32001D0264

L 101/1 *EUROPOS BENDRIJŲ OFICIALUSIS LEIDINYS* 2001 4 11

TARYBOS SPRENDIMAS
2001 m. kovo 19 d.
dėl Tarybos saugumo nuostatų patvirtinimo

(2001/264/EB)

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Europos bendrijos steigimo sutartį, ypač į jos 207 straipsnio 3 dalį,

atsižvelgdama į 2000 m. birželio 5 d. Tarybos sprendimą 2000/396/EB, EAPB, Euratomas, nustatantį Tarybos darbo tvarkos taisykles [1], ypač į jo 24 straipsnį,

kadangi:

(1) Siekiant plėtoti Tarybos veiklą tose srityse, kuriose reikalingas tam tikras konfidencialumo laipsnis, tikslinga sukurti plačią, Tarybą, jos Generalinį sekretoriatą ir valstybes nares apimančią saugumo sistemą.

(2) Ši sistema turėtų sujungti į vieną tekstą visų ankstesnių šios srities sprendimų ir nuostatų turinį.

(3) Praktiškai didžioji dalis ES KONFIDENCIALIAI ir aukštesnio slaptumo žymos laipsnio įslaptintos ES informacijos yra susijusi su bendra saugumo ir gynybos politika.

(4) Siekiant užtikrinti sukurtos saugumo sistemos veiksmingumą, valstybės narės turėtų padėti jai veikti, nacionaliniu lygmeniu imdamosi būtinų priemonių, kad jų kompetentingoms institucijoms ir tarnautojams tvarkant įslaptintą ES informaciją, būtų laikomasi šio sprendimo nuostatų.

(5) Taryba pritaria Komisijos ketinimui iki šio sprendimo įsigaliojimo dienos įdiegti visaapimančią, jo priedus atitinkančią sistemą, kad būtų užtikrintas sklandus Sąjungos sprendimų priėmimo procesas.

(6) Taryba pabrėžia, jog svarbu, kad Europos Parlamentas ir Komisija prireikus prisidėtų prie konfidencialumo taisyklių ir standartų, būtinų siekiant apsaugoti Sąjungos ir jos valstybių narių interesus, įgyvendinimo.

(7) Šis sprendimas priimamas nepažeidžiant Sutarties 255 straipsnio ir jo įgyvendinimo aktų.

(8) Šis sprendimas priimamas nepažeidžiant dabartinės valstybių narių praktikos, susijusios su nacionalinių parlamentų informavimu apie Sąjungos veiklą,

NUSPRENDĖ:

1 straipsnis

Šiuo sprendimu patvirtinami Priede pateikiami Tarybos saugumo nuostatai.

2 straipsnis

1. Generalinis sekretorius – vyriausiasis įgaliotinis imasi reikalingų priemonių, kad užtikrintų, jog, tvarkydami įslaptintą ES informaciją, Tarybos Generalinio sekretoriato (toliau – TGS) pareigūnai ir kiti tarnautojai, TGS samdyti rangovai ir į TGS deleguoti darbuotojai laikytųsi 1 straipsnyje nurodytų nuostatų tiek Sekretoriate, tiek Tarybos patalpose ir ES decentralizuotose agentūrose [2].

[1] OL L 149, 2000 6 23, p. 21.

[2] Žr. 2000 m. lapkričio 10 d. Tarybos išvadas.

2. Vadovaudamosi nacionalinės teisės aktais, valstybės narės imasi reikiamų priemonių, kad užtikrintų, jog bus laikomasi 1 straipsnyje nurodytų nuostatų, jų tarnybose ar patalpose įslaptintą ES informaciją tvarkant šiems asmenims:

a) valstybių narių nuolatinių atstovybių Europos Sąjungoje nariams, taip pat Tarybos arba jos organų posėdžiuose ar kitoje Tarybos veikloje dalyvaujantiems nacionalinių delegacijų nariams;

b) kitiems įslaptintą ES informaciją tvarkantiems valstybių narių nacionalinių administracijų nariams, nepriklausomai nuo to, ar jie dirba valstybės narės teritorijoje, ar užsienyje;

c) įslaptintą ES informaciją tvarkantiems valstybių narių samdytiems rangovams ir deleguotiems darbuotojams.

Valstybės narės nedelsdamos informuoja TGS apie priemones, kurių yra imtasi.

3. Šio straipsnio 1 ir 2 dalyse nurodytų priemonių turi būti imtasi iki 2001 m. lapkričio 30 d.

3 straipsnis

Laikydamasis priedo I dalyje išdėstytų pagrindinių saugumo principų ir minimalių standartų, Generalinis sekretorius – vyriausiasis įgaliotinis gali imtis priedo II dalies I skyriaus 1 ir 2 punktuose numatytų priemonių.

4 straipsnis

Nuo jo taikymo dienos šis sprendimas pakeičia:

a) 1998 m. balandžio 27 d. Tarybos sprendimą 98/319/EB dėl galimybės naudotis Tarybos turima įslaptinta informacija suteikimo Tarybos Generalinio Sekretoriato pareigūnams ir darbuotojams tvarkos [1];

b) 2000 m. liepos 27 d. Generalinio sekretoriaus – vyriausiojo įgaliotinio sprendimą dėl Tarybos Generaliniam sekretoriatui taikytinų įslaptintos informacijos apsaugos priemonių [2];

c) 1997 m. gegužės 22 d. Tarybos Generalinio Sekretoriaus sprendimą 443/97 dėl asmens patikimumo pažymėjimo už *Cortesy* tinklo veikimą atsakingiems pareigūnams tvarkos.

5 straipsnis

1. Šis sprendimas įsigalioja jo paskelbimo dieną.

2. Jis taikomas nuo 2001 m. gruodžio 1 d.

Priimta Briuselyje, 2001 m. kovo 19 d.

Tarybos vardu

Pirmininkė

A. LINDH

[1] OL L 140, 1998 5 12, p. 12.
[2] OL C 239, 2000 8 23, p. 1.

PRIEDAS

EUROPOS SĄJUNGOS TARYBOS SAUGUMO NUOSTATAI

TURINYS

Puslapis

Priedėliai

I DALIS

PAGRINDINIAI SAUGUMO PRINCIPAI IR MINIMALŪS STANDARTAI

ĮVADAS

1. Šie nuostatai nustato pagrindinius saugumo principus ir minimalius standartus, kurių Taryba, Tarybos Generalinis sekretoriatas (toliau – TGS), valstybės narės ir Europos Sąjungos decentralizuotos agentūros (toliau – ES decentralizuotos agentūros) turi deramai laikytis, kad būtų garantuotas saugumas ir kad kiekvienas būtų užtikrintas, jog pasiektas bendras saugumo lygis.

2. „ES įslaptinta informacija“ – bet kokia informacija ir medžiaga, kurią atskleidus be leidimo, gali būti padaryta įvairaus laipsnio žalos ES interesams arba vienai ar daugiau jos valstybių narių, nepriklausomai nuo to, ar tokios informacijos šaltinis yra pačioje ES, ar ji gauta iš valstybių narių, trečiųjų šalių ar tarptautinių organizacijų.

3. Šiuose nuostatuose:

   a) „dokumentas“ – bet koks laiškas, užrašas, protokolas, ataskaita, memorandumas, signalas (pranešimas), eskizas, nuotrauka, skaidrė, fotojuosta, žemėlapis, schema, užrašų knygelė, trafaretas, nuorašams naudotas kalkinis popierius, rašomosios mašinėlės ar spausdintuvo juostelė, magnetofono juostelė, kasetė, kompiuterio diskas, kompaktinis diskas ar kitokia fizinė laikmena, kurioje įrašyta informacija;

   b) „medžiaga“ – a papunktyje apibrėžtas dokumentas, taip pat bet kokia jau pagaminta arba gaminama įranga ar ginkluotė.

4. Svarbiausi saugumo tikslai yra:

   a) apsaugoti įslaptintą ES informaciją nuo šnipinėjimo, neteisėto atskleidimo arba platinimo be leidimo;

   b) apsaugoti ryšių ir informacijos sistemose bei tinkluose tvarkomą ES įslaptintą informaciją nuo grėsmės jos vientisumui ir prieinamumui;

   c) apsaugoti įrangą, kurioje laikoma ES informacija, nuo sabotažo ir tyčinio žalojimo;

   d) pažeidimo atveju įvertinti padarytą žalą, apriboti jos padarinius ir imtis būtinų jos pašalinimo priemonių.

5. Patikimo saugumo pagrindas yra:

   a) kiekvienoje valstybėje narėje – nacionalinė saugumo organizacija, atsakinga už:

      i) žvalgybinės informacijos apie šnipinėjimą, sabotažą, terorizmą ir kitokią ardomąją veiklą rinkimą ir registravimą;

      ii) informacijos ir patarimų apie grėsmės saugumui pobūdį ir apsaugos nuo jos priemones teikimą savo Vyriausybei, o per ją – Tarybai;

   b) kiekvienoje valstybėje narėje ir TGS – techninė INFOSEC institucija, kuri, bendradarbiaudama su atitinkama saugumo institucija, atsako už informacijos ir patarimų dėl techninių grėsmių saugumui bei apsaugos nuo jų priemonių teikimą;

   c) nuolatinis Vyriausybinių institucijų ir agentūrų bei atitinkamų TGS tarnybų bendradarbiavimas, kad prireikus būtų nustatyta ir rekomenduota:

      i) kokia informacija, ištekliai ar įranga turi būti saugoma;

      ii) bendri apsaugos standartai.

6. Kad būtų užtikrintas konfidencialumas, atrenkant dėl slaptumo saugotiną informaciją bei medžiagą ir įvertinant, koks turi būti jos apsaugos laipsnis, reikalingas atidumas ir patirtis. Labai svarbu, kad saugotinos informacijos ir medžiagos apsaugos laipsnis atitiktų jų svarbą saugumo požiūriu. Siekiant užtikrinti sklandų informacijos judėjimą, imamasi veiksmų pernelyg dideliam įslaptinimui išvengti. Įslaptinimo sistema – šių principų įgyvendinimo priemonė; numatant ir organizuojant kovos su šnipinėjimu, sabotažu, terorizmu ir kitokiomis grėsmėmis veiksmus reikia laikytis panašios įslaptinimo sistemos, kad labiausiai apsaugotos būtų svarbiausios patalpos, kuriose laikoma įslaptinta informacija, ir lengviausiai pažeidžiamos vietos jose.

PAGRINDINIAI PRINCIPAI

7. **Saugumo priemonės:**

a) taikomos visiems galintiems naudotis įslaptinta informacija asmenims, įslaptintos informacijos laikmenoms, visoms patalpoms, kuriose laikoma tokia informacija, ir svarbiai įrangai;

b) sukuriamos, kad būtų galima nustatyti asmenis, kurių būklė gali kelti grėsmę įslaptintos informacijos ir svarbios įrangos, kurioje laikoma įslaptinta informacija, saugumui, ir numato galimybę juos nušalinti ar atleisti;

c) neleidžia jokiam leidimo neturinčiam asmeniui naudotis įslaptinta informacija arba įranga, kurioje tokia informacija laikoma;

d) užtikrina įslaptintos informacijos skleidimą tik pagal visiems saugumo aspektams svarbiausią „būtina žinoti“ principą;

e) užtikrina visos, tiek įslaptintos, tiek neįslaptintos, ir ypač elektromagnetine forma laikomos, apdorotos arba perduotos informacijos vientisumą (t. y., užkerta kelią klastojimui arba taisymui ar ištrynimui be leidimo) ir galimybę ja naudotis (t. y., naudotis informacija nėra uždraudžiama tiems, kuriems yra būtina ir leista ja naudotis).

APSAUGOS ORGANIZAVIMAS

Bendri minimalūs standartai

8. Taryba ir kiekviena valstybė narė užtikrina, kad visos administracinės ir (arba) Vyriausybės institucijos ar padaliniai, kitos ES institucijos, agentūros ir rangovai, laikysis bendrų minimalių saugumo standartų, kad įslaptinta ES informacija būtų perduodama įsitikinus, kad ji bus taip pat atsakingai tvarkoma. Prie tokių minimalių standartų priskiriami patikimumo pažymėjimų išdavimo personalui kriterijai ir įslaptintos ES informacijos apsaugos procedūros.

PERSONALO TIKRINIMAS

Leidimų išdavimas darbuotojams

9. Visi asmenys, kuriems reikia turėti galimybę naudotis informacija, pažymėta ES KONFIDENCIALIAI arba aukštesnio laipsnio slaptumo žyma, prieš suteikiant jiems tokią galimybę yra tinkamai patikrinami. Panašiai patikrinti reikalaujama ir asmenis, į kurių pareigas įeina ryšių ir informacinių sistemų, kuriose laikoma įslaptinta informacija, techninis valdymas ar priežiūra. Toks tikrinimas turi leisti nustatyti, ar tie asmenys:

a) yra neabejotinai lojalūs;

b) yra tokio charakterio ir tokie diskretiški, kad nekyla abejonių dėl jų sąžiningumo tvarkant įslaptintą informaciją;

c) gali pasiduoti užsienio arba kitų šaltinių spaudimui, pvz., dėl savo ankstesnės gyvenamosios vietos ar galinčių kelti grėsmę saugumui praeities ryšių.

Ypač atidžiai turi būti tikrinami asmenys,

d) kuriems bus suteikta galimybė naudotis slaptumo žyma ES VISIŠKAI SLAPTAI pažymėta informacija;

e) einantys pareigas, kurios reikalauja nuolat naudotis dideliu kiekiu slaptumo žyma ES SLAPTAI pažymėtos informacijos;

f) kurių pareigos suteikia jiems išskirtinę galimybę naudotis ypač svarbiomis ryšių ar informacinėmis sistemomis, kartu ir galimybę be leidimo naudotis dideliu kiekiu įslaptintos ES informacijos arba techninio sabotažo veiksmais smarkiai pakenkti užduočių vykdymui.

Esant šio punkto d, e ir f papunkčiuose nurodytoms aplinkybėms reikėtų kiek tik įmanoma panaudoti operatyvinius tyrimo metodus.

10. Kai asmenys, kurių atžvilgiu negalima remtis „būtina žinoti“ principu, turi būti įdarbinti tokioje aplinkoje, kurioje jie galėtų naudotis įslaptinta ES informacija (pvz., pasiuntiniai, apsaugos darbuotojai, techninės priežiūros personalas, valytojai ir kt.), jie pirmiausia turi būti tinkamai patikrinami saugumo požiūriu.

Asmens patikimumo pažymėjimų registravimas

11. Visos tarnybos, institucijos ir įstaigos, tvarkančios įslaptintą ES informaciją arba turinčios ypatingos svarbos ryšių ar informacines sistemas, registruoja tam paskirtam personalui išduotus asmens patikimumo pažymėjimus. Kiekvienas pažymėjimas prireikus tikrinamas, kad būtų užtikrinta, jog jis atitinka dabartines to asmens funkcijas; jie pakartotinai tikrinami prioritetine tvarka, jei gaunama naujos informacijos, kad tolesnis paskyrimas darbui su įslaptinta informacija nebeatitinka saugumo. Patikimumo pažymėjimų registrą veda tarnybos, institucijos ar įstaigos apsaugos viršininkas.

Personalo saugumo instruktažas

12. Galimybes naudotis įslaptinta informacija sudarančias pareigas einantys darbuotojai pradėdami eiti pareigas ir reguliariai vėliau saugumo sumetimais išsamiai instruktuojami apie saugumo būtinybę ir priemones jam užtikrinti. Pageidautina, kad kiekvienas darbuotojas raštu patvirtintų, jog visiškai suvokia jo funkcijoms svarbias saugumo nuostatas.

Vadovų atsakomybė

13. Vadovai privalo žinoti, kurie darbuotojai dirba su įslaptinta informacija ar turi galimybę naudotis ypatingos svarbos ryšių ar informacinėmis sistemomis, bei registruoti ir pranešti apie visus galinčius turėti įtakos saugumui incidentus ar pastebėtą pažeidžiamumą.

