Този документ е средство за документиране и не обвързва институциите

►**B**

РЕШЕНИЕ НА КОМИСИЯТА

от 29 ноември 2001 година

за изменение на нейния процедурен правилник

(нотифицирано под номер C(2001) 3031)

(2001/844/ЕО, ЕОВС, Евратом)

(ОВ L 317, 3.12.2001 г., стр. 1)

Изменено със:

		Официален вестник		
		№	страница	дата
►**M1**	Решение 2005/94/ЕО, Евратом на Комисията от 3 февруари 2005 година	L 31	66	4.2.2005 г.
►**M2**	Решение 2006/70/ЕО, Евратом на Комисията от 31 януари 2006 година	L 34	32	7.2.2006 г.
►**M3**	Решение 2006/548/ЕО, Евратом на Комисията от 2 август 2006 година	L 215	38	5.8.2006 г.
►**M4**	Регламент (ЕС) № 519/2013 на Комисията от 21 февруари 2013 година	L 158	74	10.6.2013 г.

▼B

РЕШЕНИЕ НА КОМИСИЯТА

от 29 ноември 2001 година

за изменение на нейния процедурен правилник

(нотифицирано под номер C(2001) 3031)

(2001/844/ЕО, ЕОВС, Евратом)

КОМИСИЯТА НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ,

като взе предвид Договора за създаване на Европейската общност, и по-специално член 218, параграф 2 от него,

като взе предвид Договора за създаване на Европейската общност за въглища и стомана, и по-специално член 16 от него,

като взе предвид Договора за създаване на Европейската общност за атомна енергия, и по-специално член 131 от него,

като взе предвид Договора за Европейския съюз, и по-специално член 28, параграф 1 и член 41, параграф 1 от него,

РЕШИ:

Член 1

Разпоредбите на Комисията относно сигурността, чийто текст е приложен към настоящото решение, се добавят към процедурния правилник на Комисията като приложение.

Член 2

Настоящото решение влиза в сила в деня на публикуването му в *Официален вестник на Европейските общности*.

То се прилага от 1 декември 2001 г.

▼B

ПРИЛОЖЕНИЕ

РАЗПОРЕДБИ НА КОМИСИЯТА ОТНОСНО СИГУРНОСТТА

Като има предвид, че:

(1) За да се развива дейността на Комисията в области, които изискват определена степен на поверителност, е целесъобразно да се изгради всеобхватна система за сигурност, която да се прилага в Комисията, другите институции, органи, служби и агенции, които са създадени по силата или въз основа на Договора за ЕО или Договора за Европейския съюз, в държавите-членки, както и при други получатели на класифицирана информация на Европейския съюз, оттук нататък наричана „класифицирана информация на ЕС“.

(2) С цел защита на така изградената система за сигурност, Комисията ще предоставя класифицирана информация на ЕС само на външни органи, които предлагат гаранции, че са предприели всички необходими мерки за прилагане на строго еквивалентни на настоящите разпоредби правила.

(3) Настоящите разпоредби се предвиждат, без да се засягат разпоредбите на Регламент № 3 от 31 юли 1958 г. за прилагане на член 24 от Договора за създаване на Европейската общност за атомна енергия ([1]), на Регламент (ЕО) № 1588/90 на Съвета от 11 юни 1990 г. относно предоставянето на поверителна статистическа информация на Статистическата служба на Европейските общности ([2]) и на Решение С (95) 1510 окончателен на Комисията от 23 ноември 1995 г. относно защита на информационните системи.

(4) Системата за сигурност на Комисията се основава на принципите, които са установени в Решение 2001/264/ЕО на Съвета от 19 март 2001 г. за приемане на разпоредбите относно сигурността на Съвета ([3]) с оглед гарантиране на безпрепятственото функциониране на процеса на вземане на решения в Съюза.

(5) Комисията подчертава важността на приобщаването, когато е уместно, на другите институции към правилата и стандартите за поверителност, които са необходими за защитаване на интересите на Съюза и неговите държави-членки.

(6) Комисията признава необходимостта от създаване на собствена концепция за сигурност, като отчита всички елементи на сигурността и особения характер на Комисията като институция.

(7) Настоящите разпоредби се приемат, без да се засягат разпоредбите на член 255 от Договора и на Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 г. относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията ([4]).

▼M2

(8) Тези разпоредби не засягат член 286 от Договора и Регламент (ЕО) № 45/2001 на Европейския парламент и Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни;

▼B

Член 1

Правилата на Комисията относно сигурността са посочени в приложението.

([1]) ОВ 17/58, 6.10.1958 г., стр. 406/58.
([2]) ОВ L 151, 15.6.1990 г., стр. 1.
([3]) ОВ L 101, 11.4.2001 г., стр. 1.
([4]) ОВ L 145, 31.5.2001 г., стр. 43.

▼B

Член 2

1. Членът на Комисията, който отговаря за въпросите на сигурността, предприема подходящи мерки, с които да се гарантира, че при работа с класифицирана информация на ЕС в рамките на Комисията, както и във всички сгради на Комисията, включително нейните представителства и служби в съюза и делегациите ѝ в трети страни, посочените в член 1 правила се спазват от длъжностните лица и останалите служители на Комисията, от командированите в Комисията служители и от външните за Комисията изпълнители.

▼M3

Когато даден договор или грантово споразумение между Комисията и външен изпълнител или бенефициер предполага обработка на класифицирана информация на ЕС в помещенията на изпълнителя или на бенефициера, трябва да бъдат взети подходящи мерки от съответния външен изпълнител или бенефициер, за да се гарантира, че при обработката на класифицирана информация на ЕС се спазват правилата, посочени в член 1. Те представляват неразделна част от договора или грантовото споразумение.

▼B

2. Държавите-членки, другите институции, органи, служби и агенции, които са създадени по силата или въз основа на учредителните договори, имат право да получават класифицирана информация на ЕС, при условие че гарантират, че при работа с класифицирана информация на ЕС в техните служби и помещения се спазват строго еквивалентни правила на посочените в член 1, и по-специално от:

а) членовете на постоянните представителства на държавите-членки в Европейския съюз, както и от членовете на националните делегации, които присъстват на заседания на Комисията или на нейни органи, или които участват в други дейности на Комисията;

б) други членове на националните администрации на държавите-членки, които работят с класифицирана информация на ЕС, независимо дали мястото на изпълнение на служебните им задължения се намира на територията на държавите-членки или в чужбина;

в) външни изпълнители и командировани служители, които работят с класифицирана информация на ЕС.

Член 3

Трети страни, международни организации и други органи имат право да получават класифицирана информация на ЕС, при условие че гарантират, че при работа с такава информация се спазват строго еквивалентни правила с тези, посочени в член 1.

Член 4

При съблюдаване на основните принципи и минималните стандарти за сигурност, които се съдържат в част I от приложението, членът на Комисията, който отговаря за въпросите на сигурността, може да предприема мерки в съответствие с част II от приложението.

Член 5

Считано от датата на тяхното прилагане, настоящите разпоредби заменят:

а) Решение C (94) 3282 на Комисията от 30 ноември 1994 г. относно приложимите мерки за сигурност за класифицираната информация, която се създава или предава във връзка с дейността на Европейския съюз;

б) Решение C (99) 423 на Комисията от 25 февруари 1999 г. относно процедурите, по които длъжностните лица и останалите служители на Европейската комисия могат да имат право на достъп до държаната от Комисията класифицирана информация.

▼**B**

Член 6

Считано от датата на прилагане на настоящите разпоредби, цялата класифицирана информация, която до тази дата се държи от Комисията, с изключение на класифицирана информация на Евратом:

а) ако е създадена от Комисията, се счита за прекласифицирана по правило на „►**M1** RESTREINT UE ◄“, освен ако до 31 януари 2002 г. авторът ѝ реши да ѝ определи друга степен на класифициране. В такъв случай авторът информира всички адресати на съответния документ;

б) ако е създадена от автори извън Комисията, запазва първоначалната си класификация и по този начин се третира като равностойна по степен класифицирана информация на ЕС, освен ако авторът даде съгласие за декласифициране или понижаване на степента на класифициране на информацията.

▼B

ПРИЛОЖЕНИЕ

ПРАВИЛА ЗА СИГУРНОСТ

Съдържание

ЧАСТ I: ОСНОВНИ ПРИНЦИПИ И МИНИМАЛНИ СТАНДАРТИ ЗА СИГУРНОСТ

1. ВЪВЕДЕНИЕ
2. ОБЩИ ПРИНЦИПИ
3. ОСНОВИ НА СИГУРНОСТТА
4. ПРИНЦИПИ ЗА СИГУРНОСТ НА ИНФОРМАЦИЯТА
4.1. **Цели**
4.2. **Определения**
4.3. **Класифициране**
4.4. **Цели на мерките за сигурност**
5. ОРГАНИЗАЦИЯ НА СИГУРНОСТТА
5.1. **Общи минимални стандарти**
5.2. **Организация**
6. СИГУРНОСТ НА ПЕРСОНАЛА
6.1. **Проверка на персонала преди предоставяне на достъп до секретни материали**
6.2. **Регистър на предоставените на персонала разрешения за достъп до секретни материали**
6.3. **Инструктаж за сигурност на персонала**
6.4. **Управленски отговорности**
6.5. **Статут за сигурност на персонала**
7. ФИЗИЧЕСКА СИГУРНОСТ
7.1. **Необходимост от защита**
7.2. **Проверки**
7.3. **Сигурност на сгради**
7.4. **Планове за аварийни ситуации**
8. СИГУРНОСТ НА ИНФОРМАЦИЯТА
9. МЕРКИ СРЕЩУ САБОТАЖИ И КОНТРОЛ НА ДРУГИ ФОРМИ НА УМИШЛЕНО ЗЛОНАМЕРЕНО ПРИЧИНЯВАНЕ НА ВРЕДИ
10. ПРЕДОСТАВЯНЕ НА ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ТРЕТИ ДЪРЖАВИ ИЛИ НА МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

ЧАСТ II: ОРГАНИЗАЦИЯ ЗА СИГУРНОСТ В КОМИСИЯТА

11. ЧЛЕН НА КОМИСИЯТА, КОЙТО ОТГОВАРЯ ПО ВЪПРОСИТЕ НА СИГУРНОСТТА
12. КОНСУЛТАТИВНА ГРУПА ПО ПОЛИТИКАТА ЗА СИГУРНОСТ НА КОМИСИЯТА
13. СЪВЕТ ЗА СИГУРНОСТ НА КОМИСИЯТА
14. ►M2 ДИРЕКЦИЯ ПО СИГУРНОСТТА НА КОМИСИЯТА ◄
15. ИНСПЕКЦИИ НА СИГУРНОСТТА
16. КЛАСИФИКАЦИИ, ОБОЗНАЧЕНИЯ И МАРКИРОВКИ ЗА СИГУРНОСТ
16.1. **Степени на класифициране**

▼B

16.2. **Обозначения за сигурност**

16.3. **Маркировки**

16.4. **Поставяне на класификация**

16.5. **Поставяне на обозначения за сигурност**

17. УПРАВЛЕНИЕ НА КЛАСИФИЦИРАНЕТО

17.1. **Общи положения**

17.2. **Прилагане на класификации**

17.3. **Понижаване на степента на класификация и декласифициране**

18. ФИЗИЧЕСКА СИГУРНОСТ

18.1. **Общи положения**

18.2. **Изисквания за сигурност**

18.3. **Мерки за физическа сигурност**

18.3.1. *Зони на сигурност*

18.3.2. *Административна зона*

18.3.3. *Проверки при влизане и излизане*

18.3.4. *Охранителни патрули*

18.3.5. *Контейнери за сигурност и блиндирани помещения*

18.3.6. *Ключалки*

18.3.7. *Контрол на ключове и комбинации*

18.3.8. *Устройства за откриване на неправомерен достъп*

18.3.9. *Одобрено оборудване*

18.3.10. *Физическа защита на копирни и телефаксни апарати*

18.4. **Защита срещу визуален достъп и подслушване**

18.4.1. *Визуален достъп*

18.4.2. *Подслушване*

18.4.3. *Внасяне на електронно и записващо оборудване*

18.5. **Технически обезопасени зони**

19. ОБЩИ ПРАВИЛА ОТНОСНО ПРИНЦИПА НА НЕОБХОДИМОСТ ОТ ЗНАНИЯ И ОТНОСНО ЛИЧНИТЕ РАЗРЕШЕНИЯ ЗА ДОСТЪП ДО СЕКРЕТНИ МАТЕРИАЛИ НА ЕС

19.1. **Общи положения**

19.2. **Специфични правила за достъпа до ►M1 RESTREINT UE ◄ информация**

19.3. **Специфични правила за достъпа до ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ информация**

19.4. **Специфични правила за достъпа до информация►M1 RESTREINT UE ◄**

19.5. **Предаване на материали**

19.6. **Специални инструкции**

▼B

20. ПРОЦЕДУРА ЗА ИЗДАВАНЕ НА РАЗРЕШЕНИЯ НА ДЛЪЖНОСТНИТЕ ЛИЦА И ОСТАНАЛИТЕ СЛУЖИТЕЛИ НА КОМИСИЯТА

21. ИЗГОТВЯНЕ, РАЗПРОСТРАНЕНИЕ, ПРЕДАВАНЕ, СИГУРНОСТ НА КУРИЕРСКИЯ ПЕРСОНАЛ И ДОПЪЛНИТЕЛНИ ЕКЗЕМПЛЯРИ ИЛИ ПРЕВОДИ И ИЗВЛЕЧЕНИЯ ОТ КЛАСИФИЦИРАНИ ДОКУМЕНТИ НА ЕС

21.1. **Изготвяне**

21.2. **Разпространение**

21.3. **Предаване на класифицирани документи на ЕС**

21.3.1. *Опаковане, разписки*

21.3.2. *Предаване в рамките на сграда или група от сгради*

21.3.3. *Предаване в рамките на държава*

21.3.4. *Предаване от една държава в друга държава*

21.3.5. *Предаване на документи* ►**M1** *RESTREINT UE* ◄

21.4. **Сигурност на куриерския персонал**

21.5. **Електронни и други средства за техническо предаване**

21.6. **Допълнителни екземпляри, преводи или извадки от класифицирани документи на ЕС**

22. СЛУЖБИ ЗА РЕГИСТРАЦИЯ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС, ИНВЕНТАРНИ СПИСЪЦИ, ПРОВЕРКИ И УНИЩОЖАВАНЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

22.1. **Местни служби за регистрация на класифицирана информация на ЕС**

22.2. **Служба за регистрация на ►M1 RESTREINT UE ◄ информация**

22.2.1. *Общи положения*

22.2.2. *Централна служба за регистрация на* ►**M1** *RESTREINT UE* ◄ *информация*

22.2.3. *Подразделения на службите за регистрация на* ►**M1** *RESTREINT UE* ◄ *информация*

22.3. **Стоково-материални запаси, прегледи и проверки на класифицирани документи на ЕС**

22.4. **Архивно съхранение на класифицирани документи на ЕС**

22.5. **Унищожаване на класифицирани документи на ЕС**

22.6. **Унищожаване при аварийни ситуации**

23. МЕРКИ ЗА СИГУРНОСТ ПРИ СПЕЦИФИЧНИ СРЕЩИ, КОИТО СЕ ПРОВЕЖДАТ ИЗВЪН ПОМЕЩЕНИЯТА НА КОМИСИЯТА И ПО ВРЕМЕ НА КОИТО СЕ ИЗПОЛЗВА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

23.1. **Общи положения**

23.2. **Отговорности**

23.2.1. ►**M2** *Дирекция по сигурността на Комисията* ◄

23.2.2. *Служител по сигурността на срещите (MSO)*

23.3. **Мерки за сигурност**

23.3.1. *Зони за сигурност*

23.3.2. *Пропуски*

23.3.3. *Проверка на фотографско и аудиооборудване*

▼B

23.3.4. *Проверка на куфарчета, преносими компютри и пакети*

23.3.5. *Техническа сигурност*

23.3.6. *Документи на делегациите*

23.3.7. *Безопасно съхранение на документи*

23.3.8. *Проверки на служебни помещения*

23.3.9. *Изхвърляне на класифицирани отпадъци на ЕС*

24. НАРУШЕНИЯ НА РАЗПОРЕДБИТЕ ЗА СИГУРНОСТ И ИЗЛАГАНЕ НА РИСК НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

24.1. **Определения**

24.2. **Докладване за нарушения на разпоредбите за сигурност**

24.3. **Правни действия**

25. ЗАЩИТА НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС, КОЯТО СЕ ОБРАБОТВА В ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ

25.1. **Въведение**

25.1.1. *Общи положения*

25.1.2. *Заплахи за и уязвимост на системите*

25.1.3. *Главна цел на мерките за сигурност*

25.1.4. *Декларация за специфичните изисквания за сигурност на системата (SSRS)*

25.1.5. *Режими на работа при условия на сигурност*

25.2. **Определения**

25.3. **Отговорност за сигурността**

25.3.1. *Общи положения*

25.3.2. *Акредитиращ орган по сигурността (SAA)*

25.3.3. *Орган по сигурността на информацията (IA)*

25.3.4. *Собственик на техническите системи (TSO)*

25.3.5. *Собственик на информацията (IO)*

25.3.6. *Потребители*

25.3.7. *Обучение по сигурност на информацията*

25.4. **Нетехнически мерки за сигурност**

25.4.1. *Сигурност на персонала*

25.4.2. *Физическа сигурност*

25.4.3. *Контрол на достъпа до система*

25.5. **Технически мерки за сигурност**

25.5.1. *Сигурност на информацията*

25.5.2. *Контрол и отчетност на информацията*

25.5.3. *Работа с и контрол на отделящи се електронни информационни носители*

▼B

25.5.4. *Декласифициране и унищожаване на електронни информационни носители*

25.5.5. *Сигурност на комуникациите*

25.5.6. *Инсталационна и радиационна сигурност*

25.6. **Сигурност по време на работа**

25.6.1. *Процедури за сигурност при работа (SecOPS)*

25.6.2. *Софтуерна защита/управление на конфигурации*

25.6.3. *Проверка за наличие на опасни софтуерни/компютърни вируси*

25.6.4. *Поддръжка*

25.7. **Доставки**

25.7.1. *Общи положения*

25.7.2. *Акредитация*

25.7.3. *Оценка и сертифициране*

25.7.4. *Рутинни проверки на характеристиките за сигурност за продължаване на акредитацията*

25.8. **Временно или случайно използване**

25.8.1. *Сигурност на микрокомпютри/персонални компютри*

25.8.2. *Използване на лично информационно-технологично оборудване за официалната работа на Комисията*

25.8.3. *Използване на информационно-технологично оборудване, което е собственост на изпълнител, или което се доставя от държавите-членки за официална работа на Комисията*

26. ПРЕДОСТАВЯНЕ НА ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ТРЕТИ СТРАНИ ИЛИ НА МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

26.1.1. *Принципи, които регулират предоставянето на достъп до класифицирана информация на ЕС*

26.1.2. *Степени*

26.1.3. *Споразумения за сигурност*

ДОПЪЛНЕНИЕ 1: **Съпоставка с националните класификации за сигурност**

ДОПЪЛНЕНИЕ 2: **Практическо ръководство за класифициране**

ДОПЪЛНЕНИЕ 3: **Насоки за предоставяне на достъп до класифицирана информация на ЕС на трети държави или международни организации: Сътрудничество от степен 1**

ДОПЪЛНЕНИЕ 4: **Насоки за предоставяне на достъп до класифицирана информация на ЕС на трети държави или международни организации: Сътрудничество от степен 2**

ДОПЪЛНЕНИЕ 5: **Насоки за предоставяне на достъп до класифицирана информация на ЕС на трети държави или международни организации: Сътрудничество от степен 3**

ДОПЪЛНЕНИЕ 6: **Списък на съкращенията**

▼B

ЧАСТ I: ОСНОВНИ ПРИНЦИПИ И МИНИМАЛНИ СТАНДАРТИ ЗА СИГУРНОСТ

1. ВЪВЕДЕНИЕ

Настоящите разпоредби определят основните принципи и минималните стандарти за сигурност, които трябва да се спазват по подходящ начин от Комисията на всички нейни работни места, както и от всички получатели на класифицирана информация на ЕС (EUCI) така, че да се защитава сигурността и всички да могат да бъдат сигурни, че е установен общ стандарт за сигурност.

2. ОБЩИ ПРИНЦИПИ

Политиката за сигурност на Комисията представлява неразделна част от общата ѝ политика за вътрешно управление, поради което се основава на принципите, които уреждат общата ѝ политика.

Настоящите принципи включват законосъобразност, прозрачност, отговорност и субсидиарност (пропорционалност).

Принципът на законосъобразност показва необходимостта от стриктно придържане към правната рамка при изпълнението на функции във връзка със сигурността и необходимостта от спазване на законовите изисквания. Той означава също, че отговорностите в сферата на сигурността трябва да се основават на съответни нормативни разпоредби. С пълна сила се прилагат разпоредбите в Правилника за длъжностните лица на ЕО, най-вече разпоредбите на член 17 относно задължението на служителите да проявяват дискретност по отношение на информацията на Комисията и разпоредбите в дял VI от Правилника относно дисциплинарните мерки. Накрая, този принцип означава, че нарушенията на разпоредбите за сигурност в рамките на отговорността на Комисията трябва да се третират по начин, който съответства на политиката на Комисията относно дисциплинарните мерки и на политиката ѝ на сътрудничество с държавите-членки в областта на наказателното правораздаване.

Принципът на прозрачност показва необходимостта от яснота на всички правила и разпоредби за сигурност, за баланс между различните служби и области (физическа сигурност спрямо защита на информацията и т.н.) и необходимостта от последователна и структурирана политика за сигурност. Той също определя необходимостта от ясни писмени насоки за прилагането на мерки за сигурност.

Принципът на отговорност означава, че ще бъдат ясно определени отговорностите в сферата на сигурността. Освен това той показва необходимостта от редовна проверка на правилното изпълнение на тези отговорности.

Принципът на субсидиарност или пропорционалност означава, че сигурността се организира на най-ниското възможно равнище и във възможно най-тясна връзка с генералните дирекции и службите на Комисията. Той показва също, че дейностите във връзка със сигурността се ограничават само до онези елементи, които действително се нуждаят от това. И накрая, той означава, че мерките за сигурност са пропорционални на интересите, които трябва да се защитят и на действителната или потенциалната заплаха за тези интереси, и позволяват защита, която причинява възможно най-малко сътресения.

3. ОСНОВИ НА СИГУРНОСТТА

Основите на стабилната сигурност:

а) Национална организация за сигурност във всяка държава-членка, която отговаря за:

1. събирането и записването на разузнавателни данни за шпионаж, саботаж, тероризъм и други подривни дейности, и

2. предоставянето на информация и съвети на правителствата си, а чрез тях и на Комисията, относно естеството на заплахите за сигурността и средствата за защита срещу тях.

▼B

б) Орган по сигурността на информацията (IA) във всяка държава-членка и в Комисията, който отговаря за работата със съответния орган за сигурност за предоставянето на информация и съвети относно техническите заплахи за сигурността и средствата за защита срещу тях;

в) Редовно сътрудничество между правителствените отдели и съответните служби на Европейските институции с цел установяване и когато е уместно — даване на препоръки:

1. кои лица, информация и ресурси трябва да бъдат защитени, и

2. общи стандарти за защита.

г) Тясно сътрудничество между ►M2 Дирекция по сигурността на Комисията ◄ и службите по сигурността на другите европейски институции, и със Службата по сигурността на НАТО (NOS).

4. ПРИНЦИПИ ЗА СИГУРНОСТ НА ИНФОРМАЦИЯТА

4.1. **Цели**

Сигурността на информацията има следните главни цели:

а) Защита на класифицираната информация на ЕС (EUCI) от шпионаж, излагане на риск или неразрешено оповестяване;

б) Защита на информацията на ЕС, която се обработва в комуникационни и информационни системи и мрежи, срещу заплахи за нейната поверителност, цялостност и наличност;

в) Защита на помещенията на Комисията, в които се съхранява информация на ЕС, срещу саботажи и умишлено злонамерено причиняване на вреди;

г) В случай на повреда, оценка на причинените вреди, ограничаване на последиците от нея и предприемане на необходимите мерки за отстраняването им.

4.2. **Определения**

В текста на тези правила:

а) Терминът „класифицирана информация на ЕС“ (EUCI) означава всяка информация и материал, чието неразрешено оповестяване би могло да причини различна степен на накърняване на интересите на ЕС или на една или повече от неговите държави-членки, независимо дали тази информация е с произход от ЕС или е получена от държавите-членки, трети държави или международни организации.

б) Терминът „документ“ означава всяко писмо, бележка, протокол, доклад, меморандум, сигнал/съобщение, скица, фотографска снимка, диапозитив, филм, карта, диаграма, план, бележник, циклостилна хартия, индиго, лента за пишеща машина или принтер, лента, касета, компютърен диск, CD-ROM или друго физическо средство, върху което е записана информация.

