РЕШЕНИЕ 2001/264/ЕО НА СЪВЕТА

от 19 март 2001 година

за приемане на разпоредбите на Съвета относно сигурността

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за създаване на Европейската общност и по-специално член 207, параграф 3 от него,

като взе предвид Решение 2000/396/ЕО, ЕОВС, Евратом на Съвета от 5 юни 2000 г. за приемане на Процедурните правила на Съвета[1], и по-специално член 24 от тях,

като има предвид, че:

(1) За да се развива дейността на Съвета в области, за които се изисква степен на поверителност, е целесъобразно да се изгради всеобща система за сигурност, обхващаща Съвета, неговия генерален секретариат и държавите-членки.

(2) Тази система следва да обедини в един текст материята, уредена с всички предходни решения и разпоредби в тази област.

(3) В действителност по-голямата част от информацията на ЕС, с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и по-високо от това ниво, се отнася за Общата политика на сигурност и отбрана.

(4) За да се гарантира ефективността на създадената система за сигурност, държавите-членки следва да се присъединят към нейното функциониране като предприемат национални мерки, необходими за съблюдаването на разпоредбите на настоящото решение, за случаите в които техните компетентни органи и служители работят с класифицирана информация на ЕС.

(5) Съветът приветства намерението на Комисията да въведе, от датата на прилагане на настоящото решение, всеобща система, която да е в съответствие с приложенията към него, за да се осигури безпрепятствено функциониране на процеса на вземане на решения в Съюза.

(6) Съветът подчертава значението на присъединяването, в зависимост от случая, на Европейския парламент и Комисията към правилата и стандартите за поверителност, които са необходими за да се защитят интересите на Съюза и на държавите-членки.

(7) Настоящото решение се приема без да се засяга член 255 от Договора и инструментите за неговото изпълнение.

(8) Настоящото решение се приема без да се засяга съществуващата практика в държавите-членки относно информирането на националните парламенти за дейността на Съюза,

РЕШИ:

Член 1

Одобрява разпоредбите на Съвета относно сигурността, които се съдържат в п приложението.

Член 2

1. Генералният секретар/върховният представител предприема съответстващи мерки, за да гарантира, че при работа с класифицирана информация на ЕС посочените в член 1 разпоредби се съблюдават в рамките на генералния секретариат на Съвета (наричан по-нататък „ГСС”) от висшите длъжностни лица и другите служители в ГСС, от външните контрагенти на ГСС и от персонала, командирован в ГСС, както и в рамките на помещенията на Съвета и децентрализираните агенции на ЕС.[1]

2. Държавите-членки вземат подходящи мерки, в съответствие с националните разпоредби, за да гарантират, че при работа с класифицирана информация на ЕС се съблюдават разпоредбите, посочени в член 1, в техните обекти и помещения от:

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

б) други членове на националните администрации на държавите-членки, които обработват класифицирана информация на ЕС, независимо дали работят на територията на държавите-членки или зад граница; и

в) външните контрагенти на ЕС и командированият персонал, които работят с класифицирана информация на ЕС.

Държавите-членки незабавно информират ГСС за взетите мерки.

3. Мерките, предвидени в параграфи 1 и 2, се предприемат преди 30 ноември 2001 г.

Член 3

Като съблюдава основните принципи и минималните стандарти за сигурността, които се съдържат в част I на приложение приложението, генералният секретар/върховният представител може да взема мерки в съответствие с част II, раздел I, точки 1) и 2) на приложението.

Член 4

От датата на своето прилагане, настоящото решение замества:

а) Решение 98/319/ЕО на Съвета от 27 април 1998 г. относно процедурите, чрез които може да бъде разрешен достъп на висши длъжностни лица и служители на генералния секретариат на Съвета до класифицирана информация, държана от Съвета[2] ;

б) Решение на генералния секретар/върховния представител от 27 юли 2000 г. относно мерките за защита на класифицираната информация, приложими за генералния секретариат на Съвета[3];

в) Решение 433/97 на генералния секретар на Съвета от 22 май 1997 г. относно процедурата за проучване за надеждност от гледна точка на сигурността на висшите длъжностни лица, които отговарят за функционирането на мрежата Кортеси.

Член 5

1. Настоящото решение влиза в сила в деня на публикуването му.

2. Прилага се от 1 декември 2001 година.

Съставено в Брюксел на 19 март 2001година.

За Съвета
Председател
A. LINDH

ПРИЛОЖЕНИЕ

РАЗПОРЕДБИ НА СЪВЕТА НА ЕВРОПЕЙСКИЯ СЪЮЗ ОТНОСНО СИГУРНОСТТА

СЪДЪРЖАНИЕ

ЧАСТ I

ОСНОВНИ ПРИНЦИПИ И МИНИМАЛНИ СТАНДАРТИ ЗА СИГУРНОСТ

ВЪВЕДЕНИЕ

1. Настоящите разпоредби определят основните принципи и минималните стандарти, които следва да се съблюдават надлежно от Съвета, от генералния секретариат на Съвета (наричан по-нататък „ГСС”), от държавите-членки и от децентрализираните агенции на Европейския съюз (наричани по-нататък „децентрализирани агенции на ЕС”), за да се гарантира сигурността им както и създаването на общ стандарт на защита.

2. Терминът „класифицирана информация на ЕС” означава всяка информация и материал, нерегламентираното разкриване на които би увредило в различна степен интересите на ЕС или на една или повече държави-членки, трети страни или международни организации.

3. По смисъла на настоящите разпоредби:

а) „документ” е писмо, работни бележки, протокол, отчет, меморандум, сигнал/съобщение, скица, фотография, диапозитив, филмова лента, карта, диаграма, план, записки, индигов лист, лента за пишеща машина или принтер, лента, касета, компютърен диск, CD ROM, или друг физически носител, на който е записана информация;

б) „материал” е „документ” по смисъла на а) по-горе, както и съоръжение или въоръжение, произведени или в процес на производство, както и съставни части от тях.

4. Основни цели на сигурността:

а) защита на класифицираната информация на ЕС от шпиониране, компрометиране или нерегламентирано разкриване;

б) защита на информацията на ЕС, обработвана в комуникационните и информационните системи и мрежи, от рискове, свързани с нейната цялостност и достъпност;

в) защита на съоръженията, в които се намира информация на ЕС, от саботажи или злонамерено и умишлено повреждане;

г) в случай на повреда да се направи оценка на причинените щети, да се ограничат последствията от тях и да се приемат необходимите изправителни мерки.

5. Основи на надеждната сигурност:

а) в рамките на всяка държава-членка, организацията по националната сигурност, която отговаря за:

(i) събирането и записването на информация за шпиониране, саботиране, терористични и други подривни дейности и

(ii) предоставянето на информация и съвети на собственото правителство, а чрез него и на Съвета, относно естеството на заплахите за сигурността и средствата за защита срещу тях;

б) в рамките на всяка държава-членка, и в рамките на ГСС, техническият орган по ИНФОСЕК (информационна сигурност), който отговаря за работата със съответния орган по сигурността в областта на предоставянето на информация

и съвети относно техническите заплахи за сигурността и средствата за защита срещу тях;

в) редовното взаимодействие между държавните ведомства, агенциите и съответните служби на ГСС, за да се определят и препоръчат в зависимост от случая:

(i) информацията, носителите и съоръженията, които се нуждаят от защита, и

(ii) общите стандарти за защита

6. Когато става въпрос за поверителност, са необходими внимание и опит при подбора на информацията и материала, които ще бъдат защитени, и оценката на необходимата степен на защита. Основното съображение е степента на защита да съответства на значението по отношение на сигурността на отделната информация или материал, които ще бъдат защитени. За да се гарантира безпрепятствено движение на информацията, е необходимо да се вземат мерки за предотвратяване на включване в по-висока степен на класификация. Класификационната система е инструментът за осъществяването на тези принципи; подобна класификационна система трябва да бъде приложена и при планирането и организирането на различните форми на борба с шпионирането, саботажите, тероризма и другите заплахи, така че най-голямата защитна мярка да се определи за най-важните обекти и помещения, в които се намира класифицирана информация, и за най-уязвимите точки в тях.

ОСНОВНИ ПРИНЦИПИ

7. Мерките за сигурност:

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

б) са предназначени за откриване на лицата, които поради длъжността, която заемат, биха могли да застрашат сигурността на класифицираната информация и на важни съоръжения, в които се намира класифицирана информация, и да осигурят тяхното изключване или отстраняване;

в) предотвратяват достъпа на неупълномощени лица до класифицирана информация или до съоръжения, съдържащи такава информация;

г) гарантират, че разпространението на класифицираната информация става единствено при спазване на принципа „необходимост да се знае”, който е решаващ за всички аспекти на сигурността;

д) гарантират цялостност (т.е. предпазване от компрометиране, нерегламентирано изменение или нерегламентирано заличаване) и достъпност (т.е. не се отказва достъп на лица, които имат необходимост, и на лица, получили разрешение за достъп) на цялата информация, както на класифицираната, така и на некласифицираната, и по-специално на информацията, която е съхранявана, обработвана и пренасяна в електромагнитен вид.

ОРГАНИЗИРАНЕ НА СИГУРНОСТТА

Общи минимални стандарти

8. Съветът и всяка държава-членка гарантират съблюдаването на общите минимални стандарти за сигурност във всички административни и/или държавни ведомства, другите институции на ЕС, агенциите и контрагентите, за да може класифицираната информация на ЕС да се предава с увереността, че тя ще бъде обработвана с равностойно внимание. Минималните стандарти включват критериите за проучване на надеждността на персонала от гледна точка на сигурността и процедурите по защитата на класифицираната информация на ЕС.

СИГУРНОСТ НА ПЕРСОНАЛА

Проучване на надеждността на персонала от гледна точка на сигурността

9. Всички лица, поискали достъп до информация с ниво на класификация „ПОВЕРИТЕЛНО ЗА ЕС" или по-високо от това ниво, следва да преминат през надлежно проучване на надеждността от гледна точка на сигурността преди да им бъде разрешен такъв достъп. Подобно проучване на надеждността от гледна точка на сигурността се изисква и по отношение на лицата, служебните задължения на които включват техническа експлоатация или поддържане на комуникационни или информационни системи, съдържащи класифицирана информация. Предназначението на това проучване е да се определи дали упоменатите лица:

а) притежават безспорна лоялност;

б) имат необходимия характер и отговорност, които не допускат и най-малкото съмнение по отношение на тяхната почтеност при работа с класифицирана информация; или

в) могат да бъдат уязвими при натиск от чуждестранни или други източници, например поради предишно местожителство или връзки в миналото, които биха могли да представляват заплаха за сигурността.

Процедурите по проучването на надеждността от гледна точка на сигурността подлагат на особено внимателна проверка лицата:

г) на които следва да се предостави достъп до информация с ниво на класификация „СТРОГО СЕКРЕТНО ЗА ЕС";

д) които заемат постове, включващи редовен достъп до значителна по обем информация с ниво на класификация „СЕКРЕТНО ЗА ЕС";

е) задълженията на които им дават специален достъп до комуникационни и информационни системи от решаващо значение за изпълнението на конкретно възложена задача и по този начин и възможност за получаване на нерегламентиран достъп до значителна по обем класифицирана информация на ЕС или за нанасяне на сериозна вреда на изпълнението на конкретно възложена задача чрез действия на техническия саботаж.

При обстоятелствата, дадени в подточки г), д) и е), се използват в най-пълна степен способите за разследване на биографичните данни.

10. Когато лица, за които не е установена „необходимост да се знае" следва да се наемат при обстоятелства, при които те могат да имат достъп до класифицирана информация на ЕС (например куриери, служители по сигурността, персонал по поддръжката и почистването и др.), те най-напред преминават през съответно проучване за надеждност от гледна точка на сигурността.

Документация за проучването на персонала за надеждност от гледна точка на сигурността

11. Всички служби, органи или институции, които работят с класифицирана информация на ЕС или в които се намират комуникационни и информационни системи от решаващо значение за изпълнението на конкретно възложена задача, поддържат документация за проучванията за надеждност от гледна точка на сигурността на персонала, назначен в тях. Всяко проучване за надеждност от гледна точка на сигурността се проверява във всеки конкретен случай, за да се гарантира, че проучването е в съответствие с конкретно изпълняваната задача от лицето; проучването спешно се преразглежда при получаването на нова информация, което е показателно за това, че възлагането на продължителни служебни задължения за работа с класифицирана информация вече не са в интерес на сигурността. Документацията за проучванията на персонала за надеждност от гледна точка на сигурността се води от ръководителя, отговарящ за сигурността в съответната служба, орган или институция.

Инструктиране на персонала относно сигурността

12. Всички членове на персонала, назначени на постове, на които биха могли да имат достъп до класифицирана информация, получават подробни инструкции при назначаването и през определени интервали от време относно необходимостта от сигурност и процедурите по осигуряването ѝ. Полезна процедура е да се изиска от тези членове на персонала да потвърдят писмено, че са напълно запознати с разпоредбите относно сигурността, които се отнасят за техните служебни задачи.

Задължения на ръководството

13. Ръководителите са задължени да знаят кои от техните служители работят с класифицирана информация или кои имат достъп до комуникационни и информационни системи от решаващо значение за изпълнението на конкретно възложена задача както и да водят записи и да докладват всички произшествия или случаи на предполагаема уязвимост, които могат да имат връзка със сигурността.

Сигурност на персонала

14. Създават се процедури, които гарантират, че при получаването на неблагоприятна информация за дадено лице ще се определи дали лицето работи с класифицирана информация или има достъп до комуникационни и информационни системи от решаващо значение за изпълнението на конкретно възложена задача и ще се уведоми съответния орган. Ако се установи, че лицето представлява заплаха за сигурността, то не се допуска или се отстранява от изпълнението на конкретно възложената му задача, чрез която би могло да застраши сигурността.

ФИЗИЧЕСКА СИГУРНОСТ

Необходимост от защита

15. Мерките за физическа сигурност, прилагани за да се осигури защитата на класифицираната информация на ЕС, съответстват по степен на класификацията, обема на и заплахата за държаната информация и материал. Затова се вземат мерки да не се допусне включване в по-високо или в по-ниско ниво на класификация и се извършват редовни проверки на класификацията. Всички, които притежават класифицирана информация на ЕС, следват единните практики относно класификацията на тази информация и спазват общите стандарти за защита относно поверяването, предаването и освобождаването от информация и материал, за които се изисква защита.

Проверка

16. Преди напускането на зоните, в които се намира класифицирана информация на ЕС оставена без надзор, лицата, на които тя е поверена, трябва да осигурят надеждно съхраняване на информацията и да активират всички защитни устройства (брави, алармени системи и др.). Допълнително след работното време се извършват независими проверки.

Защита на сградите

17. Сградите, в които се намира класифицирана информация на ЕС или комуникационни и информационни системи от решаващо значение за изпълнението на конкретно възложена задача, са защитени срещу нерегламентиран достъп. Естеството на защитата, предоставена на класифицираната информация на ЕС, например решетки за прозорци, брави за врати, охрана на входовете, автоматизирани контролни системи за достъп, проверки на сигурността и патрули, алармени системи, системи за откриване на нерегламентирано влизане и охранителни кучета, зависят от :

а) нивото на класификация, обема и местонахождението в сградата на информацията и материала, на които следва да се осигури защита;

б) качеството на сейфовете за тази информация и материал;

в) конструкцията и местонахождението на сградата.

18. Естеството на защитата, предоставена на комуникационните и информационните системи, също така зависи от оценката на стойността на активите, изложени на риск, и възможните щети, в случай на компрометиране на сигурността, по конструкцията и мястото на сградата, в която се намира системата, и върху мястото, на което е разположена системата в сградата.

Планове за извънредни обстоятелства

19. Предварително се изготвят подробни планове за защитата на класифицираната информация по време на настъпване на извънредни обстоятелства от местен или национален характер.

СИГУРНОСТ НА ИНФОРМАЦИЯТА (ИНФОСЕК)

20. ИНФОСЕК е свързана с идентифицирането и прилагането на мерки за сигурност с цел опазване на информацията, съхранена, преработена или предадена по комуникационните, информационните и другите електронни системи, от случайна или умишлено причинена загуба на поверителност, цялостност или достъпност. Предприемат се съответстващи контрамерки, за да се предотврати достъпът до информация на ЕС за неупълномощените потребители, за да не се допусне отказ на достъп до информация на ЕС за упълномощените потребители и за да се предотврати фалшифицирането или нерегламентираното изменение или заличаване на информация на ЕС.

БОРБА СРЕЩУ САБОТАЖИТЕ И ДРУГИТЕ ФОРМИ НА ЗЛОНАМЕРЕНО УМИШЛЕНО ПОВРЕЖДАНЕ

21. Физическите предпазни мерки за защита на важни съоръжения, в които се намира класифицирана информация, са най-добрите защитни предпазни мерки срещу саботаж и злонамерено умишлено повреждане, които не могат да бъдат ефективно заменени само с проучване на персонала за надеждност от гледна точка на сигурността. Компетентният национален орган събира разузнавателна

информация за шпионска дейност, саботажи, тероризъм и други подривни дейности.

ПРЕДОСТАВЯНЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ТРЕТИ ДЪРЖАВИ ИЛИ МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

22. Решението за предоставяне на информация, създадена в Съвета, на трета страна или международна организация се взема от Съвета. Ако създателят на информацията, която се търси за предоставяне, не е Съветът, Съветът най-напред търси съгласието на създателя на информацията, която се търси за предоставяне. Ако създателят на информацията не може да бъде установен, неговите задължения се поемат от Съвета.

23. Ако Съветът получи класифицирана информация от трети страни, от международни организации или от други трети страни, тя получава защита в съответствие с нейното ниво на класификация и равностойна на стандартите, установени с настоящите разпоредби за класифицираната информация на ЕС, или по-високите стандарти, които би могла да изиска третата страна, която предоставя информацията. Могат да се организират съвместни проверки.

24. Принципите, дадени по-горе, се прилагат в съответствие с подробните разпоредби на Част II.

ЧАСТ II

РАЗДЕЛ I

ОРГАНИЗИРАНЕ НА СИГУРНОСТТА В СЪВЕТА НА ЕВРОПЕЙСКИЯ СЪЮЗ

Генералният секретар/върховният представител

1. Генералният секретар/върховният представител:

   а) провежда политиката на Съвета в областта на сигурността;

   б) разглежда проблемите в областта на сигурността, отнесени до него от Съвета или неговите компетентни органи;

   в) проучва въпросите, свързани с промени в политиката на Съвета в областта на сигурността, в тясно взаимодействие с органите за национална сигурност (или други подходящи органи) на държавите-членки (наричани по-нататък „ОНС”). В допълнение 1 е даден списъкът на тези органи.

2. Генералният секретар/върховният представител по-специално:

   а) координира всички въпроси в областта на сигурността, свързани с дейността на Съвета;

   б) отправя молба към всяка държава-членка за създаване на централна регистратура за документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС и изисква създаването на такава регистратура в децентрализираните агенции на ЕС, в зависимост от случая;

   в) изпраща на определените за целта органи на държавите-членки молбите за извършване от страна на ОНС на проучване на персонала в ГСС за надеждност от гледна точка на сигурността в съответствие с раздел VI;

   г) разследва или назначава разследване на случаите на изтичане на класифицирана информация на ЕС, което по добро и достатъчно на пръв поглед доказателство е станало в ГСС или някоя от децентрализираните агенции на ЕС;

   д) отправя молба към съответните органи по сигурността да започнат разследване по случаите, в които изтичането на класифицирана информация на ЕС вероятно е станало извън ГСС или децентрализираните агенции на ЕС, и координира разследванията, в които участват повече от един органи по сигурността;

   е) провежда съвместно и съгласувано със съответния ОНС периодични проверки на мерките за сигурност, използвани за защитата на класифицираната информация на ЕС в държавите-членки;

   ж) поддържа тесни връзки с всички заинтересовани органи по сигурността с оглед на осъществяването на пълна координация на дейностите по сигурността;

   з) извършва непрекъснат преглед на политиката и на процедурите на Съвета в областта на сигурността, а при необходимост, изготвя и съответстващи препоръки. В тази връзка внася в Съвета годишен план за проверките, изготвен от службата за сигурност на ГСС.

Комитетът по сигурността на Съвета

3. Създава се Комитет по сигурността. Той е съставен от представителите на ОНС на всяка държава-членка. Комитетът се председателства от генералния секретар/върховния представител или негов пълномощник. Представителите на децентрализираните агенции на ЕС могат да бъдат поканени да участват, когато се обсъждат въпроси, които ги засягат.

4. Комитетът по сигурността заседава, съгласно указанията на Съвета, по молба на генералния секретар/върховния представител или на някой от ОНС. Комитетът има правомощия да извършва проучване и да прави оценка на всички въпроси в областта на сигурността, свързани с работата на Съвета, и да дава препоръки на Съвета при необходимост. Относно дейността на ГСС, Комитетът има правомощия да прави препоръки по въпросите на сигурността пред генералния секретар/върховния представител.

Службата за сигурност на генералния секретариат на Съвета

5. За изпълнението на задълженията си по параграфи 1 и 2 генералният секретар/върховният представител има на свое разположение службата за сигурност на ГГС при координирането, надзора и изпълнението на мерките за сигурност.

6. Ръководителят на службата за сигурност на ГСС е главният съветник на генералния секретар/върховния представител по въпросите на сигурността и изпълнява длъжността секретар на службата за сигурност. Като такъв той ръководи актуализирането на разпоредбите относно сигурността и координира мерките за сигурност с компетентните органи на държавите-членки, а при необходимост, и с международните организации, свързани със Съвета чрез споразумения в областта на сигурността. За целта той изпълнява длъжността лице за връзка.