Personalo saugumas

14. Nustatoma tvarka, užtikrinanti, kad, gavus tam tikram asmeniui nepalankios informacijos, būtų nustatyta, ar jis dirba su įslaptinta informacija arba turi galimybę naudotis ypatingos svarbos ryšių ar informacinėmis sistemomis ir apie tai pranešta atitinkamai institucijai. Nustačius, kad toks asmuo kelia grėsmę saugumui, jam uždraudžiama vykdyti tokias užduotis, arba jis nušalinamas nuo pareigų, kurias eidamas jis galėtų kelti grėsmę saugumui.

FIZINIS SAUGUMAS

Apsaugos poreikis

15. Fizinio saugumo priemonių, taikytinų užtikrinant ES įslaptintos informacijos apsaugą, veiksmingumo laipsnis turi būti proporcingas laikomos informacijos ir medžiagos slaptumui, kiekiui ir galimai grėsmei. Taigi turi būti pasirūpinta išvengti per didelio arba nepakankamo įslaptinimo, ir įslaptinimas turi būti reguliariai pervertinamas. Visi įslaptintos ES informacijos turėtojai laikosi vienodos tos informacijos įslaptinimo praktikos ir bendrų apsaugos standartų, reglamentuojančių saugomos informacijos ir medžiagos laikymą, perdavimą ir naikinimą.

Tikrinimas

16. Prieš išeidami iš zonų, kuriose be priežiūros paliekama ES įslaptinta informacija, už jos laikymą atsakingi asmenys užtikrina, kad ji būtų paliekama saugiai ir kad yra aktyvuotos visos apsaugos priemonės (užraktai, signalizacija ir kt.). Tolesni nepriklausomi tikrinimai atliekami po darbo valandų.

Pastatų saugumas

17. Pastatai, kuriuose laikoma įslaptinta ES informacija ar ypatingos svarbos ryšių ar informacinės sistemos, saugomi, kad į juos nepatektų leidimo neturintys asmenys. Įslaptintos ES informacijos apsaugos pobūdis, pvz., langų grotos, durų užraktai, apsauga prie įėjimų, automatizuotos priėjimo kontrolės sistemos, apsaugos darbuotojų atliekami tikrinimai ir patruliai, signalizacijos sistemos, į įsibrovimą reaguojančios sistemos ir sarginiai šunys, priklauso nuo:

a) saugotinos informacijos ir medžiagos slaptumo lygio, kiekio ir laikymo vietos pastate;

b) šios informacijos ir medžiagos apsaugos konteinerių kokybės;

c) pastato fizinių savybių ir padėties.

18. Ryšių ir informacinių sistemų apsaugos pobūdis taip pat priklauso nuo saugotino turto vertės ir galimos žalos, jei saugumas būtų pažeistas, taip pat nuo pastato, kuriame laikoma sistema, fizinių savybių bei padėties ir nuo sistemos vietos pastate.

Nenumatytoms aplinkybėms skirti planai

19. Iš anksto parengiami išsamūs planai, kaip apsaugoti įslaptintą informaciją ištikus vietinio arba nacionalinio masto nelaimei.

INFORMACIJOS SAUGUMAS (INFOSEC)

20. INFOSEC yra susijęs su ES įslaptintos informacijos apdorojimui, laikymui arba perdavimui ryšių, informacijos arba kitokiomis elektroninėmis sistemomis apsaugoti nuo tyčinio arba atsitiktinio pakenkimo jos slaptumui, vientisumui arba galimybei ja naudotis skirtų saugumo priemonių nustatymu ir taikymu. Imamasi atitinkamų atsakomųjų priemonių, sutrukdant pasinaudoti ES informacija leidimo neturintiems vartotojams ar neleisti naudotis ES įslaptinta informacija leidimą turintiems vartotojams bei užkertant kelią ES įslaptintos informacijos klastojimui arba nesankcionuotam jos taisymui ar sunaikinimui.

PRIEMONĖS PRIEŠ SABOTAŽĄ IR KITAS TYČINIO ŽALOS DARYMO FORMAS

21. Nuo sabotažo ir tyčinio žalos padarymo geriausiai apsaugo fizinės atsargumo priemonės svarbiems įrenginiams, kuriuose kaupiama įslaptinta informacija, apsaugoti; vien personalo tikrinimas nėra pakankamas šių priemonių pakaitalas. Kompetentinga nacionalinė institucija renka žvalgybinę informaciją apie šnipinėjimą, sabotažą, terorizmą ir kitokią ardomąją veiklą.

ĮSLAPTINTOS INFORMACIJOS PERDAVIMAS TREČIOSIOMS ŠALIMS IR TARPTAUTINĖMS ORGANIZACIJOMS

22. Sprendimą dėl Tarybos sukurtos ES įslaptintos informacijos perdavimo trečiajai šaliai arba tarptautinei organizacijai priima Taryba. Jei Taryba nėra norimos perduoti informacijos autorius, ji pirmiausia bando gauti autoriaus sutikimą perduoti tą informaciją. Jei autoriaus negalima nustatyti, už jį atsakomybę prisiima Taryba.

23. Jei Taryba gauna įslaptintos informacijos iš trečiųjų valstybių, tarptautinių organizacijų ar kitų trečiųjų šalių, jai garantuojama apsauga, atitinkanti jos slaptumo lygį ir prilygstanti šiuose nuostatuose ES įslaptintai informacijai nustatytiems standartams arba informaciją perduodančios trečiosios šalies reikalaujamiems aukštesnio lygio standartams. Gali būti atliekami abipusiai tikrinimai.

24. Pirmiau išdėstyti principai įgyvendinami pagal II dalyje pateiktas išsamias nuostatas.

II DALIS

I SKYRIUS

SAUGUMO ORGANIZAVIMAS EUROPOS SĄJUNGOS TARYBOJE

Generalinis sekretorius – vyriausiasis įgaliotinis

1. Generalinis sekretorius – vyriausiasis įgaliotinis:

   a) įgyvendina Tarybos saugumo politiką;

   b) svarsto Tarybos arba jos kompetentingų įstaigų nurodytas saugumo problemas;

   c) glaudžiai bendradarbiaudamas su valstybių narių nacionalinėmis saugumo (arba kitomis atitinkamomis) institucijomis (toliau – NSI), nagrinėja su Tarybos saugumo politikos pokyčiais susijusius klausimus. 1 priedėlyje pateikiamas šių institucijų sąrašas.

2. Generalinis sekretorius – vyriausiasis įgaliotinis visų pirma atsako už:

   a) visų su Tarybos veikla susijusių saugumo reikalų koordinavimą;

   b) reikalavimą, kad kiekviena valstybė narė įsteigtų centrinę informacijos su slaptumo žyma ES VISIŠKAI SLAPTAI registratūrą ir kad tokia registratūra prireikus būtų įsteigta ES decentralizuotose agentūrose;

   c) prašymų, kad NSI VI skyriuje nustatyta tvarka išduotų asmens patikimumo pažymėjimus TGS darbuotojams, perdavimą valstybių narių įgaliotoms institucijoms;

   d) ES įslaptintos informacijos nutekėjimo tyrimą arba nurodymą atlikti tokį tyrimą, jei, pagal *prima facie* (pirminius) įrodymus, jis įvyko TGS arba vienoje iš ES decentralizuotų agentūrų;

   e) prašymą atitinkamoms saugumo institucijoms pradėti tyrimą, kai yra tikėtina, jog įslaptinta ES informacija nutekėjo už TGS ir ES decentralizuotų agentūrų ribų, ir tyrimo koordinavimą, kai jame dalyvauja daugiau nei viena saugumo institucija;

   f) reguliarius ES įslaptintos informacijos apsaugai valstybėse narėse skirtų saugumo priemonių patikrinimus kartu su atitinkama NSI ir suderinus su ja;

   g) glaudaus bendradarbiavimo su visomis suinteresuotomis saugumo institucijomis palaikymą, siekiant bendro saugumo koordinavimo;

   h) nuolatinį Tarybos saugumo politikos bei procedūrų patikslinimą ir, jei būtina, atitinkamų rekomendacijų rengimą. Tuo tikslu jis pateikia Tarybai TGS Saugumo biuro parengtą metinį tikrinimų planą.

Tarybos Saugumo komitetas

3. Įsteigiamas Saugumo komitetas. Į jo sudėtį įeina kiekvienos valstybės narės NSI atstovai. Komitetui pirmininkauja Generalinis sekretorius – vyriausiasis įgaliotinis arba jo deleguotas asmuo. ES decentralizuotų agentūrų atstovai taip pat gali būti kviečiami dalyvauti svarstant jiems svarbius klausimus.

4. Saugumo komiteto posėdžiai rengiami pagal Tarybos nurodymus Generalinio sekretoriaus – vyriausiojo įgaliotinio arba NSI kvietimu. Komitetas turi įgaliojimus tirti ir vertinti visus su Tarybos veikla susijusius saugumo klausimus bei prireikus teikti rekomendacijas Tarybai. Komitetas taip pat yra įgaliotas teikti rekomendacijas Generaliniam sekretoriui – vyriausiajam įgaliotiniui su TGS veikla susijusiais saugumo klausimais.

Tarybos Generalinio Sekretoriato Saugumo biuras

5. Kad galėtų vykdyti 1 ir 2 punktuose nurodytas pareigas, Generalinis sekretorius – vyriausiasis įgaliotinis saugumo priemonėms koordinuoti, prižiūrėti ir įgyvendinti savo žinioje turi TGS Saugumo biurą.

6. TGS Saugumo biuro vadovas yra pagrindinis Generalinio sekretoriaus – vyriausiojo įgaliotinio patarėjas saugumo klausimais ir eina Saugumo komiteto sekretoriaus pareigas. Todėl jis vadovauja saugumo nuostatų atnaujinimo darbui, koordinuoja saugumo priemones su valstybių narių kompetentingomis institucijomis, o prireikus – su tarptautinėmis organizacijomis, sudariusiomis su Taryba saugumo sutartis. Tuo tikslu jis veikia kaip už kontaktus atsakingas pareigūnas.

7. TGS Saugumo biuro vadovas atsako už TGS informacinių technologijų sistemų ir tinklų akreditavimą. Prireikus TGS Saugumo biuro vadovas ir atitinkama NSI kartu sprendžia dėl TGS, valstybes nares, ES decentralizuotas agentūras ir (arba) trečiąsias šalis (valstybes arba tarptautines organizacijas) apimančių informacinių technologijų sistemų ir tinklų akreditavimo.

ES decentralizuotos agentūros

8. Kiekvienas ES decentralizuotos agentūros direktorius atsako už saugumo įgyvendinimą savo įstaigoje. Paprastai jis paskiria vieną savo darbuotoją eiti direktoriui atskaitingo saugumo pareigūno pareigas.

Valstybės narės

9. Kiekviena valstybė narė paskiria atsakingą už įslaptintos ES informacijos saugumą NSI ([1]).

10. Kiekvienos valstybės narės administracijoje atitinkama NSI yra atsakinga už:

a) viešosiose ar privačiose nacionalinėse institucijose, įstaigose ir agentūrose, valstybės teritorijoje ir užsienyje, laikomos įslaptintos ES informacijos saugumo priežiūrą;

b) leidimą steigti informacijos su slaptumo žyma ES VISIŠKAI SLAPTAI registratūras (šis įgaliojimas gali būti perduotas informacijos su slaptumo žyma ES VISIŠKAI SLAPTAI centrinės registratūros kontrolės pareigūnui);

c) reguliarų įslaptintos ES informacijos apsaugai skirtų saugumo priemonių tikrinimą;

d) užtikrinimą, kad visi valstybės institucijose, įstaigose ar agentūrose dirbantys ir galimybę naudotis slaptumo žymomis ES VISIŠKAI SLAPTAI, ES SLAPTAI ar ES KONFIDENCIALIAI pažymėta įslaptinta ES informacija turintys piliečiai bei užsieniečiai turėtų asmens patikimumo pažymėjimus;

e) saugumo planų, būtinų, kad įslaptintai ES informacijai nebūtų leista pakliūti į leidimo neturinčių asmenų rankas, sudarymą.

Abipusiai saugumo tikrinimai

11. TGS Saugumo biuras kartu su suinteresuota NSI pagal abipusį susitarimą reguliariai tikrina įslaptintos ES informacijos apsaugai skirtas saugumo priemones TGS, valstybių narių nuolatinėse atstovybėse prie Europos Sąjungos, taip pat valstybių narių patalpose Tarybos pastatuose ([2]).

12. ES decentralizuotose agentūrose įslaptintos ES informacijos apsaugai skirtas saugumo procedūras reguliariai tikrina TGS Saugumo biuras arba, Generalinio Sekretoriaus prašymu, buvimo valstybės narės NSI.

([1]) Už įslaptintos ES informacijos saugumą atsakingų NSI sąrašas pateikiamas 1 priedėlyje.
([2]) Nepažeidžiant 1961 m. Vienos konvencijos dėl diplomatinių santykių.

II SKYRIUS

SLAPTUMO ŽYMOS IR KVALIFIKACINĖS ŽYMOS

SLAPTUMO ŽYMŲ LAIPSNIAI ([1])

Informacija įslaptinama šiais slaptumo žymų laipsniais:

1. ES VISIŠKAI SLAPTAI: ši žyma suteikiama tik tai informacijai ir medžiagai, kurią atskleidus be leidimo, gali būti padaryta ypač didelė žala svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams.

2. ES SLAPTAI: ši žyma suteikiama tik tai informacijai ir medžiagai, kurią atskleidus be leidimo, gali būti labai pakenkta svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams.

3. ES KONFIDENCIALIAI: ši žyma suteikiama tai informacijai ir medžiagai, kurią atskleidus be leidimo, gali būti pakenkta svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams.

4. ES RIBOTO NAUDOJIMO: ši žyma suteikiama tai informacijai ir medžiagai, kurios atskleidimas be leidimo gali būti nenaudingas Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams.

KVALIFIKACINĖS ŽYMOS

5. Kvalifikacinės žymos gali būti naudojamos, kai reikia tiksliai apibrėžti dokumento taikymo sritį arba pažymėti specialų jo platinimą vadovaujantis „būtina žinoti“ principu.

6. Dokumentams, susijusiems su Sąjungos arba vienos ar daugiau jos valstybių narių saugumu ir gynyba arba su kariniu ar nekariniu krizių valdymu, ir tų dokumentų kopijoms suteikiama ESGP kvalifikacinė žyma.

7. Tam tikriems dokumentams, t. y. su informacinių technologijų (IT) sistemomis susijusiems dokumentams, gali būti naudojamos papildomos kvalifikacinės žymos, pažyminčios atitinkamuose teisės aktuose apibrėžtas papildomas saugumo priemones.

SLAPTUMO ŽYMŲ IR KVALIFIKACINIŲ ŽYMŲ DĖJIMAS

8. Slaptumo žymos ir kvalifikacinės žymos dedamos taip:

   a) ant slaptumo žyma ES RIBOTO NAUDOJIMO žymimų dokumentų – mechaninėmis arba elektroninėmis priemonėmis;

   b) ant slaptumo žyma ES KONFIDENCIALIAI žymimų dokumentų – mechaninėmis priemonėmis ir ranka arba spausdinant ant iš anksto antspauduoto, registruoto popieriaus;

   c) ant slaptumo žymomis ES SLAPTAI ir ES VISIŠKAI SLAPTAI žymimų dokumentų – mechaninėmis priemonėmis ir ranka.

([1]) ES, NATO, VES ir valstybių narių slaptumo žymų lyginamoji lentelė pateikta 2 priedėlyje.

III SKYRIUS

ĮSLAPTINIMO TVARKYMAS

1. Informacija įslaptinama tik tada, kai tai būtina. Slaptumo žyma turi būti aiškiai ir teisingai nurodyta ir taikoma tik tol, kol informaciją reikia saugoti.

2. Atsakomybė už informacijos įslaptinimą ir už bet kokį paskesnį slaptumo žymos laipsnio sumažinimą arba informacijos išslaptinimą [1] tenka tik informacijos autoriui.

   TGS pareigūnai ir kiti tarnautojai informaciją įslaptina, jos slaptumo žymos laipsnį sumažina arba informaciją išslaptina tik gavę savo Generalinio direktoriaus nurodymą arba sutikimą.