в) Терминът „материал“ означава „документ“, както е определено в буква б), както и всяко оборудване, което е вече произведено или е в процес на производство.

г) Терминът „необходимост да се знае“ означава необходимостта отделен служител да има достъп до класифицирана информация на ЕС, за да може да изпълни дадена функция или задача.

д) „Разрешение“ означава решение на ►M2 директора на дирекцията по сигурността на Комисията ◄ за предоставяне на индивидуален достъп до класифицирана информация на ЕС (EUCI) до определено ниво въз основа на положителен резултат от извършена съгласно националното законодателство проверка (проучване) за сигурност от национален орган за сигурност.

▼B

е) Терминът „класифициране“ означава определянето на подходяща степен на сигурност на информация, чието неразрешено оповестяване би могло да причини определена степен на накърняване на интересите на Комисията или на държавите-членки.

ж) Терминът „понижаване“ означава понижаване на степента на класифициране.

з) Терминът „декласифициране“ означава премахване на всякакво класифициране.

и) Терминът „автор“ означава надлежно упълномощеният автор на класифициран документ. В рамките на Комисията началниците на отдели могат да оторизират свои подчинени служители да създават класифицирана информация на ЕС (EUCI).

й) Терминът „отдели на Комисията“ означава отделите и службите на Комисията, включително кабинетите, на всички работни места, включително Центърът за съвместни изследвания, представителствата и службите на съюза и делегациите в трети страни.

4.3. **Класифициране**

а) Когато се касае за поверителност, е необходимо да се проявява грижа и опитност при подбора на подлежащите на защита информация и материали и при оценката на необходимата степен на защита. От съществено значение е степента на защита да съответства на критичния характер на сигурността на отделните подлежащи на защита информация и материали. За да се гарантира безпрепятствения поток от информация, следва да се предприемат стъпки за избягване на прекомерно или недостатъчно висока степен на класифициране.

б) Системата за класифициране е инструментът за привеждане в действие на тези принципи; подобна система за класифициране се следва при планирането и организирането на начини за противодействие на шпионаж, саботаж, тероризъм и други заплахи, така че да се осигурява максимална степен на защита на най-важните помещения, в които се съхранява класифицирана информация и най-чувствителните точки в тях.

в) Отговорността за класифициране на информацията изцяло се носи от автора на тази информация.

г) Степента на класифициране може да се основава единствено на съдържанието на тази информация.

д) При групиране на няколко вида информация степента на класифициране, която трябва да се приложи за цялата съвкупност, е поне най-високата степен на класифициране. Въпреки това на съвкупност от различни видове информация може да се определя по-висока степен на класифициране в сравнение с определената степен за нейните съставни части.

е) Степени на класифициране се определят само когато и докато това е необходимо.

4.4. **Цели на мерките за сигурност**

Мерките за сигурност:

а) се отнасят за всички лица, които имат достъп до класифицирана информация, класифицирани информационни носители, всички помещения, в които се съдържа такава информация и важни съоръжения;

б) са предназначени да откриват лица, чието положение би могло да застрашава сигурността на класифицирана информация и важни съоръжения, в които се помещава класифицирана информация, и да предоставят тяхното изключване или отстраняване;

▼B

в) предотвратяват достъпа на всяко лице, което не е оторизирано за това, до класифицирана информация или до съоръженията, в които тя се помещава;

г) гарантират, че класифицираната информация се разпространява единствено на принципа на „необходимост да се знае“, който е основен принцип за всички аспекти на сигурността;

д) гарантират целостта (т.е. предотвратяване на повреждане или неразрешена промяна или неразрешено заличаване) и наличността (т.е. не се отказва достъп на лица, които имат нужда и са оторизирани да получат достъп) на цялата информация, класифицирана или некласифицирана, и особено на информацията, която се съхранява, обработва или предава в електромагнитна форма.

5. ОРГАНИЗАЦИЯ НА СИГУРНОСТТА

5.1. **Общи минимални стандарти**

Комисията гарантира, че се спазват общи минимални стандарти за сигурност от всички получатели на класифицирана информация на ЕС (EUCI), вътре в институцията и в службите и лицата от нейната компетенция, например от всички отдели и изпълнители, така че класифицираната информация на ЕС да може да се предава с увереността, че при работата с нея ще се полага аналогична грижа. Тези минимални стандарти включват критерии за проверка на персонала преди предоставяне на достъп до секретни материали и процедури за защита на класифицираната информация на ЕС.

Комисията разрешава достъп до класифицирана информация на ЕС на външни органи само при условие че те гарантират, че при работата с тази информация се спазват разпоредби, които са най-малко строго аналогични на настоящите минимални стандарти.

▼M3

Тези минимални стандарти също се прилагат, когато Комисията повери чрез договор или грантово споразумение на промишлени или други обекти задачи, които включват, изискват и/или съдържат класифицирана информация на ЕС: тези общи минимални стандарти са изложени в част II, раздел 27.

▼B

5.2. **Организация**

Сигурността в Комисията е организирана на две нива:

а) На ниво Комисията като цяло има ►M2 дирекция по сигурността на Комисията ◄, към която има създаден Акредитиращ орган по сигурността (SAA), който функционира и като Криптографски орган (CrA) и Орган TEMPEST, Орган по сигурността на информацията (IA) и една или повече Централни служби за регистрация на класифицирана информация на ЕС (EUCI), всяка от тях с по един или повече служители, които отговарят за контрола (RCO).

б) На ниво отдели на Комисията за сигурността отговарят един или повече служители по сигурността на местно ниво (LSO), един или повече служители по сигурността на информацията на централно ниво (CISO), служители по сигурността на информацията на местно ниво (LISO) и местните служби за регистрация на класифицирана информация на ЕС с по един или повече служители, отговарящи за контрола.

в) Централните органи за сигурност ще предоставят оперативни насоки за работа на местните органи за сигурност.

6. СИГУРНОСТ НА ПЕРСОНАЛА

6.1. **Проверка на персонала преди предоставяне на достъп до секретни материали**

На всички лица, които изискват достъп до информация, която е класифицирана като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ или с по-висока степен на класифициране, се извършва подходяща проверка, преди да им бъде разрешен достъп. Подобна проверка се изисква в случай на лица, чиито задължения включват техническа експлоатация или поддръжка на комуникационни и информационни системи, в които се съдържа класифицирана информация. Целта на настоящата проверка е да се определи дали въпросните лица:

а) са с неподлежаща на съмнение лоялност;

▼B

б) притежават личностни характеристики и дискретност, които не поставят под съмнение почтеността им при работа с класифицирана информация, или

в) могат да бъдат уязвими на натиск от външни или други източници.

По време на процедурите за проверка преди предоставяне на достъп до секретни материали особено внимателно се проверяват лицата:

г) на които следва да се предостави достъп до ►M1 RESTREINT UE ◄ информация;

д) които заемат длъжности, предполагащи редовен достъп до значителен обем ►M1 RESTREINT UE ◄ информация;

е) чиито служебни задължения им осигуряват специален достъп до защитени комуникационни или информационни системи, а оттам и възможност да получат неразрешен достъп до големи количества класифицирана информация на ЕС или да нанесат сериозни вреди на мисията чрез актове на технически саботаж.

При подчертаните в букви г), д) и е) обстоятелства в максимална практически възможна степен се използва техниката на проучване на миналото.

Когато трябва да се наемат на работа лица, които нямат установен статут на лице, което „е необходимо да знае“, при обстоятелства, при които те могат да имат достъп до класифицирана информация на ЕС (например куриери, служители, които отговарят за сигурността, персонал, който отговаря за поддръжката и почистването и др.), първо им се извършва подходяща проверка за сигурност.

6.2. **Регистър на предоставените на персонала разрешения за достъп до секретни материали**

Всички отдели на Комисията, в които се работи с класифицирана информация на ЕС или в които се помещават защитени комуникационни или информационни системи, поддържат регистър на предоставените разрешения за достъп на работещия в тях персонал. Всяко разрешение за достъп се проверява, в зависимост от случая, за да се гарантира, че е подходящо за текущата задача на лицето; то приоритетно се преразглежда всеки път, когато се получи информация, която сочи, че продължаването на работата с класифицирана информация вече не съответства на интересите на сигурността. Служителят, отговорен за сигурността на местно ниво в отдела на Комисията води регистър на разрешенията за достъп в областта, за която отговаря.

6.3. **Инструктаж за сигурност на персонала**

Всички служители, които заемат длъжности, при които биха могли да имат достъп до класифицирана информация подробно се инструктират при назначаването им на работа, а след това периодично, за необходимостта от сигурност и за процедурите за нейното осъществяване. От тези служители се изисква писмено да сертифицират, че са прочели и напълно са разбрали настоящите разпоредби за сигурност.

6.4. **Отговорност на ръководителите**

Ръководителите са длъжни да знаят кои техни служители боравят в работата си с класифицирана информация или имат достъп до защитени комуникационни или информационни системи, както и да записват и да докладват за всички инциденти или явни слабости в системата, които могат да имат последствия за сигурността.

6.5. **Статут на сигурност на персонала**

Установяват се процедури, с които да се гарантира, че при получаване на неблагоприятна информация за дадено лице може да се определи дали в процеса на работата си лицето борави с класифицирана информация или има достъп до защитени комуникационни или информационни системи, и че ►M2 дирекция по сигурността на Комисията ◄ е информирана за това. Ако се установи, че въпросното лице представлява риск за сигурността, му се налага възбрана или се отстранява от работа, когато би могло да застрашава сигурността.

▼B

7. ФИЗИЧЕСКА СИГУРНОСТ

7.2. **Необходимост от защита**

Степента на мерките за физическа сигурност, които ще се прилагат, за да се гарантира защита на класифицирана информация на ЕС, са пропорционални на степента на класифициране, обема на и заплахата за държаните информация и материали. Всички държатели на класифицирана информация на ЕС следват еднакви практики за класифицирането на тази информация и спазват общи стандарти за защита във връзка със съхранението, предаването и унищожаването на информация и материали, които изискват защита.

7.2. **Проверки**

Преди да оставят без надзор зони, в които се съдържа класифицирана информация на ЕС, лицата, които се грижат за тази информация, гарантират, че тя се съхранява сигурно и че са задействани всички устройства за сигурност (ключалки, алармени системи и др.). След работно време се извършват допълнителни независими проверки.

7.3. **Сигурност на сгради**

Сградите, в които се съхранява класифицирана информация на ЕС или защитени комуникационни и информационни системи, са защитени срещу неразрешен достъп. Естеството на осигурената защита за класифицирана информация на ЕС, например поставяне на решетки за прозорците, ключалки за врати, охрана на входовете, системи за автоматично управление на достъпа, проверки и патрули за сигурност, алармени системи, системи за откриване на неразрешен достъп и кучета пазачи, зависи от:

а) степента на класифициране, обема и местонахождението в сградата на информацията и материалите, които трябва да се охраняват;

б) качеството на контейнерите за сигурност за тази информация и материали, и

в) физическото естество и местоположение на сградата.

Естеството на осигурената защита за комуникационни и информационни системи по същия начин зависи от оценката на стойността на изложените на риск активи и от потенциалните вреди в случай на застрашаване на сигурността, от физическото естество и местоположението на сградата, в която се помещава системата и от местоположението на системата вътре в сградата.

7.4. **Планове за действие при непредвидени ситуации**

Предварително се изготвят подробни планове за защита на класифицирана информация по време на аварийно положение от местен или национален мащаб.

8. СИГУРНОСТ НА ИНФОРМАЦИЯТА

Сигурността на информацията (INFOSEC) се отнася за определянето и прилагането на мерки за сигурност за защита на класифицирана информация на ЕС, която се обработва, съхранява или предава по комуникационни, информационни и други електронни системи, срещу случайна или преднамерена загуба на нейния поверителен характер, цялост или наличност. Предприемат се необходими мерки за противодействие, за да се предотврати достъпът до класифицирана информация на ЕС на лица, които нямат разрешение за това, за да се предотврати отказването на достъп до класифицирана информация на ЕС на потребители, които имат разрешение за това, и за да се предотврати повреждане или неразрешена промяна или заличаване на класифицирана информация на ЕС.

▼B

9. МЕРКИ СРЕЩУ САБОТАЖИ И КОНТРОЛ НА ДРУГИ ФОРМИ НА УМИШЛЕНО ЗЛОНАМЕРЕНО ПРИЧИНЯВАНЕ НА ВРЕДИ

Физическите предпазни мерки за защита на важни съоръжения, в които се съхранява класифицирана информация, са най-добрите защитни мерки за сигурност срещу саботажи и умишлено злонамерено причиняване на вреди, и само извършването на проверка на персонала преди предоставянето на достъп до секретни материали не е ефективен техен заместител. От компетентния национален орган се изисква да предоставя разузнавателни сведения във връзка с шпионаж, саботажи, тероризъм и други подривни дейности.

10. ПРЕДОСТАВЯНЕ НА ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ТРЕТИ ДЪРЖАВИ ИЛИ НА МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

Решението за предоставяне на достъп до класифицирана информация на ЕС с произход от Комисията на трети държави или на международни организации се взема от Комисията като колегиален орган. Ако авторът на информацията, за която се иска разрешение за предоставяне на достъп, не е Комисията, Комисията първо иска съгласието на автора за даване на разрешение за предоставяне на достъп. Ако не може да се установи авторът, Комисията ще поеме отговорността на създателя.

Ако Комисията получава класифицирана информация от трети държави, от международни организации или от трети страни, на тази информация се осигурява подходяща за степента ѝ на класифициране защита, която е аналогична на установените в настоящите разпоредби стандарти за класифицирана информация на ЕС или евентуално изисквани по-високи стандарти от третата страна, която предоставя достъп до информацията. Организира се извършването на взаимни проверки.

Горепосочените принципи се прилагат в съответствие с подробните разпоредби, посочени в част II, раздел 26 и в допълнения 3, 4 и 5.

ЧАСТ II: ОРГАНИЗАЦИЯ ЗА СИГУРНОСТ В КОМИСИЯТА

11. ЧЛЕНЪТ НА КОМИСИЯТА, КОЙТО ОТГОВАРЯ ПО ВЪПРОСИТЕ НА СИГУРНОСТТА

Членът на Комисията, който отговаря по въпросите на сигурността:

а) прилага политиката за сигурност на Комисията;

б) разглежда проблеми на сигурността, за които е сезиран от Комисията или от нейните компетентни органи;

в) разглежда въпроси, свързани с промени в политиката за сигурност на Комисията, в тясно сътрудничество с националните органи за сигурност (или други подходящи органи) на държавите-членки (оттук нататък наричани „НОС“).

По-специално членът на Комисията, който отговаря по въпросите на сигурността, отговаря за:

а) координиране на всички въпроси на сигурността, които са свързани с дейността на Комисията;

б) отправя до определените органи на държавите-членки искания за предоставяне от националния орган за сигурност на проверки за сигурност за наетия персонал на работа в Комисията в съответствие с раздел 20;

в) разследва или нарежда провеждането на разследване във връзка с всяко изтичане на класифицирана информация на ЕС, за което са налице добри и достатъчни доказателства на пръв поглед, че е настъпило в Комисията;

г) изисква от съответните органи за сигурност да образуват следствие, когато са налице данни за изтичане на класифицирана информация на ЕС извън Комисията и координира запитванията, когато участващите органи за сигурност са повече от един;

д) извършва периодични проверки на мерките за сигурност за защита на класифицирана информация на ЕС;

▼B

е) поддържа тесни контакти с всички заинтересовани органи за сигурност с цел постигане на цялостна координация на сигурността;

ж) непрекъснато преразглежда политиката и процедурите за сигурност на Комисията, и при необходимост изготвя подходящи препоръки. В тази връзка членът на Комисията, който отговаря по въпросите на сигурността, представя на Комисията годишния план за проверки, изготвен от ►M2 дирекция по сигурността на Комисията ◄.

12. КОНСУЛТАТИВНА ГРУПА ПО ПОЛИТИКАТА ЗА СИГУРНОСТ НА КОМИСИЯТА

Създава се Консултативна група по политика за сигурност на Комисията. Тя се състои от члена на Комисията, който отговаря по въпросите на сигурността или негов/неин представител, който председателства групата и от представители на националните органи за сигурност на всяка държава-членка. Могат да бъдат поканени и представители на други европейски институции. Когато се обсъждат въпроси, които ги касаят, на заседанията на консултативната група за сигурност могат да бъдат поканени да присъстват и представители на съответните децентрализирани агенции на ЕО и ЕС.

Консултативната група по политиката за сигурност на Комисията се свиква на заседания по искане на председателя или на всеки от нейните членове. Групата има за задача да разглежда и преценява всички съответни въпроси на сигурността и когато е уместно — да представя препоръки на Комисията.

▼M2

13. СЪВЕТ ПО СИГУРНОСТТА НА КОМИСИЯТА

Създава се Съвет по сигурността на Комисията. Той се състои от генералния директор за администрацията и персонала, който ще го председателства, член на кабинета на комисаря, отговарящ за въпросите по сигурността, член на кабинета на председателя, заместник-генералния секретар, който оглавява групата на Комисията за управление на кризи, генералните директори на Правната служба, генерални дирекции „Външни отношения“, „Правосъдие, свобода и сигурност“, Съвместния изследователски център, генералната дирекция по информатика и Службата за вътрешен одит, както и директора на дирекцията по сигурността на Комисията или техните представители. Други длъжностни лица на Комисията могат да бъдат поканени. Неговият мандат е да оценява мерките за сигурност в рамките на Комисията и да прави препоръки в тази област на члена на Комисията, отговарящ за въпросите на сигурността.

▼B

14. ►M2 ДИРЕКЦИЯ ПО СИГУРНОСТТА НА КОМИСИЯТА ◄

За да може да изпълнява отговорностите, посочени в раздел 11, членът на Комисията, който отговаря по въпросите на сигурността, разполага със ►M2 дирекция по сигурността на Комисията ◄ за координиране, надзор и прилагане на мерките за сигурност.

Началникът на ►M2 директор на дирекцията по сигурността на Комисията ◄ е главният съветник на члена на Комисията, който отговаря по въпросите на сигурността, и изпълнява функциите на секретар на консултативната група по политиката за сигурност. В тази връзка той/тя ръководи актуализирането на регламентите за сигурност и координира мерките за сигурност с компетентните органи на държавите-членки, и по целесъобразност, с международните организации, които са свързани с Комисията по силата на споразумения за сигурност. За целта той/тя изпълнява функциите на лице за връзка.

►M2 Директор на дирекцията по сигурността на Комисията ◄ отговаря за акредитацията на информационно-технологичните системи и мрежи в Комисията. ►M2 Директор на дирекцията по сигурността на Комисията ◄, съгласувано със съответния национален орган за сигурност, взема решения относно акредитацията на информационно-технологични системи и мрежи, в които от една страна участва Комисията, а от друга страна, всеки друг получател на класифицирана информация на ЕС.

▼B

15. ПРОВЕРКИ ЗА СИГУРНОСТ

►M2 Дирекция по сигурността на Комисията ◄ извършва периодични проверки на мерките за сигурност за защита на класифицираната информация на ЕС.

При изпълнението на тази задача ►M2 дирекция по сигурността на Комисията ◄ може да се подпомага от службите по сигурността на другите институции на ЕС, които държат класифицирана информация на ЕС (EUCI), или от националните органи за сигурност на държавите-членки ([1]).

По искане на държава-членка в Комисията може да се извършва проверка на класифицирана информация на ЕС (EUCI) от нейния национален орган за сигурност, по взаимно съгласие и съвместно със ►M2 дирекция по сигурността на Комисията ◄.

16. КЛАСИФИКАЦИИ, ОБОЗНАЧЕНИЯ И МАРКИРОВКИ ЗА СИГУРНОСТ

16.1. **Степени на класифициране** ([2])

Информацията се класифицира на следните степени (виж също допълнение 2):

►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ: Тази степен на класифициране се прилага само за информация и материали, чието неразрешено оповестяване би могло да причини изключително тежко накърняване на съществените интереси на Европейския съюз или на една или повече от неговите държави-членки.

►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ: Тази степен на класифициране се прилага само за информация и материали, чието неразрешено оповестяване би могло сериозно да накърни съществените интереси на Европейския съюз или на една или повече от неговите държави-членки.

►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ: Тази степен на класифициране се прилага за информация и материали, чието неразрешено оповестяване би могло да накърни съществените интереси на Европейския съюз или на една или повече от неговите държави-членки.

ИНФОРМАЦИЯ ►M1 RESTREINT UE ◄: Тази степен на класифициране се прилага за информация и материали, чието неразрешено оповестяване би могло да причини неблагоприятни последици за интересите на Европейския съюз или на една или повече от неговите държави-членки.

Не се разрешават други степени на класифициране.

16.2. **Обозначения за сигурност**

За определяне на срока на валидност на дадена класификация (за класифицирана информация, обозначаваща автоматично понижаване на степента на класифициране или декласифициране), може да се използва уговорено обозначение за сигурност. Това обозначение е „ДО … (време/дата)“ или „ДО … (събитие)“.

При необходимост от ограничено разпространение и специално боравене, в допълнение към обозначението за класификация за сигурност, могат да се прилагат допълнителни обозначения за сигурност като CRYPTO или всяко друго признато в ЕС обозначение за сигурност.

Обозначенията за сигурност се използват само в съчетание със степен на класифициране.

16.3. **Маркировки**

За определяне на областта, за която се отнася документът, или за указване на особено разпространение въз основа на принципа за „необходимост да се знае“, или за обозначаване на края на ембарго (за некласифицирана информация), може да се използва маркировка.

Маркировката не е класификация и не трябва да се използва вместо нея.

([1]) Без да се засягат разпоредбите на Виенската конвенция от 1961 г. за дипломатическите взаимоотношения и на Протокола за привилегиите и имунитета на Европейските общности от 8 април 1965 г.

([2]) Виж сравнителната таблица за класификациите за сигурност на ЕС, НАТО, ЗЕС и държавите-членки в допълнение 1.

▼B

Маркировката за Европейска политика за сигурност и отбрана (ESDP) се прилага за документи и копия от тях, които касаят сигурността и отбраната на съюза или на една или повече от неговите държави-членки, или които се отнасят за управлението по време на военни или невоенни кризи.

16.4. **Поставяне на класификация**

Класификацията се поставя, както следва:

а) върху документи, класифицирани като информация►M1 RESTREINT UE ◄, чрез механични или електронни средства;

б) върху документи, класифицирани като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, чрез механични средства или на ръка, или чрез отпечатване върху хартиени бланки с предварително отпечатан щемпел;

в) върху документи, класифицирани като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, чрез механични средства или на ръка.

16.5. **Поставяне на обозначения за сигурност**

Обозначенията за сигурност се поставят непосредствено под класификацията със същите средства, които се използват за поставянето на класификациите.

17. УПРАВЛЕНИЕ НА КЛАСИФИЦИРАНЕТО

17.1. **Общи положения**

Информация се класифицира само при необходимост. Класификацията се посочва ясно и точно и се поддържа само докато информацията се нуждае от защита.

Отговорността за класифициране на информацията и за всяко евентуално последващо понижаване на степента на класифициране или декласифициране е изцяло на автора.

Длъжностните лица и останалите служители на Комисията класифицират, понижават степента на класифициране или декласифицират информация по нареждане или със съгласието на своя началник на отдел.

Подробните процедури за обработване на класифицирани документи са изработени така, че да се гарантира, че те са обект на защита, която е подходяща за съдържащата се в тях информация.

Броят на лицата, оторизирани да създават документи, класифицирани като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, се свежда до минимум, а имената им се пазят в списък, изготвен от ►M2 дирекция по сигурността на Комисията ◄.

17.2. **Прилагане на класификации**

Класификацията на документ се определя от степента на чувствителност на неговото съдържание в съответствие с определението в раздел 16. Важно е класификацията да се използва правилно и умерено. Това особено важи за класификацията ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ.

Авторът на подлежащ на класифициране документ следва да има предвид изложените по-горе правила и да се въздържа от всякаква склонност към определяне на прекомерно висока или недостатъчно висока степен на класифициране.

В допълнение 2 се съдържа практическо ръководство за класифициране.

Отделни страници, параграфи, раздели, приложения, допълнения и прикрепени части към даден документ могат да изискват различна степен на класифициране и това се извършва по съответен начин. В такъв случай документът като цяло получава класификацията на онази негова част, която е с най-висока степен на класифициране.

▼B

Класификацията на писмо или записка, включващи прикрепени части, съответства на най-високата степен на класифициране на тези части към тях. Авторът трябва ясно да посочи степента на класифициране, която писмото или записката трябва да получат след отделянето им от приложенията.

Публичният достъп продължава да се регулира от Регламент (ЕО) № 1049/2001.

17.3. **Понижаване на степента на класифициране и декласифициране**

Класифицирани документи на ЕС могат да се декласифицират или да се понижава степента им на класифициране само с разрешение на автора, а при необходимост след обсъждане с други заинтересовани страни. Понижаването на степента на класифициране или декласифицирането се потвърждават писмено. Авторът носи отговорност за информиране на адресатите на информацията за промяната, а те на свой ред са отговорни да информират за промяната всички евентуални следващи адресати, до които са изпратили, или за които са направили копия от документа.