7. Ръководителят на службата за сигурност на ГСС отговаря за акредитацията на ИТ системите и мрежите в рамките на ГСС. Ръководителят на службата за сигурност на ГСС и съответната ОНС решават съвместно, в зависимост от случая, акредитацията на ИТ системите и мрежите, в които участват ГСС, държавите-членки, децентрализираните агенции на ЕС и/или трети страни (държави или международни организации).

Децентрализирани агенции на ЕС

8. Директорът на децентрализирана агенция на ЕС отговаря за въвеждането на мерки за сигурност в неговото ведомство. Директорът обикновено определя един от своите служители за отговорник, който се отчита пред него в тази област. Този служител се определя като служител по сигурността.

Държави-членки

9. Всяка държава-членка определя един от органите за национална сигурност, който да отговаря за сигурността на класифицираната информация на ЕС[1].

10. В рамките на администрацията на всяка държава-членка съответният ОНС следва да отговаря за:

а) поддържането на сигурността на класифицираната информация на ЕС, която се намира във всички национални ведомства, органи или агенции, както в публичните, така и в частните, в домовете или зад граница;

б) даването на разрешение за създаване на регистратурите за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС (това правомощие може

да бъде предадено на служителя по контрола на документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС в централната регистратура);

в) периодичната проверка на мерките за сигурност с оглед на защитата на класифицираната информация на ЕС;

г) осигуряването за всички граждани на страната или чуждестранни граждани, назначени в национални ведомства, органи или агенции, които биха могли да имат достъп до информация на ЕС с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, СЕКРЕТНО ЗА ЕС и ПОВЕРИТЕЛНО ЗА ЕС, да преминат през проучване за надеждност от гледна точка на сигурността;

д) съставянето на планове по сигурността, необходими за да се предотврати попадането на класифицирана информация на ЕС в ръцете на лице, което не е получило разрешение за достъп.

Взаимни проверки на сигурността

11. Периодичните проверки на мерките за сигурност с цел защита на класифицираната информация на ЕС в ГСС и Постоянните представителства на държавите-членки в Европейския съюз както и в помещенията на държавите-членки в сградите на Съвета се извършват от служителя по сигурността на ГСС и от съответния ОНС съвместно и по взаимно съгласие[1].

12. Периодичните проверки на мерките за сигурност с цел защита на класифицираната информация на ЕС в децентрализираните агенции на ЕС се извършват от служителя по сигурността на ГСС или, по молба на генералния секретар, от ОНС на държавата-членка, в която се извършва проверката.

[1] Без да засягат Виенската конвенция от 1961г. за дипломатическите отношения.

РАЗДЕЛ II

НИВА НА КЛАСИФИКАЦИЯ И МАРКИРОВКА

НИВА НА КЛАСИФИКАЦИЯ[1]

Информацията е класифицирана по нива както следва:

1. СТРОГО СЕКРЕТНО ЗА ЕС: тази класификация се отнася само за информация и материал, нерегламентираното разкриване на които би застрашило в изключително висока степен съществените интереси на Европейския съюз или на една или повече държави-членки.

2. СЕКРЕТНО ЗА ЕС: тази класификация се отнася само за информация и материал, нерегламентираното разкриване на които би застрашило във висока степен съществените интереси на Европейския съюз или на една или повече държави-членки.

3. ПОВЕРИТЕЛНО ЗА ЕС: тази класификация се отнася само за информация и материал, нерегламентираното разкриване на които би причинило вреди на съществените интереси на Европейския съюз или на една или повече държави-членки.

4. ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС: тази класификация се отнася само за информация и материал, нерегламентираното разкриване на които би се отразило неблагоприятно на интересите на Европейския съюз или на една или повече държави-членки.

МАРКИРОВКА

5. Предупредителна маркировка може да се използва, за да се определи областта на приложение на документа или за конкретно предоставяне на документа при спазване на принципа „необходимост да се знае”.

6. ESDP/PESD маркировка се поставя на документите и копията на документите, които се отнасят за сигурността и отбраната на Съюза или на една или повече държави-членки или се отнасят за управление на военни и невоенни кризи.

7. Допълнителна маркировка, налагаща допълнителни мерки за сигурност по смисъла на съответните разпоредби, може да се постави на някои документи, предимно документите, свързани със системите за информационни технологии (ИТ).

ПОСТАВЯНЕ НА КЛАСИФИКАЦИЯ И МАРКИРОВКА

8. Класификацията и маркировката се поставят както следва:

а) върху документите с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС, чрез механични или електронни средства,

б) върху документите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС, чрез механични средства и на ръка, или чрез отпечатване върху хартия с гриф за сигурност,

в) върху документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, чрез механични средства или на ръка

[1] Сравнителната таблица за степенуването на нивата на класификация за ЕС, НАТО, ЗЕС и държавите-членки се намира в приложение 2

РАЗДЕЛ III

УПРАВЛЕНИЕ НА КЛАСИФИКАЦИЯТА

1. Информацията се класифицира само при необходимост. Класификацията се обозначава ясно и правилно и се поддържа само за периода, през който информацията се нуждае от защита.

2. Отговорността за класифицирането на информацията и за всяко последващо понижаване на класификацията или премахване на класификацията[1] се носи единствено от лицето, създало документа или материала, съдържащ класифицирана информация.

Висшите длъжностни лица и другите служители на ГСС извършват класификация, понижаване или премахване на класификацията на информацията по указание на или със съгласието на генералния директор.

3. Подробните процедури за работа с класифицирани документи са оформени по начин, който гарантира, че те подлежат на защита, съответна на информацията, която съдържат.

4. Броят на лицата, на които е разрешено да създават документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, се свежда до минимум, а имената им се включват в списък, съставен от ГГС, всяка държава-членка, а при необходимост, и от всяка децентрализирана агенция на ЕС.

ОПРЕДЕЛЯНЕ НА КЛАСИФИКАЦИЯТА

5. Класификацията на документа се определя в зависимост от нивото на чувствителност на информацията, която се съдържа в документа, в съответствие с определението в раздел II, параграфи 1 до 4. Важно е класифицирането да се прилага правилно и предпазливо. Това се отнася по-специално за нивото на класификация СТРОГО СЕКРЕТНО ЗА ЕС.

6. Лицето, създало документа подлежащ на класификация, взема под внимание разпоредбите, дадени по-горе, и контролира евентуалните тенденции за повишаване или понижаване на нивото на класификация.

Независимо то това, че по-високото ниво на класификация може на пръв поглед да изглежда като гаранция за по-голяма защита на документа, рутинното използване на по-високо ниво на класификация може да доведе до загуба на доверие във валидността на класификационната система.

От друга страна, не бива да се определя по-ниско ниво на класификация с цел да се избегнат ограниченията, свързани със защитата.

В допълнение 3 е дадено практическо ръководство за нивата на класификация.

7. Отделни страници, параграфи, раздели, анекси, допълнения и различни приложения на даден документ може да изискват различно ниво на класификация и съответна маркировка. Нивото на класификация на целия документ е съответно на тази част от документа, която има най-високото ниво на класификация.

8. Нивото на класификация на писмо или нота с приложения е съответно на най-високото ниво на класификация на приложенията към тях.

Създателят следва ясно да покаже към кое ниво тя следва да бъде класифицирана, когато тя се намира извън своето приложение.

---

[1] Понижаване на класификацията е понижаването на нивото на класификация; премахване на класификацията е премахване на всички нива на класификация

ПОНИЖАВАНЕ И ПРЕМАХВАНЕ НА КЛАСИФИКАЦИЯТА

9. Класификацията на документи на ЕС може да бъде понижена или премахната само с разрешението на лицето, създало документа, а при необходимост, и след обсъждане с другите заинтересовани страни. Понижаването или премахването на класификацията се потвърждава писмено. Институцията, държавата-членка, службата, организацията-правоприемник или висшестоящият орган са отговорни за информирането на адресатите си за промяната, а те от своя страна са отговорни за информирането на всички следващи адресати, на които са изпратили или за които са копирали документа, за промяната.

10. Лицата, създали документите, при възможност определят върху класифицираните документи дата или срок, след изтичането на който е възможно понижаване или премахване на класификацията на съдържанието на документите. В противен случай те извършват преглед на документите най-малко на всеки пет години, за да гарантират, че оригиналната класификация е необходима.

РАЗДЕЛ IV

ФИЗИЧЕСКА СИГУРНОСТ

ОБЩИ ПОЛОЖЕНИЯ

1. Основната цел на мерките за физическа сигурност е да се предотврати достъпът до класифицирана информация и/или материали на ЕС на неупълномощени лица.

ИЗИСКВАНИЯ КЪМ СИГУРНОСТТА

2. Всички помещения, зони, сгради, офиси, стаи, комуникационни и информационни системи и др., в които се съхранява и/или обработва класифицирана информация или материал на ЕС са защитени чрез прилагането на съответстващи мерки за физическа сигурност.

3. При определяне на необходимата степен на защита за физическа сигурност се вземат пред вид всички важни фактори като:

а) нивото на класификация на информацията и/или материала;

б) количеството и формата (например хартиен носител, носители на електронно съхранена информация) на държаната информация;

в) оценката за локална заплаха, предимно от саботажи, терористична дейност и друга подривна и/или престъпна дейност, създавана от разузнавателните служби, чиито обект са ЕС, държавите-членки и/или други институции или трети страни, работещи с класифицирана информация на ЕС.

4. Мерките за физическа сигурност се прилагат с цел:

а) да се предотврати нелегално или насилствено влизане от страна на нарушител;

б) да се възпират, възпрепятстват и откриват действия на нелоялни членове на персонала (вътрешния шпионин);

в) да се препятства достъпът на длъжностните лица и другите служители на ГСС, на държавните ведомства на държавите-членки и/или други институции или трети страни, за които няма необходимост да знаят, до класифицирана информация на ЕС;

МЕРКИ ЗА ФИЗИЧЕСКА СИГУРНОСТ

Зони за сигурност

5. Зоните, в които се обработва и съхранява информация с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или по-високо от това ниво, се организират и структурират по такъв начин, че да отговарят на изискванията, дадени в една от подточките по-долу:

а) Зона за сигурност от клас I: зона, в която информацията с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или по-високо от това ниво, се обработва и съхранява по такъв начин, че влизането в зоната представлява на практика достъп до класифицирана информация. За такава зона се изисква:

(i) въвеждане на точно определен защитен периметър, с контролиран режим на влизане и излизане;

(ii) система за контрол при влизане, която допуска само лицата, които са надлежно проучени за надеждност от гледна точка на сигурността и са получили специално разрешение за влизане в зоната;

(iii) спецификация на класификацията на информацията, която обикновено се намира в зоната, т.е. информацията, до която влизането в зоната осигурява достъп;

б) Зона за сигурност от клас II: зона, в която информацията с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или по-високо от това ниво, може да бъде защитена от достъпа на неупълномощени лица, чрез създадените вътрешни средства за контрол, например помещения, в които са разположени офисите, в които редовно се обработва и съхранява информация с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или по-високо от това ниво. За такава зона се изисква:

(i) въвеждане на точно определен защитен периметър, с контролиран режим на влизане и излизане;

(ii) система за контрол при влизане, която допуска без придружител само лицата, които са надлежно проучени за надеждност от гледна точка на сигурността и са получили специално разрешение за влизане в зоната. За всички други лица са предвидени мерки за осигуряване на придружаване или равностойни контролни средства, за да се предотврати нерегламентиран достъп до класифицираната информация на ЕС и неконтролирано влизане в зоните, които подлежат на проверки за техническа сигурност.

Зоните, в които няма дежурен персонал през цялото денонощие, се проверяват веднага след приключване на нормалното работно време с цел да се гарантира подходяща защита на класифицираната информация на ЕС.

Административна зона

6. Около и към зоните за сигурност от клас I и клас II могат да се създават административни зони, които са с по-ниско ниво на сигурност. Такива зони изискват определяне на добре видим периметър, в който е създадена възможност за проверка на персонала и превозните средства.

Средства за контрол при влизане и излизане

7. Влизането на постоянния персонал в зоните за сигурност от клас I и клас II се контролира чрез използването на пропуск или разпознаваща система. Създава се и система за проверка на посетителите с цел предотвратяване на нерегламентиран достъп до класифицираната информация на ЕС. Системата с използване на пропуски може да бъде придружена от автоматична идентификация, която се счита за допълнителна, но не може изцяло да замести необходимостта от охрана. Промяна в оценката на заплахите може да доведе до засилване на мерките за контрол при влизане и излизане, например при посещения на известни личности.

Охранително патрулиране

8. Патрулирането в зоните за сигурност от клас I и клас II се организира извън нормалното работно време с цел защита на активите на ЕС от фалшифициране, увреждане или погубване. Честотата на патрулиране зависи от конкретните обстоятелства, но се препоръчва да става на всеки два часа.

Сейфове и трезори

9. За съхраняването на класифицирана информация на ЕС се използват три вида сейфове:

- Клас А: сейфове, одобрени в рамките на държавата, за съхраняване на информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС в зоните за сигурност от клас I и клас II;
- Клас Б: сейфове, одобрени в рамките на държавата, за съхраняване на информация с ниво на класификация СЕКРЕТНО ЗА ЕС и ПОВЕРИТЕЛНО ЗА ЕС в зоните за сигурност от клас I и клас II;
- Клас В: офис оборудване, подходящо за съхраняване само на информация с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС.

10. За трезорите, изградени в зоните за сигурност от клас I и клас II, и за всички зони за сигурност от клас I, където информацията с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или по-високо от това ниво се съхранява върху открити рафтове или е изложена върху диаграми, карти и др., стените, подовете и таваните, вратата/вратите с брава/брави се сертифицират от ОНС с цел предоставяне на защита, равностойна на защитата на класа сейфове, одобрен за съхраняването на информация със същата класификация.

Брави

11. Бравите, използвани за сейфовете и трезорите, в които се съхранява класифицирана информация на ЕС , отговарят на следните стандарти:

- Група А: одобрени в рамките на държавата за сейфове от клас А;
- Група Б: одобрени в рамките на държавата за сейфове от клас Б;
- Група В: одобрени в рамките на държавата за сейфове от клас В;

Контрол на ключовете и комбинациите

12. Не могат да се изнасят извън сградата на службата ключове от сейфовете. Комбинациите за бравите на сейфовете се запаметяват от лицата, на които е необходимо да ги знаят. Съхраняват се от служителя по сигурността на заинтересованата институция резервни ключове и запис в писмена форма на всяка комбинация, за да бъдат използвани в случай на настъпване на извънредни обстоятелства; те се съхраняват в отделни запечатани непрозрачни пликове. Работните ключове, резервните ключове и комбинациите се съхраняват в отделни сейфове. За тези ключове и комбинации следва да се осигури защита с ниво на сигурност, което не е по-ниско от това на материала, до който осигуряват достъп.

13. Възможно най-малък брой хора се запознават с комбинациите за сейфовете. Комбинациите се променят:

а) при получаване на нов сейф;

б) в случай на промяна на персонала;

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

г) за предпочитане на всеки шест месеца, но не по-рядко от веднъж на 12 месеца.

Устройства за откриване на нарушители

14. Когато за защитата на класифицирана информация на ЕС се използват алармени системи, затворена телевизионна система и други електрически устройства, се осигурява достъп до аварийно захранване, за да се осигури непрекъсната работа на системата при прекъсване на електроснабдяването от мрежата. Друго основно изискване е повреда в такива системи или неумелото им

използване да води до задействане на сигнализатор за тревога или друга надеждна предупредителна сигнализация за персонала по контрола.

Одобрени устройства

15. В ОНС се поддържат, от техни собствени или от двустранни източници, актуализирани списъци на видовете и моделите защитни устройства, одобрени от тях за пряка или непряка защита на класифицираната информация при различни конкретно определени обстоятелства и условия. Службата за сигурност на ГСС поддържа подобен списък на базата и на информация от ОНС. Децентрализираните агенции на ЕС се консултират със службата за сигурност на ГСС, а в зависимост от случая и със ОНС на държавата-членка в която се намират, преди да закупят такива устройства.

Физическа защита на копирни и телефаксни машини

16. Копирните и телефаксните машини са защитени до степента, необходима за да се гарантира, че могат да бъдат използвани само от упълномощени лица, и всички класифицирани продукти са обект на подходящи средства за контрол.

ЗАЩИТА СРЕЩУ НЕБРЕЖНОСТ И ПОДСЛУШВАНЕ

Небрежност

17. През деня и през нощта се вземат всички необходими мерки, за да се гарантира, че класифицираната информация на ЕС няма да бъде видяна, дори случайно, от неупълномощено лице.

Подслушване

18. За службите или зоните, в които редовно се обсъжда информация с ниво на класификация СЕКРЕТНО ЗА ЕС или по-високо от това ниво, се осигурява защита срещу атаки на активно или пасивно подслушване в случаите, когато съществува такава опасност. За оценката на риска от такива атаки отговорност носи компетентният орган по сигурността след консултации, при необходимост, с ОНС.

19. За определяне на защитните мерки, които следва да се вземат в помещения, изложени на пасивно подслушване (например поставяне на изолация на стените, вратите, подовете и таваните, измерване на компрометиращото изтичане на информация) и на активно подслушване (например търсене на микрофони) службата за сигурност на ГСС може да поиска помощ от експерти на ОНС. Служителите по сигурността в децентрализираните агенции на ЕС могат да поискат да бъдат направени технически проверки от службата за сигурност на ГСС и/или помощ от експерти на ОНС.

20. Също така, когато обстоятелствата го изискват, може да се извърши проверка на телекомуникационните съоръжения и на всички видове електрическо и електронно офис оборудване, използвано по време на срещи с ниво на класификация СЕКРЕТНО ЗА ЕС или по-високо от това ниво, от специалисти на ОНС по техническата сигурност по молба на компетентния служител по сигурността.

ТЕХНИЧЕСКИ БЕЗОПАСНИ ЗОНИ

21. Някои зони могат да бъдат обозначени като технически безопасни зони. При влизане в тях се извършва специална проверка. Такива зони се държат заключени по одобрен начин, когато в тях не се работи, и всички ключове се третират като секретни ключове. Такива зони са обект на редовни физически проверки, които

също се правят и след всяко нерегламентирано влизане или подозрение за такова влизане.

22. Прави се подробна инвентаризация, за да се следи движението на оборудването и мебелите. В такава зона не могат да се внесат части от оборудването и мебелите без да са преминали през внимателна проверка, извършена от специално обучен персонал по сигурността, с цел да бъдат открити подслушвателни устройства, ако има такива. Общото правило е да се избягва монтирането на комуникационни линии в технически безопасните зони.

РАЗДЕЛ V

ОБЩИ ПРАВИЛА ОТНОСНО ПРИНЦИПА”НЕОБХОДИМОСТ ДА СЕ ЗНАЕ” И ПРОУЧВАНЕТО ЗА НАДЕЖДНОСТ ОТ ГЛЕДНА ТОЧКА НА СИГУРНОСТТА

1. Достъп до класифицирана информация се предоставя само на лица, чиито служебни задължения или конкретно възложена задача налагат „необходимост да се знае”. Достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, СЕКРЕТНО ЗА ЕС или ПОВЕРИТЕЛНО ЗА ЕС се предоставя само на лица, които притежават съответстващо проучване за надеждност от гледна точка на сигурността.

2. Определянето на „необходимостта да се знае” е отговорност на ГСС, децентрализираните агенции на ЕС и на службата или ведомството на държавата-членка, в която ще бъде назначено лицето, в съответствие с изискванията на задачата.

3. Проучването на персонала за надеждност от гледна точка на сигурността е отговорност на работодателя и се извършва на основата на приложимите в тази област процедури. Процедурата по проучването за надеждност от гледна точка на сигурността на висшите длъжностни лица и другите служители на ГСС е предвидена в раздел VI.

В резултат на процедурата се издава удостоверение за сигурност, което показва нивото на класифицираната информация, до която проученото за надеждност лице може да има достъп, и срока на изтичане на удостоверението.

Удостоверението за сигурност, издадено за информация с определено ниво на класификация, може да осигури на притежателя на удостоверението и достъп до информация с по-ниско ниво на класификация.

4. Лица, които не са висши длъжностни лица или други служители на ГСС или на държавите-членки, например членове, висши длъжностни лица или служители на институции на ЕС, с които може да се наложи да се обсъжда или на които може да се наложи да се показва класифицирана информация на ЕС, трябва да имат проучване за надеждност от гледна точка на сигурността по отношение на класифицираната информация на ЕС и да са запознати с отговорностите, които имат по отношение на сигурността. Същото правило се прилага, при сходни обстоятелства, за външните контрагенти, експерти или консултанти.

СПЕЦИАЛНИ ПРАВИЛА ЗА ДОСТЪП ДО ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ СТРОГО СЕКРЕТНО ЗА ЕС

5. Всички лица, които следва да имат достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, най-напред се проучват за надеждност за достъп до такава информация.

6. Всички лица, на които се налага да имат достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, се определят от ръководителя на съответното ведомство и имената им се вписват в съответната регистратура за информацията с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС.

7. Преди да получат достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС всички лица подписват удостоверение в уверение на това, че са запознати с процедурите по сигурността на Съвета и напълно разбират специалната отговорност, която носят за безопасното съхраняване на информацията с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС и

последствията, предвидени от правилата на ЕС и националното законодателство или административните правила в случай на преминаване на класифицирана информация в ръцете на неупълномощени лица в резултат на умишлено действие или небрежност.

8. Когато достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС имат лица по време на срещи и др., компетентният служител по контрола на службите или органите, в които са наети лицата, уведомяват органа, който организира срещата, че конкретното лице има такова разрешение.