3. Detali įslaptintų dokumentų naudojimo tvarka parengta, stengiantis užtikrinti, kad dokumentams skiriama apsauga atitiktų jų turinį.

4. Asmenų, galinčių būti slaptumo žyma ES VISIŠKAI SLAPTAI žymimų dokumentų autoriais, turi būti kuo mažiau, o jų pavardės turi būti įtrauktos į TGS, kiekvienos valstybės narės ir, jei reikia, kiekvienos ES decentralizuotos agentūros sudarytą sąrašą.

SLAPTUMO ŽYMŲ NAUDOJIMAS

5. Dokumento slaptumo žyma nustatoma pagal II skyriaus 1–4 punktuose apibrėžtą jo turinio slaptumo lygį. Svarbu, kad įslaptinimas būtų taikomas teisingai ir nuosaikiai. Tai ypač taikytina ES VISIŠKAI SLAPTAI slaptumo žymai.

6. Įslaptinamo dokumento autorius turi atsižvelgti į pirmiau išdėstytas nuostatas ir išvengti pernelyg aukšto ar pernelyg žemo slaptumo žymos laipsnio suteikimo.

   Nors iš pirmo žvilgsnio gali atrodyti, kad aukšto laipsnio slaptumo žyma gali garantuoti geresnę dokumento apsaugą, dėl nuolatinio pernelyg didelio įslaptinimo gali sumažėti pasitikėjimas įslaptinimo sistemos tinkamumu.

   Kita vertus, nepriimtinas ir nepakankamas dokumentų įslaptinimas siekiant išvengti su apsauga susijusių suvaržymų.

   Praktinis įslaptinimo vadovas pateikiamas 3 priedėlyje.

7. Atskiriems dokumento lapams, dalims, skirsniams, priedams, priedėliams gali būti suteikiamos skirtingos slaptumo žymos ir jie atitinkamai paženklinami. Visas dokumentas įslaptinamas pagal aukščiausią slaptumo žymos laipsnį turinčią jo dalį.

8. Pridedamų dokumentų lydraščių arba atžymų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymas. Jei tokie dokumentai pateikiami atskirai nuo priedų, autorius turi aiškiai nurodyti, koks slaptumo žymos laipsnis jiems suteikiamas.

SLAPTUMO ŽYMOS LAIPSNIO SUMAŽINIMAS IR IŠSLAPTINIMAS

9. ES įslaptintų dokumentų slaptumo žymos laipsnis gali būti sumažintas arba jie gali būti visai išslaptinti tik leidus jų autoriui, ir prireikus pasitarus su kitomis suinteresuotomis šalimis. Dokumentų slaptumo žymos laipsnio sumažinimas arba jų išslaptinimas patvirtinamas raštu. Dokumentą sukūrusi institucija, valstybė narė, tarnyba, teises perėmusi organizacija ar aukštesnė institucija atsako už to dokumento gavėjų informavimą apie slaptumo žymos pakeitimą, o šie atitinkamai atsako už kitų adresatų, kuriems jie yra nusiuntę dokumentą arba jo kopiją, informavimą apie slaptumo žymos pakeitimą.

10. Jei įmanoma, ant įslaptinto dokumento jo autorius nurodo datą arba terminą, kada slaptumo žymos laipsnis gali būti sumažintas arba dokumentas išslaptintas. Priešingu atveju dokumentų autoriai peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad garantuotų, jog pradinis įslaptinimas yra būtinas.

---

[1] „Laipsnio sumažinimas“ (*déclassement*) – slaptumo žymos laipsnio sumažinimas; „išslaptinimas“ (*déclassification*) – visų slaptumo žymų panaikinimas.

IV SKYRIUS

FIZINIS SAUGUMAS

BENDROSIOS NUOSTATOS

1. Svarbiausia fizinio saugumo priemonių paskirtis – neleisti leidimo neturintiems asmenims pasinaudoti įslaptinta ES informacija ir (arba) medžiaga.

SAUGUMO REIKALAVIMAI

2. Visos patalpos, zonos, pastatai, biurai, kambariai, ryšių ir informacinės sistemos ir kt., kuriuose yra saugoma įslaptinta ES informacija ir medžiaga ir (arba) su ja dirbama, saugomos tinkamomis fizinės apsaugos priemonėmis.

3. Sprendžiant, koks fizinio saugumo lygis reikalingas, atsižvelgiama į visus svarbius veiksnius, pvz.:

   a) informacijos ir (arba) medžiagos slaptumo žymą;

   b) laikomos informacijos kiekį ir formą (pvz., spausdintinė kopija, kompiuterinių duomenų saugojimo laikmenos);

   c) vietoje įvertinta prieš ES, valstybes nares ir (arba) kitas ES įslaptintą informaciją laikančias institucijas arba trečiąsias šalis nukreiptų žvalgybos tarnybų keliama grėsmė, ypač dėl sabotažo, terorizmo ir kitų rūšių ardomosios ir (arba) nusikalstamos veiklos.

4. Fizinio saugumo priemonės sukuriamos tam, kad būtų:

   a) sutrukdyta įsibrauti slaptai arba įsiveržti jėga;

   b) sutrukdyti ir atskleisti nelojalaus personalo veiksmai arba atgrasinta nuo tokių veiksmų;

   c) neleista ES įslaptinta informacija pasinaudoti tiems TGS, valstybių narių Vyriausybių institucijų ir (arba) kitų institucijų ar trečiųjų šalių pareigūnams bei kitiems tarnautojams, kuriems nėra būtina ją žinoti.

FIZINĖS APSAUGOS PRIEMONĖS

Saugumo zonos

5. Zonos, kuriose dirbama su ES KONFIDENCIALIAI arba aukštesnio laipsnio slaptumo žyma pažymėta informacija arba kuriose tokia informacija saugoma, yra tvarkomos ir įrengiamos taip, kad atitiktų vieną iš šių reikalavimų:

   a) I klasės saugumo zona: zona, kurioje dokumentai su ES KONFIDENCIALIAI arba aukštesnio laipsnio slaptumo žyma yra tvarkomi ir saugomi tokiu būdu, kad įėjus į zoną, galima visais praktiniais tikslais naudotis įslaptinta informacija. Tokiai zonai yra reikalinga:

      i) aiškiai apibrėžta ir saugoma išorinė riba, per kurią kiekvienas įėjimas ir išėjimas yra kontroliuojamas;

      ii) įėjimo kontrolės sistema, leidžianti įeiti į zoną tik deramai patikrintiems ir specialų leidimą turintiems asmenims;

      iii) paprastai zonoje laikomos informacijos, t. y. informacijos, kuria galima naudotis įėjus, slaptumo žymų laipsnio specifikacija;

   b) II klasės saugumo zona: zona, kurioje su ES KONFIDENCIALIAI arba aukštesnio laipsnio slaptumo žyma pažymėtais dokumentais dirbama arba jie saugomi tokiu būdu, kad dėl viduje sukurtų kontrolės priemonių jie yra apsaugomi taip, kad jais negalėtų pasinaudoti leidimo neturintys asmenys, pavyzdžiui, patalpos, kuriose yra biurai, kuriuose reguliariai dirbama su ES KONFIDENCIALIAI arba aukštesnio laipsnio slaptumo žyma pažymėtais dokumentais ar tokie dokumentai saugomi. Tokiai zonai yra reikalinga:

      i) aiškiai apibrėžta ir saugoma išorinė riba, per kurią kiekvienas įėjimas ir išėjimas yra kontroliuojamas;

      ii) įėjimo kontrolės sistema, kuri be palydos leidžia į zoną įeiti tik deramai patikrintiems ir specialų leidimą turintiems asmenims. Visiems kitiems asmenims turi būti užtikrinta palyda arba lygiavertė kontrolė, užkertant kelią naudojimuisi įslaptinta ES informacija neturint tam leidimo ir nekontroliuojamam įėjimui į zonas, kuriose taikomas techninis saugumo patikrinimas.

Zonos, kuriose nėra visą parą budinčio personalo, tikrinamos iškart po įprastų darbo valandų, kad būtų užtikrinta, jog ES įslaptinta informacija yra tinkamai saugoma.

Administracinė zona

6. Aplink I ir II klasės saugumo zonas ar jų prieigose gali būti sukurta mažesnio saugumo administracinė zona. Tokiai zonai reikalingos aiškiai apibrėžtos išorinės ribos, kurios leistų tikrinti personalą ir transporto priemones. Administracinėse zonose dirbama tik su slaptumo žyma ES RIBOTO NAUDOJIMO pažymėta informacija, tik tokia informacija gali būti jose saugoma.

Įėjimo ir išėjimo kontrolė

7. Įėjimas į I ir II klasės saugumo zonas ir išėjimas iš jų kontroliuojamas leidimų arba asmens atpažinimo sistemomis, taikomomis nuolatiniams darbuotojams. Taip pat sukuriama lankytojų tikrinimo sistema, kuri neleidžia ES įslaptinta informacija naudotis neturint atitinkamo leidimo. Papildomai prie leidimų sistemos gali būti naudojami automatizuoti identifikavimo įrenginiai, tačiau jie laikytini papildoma, bet apsaugos personalo visiškai nepakeičiančia priemone. Pasikeitus grėsmės įvertinimui, pvz., per žymių asmenų vizitus, gali prireikti imtis griežtesnių įėjimo ir išėjimo kontrolės priemonių.

Apsaugos patruliai

8. I ir II klasės saugumo zonose, siekiant ES turtą apsaugoti nuo pavojaus, žalos ar praradimo, turi būti patruliuojama ne darbo valandomis. Patruliavimo dažnumas nustatomas atsižvelgiant į vietos aplinkybes, tačiau rekomenduotina patruliuoti kas dvi valandas.

Apsaugos konteineriai ir saugyklos

9. Įslaptintai ES informacijai saugoti naudojami trijų klasių konteineriai:

— A klasė: nacionaliniu lygiu sertifikuoti informacijai, pažymėtai slaptumo žyma ES VISIŠKAI SLAPTAI, I arba II klasės saugumo zonose saugoti skirti konteineriai;

— B klasė: nacionaliniu lygiu sertifikuoti informacijai, pažymėtai slaptumo žyma ES SLAPTAI ir ES KONFIDENCIALIAI, I arba II klasės saugumo zonose saugoti skirti konteineriai;

— C tipas: biuro baldai, tinkami tik slaptumo žyma ES RIBOTO NAUDOJIMO pažymėtai informacijai laikyti.

10. I ar II klasės saugumo zonose įrengtų saugyklų, taip pat visų I klasės saugumo zonų, kuriose atvirose lentynose arba brėžiniuose, žemėlapiuose ir pan. yra laikoma informacija su ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma, sienos, grindys, lubos, durys su užraktais turi būti NSI sertifikuotos kaip suteikiančios apsaugą, kuri atitinka apsaugos konteinerio klasę, patvirtintą to paties laipsnio slaptumo žymos informacijai saugoti.

Užraktai

11. Apsaugos konteinerių ir saugyklų, kuriuose laikoma ES įslaptinta informacija, užraktai turi atitikti tokius standartus:

— A grupė: nacionaliniu lygiu sertifikuoti A klasės konteineriams;

— B grupė: nacionaliniu lygiu sertifikuoti B klasės konteineriams;

— C grupė: tinkami tik C klasės biuro baldams.

Raktų ir kodų kontrolė

12. Apsaugos konteinerių raktai neišnešami iš įstaigos pastato. Apsaugos konteinerių kodus įsimena asmenys, kuriems privalu juos žinoti. Nenumatytiems atvejams įstaigos saugumo pareigūnas turi atsarginius raktus ir visų kodų sąrašą. Užrašyti kodai laikomi atskiruose antspauduotuose nepermatomuose vokuose. Naudojami raktai, atsarginiai apsaugos raktai ir spynų atrakinimo kodai laikomi atskiruose apsaugos konteineriuose. Šie raktai ir kodai saugomi ne mažiau griežtai, nei medžiaga, kuria naudotis jie suteikia galimybę.

13. Apsaugos konteinerių kodus turi žinoti kiek įmanoma mažiau asmenų. Kodai keičiami:

a) gavus naują konteinerį;

b) pasikeitus darbuotojams;

c) neteisėtai atskleidus informaciją arba įtarus, kad tai padaryta;

d) pageidautina kas šešis mėnesius ir būtinai ne rečiau kaip kartą per metus.

Į įsibrovimą reaguojanti įranga

14. Įslaptintai ES informacijai apsaugoti naudojant signalizacijos sistemas, uždarosios grandinės videostebėjimo sistemas ar kitą elektroninę įrangą, būtinas atsarginis elektros tiekimo šaltinis, kuris užtikrintų nepertraukiamą sistemos darbą nutrūkus pagrindiniam energijos tiekimui. Kitas esminis reikalavimas yra tas, kad signalizacija įsijungtų ar apsaugos personalas būtų kitaip patikimai įspėtas sutrikus šioms sistemoms ar mėginant jas sugadinti.

Aprobuota įranga

15. NSI, naudodamosi savo ar abipusiais ištekliais, sudaro nuolat atnaujinamus įrangos, kurią jos aprobavo tiesioginei ar netiesioginei įslaptintos informacijos apsaugai įvairiomis nurodytomis aplinkybėmis ir sąlygomis, sąrašus pagal tipą ir modelį. Panašų sąrašą sudaro TGS Saugumo biuras, *inter alia* remdamasis iš NSI gauta informacija. Prieš įsigydamos tokią įrangą, ES decentralizuotos agentūros konsultuojasi su TGS Saugumo biuru, o prireikus – ir su jų buvimo valstybės narės NSI.

Fizinė kopijavimo ir telefakso aparatų apsauga

16. Kopijavimo aparatai ir telefaksai fiziškai apsaugomi taip, kad būtų užtikrinta, jog jais naudotųsi tik leidimą turintys asmenys ir kad visa įslaptinta medžiaga būtų tinkamai kontroliuojama.

APSAUGA NUO PAMATYMO IR PASIKLAUSYMO

Pamatymas

17. Tiek dieną, tiek naktį imamasi visų būtinų priemonių, užtikrinančių, kad ES įslaptintos informacijos netgi atsitiktinai nepamatytų joks leidimo tam neturintis asmuo.

Pasiklausymas

18. Biurai ir zonos, kuriose nuolat yra svarstoma informacija su ES SLAPTAI ir aukštesnio laipsnio slaptumo žyma, esant atitinkamai rizikai, turi būti apsaugomi nuo galimo pasyvaus arba aktyvaus slapto pasiklausymo. Už tokio pasiklausymo rizikos įvertinimą atsako kompetentinga saugumo institucija, prireikus pasikonsultavusi su NSI.

19. Kad nustatytų, kokios apsaugos priemonės reikalingos patalpų, kuriose egzistuoja pasyvaus (pvz., sienų, durų, grindų ir lubų izoliacija, sklindančio garso matavimas) ir aktyvaus (pvz., mikrofonų paieška) slapto pasiklausymo pavojus, atžvilgiu, TGS Saugumo biuras gali prašyti NSI ekspertų pagalbos. ES decentralizuotų agentūrų saugumo pareigūnai gali prašyti, kad TGS Saugumo biuras atliktų techninį patikrinimą ir (arba) prašyti NSI ekspertų pagalbos.

20. Taip pat kompetentingo saugumo pareigūno prašymu NSI techninio saugumo ekspertai prireikus gali patikrinti telekomunikacijų įrangą ir bet kokią elektros ar elektroninę biuro įrangą, naudojamą per ES SLAPTAI ar aukštesnio slaptumo žymos laipsnio posėdžius.

TECHNIŠKAI SAUGIOS ZONOS

21. Tam tikros zonos gali būti išskiriamos kaip techniškai saugios zonos. Atliekamas specialus tikrinimas į jas įeinant. Tokios zonos, kai jose nedirbama, patvirtintu būdu laikomos užrakintos, o visi raktai saugomi kaip apsaugos raktai. Tokios zonos reguliariai fiziškai tikrinamos taip pat ir tuo atveju, kai nustatoma ar įtariama, kad į jas įeita be leidimo.