По възможност авторите посочват върху класифицираните документи дата, срок или събитие, когато съдържанието може да се декласифицира или да се понижи степента му на класифициране. В противен случай те преразглеждат документите най-много на всеки пет години, за да се гарантира необходимостта от първоначалното класифициране.

18. ФИЗИЧЕСКА СИГУРНОСТ

18.1. **Общи положения**

Главните цели на мерките за физическа сигурност са да се предотвратява достъпът до класифицирана информация и/или материали на ЕС на лице, което няма разрешение за това, да се предотвратяват кражби или унищожаване на оборудване и друго имущество и да се предотвратява причиняването на безпокойство или всякакъв друг вид агресия срещу работници и служители и посетители.

18.2. **Изисквания за сигурност**

Всички помещения, зони, сгради, стаи, комуникационни и информационни системи и т.н., в които се съхранява и/или се работи с класифицирана информация и материали на ЕС, са защитени с подходящи мерки за физическа сигурност.

При вземане на решение каква степен на защита е необходима за осигуряването на физическа сигурност, се вземат под внимание всички съществени фактори като:

а) класифицирането на информацията и/или материалите;

б) количеството и формата (например хартиен носител, електронен носител) на държаната информация;

в) оценената от разузнавателните служби на място заплаха, насочена срещу ЕС, държавите-членки и/или други институции или трети страни, които държат класифицирана информация на ЕС, а именно саботажна, терористична и друга подривна и/или престъпна дейност.

Мерките за физическа сигурност са предназначени да:

а) предотвратяват незаконно или насилствено проникване на нарушители;

б) възпират, възпрепятстват или откриват действия на нелоялни служители;

в) предотвратяват достъпа до класифицирана информация на ЕС на лица, които не е необходимо да я узнават.

▼B

18.3. **Мерки за физическа сигурност**

18.3.1. *Зони за сигурност*

Зоните, в които се работи с или се съхранява информация, която е класифицирана като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ или като информация с по-висока степен на класифициране, се организират и структурират така, че да съответстват на една от следните категории:

а) Зона за сигурност от клас I: зона, в която работата или съхранението на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ или информация с по-висока степен на класифициране се извършва по такъв начин, че влизането в зоната с каквато и да е практическа цел съставлява достъп до класифицирана информация. Такава зона изисква:

i) ясно определен и защитен периметър, в който всички влизащи и излизащи се проверяват;

ii) система за входящ контрол, която допуска само лицата, които са надлежно проверени и специално упълномощени да влизат в зоната;

iii) посочване на степента на класифициране на обичайно държаната в зоната информация, т.е. информацията, до която влизането предоставя достъп.

б) Зона за сигурност от клас II: зона, в която работата или съхранението на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ или информация с по-висока степен на класифициране се извършва по такъв начин, че може да бъде защитена от достъпа на лица, които нямат разрешение за това, чрез вътрешно установени проверки, например помещения на служби, в които редовно се работи с или се съхранява ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ или информация с по-висока степен на класифициране. Такава зона изисква:

i) ясно определен и защитен периметър, в който всички влизащи и излизащи се проверяват;

ii) система за входящ контрол, която допуска без придружител само лицата, които са надлежно проверени и специално упълномощени да влизат в зоната. За всички останали лица се предвиждат придружители или аналогични проверки с цел предотвратяване на неразрешен достъп до класифицирана информация на ЕС и неконтролирано влизане в зони, които са обект на проверки за техническа сигурност.

Зоните, в които няма денонощно дежурен персонал, се проверяват веднага след изтичане на обичайното работно време, за да се гарантира правилната защита на класифицираната информация на ЕС.

18.3.2. *Административна зона*

В зоната около или водеща до зони за сигурност от клас I или клас II може да се създаде административна зона с по-ниска степен на сигурност. Тази зона изисква наличието на видимо определен периметър, в който могат да се извършват проверки на персонал и превозни средства. В такива зони се съхранява и се работи единствено с информация, класифицирана като информация►M1 RESTREINT UE ◄ или некласифицирана информация.

18.3.3. *Проверки при влизане и излизане*

Влизането в и излизането от зони за сигурност от клас I и клас II се контролира чрез пропуск или система за лично разпознаване, която се прилага за всички обичайно работещи в тези зони служители. Създава се и система за проверка на посетителите, която е предназначена да не се допуска неразрешен достъп до класифицирана информация на ЕС. Пропускателните системи могат да се допълват от система за автоматизирано идентифициране на самоличността, която се счита за допълнение, но не и за пълно заместване на служителите от охраната. Промяна в оценката на заплахата може да доведе до засилване на мерките за контрол при влизане и излизане, например при посещение на видни личности.

▼B

18.3.4. *Охранителни патрули*

В зоните за сигурност от клас I и клас II следва да се извършва патрулиране извън обичайното работно време с оглед защита на имуществото на ЕС срещу излагане на риск, повреда или загуба. Честота на патрулиране ще се определя от обстоятелствата на място, но поначало следва да се извършва веднъж на всеки 2 часа.

18.3.5. *Контейнери за сигурност и блиндирани помещения*

За съхранението на класифицирана информация на ЕС се използват три категории контейнери:

— Клас А: национално одобрени контейнери за съхранение на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ в зона за сигурност от клас I или клас II;

— Клас Б: национално одобрени контейнери за съхранение на ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ в зона за сигурност от клас I или клас II;

— Клас В: канцеларски мебели, които са подходящи за съхранение единствено на информация►M1 RESTREINT UE ◄.

За блиндирани помещения, които са изградени в зона за сигурност от клас I или клас II и за всички зони за сигурност от клас I, в които се съхранява на открити рафтове или е показана на диаграми, карти и друга информация, която е класифицирана като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ или информация с по-висока степен на класифициране, стените, подовете, таваните и вратата/ите с ключалка/и трябва да са сертифицирани от акредитиращия орган по сигурността (SAA), че предлагат аналогична защита, както контейнера за сигурност от категорията, която е одобрена за съхранение на информация със същата степен на класифициране.

18.3.6. *Ключалки*

Ключалките, които се използват за контейнери за сигурност и блиндирани помещения, в които се съхранява класифицирана информация на ЕС, отговарят на следните стандарти:

— Група А: национално одобрени за контейнери от клас А;

— Група Б: национално одобрени за контейнери от клас Б;

— Група В: подходящи само за канцеларски мебели от клас В.

18.3.7. *Контрол на ключове и комбинации*

Ключовете за контейнери за сигурност не се изнасят извън сградите на Комисията. Комбинациите за контейнерите за сигурност се научават наизуст от лицата, които трябва да ги знаят. С цел използване в аварийна ситуация служителят, отговарящ за сигурността на съответния отдел в Комисията, е длъжен да държи резервни ключове и писмен архив на всяка комбинация; последните се държат в отделно запечатани непрозрачни пликове. Работните ключове, резервните ключове и комбинациите се съхраняват в отделни контейнери за сигурност. За тези ключове и комбинации се осигурява същата степен на защита, която се осигурява за материалите, до които те предоставят достъп.

Комбинациите за контейнерите за сигурност се знаят от възможно най-ограничен брой лица. Комбинациите се сменят:

а) при получаване на нов контейнер;

б) при смяна на персонала;

в) при действителна или предполагаема опасност от излагане на риск;

г) периодично, за предпочитане на шест месеца, но най-малко веднъж годишно.

▼B

18.3.8. *Устройства за откриване на неправомерен достъп*

Когато за защитата на класифицирана информация на ЕС се използват алармени системи, телевизионни камери и други електрически устройства, се осигурява аварийно електрическо захранване, което да гарантира непрекъснатото функциониране на системата при прекъсване на главното електрическо захранване. Друго основно изискване е всяка неизправност или вмешателство в такива системи да води до алармено или друго надеждно предупреждение на надзорния персонал.

18.3.9. *Одобрено оборудване*

►M2 Дирекция по сигурността на Комисията ◄ поддържа актуални списъци по видове и модели на оборудването за сигурност, което е одобрила за защитата на класифицирана информация при различни конкретно посочени обстоятелства и условия. ►M2 Дирекция по сигурността на Комисията ◄ изготвя тези списъци *inter alia* и въз основа на информация от националните органи за сигурност.

18.3.10. *Физическа защита на копирни и телефаксни машини*

За копирни и телефаксни машини се осигурява необходимата степен на физическа защита, за да се гарантира, че само упълномощени лица могат да ги използват за обработка на класифицирана информация и че всички класифицирани материали се подлагат на подходящи проверки.

18.4. **Защита срещу визуален достъп и подслушване**

18.4.1. *Визуален достъп*

Денонощно се предприемат всички необходими мерки, за да се гарантира липсата на дори случаен визуален достъп до класифицирана информация на ЕС от лица, които не са оторизирани за това.

18.4.2. *Подслушване*

Службите или зоните, в които редовно се обсъжда информация, класифицирана като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ или с по-висока степен на класифициране, се защитават срещу пасивно и активно подслушване, когато рискът изисква това. Оценката на риска от такива атаки се извършва от ►M2 дирекция по сигурността на Комисията ◄, при необходимост след консултации с националните органи за сигурност.

18.4.3. *Внасяне на електронно и записващо оборудване*

Не се разрешава внасянето на мобилни телефони, лични компютри, записващи устройства, фотоапарати и други електронни или записващи устройства в зони за сигурност или в технически обезопасени зони без предварително разрешение от ►M2 директор на дирекцията по сигурността на Комисията ◄.

За определяне на предпазните мерки, които следва да се вземат в помещения, които са чувствителни по отношение на пасивно подслушване (например изолация на стени, врати, подове и тавани, измерване на рискови излъчвания) и активно подслушване (например претърсване за микрофони), ►M2 дирекция по сигурността на Комисията ◄ може да поиска съдействието на специалисти от националните органи за сигурност.

По същия начин, когато обстоятелствата го изискват, далекосъобщителното оборудване и всякакъв вид електрическо или електронно канцеларско оборудване, които се използват по време на заседания на ►M1 RESTREINT UE ◄ или по-високо ниво, може по искане на ►M2 директор на дирекцията по сигурността на Комисията ◄ да се проверяват от технически специалисти по сигурността от националните органи за сигурност.

▼B

18.5. **Технически обезопасени зони**

Някои зони могат да бъдат определени като технически обезопасени зони. Извършват се специални проверки при влизане. Когато в тях няма никой, такива зони се държат заключени по одобрен метод и всички ключове се третират като ключове за сигурност. Тези зони са обект на редовни физически инспекции, които ще се извършват и след проникване в тях без разрешение или при подозрение за такова проникване.

Води се подробен инвентарен списък на оборудването и мебелите, за да се следи тяхното движение. В такава зона не се внасят никакви мебели или оборудване, преди да са преминали внимателна проверка от специално обучен персонал по сигурността, чиято цел е да бъдат открити евентуални подслушвателни устройства. По правило в технически обезопасени зони не се разрешава инсталиране на комуникационни линии без предварително разрешение от съответния орган.

19. ОБЩИ ПРАВИЛА ОТНОСНО ПРИНЦИПА ЗА „НЕОБХОДИМОСТ ДА ЗНАЕ“ И ОТНОСНО ЛИЧНИТЕ РАЗРЕШЕНИЯ ЗА ДОСТЪП ДО СЕКРЕТНИ МАТЕРИАЛИ НА ЕС

19.1. **Общи положения**

Достъп до класифицирана информация на ЕС се разрешава само на лица, които е „необходимо да знаят“, за да изпълняват своите задължения или мисии. Достъп до ►M1 RESTREINT UE ◄, ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ се разрешава само на лица, които притежават съответното разрешение за достъп до секретни материали.

Отговорността за определяне на „необходимостта да знае“ е на отдела, в който ще се назначава съответното лице.

Всеки отдел отговаря за това да поиска да бъде извършена проверка за сигурност на персонала.

Това ще води до издаването на „личен сертификат за сигурност на ЕС“, в което ще бъде посочена степента на класифицирана информация, до която провереното лице може да има достъп и датата на изтичане на срока на сертификата.

Личният сертификат за сигурност на ЕС за дадена степен на класифициране може да дава на притежателя право на достъп до информация с по-ниска степен на класифициране.

Други лица, освен длъжностни лица или други служители като външни изпълнители, експерти или консултанти, с които може да е необходимо да се обсъжда или на които може да е необходимо да се показва класифицирана информация на ЕС, трябва да имат лично разрешение на ЕС за сигурност по отношение на класифицирана информация на ЕС и да бъдат инструктирани за отговорността, която носят по отношение на сигурността.

Публичният достъп продължава да се регулира с Регламент (ЕО) № 1049/2001.

19.2. **Специфични правила за достъпа до ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ**

Всички лица, които трябва да имат достъп до ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, първо се проучват, преди да получат достъп до такава информация.

Всички лица, които трябва да имат достъп до ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, се определят от члена на Комисията, който отговаря за въпросите на сигурността, а имената им се записват в съответния ►M1 RESTREINT UE ◄ регистър. Този регистър се създава и поддържа от ►M2 дирекция по сигурността на Комисията ◄.

▼B

Преди да получат достъп до ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, всички лица подписват сертификат, че са инструктирани за процедурите за сигурност на Комисията, и че напълно разбират особената отговорност, която носят за опазването на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, и последиците, които са предвидени от правилата на ЕС и националното законодателство, или от административни правила, когато умишлено или поради небрежност класифицирана информация премине в ръцете на лица, които нямат разрешение за това.

В случай на лица, които имат достъп до ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ по време на заседания и други, компетентният служител, който отговаря за контрола на службата или органа, в който работи съответното лице, нотифицира органа, който организира заседанието, че съответните лица имат такова разрешение.

Имената на всички лица, които спират да изпълняват служебни задължения, изискващи достъп до ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, се заличават от ►M1 RESTREINT UE ◄ СПИСЪК. Освен това на тези лица отново се обръща внимание на особената отговорност, която носят за опазването на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ. Те подписват и декларация, в която заявяват, че няма да използват или да предават притежаваната от тях ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ.

19.3. **Особени правила за достъп до ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ**

Всички лица, които ще имат достъп до ►M1 RESTREINT UE ◄ или ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, първо се проучват до съответната степен.

Всички лица, които ще имат достъп до ►M1 RESTREINT UE ◄ или ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, се запознават със съответните разпоредби за сигурност и се информират за последиците от проявена небрежност.

В случай на лица, които имат достъп до ►M1 RESTREINT UE ◄ или ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ по време на заседания и други, компетентният служител, който отговаря за контрола на службата или органа, в който работи съответното лице, нотифицира органа, който организира заседанието, че съответните лица имат такова разрешение.

19.4. **Специфични правила за достъп до информация ►M1 RESTREINT UE ◄**

Лицата, които имат достъп до информация ►M1 RESTREINT UE ◄, се информират за правилата и последиците от проявена небрежност.

19.5. **Предаване на материали**

При преместване на служител от длъжност, която предполага работа с класифицирани материали на ЕС, службата за регистрация следи за правилното предаване на тези материали от напускащото на новодошлото длъжностно лице.

При преместване на служител на друга длъжност, която предполага работа с класифицирани материали на ЕС, завеждащият сигурността на местно равнище му провежда съответен инструктаж.

19.6. **Специални инструкции**

Лицата, които трябва да боравят с класифицирана информация на ЕС, при постъпване на работа, а след това периодично, се информират за:

а) опасностите, които възникват за сигурността от недискретни разговори;

б) предпазните мерки, които да вземат при взаимоотношенията си с пресата и с представители на групи със специални интереси;

▼B

в) заплахата, която представлява дейността на разузнавателни служби, която е насочена към ЕС и държавите-членки по отношение на класифицираната информация и дейността на ЕС;

г) задължението незабавно да докладват на съответните органи за сигурност за всякакви постъпки или ходове, които пораждат подозрение за шпионска дейност или за всякакви необичайни обстоятелства, свързани със сигурността.

Всички лица, които обичайно са изложени на контакт с представители на страни, дейността на чиито разузнавателни служби е насочена към ЕС и държавите-членки по отношение на класифицираната информация и дейност на ЕС, се инструктират за техниките, които е известно, че се използват от различните разузнавателни служби.

Няма разпоредби за сигурност на Комисията относно частните пътувания на служители, които притежават разрешение за достъп до класифицирана информация на ЕС. Въпреки това ►M2 дирекция по сигурността на Комисията ◄ запознава длъжностните лица и останалите служители, за които отговаря с евентуалните правила, които те следва да съблюдават при пътуване.

20. ПРОЦЕДУРА ЗА ИЗДАВАНЕ НА РАЗРЕШЕНИЯ НА ДЛЪЖНОСТНИ ЛИЦА И ДРУГИ СЛУЖИТЕЛИ НА КОМИСИЯТА ЗА ДОСТЪП ДО ►M1 RESTREINT UE ◄ МАТЕРИАЛИ

а) Само длъжностни лица и служители на Комисията или лица, които работят в Комисията, които поради естеството на работата и поради изискванията във връзка със служебните им задължения трябва да са запознати или да използват класифицирана информация, която се държи от Комисията, имат достъп до такава информация.

б) За да получат достъп до информация, която е класифицирана като ►M1 RESTREINT UE ◄, ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, лицата, посочени в буква а) по-горе, трябва да са оторизирани в съответствие с процедурата, посочена в букви в) и г) от настоящия раздел.

в) Разрешение се дава само на лица, които са преминали проучване за сигурност от компетентните национални органи за сигурност на държавите-членки в съответствие с процедурата, посочена в букви и)—н).

г) ►M2 директор на дирекцията по сигурността на Комисията ◄ отговаря за издаването на разрешенията, посочени в букви а), б) и в).

д) Той/тя оторизира след получаване на становището на компетентните национални органи за сигурност на държавите-членки въз основа на проучването за сигурност, извършено в съответствие с букви и)—н).

е) ►M2 Дирекция по сигурността на Комисията ◄ поддържа актуален списък на всички деликатни постове в съответните отдели на Комисията и на всички лица, на които е издадено (временно) разрешение.

ж) Разрешението, чийто срок на валидност е пет години, не може да надвишава продължителността на задачите, въз основа на които е било издадено. То може да се подновява в съответствие с процедурата, посочена в буква д).

з) Разрешението се отменя от ►M2 директор на дирекцията по сигурността на Комисията ◄, когато той/тя счита, че са налице основания за това. Всяко решение за отнемане на разрешение се съобщава на съответното лице, което може да поиска да бъде изслушано от ►M2 директор на дирекцията по сигурността на Комисията ◄, и на компетентния национален орган.

▼B

и) Проучването за сигурност се извършва със съдействието на съответното лице и по искане на ►M2 директор на дирекцията по сигурността на Комисията ◄. Компетентният национален орган за проучването е органът на държавата-членка, чийто гражданин е лицето, което трябва да получи разрешение. Когато съответното лице не е гражданин на държава-членка на ЕС, ►M2 директор на дирекцията по сигурността на Комисията ◄ изисква проучването да се извърши от държавата-членка по постоянно местожителство или обичайно местопребиваване на лицето.

й) Като част от процедурата на проучване от съответното лице се изисква да попълни формуляр за лични данни.

к) ►M2 Директор на дирекцията по сигурността на Комисията ◄ посочва в искането си вида и степента на класифицираната информация, която ще се предоставя на съответното лице, така че компетентните национални органи да могат да извършат процеса на проучване и дадат становището си относно степента на разрешение, която би било подходящо да се предостави на лицето.

л) Целият процес на проучване за сигурност, заедно с получените резултати, подлежи на съответните действащи правила и разпоредби в съответната държава-членка, включително онези, които се отнасят за обжалването.

м) Когато компетентните национални органи на държавата-членка дадат положително становище, ►M2 директор на дирекцията по сигурността на Комисията ◄ може да издаде разрешение на съответното лице.

н) Всяко отрицателно становище на компетентните национални органи се нотифицира на съответното лице, което може да поиска да бъде изслушано от ►M2 директор на дирекцията по сигурността на Комисията ◄. Ако счита за необходимо, ►M2 Директор на дирекцията по сигурността на Комисията ◄ може да поиска от компетентните национални органи допълнителни пояснения, които те евентуално могат да предоставят. Ако отрицателното становище се потвърди, разрешение не се издава.

о) Всички лица, на които е издадено разрешение по смисъла на букви г) и д), при издаване на разрешението, а след това периодично, получават всички необходими инструкции относно защитата на класифицирана информация и за средствата, които осигуряват тази защита. Тези лица подписват декларация, сертифицираща че са получили инструкции и че се задължават да ги съблюдават.

п) ►M2 Директор на дирекцията по сигурността на Комисията ◄ предприема всички необходими мерки за прилагане на разпоредбите на настоящия раздел, и по-специално във връзка с правилата за достъп до списъка на лицата, на които е издадено разрешение.

р) По изключение, ако службата го изисква, ►M2 директор на дирекцията по сигурността на Комисията ◄ може, след като уведоми компетентните национални органи и при условие че те не са реагирали в срок от един месец, да издаде временно разрешение за срок не повече от шест месеца, докато се получи резултатът от проучването, посочено в буква и).

с) Издадените по този начин условни и временни разрешения не дават право на достъп до ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ; такъв достъп се ограничава до длъжностни лица, които действително са преминали проучване с положителни резултати в съответствие с буква и). До получаване на резултатите от проучването на длъжностните лица, за които е поискано да бъдат проверени за ►M1 RESTREINT UE ◄ СТЕПЕН, може временно и условно да бъде разрешен достъп до информация, класифицирана до и включително ►M1 RESTREINT UE ◄ СТЕПЕН.

▼B

21. ИЗГОТВЯНЕ, РАЗПРОСТРАНЕНИЕ, ПРЕДАВАНЕ, СИГУРНОСТ НА КУРИЕРСКИЯ ПЕРСОНАЛ И ДОПЪЛНИТЕЛНИ ЕКЗЕМПЛЯРИ ИЛИ ПРЕВОДИ И ИЗВАДКИ ОТ КЛАСИФИЦИРАНИ ДОКУМЕНТИ НА ЕС

21.1. **Изготвяне**

1. Класификациите на ЕС се прилагат, както е определено в раздел 16, а за ►M1 RESTREINT UE ◄ и по-висока степен на класифициране обозначението за класификация се поставя в средата на горното и долното поле на всяка страница, като всяка страница се номерира. Всеки класифициран документ на ЕС се обозначава с референтен номер и дата. В случай на ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ ДОКУМЕНТИ настоящият референтен номер фигурира на всяка страница. Ако тези документи трябва да бъдат разпространени в няколко екземпляра, върху първата страница на всеки от тях се обозначава номера на екземпляра и общият брой страници. На първата страница на документ с ►M1 RESTREINT UE ◄ или по-висока степен на класифициране на ЕС се изброяват всички приложения към документа.

2. Документи с ►M1 RESTREINT UE ◄ и по-висока степен на класифициране на ЕС се печатат, превеждат, съхраняват, фотокопират, възпроизвеждат по магнитен способ или се записват на микрофилми само от лица, на които им е разрешен достъп до класифицирана информация на ЕС най-малко до съответната степен на класифициране на въпросния документ.

3. Разпоредбите, регулиращи компютъризираното създаване на класифицирани документи, са посочени в раздел 25.

21.2. **Разпространение**

1. Класифицирана информация на ЕС се разпространява само сред лица, които е необходимо да я знаят и имат съответното разрешение за достъп. Авторът посочва първоначалното разпределение.

2. ►M1 RESTREINT UE ◄ ДОКУМЕНТИ НА ЕС се разпространяват чрез службите за регистрация на ►M1 RESTREINT UE ◄ МАТЕРИАЛИ (виж раздел 22.2). В случай на ►M1 RESTREINT UE ◄ СЪОБЩЕНИЯ компетентната служба за регистрация може да упълномощи началника на центъра за съобщения да изготви толкова броя екземпляри, колкото са посочени в списъка на адресатите на съобщението.

3. Документи със ►M1 RESTREINT UE ◄ и по-ниска степен на класифициране на ЕС могат да се преразпределят от първоначалния адресат до други адресати въз основа на принципа за „необходимост да се знае“. Въпреки това органът — автор на документите, ясно посочва всички възражения, които желае да наложи. При налагане на такива възражения адресатите могат да преразпределят документите само с разрешение на органа автор.

4. Всеки документ с ►M1 RESTREINT UE ◄ или по-висока степен на класифициране на ЕС при пристигане в или напускане на генерална дирекция или служба се регистрира от местната служба за регистрация на класифицирана информация на ЕС към отдела. Данните, които трябва да се вписват (референтни номера, дата, и по целесъобразност брой на екземплярите), са такива, че по тях да може да се идентифицират документите и се вписват в дневник или специално защитен електронен информационен носител (виж раздел 22.1).

21.3. **Предаване на класифицирани документи на ЕС**

21.3.1. *Опаковане, разписки*

1. Документи с ►M1 RESTREINT UE ◄ и по-висока степен на класифициране на ЕС се предават в устойчиви, непрозрачни двойни пликове. Върху вътрешния плик се обозначава съответната степен на класификация за сигурност на ЕС, както и по възможност пълни данни за длъжността и адреса на получателя.