9. Имената на всички лица, които са престанали да изпълняват конкретно възложени задачи, изискващи достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, се изваждат от списъка на лицата с достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС. Освен това, вниманието на тези лица се насочва отново към специалните им задължения за безопасно съхраняване на информацията с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС. Те подписват и декларация в уверение на това, че няма да използват или предават информацията с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, която се намира в тяхно владение.

СПЕЦИАЛНИ ПРАВИЛА ЗА ДОСТЪП ДО ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ СЕКРЕТНО ЗА ЕС И ПОВЕРИТЕЛНО ЗА ЕС

10. Всички лица, които следва да имат достъп до информация с ниво на класификация СЕКРЕТНО ЗА ЕС И ПОВЕРИТЕЛНО ЗА ЕС, най-напред се проучват за надеждност за достъп до информация със съответното ниво на класификация.

11. Всички лица, които следва да имат достъп до информация с ниво на класификация СЕКРЕТНО ЗА ЕС И ПОВЕРИТЕЛНО ЗА ЕС се запознават със съответните разпоредби относно сигурността и последствията в случай на проявена небрежност.

12. Когато достъп до информация с ниво на класификация СЕКРЕТНО ЗА ЕС И ПОВЕРИТЕЛНО ЗА ЕС имат лица по време на срещи и др., компетентният служител по контрола на службите или органите, в които са наети лицата, уведомяват органа, който организира срещата, че конкретното лице има такова разрешение.

СПЕЦИАЛНИ ПРАВИЛА ЗА ДОСТЪП ДО ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС

13. Лицата с достъп до информация с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС се запознават с настоящите разпоредби относно сигурността и последствията в случай на проявена небрежност.

ПРЕХВЪРЛЯНЕ

14. Когато член на персонала е преместен от пост, който включва обработката на класифициран материал на ЕС, Регистратурата упражнява надзор над прехвърлянето на материала от висшия чиновник, което напуска поста, на висшия чиновник, което поема поста.

СПЕЦИАЛНИ УКАЗАНИЯ

15. Лицата, на които се налага да обработват класифицирана информация на ЕС, най-напред в началото на изпълнението на задълженията си, а след това периодично се запознават с:

а) опасностите за сигурността в следствие на непредпазливост при разговори;

б) предпазните мерки, които следва да вземат при връзки с пресата;

в) заплахата, създадена от дейността на разузнавателните служби, чиито обект са ЕС и държавите-членки, с оглед на класифицираната информация и дейност на ЕС;

г) задължението да докладват незабавно на съответните органи по сигурността за всеки опит за сближаване или маневри, пораждащи подозрения за шпионска дейност, и за всички необичайни обстоятелства, свързани със сигурността.

16. Всички лица, които обикновено са изложени на чести контакти с представители на страни, чиито разузнавателни служби имат за обект ЕС и държавите-членки, с оглед на класифицираната информация и дейност на ЕС, се запознават със способите, за които е известно, че се използват от различните разузнавателни служби.

17. Не съществуват разпоредби на Съвета относно сигурността, които да се отнасят за частните пътувания с различна цел, извършвани от персонала с разрешение за достъп до класифицирана информация на ЕС. Но компетентните органи по сигурността запознават висшите длъжностни лица и другите служители, които попадат под тяхна отговорност, с правилата при пътуване, под чието действие могат да попаднат. Задължение на служителите по сигурността е да организират срещи за консултиране на членовете на персонала по тези специални указания.

РАЗДЕЛ VI

ПРОЦЕДУРА ЗА ПРОУЧВАНЕ НА ВИСШИ ДЛЪЖНОСТНИ ЛИЦА И ДРУГИ СЛУЖИТЕЛИ НА ГСС ЗА НАДЕЖДНОСТ ОТ ГЛЕДНА ТОЧКА НА СИГУРНОСТТА

1. Само висши длъжностни лица и други служители на ГСС или лица, работещи в рамките на ГСС, които поради поста, който заемат и служебните изисквания имат необходимост да знаят или да използват класифицирана информация, държана от Съвета, получават достъп до такава информация.

2. За да получат достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, СЕКРЕТНО ЗА ЕС и ПОВЕРИТЕЛНО ЗА ЕС, лицата по параграф 1 трябва да са получили разрешение в съответствие с процедурата, предвидена в параграфи 4 и 5.

3. Разрешение се издава само на лица, преминали през проучване за надеждност от гледна точка на сигурността, извършено от компетентните национални органи на държавите-членки (ОНС) в съответствие с процедурата, предвидена в параграфи 6 до 10.

4. Органът, назначил лицето, по смисъла на член 2, първа алинея на Правилника за персонала, е отговорен за издаването на разрешенията, предвидени в параграфи 1, 2 и 3.

Органът, назначил лицето, издава разрешение след като получи становището на компетентните национални органи на държавите-членки, изготвено на основата на проучването за надеждност от гледна точка на сигурността, извършено в съответствие с параграфи 6 до 12.

5. Разрешение, което е със срок на валидност пет години, не може да превишава срока на задачата, въз основа на която е било издадено. То може да се поднови от органа, назначил лицето, в съответствие с процедурата, предвидена в параграф 4.

Разрешението се отменя от органа, назначил лицето, когато той счете, че има законни основания за това. За всяко решение за отмяна на разрешение се уведомява заинтересованото лице, което може да поиска да бъде изслушано от органа, назначил лицето, и компетентния национален орган.

6. Целта на проучването за надеждност от гледна точка на сигурността е да се установи, че не са налице възражения срещу това да се разреши на лицето достъп до класифицирана информация, държана от Съвета.

7. Проучването за надеждност от гледна точка на сигурността се извършва със съдействието на заинтересованото лице и по молба на органа, назначил лицето, от компетентните национални органи на държавата-членка, на която лицето, обект на разрешението, е гражданин. Когато заинтересованото лице пребивава на територията на друга държава-членка, заинтересованите национални органи могат да получат съдействие от органите в държавата на местопребиваване на лицето.

8. Като част от процедурата по проучването за надеждност от гледна точка на сигурността, от заинтересованото лице се изисква да попълни личен формуляр с биографични данни.

9. Органът, назначил лицето, уточнява в молбата си вида и нивото на класифицираната информация, до която заинтересованото лице следва да има достъп, за да могат компетентните национални органи да извършат проучването и

да дадат становището си в съответствие с нивото на разрешението, което би било най-подходящо да се предостави на лицето.

10. Целият процес на проучване за надеждност от гледна точка на сигурността и получените от него резултати са в съответствие с действащите правила и разпоредби в тази област в заинтересованата държава-членка, включително и тези за обжалване.

11. Когато становището, дадено от компетентните национални органи на държавата-членка, е положително, органът, назначил лицето, може да издаде разрешение на заинтересованото лице.

12. Когато становището, дадено от компетентните национални органи, е отрицателно, се уведомява заинтересованото лице, което може да поиска да бъде изслушано от органа, назначил лицето. Ако счете за необходимо, органът, назначил лицето, може да поиска от компетентните национални органи да предоставят при възможност допълнителни обяснения. При потвърждаване на отрицателното становище не се издава разрешение.

13. Всички лица, на които е издадено разрешение по смисъла на параграфи 4 и 5, получават, в момента на издаване на разрешението и през еднакви периоди от време след това, всички необходими указания относно защитата на класифицираната информация и средствата за осигуряване на такава защита. Тези лица подписват декларация, с която потвърждават получаването на указанията, и поемат задължението да ги спазват.

14. Органът, назначил лицето, взема всички необходими мерки, за да изпълни изискванията на настоящия раздел, и по-специално тези по отношение на правилата, които определят достъпа до списъка на лицата, получили разрешение.

15. Като изключение, във връзка с изпълнението на служебни задължения, органът, назначил лицето, може, след като уведоми компетентните национални органи и при условие, че не е получил отговор от тях в срок от един месец, да издаде временно разрешение за срок до шест месеца до получаване на резултата от проучването, предвидено в параграф 7.

16. Временните и за определен срок разрешения, издадени по този начин, не разрешават достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС; такъв достъп е ограничен само до висшите длъжностни лица, които успешно са преминали проучване за надеждност от гледна точка на сигурността в съответствие с параграф 7. До получаването на резултата от проучването, висшите длъжностни лица, подали молба за проучване за надеждност от гледна точка на сигурността за обработка на информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, могат да получат временно разрешение с определен срок за достъп до информация с нива на класификация до и включително СЕКРЕТНО ЗА ЕС.

РАЗДЕЛ VII

СЪЗДАВАНЕ, ПРЕДОСТАВЯНЕ, ПРЕДАВАНЕ, СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА КЛАСИФИЦИРАНИ МАТЕРИАЛИ НА ЕС

Съдържание

ОБЩИ РАЗПОРЕДБИ

В настоящия раздел са разгледани подробно мерките за създаване, предоставяне, предаване, съхраняване и унищожаване на класифицирани документи на ЕС по смисъла на параграф 3, буква а) от „Основни принципи и минимални стандарти за сигурност” в част 1 от настоящото приложение. Настоящият раздел се използва като изходен материал за адаптирането на тези мерки за други класифицирани материали в зависимост от вида на материала и от конкретния случай.

Глава I

Създаване и предоставяне на класифицирани документи на ЕС

СЪЗДАВАНЕ

1. Поставят се класификации и маркировки по реда и условията на раздел II горе и долу в средата на всяка страница като всяка страница се номерира. Върху всеки документ с ниво на класификация за ЕС се поставя уникалният регистрационен номер на документа и датата. Върху документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС и СЕКРЕТНО ЗА ЕС този номер се поставя върху всяка страница. Когато документи се предоставят в няколко копия, за всяко копие се определя номер, който се поставя на първата страница заедно с общия брой на страниците. Всички приложения към документ с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или по-високо от това ниво, се изброяват на първата страница.

2. Документите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или по-високо от това ниво се печатат, превеждат, фотокопират, възпроизвеждат на магнитен носител или микрофилм само от лица, получили разрешение за достъп до класифицирана информация на ЕС с ниво на класификация не по-малко от съответното ниво на въпросния документ, с изключение на специалните случаи по параграф 27 на този раздел.

Разпоредбите, които регламентират създаването на класифицирани документи по електронен път, са разгледани в раздел XI.

ПРЕДОСТАВЯНЕ

3. Класифицирана информация на ЕС се предоставя само на лицата, които имат необходимост да знаят и са преминали през съответстващо проучване за надеждност от гледна точка на сигурността. Първоначалното предоставяне на информацията се определя от създателя на информацията.

4. Движението на документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС се извършва чрез регистратурите за информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС (виж раздел VIII). Когато става въпрос за съобщения с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, компетентната регистратура може да упълномощи ръководителя на комуникационния център да произведе копията, чиито брой е определен в списъка на адресатите.

5. Документите с ниво на класификация СЕКРЕТНО ЗА ЕС или по-ниско от това ниво могат да бъдат преразпределени от първоначалния адресат на други адресати при спазване на принципа „необходимост да се знае” като органите, създали документа, посочват ясно дали желаят да се постави предупредителна маркировка. В случаите, когато е поставена такава предупредителна маркировка, адресатите могат да предоставят документите на други адресати само с разрешението на органите, създали документа.

6. Всеки документ с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или по-високо от това ниво при влизане или излизане от институцията се завежда в нейната регистратура. Данните, които се завеждат (уникален регистрационен номер, дата, а при необходимост, и номер на копието), са данните, чрез които документът може да бъде идентифициран; те се записват в дневник или на специално защитен електронен носител.

Глава II

Предаване на класифицирани документи на ЕС

ОПАКОВАНЕ

7. Предаването на документите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или по-високо от това ниво става в здрави, непрозрачни, поставени един в друг пликове. Вътрешният плик се обозначава с маркировката за съответното ниво на класификация на ЕС, а при възможност, се изписват и пълните данни за поста, заеман от получателя, и неговият адрес.

8. Само служителят по контрола в регистратурата, или неговият заместник, могат да отворят вътрешния плик и да потвърдят получаването на приложените документи, освен в случаите, когато пликът е адресиран до конкретно лице. В такива случаи в дневника на съответната регистратура се записва получаването на плика, но само лицето, до което е адресиран плика, може да отвори вътрешния плик и да потвърди получаването на документите, които се съдържат в него.

9. Във вътрешния плик се поставя разписка за получаване. Разписката, която не е класифицирана, следва да съдържа уникалния идентификационен номер на документа, датата и номера на копието на документа, но не и предмета на документа.

10. Вътрешният плик се поставя във външен плик, върху който е отбелязан номерът на пакета, записан в разписката. При никакви обстоятелства класификацията от гледна точка на сигурността не може да бъде обозначена върху външния плик.

11. За документите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и по-високо от това ниво куриерите получават разписки, в които е отбелязан номера на пакета.

ПРЕДАВАНЕ В РАМКИТЕ НА ОТДЕЛНА СГРАДА ИЛИ ГРУПА СГРАДИ

12. В рамките на отделна сграда или група от сгради класифицираните документи могат да се пренасят в запечатан плик, върху който е написано само името на адресата при условие, че пликът са пренася от лице, получило разрешение за достъп, съответстващо на нивото на класификация на документите.

ПРЕДАВАНЕ НА ДОКУМЕНТИ НА ЕС В РАМКИТЕ НА ОТДЕЛНА ДЪРЖАВА

13. В рамките на отделна държава класифицираните документи се пренасят само чрез специална куриерска служба или от лица, получили разрешение за достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС.

14. Когато за пренасянето на документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС извън пределите на отделна сграда или група сгради се

използва куриерска служба, се спазват разпоредбите относно опаковането и получаването, определени в настоящата глава. Персоналът в службите за доставяне на документи е така комплектован, че е осигурен пряк надзор на пакетите, съдържащи документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, от страна на отговорен служител през цялото време.

15. По изключение документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС могат да се изнасят извън пределите на отделна сграда или група сгради от висши длъжностни лица, които не са куриери, за да бъдат използвани по време на срещи и обсъждания при условие, че:

а) приносителят е получил разрешение за достъп до документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС;

б) начинът на транспортиране е в съответствие с националните правила за предаване на документи с национално ниво на класификация СТРОГО СЕКРЕТНО.

в) при никакви обстоятелства документи с ниво на класификация СТРОГО СЕКРЕТНО не са оставени без надзор от упоменатия висш чиновник;

г) са взети мерки списъкът на документите, пренасяни по този начин, да се съхрани в регистратурата за документи с ниво на класификация СТРОГО СЕКРЕТНО, документите да се запишат в дневник и да се сравнят с данните в дневника при връщането им.

16. В рамките на страната документите с ниво на класификация СЕКРЕТНО ЗА ЕС и ПОВЕРИТЕЛНО ЗА ЕС могат да се изпращат по пощата, ако такъв вид предаване е предвидено в националните подзаконови актове и е в съответствие с техните разпоредби, или по куриерска служба или по лица, получили разрешение за достъп до класифицирана информация на ЕС.

17. Всяка държава-членка, или децентрализирана агенция на ЕС, изготвя указания за лично пренасяне на класифицирани документи на ЕС на основата на настоящите разпоредби. От приносителя следва да се изисква да прочете и подпише тези указания. Указанията следва ясно да показват, че при никакви обстоятелства документите не могат по-специално да:

а) напускат приносителя, освен когато се съхраняват надлежно в сейф в съответствие с разпоредбите в раздел IV;

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

в) се четат на обществени места като например самолети и влакове.

ПРЕДАВАНЕ ОТ ЕДНА НА ДРУГА ДЪРЖАВА ЧЛЕНКА

18. Материалите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и по-високо от това ниво се пренасят от една държава-членка в друга с дипломатическа или военна куриерска служба.

19. Разрешава се, обаче, лично пренасяне на материал с ниво на класификация СЕКРЕТНО ЗА ЕС и ПОВЕРИТЕЛНО ЗА ЕС ако са налице мерки по време на пренасянето, които гарантират, че той няма да попадне в ръцете на неупълномощено лице.

20. ОНС могат да разрешат лично пренасяне на материал, когато не са налице дипломатически или военни куриери или използването им би забавило предаването и би навредило на дейността на ЕС, когато лицето, за което е предназначен материалът, спешно се нуждае от него. Всяка държава-членка изготвя указания за лично пренасяне на материалите с ниво на класификация до и включително СЕКРЕТНО ЗА ЕС извън страната от лица, които не са дипломатически или военни куриери. Указанията следва да изискват:

а) приносителят да притежава съответстващо проучване за надеждност от гледна точка на сигурността, издадено от държавите-членки;

б) да се води запис на всички материали, пренасяни по този начин, в съответната служба или регистратура;

в) пакетите или торбите, съдържащи материали на ЕС, да имат официален печат, за да се предотврати или да се попречи да се извърши митническа проверка, и етикет с идентификационни данни и указания за лицето, намерило материала;

г) приносителят да носи у себе си удостоверение за куриер и/или заповед за изпълнение на задачата, признати от всички държави-членки на ЕС, с което лицето се упълномощава да пренесе пакета, посочен в документа;

д) да не се пресича държава, която не е членка на ЕС, или нейна граница при пътуване по сушата, освен ако тази държава не е предоставила специални гаранции на държавата - изпращач;

е) договореностите по пътуването на приносителя относно местоназначения, маршрутите до тях и транспортните средства, които ще се използват, да отговарят на изискванията на Разпоредбите на ЕС или - когато националните разпоредби относно тези въпроси са по-строги - да отговарят на тези разпоредби;

ж) материалите да не напускат приносителя,освен когато се съхраняват надлежно в сейф в съответствие с разпоредбите на раздел IV;

з) материалите да не се оставят без надзор в обществения транспорт или в частни превозни средства, или на такива места като ресторанти и хотели. Те не могат да се съхраняват в хотелски сейфове и да бъдат оставени 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.).

Лицата, определени за пренасяне на класифициран материал, са длъжни да прочетат и подпишат информация, свързана със сигурността, която съдържа най-малко указанията, изброени по-горе, и процедурите, които трябва да се спазват при извънредни обстоятелства или в случай, че преминаването без проверка на пакета, съдържащ класифициран материал, се оспорва от митническите служители или летищните служители по сигурността.

ПРЕДАВАНЕ НА ДОКУМЕНТИ С НИВО НА КЛАСИФИКАЦИЯ „ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС”

21. Не са предвидени други разпоредби за пренасянето на документи с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС освен тези, гарантиращи, че те няма да попаднат в ръцете на неупълномощено лице.

СИГУРНОСТ НА КУРИЕРИТЕ

22. Всички куриери, които участват в пренасянето на документи с ниво на класификация СЕКРЕТНО ЗА ЕС и ПОВЕРИТЕЛНО ЗА ЕС, преминават през съответстващо проучване за надеждност от гледна точка на сигурността.

Глава III

Електрически и други технически средства за предаване на информация

23. Предназначението на мерките за комуникационна сигурност е да осигурят безопасно предаване на класифицираната информация на ЕС. Подробните правила, които се отнасят за предаване на класифицираната информация на ЕС, са разгледани в раздел XI.

24. Само акредитираните комуникационни центрове и мрежи и/или терминали и системи могат да предават информация с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и СЕКРЕТНО ЗА ЕС.

Глава IV

Допълнителни копия, преводи на класифицирани документи на ЕС и извлечения от тях

25. Само създателят на документа може да разреши копиране или превод на документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС.

26. Ако от лица, които нямат проучване за надеждност от гледна точка на сигурността за ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, е поискана информация, която въпреки че се съдържа в документ с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС няма същото ниво на класификация, може да се разреши на ръководителя на регистратурата за информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС да направи необходимия брой извлечения от такъв документ. Но той междувременно взема необходимите мерки да се даде съответстващо ниво на класификация на извлеченията.

27. Документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС и по-ниско от това ниво могат да бъдат възпроизвеждани и превеждани от адресата в рамките на разпоредбите за национална сигурност и при условие, че той спазва стриктно принципа „необходимост да се знае”. Мерките за сигурност, които се отнасят за оригиналния документ, се отнасят също и при неговото възпроизвеждане и/или превод.

Глава V

Инвентаризации и проверки, съхраняване и унищожаване на класифицирани документи на ЕС

ИНВЕНТАРИЗАЦИИ И ПРОВЕРКИ

28. Ежегодно всяка регистратура за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, упомената в раздел VIII, извършва инвентаризация по списък на документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС в съответствие с разпоредбите на раздел VIII, параграфи от 9 до 11. Класифицираните документи на ЕС под ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС се подлагат на вътрешни проверки в съответствие с националните указания, а в ГСС и децентрализираните агенции на ЕС - в съответствие с указанията на генералния секретар/върховния представител.

Тези операции дават възможност да се осъществят вижданията на упоменатите институции относно:

а) възможността за понижаване или премахване на класификацията за някои документи;

б) унищожаването на документи.

СЪХРАНЯВАНЕ В АРХИВ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

29. За да се минимизират проблемите, свързани със съхраняването на информацията, на служителите по контрола във всички регистратури е разрешено да съхраняват документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, СЕКРЕТНО ЗА ЕС и ПОВЕРИТЕЛНО ЗА ЕС на микрофилми или на магнитни или оптични носители при създаването на архив при условие, че:

а) процесът на микрофилмиране/съхраняване се извършва от персонал, който има разрешение за достъп до съответното ниво на класификация на информацията;

б) за микрофилма/носителя се осигурява същата защита като тази за оригиналните документи;

в) микрофилмирането/съхраняването на документ с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС се докладва на създателя на документа;

г) филмовите ленти или други носители съдържат само документи с едно и също ниво на класификация - СТРОГО СЕКРЕТНО ЗА ЕС, СЕКРЕТНО ЗА ЕС или ПОВЕРИТЕЛНО ЗА ЕС;

д) микрофилмирането/съхраняването на документ с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС или СЕКРЕТНО ЗА ЕС е посочено ясно в записа, използван за годишната инвентаризация;

е) оригиналните документи, които са били микрофилмирани или съхранени по друг начин, се унищожат в съответствие с разпоредбите на параграфи 31 до 36;

30. Тези правила се отнасят и за всички други форми на съхраняване, разрешени от ОНС, като например електромагнитни носители и оптични дискове.