22. Sudaromas išsamus įrangos ir baldų sąrašas, kad būtų galima kontroliuoti jų vietos keitimą. Joks baldas ar įrenginys nepakliūna į tokią zoną, prieš tai nuodugniai neapžiūrėtas specialiai parengtų apsaugos darbuotojų, kad būtų nustatyta, ar nėra pasiklausymo įrangos. Paprastai techniškai saugiose zonose reikėtų vengti tiesti ryšių linijas.

V SKYRIUS

BENDROS „BŪTINA ŽINOTI“ PRINCIPO TAIKYMO IR ASMENS PATIKIMUMO TIKRINIMO TAISYKLĖS

1. Naudotis įslaptinta ES informacija leidžiama tik asmenims, kuriems ją būtina žinoti, kad galėtų atlikti savo pareigas ar vykdyti užduotis. Naudotis žymomis ES VISIŠKAI SLAPTAI, ES SLAPTAI ir ES KONFIDENCIALIAI pažymėta informacija leidžiama tik asmenims, turintiems atitinkamą asmens patikimumo pažymėjimą.

2. Nustatyti, kiek darbuotojui taikytinas „būtina žinoti“ principas, atsižvelgdamas į jo užduoties reikalavimus turi TGS, ES decentralizuotos agentūros ar valstybės narės tarnyba ar padalinys, kuriame atitinkamas asmuo įdarbinamas.

3. Už personalo patikimumo patikrinimą nustatyta tvarka atsako pareigūno darbdavys. TGS pareigūnų ir kitų tarnautojų asmens patikimumo patikrinimo tvarka pateikiama VI skyriuje.

   Asmenį patikrinus, jam yra išduodamas „asmens patikimumo pažymėjimas“, kuriame nurodomas informacijos, kuria asmuo gali naudotis, slaptumo žymos laipsnis ir pažymėjimo galiojimo laikas.

   Tam tikram slaptumo žymos laipsniui išduotas asmens patikimumo pažymėjimas gali suteikti jo turėtojui teisę naudotis žemesnio slaptumo žymos laipsnio informacija.

4. TGS ar valstybių narių pareigūnais ar kitais tarnautojais nesantys asmenys, pvz., ES institucijų pareigūnai ar tarnautojai, su kuriais gali prireikti aptarti arba kuriems gali prireikti parodyti įslaptintą ES informaciją, privalo turėti ES asmens patikimumo pažymėjimus dėl teisės naudotis ES įslaptinta informacija bei yra trumpai supažindinami su jų atsakomybe už saugumą. Ši taisyklė panašiomis aplinkybėmis taikoma samdytiems rangovams, ekspertams ar konsultantams.

SPECIALIOS NAUDOJIMOSI SLAPTUMO ŽYMA ES VISIŠKAI SLAPTAI PAŽYMĖTA INFORMACIJA TAISYKLĖS

5. Visi asmenys, kuriems reikia naudotis slaptumo žyma ES VISIŠKAI SLAPTAI pažymėta informacija, prieš tai patikrinami.

6. Visus asmenis, kurie turi naudotis slaptumo žyma ES VISIŠKAI SLAPTAI pažymėta informacija, nurodo jų departamento vadovas, o jų pavardės įrašomos atitinkamame įslaptintos informacijos, pažymėtos slaptumo žyma ES VISIŠKAI SLAPTAI, registre.

7. Prieš įgydami galimybę naudotis informacija, pažymėta slaptumo žyma ES VISIŠKAI SLAPTAI, visi asmenys pasirašo dokumentą, patvirtinantį, kad jie buvo supažindinti su Tarybos saugumo procedūromis, kad visiškai supranta savo ypatingą atsakomybę už slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtos informacijos išsaugojimą ir supranta pasekmes, kurias numato ES taisyklės bei nacionaliniai teisės ir administraciniai aktai, jei įslaptinta informacija tyčia arba dėl neatsargumo patektų į leidimo neturinčio asmens rankas.

8. Jei asmuo dalyvauja posėdyje ar panašiame renginyje, kuriame gali susipažinti su slaptumo žyma ES VISIŠKAI SLAPTAI pažymėta informacija, kompetentingi tarnybos arba įstaigos, kurioje tas asmuo dirba, kontrolės pareigūnai posėdį organizuojančią įstaigą informuoja, kad tas asmuo turi atitinkamą leidimą.

9. Visų asmenų, kurie toliau nebeeina su būtinybe naudotis slaptumo žyma žyma ES VISIŠKAI SLAPTAI pažymėta informacija susijusių pareigų, pavardės išbraukiamos iš turinčių teisę naudotis informacija su slaptumo žyma ES VISIŠKAI SLAPTAI asmenų sąrašo. Be to, visų tokių asmenų dėmesys dar kartą atkreipiamas į jų ypatingą pareigą saugoti informaciją, pažymėtą slaptumo žyma ES VISIŠKAI SLAPTAI. Jie taip pat pasirašo pasižadėjimus, kad nenaudos ir neperduos turimų žinių apie slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtą informaciją.

SPECIALIOS NAUDOJIMOSI SLAPTUMO ŽYMOMIS ES SLAPTAI IR ES KONFIDENCIALIAI PAŽYMĖTA INFORMACIJA TAISYKLĖS

10. Visi asmenys, kuriems turi būti suteikta galimybė naudotis slaptumo žymomis ES SLAPTAI ir ES KONFIDENCIALIAI pažymėta informacija, pirmiausia yra patikrinami atitinkamai slaptumo žymos laipsniui.

11. Visi asmenys, kuriems turi būti suteikta galimybė naudotis slaptumo žymomis ES SLAPTAI ir ES KONFIDENCIALIAI pažymėta informacija, supažindinami su atitinkamomis saugumo taisyklėmis ir neatsargumo pasekmėmis.

12. Jei asmuo dalyvauja posėdyje ar panašiame renginyje, kuriame gali susipažinti su slaptumo žyma ES SLAPTAI ar ES KONFIDENCIALIAI pažymėta informacija, jo darbovietės kompetentingas saugumo pareigūnas posėdį rengiančią įstaigą informuoja, kad asmuo turi atitinkamą leidimą.

SPECIALIOS NAUDOJIMOSI SLAPTUMO ŽYMA ES RIBOTO NAUDOJIMO PAŽYMĖTA INFORMACIJA TAISYKLĖS

13. Asmenys, galintys naudotis slaptumo žyma ES RIBOTO NAUDOJIMO pažymėta informacija, supažindinami su šiais saugumo nuostatais ir neatsargumo pasekmėmis.

PERKĖLIMAI

14. Kai personalo narys perkeliamas iš pareigų, kurias eidamas turėjo dirbti su įslaptinta ES medžiaga, registratūra prižiūri, kad pareigas paliekantis pareigūnas tinkamai perduotų medžiagą jo pareigas eisiančiam pareigūnui.

SPECIALIOS INSTRUKCIJOS

15. Asmenys, kurie turi dirbti su ES įslaptinta informacija, pradėdami eiti pareigas ir vėliau periodiškai yra supažindinami su:

    a) dėl neatsargių pokalbių saugumui kylančiais pavojais;

    b) atsargumo priemonėmis, kurių jie turi imtis bendraudami su spauda;

    c) prieš ES ir valstybes nares nukreiptos žvalgybos tarnybų veiklos, kiek ji siejasi su ES įslaptinta informacija ir veikla, keliama grėsme;

    d) įpareigojimu nedelsiant informuoti atitinkamas saugumo institucijas apie kiekvieną įtarimų dėl šnipinėjimo sukeliantį mėginimą užmegzti ryšius ar veiksmą, arba apie bet kokias neįprastas su saugumu susijusias aplinkybes.

16. Visi asmenys, kurie paprastai dažnai bendrauja su atstovais tų valstybių, kurių žvalgybos tarnybų veikla, kiek tai siejasi su ES įslaptinta informacija ir veikla, yra nukreipta prieš ES ir valstybes nares, yra trumpai instruktuojami apie įprastinius įvairių žvalgybos tarnybų darbo metodus.

17. Taryba nėra nustačiusi saugumo nuostatų, reglamentuojančių įslaptinta informacija galinčių naudotis darbuotojų privačių kelionių į bet kurią vietą. Tačiau kompetentingos saugumo institucijos jų kompetencijai priklausančius pareigūnus ir kitus tarnautojus supažindina su kelionių taisyklėmis, kurios gali būti jiems taikomos. Saugumo pareigūnai turi rengti darbuotojams posėdžius, kuriuose būtų primenama apie šias specialias instrukcijas.

VI SKYRIUS

ASMENS PATIKIMUMO PAŽYMĖJIMŲ IŠDAVIMO TGS PAREIGŪNAMS IR KITIEMS TARNAUTOJAMS TVARKA

1. Galimybė naudotis Tarybos turima įslaptinta informacija suteikiama tik TGS pareigūnams ir kitiems tarnautojams bei TGS dirbantiems asmenims, kuriems dėl savo pareigų ir tarnybos specifikos yra būtina žinoti ar naudoti tokią įslaptintą informaciją.

2. Kad galėtų naudotis slaptumo žymomis ES VISIŠKAI SLAPTAI, ES SLAPTAI ir ES KONFIDENCIALIAI pažymėta informacija, 1 punkte nurodyti asmenys privalo 4 ir 5 punktuose nurodyta tvarka gauti leidimą.

3. Leidimas išduodamas tik asmenims, kurių patikimumą 6–10 punktuose nurodyta tvarka yra patikrinusios valstybių narių kompetentingos nacionalinės institucijos (NSI).

4. Tarnybos nuostatų 2 straipsnio pirmojoje pastraipoje apibrėžta paskyrimų tarnyba yra atsakinga už 1, 2 ir 3 punktuose nurodyto leidimo išdavimą.

   Paskyrimų tarnyba išduoda leidimą gavusi valstybių narių kompetentingų nacionalinių institucijų nuomonę, pagrįstą 6–12 punktuose nurodyta tvarka atlikto patikimumo patikrinimo rezultatais.

5. Penkerius metus galiojantis leidimas negali galioti ilgiau, nei reikia užduotims, kurioms jis buvo išduotas, atlikti. Pakyrimų tarnyba gali atnaujinti leidimą 4 punkte nurodyta tvarka.

   Paskyrimų tarnyba panaikina leidimą, jei mano, kad tam yra pakankamai pagrindo. Apie kiekvieną sprendimą panaikinti leidimą informuojamas jo turėtojas, kuris gali prašyti, kad paskyrimų tarnyba ir kompetentinga nacionalinė institucija jį išklausytų.

6. Patikimumo patikrinimo tikslas – įsitikinti, jog nėra prieštaravimų, kad tam tikram asmeniui būtų leista naudotis Tarybos turima įslaptinta informacija.

7. Patikimumo patikrinimą, padedant suinteresuotam asmeniui, paskyrimų tarnybos prašymu atlieka valstybės narės, kurios pilietis yra leidimo prašantis asmuo, kompetentingos nacionalinės institucijos. Jei suinteresuotas asmuo nuolat gyvena kitos valstybės narės teritorijoje, atitinkamos nacionalinės institucijos gali bendradarbiauti su šios valstybės institucijomis.

8. Suinteresuotas asmuo turi užpildyti asmeninės informacijos anketą, kuri yra viena iš tikrinimo procedūros dalių.

9. Paskyrimų tarnyba savo prašyme nurodo įslaptintos informacijos, kuria suinteresuotam asmeniui turėtų būti leista naudotis, pobūdį ir slaptumo žymos laipsnį, kad kompetentinga nacionalinė institucija galėtų atlikti tikrinimą ir pateikti savo nuomonę dėl to, kokio slaptumo žymos laipsnio informacija derėtų leisti naudotis šiam asmeniui.

10. Visą patikimumo tikrinimo procesą bei jo rezultatus reglamentuoja atitinkamoje valstybėje narėje galiojančios normos ir taisyklės, įskaitant su apeliacijomis susijusias normas ir taisykles.

11. Gavusi iš valstybės narės kompetentingų nacionalinių institucijų teigiamą nuomonę, paskyrimų tarnyba gali suinteresuotam asmeniui išduoti leidimą.

12. Apie neigiamą kompetentingų nacionalinių institucijų nuomonę pranešama suinteresuotam asmeniui, kuris gali prašyti, kad paskyrimų tarnyba jį išklausytų. Jei paskyrimų tarnyba mano, kad tai tikslinga, ji gali prašyti kompetentingų nacionalinių institucijų išsamesnio paaiškinimo. Jei neigiama nuomonė patvirtinama, leidimas neišduodamas.

13. Visi asmenys, kuriems leidimas išduodamas pagal 4 ir 5 punktus, išduodant leidimą ir reguliariai vėliau reikiamai instruktuojami dėl įslaptintos informacijos apsaugos ir jos užtikrinimo priemonių. Tokie asmenys pasirašo deklaraciją, kurioje patvirtina išklausę instrukcijas ir įsipareigoja jų laikytis.

14. Paskyrimų tarnyba imasi visų reikiamų priemonių šiam skyriui, ypač teisę naudotis leidimą turinčių asmenų sąrašu reglamentuojančioms taisyklėms įgyvendinti.

15. Išskirtiniais atvejais, esant tarnybinei būtinybei, paskyrimų tarnyba, pranešusi kompetentingoms nacionalinėms institucijoms ir per mėnesį negavusi jų atsakymo, gali, kol laukiama 7 punkte nurodyto patikrinimo rezultatų, išduoti laikinąjį leidimą ne daugiau kaip šešiems mėnesiams.

16. Taip išduoti preliminarūs ir laikinieji leidimai nesuteikia teisės naudotis slaptumo žyma ES VISIŠKAI SLAPTAI pažymėta informacija; teisė naudotis šia informacija suteikiama tik pareigūnams, kurių pagal 7 punktą atlikto patikimumo tikrinimo rezultatai buvo teigiami. Laukiant tikrinimo rezultatų, pareigūnams, kuriuos prašoma patikrinti dėl galėjimo naudotis slaptumo žyma ES VISIŠKAI SLAPTAI pažymėta informacija, galima išduoti tiek preliminarius, tiek laikinuosius leidimus naudotis informacija, pažymėta ES SLAPTAI ar žemesnio laipsnio slaptumo žymomis.

VII SKYRIUS

ĮSLAPTINTOS ES MEDŽIAGOS RENGIMAS, PLATINIMAS, PERDAVIMAS, SAUGOJIMAS IR NAIKINIMAS

Turinys

Bendrosios nuostatos

Šiame skyriuje detalizuojamos šio priedo I dalies „Pagrindiniai saugumo principai ir minimalūs standartai“ 3 punkto a papunktyje apibrėžtos įslaptintų ES dokumentų rengimo, platinimo, perdavimo, saugojimo ir sunaikinimo priemonės. Juo kiekvienu konkrečiu atveju vadovaujamasi taikant šias priemones kitai įslaptintai ES medžiagai, atsižvelgiant į jos pobūdį.

I poskyris

Įslaptintų ES dokumentų rengimas ir platinimas

RENGIMAS

1. ES kategorijos slaptumo žymos ir kvalifikacinės žymos naudojamos II skyriuje nustatyta tvarka ir dedamos centre kiekvieno puslapio viršuje ir apačioje; puslapiai numeruojami. Kiekviename įslaptintame ES dokumente turi būti nurodomi jo numeris ir data. Dokumentuose, pažymėtuose slaptumo žymomis ES VISIŠKAI SLAPTAI ir ES SLAPTAI, dokumento numeris nurodomas kiekviename puslapyje. Jei platinamos kelios dokumento kopijos, kiekvienos iš jų pirmajame puslapyje kartu su bendru puslapių skaičiumi užrašomas kopijos numeris. Visi priedai ir pridedami dokumentai išvardijami dokumento su ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma pirmajame puslapyje.

2. Dokumentus su ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma spausdina, verčia, saugo, kopijuoja, kopijuoja į magnetines laikmenas arba mikrofilmuoja tik leidimą naudotis ne žemesnio už svarstomojo dokumento slaptumo žymos laipsnio įslaptinta ES informacija turintys asmenys, išskyrus šio skyriaus 27 punkte nurodytą atvejį.

   Įslaptintų dokumentų gamybą kompiuteriu reglamentuojančios nuostatos išdėstytos XI skyriuje.

PLATINIMAS

3. ES įslaptinta informacija platinama tik ją žinoti privalantiems asmenims, turintiems atitinkamus asmens patikimumo pažymėjimus. Pirmojo platinimo adresatus nustato dokumento autorius.