▼B

2. Единствено служител, отговорен за контрол на регистрацията (виж точка 22.1), или негов заместник може да отваря вътрешния плик и да потвърждава получаването на приложените документи, освен ако пликът е адресиран до физическо лице. В такъв случай съответната служба за регистрация (виж раздел 22.1) вписва в дневник пристигането на плика и само физическото лице, до което същият е адресиран, може да отваря вътрешния плик и да потвърждава получаването на съдържащите се в него документи.

3. Във вътрешния плик се поставя формуляр на разписка. На разписката, която няма да се класифицира, следва да са посочени референтния номер, датата и номера на екземпляра от документа, но никога информация за какво се отнася документът.

4. Вътрешният плик се поставя във външен плик, върху който се обозначава номер на пратката за целите на получаването. При никакви обстоятелства върху външния плик не се обозначава класификацията за сигурност.

5. За документи с ►M1 RESTREINT UE ◄ и по-висока степен на класифициране на ЕС куриерите и пратениците получават разписки срещу номерата на пратките.

21.3.2. *Предаване в рамките на сграда или група от сгради*

В рамките на дадена сграда или група от сгради класифицираните документи могат да се пренасят в запечатан плик, върху който е обозначено само името на адресата, при условие че пратката се пренася от лице, което има разрешение за достъп до степента на класифициране на документите.

21.3.3. *Предаване в рамките на държава*

1. В рамките на дадена държава ►M1 RESTREINT UE ◄ документи следва да се изпращат единствено чрез официална куриерска служба или чрез лица, които имат право на достъп до ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ.

2. Когато за предаването на ►M1 RESTREINT UE ◄ ДОКУМЕНТ извън пределите на сграда или група от сгради се използва куриерска служба, се съблюдават съдържащите се в настоящата глава разпоредби за опаковане и получаване. Персоналът в службите за доставка се подбира така, че да се гарантира непрекъснат надзор на пратките, които съдържат ►M1 RESTREINT UE ◄ ДОКУМЕНТИ от отговорно длъжностно лице.

3. По изключение ►M1 RESTREINT UE ◄ ДОКУМЕНТИ могат да се пренасят от други длъжностни лица, освен куриери, извън пределите на сграда или група от сгради за ползване на място по време на заседания и обсъждания, при условие че:

   а) приносителят има право на достъп до тези ►M1 RESTREINT UE ◄ ДОКУМЕНТИ;

   б) начинът на пренасяне отговаря на правилата, регулиращи предаването на ►M1 RESTREINT UE ◄ ДОКУМЕНТИ;

   в) длъжностното лице при никакви обстоятелства не оставя без надзор ►M1 RESTREINT UE ◄ ДОКУМЕНТИ;

   г) са взети мерки в службата за регистрация на ►M1 RESTREINT UE ◄ документи, в която се държат документите, да има списък на пренасяните по този начин документи и те да бъдат записани в дневник, в който да се извърши отметка при връщането им.

4. В рамките на дадена държава ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ ДОКУМЕНТИ могат да се изпращат по пощата, ако такъв вид предаване е разрешено съгласно националните разпоредби и отговаря на изискванията на тези разпоредби, или чрез куриерска служба, или чрез лица, които имат право на достъп до класифицирана информация на ЕС.

▼B

5. ►M2 Дирекция по сигурността на Комисията ◄ ще изготви инструкции за личното пренасяне на класифицирани документи на ЕС въз основа на настоящите правила. Приносителят трябва да прочете и подпише тези инструкции. По-конкретно в инструкциите ясно се посочва, че при никакви обстоятелства документите не могат:

   а) да напускат притежанието на приносителя, освен ако са на безопасно съхранение в съответствие с разпоредбите на раздел 18;

   б) да бъдат оставяни без надзор в обществен транспорт или в частни превозни средства, или на такива места, като ресторанти или хотели. Те не могат да се съхраняват в хотелски сейфове или да се оставят без надзор в хотелски стаи;

   в) да се четат на обществени места като самолети или влакове.

21.3.4. *Предаване от една държава в друга държава*

1. Материали с ►M1 RESTREINT UE ◄ или по-висока степен на класифициране на ЕС се пренасят чрез дипломатически или военни куриерски служби.

2. Въпреки това може да се разрешава лично пренасяне на материали със ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ степен на класифициране, ако разпоредбите за пренасянето гарантират, че материалите не могат да попаднат в лице, което няма разрешение за това.

3. Членът на Комисията, който отговаря за въпросите на сигурността, може да дава разрешение за лично пренасяне, когато няма на разположение дипломатически и военни куриери, или когато използването на такива куриери би довело до забавяне, което би било пагубно за операциите на ЕС и получателят, за когото е предназначен материалът, спешно се нуждае от него. ►M2 Дирекция по сигурността на Комисията ◄ ще изготви инструкции за личното пренасяне през граница на материали със степен на класифициране до и включително ►M1 RESTREINT UE ◄ степен на класифициране от други лица, освен дипломатически и военни куриери. Инструкциите изискват:

   а) приносителят да има съответното разрешение за достъп до секретни материали;

   б) в съответния отдел или служба за регистрация да се води досие за всички пренасяни по този начин материали;

   в) върху пакетите или чантите, съдържащи материали на ЕС, да има поставен официален печат, който да предотвратява или възпира извършването на митнически проверки, както и етикети с идентификационни данни и инструкции за лицата, намерили такива пакети или чанти;

   г) приносителят да носи куриерско сертификат и/или заповед за мисия, които се признават от всички държави-членки на ЕС и му дават право да пренася посочения пакет;

   д) при пътуване по суша да не се пресича границата или да не се преминава през територията на държава, която не е държава-членка на ЕС, освен ако изпращащата държава разполага с особени гаранции от тази държава;

   е) организацията на пътуването на приносителя по отношение на местоназначения, маршрути и транспортни средства, които ще се използват, трябва да са в съответствие с правилата на ЕС или — ако националните разпоредби по тези въпроси са по-строги — в съответствие с тези разпоредби;

   ж) материалът не трябва да напуска притежанието на приносителя, освен ако се съхранява в съответствие с разпоредбите за безопасно съхранение, посочени в раздел 18;

   з) материалът не трябва да се оставя без надзор в обществени или частни превозни средства или на такива места като ресторанти или хотели. Той не трябва да се съхранява в хотелски сейфове или да се оставя без надзор в хотелски стаи;

   и) ако пренасяният материал съдържа документи, те не трябва да се четат на обществени места (например самолети, влакове и др.).

▼B

4. Лицето, което е определено да пренася класифицирания материал, трябва да прочете и да подпише инструктаж за сигурност, който да съдържа най-малко изброените по-горе инструкции и процедурите, които трябва да се следват в аварийна ситуация или в случай че пакетът, който съдържа класифицирания материал, е подложен на проверка от митнически служители или служители, отговарящи за сигурността на летищата.

21.3.5. *Предаване на документи* ►**M1** *RESTREINT UE* ◄

Не се предвиждат особени разпоредби за пренасянето на документи ►**M1** RESTREINT UE ◄, освен че пренасянето им трябва да се осъществява така, че те да не могат да попаднат у лице, което няма разрешение за това.

21.4. **Сигурност на куриерския персонал**

Всички куриери и пратеници, които се наемат да пренасят ►**M1** RESTREINT UE ◄ и ►**M1** RESTREINT UE ◄ документи, имат подходящо разрешение за достъп до секретни материали.

21.5. **Електронни и други средства за техническо предаване**

1. Предвиждат се мерки за сигурност на комуникациите, които да гарантират безопасното предаване на класифицирана информация на ЕС. Подробните правила за предаването на такава класифицирана информация на ЕС са разгледани в раздел 25.

2. ►**M1** RESTREINT UE ◄ и ►**M1** RESTREINT UE ◄ информация може да се предава само от акредитирани комуникационни центрове и мрежи и/или терминали и системи.

21.6. **Допълнителни екземпляри, преводи или извлечения от класифицирани документи на ЕС**

1. Единствено авторът може да дава разрешение за копиране или превод на ►**M1** RESTREINT UE ◄ ДОКУМЕНТИ.

2. Ако лица, които нямат разрешение за достъп до ►**M1** RESTREINT UE ◄ МАТЕРИАЛИ, се нуждаят от информация, която макар и съдържаща се в ►**M1** RESTREINT UE ◄ документ, няма такава степен на класифициране, началникът на службата за регистрация на ►**M1** RESTREINT UE ◄ МАТЕРИАЛИ (виж раздел 22.2) може да бъде оторизиран да изготви необходимия брой извлечения от този документ. Същевременно той/тя предприема необходимите стъпки, с които да се гарантира определянето на подходяща степен на класификация за сигурност на тези извлечения.

3. Документите със ►**M1** RESTREINT UE ◄ или ПО-НИСКА СТЕПЕН НА КЛАСИФИЦИРАНЕ могат да се възпроизвеждат и превеждат от адресата в пределите, определени от настоящите разпоредби за сигурност, и при условие че стриктно се съблюдава принципа за „необходимост да се знае“. Приложимите мерки за сигурност за оригиналния документ са приложими и за неговото възпроизвеждане и/или превод.

22. СЛУЖБИ ЗА РЕГИСТРАЦИЯ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС, ИНВЕНТАРНИ СПИСЪЦИ, ПРОВЕРКИ И УНИЩОЖАВАНЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

22.1. **Местни служби за регистрация на класифицирана информация на ЕС**

1. В рамките на Комисията, при необходимост във всеки отдел, една или повече служби за регистрация на класифицирана информация на ЕС отговарят за регистрацията, възпроизвеждането, изпращането, архивирането и унищожаването на документи със ►**M1** RESTREINT UE ◄ и ►**M1** RESTREINT UE ◄ СТЕПЕН НА КЛАСИФИЦИРАНЕ.

2. Когато в даден отдел няма служба за регистрация на класифицирана информация на ЕС, нейните функции се изпълняват от местната служба за регистрация на класифицирана информация на ЕС на генералния секретариат.

3. Местните служби за регистрация на класифицирана информация на ЕС докладват пред началника на отдела, от който получават инструкции. Началникът на тези служби за регистрация на класифицирана информация на ЕС е отговорен за регистрирането на контрола на службата.

▼B

4. Те подлежат на надзор от страна на служителя, отговорен за сигурността на местно равнище по отношение на прилагането на разпоредбите за работа с класифицирани документи на ЕС и съблюдаването на съответните мерки за сигурност.

5. Длъжностните лица, които работят в местните служби за регистрация на класифицирана информация на ЕС, имат достъп до такава информация в съответствие с разпоредбите на раздел 20.

6. Под ръководството на съответния началник на отдел, местните служби за регистрация на класифицирана информация на ЕС:

   а) ръководят операциите по регистрация, възпроизвеждане, превод, предаване, изпращане и унищожаване на такава информация;

   б) актуализират списъка с данни за класифицираната информация;

   в) периодично разглеждат въпроси, свързани с необходимостта от поддържане на класификацията на информацията.

7. Местните служби за регистрация на класифицирана информация на ЕС водят регистър на следните данни:

   а) датата на изготвяне на класифицираната информация;

   б) степента на класифициране;

   в) датата на изтичане на срока на класификацията;

   г) името и отдела на потребителя;

   д) получателя или получателите с пореден номер;

   е) предмета на информацията;

   ж) номер;

   з) брой разпространени екземпляри;

   и) изготвянето на инвентарни списъци на предоставената на отдела класифицирана информация;

   й) регистър за декласифициране или понижаване на степента на класифициране на класифицирана информация.

8. За местните служби за регистрация на класифицирана информация на ЕС се прилагат за общите правила, предвидени в раздел 21, освен ако те са изменени с особените правила, предвидени в настоящия раздел.

22.2. **Служба за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ**

22.2.1. *Общи положения*

1. Централна служба за регистрация на класифицирана информация на ЕС гарантира регистрирането, работата и разпространението на ►M1 RESTREINT UE ◄ ДОКУМЕНТИ в съответствие с настоящите разпоредби за сигурност. Началникът на СЛУЖБАТА ЗА РЕГИСТРАЦИЯ НА ►M1 RESTREINT UE ◄ информация ще изпълнява функциите на служителя, които отговаря за контрола на службата за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ.

2. Централната служба за регистрация на класифицирана информация на ЕС ще изпълнява функциите на главен получаващ и изпращащ орган на Комисията при взаимоотношенията ѝ с останалите институции на ЕС, държавите-членки, международни организации и трети държави, с които Комисията има споразумения относно процедурите за сигурност при размяната на класифицирана информация.

3. Когато е необходимо, се създават подразделения, които ще отговарят за вътрешното управление на ►M1 RESTREINT UE ◄ ДОКУМЕНТИ; те водят актуални регистри за движението на всеки документ, за който отговаря подразделението.

▼B

4. При наличие на дългосрочна необходимост се създават подразделения на службите за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, както е посочено в раздел 22.2.3, които са подчинени на една централна служба за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ. При необходимост от временно и извънредно извършване на справка със ►M1 RESTREINT UE ◄ ДОКУМЕНТИ, тези документи могат да се предоставят без да се създава подразделение за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, при условие че се предвидят правила, които да гарантират, че документите остават под контрола на съответната служба за регистрация на класифицирана информация на ЕС и че се съблюдават всички физически мерки за сигурност и такива, които се отнасят за персонала.

5. Подразделенията не могат пряко да предават ►M1 RESTREINT UE ◄ ДОКУМЕНТИ на други подразделения на същата централна служба за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ без нейно изрично съгласие.

6. Всяка размяна на ►M1 RESTREINT UE ◄ ДОКУМЕНТИ между подразделения, които не са подчинени на една и съща централна служба за регистрация, се извършва чрез централните служби за регистрация на ►M1 RESTREINT UE ◄ информация.

22.2.2. *Централна служба за регистрация на* ►M1 *RESTREINT UE* ◄ *информация*

В качеството си на служител, отговорен за контрола, началникът на централната служба за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ отговаря за:

а) предаването на ►M1 RESTREINT UE ◄ ДОКУМЕНТИ в съответствие с разпоредбите, определени в раздел 21.3;

б) поддържането на списък на всички подразделения на службата за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, които са нейно подчинение, заедно с имената и подписите на назначените контрольори и техните упълномощени заместници;

в) съхранението на разписките от службите за регистрация за всички ►M1 RESTREINT UE ◄ ДОКУМЕНТИ, които са разпространени от централната служба;

г) поддържането на регистър на съхраняваните и разпространени ►M1 RESTREINT UE ◄ ДОКУМЕНТИ;

д) поддържането на актуален списък на всички централни служби за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, с които той/тя обичайно отговаря, заедно с имената и подписите на назначените в тях контрольори и техните упълномощени заместници;

е) физическата защита на всички съхранявани в службата за регистрация ►M1 RESTREINT UE ◄ ДОКУМЕНТИ в съответствие с разпоредбите, предвидени в раздел 18.

22.2.3. *Подразделения на службите за регистрация на* ►M1 *RESTREINT UE* ◄ *ИНФОРМАЦИЯ*

В качеството си на служител, който осъществява контрола, началникът на подразделение на служба за регистрация на ►M1 RESTREINT UE ◄ информация отговаря за:

а) предаването на ►M1 RESTREINT UE ◄ ДОКУМЕНТИ в съответствие с разпоредбите, определени в точка 21.3;

б) поддържането на актуален списък на всички лица, които имат разрешение за достъп до контролираната от него ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ;

в) разпространението на ►M1 RESTREINT UE ◄ ДОКУМЕНТИ в съответствие с указанията на автора или въз основа на принципа за „необходимост да се знае“ след предварителна проверка дали адресатът има необходимото разрешение за достъп до ►M1 RESTREINT UE ◄ материали;

г) поддържането на актуален регистър на всички ►M1 RESTREINT UE ◄ ДОКУМЕНТИ, които се съхраняват или разпространяват под негов контрол, или които са предадени на други служби за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, и за съхранението на всички съответни разписки;

▼B

д) поддържането на актуален списък на службите за регистрация на ►M1 RESTREINT UE ◄ информация, с които той има право да обменя ►M1 RESTREINT UE ◄ ДОКУМЕНТИ, заедно с имената и подписите на назначените в тях служители, отговорни за контрола и техните упълномощени заместници;

е) физическата защита на всички съхранявани в подразделението ►M1 RESTREINT UE ◄ ДОКУМЕНТИ в съответствие с разпоредбите, предвидени в раздел 18.

22.3. **Инвентарни описи, прегледи и проверки на класифицирани документи на ЕС**

1. Всяка година всяка от посочените в настоящия раздел служби за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ извършват подробна инвентаризация на ►M1 RESTREINT UE ◄ ДОКУМЕНТИ. Даден документ се счита за инвентаризиран, ако службата за регистрация физически разполага с него или с разписка от службата за регистрация на ►M1 RESTREINT UE ◄ ДОКУМЕНТИ, на която документът е бил прехвърлен, със сертификат за унищожаването на документа или с указание за понижаване на степента на класифициране или за декласифициране на този документ. Най-късно до 1 април всяка година те изпращат констатациите от годишните инвентаризации на члена на Комисията, който отговаря за въпросите на сигурността.

2. Подразделенията на службите за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ изпращат констатациите от годишните си инвентаризации на централната служба за регистрация, на която са подчинени на определена от нея дата.

3. Класифицираните документи на ЕС с по-ниска от ►M1 RESTREINT UE ◄ степен на класифициране подлежат на вътрешни проверки в съответствие с указанията на члена на Комисията, който отговаря по въпросите на сигурността.

4. Тези действия имат за цел да се получи становището на притежателите на документите относно:

а) възможността за понижаване на степента на класифициране или за декласифициране на определени документи;

б) подлежащите на унищожаване документи.

22.4. **Архивно съхранение на класифицирана информация на ЕС**

1. Класифицираната информация на ЕС се съхранява при условия, които отговарят на съответните изисквания, изброени в раздел 18.

2. С оглед свеждане до минимум на проблемите, които са свързани със съхранението, контрольорите на всички служби за регистрация имат право да разпореждат ►M1 RESTREINT UE ◄, ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ ДОКУМЕНТИ да се заснемат на микрофилми или да се съхраняват по друг начин на магнитни или оптични информационни носители с архивна цел, при условие че:

а) процесът на микрофилмиране/съхранение се извършва от персонал с валидно разрешение за достъп до секретни материали със съответната степен на класифициране;

б) на микрофилма/информационния носител се осигурява същата сигурност, каквато се осигурява на оригиналните документи;

в) заснемането на микрофилм/съхранението на всеки ►M1 RESTREINT UE ◄ ДОКУМЕНТ се съобщава на автора;

г) филмовите ролки или други видове информационни носители съдържат само документи с една и съща ►M1 RESTREINT UE ◄, ►M1 RESTREINT UE ◄ или ►M1 RESTREINT UE ◄ степен на класифициране;

▼B

д) микрофилмирането/съхранението на ►M1 RESTREINT UE ◄ или ►M1 RESTREINT UE ◄ ДОКУМЕНТ ясно се посочва в регистъра, който се използва за годишната инвентаризация;

е) оригиналните документи, които са заснети на микрофилм или са съхранени другояче, се унищожават в съответствие с правилата, посочени в раздел 22.5.

3. Тези правила важат и за всяка друга форма на оторизирано съхранение, като електромагнитен носител или оптичен диск.

22.5. **Унищожаване на класифицирани документи на ЕС**

1. За да се предотврати ненужното натрупване на класифицирани документи на ЕС, онези от тях, които началникът на отдела, който ги държи, счита за остарели или прекомерно много на брой, възможно най-скоро се унищожават по следния начин:

а) ►M1 RESTREINT UE ◄ ДОКУМЕНТИ се унищожават само от централната служба по регистрация, която отговаря за тях. Всеки унищожен документ се изброява в сертификат за унищожаване, което се подписва от контрольора на службата за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ и от длъжностното лице, което присъства на унищожаването, и което трябва да има разрешение за достъп до ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ. Унищожаването се отбелязва в дневника;

б) службата за регистрация съхранява сертификатите за унищожаване заедно с формулярите за разпространение в продължение на десет години. Копия се изпращат на автора и съответната централна служба за регистрация само при изрично поискване;

в) ►M1 RESTREINT UE ◄ ДОКУМЕНТИ, включително всички класифицирани отпадъци от изготвянето на ►M1 RESTREINT UE ◄ ДОКУМЕНТИ като повредени екземпляри, работни проекти, печатни записки, флопи дискове, се унищожават под надзора на служител, отговорен за контрола на службата за регистрация на ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, чрез изгаряне, претопяване, нарязване на тънки ивици или чрез намаляване по друг начин до неузнаваема и неподлежаща на възстановяване форма.

2. ►M1 RESTREINT UE ◄ ДОКУМЕНТИ се унищожават от службата за регистрация, която отговаря за тях, под надзора на лице, което има разрешение за достъп до секретни материали, с помощта на един от процесите, посочени в параграф 1, буква в). Унищожените ►M1 RESTREINT UE ◄ ДОКУМЕНТИ се изброяват в подписани сертификати за унищожаване, които се съхраняват в службата за регистрация, заедно с формулярите за разпространение, в продължение на най-малко три години.

3. ►M1 RESTREINT UE ◄ ДОКУМЕНТИ се унищожават от службата за регистрация, която отговаря за тях, под надзора на лице, което има разрешение за достъп до такива материали, с помощта на един от процесите, посочени в параграф 1, буква в). Тяхното унищожаване се регистрира съгласно указанията на члена на Комисията, който отговаря за въпросите на сигурността.

4. Документи ►M1 RESTREINT UE ◄ се унищожават от службата за регистрация, която отговаря за тях или от потребителя съгласно указанията на члена на Комисията, който отговаря за въпросите на сигурността.

22.6. **Унищожаване в аварийни ситуации**

1. Отделите на Комисията изготвят съобразени с условията на място планове за защита на класифицирани материали на ЕС в кризисна ситуация, при необходимост включително планове за унищожаване и евакуация. Те разпространяват инструкции, които считат за необходими за предотвратяване попадането на класифицирана информация на ЕС у лица, които нямат разрешение за това.

▼B

2. Мерките за защита и/или унищожаване на ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ материали в кризисна ситуация при никакви обстоятелства не се отразяват неблагоприятно на защитата или унищожаването на ►M1 RESTREINT UE ◄ МАТЕРИАЛИ, включително шифриращото оборудване, чието третиране има предимство пред всички останали задачи.

3. Мерките, които трябва да се предприемат за защита и унищожаване на шифриращо оборудване в аварийна ситуация, са предмет на специални инструкции.

4. На място трябва да има инструкции в запечатан плик. Трябва да са на разположение средства/инструменти за унищожаване.

23. МЕРКИ ЗА СИГУРНОСТ ПРИ СПЕЦИФИЧНИ СРЕЩИ, КОИТО СЕ ПРОВЕЖДАТ ИЗВЪН ПОМЕЩЕНИЯТА НА КОМИСИЯТА И ПО ВРЕМЕ НА КОИТО СЕ ИЗПОЛЗВА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

23.1. **Общи положения**

Когато се провеждат заседания на Комисията или други важни срещи извън помещенията на Комисията, и когато това е обосновано от особени изисквания за сигурност във връзка с високата степен на деликатност на разглежданите въпроси или информация, се предприемат описаните по-долу мерки за сигурност. Тези мерки се отнасят само за защитата на класифицирана информация на ЕС; могат да се планират и други мерки за сигурност.

23.2. **Отговорности**

23.2.1. ►M2 *Дирекция по сигурността на Комисията* ◄

►M2 Дирекция по сигурността на Комисията ◄ сътрудничи с компетентните органи на държавата-членка, на чиято територия се провежда срещата (приемащата държава-членка), за да се гарантира сигурността на заседанието на Комисията или на други важни срещи, както и сигурността на делегатите и техните служители. По отношение на защитата на сигурността, ►M2 дирекция по сигурността на Комисията ◄ по-конкретно гарантира, че:

а) са изготвени планове за справяне със заплахи за сигурността и с инциденти, свързани със сигурността, като въпросните мерки по-конкретно включват безопасното съхранение на класифицирана информация на ЕС в служебни помещения;

б) са предприети мерки за евентуално предоставяне на достъп до комуникационните системи на Комисията за получаване и предаване на класифицирани съобщения на ЕС. При необходимост от приемащата държава-членка ще се изисква да предоставя достъп до сигурни телефонни системи.

►M2 Дирекция по сигурността на Комисията ◄ изпълнява функциите на съветник по сигурността при подготовката на срещата; на срещата трябва да присъства неин представител, който при необходимост да подпомага и да съветва завеждащия сигурността на срещата и делегациите.

От всяка делегация се изисква да определи свой завеждащ сигурността, който ще отговаря за въпросите на сигурността в рамките на своите пълномощия и за поддържането на връзка със завеждащия сигурността на срещата, както и при необходимост със ►M2 дирекция по сигурността на Комисията ◄.