РУТИННО УНИЩОЖАВАНЕ НА КЛАСИФИЦИРАНИ ДОКУМЕНТИ НА ЕС

31. За да не се допусне ненужно натрупване на класифицирани документи на ЕС, тези документи, които ръководителят на институцията, в която се намират, счита за остарели или в ненужно голям брой, се унищожават при първа възможност по следния начин:

а) документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС се унищожават само от Централната регистратура, която отговаря за тях. Всеки унищожен документ се вписва в удостоверение за унищожаването на документа, което се подписва от служителя по контрола на документацията с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС и от служител, присъствал на унищожаването, който има разрешение за достъп до информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС. Извършеното унищожаване се вписва в дневника;

б) регистратурата съхранява удостоверенията за унищожените документи, заедно с формулярите за предоставените документи, за срок от десет години.

Предоставянето на копия на документа на неговия създател или на съответната централна регистратура става само по тяхна изрична молба;

в) документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, включително и всички класифицирани отпадъци в резултат на изготвянето на документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС като например повредени копия, работни проекти, напечатани записки и индигови листове, се унищожават под надзора на служителя по контрола на документацията с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС чрез изгаряне, претопяване, нарязване на ивици или по друг начин, който ги превръща в негодни за разпознаване или възстановяване.

32. Документите с ниво на класификация СЕКРЕТНО ЗА ЕС се унищожават само от регистратурата, която отговаря за тях, под надзора на лице, което има разрешение за достъп до информацията, чрез един от начините, посочени в параграф 31, буква в). Унищоженият документ с ниво на класификация СЕКРЕТНО ЗА ЕС се вписва в удостоверение за унищожаването на документа, което се подписва и се съхранява от регистратурата, заедно с формуляра за предоставените документи, за срок не по-малък от три години.

33. Документите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС се унищожават от регистратурата, която отговаря за тях, под надзора на лице, което има разрешение за достъп до информацията, чрез един от начините, посочени в параграф 31, буква в). Унищожаването им се записва в съответствие с националните разпоредби, а когато става въпрос за ГСС или децентрализираните агенции на ЕС, в съответствие с указанията на генералния секретар/върховния представител.

34. Документите с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС се унищожават от регистратурата, която отговаря за тях или от потребителя в съответствие с националните разпоредби, а когато става въпрос за ГСС или децентрализираните агенции на ЕС, в съответствие с указанията на генералния секретар/върховния представител.

УНИЩОЖАВАНЕ ПРИ НАСТЪПВАНЕ НА ИЗВЪНРЕДНИ ОБСТОЯТЕЛСТВА

35. ГСС, държавите-членки и децентрализираните агенции на ЕС изготвят планове, съобразени с местните условия, за безопасно съхраняване на класифицираните материали на ЕС по време на криза, включително, при необходимост, и планове за унищожаване на материалите при настъпване на извънредни обстоятелства и за евакуация; те оповестяват, в рамките на собствените си организации, указанията, които считат за необходими, за да се предотврати попадането на класифицирана информация на ЕС в ръцете на неупълномощени лица.

36. Мерките за безопасно съхраняване и/или унищожаване на материали с ниво на класификация СЕКРЕТНО ЗА ЕС и ПОВЕРИТЕЛНО ЗА ЕС по време на криза не следва при никакви обстоятелства да се отразят неблагоприятно на безопасното съхраняване или унищожаването на материали с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, включително и на устройствата за кодиране, чието безопасно съхраняване или унищожаване има предимство пред всички останали задачи. Мерките, които следва да се приемат за безопасно съхраняване или унищожаване на устройствата за кодиране при настъпване на извънредни обстоятелства, се разглеждат в специални указания.

Глава VI

Специални правила, приложими за документи, които са предназначени за Съвета

37. В рамките на ГСС наблюдението на информацията с ниво на класификация СЕКРЕТНО ЗА ЕС или ПОВЕРИТЕЛНО ЗА ЕС, която се съдържа в документи, предназначени за Съвета, се извършва от службата за класифицирана информация.

Под ръководството на генералния директор, отговарящ за персонала и администрацията, тя:

а) ръководи дейностите, свързани с регистрацията, възпроизвеждането, превода, предаването, изпращането и унищожаването на тази информация;

б) актуализира списъка с данните по състоянието на класифицираната информация;

в) поставя периодично въпроса за необходимостта от промяна на класификацията на информацията;

г) определя, в сътрудничество със службата по сигурността, практическите мерки за класифициране и премахване на класификацията на информацията.

38. Службата за класифицирана информация поддържа регистър със следните данни:

а) дата на изготвяне на класифицираната информация;

б) ниво на класификацията;

в) краен срок на класификацията;

г) име и отдел на създателя на информацията;

д) получател или получатели, със серийния номер;

е) предмет;

ж) номер;

з) брой на тиражираните копия;

и) изготвяне на опис на класифицираната информация, предоставена на Съвета;

(й) регистър на класифицираната информация с премахната класификацията или с понижено ниво на класификация.

39. Общите правила, предвидени в главите от I до V на настоящия раздел, се отнасят за службата за класифицирана информация на ГСС, ако не са променени от специалните правила, предвидени в настоящата глава.

РАЗДЕЛ VIII

РЕГИСТРАТУРИ ЗА ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ „СТРОГО СЕКРЕТНО ЗА ЕС”

1. Регистратурите за информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС се създават с цел да се осигури отчитане, обработка и предоставяне на документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС в съответствие с разпоредбите относно сигурността. Ръководител на регистратурата за информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, съответно за всяка държава-членка, в ГСС, а при необходимост, и в децентрализираните агенции на ЕС, е служителят по сигурността на информацията с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС.

2. Централните регистратури изпълняват функциите на главен орган по получаването и изпращането на информация в държавите-членки, ГСС и децентрализираните агенции на ЕС, в които са създадени такива регистратури, а при необходимост, и в други институции на ЕС, международни организации и трети страни, с които Съветът има споразумения за процедурите по сигурността при обмен на класифицирана информация.

3. При необходимост се създават под-регистратури, които отговарят за вътрешното управление на документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС; те поддържат актуализирани записи за движението на всеки документ, който се води на отчет в под-регистратурата.

4. Под-регистратурите за документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС се създават в съответствие с разпоредбите на раздел I в отговор на дългосрочна необходимост и са прикрепени към централна регистратура за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС. Когато е налице временна или нередовна необходимост за консултиране с документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, те могат да се предоставят без да се създава под-регистратура за документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС при условие, че са създадени правила, които да гарантират, че те продължават да бъдат под надзора на съответната регистратура за документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС и се съблюдават всички мерки за физическа сигурност и сигурност на персонала.

5. Под-регистратурите не могат да предават документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС директно на други под-регистратури на една и съща централна регистратура за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС без изричното одобрение на последната.

6. Обменът на документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС между под-регистратурите минава през централните регистратури за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС.

ЦЕНТРАЛНИ РЕГИСТРАТУРИ ЗА ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ „СТРОГО СЕКРЕТНО ЗА ЕС”

7. Като служител по контрола, ръководителят на централна регистратура за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС е отговорен за:

а) предаването на документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС в съответствие с разпоредбите на раздел VII;

б) поддържането на списък на всички подчинени на него под-регистратури за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС заедно с имената и подписите на назначените служители по контрола и упълномощените от тях представители;

в) съхраняването на разписките от регистратурите за всички документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, предоставени от централната регистратура;

г) поддържането на документация за всички съхранявани и предоставяни документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС;

д) поддържането на актуализиран списък на всички централни регистратури за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, с които обикновено си кореспондира, заедно с имената и подписите на назначените служители по контрола и упълномощените от тях представители;

е) физическото съхранение на всички документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, съхранявани в регистратурата в съответствие с разпоредбите на раздел IV.

ПОД-РЕГИСТРАТУРИ ЗА ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ „СТРОГО СЕКРЕТНО ЗА ЕС”

8. Като служител по контрола, ръководителят на под-регистратура за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС е отговорен за:

а) предаването на документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС в съответствие с разпоредбите на раздел VII и параграфи 5 и 6 на раздел VIII;

б) поддържането на списък на всички лица, получили разрешение за достъп до информацията с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС под негов контрол;

в) предоставянето на документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС в съответствие с указанията на създателя на документа или при съблюдаване на принципа”необходимост да се знае” като най-напред провери дали на адресата е направено необходимото проучване за надеждност от гледна точка на сигурността;

г) поддържането на актуализирана документация за всички документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, съхранявани и предоставяни под негов контрол или предадени на други регистратури за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, и съхраняването на всички разписки;

д) поддържане на актуализиран списък на всички централни регистратури за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, с които му е разрешено да обменя документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, заедно с имената и подписите на техните служители по контрола и упълномощените от тях представители;

е) физическото съхранение на всички документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, съхранявани в под-регистратурата в съответствие с разпоредбите на раздел IV.

ИНВЕНТАРИЗАЦИЯ

9. На всеки дванадесет месеца всяка регистратура за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС извършва инвентаризация по опис на всички документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, за които води отчет. Документът се счита за воден на отчет, когато физически е включен в инвентарния опис на регистратурата или за него се съхранява разписка, издадена от регистратурата за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, на която е бил прехвърлен документът, удостоверение за унищожаване на документа или указание за понижаване на нивото на класификация или премахване на класификацията на документа.

10. Под-регистратурите изпращат констатациите от годишната си инвентаризация на централната регистратура, на която са подчинени, в срок, определен от последната.

11. ОНС както и тези институции на ЕС, международни организации и децентрализирани агенции на ЕС, в които е създадена централна регистратура за документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, изпращат констатациите от годишната инвентаризация, извършена в централните регистратури за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, на генералния секретар/върховния представител в срок до 1 април всяка година.

РАЗДЕЛ IX

МЕРКИ ЗА СИГУРНОСТ, КОИТО СЕ ПРИЛАГАТ ПО ВРЕМЕ НА СПЕЦИАЛНИ СРЕЩИ, ПРОВЕЖДАНИ ИЗВЪН ПОМЕЩЕНИЯТА НА СЪВЕТА ПО ВЪПРОСИ С ВИСОКА ЧУВСТВИТЕЛНОСТ

ОБЩИ РАЗПОРЕДБИ

1. Когато се провеждат срещи на Европейския съвет, на Съвета, на министрите или други важни срещи извън помещенията на Съвета в Брюксел и Люксембург и когато е оправдано от конкретните изисквания по сигурността, свързани с високата чувствителност на въпросите или информацията, която се разглежда, се прилагат мерките за сигурност, разгледани по-долу. Те засягат единствено защитата на класифицираната информация на ЕС; възможно е да се наложи планирането и на други мерки за сигурност.

ОТГОВОРНОСТИ

Държавата-членка - домакин

2. Държавата-членка, на чиято територия се провежда срещата (държавата-членка - домакин) следва да отговаря, съвместно със службата за сигурност на ГСС, за сигурността на срещите на Европейския съвет, на Съвета, на министрите или други важни срещи и за физическата сигурност на основните участници и техните служители.

Защитата на сигурността следва да осигури по-специално:

а) изготвянето на планове за борба със заплахите за сигурността и инцидентите, свързани със сигурността като въпросните мерки обхващат по-специално безопасното съхраняване на класифицирани документи на ЕС в службите;

б) използването на мерки, които създават възможност за достъп до комуникационните системи на Съвета с цел получаване и предаване на класифицирани съобщения на ЕС. държавата-членка - домакин осигурява при необходимост и достъп до защитени телефонни системи.

Държавите-членки

3. Органите на държавите-членки предприемат необходимите действия, за да осигурят:

а) сертифициране на националните си представители за съответното ниво на проучване за надеждност от гледна точка на сигурността чрез кодирано съобщение или факс, изпратени директно на служителя по сигурността на срещата или чрез службата за сигурност на ГСС;

б) всяка конкретна заплаха да бъде доведена до знанието на органите в държавата-членка - домакин, а при необходимост, и до знанието на службата за сигурност на ГСС, за да бъдат предприети съответстващи действия.

Служител по сигурността на срещите

4. Назначава се служител по сигурността, който отговаря за общата подготовка и контрола върху общите мерки за вътрешна сигурност и за координацията с

другите заинтересовани органи по сигурността. Мерките, които той предприема, най-общо се отнасят до:

а) (i) защитни мерки на мястото на срещата, за да се гарантира, че срещата ще протече без инциденти, които биха компрометирали сигурността на класифицираната информация на ЕС, която може да бъде използвана там;

(ii) проверка на персонала, на който е разрешен достъп до мястото на срещата, зоните на делегациите и конферентната зала, и проверка на съоръженията;

(iii) непрекъсната координация с компетентните органи на държавата-членка - домакин и със службата за сигурност на ГСС;

б) включване на инструкциите по сигурността в досието на срещата като се отдаде дължимото внимание на изискванията, определени в настоящите разпоредби по сигурността и всички други указания по сигурността, които се преценят като необходими.

Служба за сигурност на ГСС

5. Службата за сигурност на ГСС следва да предоставя съвети по сигурността, свързани с подготовката на срещата; нейни представители следва да оказват помощ и да предоставят съвети на служителя по сигурността на срещата и на делегациите при необходимост.

6. Всяка делегация на срещата следва да определи служител по сигурността, който е отговорен за решаването на въпросите, свързани със сигурността в собствената му делегация и за поддържането на връзка със служителя по сигурността на срещата както и с представителя на Службата за сигурност на ГСС при необходимост.

МЕРКИ ЗА СИГУРНОСТ

Зони за сигурност

7. Необходимо е да се създадат следните зони за сигурност:

а) Зона за сигурност клас II, съставена от работна стая, офисите и оборудването за отпечатване и размножаване на материалите както и офисите на делегациите при необходимост;

б) Зона за сигурност клас I, съставена от конферентната зала и кабините на преводачите и адио инженерите;

в) административни зони, съставени от зона на пресата и тези сектори от мястото на срещата, които се заемат от администрацията, заведенията за хранене и настаняване както и зоната в непосредствена близост до Пресцентъра и мястото на срещата.

Пропуски

8. Служителят по сигурността на срещата следва да издаде подходящи значки по заявка на делегациите, съответстваща на техните потребности. При необходимост може да се използват различни значки, осигуряващи достъп до различни зони за сигурност.

9. Указанията за сигурността по време на срещата следва да изискват от всички заинтересовани лица да носят значките си на видно място през цялото

време в рамките на мястото на срещата, за да могат да бъдат проверявани при необходимост от персонала по сигурността.

10. Освен участниците със значки, на мястото на срещата следва да се допускат възможно най-малък брой хора. Националните делегации, желаещи да приемат посетители по време на срещата, следва да уведомят служителя по сигурността на срещата. На посетителите се дава значка за посетител. Необходимо е да се попълни пропуск, на който е написано името на посетителя и името на лицето, което се посещава. Посетителите следва да бъдат придружавани през цялото време от охрана или от лицето, което посещават. Пропускът за посетител следва да се носи от придружаващото лице, което следва да върне пропуска заедно със значката за посетител на персонала по сигурността след като посетителят напусне мястото на срещата.

Контрол върху фотографската и звукозаписната апаратура

11. В зоната за сигурност клас I не мога да се внасят фотоапарати или звукозаписна апаратура, с изключение на апаратурата, донесена от фотографите и звукозаписните инженери, получили надлежно разрешение от служителя по сигурността на срещата.

Проверка на чанти за документи, преносими компютри и пакети

12. Лицата с пропуск, на които е разрешен достъп до зона за сигурност мога обикновено да внесат чантите си за документи и преносимите си компютри (само със собствено електрозахранване) без извършване на проверка. Когато става въпрос за пакети за делегациите, те могат да бъдат получени от делегациите след като бъдат проверени от служителя по сигурността на делегацията, проверени на скенер или отворени за проверка от персонала по сигурността. Ако служителят по сигурността на срещата счете за необходимо, той може да въведе по-строги мерки за проверка на чантите за документи и пакетите.

Техническа сигурност

13. Конферентната зала може да се обезопаси технически от екипа за техническа сигурност, който може също да организира електронно наблюдение по време на срещата.

Документи на делегациите

14. Делегациите следва да носят отговорност за внасянето в залата и изнасянето от нея на класифицирана информация на ЕС. Те следва също да носят отговорност за проверката и сигурността на тези документи по време на използването им в помещенията, които са определени за тях. За транспортирането на класифицираните документи до и от мястото на срещата може при необходимост да се потърси помощ от държавата-членка - домакин.

Безопасно съхраняване на документите

15. Когато ГСС, Комисията или делегациите не могат да съхранят класифицираните си документи в съответствие с приетите стандарти, те могат да оставят документите в запечатан плик на служителя по сигурността на срещата срещу разписка, за да бъдат съхранени от него в съответствие с приетите стандарти.

Проверка на офисите

16. Служителят по сигурността на срещата следва да организира проверка на офисите на ГСС и на делегациите в края на всеки работен ден, за да гарантира, че

всички класифицирани документи на ЕС се съхраняват на безопасно място.; в противен случай той следва да предприеме необходимите мерки.

Освобождаване от класифицирани отпадъци на ЕС

17. Всички отпадъци следва да се третират като класифицирани за ЕС и на ГСС и делегациите следва да се предоставят кошчета или торби за хартиени отпадъци. Преди ГСС и делегациите да напуснат определените за тях помещения те следва да предадат отпадъците си на служителя по сигурността на срещата, който следва да организира унищожаването им в съответствие с разпоредбите.

18. В края на срещата всички документи, които се намират в ГСС и делегациите, но вече не са необходими, следва да се третират като отпадъци. Преди да се вдигнат приетите мерки за сигурност по време на срещата следва да се направи пълен оглед на помещенията на ГСС и делегациите. Документите, за които са подписани разписки, следва в зависимост от случая да се унищожат съгласно разпоредбите на раздел VII.

РАЗДЕЛ X

НАРУШЕНИЯ НА СИГУРНОСТТА И КОМПРОМЕТИРАНЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

1. Нарушение на сигурността настъпва в резултат на действие или бездействие в противоречие с разпоредба на Съвета или разпоредба относно националната сигурност, което би застрашило или компрометирало класифицирана информация на ЕС.

2. Компрометиране на класифицирана информация на ЕС настъпва когато информацията като цяло или част от нея попадне в ръцете на неупълномощени лица, т.е. лица, които не са преминали през съответстващо проучване за надеждност от гледна точка на сигурността или които нямат необходимост да знаят или когато е налице вероятност, че е настъпило такова събитие.

3. Класифицирана информация на ЕС може да бъде компрометирана в резултат на невнимание, небрежност или непредпазливост както и чрез дейността на службите, чиито обект са ЕС или държавите-членки с оглед на класифицираната информация и дейност на ЕС, или от подривни организации.

4. Всички лица, от които се изисква обработване на класифицирана информация на ЕС, е важно да бъдат подробно запознати с процедурите по сигурността, опасностите, породени от непредпазливост по време на разговори, и взаимоотношенията им с пресата. Те следва да се информирани за значението на незабавното докладване на всяко нарушение на сигурността, което са забелязали, на органите по сигурността на държавата-членка, институцията или агенцията, в която работят.

5. Когато органът по сигурността открие или е информиран за нарушение на сигурността, свързано с класифицирана информация на ЕС, или за изгубени или изчезнали класифицирани материали на ЕС, той своевременно взема мерки с цел:

а) да установи фактите;

б) да направи оценка и да сведе до минимум нанесената вреда;

в) да предотврати повторно нарушение;

г) да уведоми съответните органи за последиците от нарушението на сигурността;

В този контекст се предоставя следната информация:

(i) описание на информацията, за която става въпрос, включващо и нивото на класификация, уникален идентификационен номер и номер на копието, дата, създател на информацията, предмет и обхват;

(ii) кратко описание на обстоятелствата, при които е извършено нарушението на сигурността, включващо датата и времето през което информацията е била изложена на опасност от компрометиране;

(iii) декларация, че създателят на информацията е бил уведомен.

6. Всеки орган по сигурността е задължен, веднага след като е уведомен за възможността да е настъпило нарушение на сигурността, да докладва факта незабавно като използва следната процедура: под-регистратурата за документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС докладва въпроса на службата за сигурност на ГСС чрез нейната централна регистратура за документи с ниво на

класификация СТРОГО СЕКРЕТНО ЗА ЕС; в случай на компрометиране на класифицирана информация на ЕС, настъпило в юрисдикцията на държава-членка, случаят се докладва на службата за сигурност на ГСС по реда и условията на параграф 5, чрез отговорния ОНС.

7. Случаите, които се отнасят за информация с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС, е необходимо да се докладват само когато са необичайни.

8. След като е информиран за настъпило нарушение на сигурността, генералният секретар/върховният представител:

а) уведомява органът, който е създал въпросната информация;

б) обръща се към съответните органи по сигурността с искане за започване на разследване;

в) координира разследването, когато в него участват повече от един орган по сигурността;

г) получава доклад за обстоятелствата, при които е настъпило нарушението, датата или периодът през който вероятно е настъпило нарушението и е било разкрито, с подробно описание на съдържанието и нивото на класификация на въпросния материал. Нанесената вреда на интересите на ЕС или на една или повече държави-членки и мерките, предприети за предотвратяване на повторно нарушение, следва също да бъдат докладвани.