4. Slaptumo žyma ES VISIŠKAI SLAPTAI pažymėti dokumentai platinami per ES VISIŠKAI SLAPTAI registratūras (žr. VIII skyrių). Kompetentinga registratūra gali įgalioti ryšių centro vadovą padaryti tiek pranešimų su slaptumo žyma ES VISIŠKAI SLAPTAI kopijų, kiek nurodyta gavėjų sąraše.

5. Dokumentus su ES SLAPTAI ir žemesnio laipsnio slaptumo žyma gavėjas gali vadovaudamasis „būtina žinoti“ principu platinti kitiems adresatams. Tačiau dokumentą sukūrusios institucijos turi aiškiai suformuluoti norimus dokumento platinimo apribojimus. Kai tokie apribojimai yra nurodyti, adresatai gali perskirstyti dokumentus tik gavę juos pateikusių institucijų leidimą.

6. Kiekvieną dokumentą su ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma, jį atsiuntus į įstaigą ar iš jos išsiunčiant, registruoja įstaigos registratūra. Įrašyti duomenys (identifikacijos numeris, data, tam tikrais atvejais – kopijos numeris) turi padėti identifikuoti dokumentą ir yra įrašomi į registracijos knygą arba specialią apsaugotą kompiuterinę laikmeną.

II poskyris

Įslaptintų ES dokumentų perdavimas

PAKAVIMAS

7. Dokumentai su ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma perduodami patvariuose, nepermatomuose dvigubuose vokuose. Vidinis vokas pažymimas atitinkama ES slaptumo žyma, ir, jei įmanoma, ant jo taip pat yra užrašomos tikslios gavėjo pareigos ir jo adresas.

8. Atplėšti vidinį voką ir patvirtinti įdėtų dokumentų gavimą gali tik registro kontrolės pareigūnas arba jo pavaduotojas, jei laiškas nėra adresuotas konkrečiam asmeniui. Tokiu atveju atitinkama registratūra užregistruoja laiško gavimą, ir tik asmuo, kuriam jis adresuotas, gali atplėšti vidinį voką ir patvirtinti jame esančių dokumentų gavimą.

9. Gavimo kvitas įdedamas į vidinį voką. Kvite, kuris neįslaptinamas, nurodomas registracijos numeris, data ir dokumento kopijos numeris, tačiau niekada nenurodoma dokumento antraštė.

10. Vidinis vokas įdedamas į išorinį voką, ant kurio, kad būtų galima patvirtinti gavimą, nurodomas paketo numeris. Slaptumo žyma niekuomet nededama ant išorinio voko.

11. Dokumentams su ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma kurjeriams ir pasiuntiniams duodami pakvitavimai, kuriuose nurodomas gauto paketo numeris.

PERDAVIMAS PASTATE AR PASTATŲ KOMPLEKSE

12. Tam tikrame pastate ar pastatų komplekse įslaptinti dokumentai gali būti gabenami antspauduotame voke, ant kurio užrašoma tik adresato pavardė, jei tą voką gabena asmuo, turintis dokumento slaptumo žymos laipsnį atitinkantį patikimumo pažymėjimą.

ES DOKUMENTŲ PERDAVIMAS VALSTYBĖJE

13. Valstybėje slaptumo žyma ES VISIŠKAI SLAPTAI pažymėti dokumentai perduodami tik per oficialią kurjerių tarnybą arba asmenis, kuriems leista naudotis slaptumo žyma ES VISIŠKAI SLAPTAI pažymėta informacija.

14. Kai slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtam dokumentui perduoti už pastato arba pastatų komplekso ribų naudojamasi kurjerių tarnyba, laikomasi šiame skyriuje nustatytų įpakavimo ir kvitų išrašymo nuostatų. Pristatymo tarnybos turi būti taip aprūpintos darbuotojais, kad būtų užtikrinta, jog paketus su slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtais dokumentais visą laiką tiesiogiai prižiūrėtų atsakingas pareigūnas.

15. Išimtiniais atvejais slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtus dokumentus tik naudojimui posėdžiuose ir diskusijose už pastato arba pastatų komplekso ribų gali išsinešti pasiuntiniais nesantys pareigūnai, jeigu:

a) atitinkamas pareigūnas turi leidimą naudotis slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtais dokumentais;

b) gabenimo būdas atitinka dokumentų, pažymėtų nacionaline slaptumo žyma VISIŠKAI SLAPTAI, gabenimą reglamentuojančias nacionalines taisykles;

c) pareigūnas jokiomis aplinkybėmis nepalieka slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtų dokumentų be priežiūros;

d) yra pasirengta taip pasiimamų dokumentų sąrašą laikyti dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūroje, kurioje jie laikomi, juos pažymėti registre ir pagal šį sąrašą patikrinti grąžinus.

16. Konkrečioje valstybėje dokumentus, pažymėtus slaptumo žymomis ES SLAPTAI ir ES KONFIDENCIALIAI, galima siųsti arba paštu, jei tokį perdavimo būdą leidžia nacionalinės teisės aktai ir jis atitinka tokių teisės aktų nuostatas, arba per kurjerių tarnybą, arba per asmenis, kuriems yra suteiktas leidimas naudotis ES įslaptinta informacija.

17. Kiekviena valstybė narė arba ES decentralizuota agentūra, remdamasi šiais nuostatais, parengia instrukcijas įslaptintus ES dokumentus gabenantiems darbuotojams. Gabentojas privalo perskaityti ir pasirašyti tas instrukcijas. Visų pirma instrukcijose turi būti pabrėžta, kad dokumentai jokiomis aplinkybėmis:

a) negali likti be juos gabenančio asmens priežiūros, nebent jie saugiai padedami pagal IV skyriaus nuostatas;

b) negali likti be priežiūros viešajame transporte arba asmeniniame automobilyje, restoranuose, viešbučiuose ir panašiose vietose. Jų negalima laikyti viešbučių seifuose ar palikti be priežiūros viešbučių kambariuose;

c) negali būti skaitomi viešosiose vietose, pvz., lėktuvuose ar traukiniuose.

PERDAVIMAS IŠ VIENOS VALSTYBĖS NARĖS Į KITĄ

18. Medžiagą su ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma iš vienos valstybės narės į kitą gabena diplomatinių ar karinių kurjerių tarnybos.

19. Tačiau gali būti leista asmeniškai gabenti slaptumo žymomis ES SLAPTAI ir ES KONFIDENCIALIAI pažymėtą medžiagą, jei gabenimo sąlygos užtikrina, kad tokia medžiaga nepaklius į leidimo neturinčių asmenų rankas.

20. NSI gali leisti asmeniškai gabenti dokumentus tuomet, kai nėra galimybės pasinaudoti diplomatiniais arba kariniais kurjeriais arba kai pasinaudojus tokiais kurjeriais būtų vėluojama ir tai pakenktų ES veiklai, nes medžiaga adresatui skubiai reikalinga. Kiekviena valstybė narė parengia ES SLAPTAI ir žemesnio laipsnio slaptumo žyma pažymėtos medžiagos gabenimo iš vienos valstybės į kitą, kai tai daro diplomatiniais arba kariniais kurjeriais nesantys asmenys, instrukcijas. Instrukcijose reikalaujama, kad:

a) dokumentus gabenantis asmuo turėtų atitinkamą valstybių narių išduotą asmens patikimumo pažymėjimą;

b) visa tokiu būdu gabenama medžiaga būtų registruojama atitinkamame biure ar registratūroje;

c) ant paketų arba maišų su ES medžiaga būtų specialus spaudas, kuris užkirstų kelią muitinės tikrinimui, ir identifikavimo etiketės bei nurodymai radėjui;

d) dokumentus gabenantis asmuo su savimi turėtų visų ES valstybių pripažįstamą kurjerio pažymėjimą ir (arba) misijos orderį, įgalinantį jį gabenti atitinkamą paketą nurodytu būdu;

e) keliaujant sausuma, nebūtų kertama ES nepriklausančių valstybių teritorija ar jų sienos, išskyrus atvejus, kai siunčiančioji valstybė yra gavusi specialią tokios valstybės garantiją;

f) dokumentus gabenančio asmens kelionės tikslo, maršrutų ir transporto priemonių pasirinkimas atitiktų ES reglamentus arba atitinkamus nacionalinės teisės aktus, jei šie nustato griežtesnes taisykles;

g) medžiaga neliktų be ją gabenančio asmens priežiūros, išskyrus atvejus, kai ji saugiai padedama pagal IV skyriuje nurodytas saugaus laikymo taisykles;

h) medžiaga neliktų be priežiūros viešajame transporte arba privačiuose automobiliuose, restoranuose, viešbučiuose ir panašiose vietose. Jos negalima laikyti viešbučių seifuose ar palikti be priežiūros viešbučių kambariuose;

i) jei tarp gabenamos medžiagos yra dokumentų, jų negalima skaityti viešosiose vietose (pvz., lėktuvuose, traukiniuose ir pan.).

Įslaptintą medžiagą gabenti įgaliotas asmuo privalo perskaityti ir pasirašyti saugumo instrukciją, kurioje suformuluojami bent jau pirmiau išvardyti nurodymai ir procedūros, kurių reikia laikytis kritiniu atveju arba tuomet, kai paketą su įslaptinta medžiaga nori patikrinti muitinės arba oro uosto apsaugos pareigūnai.

ES RIBOTO NAUDOJIMO DOKUMENTŲ PERDAVIMAS

21. Dokumentų, pažymėtų ES RIBOTO NAUDOJIMO slaptumo žyma gabenimo nereglamentuoja jokios specialios nuostatos, tačiau turi būti užtikrinta, kad jie nepakliūtų į leidimo neturinčių asmenų rankas.

KURJERIŲ ASMENS PATIKIMUMAS

22. Visi slaptumo žymomis ES SLAPTAI ir ES KONFIDENCIALIAI pažymėtiems dokumentams gabenti įdarbinti kurjeriai ir pasiuntiniai privalo turėti atitinkamus asmens patikimumo pažymėjimus.

III poskyris

Elektroninės ir kitokios techninės perdavimo priemonės

23. Ryšių saugumo priemonės skirtos saugiam įslaptintos ES informacijos perdavimui užtikrinti. Įslaptintos ES informacijos perdavimui taikomos išsamios taisyklės išdėstytos XI skyriuje.

24. ES KONFIDENCIALIAI ir ES SLAPTAI slaptumo žymomis pažymėtą informaciją gali perduoti tik akredituoti ryšių centrai, tinklai ir (arba) terminalai bei sistemos.

IV poskyris

ES įslaptintų dokumentų papildomos kopijos, vertimai ir išrašai

25. Kopijuoti arba versti slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtus dokumentus galima tik dokumentų autoriui leidus.

26. Jei asmenys, neturintys asmens patikimumo pažymėjimų, suteikiančių teisę naudotis dokumentais su slaptumo žyma ES VISIŠKAI SLAPTAI, prašo informacijos, kuri, nors ir yra dokumentuose su slaptumo žyma ES VISIŠKAI SLAPTAI, bet jai ši žyma netaikoma, ES VISIŠKAI SLAPTAI registratūros vadovui gali būti leista parengti reikalingą kiekį to dokumento išrašų. Jis kartu imasi reikalingų veiksmų, užtikrindamas, kad tiems išrašams būtų suteikta tinkamo laipsnio slaptumo žyma.

27. Dokumentus su ES SLAPTAI ir žemesnio laipsnio slaptumo žyma adresatas gali kopijuoti ir versti laikydamasis nacionalinių saugumą reglamentuojančių teisės aktų ir tik tuomet, kai tai griežtai atitinka „būtina žinoti“ principą. Dokumentų kopijoms ir vertimams taikomos tos pačios saugumo priemonės, kaip ir dokumento originalui. ES decentralizuotos agentūros laikosi šių saugumo nuostatų.

V poskyris

ES įslaptintų dokumentų apžiūros, patikrinimai, saugojimas ir naikinimas

APŽIŪROS IR PATIKRINIMAI

28. Kasmet kiekviena VIII skyriuje nurodyta dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūra vadovaudamasi VIII skyriaus 9–11 punktų nuostatomis atlieka išsamią dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI apžiūrą. Žemesnio nei ES VISIŠKAI SLAPTAI slaptumo žymos laipsnio ES įslaptintų dokumentų vidiniai patikrinimai atliekami vadovaujantis nacionalinėmis rekomendacijomis, o TGS ir ES decentralizuotose agentūrose – Generalinio sekretoriaus – vyriausiojo įgaliotinio instrukcijomis.

Šie patikrinimai suteikia galimybę nustatyti, ar, dokumentų saugotojo nuomone:

a) galima sumažinti kai kurių dokumentų slaptumo žymos laipsnį arba juos išslaptinti;

b) dokumentai turėtų būti sunaikinti.

ĮSLAPTINTOS ES INFORMACIJOS ARCHYVAVIMAS

29. Kad būtų sumažinta archyvavimo problemų, visų registratūrų kontrolės pareigūnams leidžiama dokumentus, pažymėtus slaptumo žymomis ES VISIŠKAI SLAPTAI, ES SLAPTAI ir ES KONFIDENCIALIAI, mikrofilmuoti arba kitaip perrašyti į magnetines arba optines laikmenas, jei:

a) mikrofilmuoja/perrašo asmenys, turintys galiojantį darbui su atitinkamo slaptumo žymos laipsnio dokumentais tinkamą asmens patikimumo pažymėjimą;

b) mikrofilmas/laikmena saugomi taip pat saugiai, kaip ir dokumentų originalai;

c) apie kiekvieno dokumento su slaptumo žyma ES VISIŠKAI SLAPTAI mikrofilmavimą/perrašymą informuojamas jo autorius;

d) filmų ritėse arba kitose laikmenose laikomi tik dokumentai, pažymėti ta pačia slaptumo žyma ES VISIŠKAI SLAPTAI, ES SLAPTAI arba ES KONFIDENCIALIAI;

e) bet kurio dokumento, pažymėto žymomis ES VISIŠKAI SLAPTAI arba ES SLAPTAI, mikrofilmavimas/perrašymas aiškiai fiksuojamas metinės inventorizacijos apraše;

f) mikrofilmuotų arba kitaip perrašytų dokumentų originalai sunaikinami pagal 31–36 punktuose išdėstytas taisykles.

30. Šios taisyklės taip pat taikomos bet kuriai kitai NSI sankcionuotai saugojimo formai, pvz., elektromagnetinėms laikmenoms arba optiniams diskams.

ĮPRASTINIS ĮSLAPTINTŲ ES DOKUMENTŲ NAIKINIMAS

31. Kad ES įslaptinti dokumentai nebūtų be reikalo kaupiami, dokumentai, kuriuos įstaigos vadovas laiko pasenusiais arba kurių yra daugiau nei reikia, kaip įmanoma skubiau sunaikinami laikantis tokios tvarkos:

a) slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtus dokumentus sunaikina tik už juos atsakinga centrinė registratūra. Kiekvienas sunaikintas dokumentas užfiksuojamas sunaikinimo akte, kurį pasirašo dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI kontrolės pareigūnas ir naikinimą stebėjęs pareigūnas, turintis dirbti su dokumentais, pažymėtais slaptumo žyma ES VISIŠKAI SLAPTAI, tinkamą patikimumo pažymėjimą. Tai pažymima atitinkamoje registro knygoje;

b) sunaikinimo aktus kartu su platinimo žiniaraščiais registratūra saugo 10 metų. Kopijos dokumento autoriui arba atitinkamai centrinei registratūrai siunčiamos tik tuomet, kai jų paprašoma;

c) dokumentai su slaptumo žyma ES VISIŠKAI SLAPTAI, taip pat ir visos juos rengiant susidariusios atliekos, pavyzdžiui, sugadintos kopijos, juodraščiai, spausdinti užrašai ir naudotas kalkinis popierius, stebint dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registro kontrolės pareigūnui, sunaikinami juos sudeginant, paverčiant popieriaus mase, supjaustant arba kitaip susmulkinant, kad jie taptų neatgaminami ir neatkuriamos formos.