23.2.2. *Завеждащ сигурността на среща (MSO)*

Определя се служител, отговарящ за сигурността на срещата, който отговаря за общата подготовка и контрол на общите вътрешни мерки за сигурност, и за сътрудничеството с останалите заинтересовани органи за сигурност. Мерките, които се предприемат от завеждащия сигурността на срещата, поначало се отнасят за:

а) предпазните мерки на мястото на срещата, които да гарантират провеждането на срещата без инциденти, които биха могли да изложат на риск сигурността на всяка евентуално използвана там класифицирана информация на ЕС;

▼B

б) проверката на персонала, който има право на достъп до мястото на срещата, до зоните, които са определени за делегациите и до конферентните зали, както и проверката на всякаква апаратура;

в) постоянната координация с компетентните органи на приемащата държава-членка и със ►M2 дирекция по сигурността на Комисията ◄;

г) включването на инструкции за сигурност в досието за срещата при надлежно съблюдаване на изискванията, предвидени в настоящите правила за сигурност, както и всякакви други инструкции за сигурност, които се считат за необходими.

23.3. **Мерки за сигурност**

23.3.1. *Зони на сигурност*

Създават се следните зони на сигурност:

а) зона за сигурност от клас II, състояща се от редакционна зала, служебните помещения на Комисията и репрографско оборудване, както и служебните помещения на делегациите, когато е уместно;

б) зона за сигурност от клас I, състояща се от конферентната зала и кабините на преводачите и специалистите по озвучаване;

в) административни зони, състоящи се от зоната за журналисти и онези части от мястото на срещата, които се използват за административни цели, снабдяване с храни и напитки и настаняване, както и зоната, която се намира в непосредствена близост до пресцентъра и мястото на срещата.

23.3.2. *Пропуски*

Завеждащият сигурността на срещата издава съответни обозначителни знаци съгласно изискванията на делегациите и в зависимост от техните потребности. Когато е необходимо, може да се прави разграничение по отношение на достъпа до различни зони за сигурност.

Инструкциите за сигурност във връзка със срещата изискват всички съответни лица непрекъснато да носят обозначителните си знаци, поставени на видно място, в рамките на мястото на срещата, така че при необходимост те да могат да бъдат проверявани от служителите, които отговарят за сигурността.

Освен участниците, които носят обозначителни знаци, до мястото на срещата се допускат възможно най-малък брой хора. Завеждащият сигурността на срещата разрешава на националните делегации да приемат посетители по време на срещата само по тяхно искане. На посетителите следва да се дава обозначителен знак за посетители. Попълва се формуляр за издаване на пропуск за посетители, в който се посочва името на посетителя и името на лицето, при което той/тя отива. Посетителите през цялото време се придружават от служител от охраната или от посетеното лице. Формулярът за издаване на пропуск на посетител се носи от придружаващото лице и при напускане на посетителя на мястото на срещата, заедно с обозначителния знак за посетители се връща на служителите, които отговарят за сигурността.

23.3.3. *Проверка на фотографска и аудиотехника*

В зона за сигурност от клас I не могат да се внасят фотоапарати или записваща техника, с изключение на техниката, която се внася от надлежно упълномощените от завеждащия сигурността на срещата фотографи и озвучители.

23.3.4. *Проверка на чанти за документи, преносими компютри и пакети*

Притежателите на пропуски, които имат право на достъп до зона за сигурност, обикновено могат да внасят своите чанти за документи и преносими компютри (само такива, които са със собствено захранване), без да се извършва проверка. В случай на пакети за делегации, делегациите могат да получават пакетите, които се проверяват от завеждащия сигурността на делегацията, проверяват се с помощта на специална техника или се отварят за проверка от служителите, които отговарят за сигурността. По преценка на завеждащия сигурността на срещата могат да се предвидят по-строги мерки за проверка на чанти за документи и пакети.

▼B

23.3.5. *Техническа сигурност*

Залата, в която се провежда срещата, може технически да се обезопаси от технически екип за сигурност, който може да провежда и електронно наблюдение по време на срещата.

23.3.6. *Документи на делегациите*

Делегациите отговарят за донасянето и отнасянето от срещите на класифицирани документи на ЕС. Те отговарят и за проверката и сигурността на тези документи по време на използването им в определените за делегациите помещения. За транспортирането на класифицирани документи до и от мястото на срещата може да се иска съдействие от приемащата държава-членка.

23.3.7. *Безопасно съхранение на документи*

Ако Комисията или делегациите не могат да съхраняват класифицираните си документи в съответствие с одобрените стандарти, те могат да депозират тези документи в запечатан плик при завеждащия сигурността на срещата срещу разписка, така че той да съхранява документите в съответствие с одобрените стандарти.

23.3.8. *Проверки на служебни помещения*

Завеждащият сигурността на срещата разпорежда служебните помещения на Комисията и на делегациите да се проверяват в края на всеки работен ден, за да се гарантира, че всички класифицирани документи на ЕС се съхраняват на сигурно място. В противен случай той/тя предприема необходимите мерки.

23.3.9. *Изхвърляне на класифицирани отпадъци на ЕС*

Всички отпадъци се третират като класифицирани отпадъци на ЕС, а кошчетата или торбите за хартиени отпадъци следва да се предават на Комисията и делегациите за изхвърляне. Преди да напуснат определените им помещения, Комисията и делегациите отнасят отпадъците си на завеждащия сигурността на срещата, който разпорежда унищожаването им съгласно правилата.

В края на срещата всички документи, които се притежават, но вече не са нужни на Комисията или делегациите, се третират като отпадъци. Преди да бъдат вдигнати предприетите за срещата мерки за сигурност, се извършва щателна проверка на помещенията на Комисията и на делегациите. Документите, за които е подписана разписка, доколкото е практически приложимо, се унищожават в съответствие с предписанията в раздел 22.5.

24. НАРУШЕНИЯ НА РАЗПОРЕДБИТЕ ЗА СИГУРНОСТ И ИЗЛАГАНЕ НА РИСК НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

24.1. **Определения**

Нарушение на сигурността настъпва в резултат на действие или бездействие, противоречащо на разпоредба за сигурност на Комисията, което би могло да застраши или да изложи на риск класифицирана информация на ЕС.

Излагане на риск на класифицирана информация на ЕС настъпва, когато тя изцяло или отчасти е попаднала у лица, които нямат разрешение за това, т.е. лица, които нито имат съответното разрешение за достъп до секретни материали, нито е „необходимо да знаят“, или когато съществува вероятност от настъпване на такова събитие.

Класифицирана информация на ЕС може да бъде изложена на риск вследствие на небрежност, непредпазливост или недискретност, както и от служби, чиято дейност е насочена срещу ЕС или неговите държави-членки по отношение на класифицирана информация и дейности на ЕС, или от организации, занимаващи се с подривна дейност.

24.2. **Докладване за нарушения на разпоредбите за сигурност**

Всички лица, които трябва да работят с класифицирана информация на ЕС, подробно се инструктират за отговорностите им в това отношение. Те веднага докладват за всяко нарушение на сигурността, което евентуално е достигнало да знанието им.

▼B

Когато служител, отговорен за сигурността на местно равнище или завеждащ сигурността на среща установи или е информиран за нарушение на сигурността, свързано с класифицирана информация на ЕС, или за загубата или изчезването на класифициран материал на ЕС, той/тя предприема своевременни действия за:

а) запазване на доказателствата;

б) установяване на обективната истина;

в) оценка и свеждане до минимум на нанесените щети;

г) предотвратяване на повторно извършване на нарушението;

д) нотифициране на съответните органи за последиците от нарушението на сигурността.

В този контекст се предоставя следната информация:

i) описание на съответната информация, включително нейната степен на класифициране, референтен номер и брой копия, дата, автор, предмет и приложно поле;

ii) кратко описание на обстоятелствата, при които е извършено нарушението на сигурността, включително датата и периодът, през който информацията е била изложена на риск;

iii) дали авторът е бил информиран.

Всеки орган за сигурност е длъжен веднага, след като бъде нотифициран за евентуалното извършване на такова нарушение на сигурността, да докладва за това на ►M2 дирекция по сигурността на Комисията ◄.

Случаите, които касаят информация►M1 RESTREINT UE ◄, трябва да се докладват само, когато се характеризират с необичайни особености.

След като бъде информиран за извършването на нарушение на сигурността, членът на Комисията, който отговаря за въпросите на сигурността:

а) нотифицира органа, който е автор на въпросната класифицирана информация;

б) изисква от съответните органи за сигурност да започнат разследване;

в) координира разследването, когато от случая са заинтересовани повече от един орган за сигурност;

г) получава доклад за обстоятелствата, при които е извършено нарушението, датата или периода на евентуалното му извършване и разкриване, заедно с подробно описание на съдържанието и степента на класифициране на съответния материал. В доклада се посочват и нанесените вреди на интересите на ЕС или на една или повече от неговите държави-членки, и предприетите действия за предотвратяване на повторното извършване на нарушението.

Органът автор информира адресатите и дава подходящи указания.

24.3. **Правни действия**

Всяко физическо лице, което носи отговорност за излагането на риск на класифицирана информация на ЕС, подлежи на дисциплинарно производство съгласно съответните правила и нормативни разпоредби, особено разпоредбите на дял VI от Правилника за длъжностните лица на ЕО. Това производство не е пречка за предприемането на други допълнителни правни действия.

В съответните случаи, въз основа на доклада, посочен в раздел 24.2, членът на Комисията, който отговаря за въпросите на сигурността, предприема необходимите стъпки за предоставяне на възможност на компетентните национални органи да образуват наказателно производство.

▼B

25. ЗАЩИТА НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС, КОЯТО СЕ ОБРАБОТВА В ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ

25.1. **Въведение**

25.1.1. *Общи положения*

Политиката и изискванията за сигурност се прилагат за всички комуникационни и информационни системи и мрежи (наричани по-долу системи), в които се обработва информация с ►M1 RESTREINT UE ◄ и по-висока степен на класифициране. Те се прилагат в допълнение към изискванията, предвидени в окончателния вариант на Решение C (95) 1510 на Комисията от 23 ноември 1995 г. относно защитата на информационните системи.

Системите, в които се обработва информация ►M1 RESTREINT UE ◄, също се нуждаят от мерки за сигурност с оглед запазване на поверителния характер на тази информация. Всички системи се нуждаят от мерки за сигурност, за да се защитава целостта и съществуването на тези системи и на съдържащата се в тях информация.

Прилаганата от Комисията политика за информационно-технологична сигурност се характеризира със следните елементи:

— тя представлява неразделна част от сигурността изобщо и допълва всички елементи на информационната сигурност, сигурността на персонала и физическата сигурност,

— поделяне на отговорностите между собствениците на техническите системи, собствениците на съхраняваната или обработваната в техническите системи класифицирана информация на ЕС, специалистите по информационно-технологична сигурност и потребителите,

— описание на принципите и изискванията за сигурност на всяка информационно-технологична система,

— утвърждаване на тези принципи и изисквания от определен орган,

— отчитане на специфичните заплахи и уязвими места в сферата на информационните технологии.

25.1.2. *Заплахи за и уязвимост на системите*

Заплахата може да се определи като потенциална възможност за случайно или умишлено излагане на риск на сигурността. При системи такова излагане на риск предполага загуба на едно или повече от свойствата поверителност, цялост и наличност. Уязвимостта може да се определи като слабост или липса на контрол, които биха улеснили или позволили поставянето под заплаха на конкретно имущество или цел.

Класифицираната и некласифицираната информация на ЕС, която се обработва в системи в концентрирана форма, предназначена да осигурява бързо извличане, съобщаване и използване, е уязвима за много заплахи. Те включват достъп до информацията на неоторизирани потребители, или обратно — отказ на достъп на оторизирани потребители. Това са също така рисковете от неразрешено оповестяване, повреждане, промяна или заличаване на информацията. Освен това сложното и понякога чупливо оборудване често е трудно и скъпо да се ремонтира или бързо да се подмени.

25.1.3. *Главна цел на мерките за сигурност*

Главната цел на посочените в настоящия раздел мерки за сигурност е да се осигурява защита срещу неоторизирано оповестяване на класифицирана информация на ЕС (загуба на поверителния характер) и срещу загуба на целостта и наличието на информацията. За да се постигне достатъчна защита на сигурността на система, в която се обработва класифицирана информация на ЕС, ►M2 дирекция по сигурността на Комисията ◄ определя подходящите стандарти за конвенционална сигурност, заедно с подходящи специални процедури и техники за сигурност, които са конкретно предназначени за всяка система.

▼B

25.1.4. *Декларация за специфичните изисквания за сигурност на системата (SSRS)*

За всички системи, в които се обработва информация с ►M1 RESTREINT UE ◄ и по-висока степен на класифициране, се изисква да се изготви декларация за специфичните изисквания за сигурност на системата от собственика на техническата система (TSO, виж раздел 25.3.4) и собственика на информацията (виж раздел 25.3.5), когато е необходимо в сътрудничество и с помощта на персонала, който отговаря за проекта и на ►M2 дирекция по сигурността на Комисията ◄ (в качеството на орган по сигурността на информацията — ОСИ, виж раздел 25.3.3), която декларация се одобрява от акредитиращия орган по сигурността (SAA, виж раздел 25.3.2).

Декларация за специфичните изисквания за сигурност на системата се изисква, и когато акредитиращият орган по сигурността (SAA) счита, че наличието и целостта на информация ►M1 RESTREINT UE ◄ или на некласифицирана информация са от съществено значение.

Декларацията за специфичните изисквания за сигурност на системата се формулира на най-ранния етап от разработването на проект, след което се доразвива и усъвършенства с напредването на проекта, като изпълнява различна роля на различните етапи от проекта и от жизнения цикъл на системата.

25.1.5. *Режими на работа при условия на сигурност*

Всички системи, в които се обработва информация с ►M1 RESTREINT UE ◄ и по-висока степен на класифициране, се акредитират за работа в един или когато това е обосновано от изискванията през различни периоди от време, повече от един от следните режими на работа при условия на сигурност или техен национален аналог:

а) специален,

б) високосистемен, и

в) многостепенен.

25.2. **Определения**

„Акредитация“ означава даденото за определена система разрешение и одобрение да обработва класифицирана информация на ЕС в нейната операционна среда.

Забележка:

Такава акредитация следва да се дава, след като са изпълнени всички необходими процедури за сигурност и е постигната достатъчна степен на защита на системните ресурси. Обикновено акредитацията се извършва въз основа на декларацията за специфичните изисквания за сигурност на системата и включва следното:

а) декларация за целите на акредитиране на системата; по-специално, информация с каква/и степен/и на класифициране ще се обработва и какъв/ви режим/и на работа при условия на сигурност на системата или мрежата се предлагат;

б) представяне на проучване относно управлението на риска с цел идентифициране на заплахите и уязвимите места, и на мерките за противодействие на тези заплахи и уязвими места;

в) процедурите за сигурност при работа (SecOPS) с подробно описание на предлаганите операции (например режими и обслужване, които трябва да се осигурят), включително описание на характеристиките за сигурност на системата, на които се основава акредитацията;

г) плана за осъществяване и поддръжка на характеристиките за сигурност;

д) плана за първоначалното и последващо изпитване, оценка и сертифициране за сигурност на системата или мрежата, и

е) когато е необходимо — сертифициране, заедно с други елементи на акредитиране.

▼B

„Служител, отговарящ за сигурността на информацията на централно равнище“ (CISO) означава длъжностното лице в централна информационно-технологична служба, което координира и контролира мерките за сигурност за централно организираните системи.

„Сертифициране“ означава издаването на официална декларация, подкрепена от независим преглед на начина на извършване на оценка и резултатите от нея, който показва до каква степен дадена система отговаря на изискванията за сигурност или даден продукт за компютърна сигурност осигурява предварително зададените характеристики за сигурност.

„Сигурност на комуникациите“ (COMSEC) означава прилагането на мерки за сигурност спрямо далекосъобщенията с цел отказване на достъп на неупълномощени лица до ценна информация, която би могла да се придобие чрез притежаването и проучването на такива далекосъобщения, или за да се гарантира достоверността на тези далекосъобщения.

Забележка:

Тези мерки включват сигурност при криптография, предаване и излъчване, както и сигурност на процедурите, физическа сигурност, сигурност на персонала, документна и компютърна сигурност.

„Компютърна сигурност“ (COMPUSEC) означава прилагането към компютърна система на хардуерни, фърмуерни и софтуерни характеристики за сигурност с цел защита от или предотвратяване на неразрешено оповестяване, манипулиране, изменение/заличаване на информация или за предотвратяване на прекъсване в обслужването.

„Продукт за компютърна сигурност“ означава родово определен компютърен елемент за сигурност, който е предназначен за включване в информационно-технологична система за усъвършенстване или осигуряване на поверителност, цялост или наличие на обработваната информация.

„Специален режим на работа при условия на сигурност“ означава режим на работа, при който ВСИЧКИ физически лица, които имат достъп до системата, имат разрешение за достъп до най-високата степен на класифициране на обработваната в системата информация, и имат обща „необходимост да знаят“ ЦЯЛАТА обработвана в системата информация.

Забележки:

(1) Общата „необходимост да се знае“ показва, че няма задължително изискване за компютърни характеристики за сигурност, които да осигуряват разделяне на информацията в системата.

(2) Другите характеристики за сигурност (например физическа сигурност, сигурност на персонала и процедурите) отговарят на изискванията за най-високата степен на класифициране и за всички означения за категория на обработваната в системата информация.

„Оценка“ означава подробна техническа проверка от подходящ орган на аспектите за сигурност на система или на продукт за криптографска или компютърна сигурност.

Забележки:

(1) Оценката проучва присъствието на необходимата функционалност за сигурност и отсъствието на излагащи на риск странични ефекти на тази функционалност, и оценява невъзможността за повреждане на тази функционалност.

(2) Оценката определя степента, до която са изпълнени изискванията за сигурност на дадена система или характеристиките за сигурност на даден продукт за компютърна сигурност, и установява степента на надеждност на системата или на поверената функция на продуктите за криптографска или компютърна сигурност.

„Собственик на информацията“ (IO) означава органът (началник на отдел), който отговаря за създаването, обработката и използването на информацията, включително за вземането на решение кой има достъп до тази информация.

▼B

„Сигурност на информацията“ (INFOSEC) означава прилагането на мерки за сигурност за защита на информацията, която се обработва, съхранява или предава чрез комуникационни системи, на информационни и други електронни системи срещу случайна или умишлена загуба на поверителност, цялост или наличност, и за предотвратяване на загубата на целостта и наличието на самите системи.

„Мерките за сигурност на информацията“ включват компютърната сигурност, криптографската сигурност и сигурността на предаване и излъчване, и откриването, документирането и противодействието на заплахи за информацията и системите.

„Информационно-технологична зона“ означава зона, която съдържа един или повече компютри, техните локални периферни и запаметяващи устройства, блокове за управление и специално мрежово и комуникационно оборудване.

Забележка:

Определението не включва отделна зона, в която са разположени отдалечени периферни устройства или терминали/работни станции, дори и тези устройства да са свързани с оборудване в информационно-технологичната зона.

„Информационно-технологична мрежа“ означава географски разпръсната организация от взаимосвързани информационно-технологични системи за обмен на данни, която включва компонентите на взаимно свързаните информационно-технологични системи и техния интерфейс с поддържащите мрежи за данни или комуникационни мрежи.

Забележки:

(1) Дадена информационно-технологична мрежа може да ползва услугите на една или няколко взаимосвързани комуникационни мрежи за обмен на данни; няколко информационно-технологични мрежи могат да използват услугите на обща комуникационна мрежа.

(2) Дадена информационно-технологична мрежа се нарича „локална“, ако свързва няколко компютъра на едно и също място.

„Характеристиките за сигурност на информационно-технологична мрежа“ включват характеристиките за сигурност на отделните информационно-технологични системи, които съставляват мрежата, заедно с онези допълнителни компоненти и характеристики, които са свързани с мрежата като такава (например мрежови комуникации, механизми и процедури за идентификацията и етикетирането за сигурност, средства за управление на достъпа, програми и методи за проверка), които са необходими за осигуряването на приемлива степен на защита на класифицирана информация.

„Информационно-технологична система“ означава съвкупност от оборудване, методи и процедури, и когато е необходимо персонал, които са организирани да изпълняват функции по обработка на информация.

Забележки:

(1) Определението следва да се разбира, че означава съвкупност от съоръжения, които са конфигурирани да обработват информация в рамките на системата.

(2) Такива системи могат да подпомагат справочни, командни, контролни, комуникационни, научни или административни приложения, включително текстообработка.

(3) Границите на дадена система най-общо ще се определят от елементите, които са под контрола на един единствен собственик на технически системи.

(4) Дадена информационно-технологична система може да съдържа подсистеми, някои от които самите са информационно-технологични системи.

▼B

„Характеристиките за сигурност на информационно-технологична система“ включват всички хардуерни/фърмуерни/софтуерни функции и характеристики, операционните процедури, процедурите за отчитане и средствата за управление на достъпа, информационно-технологичната зона, зоната на отдалечен терминал/работна станция и ограниченията за управление, физическата структура и устройствата, персонала и комуникационните средства за управление, които са необходими за осигуряването на приемлива степен на защита на класифицираната информация, която ще се обработва в дадена информационно-технологична система.

„Завеждащ сигурността на информацията на местно ниво“ означава длъжностното лице в отдел на Комисията, което отговаря за координирането и контрола на мерките за сигурност в неговата сфера на компетентност.

„Многостепенен режим на работа при условия на сигурност“ означава режим на работа, при който НЕ ВСИЧКИ физически лица, които имат достъп до системата имат разрешение за достъп до обработваната в системата информация с най-висока степен на класифициране, и НЕ ВСИЧКИ физически лица, които имат достъп до системата имат обща „необходимост да знаят“ обработваната в системата информация.

Забележки:

(1) Понастоящем този режим на работа позволява обработката на информация с различна степен на класифициране и на информация със смесени обозначения за категория.

(2) Фактът, че не всички физически лица имат разрешение за достъп до най-високите степени на класифициране, което е свързано с липсата на обща „необходимост да се знае“, показва, че има изискване за характеристики за компютърна сигурност, които да осигуряват избирателен достъп до и разделяне на информацията в системата.

„Зона на отдалечен терминал/работна станция“ означава зона, в която се съдържа известно компютърно оборудване, неговите локални периферни устройства или терминали/работни станции и евентуално свързано комуникационно оборудване, отделно от дадена информационно-технологична зона.

Висококосистемен режим на работа при условия на сигурност означава режим на работа, при който ВСИЧКИ физически лица, които имат достъп до системата имат разрешение за достъп до обработваната в системата информация с най-висока степен на класифициране, но НЕ ВСИЧКИ физически лица, които имат достъп до системата имат обща „необходимост да знаят“ обработваната в системата информация.

Забележки:

(1) Липсата на обща „необходимост да се знае“ показва, че има изискване за характеристики за компютърна сигурност, които да осигуряват избирателен достъп до и разделяне на информацията в системата.

(2) Другите характеристики за сигурност (например, физическа сигурност, сигурност на персонала и процедурите) съответстват на изискванията за най-високата степен на класифициране и на всички категории обозначения на обработваната в системата информация.

(3) Цялата информация, която се обработва или е поставена на разположение в система, която функционира при този режим на работа, заедно с произтичащите от нея резултати, се защитават като потенциално попадащи в обозначението за категория на информацията и като обработвана информация с най-висока степен на класифициране до доказване на противното, освен ако е налице приемлива степен на доверие спрямо съществуващата функционалност на етикетирането.

▼B

„Декларация за специфичните изисквания за сигурност на системата“ (SSRS) означава пълна и ясна декларация във връзка с принципите за сигурност, които следва да се съблюдават, и подробно описание на изискванията за сигурност, които трябва да бъдат изпълнени. Тя се основава на политиката за сигурност на Комисията и оценката на риска или се налага от параметри, касаещи операционната среда, най-ниската степен на проверка за сигурност на персонала, най-високата степен на класифициране на обработваната информация, режима на работа при условия на сигурност или изискванията на потребителите. SSRS е неразделна част от проектодокументацията, която се представя на съответните органи за техническо и бюджетно одобрение, и одобрение от гледна точка на сигурността. В окончателния си вид SSRS представлява цялостна декларация за това какво значи системата да е сигурна.

„Собственик на технически системи“ (TSO) означава органът, който отговаря за създаването, поддръжката, експлоатацията и закриването на система.

Мерки за противодействие на „ефекта на бурята“ означава мерки за сигурност, които са предназначени да защитават оборудването и комуникационните инфраструктури срещу излагането на риск на класифицирана информация чрез неволни електромагнитни излъчвания и проводимост.

25.3. **Отговорност за сигурността**

25.3.1. *Общи положения*

Консултативните отговорности на Консултативната група по политиката за сигурност на Комисията, определена в раздел 12, включват въпроси, свързани със сигурността на информацията. Тази група организира дейността си така, че да може да дава експертни съвети по горепосочените въпроси.

►M2 Дирекция по сигурността на Комисията ◄ отговаря за издаването на подробни разпоредби за сигурност на информацията въз основа на разпоредбите, които се съдържат в настоящата глава.