9. Органът, който е създал информацията, информира адресатите и предоставя необходимите указания.

10. Всяко лице, което е отговорно за компрометирането на класифицирана информация на ЕС, подлежи на дисциплинарно наказание в съответствие с правилата и разпоредбите в тази област. Това наказание се налага независимо от съдебното преследване.

РАЗДЕЛ XI

ЗАЩИТА НА ИНФОРМАЦИЯТА, ОБРАБОТВАНА В СИСТЕМИ ЗА ИНФОРМАЦИОННИ ТЕХНОЛОГИИ И КОМУНИКАЦИИ

Съдържание

Глава I

Въведение

ОБЩИ АСПЕКТИ

1. Политиката и изискванията от гледна точка на сигурността, разгледани в настоящия раздел, се отнасят за всички комуникационни и информационни системи и мрежи (наричани по-нататък СИСТЕМИ), които обработват информация с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и по-високо от това ниво.

2. СИСТЕМИТЕ, обработващи информация с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС, също се нуждаят от мерки за сигурност с цел защита на поверителността на тази информация. Всички СИСТЕМИ се нуждаят от мерки за сигурност с цел защита на тяхната и на информацията, която се съдържа в тях, цялостност и достъпност. Мерките за сигурност, които се използват при тези системи, се определят от органа по акредитация на сигурността (ОАС) и са пропорционални на оценката на риска и съвместими с политиката, заявен в настоящите разпоредби по сигурността.

3. Защитата на сензорните системи, съдържащи вградени СИСТЕМИ за информационни технологии, се определя и конкретизира в общия контекст на системите, към които принадлежат, като при възможност се използват приложимите разпоредби на настоящия раздел.

ЗАПЛАХИ ЗА И УЯЗВИМОСТ НА СИСТЕМИТЕ

4. Заплахата най-общо може да се определи като възможност за случайно или предумишлено компрометиране на сигурността. Когато става въпрос за СИСТЕМИ, компрометиране означава загуба на едно или повече качества на поверителност, на цялостност и на достъпност. Уязвимостта може да се определи като слабост или отсъствие на контролни мерки, което би улеснило или позволило осъществяване на заплаха срещу конкретен актив или конкретна цел. Уязвимостта може да бъде бездействие, но може да бъде свързана и с недостатъци в силата, цялостността и последователността на контрола; уязвимостта може да бъде от технически, процедурен или оперативен характер.

5. Класифицираната и некласифицираната информация на ЕС, обработвана в СИСТЕМИ в концентрирана форма, предназначена за бързо обработване, съобщаване и използване, е уязвима по отношение на много рискове. Те включват достъп до информацията на неупълномощени потребители или точно обратното - отказ на достъп на упълномощени потребители. Съществуват и рискове, свързани с нерегламентирано разкриване, подправяне, изменение и заличаване на информацията. Освен това, сложното и понякога лесно чупливо оборудване е скъпо и често е трудно да бъде поправено или бързо подменено. Тези СИСТЕМИ, поради това, са привлекателна цел за извършване на операции за събиране на информация и за саботаж, особено ако се счита, че мерките за сигурност са неефикасни.

МЕРКИ ЗА СИГУРНОСТ

6. Главната цел на мерките за сигурност, разгледани в настоящия раздел, е да се осигури защита срещу нерегламентирано разкриване на информация (загуба на поверителност) и срещу загуба на цялостност и достъпност на информацията. За да се постигне съответстваща защита на сигурността на СИСТЕМА, която

обработва класифицирана информация на ЕС, се определят подходящите стандарти за обикновена сигурност заедно със специфичните процедури и техники по сигурността, предназначени за всяка конкретна СИСТЕМА.

7. С цел създаване на безопасна среда за работа на СИСТЕМАТА се определят и въвеждат взаимодопълващи се мерки за сигурност. Областите на приложение на тези мерки включват физическите елементи, персонала, нетехническите процедури и процедурите за работа на компютрите и комуникационните съоръжения.

8. Мерките за компютърна сигурност (характеристиките за сигурност на хардуера и софтуера) следва да се прилагат при съблюдаване на принципа „необходимост да се знае" и да предотвратяват или откриват нерегламентираното разкриване на информация. До каква степен следва да се разчита на мерките за компютърна сигурност се определя в процеса на създаване на изискването за сигурност. Процесът на акредитация определя дали е налице съответстващо ниво на осигуряване, което да поддържа надеждността на мерките за компютърна сигурност.

9. За всички СИСТЕМИ, обработващи информация с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или с по-високо от това ниво, се изисква да се създаде Специфичен за системата регламент за изискване за сигурност (СРИС) от Органа за експлоатация на ИТ системи (ОЕИТС) заедно с входящите ресурси и помощта при необходимост от служителите по проекта и органът по ИНФОСЕК, и одобрени от ОАС.

10. СРИС се формулира в началния етап от започването на проекта и се развива и усъвършенства с развитието на самия проект като изпълнява различна роля през различните етапи на проекта и жизнения цикъл на СИСТЕМАТА.

11. СРИС създава обвързващото споразумение между Оперативния орган за системите за информационни технологии и ОАС, на основата на което СИСТЕМАТА следва да се акредитира.

12. СРИС представлява пълен и ясен регламент на принципите за сигурност, които следва да се спазват, и на подробните изисквания за сигурност, които следва да се изпълнят. СРИС се основава на водената от Съвета политика за сигурност и оценка на риска или се налага от параметрите на операционната среда, най-ниското ниво на проучване на персонала за надеждност от гледна точка на сигурността, най-високото ниво на класификация на обработваната информация, безопасния режим на работа и изискванията на потребителите. СРИС е неделима част от документацията по проекта, която се предоставя на съответните органи за одобрение на техническата част, финансовата част и сигурността на проекта. Окончателният вид на СРИС е цялостен регламент на значението на сигурността на СИСТЕМАТА.

БЕЗОПАСНИ РЕЖИМИ НА РАБОТА

13. Всички СИСТЕМИ, които обработват информация с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и с по-високо от това ниво, се акредитират за работа при един, а при необходимост в зависимост от изискванията през различните часови периоди, и при повече от един от дадените по-долу безопасни режими на работа, или техните национални еквиваленти:

а) специален;

б) висок; и

в) многостепенен .

Глава II

Определения

ДОПЪЛНИТЕЛНА МАРКИРОВКА

14. Допълнителна маркировка като например КРИПТО или друго признато в ЕС обозначение за специална обработка се поставя когато е необходимо ограничено предоставяне и специално обработване освен определеното от класификацията за сигурност.

15. „СПЕЦИАЛЕН" БЕЗОПАСЕН РЕЖИМ НА РАБОТА" е режимът на работа, при който ВСИЧКИ лица с достъп до СИСТЕМАТА са проучени за надеждност от гледна точка на сигурността до най-високото ниво на класификация на информацията, обработвана в СИСТЕМАТА, и имат обща необходимост да се знае с оглед на ЦЯЛАТА информация, обработвана в СИСТЕМАТА.

Забележки:

(1) Обща необходимост да се знае означава, че не е налице задължително изискване за характеристиките на компютърна сигурност да осигуряват разделяне на информацията в рамките на СИСТЕМАТА.

(2) Другите характеристики на сигурността (например физическа, на персонала и процедурите) отговарят на изискванията за най-високото ниво на класификация и всички категорийни обозначения на информацията, обработвана в СИСТЕМАТА.

16. „ВИСОК" БЕЗОПАСЕН РЕЖИМ НА РАБОТА е режимът на работа, при който ВСИЧКИ лица с достъп до СИСТЕМАТА са проучени за надеждност от гледна точка на сигурността до най-високото ниво на класификация на информацията, обработвана в СИСТЕМАТА, но НЕ ВСИЧКИ лица с достъп до СИСТЕМАТА имат обща необходимост да се знае с оглед на информацията, обработвана в СИСТЕМАТА.

Забележки:

(1) Отсъствието на обща необходимост да се знае показва, че е налице изискване към характеристиките за компютърна сигурност да предоставят селективен достъп до и разделяне на информацията в рамките на СИСТЕМАТА.

(2) Другите характеристики на сигурността (например физическа, на персонала и процедурите) отговарят на изискванията за най-високото ниво на класификация и всички категорийни обозначения на информацията, обработвана в СИСТЕМАТА.

(3) Цялата информация, която се обработва или до която има достъп СИСТЕМА с този режим на работа, заедно с изходящия ресурс са потенциално защитени от обозначението за информационна категория и за най-високото ниво на класификация на информацията, която се обработва до определянето на друго, освен ако не е налице приемливо ниво на доверие, което може да се определи за всички налични обозначаващи функции.

17. „МНОГОСТЪПАЛЕН" БЕЗОПАСЕН РЕЖИМ НА РАБОТА е режимът на работа, при който НЕ ВСИЧКИ лица с достъп до СИСТЕМАТА са проучени за надеждност от гледна точка на сигурността до най-високото ниво на класификация на информацията, обработвана в СИСТЕМАТА, и НЕ ВСИЧКИ лица с достъп до СИСТЕМАТА имат обща необходимост да се знае с оглед на информацията, обработвана в СИСТЕМАТА.

Забележки:

(1) Този режим на работа разрешава, текущо, обработването на информация с различни нива на класификация и със смесени обозначения за информационна категория.

(2) Фактът, че не всички лица са проучени за надеждност от гледна точка на сигурността до най-високото ниво на класификация на информацията, свързван с отсъствието на обща

необходимост да се знае, показва че е налице изискване към характеристиките за компютърна сигурност да предоставят селективен достъп до и разделяне на информацията в рамките на СИСТЕМАТА.

18. ИНФОСЕК е прилагането на мерки за сигурност с цел защита на информацията, която се обработва, съхранява или предава чрез комуникационни, информационни и други електронни системи, от загуба на поверителност, цялостност и достъпност, независимо дали е случайна или предумишлена, и за да се предотврати загубата на цялостност и достъпност на самите системи. Мерките по ИНФОСЕК включват мерките за компютърна, предавателна, емисионна и криптографска сигурност и откриването, документирането и парирането на заплахите за информацията и за СИСТЕМИТЕ.

19. КОМПЮТЪРНА СИГУРНОСТ (КОМПЮСЕК) е приложението на характеристики за сигурност на хардуера, софтуер от ниско ниво, и софтуера в компютърна система с цел да се защити от, или предотврати, нерегламентирано разкриване, манипулиране, изменение/заличаване на информация или отказ на обслужване.

20. ПРОДУКТ ЗА КОМПЮТЪРНА СИГУРНОСТ е изделие за компютърна сигурност с широко приложение, предназначено за монтиране в система за информационни технологии с цел повишаване, или осигуряване, на поверителност, цялостност и достъпност на обработваната информация.

21. КОМУНИКАЦИОННА СИГУРНОСТ (КОМСЕК) е прилагането на мерки за сигурност по отношение на телекомуникационни съоръжения с цел отказ на неупълномощените лица на ценна информация, която може да се извлече при притежаването или изучаването на тези съоръжения, и гарантиране на тяхната автентичност.

Забележка:

Тези мерки включват криптографска, предавателна и емисионна сигурност; те включват също и процедурна, физическа, на персонала, документна и компютърна сигурност.

22. ОЦЕНКА е подробната техническа проверка от гледна точка на сигурността, извършена от съответен орган, на СИСТЕМА или на продукт за криптографска или компютърна сигурност.

Забележка:

(1) Оценката изследва наличието на задължителните защитни функции и отсъствието на компрометиращ страничен ефект от тях и преценява невъзможността за фалшифицирането им.

(2) Оценката определя в каква степен са удовлетворени изискванията за сигурност на СИСТЕМАТА, или обявените изисквания за сигурност на продукта за компютърна сигурност, и определя нивото на осигуряване на СИСТЕМАТА, или на криптографската доверителна функция и на доверителната функция на продукта за компютърна сигурност.

23. СЕРТИФИКАЦИЯ е издаването на официален документ, придружен от констатациите от независима проверка за извършената оценка и резултатите от нея, удостоверяващ в каква степен СИСТЕМАТА отговаря на изискването за сигурност или продуктът за компютърна сигурност отговаря на обявените за него изисквания за сигурност.

24. АКРЕДИТАЦИЯ е оторизацията и одобряването на СИСТЕМА с цел обработване на класифицирана информация на ЕС в операционната й среда.

Забележка:

Такава акредитация следва да се направи след изпълнението на всички необходими процедури по сигурността и постигането на достатъчно ниво на защита на системния ресурс. Акредитацията обикновено се прави на основата на СРИС и включва следното:

а) декларация за целта на акредитацията на системата; по-специално информация с какво ниво/какви нива на класификация ще се обработва и какви системни или мрежови безопасни режими на работа се предлагат;

б) представяне на преглед за управлението на риска с оглед на определянето на заплахите и уязвимостта и мерките за борба с тях;

в) оперативните процедури по защитата (СекОпс) с подробно описание на предложените операции (например режими, услуги, които ще се предоставят) включително и описание на защитните характеристики на СИСТЕМАТА, които съставляват базата за акредитация;

г) план за въвеждането и поддържането на защитните характеристики;

д) план за първоначално и последващо изпитване, оценка и сертифициране на сигурността на системата и мрежата; и

е) сертифициране, при необходимост, съвместно с другите елементи на акредитацията.

25. ИТ СИСТЕМА е блок от оборудване, методи и процедури, а при необходимост, и персонал, организирани така, че да изпълняват функции за обработка на информацията.

Забележки:

(1) Това е блок от съоръжения, конфигурирани за обработка на информацията в рамките на системата.

(2) Такива системи могат да поддържат приложения за консултации, управление, контрол, комуникации, научни или административни приложения, включително и текстообработващи приложения.

(3) Границите на системата най-общо се определят като елементите, които се контролират от един ООСИТ.

(4) Системата за информационни технологии може да съдържа под-системи, като някои от тях самите представляват системи за информационни технологии.

26. ХАРАКТЕРИСТИКИТЕ ЗА СИГУРНОСТ НА ИТ СИСТЕМИТЕ обхващат всички хардуерни, софтуерни от ниско ниво и софтуерни функции и характеристики; процедурите по експлоатацията, процедурите по отчетността и видовете контрол за достъп, ИТ зоната, зоната на дистанционния терминал/работната станция и ограниченията за управлението, физическа конструкция и устройства, персонал и контрол на комуникациите, необходим за осигуряване на приемливо ниво на защита на класифицираната информация, за да бъде обработвана в ИТ система.

27. ИТ МРЕЖА е организирането на ИТ системи, от една и съща географска област, свързани помежду си с цел обмен на данни, и обединяването на елементите на взаимосвързаните ИТ системи и техния интерфейс с поддържащите мрежи с данни или с комуникационните мрежи.

Забележки:

(1) ИТ мрежата може да използва услугите на една или няколко комуникационни мрежи, свързани помежду си с цел обмен на данни; няколко ИТ мрежи могат да използват услугите на обща комуникационна мрежа.

(2) ИТ мрежата се нарича „локална” ако свързва няколко компютри в един и същ обект.

28. ХАРАКТЕРИСТИКИТЕ ЗА СИГУРНОСТ НА ИТ МРЕЖИТЕ включват характеристиките за сигурност на ИТ системите на отделните ИТ системи, образуващи мрежата, заедно с допълнителните елементи и характеристики, свързвани със системата като такава (например комуникации в мрежа,

идентификация за достъп и механизми и процедури по обозначаването, видове контрол за достъп, програми и последващи одити) необходими за осигуряване на приемливо ниво на защита на класифицираната информация.

29. ИТ зона е зоната, в която се намират един или повече компютри, техните локални периферни и запаметяващи устройства, контролните устройства и свързаното с тях мрежово и комуникационно оборудване.

Забележка:

Тя не включва отделна зона с разположени в нея дистанционни периферни устройства или терминали/работни станции дори когато тези устройства са свързани със съоръжения в ИТ зоната.

30. ЗОНА ЗА ДИСТАНЦИОНЕН ТЕРМИНАЛ/РАБОТНА СТАНЦИЯ е зона, в която има някакво компютърно оборудване, неговите локални периферни устройства или терминали/работни станции и всички свързани с тях комуникационни съоръжения, и е отделена от ИТ зоната.

31. Мерки за противодействие ТЕМПЕСТ: мерки за сигурност, предназначени за защита на съоръженията и комуникационните инфраструктури от компрометирането на класифицирана информация чрез неумишлени електромагнитни емисии.

Глава III

Отговорности, свързани със сигурността

ОБЩИ ПОЛОЖЕНИЯ

32. Отговорностите на Комитета за сигурност, разгледан в раздел I, параграф 4, включват въпросите на сигурността на информацията. Комитетът за сигурност организира дейността си по начин, който му дава възможност да предоставя експертна помощ по упоменатите по-горе въпроси.

33. При възникването на проблеми, свързани със сигурността (инциденти, нарушения и др.), отговорният национален орган и/или службата за сигурност на ГСС вземат незабавни мерки. Всички въпроси се отнасят до службата за сигурност на ГСС.

34. Генералният секретар/върховният представител, а при необходимост, и ръководителят на децентрализирана агенция на ЕС създават служба за сигурност на информацията с цел предоставяне на указания на органа по сигурността относно изграждането и контрола на специалните характеристики за сигурност, проектирани като част от СИСТЕМИТЕ.

ОРГАНА ПО АКРЕДИТАЦИЯ НА СИГУРНОСТТА (ОАС)

35. ОАС е:

- ОНС,
- Орган, определен от генералния секретар/върховния представител,
- Орган по сигурността на децентрализирана агенция на ЕС или
- Техните упълномощени/номинирани представители в зависимост от СИСТЕМАТА, която ще се акредитира.

36. ОАС е отговорен за осигуряване на съответствие на СИСТЕМИТЕ с политиката на Съвета в областта на сигурността. Едно от неговите задължения е одобряването на СИСТЕМИТЕ, които ще обработват в операционната си среда класифицирана информация на ЕС с определено ниво на класификация. По

отношение на ГСС, а при необходимост, и по отношение на децентрализираните агенции на ЕС, ОАС е отговорен за сигурността от името на генералния секретар/върховния представител или на ръководителите на децентрализираните агенции на ЕС.

Юрисдикцията на ОАС в ГСС обхваща всички СИСТЕМИ, които са в експлоатация в рамките на помещенията на ГСС. СИСТЕМИ и елементи на СИСТЕМИ, които са в експлоатация в държава-членка остават под юрисдикцията на държавата-членка. Когато отделни елементи на една СИСТЕМА попадат под юрисдикцията на ОАС в ГСС и други ОАС, всички страни назначават съвместен съвет по акредитация под ръководството на ОАС в ГСС.

ОРГАН ПО ИНФОСЕК (ОИ)

37. Органът по ИНФОСЕК е отговорен за служебните дейности в областта на ИНФОСЕК. По отношение на ГСС, а при необходимост, и по отношение на децентрализираните агенции на ЕС Органът по ИНФОСЕК е отговорен за:

- предоставяне на техническа помощ на ОАС,
- помощ при разработването на СРИС,
- преглед на СРИС с цел осигуряване на съответствие с настоящите разпоредби относно сигурността, политиките в областта на ИНФОСЕК и архитектурно-техническата документация,
- участие в съветите по акредитация, при необходимост, и предоставяне на ОАС на препоръки в областта на ИНФОСЕК относно акредитацията,
- осигуряване на подкрепа за обучение и образование в областта на ИНФОСЕК,
- осигуряване на техническа помощ при разследване на инциденти, свързани с ИНФОСЕК,
- създаване на техническо ръководство, за де се осигури използването само на оторизиран софтуер.

ОРГАН ЗА ЕКСПЛОАТАЦИЯТА НА ИТ СИСТЕМИ (ОЕИТС)

38. Органът по ИНФОСЕК предава пълномощия на ОЕИТС на възможно най-ранен етап отговорността за въвеждането и експлоатацията на контролни устройства и специални характеристики за сигурност на СИСТЕМАТА. Тази отговорност продължава през целия жизнен цикъл на СИСТЕМАТА от етапа на идейния проект до окончателното демонтиране.

39. ОЕИТС е отговорен за всички мерки за сигурност, проектирани като част от самата СИСТЕМА. В отговорностите му е включена и подготовката на СекОпс. ОЕИТС определя стандартите за сигурност и практиките, които следва да се спазват от доставчика на СИСТЕМАТА.

40. При необходимост ОЕИТС може да предаде пълномощия по част от отговорностите си на служителя по сигурността в областта на ИНФОСЕК и на служителя по сигурността на обект в областта на ИНФОСЕК.

ПОТРЕБИТЕЛИ

41. Всички потребители носят отговорност, че действията им няма да имат неблагоприятно въздействие върху сигурността на СИСТЕМАТА, която използват.

ОБУЧЕНИЕ В ОБЛАСТТА НА ИНФОСЕК

42. Достъп до образование и обучение в областта на ИНФОСЕК се осигурява на различните нива и за различните видове персонал от ГСС, децентрализираните агенции на ЕС или държавните ведомства в държавите-членки.

Глава IV

Нетехнически мерки за сигурност

СИГУРНОСТ НА ПЕРСОНАЛА

43. Потребителите на СИСТЕМАТА се проучват за надеждност от гледна точка на сигурността при спазване на принципа „необходимост да се знае" в съответствие с нивото на класификация и съдържанието на информацията, която се обработва в тяхната конкретна СИСТЕМА. Достъпът до някои съоръжения или специфична информация за сигурността на СИСТЕМИТЕ изисква специално проучване и издаване на разрешение в съответствие с процедурите на Съвета.

44. ОАС определя всички чувствителни длъжности и конкретизира нивото на проучване и надзора, задължителни за всички служители, които заемат такива длъжности.

