменя;

в) въведените мерки и процедури за сигурност за защита на класифицирана информация; както и

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

9. КИЕС не се обменя преди да се извърши посещение за оценка и да се определи нивото, на което може да се обменя класифицирана информация между страните, въз основа на равностойността на нивото на защита, с което ще бъде обозначена.

Ако преди посещението за оценка ВП узнае за извънредни или неотложни причини, които налагат обмен на класифицирана информация, ЕСВД извършва следните действия:

а) първо иска писмено съгласие от създателя на информацията, за да потвърди, че няма възражения за предоставяне на информацията;

б) препраща въпроса към органа по сигурността на ЕСВД, който може да вземе решение за предоставяне на КИЕС, ако бъде получено единодушно положително становище от държавите членки, представени в Комитета по сигурността на ЕСВД.

Ако ЕСВД не може да определи създателя на информацията, органът по сигурността на ЕСВД поема отговорността на създателя след като получи единодушно положително становище от Комитета по сигурността на ЕСВД.

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

10. Когато е въведена рамка в съответствие с член 10, параграф 1 от приложение А за обмен на класифицирана информация с трета държава или международна организация, решението за предоставяне на КИЕС от ЕСВД на трета държава или международна организация се взема от органа по сигурността на ЕСВД, който може да делегира това разрешение на висши длъжностни лица на ЕСВД или други лица под негово ръководство.

11. Ако класифицираната информация, която ще бъде предоставена, включително изходния материал, който може да се съдържа, не е създадена от ЕСВД, ЕСВД първо иска писмено съгласие от създателя на информацията, за да се увери, че няма възражения срещу предоставянето на информацията. Ако ЕСВД не може да установи създателя на информацията, органът по сигурността на ЕСВД поема отговорността на създателя след като получи единодушно положително становище от държавите членки, представени в Комитета по сигурността на ЕСВД.

V. ИЗВЪНРЕДНО AD HOC ПРЕДОСТАВЯНЕ НА КИЕС

12. В отсъствието на една от рамките, посочени в член 10, параграф 1 от приложение А, и когато интересите на ЕС или една или повече от държавите членки налагат предоставяне на КИЕС по политически, оперативни или неотложни причини, КИЕС може по изключение да бъде предоставена на трета държава или международна организация след предприемане на описаните по-долу действия.

След като гарантира, че са спазени условията, посочени в точка 11 по-горе, дирекция „Сигурност“ на ЕСВД извършва следните действия:

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;

б) приканва Комитета по сигурността на ЕСВД, въз основа на наличната информация, да издаде становище относно надеждността на разпоредбите, структурите и процедурите за сигурност на третата държава или международната организация, на която следва да се предостави КИЕС;

в) обръща се към органа по сигурността на ЕСВД, който може да вземе решение за предоставяне на информацията, при условие че е получено единодушно положително становище от държавите членки, представени в Комитета по сигурността на ЕСВД.

13. В отсъствието на една от рамките, посочени в член 10, параграф 1 от приложение А, съответната трета страна предприема писмено подходящи действия за защита на КИЕС.

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 разрешение от органа по сигурността на ЕСВД, дадено в съответствие с настоящото решение след издаване на РДП от компетентните органи на държава 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, при условие че бъде установена „необходимост да се знае“ — вж. член 2 от приложение A I.

„Нарушение на сигурността“ означава действие или бездействие от физическо лице, което противоречи на правилата за сигурност, установени в настоящото решение, и/или политиките или насоките за сигурност, в които се определят всички необходими мерки за изпълнението му.

„Жизнен цикъл на КИС“ означава целият 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, сключен от ЕСВД 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 ЕСВД 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) означава всяка система, даваща възможност за работа с информация в електронна форма. Една комуникационна и информационна система обхваща всички активи, необходими за нейното функциониране, включително инфраструктура, организация, персонал и информационни ресурси — вж. член 8, параграф 2 от приложение A.

„Излагане на риск на КИЕС“ означава цялостно или частично разкриване на КИЕС на неоправомощени лица или субекти — вж. член 8, параграф 2.