►M2 Дирекция по сигурността на Комисията ◄ предприема незабавни действия в случай на проблеми, свързани със сигурността (инциденти, нарушения и т.н.).

В ►M2 дирекция по сигурността на Комисията ◄ има звено, което отговаря за сигурността на информацията.

25.3.2. *Акредитиращ орган по сигурността (SAA)*

►M2 Директор на дирекцията по сигурността на Комисията ◄ е акредитиращият орган по сигурността в Комисията. SAA отговаря за сигурността изобщо и за специфичните области като сигурност на информацията, сигурност на комуникациите, сигурност на криптографията и сигурност срещу „ефекта на бурята“.

SAA отговаря за гарантиране на съответствието на системите с политиката за сигурност на Комисията. Една от задачите му е да одобрява система за обработка в операционната ѝ среда на класифицирана информация на ЕС до определена степен на класифициране.

Юрисдикцията на SAA на Комисията обхваща всички системи, които функционират в помещенията на Комисията. Когато различни компоненти на дадена система попадат под юрисдикцията на SAA на Комисията и други акредитиращи органи по сигурността, всички заинтересовани страни могат да назначат смесен акредитационен съвет под ръководството на SAA на Комисията.

25.3.3. *Орган по сигурността на информацията (IA)*

Началникът на звеното за сигурност на информацията в ►M2 дирекция по сигурността на Комисията ◄ е органът по сигурността на информацията в Комисията. Органът по сигурността на информацията отговаря за:

— предоставяне на технически консултации и помощ на SAA,

— оказване на съдействие при разработването на SSRS,

▼B

— преразглеждане на SSRS с оглед гарантиране на съответствие на настоящите правила за сигурност с документите за политиката и устройството на сигурността на информацията,

— когато е необходимо, участие в акредитационните комисии/съвети и предоставяне на SAA на препоръки във връзка със сигурността на информацията,

— осигуряване на подкрепа при мероприятия, свързани с обучение по въпросите на сигурността на информацията,

— предоставяне на технически консултации при разследването на инциденти, свързани със сигурността на информацията,

— определяне на стратегически технически насоки, с които да се гарантира използването само на разрешен софтуер.

25.3.4. *Собственик на техническите системи (TSO)*

Отговорността за осъществяването на проверки и за функционирането на специфичните характеристики за сигурност на дадена система се носи от собственика на тази система, собственика на техническите системи (TSO). За централно притежавани системи се назначава завеждащ сигурността на информацията на централно равнище (CISO). По целесъобразност, всеки отдел назначава завеждащ сигурността на информацията на местно равнище (LISO). Отговорността на TSO включва създаването на процедури за сигурност при работа (SecOPS) и се носи през целия жизнен цикъл на дадена система, от етапа на създаване на системата до окончателното ѝ унищожаване.

TSO определя стандартите и практиките за сигурност, които трябва да се спазват от доставчика на системата.

По целесъобразност TSO може да делегира част от отговорностите си на завеждащ сигурността на информацията на местно равнище. Различните функции във връзка със сигурността на информацията могат да се изпълняват от едно лице.

23.3.5. *Собственик на информацията (IO)*

Собственикът на информацията (IO) отговаря за класифицираната информация на ЕС (и друга информация), която ще се въвежда, обработва и създава в техническите системи. Той определя изискванията за достъп до тази информация в системите. Той може да делегира тази отговорност на завеждащ информацията или на завеждащ бази данни в сектора, за който отговаря.

25.3.6. *Потребители*

Всички потребители са длъжни да гарантират, че действията им не се отразяват неблагоприятно на сигурността на системата, която използват.

25.3.7. *Обучение по сигурност на информацията*

За всички служители, които имат нужда от това, се осигурява обучение по сигурност на информацията.

25.4. **Нетехнически мерки за сигурност**

25.4.1. *Сигурност на персонала*

Потребителите на системата трябва да имат разрешение за достъп и „необходимост да знаят“ съобразно класификацията и съдържанието на информацията, която се обработва в тяхната конкретна система. Достъпът до определено оборудване или до информация, която е от специфично значение за сигурността, ще изисква специално разрешение за достъп, което се издава съгласно процедури на Комисията.

SAA определя всички деликатни длъжности и определя необходимата степен на разрешение за достъп и контрол за всички служители, които заемат тези длъжности.

Системите се специфицират и проектират по начин, който да улеснява разпределението на служебните задължения и отговорностите между персонала така, че да се предотвратява възможността едно лице да разполага с пълни сведения или контрол върху ключовите места за сигурността на системата.

▼B

В информационно-технологични зони и зони на отдалечени терминали/ работни станции, в които може да се променя сигурността на системата, не трябва да работи само едно упълномощено длъжностно лице или друг работник или служител.

Настройките за сигурност на дадена система се променят само от най-малко двама съвместно работещи упълномощени служители.

25.4.2. *Физическа сигурност*

Информационно-технологичните зони и зоните на отдалечени терминали/ работни станции (съгласно определението в раздел 25.2), в които с информационно-технологични средства се обработва информация с ►M1 RESTREINT UE ◄ или по-висока степен на класифициране, или в които е възможен потенциален достъп до тази информация, се изграждат като зони за сигурност на ЕС от клас I или клас II, в зависимост от случая.

25.4.3. *Контрол на достъпа до система*

Всички материали и информация, които позволяват контрол на достъпа до система, се защитават чрез мерки, съответстващи на най-високата степен на класифициране и на обозначението за категория на информацията, до която те могат да осигурят достъп.

Когато престанат да се използват за тази цел, информацията и материалите, които служат за контрол на достъпа се унищожават съобразно разпоредбите на раздел 25.5.4.

25.5. **Технически мерки за сигурност**

25.5.1. *Сигурност на информацията*

Авторът на информацията е длъжен да определя и класифицира всички документи, които са носители на информация, независимо дали те са във вид на хартиен или електронен носител. Класификацията се обозначава в горното и долното поле на всяка страница на хартиен носител. Създадените документи, независимо дали са във вид на хартиен или електронен носител, се обозначават с най-високата степен на класифициране на информацията, която е използвана за тяхното създаване. Начинът, по който функционира дадена система, също може да оказва въздействие върху класифицирането на създадените от тази система документи.

Отделите на Комисията и работещите в тях лица, които притежават информация, са длъжни да вземат предвид проблемите във връзка с натрупването на отделни информационни елементи и конфликтите, които могат да се породят от свързаните с тях елементи, и да определят дали е или не е целесъобразно да се определи по-висока степен на класифициране на съвкупността от информация.

Фактът, че информацията може да се формулира като съкратен код, код за предаване или каквато и да е форма на двойно представяне, не предоставя никаква защита за сигурността, поради което не трябва да оказва влияние върху класифицирането на информацията.

При прехвърляне на информация от една система в друга информацията се защитава по време на прехвърлянето и в получаващата система по начин, който съответства на първоначалната класификация и категория на информацията.

С всички електронни информационни носители се борави по начин, който съответства на най-високата степен на класифициране на съхраняваната информация или на етикета на носителя, и по всяко време се ползва с подходяща защита.

Повторно използваемите електронни информационни носители, които са използвани за записване на класифицирана информация на ЕС, запазват най-високата степен на класифициране, за която някога са били използвани до понижаване по съответния начин на степента на класифициране на съхраняваната в тях информация или до нейното декласифициране, и съответното прекласифициране, декласифициране или унищожаване на носителя съгласно одобрена от SAA процедура (виж раздел 25.5.4).

▼B

25.5.2. *Контрол и отчетност на информацията*

За проследяване на достъпа до информация със ►M1 RESTREINT UE ◄ или по-висока степен на класифициране се водят автоматични (архив за проверка) или ръчни дневници. Тази информация се съхранява в съответствие с настоящите правила за сигурност.

Класифицирани материали на ЕС, които се съхраняват в информационно-технологичната зона като един класифициран материал, не е необходимо да се регистрират, при условие че материалът е идентифициран, обозначен със собствена класификация и се контролира по подходящ начин.

Когато система, в която се обработва класифицирана информация на ЕС, създава данни, които се предават от информационно-технологична зона до зона на отдалечен терминал/работна станция, съгласувано с SAA се установяват процедури за контрол и регистриране на тези данни. За данни със ►M1 RESTREINT UE ◄ или по-висока степен на класифициране тези процедури включват специфични инструкции за отчетност на информацията.

25.5.3. *Работа с и контрол на отделящи се електронни информационни носители*

Всички отделящи се електронни информационни носители с ►M1 RESTREINT UE ◄ и по-висока степен на класифициране се третират като материали и за тях се прилагат общите правила. В зависимост от специфичния физически външен вид на носителите е необходимо да се приспособят подходящи идентификационни и класификационни маркировки, които да позволяват ясното им разпознаване.

Потребителите поемат отговорността да гарантират, че класифицираната информация на ЕС се съхранява на носители с подходяща класификационна маркировка и защита. Установяват се процедури, с които да се гарантира, че за всички степени на класифициране на ЕС съхранението на информацията на електронни носители се извършва в съответствие с настоящите правила за сигурност.

25.5.4. *Декласифициране и унищожаване на електронни информационни носители*

Електронните информационни носители, които са използвани за записване на класифицирана информация на ЕС, могат да претърпяват понижаване на степента на класифициране или да бъдат декласифицирани в съответствие с одобрена от SAA процедура.

Електронни носители, на които е била съхранявана ►M1 RESTREINT UE ◄ информация или специална категория информация, не се декласифицират и не се използват повторно.

Ако електронен информационен носител не може да бъде декласифициран или повторно използван, той се унищожава в съответствие с горепосочената процедура.

25.5.5. *Сигурност на комуникациите*

►M2 Директор на дирекцията по сигурността на Комисията ◄ е криптографският орган.

При предаване на класифицирана информация на ЕС по електромагнитен път се прилагат специални мерки за защита на поверителния характер, целостта и наличието на такива предавания. SAA определя изискванията за защита на предаванията срещу откриване и прихващане. Информацията, която се предава по комуникационна система, се защитава въз основа на изискванията за поверителност, цялост и наличност.

Когато са необходими криптографски методи за осигуряването на поверителност, цялост и наличност, тези методи и свързаните с тях продукти изрично се одобряват за целта от SAA и криптографския орган.

▼B

По време на предаване поверителният характер на информация, класифицирана като ►M1 RESTREINT UE ◄ информация или с по-висока степен на класифициране, се защитава чрез криптографски методи или продукти, одобрени от члена на Комисията, който отговаря за въпросите на сигурността, след консултации с Консултативната група по политиката за сигурност на Комисията. По време на предаване поверителният характер на информация, класифицирана като ►M1 RESTREINT UE ◄ информация или като информация ►M1 RESTREINT UE ◄, се защитава чрез криптографски методи или продукти, одобрени от криптографския орган на Комисията след консултации с Консултативната група по политиката за сигурност на Комисията.

В специфични инструкции за сигурност, които се одобряват от ►M2 дирекция по сигурността на Комисията ◄, след консултации с Консултативната група по политиката за сигурност на Комисията се определят подробни правила за предаването на класифицирана информация на ЕС.

При изключителни оперативни обстоятелства, информация, която е класифицирана като информация►M1 RESTREINT UE ◄, ►M1 RESTREINT UE ◄ информация и ►M1 RESTREINT UE ◄ информация, може да се предава под формата на ясен текст, като за всеки отделен случай се изисква изрично разрешение и всеки такъв случай се регистрира от собственика на информацията. Тези изключителни обстоятелства са следните:

а) по време на предстояща или действителна криза, конфликт или военно положение, и

б) когато бързината на предаване е от първостепенно значение и няма налице средства за кодиране, и е направена оценка, че предаваната информация не може да бъде своевременно използвана така, че да се окаже неблагоприятно влияние на операциите.

Дадена система трябва да бъде способна успешно да отказва достъп до класифицирана информация на ЕС на всеки или всички нейни отдалечени работни станции или терминали, когато това се налага от физическо прекъсване на връзката или от особени софтуерни характеристики, одобрени от SAA.

25.5.6.
Инсталационна и радиационна сигурност

Спецификациите за първоначалното инсталиране на системите и за всички големи промени по тях предвиждат инсталирането да се извършва от технически специалисти, които имат разрешение за достъп до секретни материали, под постоянния надзор на технически квалифициран персонал, който има разрешение за достъп до класифицирана информация на ЕС, чиято степен съответства на най-високата степен на класифициране на информацията, която системата се очаква да съхранява или обработва.

Системите, в които се обработва информация, класифицирана като ►M1 RESTREINT UE ◄ информация или с по-висока степен на класифициране, се защитават така, че сигурността им да не може да се застрашава от излагащи на риск излъчвания или проводимост, чието изследване и контрол се обозначава с термина „TEMPEST“.

Мерките за противодействие на „ефекта на бурята“ се проверяват и одобряват от органа „TEMPEST“ (виж раздел 25.3.2).

25.6. **Сигурност по време на работа**

25.6.1. *Процедури за сигурност при работа (SecOPS)*

Процедурите за сигурност при работа (SecOPS) определят принципите, които трябва да бъдат възприети относно въпросите на сигурността, оперативните процедури, които трябва да се следват и отговорностите на персонала. Процедурите за сигурност при работа се изготвят под контрола на собственика на техническите системи (TSO).

25.6.2. *Софтуерна защита/управление на конфигурации*

Защитата за сигурност на приложните програми се определя въз основа на оценка на класификацията за сигурност на самата система, а не на класификацията на информацията, която тази система ще обработва. Използваните софтуерни версии редовно се проверяват, за да се гарантира тяхната цялост и правилно функциониране.

▼B

Нови или изменени софтуерни версии не се използват за обработка на класифицирана информация на ЕС, докато не бъдат проверени от TSO.

25.6.3. *Проверка за наличие на опасни софтуерни/компютърни вируси*

Периодично се извършват проверки за наличие на зловредни софтуерни/компютърни вируси в съответствие с изискванията на SAA.

Всички електронни информационни носители, които се получават в Комисията, се проверяват за наличие на евентуални софтуерни или компютърни вируси, преди да бъдат въведени в която и да е система.

25.6.4. *Поддръжка*

В договорите и процедурите за планирана поддръжка и поддръжка при поддържане на системи, за които и изготвена SSRS, се посочват изискванията и разпоредбите относно персонала за поддръжка и съответното оборудване, което се внася в информационно-технологична зона.

Тези изисквания и процедури ясно се посочват съответно в SSRS и в процедурите за сигурност при работа (SecOPS). Поддръжка от страна на изпълнител, която изисква диагностични процедури с отдалечен достъп, се разрешава само при изключителни обстоятелства, при условия на строг контрол за сигурност и само с одобрението на SAA.

25.7. **Доставки**

25.7.1. *Общи положения*

Всеки продукт за сигурност, който трябва да се използва с подлежащата на доставка система, трябва или да е оценен и сертифициран, или да се намира в процес на оценка и сертифициране от подходящ орган за оценка или сертифициране на една от държавите-членки на ЕС по международно признати критерии (като Общите критерии за оценка на сигурността на информационните технологии, виж ISO 15408). За получаването на одобрение от ACPC са необходими специфични процедури.

При вземането на решение, дали дадено оборудване, особено електронни информационни носители, да се наеме, а не да се закупува, следва да се има предвид, че това оборудване, след като веднъж е използвано за обработка на класифицирана информация на ЕС, не може да се предоставя за ползване извън подходящо защитена среда, без преди това да е декласифицирано с одобрението на SAA, и че не винаги е възможно да се даде такова одобрение.

25.7.2. *Акредитация*

Всички системи, за които трябва да се изготви SSRS, преди в тях да се обработва класифицирана информация на ЕС, се акредитират от SAA въз основа на информацията, която е предоставена в SSRS, SecOPS и евентуално друга съответна документация. Подсистемите и отдалечените терминали/работни станции се акредитират като част от системите, към които са свързани. Когато дадена система обслужва едновременно Комисията и други организации, Комисията и съответните органи за сигурност взаимно се договарят относно акредитацията.

Процесът на акредитация може да се извършва в съответствие с подходяща за конкретната система стратегия за акредитация, която се определя от SAA.

25.7.3. *Оценка и сертифициране*

В определени случаи, преди да се акредитират, хардуерните, фърмуерните и софтуерните характеристики за сигурност на дадена система се оценяват и сертифицират, че могат да осигуряват защита на информацията до планираната степен на класифициране.

Изискванията за оценка и сертифициране се включват в планирането на системата и ясно се посочват в SSRS.

▼B

Процесите на оценка и сертифициране се извършват в съответствие с одобрени насоки от технически квалифициран персонал, който притежава подходящо разрешение за достъп до секретни материали и действа от името на TSO.

Екипите могат да се осигуряват от определен от държава-членка орган за оценка или сертифициране или от определени от него представители, например компетентен изпълнител с разрешение за достъп до секретни материали.

Степента на процесите на оценка и сертифициране може да бъде занижена (например, да включва само аспекти на интегриране), когато системите се основават на съществуващи продукти за компютърна сигурност, които са оценени и сертифицирани на национално равнище.

25.7.4. *Рутинни проверки на характеристиките за сигурност за продължаване на акредитацията*

TSO установява процедури за рутинен контрол, които да гарантират, че всички характеристики за сигурност на системата продължават да бъдат валидни.

В SSRS ясно се определят и посочват видовете промени, които биха могли да доведат до повторно акредитиране, или които изискват предварително одобрение от SAA. След всяка промяна, ремонт или неизправност, която би могла да даде отражение върху характеристиките за сигурност на системата, TSO гарантира извършването на проверка, която да гарантира правилното функциониране на характеристиките за сигурност. Продължаването на акредитацията на системата обикновено зависи от удовлетворителния резултат от проверките.

SAA редовно проверява и преразглежда всички системи, при които се прилагат характеристики за сигурност. По отношение на системите, в които се обработва ►M1 RESTREINT UE ◄ информация, проверките се извършват най-малко веднъж годишно.

25.8. **Временно или случайно използване**

25.8.1. *Сигурност на микрокомпютри/персонални компютри*

Микрокомпютрите/персоналните компютри с постоянни дискове (или други постоянни информационни носители), които функционират в самостоятелен режим или като мрежови конфигурации, както и преносимите електронно-изчислителни устройства (например, преносими персонални компютри и електронни „бележници“) с постоянни твърди дискове, се считат за информационни носители в същия смисъл, както флопи дисковете или други отделящи се електронни информационни носители.

Това оборудване се ползва със степента на защита, от гледна точка на достъп, обработка, съхранение и транспортиране, която съответства на най-високо класифицираната информация, която някога е съхранявана или обработвана (докато понижаване на степента на класифициране или декласифициране в съответствие с одобрени процедури).

25.8.2. *Използване на лично информационно-технологично оборудване за официална работа на Комисията*

Забранява се използването на лични преносими електронни информационни носители, софтуер и информационно-технологичен хардуер (например персонални компютри и преносими електронно-изчислителни устройства) за обработка на класифицирана информация на ЕС.

В нито една зона от клас I или клас II, където се обработва класифицирана информация на ЕС, не се внася личен хардуер, софтуер и носители без писмено разрешение на ►M2 директор на дирекцията по сигурността на Комисията ◄. Това разрешение може да се дава в извънредни случаи по технически съображения.

▼B

25.8.3. *Използване на информационно-технологично оборудване, което е собственост на изпълнител, или което се доставя от държавите-членки за официална работа на Комисията*

►M2 Директор на дирекцията по сигурността на Комисията ◄ може да разрешава използването на информационно-технологично оборудване и софтуер, които са собственост на изпълнител в организации, които подпомагат официалната работа на Комисията. Може да се разрешава и използването на информационно-технологично оборудване и софтуер, които се доставят от държавите-членки; в такъв случай въпросното информационно-технологично оборудване се вписва и поставя под контрола на съответния инвентарен списък на Комисията. И в двата случая, ако информационно-технологичното оборудване ще се използва за обработка на класифицирана информация на ЕС, се извършва консултация с SAA с оглед на извършването на правилна преценка и прилагане на елементите за сигурност на информацията, които са приложими за използването на това оборудване.

26. ПРЕДОСТАВЯНЕ НА ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ТРЕТИ ДЪРЖАВИ ИЛИ МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

26.1.1. *Принципи, които регулират предоставянето на достъп до класифицирана информация*

Решението за предоставяне на достъп до класифицирана информация на ЕС на трети държави или международни организации се взема от Комисията като колегиален орган въз основа на:

— естеството и съдържанието на тази информация,

— необходимостта на получателите да знаят тази информация,

— мащаба на предимствата за ЕС.

Иска се съгласието на автора на класифицираната информация на ЕС, до която ще се предостави достъп.

Тези решения се вземат за всеки случай поотделно, в зависимост от:

— желаната степен на сътрудничество със съответните трети държави или международни организации,

— доверието, което може да им се окаже, което е функция от степента на сигурност, която би била прилагана спрямо поверената на тези държави или организации класифицирана информация на ЕС и от съответствието между приложимите в тези държави или организации правила за сигурност и правилата, които се прилагат в ЕС. Консултативната група по политиката за сигурност на Комисията дава техническото си становище по този въпрос.

Приемането на класифицирана информация на ЕС от трети държави или международни организации ще предполага даването на уверение, че информацията няма да се използва за никакви други цели, освен тези, които са мотивирали предоставянето или обмяната на информация, и че те осигуряват изискваната от Комисията защита.

26.1.2. *Степени*

След като Комисията вземе решение, че класифицирана информация може да се предостави или обмени с дадена държава или международна организация, тя взема решение за възможната степен на сътрудничество. Поспециално това зависи от прилаганите от тази държава или организация политика и нормативни разпоредби за сигурност.

Има три степени на сътрудничество:

Степен 1

Сътрудничество с трети държави или международни организации, чиито политика за сигурност и нормативни разпоредби са много сходни с тези на ЕС.

Степен 2

Сътрудничество с трети държави или международни организации, чиито политика за сигурност и разпоредби силно се отличават от тези на ЕС.

▼B

Степен 3

Нередовно сътрудничество с трети държави или международни организации, чиито политика и разпоредби за сигурност не могат да бъдат оценени.

Всяка степен на сътрудничество обуславя процедурите и разпоредбите за сигурност, които са подробно описани в допълнения 3, 4 и 5.

26.1.3. *Споразумения за сигурност*

След като Комисията вземе решение, че е налице постоянна или дългосрочна необходимост от обмен на класифицирана информация между Комисията и трети държави или международни организации, тя изготвя „споразумения за процедурите за сигурност при обмяна на класифицирана информация“ с тях, в които се определя целта на сътрудничеството и взаимните правила за защита на обменяната информация.

В случай на нередовно сътрудничество от степен 3, което по дефиниция е ограничено откъм време и цел, вместо „споразумението за процедурите за сигурност при обмяна на класифицирана информация“ може да се подпише обикновен меморандум за разбирателство, в който да се определи естеството на класифицираната информация, която ще се обменя и взаимните задължения във връзка с тази информация при условие, че се касае за информация със степен на класифициране, която не е по-висока от информация ►M1 RESTREINT UE ◄.

Преди да бъдат представени на Комисията за вземане на решение, проектоспоразуменията за процедурите за сигурност или меморандумите за разбирателство се обсъждат от Консултативната група по политиката за сигурност на Комисията.

Членът на Комисията, който отговаря за въпросите на сигурността, изисква цялото необходимо съдействие от националните органи за сигурност на държавите-членки, за да се гарантира, че информацията, която ще се предостави, се използва и защитава в съответствие с разпоредбите на споразуменията за процедурите за сигурност или на меморандумите за разбирателство.

▼M3

27. ОБЩИ МИНИМАЛНИ НОРМИ В ОБЛАСТТА НА ПРОМИШЛЕНАТА СИГУРНОСТ

27.1. **Въведение**

Настоящият раздел се отнася до аспектите на сигурността на промишлените дейности, които са предмет на преговори и сключване на договори или грантови споразумения, които договори или грантови споразумения се изпълняват от промишлени или други обекти, и в рамките на които са възложени задачи, които включват, изискват и/или съдържат класифицирана информация на ЕС, включително предоставянето на такава информация или достъпа до нея по време на процедурите по обществена поръчка или покана за участие в търг или конкурс (период на наддаване и преговори за предварителен договор).