45. СИСТЕМИТЕ се определят и проектират по начин, който улеснява разпределението на служебните задължения и отговорностите на персонала така, че да не се допусне едно лице да знае всичко за или да има пълен контрол върху точките, в които са поставени ключовете за сигурност на СИСТЕМАТА. Целта е да не се позволява на по-малко от две лица да могат да правят изменения или преднамерено понижаване на нивото на класификация на системата или мрежата.

ФИЗИЧЕСКА СИГУРНОСТ

46. Създават се зони за ИТ и дистанционни терминали/работни станции (по смисъла на параграфи 29 и 30) , в които се обработва информация с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и с по-високо от това ниво с помощта на ИТ и там, където е възможен потенциален достъп до такава информация, като Клас I и Клас II зони за сигурност на ЕС или националния им еквивалент в зависимост от случая.

47. В зоните за ИТ и дистанционни терминали/работни станции, в които сигурността на СИСТЕМАТА може да бъде променена, не може да се намира само един упълномощен висш чиновник/друг служител.

КОНТРОЛ НА ДОСТЪПА ДО СИСТЕМАТА

48. Информация или материал, позволяващи контрол на достъпа до СИСТЕМАТА, са защитени с мерки, съизмерими с тези при най-високото ниво на класификация и носят обозначение за категорията на информацията, до която могат да осигурят достъп.

49. Когато престанат да се използват с такова предназначение, информацията или материалът за контрол на достъпа се унищожават по реда и условията на параграфите 61 – 63.

Глава V

Технически мерки за сигурност

СИГУРНОСТ НА ИНФОРМАЦИЯТА

50. Задължение на създателя на информацията е да идентифицира и класифицира всички документи с информация, независимо дали са на хартиен носител или на

електронен носител. Върху всяка страница на хартиения носител, в горния и долния й край, се поставя маркировка за нивото на класификация. Изходящите материали, независимо дали са на хартиен или на електронен носител, имат ниво на класификация, съответно на най-високото ниво на класификация на информацията, използвана за създаването им. Начинът, по който се оперира със СИСТЕМАТА, може също да повлияе на нивото на класификация на изходящите материали от системата.

51. Задължение на организацията и лицата, които държат информацията в нея, е да разгледат проблемите, свързани с обединяването на отделните елементи на информацията, и изводите, които могат да се направят след като елементите се свържат, и да решат дали е необходимо да се даде по-високо ниво на класификация на цялата информация.

52. Фактът, че информацията може да бъде с код за минимизиране или предаване, или може да е представена под някаква форма с двоичен код не дава никаква защита от гледна точка на сигурността и затова не бива да влияе на нивото на класификация на информацията.

53. При прехвърлянето на информация от една СИСТЕМА в друга, информацията е защитена по време на трансфера и в СИСТЕМАТА-получател по начин, който е съизмерим с оригиналното ниво на класификация и категория на информацията.

54. Всички носители на електронно съхранена информация се обработват по начин, който е съизмерим с най-високото ниво на класификация на съхраняваната върху тях информация, или с обозначението върху носителя като им се осигурява непрекъсната подходяща защита.

55. Носителите на електронно съхранена информация за многократно употреба, използвани за записване на класифицирана информация на ЕС, запазват най-високото ниво на класификация, за която някога са били използвани, докато надлежно се понижи или премахне нивото на класификация на информацията и съответно се промени нивото на класификация на носителя или се премахне класификацията на носителя, или носителят се унищожи с помощта на одобрена процедура на ГСС или национална процедура (виж параграфите от 61 до 63).

КОНТРОЛ И ОТЧЕТНОСТ НА ИНФОРМАЦИЯТА

56. Водят се автоматизирани (последващ одит) или попълвани на ръка дневници като форма на документация за случаите на осигурен достъп до информация с ниво на класификация СЕКРЕТНО ЗА ЕС или по-високо от това ниво. Тази документация се съхранява в съответствие с настоящите разпоредби относно сигурността.

57. Класифицираните изходящи материали на ЕС, които се държат в ИТ зоната, могат да се обработват като един класифициран продукт и не е необходимо да се регистрират при условие, че материалът е надлежно идентифициран, маркиран за съответното ниво на класификация и контролиран.

58. Когато са произведени изходящи материали от СИСТЕМА, обработваща класифицирана информация на ЕС, и са предадени от ИТ зона на зона за дистанционен терминал/работна станция, се създават процедури, съгласувани с ОАС, по контролирането на дистанционните изходящи материали. За информацията с ниво на класификация СЕКРЕТНО ЗА ЕС или по-високо от това ниво процедурите включват специални инструкции за отчетност на информацията.

ОБРАБОТКА И КНОТРОЛ НА ПРЕНОСИМИТЕ НОСИТЕЛИ НА ЕЛЕКТРОННО СЪХРАНЕНА ИНФОРМАЦИЯ

59. Всички преносими носители на електронно съхранена информация с ниво на класификация СЕКРЕТНО ЗА ЕС или по-високо от това ниво се обработват като материал и към тях се прилагат общите правила. Необходимо е тяхната маркировка за идентификация и ниво на класификация да е съобразена със специфичната външна форма на носителите, за да може лесно да се разпознава.

60. Потребителите носят отговорност относно осигуряването на съхраняване на класифицираната информация на ЕС на носители със съответстваща маркировка за ниво на класификация и защита. Създават се процедури, които да гарантират, че за всички нива на информацията на ЕС, съхраняването на информацията върху носители на електронно съхранена информация става в съответствие с настоящите разпоредби относно сигурността на информацията.

ПРЕМАХВАНЕ НА КЛАСИФИКАЦИЯТА И УНИЩОЖАВАНЕ НА НОСИТЕЛИ НА ЕЛЕКТРОННО СЪХРАНЕНА ИНФОРМАЦИЯ

61. Носителите на електронно съхранена информация, които се използват за записване на класифицирана информация на ЕС, могат да получат по-ниско ниво на класификация или класификацията им да бъде премахната ако се използват одобрени процедури на ГСС или национални процедури.

62. За носителите на електронно съхранена информация, на които е била съхранявана информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС или информация със специална категория, не се прилага премахване на класификацията и те не могат да бъдат повторно използвани.

63. Когато не може да се премахне класификацията на носители на електронно съхранена информация или те не могат да се използват повторно, те се унищожават с помощта на одобрена процедура на ГСС или национална процедура.

КОМУНИКАЦИОННА СИГУРНОСТ

64. Когато класифицирана информация на ЕС се предава по електромагнитен път, се прилагат специални мерки за защита на поверителността, цялостността и достъпността на предаването на информация. ОАС определя изискванията за защита на предаването на информация от разкриване и прехващане. Информацията предавана в комуникационна система е защитена на основата на изискванията за поверителност, цялостност и достъпност.

65. Когато за осигуряването на защита на поверителността, цялостността и достъпността са необходими криптографски методи, тези методи и свързаните с тях продукти се одобряват специално за тази цел от ОАС.

66. По време на предаване, поверителността на информацията с ниво на класификация СЕКРЕТНО ЗА ЕС и по-високо от това ниво е защитена чрез криптографски методи или продукти, одобрени от Съвета по препоръка на Комитета за сигурност на Съвета. По време на предаване, поверителността на информацията с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС е защитена чрез криптографски методи или продукти, одобрени от ГС/ВП по препоръка на Комитета за сигурност на Съвета или от държава-членка.

67. Подробните правила, приложими за предаването на класифицирана информация на ЕС се определят в специалните указания по сигурността, одобрени от Съвета по препоръка на Комитета за сигурност на Съвета.

68. При настъпване на извънредни оперативни обстоятелства, информацията с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС, ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС и СЕКРЕТНО ЗА ЕС може да бъде предавана като незакодиран текст при условие, че за всеки отделен случай е получено изрично разрешение. Тези извънредни обстоятелства са както следва:

а) по време на предстояща или действителна криза, конфликт или състояние на война; и

б) когато скоростта на доставяне на информацията е от най-голямо значение, а липсват средства за кодиране, и е преценено, че предадената информация не може да бъде използвана на време, за да окаже неблагоприятно въздействие върху операциите.

69. СИСТЕМАТА има способност за позитивен отказ на достъп до класифицирана информация на ЕС при някои или при всички свои дистанционни работни станции или терминали, когато това се налага поради физическо разкъсване на връзката или специални технически характеристики на софтуера, одобрени от ОАС.

МОНТАЖНА И РАДИАЦИОННА СИГУРНОСТ

70. Първоначалното монтиране на СИСТЕМИТЕ и всички по-големи промени в тях се специфицира по такъв начин, че монтажът да се извърши от монтажни специалисти, проучени за надеждност от гледна точка на сигурността, под непрекъснатия надзор на служители с техническа квалификация, които имат разрешение за достъп до класифицирана информация на ЕС с ниво съответно на най-високото ниво на класификация, което се очаква да бъде съхранявано и обработвано от СИСТЕМАТА.

71. Всички съоръжения се монтират в съответствие с текущата политика на Съвета в областта на сигурността.

72. СИСТЕМИТЕ, обработващи информация с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и по-високо от това ниво, са защитени по начин, който не позволява сигурността им да бъде застрашена от компрометиращи емисии, които се изучават и контролират чрез „ТЕМПЕСТ”.

73. Мерките за противодействие ТЕМПЕСТ, предназначени за защита на инсталациите на ГСС и децентрализираните агенции на ЕС, се проверяват и одобряват от органа по ТЕМПЕСТ, определен от органа по сигурността на ГСС. За националните инсталации, които обработват класифицирана информация на ЕС, те се одобряват от признатия национален орган за одобряване на ТЕМПЕСТ.

Глава VI

Сигурност при обработката на информацията

ОПЕРАТИВНИ ПРОЦЕДУРИ ПО СИГУРНОСТТА

74. СекОпс определят принципите, което следва да се приемат относно въпросите на сигурността, оперативните процедури, които следва да се изпълняват и отговорностите на персонала. Отговорност за изготвянето на СекОпс носи ОЕИТС.

УПРАВЛЕНИЕ НА ЗАЩИТАТА/КОНФИГУРАЦИЯТА НА СОФТУЕРА

75. Защитата на сигурността на приложните програми се определя по-скоро на основата на оценка на нивото на класификация на програмата, отколкото от нивото на класификация на информацията, която ще се обработва с тази програма. Влезлите в употреба софтуерни версии следва да се проверяват периодично, за да се осигури тяхната цялостност и правилно функциониране.

76. Нови или модифицирани версии на софтуер не следва да се използват за обработване на класифицирана информация на ЕС преди да са проверени от ОЕИТС.

ПРОВЕРКА ЗА НАЛИЧИЕ НА ЗЛОНАМЕРЕН СОФТУЕР/КОМПЮТЪРНИ ВИРУСИ

77. Проверката за наличието на злонамерен софтуер/компютърни вируси се извършва периодично в съответствие с изискванията на ОЕИТС.

78. Всички носители на електронно съхранена информация, влизащи в ГСС, децентрализираните агенции на ЕС или държавите-членки следва да бъдат проверени за наличието на злонамерен софтуер/компютърни вируси преди да бъдат въведени в някоя СИСТЕМА.

ТЕХНИЧЕСКО ОБСЛУЖВАНЕ

79. Договорите и процедурите по плановото и аварийното техническо обслужване на СИСТЕМИТЕ, за които е създаден СРИС, определят изискванията към и договореностите относно персонала за техническо обслужване и свързаните с него съоръжения, които влизат в ИТ зона.

80. Изискванията са ясно определени в СРИС, а процедурите – в СекОпс. Техническо обслужване от изпълнителя по договора, изискващо прилагане на процедури по диагностиката чрез дистанционен достъп, е разрешено само при извънредни обстоятелства, под строг контрол на сигурността и само с разрешението на ОАС.

Глава VII

Поръчки

81. Всеки продукт за сигурност, който ще се използва в СИСТЕМАТА, за да бъде доставен следва да бъде оценен и сертифициран или да бъде в процес на оценяване и сертифициране от съответния орган по оценка и сертификация на основата на международно признати критерии (като Общите критерии за оценка на сигурността на информационните технологии, виж ISO 15 408).

82. Когато се решава дали оборудването, и по-специално носителите на електронно съхранена информация, могат да бъдат наети вместо закупени, не бива да се забравя, че оборудването, което веднъж е било използвано за обработка на класифицирана информация на ЕС не може да напуска надлежно защитената среда без преди това да е премахната класификацията му с разрешението на ОАС и че не винаги може да се получи такова разрешение.

АКРЕДИТАЦИЯ

83. Всички СИСТЕМИ, за които се изисква създаването на СРИС, преди да започнат да обработват класифицирана информация на ЕС се акредитират на основата на информацията, предоставена в СРИС, СекОпс и друга важна документация от ОАС. Подсистемите и дистанционните терминали/работни станции се акредитират като част от СИСТЕМИТЕ, към които са свързани.

Когато една СИСТЕМА обслужва едновременно Съвета и други организации, ГСС и съответните органи по сигурността постигат взаимно съгласие по акредитацията.

84. Процесът на акредитиране може да се извърши в съответствие със стратегия за акредитация, подходяща за конкретната СИСТЕМА и определена от ОАС.

ОЦЕНКА И СЕРТИФИКАЦИЯ

85. Преди акредитацията, в някои случаи, техническите характеристики за сигурност на хардуера, фърмуера и софтуера на СИСТЕМАТА се оценява и сертифицира за способност за безопасно съхраняване на информацията на определеното ниво на класификация.

86. Изискванията за оценка и сертификация се включват в планирането на системата и са ясно формулирани в СРИС.

87. Оценяването и сертифицирането се извършват в съответствие с одобрените ръководства от технически квалифициран персонал, надлежно проучен и с разрешение за достъп, който представлява ОЕИТС.

88. Екипите могат да се осигурят от номинирания орган по оценяване или сертификация или негови представители, например компетентен, надлежно проучен и с разрешение за достъп изпълнител.

89. Степента на оценка и сертификация може да се намали (например да се включат само интеграционни аспекти), когато СИСТЕМИТЕ са базирани на съществуващите национално оценени и сертифицирани продукти за компютърна сигурност.

РУТИННА ПРОВЕРКА НА ТЕХНИЧЕСКИТЕ ХАРАКТЕРИСТИКИ ЗА СИГУРНОСТ ЗА ПРОДЪЛЖАВАНЕ НА АКРЕДИТАЦИЯТА

90. ОЕИТС създава рутинни процедури по контрола с цел да се гарантира, че всички технически характеристики за сигурност на СИСТЕМАТА са все още валидни.

91. Видовете промени, които биха предизвикали нова акредитация или изискват предварително одобрение от ОАС се определят точно и ясно в СРИС. След изменение, ремонт или повреда, които биха накърнили техническите характеристики за сигурност на СИСТЕМАТА, ОЕИТС осигурява извършването на проверка, за да се гарантира правилното функциониране на техническите характеристики за сигурност. Продължаването на акредитацията на СИСТЕМАТА обикновено зависи от успешното приключване на проверката.

92. Всички СИСТЕМИ, в които са въведени техническите характеристики за сигурност, преминават периодично през проверка или преглед, извършвани от ОАС. Проверките на СИСТЕМИТЕ, обработващи информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС или с допълнителна маркировка, се извършват не по-рядко от веднъж в годината.

Глава VIII

Временна или нередовна употреба

СИГУРНОСТ НА МИКРОКОМПЮТРИТЕ/ПЕРСОНАЛНИТЕ КОМПЮТРИ

93. Микрокомпютрите/персоналните компютри с фиксирани дискове (или други носители на съхранена информация след изключване на захранването), които

работят в самостоятелен режим или като конфигурации в мрежа и преносими компютърни устройства (например преносими персонални компютри и електронни „тетрадки” с фиксирани твърди дискове се считат за носители на съхранена информация също както флопи дискетите или другите сменяеми носители на електронно съхранена информация.

94. Тези съоръжения получават ниво на защита по отношение на достъп, обработка, съхраняване и пренасяне съотносим с най-високото ниво на класификация на информацията, която е била съхранявана или обработвана (докато не се понижи нивото им на класификация или премахне в съответствие с одобрените процедури).

ИЗПОЛЗВАНЕ НА ОБОРУДВАНЕ, КОЕТО Е ЧАСТНА СОБСТВЕНОСТ, ЗА СЛУЖЕБНИ ЦЕЛИ НА СЪВЕТА

95. Използването на частни сменяеми носители на електронно съхранена информация, софтуер и ИТ хардуер (например персонални компютри и преносими компютърни устройства) със способност за съхраняване на информация е забранено при обработката на класифицирана информация на ЕС.

96. Хардуер, софтуер и носители на информация не се внасят в зона от клас I или клас II, където се обработва класифицирана информация на ЕС, без разрешението на ръководителя на службата за сигурност на ГСС, ведомство на държава-членка или съответната децентрализирана агенция на ЕС.

ИЗПОЛЗВАНЕ НА ОБОРУДВАНЕ, КОЕТО Е СОБСТВЕНОСТ НА ИЗПЪЛНИТЕЛЯ, ИЛИ ПРЕДОСТАВЕНО ОТ ДЪРЖАВАТА ЗА СЛУЖЕБНИ ЦЕЛИ НА СЪВЕТА

97. Използване на ИТ оборудване и софтуер, които са собственост на изпълнителя, в организациите в помощ на служебните цели на Съвета може да се разреши от ръководителя на службата за сигурност на ГСС, от ведомство на държава-членка или от съответната децентрализирана агенция на ЕС. Използване на ИТ оборудване и софтуер, предоставени от държавата, от служители на ГСС или децентрализирана агенция на ЕС може също да се разреши; в такъв случай ИТ оборудването се поставя под контрола на съответния инвентарен опис на ГСС. И в двата случая, ако ИТ оборудването ще се използва за обработване на класифицирана информация на ЕС се извършват консултации със съответния ОАС с оглед на надлежното разглеждане и въвеждане на елементите на ИНФОСЕК, приложими към използването на този вид оборудване.

РАЗДЕЛ XII

ПРЕДОСТАВЯНЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ТРЕТИ ДЪРЖАВИ ИЛИ МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

ПРИНЦИПИ, РЕГЛАМЕНТИРАЩИ ПРЕДОСТАВЯНЕТО НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

1. Решението за предоставяне на класифицирана информация на ЕС на трети държави или международни организации се взема от Съвета въз основа на:

   - естеството и съдържанието на информацията;
   - необходимостта на получателя на информацията да знае;
   - оценка на предимствата за ЕС.

   За предоставянето на класифицирана информация на ЕС се иска съгласието на държавата-членка, създала информацията.

2. Решенията се вземат за всеки отделен случай в зависимост от:

   - желаното ниво на сътрудничество със заинтересованите трети държави или международни организации;
   - доверието, което може да им се окаже, в зависимост от нивото на сигурност, приложено към класифицирана информация на ЕС, поверена на тези държави или международни организации, и от съвместимостта на правилата за сигурност, прилагани от тях, и правилата за сигурност, прилагани в ЕС; Комитета по сигурността на Съвета предоставя на Съвета техническо становище по този въпрос.

3. Приемането на класифицирана информация на ЕС от трети държави или международни организации означава предварително да се установи, че предоставената или обменена информация няма да бъде използвана за други цели освен целите, послужили като мотив за предоставянето или обмена, и че те ще осигурят защитата, изисквана от Съвета.

НИВА

4. След вземането на решение от страна на Съвета, че може да бъде предоставена или обменена информация с дадена държава или международна организация, Съветът взема решение относно възможното ниво на сътрудничество. То се определя по-специално от политиката и приложимото законодателство в областта на сигурността на информацията в дадената държава или международна организация.

5. Има три нива на сътрудничество:

Първо ниво

Сътрудничество с трети държави или международни организации, чиято политиката и законодателство в областта на сигурността на информацията са много близки до тези на ЕС.

Второ ниво

Сътрудничество с трети държави или международни организации, чиято политиката и законодателство в областта на сигурността на информацията чувствително се отличават от тези на ЕС.

Трето ниво

Нередовно сътрудничество с трети държави или международни организации, за чиято политиката и законодателство в областта на сигурността на информацията не може да се даде оценка.

6. За всяко ниво на сътрудничество се определят разпоредби относно сигурността на информацията, които в отделните случаи получават нова редакция предвид на техническото становище на Комитета по сигурността на информацията на Съвета и от бенефициентите се изисква да ги прилагат с цел защита на предадената им класифицирана информация.

СПОРАЗУМЕНИЯ

7. След вземането на решение от страна на Съвета, че е налице трайна и дългосрочна необходимост от обмен на класифицирана информация между ЕС и трети държави или международни организации, Съветът изготвя „споразумения за процедурите по сигурността при обмен на класифицирана информация" с тях като определя целта на сътрудничеството и реципрочните правила относно защитата на обменената информация.

8. Когато се касае за нередовно сътрудничество от трето ниво, което по дефиниция има ограничено времетраене и цел, „споразуменията за процедурите по сигурността при обмен на класифицирана информация" могат да се заменят от меморандум за договореност в опростена форма, който определя естеството на класифицираната информация, която ще бъде обменена и реципрочните задължения относно тази информация.

9. Проектите на споразуменията за процедурите по сигурността или меморандумите за договореност се одобряват от Комитета по сигурността преди да се представят на Съвета за вземане на решение.

10. ОНС оказват необходимото съдействие на генералния секретар/върховния представител, за да гарантират, че предоставената информация ще бъде използвана и защитена в съответствие с клаузите на споразуменията за процедурите по сигурността или меморандумите за договореност.