32. Slaptumo žyma ES SLAPTAI pažymėtus dokumentus vienu iš 31 punkto c papunktyje nurodytų būdų sunaikina už juos atsakinga registratūra, stebint asmens patikimumo pažymėjimą turinčiam asmeniui. Naikinami dokumentai su slaptumo žyma ES SLAPTAI išvardijami pasirašytuose sunaikinimo aktuose, kuriuos kartu su platinimo žiniaraščiais registratūra saugo ne mažiau kaip trejus metus.

33. Slaptumo žyma ES KONFIDENCIALIAI pažymėtus dokumentus vienu iš 31 punkto c papunktyje nurodytų būdų sunaikina už juos atsakinga registratūra, stebint asmens patikimumo pažymėjimą turinčiam asmeniui. Jų sunaikinimas užregistruojamas vadovaujantis nacionaliniais teisės aktais, o TGS ir ES decentralizuotose agentūrose – Generalinio sekretoriaus – vyriausiojo įgaliotinio instrukcijomis.

34. Slaptumo žyma ES RIBOTO NAUDOJIMO pažymėtus dokumentus, vadovaudamiesi nacionaliniais teisės aktais, o TGS ir ES decentralizuotose agentūrose – Generalinio sekretoriaus – vyriausiojo įgaliotinio instrukcijomis, sunaikina už juos atsakinga registratūra arba naudotojas.

NAIKINIMAS NENUMATYTAIS ATVEJAIS

35. TGS, valstybės narės ir ES decentralizuotos agentūros, atsižvelgdami į vietos sąlygas, parengia ES įslaptintos medžiagos apsaugojimo kritiniais atvejais planus, kurie prireikus gali apimti ir sunaikinimo ar evakuacijos nenumatytais atvejais planus. Savo žinioje esančioms organizacijoms jos pateikia instrukcijas, kurių būtina laikytis norint apsaugoti ES įslaptintą informaciją nuo patekimo į leidimo ja naudotis neturinčių asmenų rankas.

36. Priemonės, skirtos slaptumo žymomis ES SLAPTAI ir ES KONFIDENCIALIAI pažymėtai medžiagai apsaugoti ir (arba) sunaikinti kritiniais atvejais, jokiomis aplinkybėmis neturi pakenkti medžiagos, pažymėtos slaptumo žyma ES VISIŠKAI SLAPTAI, apsaugai arba sutrukdyti ją, taip pat ir šifravimo įrangą, sunaikinti – tai yra aukščiausio prioriteto užduotis. Priemones, kurių imamasi šifravimo įrangos apsaugai ir sunaikinimui nenumatytais atvejais, nustato specialios instrukcijos.

VI poskyris

Specialios Tarybai skirtiems dokumentams taikytinos taisyklės

37. TGS slaptumo žymomis ES SLAPTAI arba ES KONFIDENCIALIAI pažymėtą informaciją, esančią Tarybai skirtuose dokumentuose, prižiūri Įslaptintos informacijos biuras.

Būdamas pavaldus personalo ir administracijos generaliniam direktoriui, jis

a) administruoja su tokios informacijos registravimu, dauginimu, vertimu, siuntimu ir naikinimu susijusią veiklą;

b) veda įslaptintos informacijos registrą;

c) periodiškai kelia būtinybės išlaikyti informacijos įslaptinimą klausimą;

d) bendradarbiaudamas su Saugumo biuru, nustato praktinę informacijos įslaptinimo ir išslaptinimo tvarką.

38. Įslaptintos informacijos biuras veda šių duomenų registrą:

a) įslaptintos informacijos parengimo data;

b) slaptumo žymos laipsnis;

c) slaptumo žymos galiojimo terminas;

d) autoriaus pavardė ir padalinys;

e) gavėjas(-ai) ir jų eilės numeris;

f) antraštė;

g) numeris;

h) išplatintų kopijų skaičius;

i) Tarybai pateiktos įslaptintos informacijos aprašų rengimas;

j) įslaptintos informacijos išslaptinimo ir slaptumo žymos lapsnio sumažinimo registras.

39. TGS Įslaptintos informacijos biurui taikomos šio skyriaus I–V poskyriuose nustatytos bendrosios taisyklės, išskyrus atvejus, kai jas pakeičia šiame poskyryje išdėstytos specialios taisyklės.

VIII SKYRIUS

DOKUMENTŲ SU SLAPTUMO ŽYMA ES VISIŠKAI SLAPTAI REGISTRATŪROS

1. Dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūrų paskirtis – užtikrinti, kad dokumentai su slaptumo žyma ES VISIŠKAI SLAPTAI būtų registruojami, tvarkomi ir platinami laikantis saugumo nuostatų. Dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūroms kiekvienoje valstybėje narėje, TGS ir tam tikrais atvejais – ES decentralizuotose agentūrose vadovauja dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI kontrolės pareigūnas.

2. Centrinės registratūros valstybėse narėse, TGS ir ES decentralizuotose agentūrose, kuriose tokios registratūros įsteigtos, bei tam tikrais atvejais – kitose ES institucijose, tarptautinėse organizacijose ir trečiosiose šalyse, su kuriomis Taryba yra sudariusi sutartis dėl saugumo procedūrų keičiantis įslaptinta informacija, veikia kaip pagrindinė gaunančioji ir siunčiančioji institucija.

3. Prireikus steigiamos už vidinį slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtų dokumentų valdymą atsakingos subregistratūros; jos veda nuolat aktualizuojamą jų saugomų dokumentų platinimo registrą.

4. Esant ilgalaikiam poreikiui, I skyriuje nustatyta tvarka steigiamos centrinei dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūrai pavaldžios dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI subregistratūros. Jei slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtais dokumentais reikia naudotis tik kartais ir laikinai, tokie dokumentai gali būti išduodami ir nesteigiant dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI subregistratūros, jei nustatomos taisyklės, užtikrinančios, kad tie dokumentai išliktų atitinkamos dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūros kontroliuojami ir kad būtų laikomasi visų fizinių ir personalo saugumo priemonių.

5. Be specialaus centrinės dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūros leidimo subregistratūros negali tiesiogiai perduoti dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI kitoms tos pačios centrinės registratūros subregistratūroms.

6. Tai pačiai centrinei registratūrai nepriklausančios subregistratūros dokumentais su slaptumo žyma ES VISIŠKAI SLAPTAI keičiasi per centrines dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūras.

CENTRINĖS DOKUMENTŲ SU SLAPTUMO ŽYMA ES VISIŠKAI SLAPTAI REGISTRATŪROS

7. Kaip kontrolės pareigūnas, centrinės dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūros vadovas atsako už

   a) ES VISIŠKAI SLAPTAI dokumentų perdavimą pagal VII skyriaus nuostatas;

   b) visų jam pavaldžių dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI subregistratūrų, paskirtų kontrolės pareigūnų ir jų įgaliotų pavaduotojų pavardžių ir parašų sąrašo vedimą;

   c) iš registratūrų gautų kvitų už visų centrinės registratūros išplatintus slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtus dokumentus saugojimą;

   d) laikomų ir platinamų dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registro tvarkymą;

   e) nuolat atnaujinamo visų centrinių dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūrų, su kuriomis jis paprastai susirašinėja, jų paskirtų kontrolės pareigūnų bei įgaliotų jų pavaduotojų pavardžių ir parašų sąrašo vedimą;

   f) visų registratūroje laikomų slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtų dokumentų fizinį saugumą pagal IV skyriaus nuostatas.

DOKUMENTŲ SU SLAPTUMO ŽYMA ES VISIŠKAI SLAPTAI SUBREGISTRATŪROS

8. Kaip kontrolės pareigūnas, dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI subregistratūros vadovas atsako už

   a) dokumentų, pažymėtų slaptumo žyma ES VISIŠKAI SLAPTAI, perdavimą pagal VII skyriaus ir VIII skyriaus 5 ir 6 punktų nuostatas;

b) nuolat atnaujinamo visų turinčių teisę naudotis jo priežiūrima informacija su slaptumo žyma ES VISIŠKAI SLAPTAI asmenų sąrašo vedimą;

c) slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtų dokumentų platinimą pagal dokumento autoriaus instrukcijas arba pagal „būtina žinoti“ principą, pirmiausia patikrinus, ar adresatas turi būtiną asmens patikimumo pažymėjimą;

d) nuolat atnaujinamo visų slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtų dokumentų, laikomų ar cirkuliuojančių jam kontroliuojant, bei kitoms dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūroms perduotų dokumentų registro tvarkymą ir visų atitinkamų kvitų saugojimą;

e) nuolat atnaujinamo dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūrų, su kuriomis keistis slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtais dokumentais jis yra įgaliotas, paskirtų kontrolės pareigūnų ir jų pavaduotojų pavardžių ir parašų sąrašo vedimą;

f) visų subregistratūroje laikomų slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtų dokumentų fizinį saugumą pagal IV skyriaus nuostatas.

INVENTORIZACIJOS

9. Kas dvylika mėnesių kiekviena dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūra atlieka nuodugnią ES VISIŠKAI SLAPTAI dokumentų, už kuriuos ji atsako, inventorizaciją. Dokumentas laikomas inventorizuotu, jei jis fiziškai yra registratūroje, yra dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūros, į kurią jis išsiųstas, kvitas, dokumento sunaikinimo aktas arba nurodymas sumažinti šio dokumento slaptumo žymos laipsnį arba dokumentą išslaptinti.

10. Dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI subregistratūros kasmetinės inventorizacijos duomenis centrinei registratūrai, kuriai jos pavaldžios, perduoda jos nustatytą dieną.

11. NSI, taip pat tos ES institucijos, tarptautinės organizacijos ir ES decentralizuotos agentūros, kuriose įsteigta centrinė dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūra, ne vėliau kaip kiekvienų metų balandžio 1 d. pateikia Generaliniam sekretoriui – vyriausiajam įgaliotiniui centrinėse dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūrose atliktų kasmetinių inventorizacijų duomenis.

IX SKYRIUS

PER SPECIALIUS NE TARYBOS PATALPOSE VYKSTANČIUS POSĖDŽIUS, KURIUOSE SVARSTOMI SLAPTI KLAUSIMAI, TAIKYTINOS SAUGUMO PRIEMONĖS

BENDROSIOS NUOSTATOS

1. Kai Europos Vadovų Tarybos, Tarybos, ministrų ar kiti svarbūs posėdžiai vyksta ne Tarybos patalpose Briuselyje ir Liuksemburge, ir kai dėl svarstomų problemų ar informacijos didelio opumo būtina laikytis tam tikrų ypatingų saugumo reikalavimų, turi būti imamasi toliau išdėstytų saugumo priemonių. Šios priemonės skirtos tik įslaptintos ES informacijos apsaugai; gali būti numatytos ir kitos saugumo priemonės.

ATSAKOMYBĖ

Priimančiosios valstybės narės

2. Valstybė narė, kurios teritorijoje vyksta posėdis (priimančioji valstybė narė), bendradarbiaudama su TGS Saugumo biuru, atsako už Europos Vadovų Tarybos, Tarybos, ministrų bei kitų svarbių posėdžių saugumą ir už pagrindinių delegatų bei jų personalo fizinį saugumą.

Saugumo užtikrinimo požiūriu ji turi garantuoti, kad:

a) būtų parengti planai, kokių priemonių bus imtasi esant saugumo rizikai ar kilus su saugumu susijusių incidentų, ypač numatant ES įslaptintų dokumentų saugaus laikymo biuruose priemones;

b) būtų imtasi priemonių, leidžiančių naudotis Tarybos ryšių sistemomis įslaptintiems ES pranešimams gauti ir perduoti. Priimančioji valstybė narė prireikus taip pat užtikrina galimybę naudotis saugiomis telefono sistemomis.

Valstybės narės

3. Valstybių narių institucijos turi imtis reikiamų priemonių, užtikrinančių, kad:

a) signalu ar faksu tiesiogiai posėdžio saugumo pareigūnui arba per TGS Saugumo biurą būtų pateikti jų valstybių delegatų atitinkami asmens patikimumo pažymėjimai;

b) priimančiosios valstybės narės institucijos ir, jei reikia, TGS Saugumo biuras būtų informuojami apie kiekvieną konkrečią grėsmę, kad būtų galima imtis reikalingų veiksmų.

Posėdžio apsaugos pareigūnas

4. Paskiriamas saugumo pareigūnas, kuris atsako už bendrų vidaus saugumo priemonių bendrą parengimą bei kontrolę ir už koordinavimą su kitomis suinteresuotomis saugumo institucijomis. Priemonės, kurių jis imasi, daugiausia yra susijusios su:

a) i) apsaugos priemonėmis posėdžio vietoje, siekiant užtikrinti, kad posėdis vyktų be jokių pavojų bet kokios jame naudojamos ES įslaptintos informacijos saugumui galinčių sukelti incidentų;

ii) personalo, kuriam leidžiama būti posėdžio vietoje, delegacijų zonose ir konferencijų salėse, ir bet kokios įrangos tikrinimu;

iii) nuolatiniu koordinavimu su priimančiosios valstybės narės kompetentingomis institucijomis ir TGS Saugumo biuru;

b) saugumo instrukcijų įtraukimu į posėdžių dosjė, tinkamai atsižvelgiant į šiuose saugumo nuostatuose ir kitose svarbiose saugumo instrukcijose išdėstytus reikalavimus.

TGS Saugumo biuras

5. Rengiantis posėdžiui TGS Saugumo biuras veikia kaip patarėjas saugumo klausimais; prireikus jo atstovai turi padėti ir patarti posėdžio apsaugos pareigūnui ir delegacijoms.

6. Kiekviena posėdyje dalyvaujanti delegacija turi paskirti apsaugos pareigūną, kuris atsako už darbą saugumo klausimais savo delegacijoje, taip pat už ryšių su posėdžio apsaugos pareigūnu ir, prireikus, su TGS Saugumo biuro atstovu palaikymą.

SAUGUMO PRIEMONĖS

Saugumo zonos

7. Sukuriamos šios saugumo zonos:

   a) II klasės saugumo zona, į kurią pagal poreikį gali įeiti projektų rengimo kambarys, TGS biurai ir dauginimo įranga bei delegacijų biurai;

   b) I klasės saugumo zona, kurioje yra konferencijų salė ir vertėjų bei garso inžinierių kabinos;

   c) administracinės zonos, kuriose yra spaudos zona ir tos posėdžio vietos patalpos, kurios naudojamos administravimui, maitinimui ir apgyvendinimui, taip pat šalia spaudos centro ir posėdžio vietos esanti zona.

Leidimai

8. Delegacijų prašymu ir atsižvelgdamas į jų poreikius, posėdžio apsaugos pareigūnas turi išduoti atitinkamus leidimus. Jei reikia, skirtingoms saugumo zonoms išduodami skirtingi leidimai.

9. Posėdžio saugumo instrukcijose turi būti reikalaujama, kad posėdžių vietoje visi susiję asmenys matomoje vietoje visą laiką segėtų leidimus, kad prireikus apsaugos personalas galėtų juos patikrinti.

10. Be leidimus turinčių posėdžio dalyvių, į posėdžio vietą turėtų būti įleista kuo mažiau žmonių. Nacionalinės delegacijos, pageidaujančios posėdžio metu priimti lankytojus, turi apie tai informuoti posėdžio apsaugos pareigūną. Lankytojams išduodamas lankytojo leidimas. Užpildomas lankytojo leidimo formuliaras, kuriame įrašoma jo pavardė ir asmens, pas kurį jis atvyko, pavardė. Lankytoją visada turi lydėti apsaugos darbuotojas arba lankomas asmuo. Lankytojo leidimo formuliarą su savimi turi jį lydintis asmuo, kuris, kai lankytojas išeina iš posėdžio vietos, ją kartu su lankytojo leidimu grąžina apsaugos darbuotojams.

Fotografinės ir garso įrangos kontrolė

11. Į I klasės saugumo zoną negalima įsinešti kamerų ir įrašymo įrangos, išskyrus įrangą, kurią įsineša atitinkamą posėdžio apsaugos pareigūno leidimą gavę fotografai ir garso inžinieriai.