27.2. **Определения**

За целите на тези общи минимални стандарти:

а) „класифициран договор“ е всеки договор или грантово споразумение с цел доставка на продукти, извършване на строително-ремонтни дейности, оборудване на сгради или предоставяне на услуги, чието осъществяване предполага достъп до класифицирана информация на ЕС или създаването на такава информация;

б) „класифициран договор за подизпълнение“ е договор, сключен от изпълнител или бенефициер на грант с друг изпълнител (т.е. подизпълнител) с цел доставка на блага, извършване на строително-ремонтни дейности, оборудване на сгради или предоставяне на услуги, чието осъществяване предполага достъп до класифицирана информация на ЕС или създаването на такава информация;

в) „изпълнител“ е икономически оператор или юридическо лице, което има правоспособност да сключва договори или да бъде бенефициер на грант;

▼**M3**

г) „обозначен орган за сигурност (DSA)“ е органът, отговорен пред националния орган за сигурност (NSA) на дадена държава-членка, отговорен да информира промишлените или други обекти за националната политика по всички въпроси на промишлената сигурност и да предоставя помощ и насоки за нейното изпълнение. Функциите на DSA могат да се осъществяват от NSA;

д) „разрешително за сигурност на оборудване (FSC)“ е административно решение на DSA или NSA, според което, от гледна точка на сигурността, дадено оборудване може да гарантира в достатъчна степен защитата на класифицирана информация на ЕС на определено ниво на сигурност и според което персоналът на оборудването, който получава достъп до тази класифицирана информация на ЕС, притежава необходимото разрешително за сигурност и е бил запознат с изискванията за сигурност за достъп и защита на класифицирана информация на ЕС;

е) „промишлена или друга единица“ е изпълнител или подизпълнител, който участва в доставката на блага, извършване на строително-ремонтни дейности, оборудване на сгради или предоставяне на услуги, който може да бъде промишлена, търговска, обслужваща, научна, изследователска, образователна, или развойна единица;

ж) „промишлена сигурност“ е прилагането на защитни мерки и процедури с цел да се предотврати или открие и спре загуба или компрометиране на класифицирана информация на ЕС от страна на изпълнител или подизпълнител в преговори за предварителен договор или класифицирани договори;

з) „национален орган за сигурност (NSA)“ е правителствен орган на държава-членка на ЕС, който носи крайната отговорност за защитата на класифицираната информация на ЕС в тази държава-членка;

и) „общо ниво на класификация за сигурност на договор“ е определянето на класификация за сигурност на целия договор или грантово споразумение, въз основа на класификацията на информация и/или материали, които трябва или може да бъдат създадени или оповестени или до които трябва или може да има достъп по силата на някой от елементите на целия договор или грантово споразумение. Общото ниво на класификация за сигурност на даден договор не може да бъде по-ниско от най-високото ниво на класификация на един от неговите елементи, но може да бъде по-високо, в резултат на натрупването;

й) „приложение за сигурност (SAL)“ е набор от специални договорни условия, издадени от договарящия орган, който представлява неразделна част от класифицирания договор, включващ достъп до класифицирана информация на ЕС или създаването на такава информация, в който са определени изискванията за сигурност или елементите на класифицирания договор, които трябва да бъдат защитени.

к) „ръководство за класификация за сигурност (SCG)“ е документ, в който са описани класифицираните елементи на дадена програма, договор или грантово споразумение и уточнени нивата на класификация за сигурност. SCG може да бъде допълван в периода на изпълнение на програмата, договора или грантовото споразумение и елементите могат да бъдат добавяни или изваждани. SCG трябва да бъде част от SAL.

27.3 **Организация**

а) Комисията може чрез класифициран договор да повери на промишлени или други субекти, регистрирани в дадена държава-членка, задачи, които включват, изискват и/или съдържат класифицирана информация на ЕС.

б) Комисията гарантира, че всички изисквания, произтичащи от настоящите минимални стандарти, са спазени при сключването на класифицирани договори.

в) Комисията ангажира компетентните NSA с прилагането на настоящите минимални стандарти в областта на промишлената сигурност. NSA могат да прехвърлят тези задачи на един или повече DSA.

▼M3

г) Отговорността за защита на класифицираната информация на ЕС в промишлените или други обекти е в крайна сметка на тяхното ръководство.

д) Всеки път, когато се сключва класифициран договор или договор за подизпълнение, попадащ в полето на приложение на настоящите минимални стандарти, Комисията и/или NSA/DSA според случая нотифицира бързо за това NSA/DSA на държавата-членка, в която е регистриран изпълнителят или подизпълнителят.

27.4. **Класифицирани договори и решения за грант**

а) Класификацията за сигурност на класифицираните договори или грантовите споразумения трябва да се съобразяват със следните принципи:

— Комисията определя, ако е необходимо, аспектите от класифицирания договор, които трябва да бъдат защитени, и подходящата класификация за сигурност; тя се съобразява с първоначалната класификация за сигурност, определена от органа — източник на информацията, създадена преди сключването на класифицирания договор,

— общото ниво на класификация на договора не може да бъде по-ниско от най-високо ниво на класификация на някой от неговите елементи,

— класифицираната информация на ЕС, създадена в рамките на дейностите по договора, се класифицира съгласно ръководството за класификация за сигурност,

— ако е необходимо, Комисията може да промени общото ниво на класификация на договора или класификацията за сигурност на някой от неговите елементи, след консултация с органа източник, и да информира всички заинтересовани страни,

— класифицираната информация, предоставена на изпълнителя или на подизпълнителя в рамките на дейност по договора, не може да бъде използвана за други цели освен предвидените в класифицирания договор и не може да бъде разпространявана на трети лица без предварителното писмено съгласие на органа източник.

б) Комисията и NSA/DSA на съответните държави-членки гарантират, че доставчиците и подизпълнителите, с които са сключени класифицирани договори, включващи информация, класифицирана CONFIDENTIEL UE или по-високо ниво, ще вземат всички необходими мерки за защита на информация от този вид, която им е била предоставена или е била създадена при изпълнението на класифицирания договор, съгласно националните законодателни актове и правилници. Неспазването на изискванията за сигурност може да доведе до анулиране на класифицирания договор.

в) всички промишлени или други обекти, участващи в класифицирани договори, предполагащи достъп до информация, класифицирана CONFIDENTIEL UE или по-високо ниво, трябва да имат национално FSC. Това разрешително се издава от NSA/DSA на държавата-членка, за да удостовери, че даден обект може да осигури и гарантира защита на класифицираната информация на ЕС, адекватна на нивото на класификация.

г) Когато се сключи класифициран договор, отговорникът за сигурността на обекта (FSO), посочен от управителното тяло на изпълнителя или на подизпълнителя, има за задача да поиска разрешително за сигурност на персонала (PSC) за всички лица, заети в промишлените или други обекти, регистрирани в държавата-членка, чиито функции предполагат достъп до информация, класифицирана CONFIDENTIEL UE или по-високо ниво, необходима за изпълнението на класифицирания договор; това разрешително се издава от NSA/DSA на държавата-членка съгласно нейното национално законодателство.

▼M3

д) Класифицираните договори трябва да включват SAL, както е определено в точка 27.2, буква й). SAL трябва да включва SCG.

е) Преди да започне процедура за преговори за класифициран договор, Комисията се свързва с NSA/DSA на държавата-членка, в която са регистрирани промишлените или други обекти, за да получи потвърждение, че те имат валидно FSC, съответстващо на нивото на класификацията за сигурност на договора.

ж) Преговарящият орган не може да сключи класифициран договор с избрания икономически оператор, преди да получи удостоверението за FSC в срок на валидност.

з) Не е необходимо FSC за договорите, включващи информация, класифицирана RESTREINT UE, освен ако не го изисква националното законодателство на държавите-членки.

и) Поканите за участие в тръжна процедура или конкурс за класифицирани договори трябва да съдържат разпоредби, задължаващи икономическите оператори, които не подадат оферта или не бъдат избрани, да върнат всички документи в указания срок.

й) Възможно е доставчиците да трябва да договарят договори за подизпълнение с подизпълнители на различни нива. Доставчикът трябва да гарантира, че всички подизпълнителски дейности се осъществяват съгласно общите минимални стандарти за сигурност, посочени в настоящия раздел. Той не може да предостави класифицирана информация или материали на ЕС на подизпълнител без предварителното писмено съгласие на органа източник.

к) Условията, при които изпълнителят може да наеме подизпълнител за дадена дейност, трябва да бъдат определени в поканата за участие в търга или конкурса, както и в класифицирания договор. Договор за подизпълнение не може да бъде сключен с обекти, регистрирани в страни, които не са членки на ЕС, без изричното писмено съгласие на Комисията.

л) През целия период на изпълнение на класифицирания договор спазването на всички предвидени разпоредби за сигурност ще бъде проверявано съвместно от Комисията и компетентния DSA/NSA. За всеки инцидент, свързан със сигурността, се съставя доклад, съгласно разпоредбите на част II, раздел 24 от настоящите правила в областта на сигурността. Ако FSC бъде изменено или отнето, това трябва незабавно да бъде съобщено на Комисията и на всеки друг NSA/DSA, на който е било нотифицирано.

м) Когато се сключи класифициран договор или договор за подизпълнение, Комисията и/или NSA/DSA, според случая, информира бързо за това NSA/DSA на държавата-членка, в която е регистриран изпълнителят или подизпълнителят.

н) Общите минимални стандарти за сигурност, фигуриращи в настоящия раздел, остават в сила, доставчиците и подизпълнителите запазват конфиденциалния характер на класифицираната информация и след осъществяването или изтичането на класифицирания договор или договор за подизпълнение.

о) Специфични разпоредби за унищожаване на класифицираната информация след изтичане на класифицирания договор са включени в SAL или в други действащи разпоредби за сигурност.

п) Задълженията и условията, посочени в настоящия раздел, се прилагат *mutatis mutandis* по отношение на процедурите за предоставяне на грантове чрез решение, по-специално спрямо бенефициерите на тези грантове. Решението за отпускане на грант включва всички задължения на бенефициерите.

▼M3

27.5. **Посещения**

Когато служители на Комисията посещават в рамките на класифицирани договори промишлени или други обекти на държавите-членки, извършващи класифицирани договори на ЕС, тези посещения се организират съвместно с компетентния NSA/DSA. Посещенията на работещите в промишлени или други обекти в рамките на класифициран договор на ЕС следва да бъдат организирани от заинтересованите NSA/DSA. Все пак NSA/DSA, свързани с класифициран договор на ЕС, могат да договорят процедура за преки посещения на работещите в промишлени или други обекти.

27.6. **Предаване и транспортиране на класифицирана информация на ЕС**

а) По отношение на предаването на класифицирана информация на ЕС се прилагат разпоредбите на част II, раздел 21 от настоящите правила в областта на сигурността. За да се допълнят тези разпоредби, ще се прилагат всички съществуващи процедури между държавите-членки.

б) Международният транспорт на класифицирани материали на ЕС, свързани с класифицираните договори, се извършва съгласно националните процедури на държавите-членки. При прегледа на спогодбите в областта на сигурността на международния транспорт ще се прилагат следните принципи:

— сигурността е гарантирана на всеки етап от транспорта и при всички обстоятелства, от изходния пункт до крайния получател,

— степента на защита на дадена пратка се определя в съответствие с най-високото ниво на класификация на материалите, които съдържа,

— ако е необходимо, се издава FSC за дружествата, осъществяващи транспорта. В този случай персоналът, който обслужва пратката, трябва да получи разрешително за сигурност съгласно общите минимални стандарти, посочени в настоящия раздел,

— доколкото е възможно, маршрутите са преки и възможно най-бързи според обстоятелствата,

— за предпочитане е маршрутите да преминават само през територията на държавите-членки на ЕС винаги когато това е възможно. Маршрути през територии на държави, които не са членки на ЕС, се осъществяват само с разрешението на NSA/DSA на държавата експедитор и на държавата получател.

— преди всеки пренос на класифицирани материали на ЕС изпращачът изготвя план за транспортиране, който се одобрява от заинтересования NSA/DSA.

▼M1

Допълнение 1

СРАВНЕНИЕ НА НАЦИОНАЛНИТЕ НИВА НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ

Класификация на ЕС	TRÈS SECRET UEEU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Класификация на WEU	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Класификация на Евратом	Eura – TOP SECRET	Eura – SECRET	Eura - CONFIDENTIAL	Eura – RESTRICTED
Класификация на НАТО	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Белгия	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Чешка република	Přísn tajné	Tajné	Důvěrné	Vyhrazené
Дания	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Германия	Streng geheim	Geheim	VS (1) - Vertraulich	VS — Nur für den Dienstgebrauch
Естония	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Гърция	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Испания	Secreto	Reservado	Confidencial	Difusión Limitada
Франция	Très Secret Défense (2)	Secret Défense	Confidentiel Défense	

▼M4

Хърватия	Vrlo tajno	Tajno	Povjerljivo	Ograničeno

▼M1

Ирландия	Top secret	Secret	Confidential	Restricted
Италия	Segretissimo	Segreto	Riservatissimo	Riservato
Кипър	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Латвия	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Литва	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo

▼**M1**

Люксембург	Très Secret	Secret	Confidentiel	Diffusion restreinte
Унгария	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Малта	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Нидерландия	Stg. ([3]) Zeer geheim	Stg. Geheim	Stg. Confidentieel	Departementaal-ver-trouwelijk
Австрия	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Полша	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Португалия	Muito Secreto	Secreto	Confidencial	Reservado
Словения	Strogo tajno	Tajno	Zaupno	SVN Interno
Словакия	Prísne tajné	Tajné	Dôverné	Vyhradené
Финландия	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Швеция	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Обединеното кралство	Top Secret	Secret	Confidential	Restricted

([1]) VS = Verschlussache.
([2]) Класификацията Très secret défense, което покрива въпросите от приоритета на правителството, може да бъде сменена само с разрешението на министър-председателя.
([3]) Stg = staatsgeheim.

▼B

Допълнение 2

ПРАКТИЧЕСКО РЪКОВОДСТВО ЗА КЛАСИФИЦИРАНЕ

Настоящото ръководство е примерно и не може да се тълкува, че изменя съществените разпоредби, предвидени в раздели 16, 17, 20 и 21.

Класификация	Кога	Кой	Поставяне	Понижаване на степента на класифициране/декласифициране/унищожаване	
				Кой	Кога
►M1 RESTREINT UE ◄ материал: Тази степен на класифициране се прилага само за информация и материали, чието неразрешено оповестяване би могло да причини изключително тежки вреди на съществените интереси на Европейския съюз или на една или повече от неговите държави-членки [16.1].	Излагането на риск на материали, класифицирани като ►M1 RESTREINT UE ◄ материали, има вероятност: — да представлява пряка заплаха за вътрешната стабилност на ЕС или на някоя от неговите държави-членки, или на приятелски настроени държави — да причини изключително тежки вреди на взаимоотношенията с приятелски настроени правителства — пряко да доведе до масови човешки жертви — да причини изключително тежки вреди на оперативната ефективност или сигурност на държавите-членки или на други сътруднически сили, или на продължаващата ефективност на изключително ценна сигурност или на разузнавателни операции — да причини тежки и дълготрайни вреди на икономиката на ЕС или на държавите-членки.	Надлежно оторизираните лица (авторите), генерални директори, началници на служби [17.1] Авторите посочват дата, период или събитие, когато може да се понижи степента на класифициране или да се декласифицира съдържанието [16.2] В противен случай те преразглеждат документите най-малко веднъж на пет години, за да се гарантира необходимостта от първоначалната класификация [17.3].	Класификацията ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ се поставя върху ►M1 RESTREINT UE ◄ ДОКУМЕНТИ НА ЕС и когато е уместно — обозначение за сигурност и/или защитната маркировка ESDP с механични средства и на ръка [16.4, 16.5, 16.3]. Класификациите на ЕС и означенията за сигурност се поставят в средата на горното и долното поле на всяка страница, като всяка страница се номерира. Всеки документ се обозначава с референтен номер и дата; този референтен номер фигурира на всяка страница. Ако документите трябва да се разпространят в няколко екземпляра, на първата страница на всеки от тях се обозначава номерът на екземпляра и общият брой страници. На първата страница се изброяват всички приложения [21.1].	Декласифицирането или понижаването на степента на класифициране се извършва само от автора, който информира за промяната всички последващи адресати, на които е изпратил или копирал документа [17.3]. ►M1 RESTREINT UE ◄ документи се унищожават от централната служба за регистрация или от подразделението на службата за регистрация, което отговаря за тях. Всеки унищожен документ се изброява в сертификат за унищожаване, който се подписва от контрольора на службата за регистрация на ►M1 RESTREINT UE ◄ информация и от длъжностното лице, което присъства на унищожаването и което трябва да има разрешение за достъп до ►M1 RESTREINT UE ◄ информация. Унищожаването се отбелязва в дневника. Службата за регистрация съхранява сертификатите за унищожаване, заедно с формулярите за разпространение, в продължение на десет години [22.5].	Излишните екземпляри и документите, които вече не са необходими, трябва да се унищожават [22.5]. ►M1 RESTREINT UE ◄ документи, включително всички класифицирани отпадъци от изготвянето на ►M1 RESTREINT UE ◄ документи като повредени екземпляри, работни проекти, печатни записки, флопи дискове, се унищожават под надзора на контрольор на служба за регистрация на ►M1 RESTREINT UE ◄ информация чрез изгаряне, претопяване, нарязване на тънки ивици или чрез намаляване по друг начин до неузнаваема и неподлежаща на възстановяване форма [22.5].

▼B

Класификация	Кога	Кой	Поставяне	Понижаване на степента на класифициране/декласифициране/унищожаване	
				Кой	Кога
►M1 RESTREINT UE ◄ материал: Тази степен на класифициране се прилага само за информация и материали, чието неразрешено оповестяване би могло сериозно да навреди на съществените интереси на Европейския съюз или на една или повече от неговите държави-членки [16.1].	Излагането на риск на материали, класифицирани като ►M1 RESTREINT UE ◄ материали, има вероятност: — да предизвика международно напрежение — сериозно да увреди взаимоотношенията с приятелски настроени правителства — да представлява пряка заплаха за живота или сериозно да накърни обществения ред или сигурността или свободата на личността — да причини тежки вреди на оперативната ефективност или сигурност на държавите-членки или на други сътруднически сили, или на продължаващата ефективност на много ценна сигурност или на разузнавателни операции — да причини съществени материални вреди на финансовите, валутните, икономическите и търговските интереси на ЕС или на неговите държави-членки.	Упълномощените лица (авторите), генерални директори, началници на служби [17.1]. Авторите посочват дата или период, когато може да се понижи степента на класифициране или да се декласифицира съдържанието (16.2). В противен случай те преразглеждат документите най-малко веднъж на пет години, за да се гарантира необходимостта от първоначалната класификация [17.3].	Класификацията ►M1 RESTREINT UE ◄ информация се поставя върху ►M1 RESTREINT UE ◄ документи и когато е уместно — обозначение за сигурност и/или защитната маркировка ESDP с механични средства и на ръка [16.4, 16.5, 16.3]. Класификациите на ЕС и обозначенията за сигурност се поставят в средата на горното и долното поле на всяка страница, като всяка страница се номерира. Всеки документ се обозначава с референтен номер и дата; този референтен номер фигурира на всяка страница. Ако документите трябва да се разпространят в няколко екземпляра, на първата страница на всеки от тях се обозначава номерът на екземпляра и общият брой страници. На първата страница се изброяват всички приложения [21.1].	Декласифицирането или понижаването на степента на класифициране се извършва само от автора, който информира за промяната всички последващи адресати, на които е изпратил или копирал документа [17.3]. ►M1 RESTREINT UE ◄ документи се унищожават от службата за регистрация, която отговаря за тях. Унищожените ►M1 RESTREINT UE ◄ документи се изброяват в подписани сертификати за унищожаване, които се съхраняват от службата за регистрация, заедно с формулярите за разпространение, в продължение на най-малко три години [22.5].	Излишните екземпляри и документите, които вече не са необходими, трябва да се унищожават [22.5]. ►M1 RESTREINT UE ◄ документи, включително всички класифицирани отпадъци от изготвянето на ►M1 RESTREINT UE ◄ документи, като повредени екземпляри, работни проекти, печатни записки, флопи дискове, се унищожават чрез изгаряне, претопяване, нарязване на тънки ивици или чрез намаляване по друг начин до неузнаваема и неподлежаща на възстановяване форма [22.5].
►M1 RESTREINT UE ◄ МАТЕРИАЛ:	Излагането на риск на материали, класифицирани като ►M1 RESTREINT UE ◄ МАТЕРИАЛИ има вероятност: — съществено да навреди на дипломатически взаимоотношения, тоест да предизвика официален протест или други санкции;	Оторизираните лица (авторите), генерални директори, началници на служби [17.1].	Класификацията ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ се поставя върху ►M1 RESTREINT UE ◄ ДОКУМЕНТИ и когато е необходимо — обозначение за сигурност и/или защитната маркировка ESDP с механични средства и на ръка или чрез отпечатване върху хартиени бланки с предварително отпечатан щемпел [16.4, 16.5, 16.3].	Декласифицирането или понижаването на степента на класифициране се извършва само от автора, който информира за промяната всички последващи адресати, на които е изпратил или копирал документа [17.3].	Излишните екземпляри и документите, които вече не са необходими, трябва да се унищожават [22.5].

▼B

Класификация	Кога	Кой	Поставяне	Понижаване на степента на класифициране/декласифициране/унищожаване	
				Кой	Кога
Тази степен на класифициране се прилага за информация и материали, чието неразрешено оповестяване би могло да навреди на съществените интереси на Европейския съюз или на една или повече от неговите държави-членки. [16.1].	— да накърни сигурността или свободата на личността; — да причини вреди на оперативната ефективност или сигурност на държавите-членки или на други сътруднически сили, или на ефективността на ценна сигурност или на разузнавателни операции; — съществено да подкопае финансовата жизнеспособност на големи организации; — да възпрепятства разследването или да улесни извършването на тежки престъпления; — да изиграе съществена роля против финансовите, валутните, икономическите и търговските интереси на ЕС или на неговите държави-членки; — сериозно да възпрепятства развитието или функционирането на важни политики на ЕС; — да доведе до преустановяване или до друг вид съществено прекъсване на важни дейности на ЕС.	Авторите посочват дата или период, когато може да се понижи степента на класифициране или да се декласифицира съдържанието. В противен случай те преразглеждат документите най-малко веднъж на пет години, за да се гарантира необходимостта от първоначалната класификация [17.3].	Класификациите на ЕС и обозначенията за сигурност се поставят в средата на горното и долното поле на всяка страница, като всяка страница се номерира. Всеки документ се обозначава с референтен номер и дата. На първата страница се изброяват всички приложения [21.1].	►**M1** RESTREINT UE ◄ ДОКУМЕНТИ се унищожават от службата за регистрация, която отговаря за тях, под надзора на лице, което има разрешение за достъп до такива материали. Тяхното унищожаване се регистрира в съответствие с националните нормативни разпоредби, а в случай на децентрализирани агенции на Комисията или ЕС — съгласно указанията на ►**M2** члена на Комисията, отговарящ за въпросите по сигурността ◄ [22.5].	►**M1** RESTREINT UE ◄ документи, включително всички класифицирани отпадъци от изготвянето на ►**M1** RESTREINT UE ◄ документи, като повредени екземпляри, работни проекти, печатни записки, флопи дискове, се унищожават чрез изгаряне, претопяване, нарязване на тънки ивици или чрез намаляване по друг начин до неузнаваема и неподлежаща на възстановяване форма [22.5].

▼B

Класификация	Кога	Кой	Поставяне	Понижаване на степента на класифициране/декласифициране/унищожаване	
				Кой	Кога
Материал ►M1 RESTREINT UE◄: Тази степен на класифициране се прилага за информация и материали, чието неразрешено оповестяване би могло да причини неблагоприятни последици за интересите на Европейския съюз или на една или повече от неговите държави-членки. [16.1].	Излагането на риск на материали, класифицирани като материали ►M1 RESTREINT UE◄ има вероятност: — да окаже неблагоприятно въздействие върху дипломатически отношения — да предизвика значително човешко бедствие — да затрудни поддържането на оперативната ефективност или сигурност на държавите-членки или на други сътруднически сили — да причини финансови загуби или да улесни неправомерната печалба или предимство за физически лица или фирми — да наруши съответни ангажименти за запазване на поверителния характер на информация, която се предоставя от трети страни — да наруши нормативно установени ограничения за оповестяване на информация — да възпрепятства разследването или да улесни извършването на престъпления — да постави ЕС или държавите-членки в неизгодно положение по време на търговски или политически преговори с други страни — да възпрепятства ефективното развитие или функциониране на политики на ЕС — да подкопае правилното ръководство на ЕС и неговите операции.	Оторизираните лица (авторите), генерални директори, началници на служби [17.1] Авторите посочват дата, период или събитие, когато може да се понижи степента на класифициране или да се декласифицира съдържанието [16.2]. В противен случай те преразглеждат документите най-малко веднъж на пет години, за да се гарантира необходимостта от първоначалната класификация [17.3].	Класификацията информация ►M1 RESTREINT UE◄ се поставя върху документи ►M1 RESTREINT UE◄, и когато е уместно, обозначение за сигурност и/или защитната маркировка ESDP с механични или електронни средства [16.4, 16.5, 16.3]. Класификацията на ЕС и обозначенията за сигурност се поставят в горното поле на първата страница, като всяка страница се номерира. Всеки документ се обозначава с референтен номер и дата [21.1].	Декласифицирането се извършва само от автора, който информира за промяната всички последващи адресати, на които е изпратил или копирал документа [17.3]. Документи ►M1 RESTREINT UE◄ се унищожават от службата за регистрация, която отговаря за документа или от потребителя съгласно инструкциите на ►M2 члена на Комисията, отговарящ за въпросите по сигурността◄ [22.5].	Излишните екземпляри и документите, които вече не са необходими, трябва да се унищожават (22.5).