_____

Допълнение 1

Списък на органите за национална сигурност

БЕЛГИЯ

Ministère des Affaires Étrangères, du Commerce Extérieur et de la Coopération au Développement Direction de la sécurité - A 01 Rue des Petits Carmes, 15 B - 1000 Bruxelles Telephone: 32-2-501 85 14 Fax: 32-2-501 80 58 Telex: 21376
Telegraphic address: Direction de Sécurité A01 - MINAFET

ДАНИЯ

Politiets Efterretningstjeneste Borups Alle 266 DK - 2400 Copenhagen NV
Telephone: 45-33 14 88 88 Fax: 45-38 19 07 05 Forsvarsministeriet Forsvarets Efterretningstjeneste Kastellet 30 DK - 2100
Copenhagen Ø Telephone: 45-33 32 55 66 Fax: 45-33 93 13 20

ГЕРМАНИЯ

Bundesministerium des Innern Referat IS 4 Alt-Moabit 101D D - 10559 Berlin
Telephone: 49-30-39 81 15 28 Fax: 49-30-39 81 16 10

ГЪРЦИЯ

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ) Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ - Β' Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020 - Χολαργός (Αθήνα) Ελλαδα Τηλέφωνα: 30-1-655 22 03 (ώρες γραφείου)
30-1-655 22 05 (εικοσιτετράωρο)
Φαξ: 30-1-642 69 40 Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR./SEC.)
STG 1020 , Holargos - Athens Greece Telephone: 30-1-655 22 03 (office hours)
30-1-655 22 05 (24 hours)
Fax: 30-1-642 69 40

ИСПАНИЯ

Autoridad Nacional de Seguridad Oficina Nacional de Seguridad Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8500
E - 28023 Madrid Telephone: 34-91-3... Fax: 34-91-372 58 08 E-mail: nsa-sp@areatec.com

ФРАНЦИЯ

Secrétariat général de la Défense Nationale Service de Sécurité de Défense (SGDN/SSD) 51 Boulevard de la Tour-Maubourg F - 75700 Paris 07 SP Telephone: 33-0-144 18 81 80 Fax: 33-0-144 18 82 00 Telex: SEGEDEFNAT 200019 Telegraphic address: SEGEDEFNAT PARIS

ИРЛАНДИЯ

National Security Authority Department of Foreign Affairs 80 St. Stephens Green Dublin 2 Telephone: 353-1-478 08 22 Fax: 353-1-478 14 84

ИТАЛИЯ

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza Via della Pineta Sacchetti, 216 I - 00168 Roma
Telephone: 39-06-627 47 75 Fax: 39-06-614 33 97 Telex: 623876 AQUILA 1
Telegraphic address: ess: PCM-ANS-UCSI-ROMA

ЛЮКСЕМБУРГ

Autorité Nationale de Sécurité Ministère d'État Boîte Postale 2379 L - 1023 Luxembourg Telephone: 352-478 22 10 central
352-478 22 35 direct
Fax: 352-478 22 43
352-478 22 71
Telex: 3481 SERET LU
Telegraphic address: MIN D'ETAT - ANS

НИДЕРЛАНДИЯ

Ministerie van Binnenlandse Zaken Postbus 20010 NL - 2500 EA Den Haag Telephone: 31-... Fax: 31-70-320 07 33 Telex: 32166 SYTH NL Ministerie van Defensie Militaire Inlichtingendienst (MID) Postbus 20701 NL - 2500 ES Den Haag Telephone: 31-70-318 70 60 Fax: 31-70-318 79 51

АВСТРИЯ

Bundesministerium für auswärtige Angelegenheiten Abteilung I.9 Ballhausplatz 2 A - 1014
Wien Telephone: 43-1-531 15 34 64 Fax: 43-1-531 8 52 19

ПОРТУГАЛИЯ

32001D0264 – ЦПР – редактиран

Presidência do Conselho de Ministros Autoridade Nacional de Segurança Avenida Ilha da Madeira, 1 P - 1449-004
Lisboa Telephone: 351-21-301 55 10
351-21-301 00 01 , extension 20 45 37
Fax: 351-21-302 03 50

ФИНЛАНДИЯ

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet Laivastokatu/Maringatan 22 PL/PB 176 FIN - 00161
Helsinki/Helsingfors Telephone: 358-9-13 41 53 38 Fax: 358-9-13 41 53 03

ШВЕЦИЯ

Utrikesdepartementet SSSB S - 103 39
Stockholm Telephone: 46-8-... Fax: 46-8-723 11 76

ОБЕДИНЕНО КРАЛСТВО

The Secretary (for DIR/5) PO Box 5656 London EC1A 1AH
Telephone: 44-... Fax: 44-20-76 30 14 28 Telegraphic address: UK Delegation to Security Policy Dept FCO, marked (in Box 5656 for DIR/5).

Допълнение 2

Национални класификации за сигурност на информацията - сравнение

Класификация на ЕС	Строго секретно за ЕС	Секретно за ЕС	Поверително за ЕС	За служебно ползване в ЕС
Класификация на НАТО[1]				
Класификация на ЗЕС	Строго секретно за ЗЕС	Секретно за ЗЕС	Поверително за ЗЕС	За служебно ползване в ЗЕС

[1] НАТО: съответствието с нивата на класификация на информацията на НАТО ще се определи след подписването на Споразумението за сигурност между Европейския съюз и НАТО.

Допълнение 3

Практическо ръководство за класификация на информацията

Ръководството е примерно и не бива да се разглежда като изменение на съществените разпоредби, предвидени в раздели II и III

Класификация	Кога	Кой	Маркировка	Понижаване/Премахване/Унищожаване	
				Кой	Кога
СТРОГО СЕКРЕТНО ЗА ЕС: Това ниво на класификация се прилага само за информация и материал, нерегламентирано-то разкриване на които би застрашило в изключително висока степен съществените интереси на Европейския съюз или на една или повече държави-членки [PII(1)].	Компрометирането на активи с маркировка СТРОГО СЕКРЕТНО ЗА ЕС: - би застрашило пряко вътрешната стабилност на ЕС или, на една от държавите-членки или на приятелски страни - би застрашило в изключително висока степен отношенията с приятелски правителства - би довело пряко до масови човешки жертви - би застрашило в изключително висока степен оперативната ефективност на сигурността на Държавите-членки или силите на други участници, или трайната ефективност на изключително важни операции в областта на сигурността или разузнаването - би застрашило във висока степен икономиката на ЕС или държавите-членки	държавите-членки: надлежно упълномощени лица (създатели на информацията) [PIII(4)]; ГСС: надлежно упълномощени лица (създатели на информацията) [PIII(4)], ГС/ВП и DSG Създателите на информацията посочват дата или срок, когато може да се понижи нивото на класификация на съдържанието или да се премахне класификацията. В противен случай те извършват преглед на документите най-малко веднъж на всеки пет години, за да гарантират необходимостта от запазване на оригиналното ниво на класификация. [PIII(10)];	Маркировката СТРОГО СЕКРЕТНО ЗА ЕС се поставя на документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС и в зависимост от случая се въвежда маркировката от отбраната ESDP чрез механични средства или на ръка [PII(8)]. Маркировката за ниво на класификация в ЕС се поставя горе и долу в средата на всяка страница и всяка страница се номерира. Всеки документ носи уникален идентификационен номер и дата; този номер се поставя на всяка страница. Когато се предоставят няколко копия от документа, за всяко копие се определя номер, който се поставя на първата страница заедно с общия брой страници. Всички анекси и приложения се изброяват на първата страница [PVII(1)].	Премахване или понижаване нивото на класификация зависи единствено от създателя на информацията, ГС/ВП или DSG, които информират за промяната всички последващи адресати, на които са изпратили или за които са копирали документа [PVIII(9)]. Документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС се унищожават от Централната регистратура или под-регистратурата, която отговаря за тях. За всеки унищожен документ се издава удостоверение за унищожаване, подписано от служителя по контрола за ниво СТРОГО СЕКРЕТНО ЗА ЕС и от служителя, присъствал на унищожаването, който е преминал през проучване за достъп до ниво СТРОГО СЕКРЕТНО ЗА ЕС. В този смисъл се прави вписване в дневника. Регистратурата съхранява удостоверенията за унищожаване заедно с формулярите на предоставените документи за срок от десет години [PVII(31)].	Излишните копия и ненужните документи задължително се унищожават [PVII(31)]. Документите с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, включително и всички класифицирани отпадъци в резултат на изготвянето на документи с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС като повредени копия, работни проекти, напечатани записки и индигови листове се унищожават под надзора на служителя о сигурността за ниво СТРОГО СЕКРЕТНО ЗА ЕС, чрез изгаряне, претопяване, нарязване на ивици или по друг начин, който ги превръща в негодни за разпознаване или възстановяване [PVII(31)].

Класификация	Кога	Кой	Маркировка	Понижаване/Премахване/Унищожаване	
				Кой	Кога
СЕКРЕТНО: Това ниво на класификация се прилага само за информация и материал, нерегламентирано-то разкриване на които би застрашило във висока степен съществените интереси на Европейския съюз или на една или повече държави-членки [PII(2)].	Компрометирането на активи с маркировка СЕКРЕТНО ЗА ЕС: - би повишило международното напрежение - би застрашило във висока степен отношенията с приятелски правителства - би застрашило пряко човешки живот или би застрашило във висока степен обществения ред или личната сигурност или свобода - би застрашило във висока степен оперативната ефективност на сигурността на държавите-членки или силите на други участници, или трайната ефективност на много важни операции в областта на сигурността или разузнаването - би застрашило във висока степен финансовите, монетарните, икономическите и търговските интереси на ЕС или една от държавите-членки	държавите-членки: упълномощени лица (създатели на информацията) [PIII(2)]; ГСС и децентрализиранит е агенции на ЕС: упълномощени лица (създатели на информацията) [PIII(2)], Генерални директори, ГС/ВП и DSG Създателите на информацията посочват дата или срок, когато може да се понижи нивото на класификация на съдържанието или да се премахне класификацията. В противен случай те извършват преглед на документите най-малко веднъж на всеки пет години, за да гарантират необходимостта от запазване на оригиналното ниво на класификация. [PVII(1)];	Маркировката СЕКРЕТНО ЗА ЕС се поставя на документи с ниво на класификация СЕКРЕТНО ЗА ЕС и в зависимост от случая се въвежда маркировката от отбраната ESDP чрез механични средства или на ръка [PIII(8)]. Маркировката за ниво на класификация в ЕС се поставя горе и долу в средата на всяка страница и всяка страница се номерира. Всеки документ носи уникален идентификационен номер и дата; този номер се поставя на всяка страница. Когато се предоставят няколко копия от документа, за всяко копие се определя номер, който се поставя на първата страница заедно с общия брой страници. Всички анекси и приложения се изброяват на първата страница [PVII(1)].	Премахване или понижаване нивото на класификация зависи единствено от създателя на информацията, ГС/ВП или DSG, които информират за промяната всички последващи адресати, на които са изпратили или за които са копирали документа [PVII(9)]. Документите с ниво на класификация СЕКРЕТНО ЗА ЕС се унищожават от регистратурата, която отговаря за тези документи под надзора на лице, преминало през проучване за надеждност от гледна точка на сигурността. Унищожените документи с ниво на класификация СЕКРЕТНО ЗА ЕС се вписват в подписано удостоверение за унищожаване, което се съхранява от регистратурата заедно с формулярите за унищожаване за срок най-малко от три години [PVII(32)].	Излишните копия и ненужните документи задължително се унищожават [PVII(31)]. Документите с ниво на класификация СЕКРЕТНО ЗА ЕС, включително и всички класифицирани отпадъци в резултат на изготвянето на документи с ниво на класификация СЕКРЕТНО ЗА ЕС като повредени копия, работни проекти, напечатани записки и индигови листове се унищожават чрез изгаряне, претопяване, нарязване на ивици или по друг начин, който ги превръща в негодни за разпознаване или възстановяване [PVII(31), (32)].

Класификация	Кога	Кой	Маркировка	Понижаване/Премахване/Унищожаване	
				Кой	Кога
ПОВЕРИТЕЛНО ЗА ЕС: Това ниво на класификация се прилага само за информация и материал, нерегламентирано-то разкриване на които би причинило вреди на съществените интереси на Европейския съюз или на една или повече държави-членки [PII(3)].	Компрометирането на активи с маркировка ПОВЕРИТЕЛНО ЗА ЕС: - би причинило сериозни вреди на дипломатическите отношения, т.е. би причинило официален протест или други санкции - би застрашило личната сигурност или свобода - би застрашило оперативната ефективност или сигурността на държавите-членки или силите на други участници, или ефективността на важни операции в областта на сигурността или разузнаването - би застрашило значително финансовата жизнеспособност на основните организации - би препятствало разследването или улеснило извършването на сериозни престъпления - би застрашило значително финансовите, монетарните, икономическите и търговските интереси на ЕС или държавите-членки - би препятствало във висока степен разработването или прилагането на основните политики на ЕС - би закрило или по друг начин би нарушило значително важни дейности на ЕС	държавите-членки: упълномощени лица (създатели на информацията) [PIII(2)]; ГСС и децентрализирани-те агенции на ЕС: упълномощени лица (създатели на информацията) [PIII(2)], Генерални директори, ГС/ВП и DSG Създателите на информацията посочват дата или срок, когато може да се понижи нивото на класификация на съдържанието или да се премахне класификацията. В противен случай те извършват преглед на документите най-малко веднъж на всеки пет години, за да гарантират необходимостта от запазване на оригиналното ниво на класификация. [PIII(10)];	Маркировката ПОВЕРИТЕЛНО ЗА ЕС се поставя на документи с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и в зависимост от случая се въвежда маркировката от отбраната ESDP чрез механични средства и на ръка или чрез отпечатване върху хартия с гриф за сигурност [PII(8)]. Маркировката за ниво на класификация в ЕС се поставя горе и долу в средата на всяка страница и всяка страница се номерира. Всеки документ носи уникален идентификационен номер и дата. Всички анекси и приложения се изброяват на първата страница [PVII(1)].	Премахване или понижаване нивото на класификация зависи единствено от създателя на информацията, ГС/ВП или DSG , които информират за промяната всички последващи адресати, на които са изпратили или за които са копирали документа [PVII(31)]. Документите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС се унищожават от регистратурата, която отговаря за тези документи, под надзора на лице, преминало през проучване за надеждност от гледна точка на сигурността. Унищожаването им се документира в съответствие с националните разпоредби, а когато става въпрос за ГСС или децентрализираните агенции на ЕС - в съответствие с указанията от ГС/ВП или DSG [PVII(33)].	Излишните копия и ненужните документи задължително се унищожават [PVII(31)]. Документите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС, включително и всички класифицирани отпадъци в резултат на изготвянето на документи с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС като повредени копия, работни проекти, напечатани записки и индигови листове се унищожават чрез изгаряне, претопяване, нарязване на ивици или по друг начин, който ги превръща в негодни за разпознаване или възстановяване [PVII(31), (33)].

Класификация	Кога	Кой	Маркировка	Понижаване/Премахване/Унищожаване	
				Кой	Кога
ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС: Това ниво на класификация се прилага само за информация и материал, нерегламентирано-то разкриване на които би се отразило неблагоприятно на интересите на Европейския съюз или на една или повече държави-членки [PII(4)].	Компрометирането на активи с маркировка ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС: - би се отразило неблагоприятно на дипломатическите отношения - би причинило значително страдание на отделни личности - би затруднило поддържането на оперативната ефективност или сигурността на държавите-членки или силите на други участници - би причинило финансови загуби или улеснило незаконната печалба или предимство за отделни личности или компании - би нарушило надлежно поети ангажименти за поддържане на доверието към информация, предоставена от трети страни - би нарушило законовите ограничения относно разкриването на информация - би препятствало разследването или би улеснило извършването на престъпления - би затруднило ЕС или държавите-членки при воденето на търговски или политически преговори с другите - би препятствало ефективното разработване или прилагане на политиките на ЕС - би застрашило правилното управление и дейността на ЕС	държавите-членки: упълномощени лица (създатели на информацията) [PIII(2)]; ГСС и децентрализирани-те агенции на ЕС: упълномощени лица (създатели на информацията) [PIII(2)], Генерални директори, ГС/ВП и DSG Създателите на информацията посочват дата или срок, когато може да се понижи нивото на класификация на съдържанието или да се премахне класификацията. В противен случай те извършват преглед на документите най-малко веднъж на всеки пет години, за да гарантират необходимостта от запазване на оригиналното ниво на класификация. [PIII(10)];	Маркировката ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС се поставя на документи с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС и в зависимост от случая се въвежда маркировката от отбраната ESDP чрез механични или електронни средства [PII(8)]. Маркировката за ниво на класификация в ЕС се поставя горе и долу в средата на всяка страница и всяка страница се номерира. Всеки документ носи уникален идентификационен номер и дата PVII(1)].	Премахване или понижаване нивото на класификация зависи единствено от създателя на информацията, ГС/ВП или DSG , които информират за промяната всички последващи адресати, на които са изпратили или за които са копирали документа [PIII(9)]. Документите с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС се унищожават от регистратурата, която отговаря за тези документи, в съответствие с националните разпоредби, а когато става въпрос за ГСС или децентрализираните агенции на ЕС - в съответствие с указанията от ГС/ВП или DSG [PVII(34)].	Излишните копия и ненужните документи задължително се унищожават [PVII(31)].

Допълнение 4

Инструкции за предоставяне на класифицирана информация на трети държави или международни организации

Първо ниво на сътрудничество

ПРОЦЕДУРИ

1. Правото за предоставяне на класифицирана информация на ЕС на страни, които не са подписали Договора за създаване на Европейския съюз, или на други международни организации, чиято политика и законодателство в областта на сигурността са сравними с тези на ЕС, принадлежи на Съвета.

2. Съветът може да предаде пълномощие за вземане на решение за предоставяне на класифицирана информация на ЕС. При предаването на пълномощия той посочва информация с какво естество може да бъде предоставена и на какво ниво на класификация, което обикновено не е по-високо от ПОВЕРИТЕЛНО ЗА ЕС.

3. Ако не е уговорено друго в споразумение за сигурността, молбите за предоставяне на класифицирана информация на ЕС се подават до генералния секретар/върховния представител от органите по сигурността на заинтересованите държави или международни организации, в които те посочват какво ще бъде предназначението на предоставената информация и какво е нейното естество.

Молби могат да се подават и от държава членка или децентрализирана агенция на ЕС, които считат че е желателно да бъде предоставена класифицирана информация на ЕС; те посочват целта и предимството за ЕС при предоставяне на такава информация, като уточняват естеството и нивото на класификация на информацията, за която са подали молба за предоставяне.

4. Молбата се разглежда от ГСС, който:

- се обръща за становище към държавата членка или, в зависимост от случая, към децентрализираната агенция, създала информацията;
- установява необходимите контакти с органите по сигурността на страните - бенефициенти или с международните организации, за да верифицира дали тяхната политика и законодателство в областта на сигурността могат да гарантират, че предоставената им информация ще бъде защитена в съответствие с изискванията на настоящите разпоредби относно сигурността;
- се обръща за техническо становище към Службите за сигурност на държавите членки по отношение на доверието, което Съветът може да има към държавите - бенефициенти или към международните организации.

5. ГСС изпраща молбата и препоръките на Службите за сигурност на Съвета за вземане на решение.

РАЗПОРЕДБИ ОТНОСНО СИГУРНОСТТА, КОИТО СЕ ПРИЛАГАТ ОТ БЕНЕФИЦИЕНТИТЕ

6. Генералният секретар/върховният представител уведомява държавите или международните организации-бенефициенти за решението на Съвета за предоставяне на класифицирана информация на ЕС като им изпраща толкова копия от настоящите разпоредби относно сигурността, колкото е преценил, че ще бъдат необходими. Ако молбата е била направена от държава-членка, тя уведомява бенефициента, че е разрешено предоставянето на информация.

Решението за предоставянето на информация влиза в сила само след като е дадено писмено уверение от бенефициентите, че:

- ще използват предоставената информация единствено за одобрената цел;
- ще осигурят защита на предоставената информация в съответствие с настоящите разпоредби относно сигурността и по-специално специалните разпоредби, дадени по-долу.

7. *Персонал*

а) Броят на висшите длъжностни лица с достъп до класифицирана информация на ЕС ще бъде строго ограничен като се спазва принципа „необходимост да се знае" и ще обхваща лицата, чиито служебни задължения изискват такъв достъп.

б) всички висши длъжностни лица или граждани на страната упълномощени за достъп до информация с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и по-високо ниво имат или удостоверение за сигурност за необходимото ниво или еквивалентно проучване за надеждност от гледна точка на сигурността и разрешение за достъп, и двете издадени от правителството на собствената им държава.

8. *Предаване на документи*

а) конкретните процедури по предаването на документите се определят чрез споразумение въз основа на разпоредбите на раздел VII на Разпоредбите на Съвета относно сигурността. Те по-специално определят регистратурите, на които следва да се изпраща класифицираната информация на ЕС.

б) ако в класифицираната информация, чието предоставяне е разрешено от Съвета, включва информация с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС, държавата или международната организация-бенефициент създават централна регистратура, а при необходимост, и под-регистратури на ЕС. Те се ръководят от разпоредбите на раздел VIII на настоящите разпоредби относно сигурността.

9. *Регистрация*

Веднага след получаването в регистратурата на класифицирана информация на ЕС с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС документът се вписва в специален регистър, воден от организацията, в който в отделни колони се попълват дата на получаване, конкретна информация за документа (дата, уникален идентификационен номер и номер на копието), ниво на класификация, заглавие, име или длъжност на получателя, дата на връщане на разписката и дата на връщане на документа на създателя му в ЕС или на унищожаване.