Portfelių, nešiojamųjų kompiuterių ir paketų tikrinimas

12. Paprastai leidimus įeiti į saugumo zoną turintys asmenys gali be tikrinimo įsinešti portfelius ir nešiojamuosius kompiuterius (tik turinčius savo maitinimo šaltinį). Jei delegacijoms pristatomi paketai, jos gali juos priimti, paketas tokiu atveju patikrinamas delegacijos apsaugos pareigūno, peršviečiamas specialia įranga arba jį atidaro ir patikrina apsaugos personalas. Jei posėdžio apsaugos pareigūnas mano, kad tai būtina, gali būti nustatytos griežtesnės portfelių ir paketų tikrinimo priemonės.

Techninis saugumas

13. Posėdžio salės techniniam saugumui užtikrinti gali būti pasitelkta techninio saugumo grupė, kuri taip pat gali rūpintis elektronine priežiūra posėdžio metu.

Delegacijų dokumentai

14. Delegacijos turi būti atsakingos už įslaptintų ES dokumentų pristatymą į posėdžius ir išsinešimą iš jų. Jos taip pat turi būti atsakingos už tų dokumentų patikrinimą ir saugumą, kai jie yra naudojami delegacijoms skirtose patalpose. Priimančiosios valstybės narės gali būti prašoma padėti gabenti įslaptintus dokumentus į posėdžio vietą ir iš jos.

Saugus dokumentų laikymas

15. Jei TGS, Komisija ar delegacijos negali savo įslaptintų dokumentų saugoti pagal nustatytus standartus, jie gali šiuos dokumentus antspauduotame voke pasirašytinai atiduoti saugoti posėdžio apsaugos pareigūnui, kad jis dokumentus saugotų pagal nustatytus standartus.

Kabinetų tikrinimas

16. Posėdžio apsaugos pareigūnas pasirūpina TGS ir delegacijų kabinetų patikrinimu kiekvienos darbo dienos pabaigoje, kad būtų užtikrinta, jog visi ES įslaptinti dokumentai būtų laikomi saugioje vietoje. Jei taip nėra, jis turi imtis reikalingų priemonių.

ES įslaptintos informacijos atliekų atidavimas

17. Visos atliekos turi būti laikomos ES įslaptinta informacija, o TGS bei delegacijos aprūpinamos joms išmesti skirtomis šiukšlių dėžėmis arba maišais. Prieš palikdami jiems skirtas patalpas TGS ir delegacijos nuneša atliekas posėdžių apsaugos pareigūnui, kuris organizuoja jų sunaikinimą pagal taisykles.

18. Pasibaigus posėdžiui visi TGS ir delegacijų turimi nebereikalingi dokumentai turi būti laikomi atliekomis. Prieš atšaukiant posėdžiui taikytas saugumo priemones, TGS ir delegacijų patalpos atidžiai apžiūrimos. Prireikus dokumentai, kuriems buvo išrašytas kvitas, turi būti sunaikinti VII skyriuje nurodyta tvarka.

X SKYRIUS

SAUGUMO PAŽEIDIMAI IR ĮSLAPTINTOS ES INFORMACIJOS NETEISĖTAS ATSKLEIDIMAS

1. Saugumas yra pažeidžiamas dėl Tarybos ar nacionalinėms saugumo nuostatoms prieštaraujančio veiksmo arba neveikimo, galinčio kelti pavojų įslaptintai ES informacijai arba ją neteisėtai atskleisti.

2. ES įslaptintos informacijos neteisėtu atskleidimu laikomas jos visos arba jos dalies patekimas į tam leidimo neturinčių asmenų rankas, t. y. į rankas tų asmenų, kurie neturi asmens patikimumo pažymėjimo arba neatitinka „būtina žinoti“ principo, arba jei yra tikimybė, kad tai atsitiko.

3. ES įslaptinta informacija gali būti neteisėtai atskleista dėl nerūpestingumo, neapdairumo ar neatsargumo, taip pat dėl prieš ES ar jos valstybes nares nukreiptos apie ES įslaptintą informaciją ar veiklą sužinoti siekiančių tarnybų arba ardomąja veikla užsiimančių organizacijų veiklos.

4. Svarbu, kad visi su ES įslaptinta informacija dirbantys asmenys būtų tinkamai informuojami apie saugumo procedūras, neatsargių pokalbių ir santykių su spauda keliamus pavojus. Jie turi suprasti, kaip svarbu iškart pranešti apie kiekvieną pastebėtą saugumo pažeidimą valstybės narės, institucijos ar agentūros, kurioje jie dirba, saugumo tarnybai.

5. Kai saugumo tarnyba nustato arba yra informuojama apie su ES įslaptinta informacija susijusį saugumo pažeidimą, ES įslaptintos informacijos praradimą arba dingimą, ji nedelsdama imasi veiksmų, kad:

   a) nustatytų faktus;

   b) įvertintų ir kiek įmanoma sumažintų padarytą žalą;

   c) neleistų tam pasikartoti;

   d) informuotų reikiamas institucijas apie saugumo pažeidimo pasekmes;

   Atsižvelgiant į tai, turi būti pateikta tokia informacija:

   i) atitinkamos informacijos apibūdinimas, įskaitant jos slaptumo žymą, registracijos ir kopijos numerius, datą, autorių, temą ir apimtį;

   ii) trumpas saugumo pažeidimo aplinkybių apibūdinimas, įskaitant datą ir laikotarpį, per kurį informacija galėjo būti neteisėtai atskleista;

   iii) pažymima, ar informuotas tos informacijos autorius.

6. Sužinojusi apie galimą saugumo pažeidimą, kiekviena saugumo institucija privalo nedelsdama apie šį faktą pranešti laikydamasi tokios tvarkos: dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI subregistratūra praneša TGS Saugumo biurui per jos centrinę dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI registratūrą; jei įvykęs įslaptintos ES informacijos atskleidimas priklauso valstybės narės jurisdikcijai, apie tai TGS Saugumo biurui 5 punkte nurodyta tvarka pranešama per atsakingą NSI.

7. Informacijos su slaptumo žyma ES RIBOTO NAUDOJIMO saugumo pažeidimus pranešti reikia tik tuomet, kai tie pažeidimai yra neįprasto pobūdžio.

8. Gavęs pranešimą apie padarytą saugumo pažeidimą, Generalinis sekretorius – vyriausiasis įgaliotinis:

   a) praneša apie tai atitinkamą įslaptintą informaciją sukūrusiai institucijai;

   b) paprašo atitinkamų saugumo institucijų pradėti tyrimą;

   c) koordinuoja tyrimą, kai jame dalyvauja daugiau nei viena saugumo institucija;

d) gauna ataskaitą apie pažeidimo aplinkybes, datą arba laikotarpį, kuriuo jis galėjo būti padarytas ir buvo nustatytas, taip pat išsamų atitinkamos medžiagos turinio ir slaptumo žymos laipsnio aprašymą. Be to, ataskaitoje pranešama apie ES arba vienos ar daugiau jos valstybių narių interesams padarytą žalą ir apie veiksmus, kurių imtasi siekiant neleisti pažeidimui pasikartoti.

9. Informaciją parengusi institucija informuoja dokumento adresatus ir duoda jiems atitinkamas instrukcijas.

10. Asmuo, dėl kurio kaltės buvo neteisėtai atskleista ES įslaptinta informacija, baudžiamas drausmine nuobauda pagal atitinkamas teisės normas ir nuostatas. Tokia nuobauda neužkerta kelio bet kokiems tolesniems teisiniams veiksmams.

XI SKYRIUS

INFORMACINIŲ TECHNOLOGIJŲ IR RYŠIŲ SISTEMOSE TVARKOMOS INFORMACIJOS APSAUGA

Turinys

I poskyris

Įvadas

BENDRIEJI ASPEKTAI

1. Šiame skyriuje pateikta saugumo politika ir reikalavimai taikomi visoms ryšių ir informacinėms sistemoms bei tinklams (toliau – SISTEMOS), kuriose tvarkoma ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma pažymėta informacija.

2. SISTEMOMS, apdorojama slaptumo žyma ES RIBOTO NAUDOJIMO pažymėta informacija, taip pat reikalingos tos informacijos slaptumą apsaugančios saugumo priemonės. Visoms SISTEMOMS būtinos saugumo priemonės, apsaugančios jų bei jose esančios informacijos vientisumą ir prieinamumą. Kokių saugumo priemonių toms sistemoms reikia, nustato įgaliota Saugumo akreditavimo institucija (SAI). Šios priemonės turi būti proporcingos įvertintai rizikai ir atitikti šiuose saugumo nuostatuose išdėstytą politiką.

3. Sensorinių sistemų, kuriose yra įmontuotos IT SISTEMOS, apsauga nustatoma ir apibrėžiama atsižvelgiant į visą sistemos, kurioms jos priklauso, kontekstą, kiek įmanoma laikantis atitinkamų šio skyriaus nuostatų.

GRĖSMĖS SISTEMOMS IR JŲ PAŽEIDŽIAMUMAS

4. Apibendrintai grėsmę galima apibrėžti kaip atsitiktinio arba sąmoningo pakenkimo saugumui galimybę. SISTEMŲ atžvilgiu, toks pakenkimas – tai vienos ar daugiau iš šių savybių praradimas: konfidencialumo, vientisumo ar prieinamumo – praradimas. Pažeidžiamumas apibrėžtinas kaip menka arba nepakankama kontrolė, kuri padėtų ar sudarytų galimybę atsirasti grėsmei tam tikram objektui arba tikslui. Pažeidžiamumas gali atsirasti dėl neveikimo arba būti susijęs su nepakankamai griežta, nuodugnia ir nuoseklia kontrole; jis gali būti techninio, procedūrinio ir operacinio pobūdžio.

5. Įslaptinta ir neįslaptinta ES informacija, tvarkoma SISTEMOSE greitam atkūrimui, perdavimui ir naudojimui pritaikyta koncentruota forma, yra atvira daugeliui grėsmių, įskaitant galimybę leidimo neturintiems vartotojams pasinaudoti informacija arba, atvirkščiai, neleidimą ja pasinaudoti leidimą turintiems vartotojams. Taip pat egzistuoja informacijos atskleidimo, klastojimo, keitimo arba ištrynimo neturint tam leidimo grėsmė. Be to, sudėtinga ir kartais jautri įranga yra brangi, neretai būna sunku ją greitai pataisyti arba pakeisti. Todėl šios SISTEMOS yra patrauklūs taikiniai žvalgybos operacijoms ir sabotažui, ypač jei manoma, kad saugumo priemonės yra neveiksmingos.

SAUGUMO PRIEMONĖS

6. Svarbiausia šiame skyriuje nurodytų saugumo priemonių paskirtis – apsaugoti ES įslaptintą informaciją nuo jos atskleidimo neturint tam leidimo (konfidencialumo praradimas) ir nuo jos vientisumo bei prieinamumo netekimo. Kad būtų užtikrintas tinkamas įslaptintą ES informaciją tvarkančios SISTEMOS saugumas, nustatomi tam tikri įprastinio saugumo standartai ir tam tikros atskirai kiekvienai SISTEMAI sukurtos specialios saugumo procedūros bei metodai.

7. Saugiai SISTEMOS darbo aplinkai sukurti numatomas ir įgyvendinamas subalansuotas saugos priemonių kompleksas. Šių priemonių taikymo sritys apima fizinius elementus, personalą, netechnines procedūras, kompiuterių ir ryšių operacines procedūras.

8. Kompiuterių saugumo priemonės (techninės ir programinės įrangos apsauginės savybės) reikalingos „būtina žinoti“ principui įgyvendinti, taip pat keliui neteisėtam informacijos atskleidimui užkirsti arba jam susekti. Kiek patikimos kompiuterių saugumo priemonės, nusprendžiama nustatant saugumo reikalavimus. Ar pakankamos kompiuterinio saugumo priemonių patikimumo garantijos, nustatoma akredituojant.

SPECIFINIŲ SISTEMOS SAUGUMO REIKMIŲ AKTAS (SSSRA)

9. Reikalaujama, kad visoms ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma pažymėtą informaciją tvarkančioms SISTEMOMS IT sistemų operacinė institucija (ITSOI), prireikus bendradarbiaujant bei talkinant projektų darbuotojams ir INFOSEC institucijai, turi surašyti specifinių SISTEMOS saugumo reikmių aktą (SSSRA), kurį patvirtina SAI. SSSRA taip pat reikalingas, jei SAI su naudojimosi ES RIBOTO NAUDOJIMO slaptumo žyma pažymėta arba neįslaptinta informacija galimybe bei jos vientisumu susijusią padėtį laiko kritiška.

10. SSSRA parengiamas pirminiame projekto etape ir plėtojamas bei tobulinamas vykdant projektą, o jo vaidmuo įvairiuose projekto ir SISTEMOS veikimo ciklo etapuose keičiasi.

11. SSSRA – tai įpareigojantis susitarimas tarp IT Sistemų operacinės institucijos ir SAI, pagal kurį turi būti akredituojama SISTEMA.

12. SSSRA išsamiai ir aiškiai nurodo saugumo principus, kuriais reikia vadovautis, ir išsamius saugumo reikalavimus, kurių reikia laikytis. Jis pagrįstas Tarybos saugumo politika ir rizikos įvertinimu arba jį nulemia operacijų aplinkos kriterijai, žemiausias personalo saugumo patikrinimo lygis, aukščiausias tvarkomos informacijos slaptumo žymos laipsnis, saugumo operacijų režimas arba vartotojo reikalavimai. SSSRA yra neatskiriama projekto dokumentų, pateikiamų atitinkamoms institucijoms tvirtinti techniniu, biudžeto ir saugumo aspektais, dalis. Galutinės formos SSSRA yra išsamus atitinkamos sistemos saugumo prielaidų aprašas.

SISTEMOS DARBO SAUGUMO REŽIMAI

13. Visos sistemos, apdorojančios ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma pažymėtą informaciją, akredituojamos dirbti vienu, o prireikus įvairiais laiko tarpais ir daugiau nei vienu iš toliau nurodytų darbo saugumo režimų arba jų nacionalinių atitikmenų:

a) priskirtas/dedikuotas;

b) aukšto lygio sistema;

c) daugialaipsnis.

II poskyris

Sąvokų apibrėžimai

PAPILDOMOS KVALIFIKACINĖS ŽYMOS

14. Kai reikia riboti įslaptintos informacijos platinimą ir ją tvarkyti specialiu būdu, šalia slaptumo žymų naudojamos papildomos kvalifikacinės žymos, tokios kaip CRYPTO arba bet kurios kitos ES pripažįstamos specialaus tvarkymo žymos.

15. PRISKIRTAS/DEDIKUOTAS DARBO SAUGUMO REŽIMAS yra toks režimas, kai VISI galimybę naudotis SISTEMA turintys asmenys turi leidimą naudotis aukščiausio SISTEMOJE tvarkomos informacijos slaptumo žymos laipsnio informacija ir pagal „būtina žinoti“ principą turi susipažinti su VISA SISTEMOJE tvarkoma informacija.

Pastabos:

1) kadangi visi naudotojai atitinka „būtina žinoti“ principą, SISTEMOJE nebūtina kompiuterinio saugumo priemonėmis atriboti skirtingos informacijos;

2) kitos saugumo priemonės (pvz., fizinės, personalo ir procedūrinės) turi atitikti reikalavimus, keliamus aukščiausiam SISTEMOJE tvarkomos informacijos slaptumo žymos laipsniui ir visoms informacijos kategorijoms.

16. AUKŠTO LYGIO SISTEMOS DARBO SAUGUMO REŽIMAS – toks darbo saugumo režimas, kai VISI galintys naudotis SISTEMA asmenys turi leidimą naudotis aukščiausio SISTEMOJE tvarkomos informacijos slaptumo žymos laipsnio informacija, tačiau NE VISI galintys naudotis SISTEMA asmenys laikomi turinčiais pagal „būtina žinoti“ principą susipažinti su visa SISTEMOJE tvarkoma informacija.