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

„Криптографски (крипто) продукти“ 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.

„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 ООС 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) 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 — вж. член 2, буква е).

„Удостоверение за сигурност на структура“ (УСС) означава административно определяне от НОС или ООС, че от гледна точка на сигурността дадена структура може да осигури адекватна защита на КИЕС на определено ниво на класификация за сигурност и че персоналът на тази структура, който се нуждае от достъп до КИЕС, е бил проучен за надеждност по подходящ начин и е информиран за съответните изисквания за сигурност, необходими за достъп до КИЕС и за нейната защита.

„Работа“ с КИЕС означава всички възможни действия, на които може да бъде подложена КИЕС в рамките на нейния жизнен 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“ 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 — вж. член 9, параграф 1 от приложение А.

„Осигуреност на информацията“ 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 — вж. член 8, параграф 1 от приложение А.

„Взаимна свързаност“ за целите на настоящото решение означава пряка връзка между две или повече информационно-технологични системи с цел обмен на данни и други информационни ресурси (например комуникация) в еднопосочен или многопосочен план — вж. приложение А IV, точка 31.

„Управление на класифицирана информация“ представлява прилагане на административни мерки за контрол на КИЕС през жизнения ѝ цикъл в допълнение към мерките, предвидени в членове 5, 6 и 8, като по този начин се съдейства за възпиране и разкриване на умишлено или случайно излагане на риск или загуба на такава информация и нейното възстановяване. Тези мерки се отнасят по-конкретно до създаването, регистрирането, копирането, превода, преноса, работата със, съхранението и унищожаването на КИЕС — вж. член 7, параграф 1 от приложение А.

„Материал“ означава документ или част от машина или оборудване, която е вече произведена или е в процес на производство.

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

„Сигурност, свързана с персонала“ означава прилагане на мерки за гарантиране, че достъп до КИЕС се предоставя единствено на лица, които:

— е необходимо да знаят;

— за достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, са съответно проучени за надеждност или надлежно оправомощени по силата на изпълняваните от тях функции, съгласно националните законови и подзаконови актове; както и

— са информирани за отговорностите си —

вж. член 5, параграф 1 от приложение А.

„Разрешение за достъп на персонала“ (РДП) до КИЕС 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, при условие че бъде установена „необходимост да се знае“; така описаното лице се смята за „лице с разрешение за достъп“.

„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 РДП, 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“ означава прилагане на физически и технически защитни мерки за предотвратяване на неразрешен достъп до КИЕС — вж. член 6 от приложение А.

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

„Регистрация“ означава прилагането на процедури за отбелязване на жизнения цикъл на информацията, включително нейното разпространение и унищожаване. Вж. приложение A III, точка 21.

„Остатъчен риск“ означава рискът, 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 и външните 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“ означава установяване на заплахите и видовете уязвимост и извършване на 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.

„Процес на управление на риска“ означава целият 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.

„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 — вж. приложение A V, раздел II.

„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 разширявано през целия период на програмата или договора и елементите на информацията могат да бъдат прекласифицирани или да преминат в по-ниско ниво на сигурност; РКЦС, в случай че такова съществува, е част от ПАС — вж. приложение A V, раздел II.

„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 не е известна неблагоприятна информация, която да попречи на дадено лице да бъде издадено национално РДП или РДП на ЕС за достъп до КИЕС на определено ниво на класификация за сигурност (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо).

„Оперативни процедури за сигурност“ (ОПС) означава описание на изпълнението на политиката на сигурност, която следва да бъде приета, оперативните процедури, които трябва да се следват, и отговорностите на персонала.

„Правилник за специфичните изисквания за сигурност“ (ПСИС) означава задължителен набор от принципи за сигурност и подробни изисквания за сигурност, които трябва да се спазват и които са в основата на процеса на сертифициране и акредитация на КИС.

„TEMPEST“ означава разследване, проучване и контрол на излагащи на риск 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 във връзка с неговата стриктност, всеобхватност или съгласуваност и може да има технически, процедурен, физически, организационен или оперативен характер.