10. *Унищожаване*

а) класифицираните документи на ЕС се унищожават в съответствие с указанията, дадени в раздел VI на настоящите разпоредби относно сигурността. Копия от удостоверенията за унищожаване на документите с ниво на класификация СЕКРЕТНО ЗА ЕС и СТРОГО СЕКРЕТНО ЗА ЕС се изпращат на регистратурата в ЕС, която е била изпратила документите.

б) класифицираните документи на ЕС се включват в плановете за унищожаване при настъпване на необичайни обстоятелства на бенефициентите за собствените им класифицирани документи.

11. *Защита на документи*

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

12. *Копия, преводи и извлечения*

Не могат да се правят фотокопия или преводи на документите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и СЕКРЕТНО ЗА ЕС както и извлечения от тях без разрешението на ръководителя на заинтересованата организация по сигурността, който регистрира и проверява копията, преводите и извлеченията и поставя върху тях необходимата маркировка.

Възпроизводството на документ с ниво на класификация СТРОГО СЕКРЕТНО ЗА ЕС може да стане само с разрешението на създателя на документа, който посочва точния брой копия, за които е издал разрешение; когато не е възможно да се определи създателя на документа, молбата се отнася до службата за сигурност на ГСС.

13. Нарушения на сигурността

Когато е извършено нарушение на сигурността или има съмнения относно нарушение на сигурността по отношение на класифициран документ на ЕС, ако не е уговорено друго в споразумението за сигурност, незабавно се вземат следните мерки:

а) извършва се разследване, за да се установи при какви обстоятелства е настъпило нарушение на сигурността;

б) уведомяват се службата за сигурност на ГСС, Националния орган по сигурността и създателя на документа или когато последният не е бил уведомен, това изрично се посочва.

в) предприемат се действия за минимизиране на последствията от нарушението на сигурността;

г) отново се разглеждат и се прилагат мерки за предотвратяване на повторно нарушение;

д) прилагат се всички мерки, препоръчани от службата за сигурност на ГСС, за предотвратяване на повторно нарушение.

14. *Проверки*

Разрешено е на службата за сигурност на ГСС, по силата на споразумение със заинтересованите държави или международни организации, да извършва оценка на ефективността на мерките за защита на предоставена класифицирана информация на ЕС.

15. *Отчетност*

Ако не е уговорено друго в сключеното споразумение за сигурност, за периода, през който държавата или международната организация държи класифицирана информация на ЕС, тя следва да представя на дата, която се уточнява при издаването на разрешение за предоставяне на информация, годишен отчет в потвърждение на това, че са спазени настоящите разпоредби относно сигурността.

Допълнение 5

Инструкции за предоставяне на класифицирана информация на трети държави или международни организации

Второ ниво на сътрудничество

ПРОЦЕДУРИ

1. Правото за предоставяне на класифицирана информация на ЕС на държави или международни организации, чиято политика и законодателство в областта на сигурността чувствително се отличават от тези на ЕС, принадлежи на Съвета. Принципно това право е ограничено и обхваща информацията с ниво на класификация до и включително СЕКРЕТНО ЗА ЕС.; от него е изключена националната информация, специално запазена за държавите-членки, и категориите класифицирана информация на ЕС, защитена със специална маркировка.

2. Съветът може да делегира правото за вземане на решение за предоставяне на класифицирана информация на ЕС като при предаването на пълномощия, в рамките на ограниченията по смисъла на параграф 1, той посочва информация с какво естество може да бъде предоставена и на какво ниво на класификация, което обикновено не е по-високо от ПОВЕРИТЕЛНО ЗА ЕС.

3. Ако не е уговорено друго в споразумението за сигурността, молбите за предоставяне на класифицирана информация на ЕС се подават до генералния секретар/върховния представител от органите по сигурността на заинтересованите държави или международни организации, в които те посочват какво ще бъде предназначението на предоставената информация и какво е нейното естество.

Молби могат да се подават и от държава членка или децентрализирана агенция на ЕС, които считат че е желателно да бъде предоставена класифицирана информация на ЕС; те посочват целта и **предимството** за ЕС при предоставяне на такава информация, като уточняват естеството и нивото на класификация на информацията, за която са подали молба за предоставяне.

4. Молбата се разглежда от ГСС, който:

- се обръща за становище към държавата- членка или, в зависимост от случая, към децентрализираната агенция, създали информацията, **която ще бъде предоставена;**
- установява предварителни контакти с органите по сигурността на страните или международните организации - бенефициенти, за да открие информация за тяхната политика и законодателство в областта на сигурността и по-специално за да изготви сравнителна таблица на нивата на класификация, приложими в ЕС и в заинтересованата държава или организация;
- организира заседание на Комитета по сигурността на Съвета или, съгласно процедурата за изразяване на съгласие чрез мълчание при необходимост, се обръща със запитване към националните органи по сигурността на държавите членки с оглед да получи техническото становище на Комитета по сигурността.

5. Техническото становище на Комитета по сигурността на Съвета се отнася за следното:

- доверието, което може да се окаже на държавите или международните организации - бенефициенти, с оглед на преценяването на рисковете за сигурността на ЕС или държавите-членки,
- оценката на способността на бенефициентите да защитят класифицираната информация, предоставена от ЕС,
- предложенията за конкретните процедури по обработката на предадената класифицирана информация на ЕС (например предоставяне на цензурирани варианти) и документи (запазване или заличаване на означенията за ниво на класификация, специална маркировка и т.н.),
- понижаване или премахване на нивото на класификация от създателя на информацията преди тя да се предостави на страните или международните организации - бенефициенти[(1)].

6. Генералният секретар/върховният представител изпраща на Съвета за решение молбата и техническото становище на Комитета по сигурността, получено в службата за сигурност на Съвета.

РАЗПОРЕДБИ ОТНОСНО СИГУРНОСТТА, КОИТО СЕ ПРИЛАГАТ ОТ БЕНЕФИЦИЕНТИТЕ

7. Решението на Съвета относно даването на разрешение за предоставяне на класифицирана информация на ЕС се свежда до вниманието на страните или международните организации - бенефициенти от генералният секретар/върховният представител заедно със сравнителната таблица на нивата на класификация, приложими в рамките на ЕС, и в заинтересованите стари или международни организации. Ако молбата е била направена от държава-членка, тя уведомява бенефициента, че е разрешено предоставянето на информация.

Решението за предоставянето на информация влиза в сила само след като е дадено писмено уверение от бенефициентите, че:

- ще използват предоставената информация единствено за одобрената цел;
- ще осигурят защита на предоставената информация в съответствие с разпоредбите, определени от Съвета.

8. Създават се следните правила за защита, освен ако Съветът, след като е получил техническото становище на Комитета по сигурността на Съвета, не е взел решение за прилагането на конкретна процедура за обработката на класифицирани документи на ЕС (заличаване на нивото на класификация, специална маркировка и т.н.).

В такъв случай се прави адаптиране на правилата.

9. Персонал

а) Броят на висшите длъжностни лица с достъп до класифицирана информация на ЕС трябва да бъде строго ограничен като се спазва принципа „необходимост да се знае” и да обхваща лицата, чиито служебни задължения изискват такъв достъп.

[(1)] В случая от създателя на информацията се изисква да приложи процедурата, определена в параграф 9, раздел III, когато всички копия се разпространяват в рамките на ЕС.

б) Всички висши длъжностни лица или граждани на страната, упълномощени за достъп до класифицираната информация, предоставена от ЕС, имат направено проучване за надеждност от гледна точка на сигурността от правителството на собствената им държава или издадено от него разрешение за достъп, когато става въпрос за национална класифицирана информация, до необходимото ниво, съответно на това за ЕС по смисъла на сравнителната таблица.

в) Проучването за надеждност от гледна точка на сигурността, направено от правителството на собствената им държава, или издадено от него разрешение за достъп се изпраща на генералния секретар/върховния представител за сведение.

10. Предаване на документи

а) Конкретните процедури по предаването на документите се съгласуват между службата за сигурност на ГСС и органите по сигурността на държавите или международните организации - получатели въз основа на правилата, определени в раздел VII на настоящите разпоредби. Те по-специално определят точните адреси, на които трябва да бъдат изпратени документите както и куриерската служба или пощенските услуги, които се използват за предаването на класифицирана информация на ЕС.

б) Документите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и по-високо от това ниво се предават в два плика, поставени един в друг. На вътрешния плик се поставя маркировката „ЕС” за едно с обозначението за ниво на класификацията. За всеки класифициран документ се прилага разписка. Разписката, която не е класифицирана, съдържа само конкретни данни за документа (уникален идентификационен номер на документа, дата, номер на копието) и езикът, на който е създаден, но не и заглавието на документа.

в) Вътрешният плик се поставя във външен плик, върху който е отбелязан номерът на пакета, записан в разписката. Нивото на класификация не се обозначава върху външния плик.

г) Куриерите винаги получават разписка, в която е отбелязан номерът на пакета.

11. *Входяща регистрация*

Адресатът, ОНС или равностоен орган в държавата, който получава от името на правителството класифицирана информация, изпратена от ЕС, или бюрото по сигурността на международната организация, получател на информация, откриват специален регистър за вписване на класифицираната информация на ЕС при получаването ѝ. Регистърът има колони, в който се попълват дата на получаване, конкретни данни за документа (дата, уникален идентификационен номер и номер на копието), ниво на класификация, заглавие, име или длъжност на получателя, дата на връщане на разписката и дата на връщане на документа в ЕС или на унищожаване.

12. *Връщане на документи*

Когато получателят връща класифициран документ на Съвета или държавата-членка, която е предоставила документа, се процедира съгласно указаното в параграф 10.

13. *Защита*

а) Когато документите не се използват, те се съхраняват в сейф, одобрен за съхраняване на материал с национална класификация на същото ниво. Върху сейфа не е обозначено съдържанието му, до което имат достъп единствено лицата, упълномощени да обработват класифицирана информация на ЕС. При използването на брави с комбинации, комбинациите са известни само на висшите длъжностни лица в държавата или организацията, които имат разрешение з достъп до класифицираната информация на ЕС, съхранявана в сейфа, и се променят на всеки шест месеца или по-често в случай на прехвърляне на висш чиновник, отменяне на разрешението за достъп на един от висшите длъжностни лица, които знаят комбинацията или когато е налице опасност от компрометиране на информацията.

б) Класифицирани документи на ЕС се преместват от сейфа само от висшите длъжностни лица, които имат разрешение за достъп до класифицирани документи на ЕС при спазване на принципа „необходимост да се знае”. Те носят отговорност за безопасното съхраняване на документите докато се намират при тях и по-специално за гарантирането, че неупълномощени лица нямат достъп до документите. Те също гарантират, че документите се съхраняват в сейф след като са приключили работата си с тях и в извън работно време.

в) Не се разрешава правенето на фотокопия на документи с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и по-високо ниво, нито изготвянето на извлечения от тях, без разрешението на службата за сигурност на ГСС.

г) Определя се и се потвърждава от службата за сигурност на ГСС процедура за бързо и пълно унищожаване на документи при настъпване на извънредни обстоятелства.

14. *Физическа сигурност*

а) Когато не се използват, сейфовете, в които се съхраняват класифицирани документи на ЕС, се държат заключени през цялото време.

б) Когато се налага членове на персонала по поддръжката или почистването да влизат или работят в стая, където се намират сейфове, те се придружават през цялото време от служители на службата за сигурност на държавата или организацията или от висшия чиновник, който специално отговаря за надзора над сигурността на помещението.

в) Извън нормалното работно време (през нощта, в края на седмицата и на национални празници) защитата на сейфовете, в които се намират класифицирани документи на ЕС, се осигурява от охрана или от автоматична алармена система.

15. *Нарушения на сигурността*

Когато е извършено нарушение на сигурността или има съмнения относно нарушение на сигурността по отношение на класифициран документ на ЕС, незабавно се вземат следните мерки:

а) незабавно се изпраща доклад на службата за сигурност на ГСС или ОНС на държавата-членка, по чиято инициатива е изпратен документа (с копие до службата за сигурност на ГСС);

б) извършва се разследване, след приключването на което се представя пълен доклад на органа по сигурността (виж а) по-горе). След това се приемат изправителни мерки;

16. *Проверки*

Разрешено е на службата за сигурност на ГСС, по силата на споразумение със заинтересованите държави или международни организации, да извършва оценка на ефективността на мерките за защита на предоставена класифицирана информация на ЕС.

17. *Отчетност*

За периода, през който държавата или международната организация държи класифицирана информация на ЕС, тя следва да представя на дата, която се уточнява при издаването на разрешение за предоставяне на информация, годишен отчет в потвърждение на това, че са спазени настоящите разпоредби относно сигурността.

Допълнение 6

Инструкции за предоставяне на класифицирана информация на трети държави или международни организации

Трето ниво на сътрудничество

ПРОЦЕДУРИ

1. Понякога Съветът може да поиска да сътрудничи при определени специални обстоятелства с държави или организации, които не могат да предоставят уверенията, изисквани от настоящите разпоредби относно сигурността, но при такова сътрудничество може да се поиска предоставяне на класифицирана информация на ЕС. От него е изключена националната информация, специално запазена за държавите-членки.

2. При такива специални обстоятелства молбите за сътрудничество с ЕС, независимо дали са подадени от трети държави или международни организации или са по предложение на държавите-членки, а в зависимост от обстоятелствата, и от децентрализирана агенция на ЕС, най-напред се разглеждат по същество от Съвета, който при необходимост, се обръща към държавите-членки или децентрализираните агенции, създатели на информацията, за становище. Съветът обсъжда разумно ли е да се предостави класифицирана информация, прави оценка на бенефициента при спазване на принципа „необходимост да се знае" и взема решение относно естеството на класифицираната информация която може да се предостави.

3. При положителен отговор от Съвета, генералният секретар/върховният представител е отговорен за свикването на Комитета по сигурността на Съвета или за запитване на Националните органи по сигурността на държавите членки, като при необходимост използва процедурата за изразяване на съгласие чрез мълчание, с оглед да получи техническото становище на Комитета по сигурността.

4. Техническото становище на Комитета по сигурността на Съвета се отнася за следното:

а) преценяването на рисковете за сигурността на ЕС или държавите-членки;

б) нивото на класификация на информацията, която може да бъде предоставена, в зависимост от случая, предвид на нейното естество;

в) понижаване или премахване на нивото на класификация на информацията от създателя на информацията преди тя да се предостави на заинтересованите страни или международни организации[(1)].

г) процедури по обработката на документите, които ще бъдат предоставени (виж параграф 5 по-долу);

д) възможните методи за пренасяне на информацията (използване на държавни пощенски услуги, държавни или сигурни телекомуникационни системи, дипломатическа поща, куриери, преминали през проверка за надеждност от гледна точка на сигурността и др.).

[(1)] В случая от създателя на информацията се изисква да приложи процедурата, определена в параграф 9, раздел III, когато всички копия се разпространяват в рамките на ЕС.

5. Документите, които се предоставят на държавите и организациите, разгледани в настоящото допълнение, по принцип се изготвят без да съдържат позоваване на техния източник или нивото им на класификация в ЕС. Комитетът по сигурността на Съвета може да препоръча:

- използването на специална маркировка или кодово име;

- използването на специфична система на класификация, която обвързва чувствителността на информацията с контролните мерки, които бенефициентът е задължен да прилага по отношение на начина на предаване на документите (виж примерите в параграф 14).

6. Службата за сигурност на ГСС предоставя на Съвета техническото становище на Комитета по сигурността като при необходимост прилага предложенията за предаване на правомощия, необходими за изпълнението на задачите, по-специално при неотложни обстоятелства.

7. След като Съветът одобри предоставянето на класифицирана информация на ЕС и конкретните процедури по изпълнението, службата за сигурност на ГСС установява необходимия контакт с органа по сигурността на заинтересованата държава или организация с цел да улесни прилагането на предвидените мерки за сигурност.

8. Службата за сигурност на ГСС разпраща като препоръка на всички държави-членки, а в зависимост от случая, и на заинтересованите децентрализирани агенции на ЕС таблица с обобщените данни за естеството и нивото на класификация на информацията и списък на организациите и страните, на които може да бъде предоставена в резултат на решение на Съвета.

9. ОНС на държавата-членка, която предоставя информацията, или службата за сигурност на ГСС, предприема всички необходими мерки, за да улесни извършването на оценка на възможните последващи вреди и преглед на процедурите.

10. При настъпване на промени в условията за сътрудничество се прави допълнително отнасяне към Съвета.

РАЗПОРЕДБИ ОТНОСНО СИГУРНОСТТА, КОИТО СЕ ПРИЛАГАТ ОТ БЕНЕФИЦИЕНТИТЕ

11. Решението на Съвета относно даването на разрешение за предоставяне на класифицирана информация на ЕС се свежда до вниманието на страните или международните организации - бенефициенти от генералният секретар/върховният представител заедно с подробните правила за защита, предложени от Комитета по сигурността на Съвета и одобрени от Съвета. Ако молбата е била направена от държава-членка, тя уведомява бенефициента, че е разрешено предоставянето на информация.

Решението за предоставянето на информация влиза в сила само след като е дадено писмено уверение от бенефициентите, че:

- ще използват предоставената информация единствено за целите на сътрудничеството, одобрено от Съвета;
- ще осигурят защита на предоставената информация в съответствие с изискванията на Съвета.

12. Предаване на документи

а) Конкретните процедури по предаването на документите се съгласуват между службата за сигурност на ГСС и органите по сигурността на държавите или международните организации - получатели. Те по-специално определят точните адреси, на които трябва да бъдат изпратени документите.

б) Документите с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС и по-високо от това ниво се предават в два плика, поставени един в друг. На вътрешния плик се поставя специфично обозначение или определено кодово име както и обозначение за предоставеното ниво на класификация на документа. За всеки класифициран документ се прилага разписка. Разписката, която не е класифицирана, съдържа само конкретни данни за документа (уникален идентификационен номер на документа, дата, номер на копието) и езикът, на който е създаден, но не и заглавието на документа.

в) Вътрешният плик се поставя във външния плик, върху който е отбелязан номерът на пакета, записан в разписката. Нивото на класификация не се обозначава върху външния плик.

г) Куриерите винаги получават разписка, в която е отбелязан номерът на пакета.

13. *Входяща регистрация*

Адресатът, ОНС или равностоен орган в държавата, който получава от името на правителството класифицираната информация, изпратена от ЕС, или бюрото по сигурността на международната организация, получател на информацията, откриват специален регистър за вписване на класифицираната информация на ЕС при получаването ѝ. Регистърът има колони, в който се попълват дата на получаване, конкретни данни за документа (дата, уникален идентификационен номер и номер на копието), ниво на класификация на документа, заглавие, име или длъжност на получателя, дата на връщане на разписката на ЕС и дата на унищожаване на документа.

14. *Използване и защита на обменената класифицирана информация*

а) Информацията с ниво на класификация СЕКРЕТНО ЗА ЕС се обработва от специално определени висши длъжностни лица, упълномощени за достъп до информация с това ниво на класификация. Информацията се съхранява в защитени шкафове с добро качество, които могат да бъдат отваряни само от лицата, упълномощени за достъп до информацията, която се съдържа в тях. Зоните, в които се намират шкафовете, се охраняват непрекъснато и се създава система за проверка, чрез която се гарантира, че влизането в зоната е разрешено само за надлежно упълномощени лица. Информацията с ниво на класификация СЕКРЕТНО ЗА ЕС се изпраща чрез дипломатическа поща, сигурни пощенски услуги и сигурни телекомуникационни средства. Документ с ниво на класификация СЕКРЕТНО ЗА ЕС може да се копира само с писменото съгласие на органа, създал документа. Всички копия се регистрират и проследяват. За всички операции, свързани с документи с ниво на класификация СЕКРЕТНО ЗА ЕС, се издават разписки.

б) Информацията с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС се обработва от специално определени висши длъжностни лица, упълномощени да бъдат информирани по темата. Документите се съхраняват в заключени защитени шкафове в контролирани зони.

Информацията с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС се изпраща чрез дипломатическа поща, сигурни пощенски служби и сигурни

телекомуникационни средства. Могат да се правят копия от органа - получател като в специални регистри се вписва техният брой и на кого са предоставени.

в) Информацията с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС се обработва в помещения, до които неупълномощеният персонал няма достъп и се съхранява в заключени сейфове. Документите могат да се изпращат чрез държавните пощенски служби като препоръчани писма в два плика, поставени един в друг, а при настъпване на извънредни обстоятелства по време на операция - чрез незащитените държавни телекомуникационни системи. Могат да се правят копия от получателите.

г) Не се изискват специални мерки за защита на некласифицирана информация и тя може да се изпраща по пощата и чрез държавните телекомуникационни системи. Могат да се правят копия от адресатите.

15. Унищожаване

Документите, които вече не са необходими, задължително се унищожават. За документите с ниво на класификация ЗА СЛУЖЕБНО ПОЛЗВАНЕ В ЕС и ПОВЕРИТЕЛНО ЗА ЕС се прави надлежно вписване в специалните регистри. За документите с ниво на класификация СЕКРЕТНО ЗА ЕС се издават удостоверения за унищожаване, които се подписват от две лица, присъствали на унищожаването.

16. *Нарушения на сигурността*

Когато е налице компрометиране или подозрение за компрометиране на информация с ниво на класификация ПОВЕРИТЕЛНО ЗА ЕС или СЕКРЕТНО ЗА ЕС, ОНС на държавата или ръководителят на сигурността в организацията извършва разследване на обстоятелствата, при които е настъпило компрометиране на информацията. При положителен резултат от разследването се уведомява органът, създал информацията. Предприемат се стъпки, необходими за коригиране на несъответстващите процедури или начини на съхранение, ако те са породили компрометиране на информацията. генералният секретар/върховният представител на Съвета или ОНС на държавата-членка, която е предоставила компрометираната информация, могат да поискат от бенефициента подробна информация за разследването.