▼B

Допълнение 3

Насоки за предоставяне на достъп до класифицирана информация на ЕС на трети държави или международни организации: Сътрудничество от степен 1

ПРОЦЕДУРИ

1. Правото да предоставя достъп до класифицирана информация на ЕС на страни, които не са членки на Европейския съюз или на други международни организации, чиито политика и нормативни са съпоставими с тези на ЕС, принадлежи на Комисията като колегиален орган.

2. До сключването на споразумение за сигурност членът на Комисията, който отговаря за въпросите на сигурността, е компетентен да разглежда исканията за предоставяне на достъп до класифицирана информация на ЕС.

3. При това той/тя:

   — иска становището на авторите на класифицираната информация на ЕС, до която ще се предостави достъп,

   — установява необходимите контакти с органите за сигурност на държавите или международните организации бенефициери, за да провери, дали техните разпоредби и политика за сигурност гарантират, че предоставената класифицирана информация ще се защитава в съответствие с настоящите разпоредби за сигурност,

   — иска становището на Консултативната група по политиката за сигурност на Комисията относно доверието, което може да се окаже на държавите или международните организации бенефициери.

4. Членът на Комисията, който отговаря за въпросите на сигурността, изпраща на Комисията искането и становището на Консултативната група по политиката за сигурност на Комисията за вземане на решение.

РАЗПОРЕДБИ ЗА СИГУРНОСТ, КОИТО ТРЯБВА ДА СЕ ПРИЛАГАТ ОТ БЕНЕФИЦИЕНРИТЕ

5. Членът на Комисията, който отговаря за въпросите на сигурността, нотифицира държавите или международните организации бенефициери за решението на Комисията за даване на разрешение за предоставяне на достъп до класифицирана информация на ЕС.

6. Решението за предоставяне на достъп влиза в сила едва когато бенефициерите са представили писмено уверение, че:

   — няма да използват информацията за никакви други цели, освен за договорените,

   — ще защитават информацията в съответствие с настоящите разпоредби за сигурност, и по-конкретно с изложените по-долу особени правила.

7. Персонал

   а) Броят на длъжностните лица, които имат достъп до класифицираната информация на ЕС стриктно се ограничава въз основа на принципа за „необходимост да се знае“ до лицата, чиито служебни задължения изискват такъв достъп.

   б) Всички длъжностни лица или граждани, които имат право на достъп до информация, която е класифицирана като ►**M1** RESTREINT UE ◄ информация или с по-висока степен на класифициране, трябва да притежават сертификат за сигурност за подходящата степен на класифициране или аналогично разрешение за достъп до секретни материали, издадени от правителството на собствената им държава.

8. Предаване на документи

   а) Практическите процедури за предаването на документи се определят чрез споразумение. До сключването на такова споразумение се прилагат разпоредбите на раздел 21. В споразумението по-конкретно се посочват службите за регистрация, до които трябва да се изпраща класифицираната информация на ЕС.

▼B

б) Ако класифицираната информация, до която Комисията е разрешила да се предостави достъп, включва ►M1 RESTREINT UE ◄ информация, държавата или международната организация бенефициер създава централна служба за регистрация на информация на ЕС, и евентуално нейни подразделения. Тези служби за регистрация стриктно прилагат аналогични разпоредби на съдържащите се в раздел 22 от настоящите разпоредби за сигурност.

9. Регистрация

Веднага след като дадена служба за регистрация получи документ на ЕС, който е класифициран като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ или с по-висока степен на класифициране, тя вписва документа в специален регистър, който се води от организацията и съдържа колони за датата на получаване, данни за документа (дата, референтен номер и брой екземпляри), неговата класификация, заглавие, името или длъжността на получателя, датата на връщане на разписката и датата, на която документът е върнат на автора в ЕС или е унищожен.

10. Унищожаване

а) Класифицираните документи на ЕС се унищожават в съответствие с инструкциите, които са установени в раздел 22 от настоящите разпоредби за сигурност. Копия от сертификатите за унищожаване на ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ документи се изпращат до службата за регистрация на ЕС, която е изпратила документите.

б) Класифицираните документи на ЕС се включват в плановете за аварийно унищожаване, които са изготвени за собствените класифицирани документи на органите на бенефициера.

11. Защита на документите

Предприемат се всички мерки за предотвратяване на достъпа на неупълномощени лица до класифицирана информация на ЕС.

12. Копия, преводи и извлечения

Не се правят никакви фотокопия, преводи или извлечения от документ, който е класифициран като ►M1 RESTREINT UE ◄ или ►M1 RESTREINT UE ◄ ДОКУМЕНТ, без разрешение на началника на съответната организация за сигурност, който регистрира и проверява тези копия, преводи или извлечения, и когато е необходимо ги подпечатва.

Разрешение за възпроизвеждане или превод на ►M1 RESTREINT UE ◄ документ се дава само от органа автор, който определя броя на оторизираните екземпляри; ако не може да се определи кой е органът автор, искането се изпраща до ►M2 дирекция по сигурността на Комисията ◄.

13. Нарушения на разпоредбите за сигурност

В случай на действително или предполагаемо нарушение на разпоредбите за сигурност във връзка с класифициран документ на ЕС, незабавно се предприемат следните действия, при условие че има сключено споразумение за сигурност:

а) провежда се разследване за установяване на обстоятелствата, при които е извършено нарушението на разпоредбите за сигурност;

б) нотифицира се ►M2 дирекция по сигурността на Комисията ◄, съответния национален орган за сигурност и органа автор, или ясно се посочва, че последният не е нотифициран, ако това не е направено;

в) предприемат се действия за свеждане до минимум на последиците от нарушението на разпоредбите за сигурност;

г) преразглеждат се и се прилагат мерки за предотвратяване на евентуално повторно извършване на нарушението;

д) прилагат се всички мерки, които са препоръчани от ►M2 дирекция по сигурността на Комисията ◄ за предотвратяване на повторно извършване на нарушението.

▼B

14. Инспекции

По споразумение със съответните държави или международни организации на ►M2 дирекция по сигурността на Комисията ◄ се разрешава да извършва оценка на ефективността на мерките за защита на предоставената класифицирана информация на ЕС.

15. Докладване

При условие че има сключено споразумение за сигурност, докато държавата или международната организация притежава класифицирана информация на ЕС, тя представя годишен доклад до определена дата, която се посочва при даването на разрешение за предоставяне на достъп до информацията, в който се потвърждава, че са спазени настоящите разпоредби за сигурност.

▼B

Допълнение 4

Насоки за предоставяне на достъп до класифицирана информация на ЕС на трети държави или международни организации: Сътрудничество от степен 2

ПРОЦЕДУРИ

1. Правото да предоставя достъп до класифицирана информация на ЕС на трети държави или международни организации, чиито политика за сигурност и разпоредби силно се отличават от тези на ЕС, принадлежи на автора. Правото да предоставя достъп до класифицирана информация на ЕС, която е създадена в Комисията, принадлежи на Комисията в качеството ѝ на колегиален орган.

2. По принцип предоставянето на достъп се ограничава до информация, която е класифицирана като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ включително; това изключва класифицирана информация, която е защитена със специални обозначения или маркировки за сигурност.

3. До сключването на споразумение за сигурност членът на Комисията, който отговаря за въпросите на сигурността, е компетентен да разглежда исканията за предоставяне на достъп до класифицирана информация на ЕС.

4. При това той/тя:

   — иска становището на авторите на класифицираната информация на ЕС, до която ще се предостави достъп,

   — установява необходимите контакти с органите за сигурност на държавите или международните организации бенефициери, за да получи информация за техните разпоредби и политика за сигурност, и по-специално за да изготви таблица за съпоставка между приложимите класификации в ЕС и в съответната държава или организация,

   — организира заседание на Консултативната група по политиката за сигурност на Комисията или когато е необходимо съгласно процедурата на мълчаливо съгласие, извършва проучване при националните органи за сигурност на държавите-членки с оглед получаване на становището на Консултативната група по политиката за сигурност на Комисията.

5. Становището на Консултативната група по политиката за сигурност на Комисията се отнася за следното:

   — доверието, което може да се окаже на държавите или на международните организации бенефициери с оглед извършването на оценка на рисковете за сигурността, които се поемат от ЕС или нейните държави-членки,

   — оценка на способността на бенефициерите да защитават предоставената от ЕС класифицирана информация,

   — предложения относно практическите процедури за работа с класифицираната информация на ЕС (например, предоставяне на цензурирани версии на текст) и изпратените документи (запазване или заличаване на класификационни заглавия, специфични маркировки и др. на ЕС),

   — понижаване на степента на класифициране или декласифициране преди да се предостави достъп до информацията на страните или на международните организации бенефициери.

6. Членът на Комисията, който отговаря за въпросите на сигурността изпраща на Комисията искането и становището на Консултативната група по политиката за сигурност на Комисията за вземане на решение.

ПРАВИЛА ЗА СИГУРНОСТ, КОИТО ТРЯБВА ДА СЕ ПРИЛАГАТ ОТ БЕНЕФИЦИЕРИТЕ

7. Членът на Комисията, който отговаря за въпросите на сигурността, нотифицира държавите или международните организации бенефициери за решението на Комисията за даване на разрешение за предоставяне на достъп до класифицирана информация на ЕС и за определените от нея ограничения.

▼B

8. Решението за предоставяне на достъп влиза в сила едва, когато бенефициерите са представили писмено уверение, че:

   — няма да използват информацията за никакви други цели, освен за договорените,

   — ще защитават информацията в съответствие с разпоредбите на Комисията.

9. Прилагат се посочените по-долу правила за защита, освен ако Комисията, след получаване на техническото становище на Консултативната група по политиката за сигурност на Комисията, вземе решение за прилагане на особена процедура за работа с класифицираните документи на ЕС (заличаване на класификационните обозначения, специфични маркировки и др. на ЕС).

10. Персонал

    а) Броят на длъжностните лица, които имат достъп до класифицираната информация на ЕС стриктно се ограничава, въз основа на принципа на „необходимост да се знае“, до лицата, чиито служебни задължения изискват такъв достъп.

    б) Всички длъжностни лица или граждани, които имат разрешение за достъп до предоставената от Комисията класифицирана информация, притежават национално разрешение за достъп до секретни материали или разрешение за достъп до подходящата степен на класифициране, което е аналогично на това на ЕС, както е определено в сравнителната таблица.

    в) Тези национални разрешения за достъп до секретни материали или разрешения се изпращат на ►M2 директора на дирекцията по сигурността на Комисията ◄ за информация.

11. Предаване на документи

    Практическите процедури за предаването на документи се определят чрез споразумение. До сключването на такова споразумение се прилагат разпоредбите на раздел 21. В споразумението по-специално се посочват службите за регистрация, до които трябва да се изпраща класифицираната информация на ЕС, и точните адреси, на които трябва да се изпращат документите, както и куриерските или пощенските служби, които се използват за предаването на класифицирана информация на ЕС.

12. Регистрация при получаване

    Националният орган за сигурност или неговият еквивалент в държавата адресат, който от името на правителството си получава изпратената от Комисията класифицирана информация или службата по сигурността на международната организация получател, открива специален регистър за вписване на класифицираната информация на ЕС при нейното получаване. Регистърът съдържа колони, в които се посочват датата на получаване, данни за документа (дата, референтен номер и брой екземпляри), неговата класификация, заглавие, името или длъжността на получателя, датата на връщане на разписката и датата, на която документът е върнат на ЕС или е унищожен.

13. Връщане на документи

    Когато получателят връща класифициран документ на Комисията, той процедира по начина, който е посочен в параграф „Предаване на документи“ по-горе.

14. Защита

    а) Когато документите не се използват, те се съхраняват в контейнер за сигурност, който е одобрен за съхранението на национално класифициран материал със същата степен на класифициране. Контейнерът няма обозначения за съдържанието му, до което достъп имат само лица, които са оторизирани да работят с класифицирана информация на ЕС. Когато се използват ключалки с комбинации за заключване, комбинацията се знае само от длъжностните лица в държавата или организацията, които имат разрешение за достъп до съхраняваната в контейнера класифицирана информация на ЕС и комбинацията се сменя на всеки шест месеца или по-скоро при преместване на служител, при отнемане на разрешението за достъп до секретни материали на някое от длъжностните лица, които знаят комбинацията, или ако е налице опасност от излагане на риск.

▼B

б) Класифицираните документи на ЕС се изнасят от контейнера за сигурност само от длъжностните лица, които имат разрешение за достъп до класифицирани документи на ЕС и е „необходимо да знаят“. Докато притежават тези документи, те са отговорни за безопасното им съхранение, и по-специално гарантират, че неупълномощени лица нямат достъп до документите. Те гарантират също, че след приключване на справките с тези документи и извън работно време документите се съхраняват в контейнер за сигурност.

в) Не се правят никакви фотокопия или извлечения от документ, който е класифициран като ►M1 RESTREINT UE ◄ ДОКУМЕНТ или с по-висока степен на класифициране, без разрешение на ►M2 дирекция по сигурността на Комисията ◄.

г) Процедурата за бързо и пълно унищожаване на документите в аварийна ситуация се определя и потвърждава от ►M2 дирекция по сигурността на Комисията ◄.

15. Физическа сигурност

а) Когато не се използват, контейнерите за сигурност, които се използват за съхранение на класифицирани документи на ЕС, се държат непрекъснато заключени;

б) Когато е необходимо персонал, който отговаря за поддръжката или за почистването, да влиза или да работи в стая, където се помещават такива контейнери за сигурност, те по всяко време се придружават от служител от службата по сигурността на държавата или организацията, или от служителя, който по-конкретно отговаря за контрола на сигурността на стаята;

в) Извън обичайното работно време (нощем, в съботни и неделни дни и на официални празници) контейнерите за сигурност, които съдържат класифицирани документи на ЕС, се пазят или от охраняващ служител, или от автоматична алармена система.

16. Нарушения на разпоредбите за сигурност

В случай на действително или предполагаемо нарушение на разпоредбите за сигурност във връзка с класифициран документ на ЕС незабавно се предприемат следните действия:

а) Незабавно се изпраща доклад до ►M2 дирекция по сигурността на Комисията ◄ или до националния орган за сигурност на държавата-членка, която е поела инициативата при изпращането на документите (с копие до ►M2 дирекция по сигурността на Комисията ◄);

б) Провежда се разследване, след приключването на което се представя пълен доклад на органа за сигурност (виж буква а) по-горе). След това се предприемат необходимите мерки за коригиране на ситуацията.

17. Инспекции

По споразумение със съответните държави или международни организации, на ►M2 дирекция по сигурността на Комисията ◄ се разрешава да извършва оценка на ефективността на мерките за защита на предоставената класифицирана информация на ЕС.

18. Докладване

При условие че има сключено споразумение за сигурност, докато държавата или международната организация притежава класифицирана информация на ЕС, тя представя годишен доклад до определена дата, която се посочва при даването на разрешение за предоставяне на достъп до информацията, в който се потвърждава, че са спазени настоящите разпоредби за сигурност.

▼B

Допълнение 5

Насоки за предоставяне на достъп до класифицирана информация на ЕС на трети държави или международни организации: Сътрудничество от степен 3

ПРОЦЕДУРИ

1. Понякога Комисията може да желае да си сътрудничи при определени особени обстоятелства с държави или организации, които не могат да предоставят уверенията, които се изискват съгласно настоящите правила за сигурност, но това сътрудничество може да налага предоставянето на достъп до класифицирана информация на ЕС.

2. Правото да предоставя достъп до класифицирана информация на ЕС на трети държави или международни организации, чиито политика за сигурност и нормативни разпоредби силно се отличават от тези на ЕС, принадлежи на автора. Правото да предоставя достъп до класифицирана информация на ЕС, която е създадена в Комисията, принадлежи на Комисията в качеството ѝ на колегиален орган.

   По принцип предоставянето на достъп се ограничава до информация, която е класифицирана като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ включително; това изключва класифицирана информация, която е защитена със специални обозначения или маркировки за сигурност.

3. Комисията преценява дали е разумно да се предостави достъп до класифицирана информация, преценява необходимостта на бенефициерите да знаят тази информация и взема решение относно естеството на класифицираната информация, която може да се съобщи.

4. Ако решението на Комисията е положително, членът на Комисията, който отговаря за въпросите на сигурността:

   — иска становището на авторите на класифицираната информация на ЕС, до която ще се предостави достъп,

   — организира заседание на Консултативната група по политиката за сигурност на Комисията или — когато е необходимо съгласно процедурата на мълчаливо съгласие — извършва проучване при националните органи за сигурност на държавите-членки с оглед получаване на становището на Консултативната група по политиката за сигурност на Комисията.

5. Становището на Консултативната група по политиката за сигурност на Комисията се отнася за следното:

   а) оценка на рисковете за сигурността, които се поемат от ЕС или нейните държави-членки;

   б) степента на класифициране на информацията, до която може да се предостави достъп;

   в) понижаване на степента на класифициране или декласифициране преди да се предостави достъп до информацията;

   г) процедурите за работа с документите, до които ще се предостави достъп (виж буква д) по-долу);

   д) възможните методи за предаване (използване на обществени пощенски услуги, обществени или защитени телекомуникационни системи, дипломатическа поща, упълномощени куриери и т.н.).

6. Документите, които се предоставят на държавите или организациите, включени в настоящото допълнение, по принцип се изготвят без позоваване на източника или на класификация на ЕС. Консултативната група по политиката за сигурност на Комисията може да препоръча:

   — използването на специфична маркировка или кодово наименование;

   — използването на специфична система за класифициране, която да обвързва деликатността на информацията с необходимите мерки за контрол при прилаганите от бенефициерите методи за предаване на документите.

▼B

7. ►M2 Члена на Комисията, отговарящ за въпросите на сигурността ◄ изпраща на Комисията становището на Консултативната група по политиката за сигурност на Комисията за вземане на решение.

8. След като Комисията одобри предоставянето на достъп до класифицирана информация на ЕС и практическите процедури за прилагане, ►M2 дирекция по сигурността на Комисията ◄ установява необходимия контакт с органа за сигурност на съответната държава или организация с цел улесняване на прилагането на предвидените мерки за сигурност.

9. Членът на Комисията, който отговаря за въпросите на сигурността, информира държавите-членки за естеството и степента на класифициране на информацията, като представя списък на организациите и страните, на които тя може да се предоставя съгласно решението на Комисията.

10. ►M2 Дирекция по сигурността на Комисията ◄ предприема необходимите мерки за улесняване на евентуална последваща оценка на вредите и за преразглеждане на процедурите.

При промяна на условията на сътрудничество Комисията преразглежда въпроса.

РАЗПОРЕДБИ ЗА СИГУРНОСТ, КОИТО ТРЯБВА ДА СЕ ПРИЛАГАТ ОТ БЕНЕФИЦИЕРИТЕ

11. Членът на Комисията, който отговаря за въпросите на сигурността, нотифицира държавите или международните организации бенефициери за решението на Комисията за даване на разрешение за предоставяне на достъп до класифицирана информация на ЕС, заедно с предложените от Консултативната група по политиката за сигурност на Комисията и одобрени от Комисията подробни правила за защита.

12. Решението влиза в сила едва когато бенефициерите са представили писмено уверение, че:

— няма да използват информацията за никакви други цели, освен за сътрудничеството, за което е взето решение от Комисията,

— ще защитават информацията в съответствие с изискванията на Комисията.

13. Предаване на документи

а) Практическите процедури за предаването на документи се договарят между ►M2 дирекция по сигурността на Комисията ◄ и органите за сигурност на държавите или международните организации получатели. По-специално те посочват точните адреси, на които трябва да се изпращат документите.

б) Документи, които са класифицирани като ►M1 RESTREINT UE ◄ ДОКУМЕНТИ и с по-висока степен на класифициране, се предават в двойни пликове. Върху вътрешния плик се обозначава специфичния щемпел или кодово наименование, за което е взето решение, и утвърдената за документа специална класификация. За всеки класифициран документ се прилага формуляр за получаване. Във формуляра за получаване, който сам по себе си не е класифициран, се посочват само данните на документа (референтен номер, дата, брой екземпляри) и езика, на който същият е изготвен, без заглавието му.

в) След това вътрешният плик се поставя във външния плик, върху който се обозначава номер на пратката за целите на получаването. Върху външния плик не се обозначава класификация за сигурност.

г) На куриерите винаги се дава разписка, върху която е посочен номерът на пратката.

▼B

14. Регистрация при получаване

Националният орган за сигурност или неговият еквивалент в държавата адресат, който от името на правителството си получава изпратената от Комисията класифицирана информация, или службата по сигурността на международната организация получател открива специален регистър за вписване на класифицираната информация на ЕС при нейното получаване. Регистърът съдържа колони, в които се посочват датата на получаване, данни за документа (дата, референтен номер и брой екземпляри), неговата класификация, заглавие, името или длъжността на получателя, датата на връщане на разписката и датата, на която документът е върнат на ЕС или е унищожен.

15. Използване и защита на обменяната класифицирана информация

а) Информацията, която е класифицирана като ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, се обработва от специално определени длъжностни лица, които имат разрешение за достъп до информация с тази степен на класифициране. Тя се съхранява в добре обезопасени шкафове, които могат да се отварят само от лицата, които са упълномощени да имат достъп до съдържащата се в тях информация. Зоните, в които се намират тези шкафове, постоянно се охраняват и се създава система за проверка, която да гарантира, че в тях се допускат да влизат само надлежно упълномощени лица. ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ се изпраща с дипломатическа поща, защитени пощенски служби или защитени телекомуникационни системи. ►M1 RESTREINT UE ◄ ДОКУМЕНТ се копира само с писмено разрешение на органа автор. Всички копия се регистрират и следят. За всички операции, свързани със ►M1 RESTREINT UE ◄ ДОКУМЕНТИ, се издават разписки;

б) ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ се обработва от надлежно определени длъжностни лица, които са упълномощени да бъдат информирани за предмета на информацията. Документите се съхраняват в заключени шкафове за сигурност в контролирани зони.

►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ се изпраща с дипломатическа поща, военни пощенски служби и защитени телекомуникационни системи. Органът получател може да прави копия, като техният брой и разпределение се вписват в специални регистри;

в) Информация ►M1 RESTREINT UE ◄ се обработва в помещения, до които не може да има достъп неупълномощен персонал и се съхранява в заключени контейнери. Документите могат да се изпращат с обществени пощенски служби като препоръчана поща в двоен плик, а в аварийни ситуации по време на операции — чрез незащитени обществени телекомуникационни системи. Получателите могат да правят копия;

г) Некласифицираната информация не изисква специални мерки за защита и може да се изпраща по пощата и чрез обществени далекосъобщителни системи. Адресатите могат да правят копия.

16. Унищожаване

Документите, които вече не са необходими, се унищожават. В случай на документи ►M1 RESTREINT UE ◄ и ►M1 RESTREINT UE ◄ документи се извършва съответно вписване в специалните регистри. В случай на ►M1 RESTREINT UE ◄ документи се издават сертификати за унищожаване, които се подписват от две лица, които са присъствали на унищожаването.

17. Нарушения на разпоредбите за сигурност

В случай на действително или предполагаемо излагане на риск на ►M1 RESTREINT UE ◄ ИЛИ ►M1 RESTREINT UE ◄ ИНФОРМАЦИЯ, националният орган за сигурност на държавата или началникът на службата по сигурността в организацията провежда разследване на обстоятелствата във връзка с излагането на риск. ►M2 Дирекция по сигурността на Комисията ◄ се нотифицира за резултатите от разследването. Предприемат се необходимите стъпки за коригиране на неподходящите процедури или методи на съхранение, ако те са били причината за излагането на риск.

▼B

Допълнение 6

СПИСЪК НА СЪКРАЩЕНИЯТА

ACPC	Консултативен комитет за доставки и договори
CrA	Криптографски орган
CISO	Завеждащ сигурността на информацията на централно равнище
COMPUSEC	Компютърна сигурност
COMSEC	Сигурност на комуникациите
CSO	►M2 Дирекция по сигурността на Комисията ◄
ESDP	Европейска политика за сигурност и отбрана
EUCI	Класифицирана информация на ЕС
IA	Орган по сигурността на информацията
INFOSEC	Сигурност на информацията
IO	Собственик на информацията
ISO	Международна организация за стандартизация
IT	Информационна технология
LISO	Отговорник по сигурността на информацията на местно равнище
LSO	Отговорник по сигурността на местно равнище
MSO	Отговорник по сигурността на среща
NSA	Национален орган за сигурност
PC	Персонален компютър
RCO	Служител, отговорен за контрола на службата за регистрация
SAA	Акредитиращ орган по сигурността
SecOPS	Процедури за сигурност при работа
SSRS	Декларация за специфичните изисквания за сигурност на системата
TA	Орган „TEMPEST“
TSO	Собственик на технически системи

▼M3

DSA	Обозначен орган по сигурността
FSC	Разрешително за сигурност на оборудване
FSO	Отговорник по сигурността на оборудване
PSC	Разрешително за сигурност на персонала
SAL	Приложение за сигурност
SCG	Ръководство за класификация за сигурност.