Pastabos:

1) tai, kad ne visi naudotojai atitinka „būtina žinoti“ principą, lemia, jog kompiuterinio saugumo priemonėmis turi būti užtikrinta atranka pagrįsta prieiga prie SISTEMOJE esančios informacijos ir galimybė ją atriboti;

2) kitos saugumo priemonės (pvz., fizinės, personalo ir procedūrinės) turi atitikti reikalavimus, keliamus aukščiausiam SISTEMOJE tvarkomos informacijos slaptumo žymos laipsniui ir visoms informacijos kategorijoms;

3) visa šiuo darbo režimu SISTEMOJE tvarkoma arba per ją gaunama informacija, taip pat visi apdoroti duomenys saugomi kaip atitinkamos kategorijos ir aukščiausio apdorotos informacijos slaptumo žymos laipsnio informacija, kol nenustatoma kitaip, išskyrus atvejus, kai esamo žymėjimo funkcionalumas yra pakankamai patikimas.

17. DAUGIALAIPSNIS DARBO SAUGUMO REŽIMAS – toks režimas, kai NE VISI galintys aukščiausio SISTEMOJE tvarkomos informacijos slaptumo žymos laipsnio informacija ir kai NE VISI galintys naudotis SISTEMA asmenys laikomi turinčiais pagal „būtina žinoti“ principą susipažinti su bendra SISTEMOJE tvarkoma informacija.

Pastabos:

1) šiuo metu šis darbo režimas leidžia tvarkyti įvairių slaptumo žymos laipsnių ir mišrių informacijos kategorijų informaciją;

2) tai, kad ne visi naudotojai atitinka „būtina žinoti“ principą ir ne visi asmenys turi naudotis aukščiausio slaptumo žymos laipsnio informacija leidžiančius asmens patikimumo pažymėjimus, lemia, kad kompiuterinio saugumo priemonėmis turi būti užtikrinta atranka pagrįsta prieiga prie SISTEMOJE esančios informacijos ir galimybė ją atriboti.

18. INFOSAUGA (INFOSEC) – saugumo priemonių taikymas siekiant ryšių, informacijos ir kitose elektroninėse sistemose apdorojamą, saugomą arba perduodamą informaciją apsaugoti nuo atsitiktinio ar tyčinio konfidencialumo, vientisumo ar prieinamumo praradimo ir neleisti prarasti pačių sistemų vientisumo ir prieinamumo. INFOSAUGOS priemonės – kompiuterių, perdavimo, skleidimo bei kriptografinio saugumo priemonės bei grėsmių informacijai bei SISTEMOMS atskleidimo, dokumentavimo ir atrėmimo priemonės.

19. KOMPIUTERIO SAUGUMAS (COMPUSEC) – tai techninės įrangos, mikroprogramų bei programinės įrangos saugumo savybių pritaikymas kompiuterio sistemai siekiant apsaugoti informaciją, užkirsti kelią neįgaliotiems asmenims ja manipuliuoti ir ją pakeisti/ištrinti arba apsisaugoti nuo sistemos išėjimo iš rikiuotės.

20. KOMPIUTERIO SAUGUMO PRODUKTAS – bendras kompiuterio saugumo modulis, integruojamas į IT sistemą, siekiant užtikrinti ar patobulinti tvarkomos informacijos konfidencialumui, vientisumui ar prieinamumui.

21. RYŠIŲ SAUGUMAS (COMSEC) – saugumo priemonių taikymas telekomunikacijoms, neleidžiant leidimo neturintiems asmenims pasinaudoti vertinga informacija, kurią jie gautų valdydami arba analizuodami ryšių srautus, arba garantuojant tokių ryšių srautų autentiškumą.

Pastaba:

Šios priemonės apima šifravimo, perdavimo ir skleidimo saugumą, taip pat procedūrų, fizinį, personalo, dokumentų ir kompiuterių saugumą.

22. VERTINIMAS – atitinkamos institucijos atliekamas nuodugnus techninis SISTEMOS saugumo aspektų arba šifravimo ar kompiuterio saugumo produkto tyrimas.

Pastabos:

1) vertinant tikrinama, ar yra reikalaujamos saugumo funkcijos, ar nėra pavojingo pašalinio tokių funkcijų poveikio, bei įvertinamas tokių funkcijų nepažeidžiamumas;

2) atliekant vertinimą nustatomas atitikimo SISTEMOS saugumo reikalavimams arba kompiuterio saugumo produktui keliamiems reikalavimams laipsnis, bei nustatomas SISTEMOS, šifravimo ar kompiuterio saugumo produkto patikimo funkcionavimo garantijų lygis.

23. SERTIFIKAVIMAS – oficialaus liudijimo, prie kurio pridedama nepriklausomo SISTEMOS saugumo reikalavimų atitikties arba kompiuterio saugumo produkto atitikties iš anksto apibrėžtiems saugumo reikalavimams laipsnio vertinimo eigos ir rezultatų apžvalga, išdavimas.

24. AKREDITACIJA – sistemai suteiktas leidimas jos operacinėje aplinkoje apdoroti ES įslaptintą informaciją ir jos patvirtinimas.

Pastaba:

Tokia akreditacija suteikiama įdiegus visas tinkamas saugumo procedūras ir pasiekus pakankamą sistemos išteklių apsaugos lygį. Paprastai akreditacija suteikiama remiantis SSSRA ir apima:

a) sistemos akreditavimo tikslo apibrėžimą, visų pirma, kokio slaptumo žymos laipsnio informacija bus apdorojama ir koks siūlomas sistemos arba tinklo darbo saugumo režimas (-ai);

b) rizikos valdymo apžvalgos parengimą pažeidžiamumui bei grėsmėms ir kovos su jomis priemonėms nustatyti;

c) operacines saugumo priemones (OSP) su išsamiu numatytų operacijų (pvz., numatomų režimų, funkcijų) aprašymu bei SISTEMOS saugumo ypatybių aprašymu, sudarančiu pagrindą akreditacijai;

d) saugumo savybių diegimo ir palaikymo planą;

e) sistemos saugumo arba tinklo saugumo pradinio bei tolesnio testavimo, vertinimo ir sertifikavimo planą;

f) sertifikavimą, jei reikia, kartu su kitais akreditavimo elementais.

25. IT SISTEMA – įrangos, metodų ir procedūrų, o prireikus ir personalo visuma, vykdanti informacijos apdorojimo funkcijas.

Pastabos:

1) tai informacijai sistemoje tvarkyti pritaikytų įrengimų visuma;

2) tokios sistemos gali palaikyti konsultavimo, valdymo, kontrolės, ryšių, mokslines ir administracines programas, įskaitant teksto apdorojimą;

3) sistemos ribomis paprastai bus laikomi vienos ITSOI kontroliuojami elementai;

4) IT sistema gali turėti posistemes, kai kurios iš jų pačios yra IT sistemos.

26. IT SISTEMOS APSAUGINĖS SAVYBĖS apima visas techninės įrangos, mikroprogramų ir programinės įrangos funkcijas, charakteristikas ir savybes; operacines procedūras, apskaitomumo procedūras ir prieigos kontrolės priemones, IT aplinką, nuotolinio terminalo (darbo vietos) aplinką, tvarkymo apribojimus, fizinę struktūrą bei įrangą ir personalo ir ryšių kontrolės priemones, būtinas pakankamam IT sistemoje tvarkomos įslaptintos informacijos apsaugos lygiui užtikrinti.

27. IT TINKLAS – visuma geografiškai viena nuo kitos nutolusių keitimuisi duomenimis tarpusavyje sujungtų IT sistemų, apimanti sujungtų IT sistemų sudedamąsias dalis bei jų sąsajas su pagalbiniais duomenų ar ryšių tinklais.

Pastabos:

1) IT tinklas gali naudotis vienu arba keliais, tarpusavyje keitimuisi duomenimis sujungtais ryšių tinklais; keletas IT tinklų gali naudotis bendru ryšių tinklu;

2) IT tinklas vadinamas „vietiniu“, jei jis jungia kelis vienoje vietoje esančius kompiuterius.

28. IT TINKLO APSAUGINĖS SAVYBĖS – tinklą sudarančių individualių IT sistemų apsauginės savybės kartu su papildomais komponentais ir savybėmis, susijusiais su pačiu tinklu (pvz., ryšiai tinkle, saugumo identifikavimo ir ženklinimo mechanizmai bei procedūros, prieigos kontrolės priemonės, programos ir audito takeliai), reikalingi pakankamam įslaptintos informacijos apsaugos lygiui užtikrinti.

29. IT APLINKA – zona, kurioje yra vienas arba daugiau kompiuterių, jų vietiniai periferiniai ir saugojimo įrengimai, valdymo įrengimai ir priskirta tinklo bei ryšių įranga.

Pastaba:

Šiai zonai nepriklauso atskiros zonos, kuriose yra periferinė įranga arba terminalai (darbo vietos), nors tokia įranga ir būtų sujungta su IT aplinkoje esančia įranga.

30. NUOTOLINIO TERMINALO (DARBO VIETOS) APLINKA – už IT aplinkos ribų esanti zona, kurioje yra kompiuterinė įranga, jos vietinė periferinė įranga ar terminalai (darbo vietos) ir bet kokia susijusi ryšių įranga.

31. TEMPEST apsaugos priemonės: saugumo priemonės, skirtos įrangos ir ryšių infrastruktūrai apsaugoti nuo įslaptintos informacijos atskleidimo be leidimo dėl netyčinio elektromagnetinio spinduliavimo.

III poskyris

Atsakomybė saugumo srityje

BENDROSIOS NUOSTATOS

32. I skyriaus 4 punkte apibrėžtos Saugumo komiteto pareigos apima ir INFOSEC klausimus. Saugumo komitetas savo veiklą organizuoja taip, kad galėtų teikti kvalifikuotas konsultacijas šiais klausimais.

33. Iškilus su saugumu susijusių problemų (įvyksta incidentas, padaromas pažeidimas ir t. t.), atsakinga nacionalinė institucija ir (arba) TGS Saugumo biuras nedelsdami imasi veiksmų. Apie visas problemas pranešama TGS Saugumo biurui.

34. Generalinis sekretorius – vyriausiasis įgaliotinis arba, tam tikrais atvejais, ES decentralizuotos agentūros vadovas įsteigia INFOSEC biurą; kuris pataria saugumo institucijai kaip SISTEMŲ dalis sukurtų specialių apsauginių savybių įgyvendinimo ir kontrolės klausimais.

SAUGUMO AKREDITACIJOS INSTITUCIJA (SAI)

35. SAI gali būti:

— NSI,

— Generalinio sekretoriaus – vyriausiojo įgaliotinio paskirta institucija,

— ES decentralizuotos agentūros saugumo institucija.

— jų deleguoti (paskirti) atstovai, priklausomai nuo to, kokia SISTEMA turi būti akredituota.

36. SAI pareiga – užtikrinti, kad SISTEMOS atitiktų Tarybos saugumo politiką. Viena iš jos užduočių – aprobuoti savo informacinėje aplinkoje iki tam tikro slaptumo žymos laipsnio įslaptintą ES informaciją tvarkančią sistemą. TGS ir tam tikrais atvejais – ES decentralizuotose agentūrose SAI Generalinio sekretoriaus – vyriausiojo įgaliotinio arba decentralizuotų agentūrų vadovų vardu vykdo su saugumu susijusias pareigas.

TGS SAI jurisdikcijai priklauso visos TGS patalpose veikiančios SISTEMOS. Valstybėje narėje veikiančios SISTEMOS ir SISTEMŲ sudedamosios dalys ir toliau priklauso tos valstybės narės jurisdikcijai. Kai įvairios SISTEMOS sudedamosios dalys patenka į TGS SAI ir kitų SAI jurisdikciją, visos šalys paskiria TGS SAI koordinuojamą jungtinę akreditacijos komisiją.

INFOSEC INSTITUCIJA (II)

37. INFOSEC institucija atsako už INFOSEC biuro veiklą. TGS ir tam tikrais atvejais – ES decentralizuotose agentūrose INFOSEC institucija atsako už:

— techninių konsultacijų ir pagalbos teikimą SAI,

— pagalbą kuriant SSSRA,

— SSSRA peržiūrą užtikrinant jo atitiktį šiems saugumo nuostatams, INFOSEC politikai ir struktūriniams dokumentams,

— dalyvavimą, kai reikia, akreditacijos grupėse (komisijose), ir INFOSEC rekomendacijų dėl akreditacijos teikimą SAI,

— paramą INFOSEC mokymo ir švietimo veiklai,

— techninių konsultacijų teikimą tiriant su INFOSEC susijusius incidentus,

— techninės politikos gairių nustatymą siekiant užtikrinti, kad būtų naudojama tik akredituota programinė įranga.

IT SISEMOS OPERACINĖ INSTITUCIJA (ITSOI)

38. INFOSEC institucija kuo ankstesniame etape perduoda ITSOI atsakomybę už SISTEMOS kontrolės priemonių ir specialiųjų apsauginių savybių įgyvendinimą bei veikimą. Ši atsakomybė išlieka per visą SISTEMOS egzistavimo laiką nuo projekto koncepcijos sukūrimo iki galutinio sistemos utilizavimo.

39. ITSOI atsako už visas visos SISTEMOS dalimi esančias saugumo priemones. Ji atsako už OSP parengimą. ITSOI detaliai apibrėžia saugumo standartus ir procedūras, kurių turi laikytis SISTEMOS tiekėjas.

40. Prireikus ITSOI gali dalį savo pareigų perduoti, pavyzdžiui, INFOSEC saugumo pareigūnui ir INFOSEC vietos saugumo pareigūnui. Tas pats asmuo gali vykdyti įvairias INFOSEC funkcijas.

VARTOTOJAI

41. Visi vartotojai privalo užtikrinti, kad jų veiksmai nepakenks SISTEMOS, kuria jie naudojasi, saugumui.

INFOSEC MOKYMAI

42. Prireikus TGS, ES decentralizuotose agentūrose ir valstybių narių Vyriausybinėse institucijose rengiami įvairaus lygio INFOSEC švietimas ir mokymai, skirti lygio personalui.

IV poskyris

Netechninės saugumo priemonės

PERSONALO SAUGUMAS

43. SISTEMOS vartotojai, atsižvelgiant į jų specifinėje SISTEMOJE apdorojamos informacijos slaptumo žymos laipsnį ir turinį, privalo turėti atitinkamus patikimumo pažymėjimus bei atitikti „būtina žinoti“ principą. Norintiesiems naudotis tam tikra įranga ar su SISTEMOS saugumu susijusia informacija, reikalingi specialūs Tarybos nustatyta tvarka išduodami leidimai.

44. SAI nustato visas saugumo prasme svarbias pareigybes ir apibrėžia patikimumo pažymėjimo bei priežiūros lygį, reikalingą visiems tas pareigas einantiems darbuotojams.

45. SISTEMOS apibrėžiamos ir sukuriamos taip, kad darbuotojų pareigas ir atsakomybę būtų galima paskirstyti neleidžiant vienam asmeniui įgyti visaapimančių žinių arba kontroliuoti esminių sistemos saugumo elementų. Siektina, kad, norint pakeisti arba tyčia pabloginti sistemą ar tinklą, būtų reikalingas dviejų arba daugiau asmenų sąmokslas.

FIZINIS SAUGUMAS

46. IT arba nuotolinio terminalo (darbo vietos) aplinka (apibrėžta 29 ir 30 punktuose), kurioje IT priemonėmis apdorojama informacija su ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma arba kurioje yra reali galimybė pasinaudoti tokia informacija, priklausomai nuo poreikio, įrengiamos kaip ES I ir II klasės saugumo zonos arba jų nacionaliniai atitikmenys.

47. IT ir nuotolinio terminalo (darbo vietos) aplinkoje, kurioje gali būti keičiamas SISTEMOS saugumas, negali dirbti tik vienas leidimą turintis pareigūnas ar kitas darbuotojas.

PRIEIGOS PRIE SISTEMOS KONTROLĖ

48. Visa informacija ir medžiaga, kuri įgalina kontroliuoti prieigą prie SISTEMOS, saugoma pagal aukščiausiam informacijos, kuria naudotis ji sudaro galimybę, slaptumo žymos laipsniui ir atitinkamai informacijos kategorijai taikomus reikalavimus.

49. Kai prieigos kontrolės informacija ir medžiaga nebenaudojama šiuo tikslu, ji sunaikinama pagal 61–63 punktų nuostatas.

V poskyris

Techninės saugumo priemonės

INFORMACIJOS SAUGUMAS

50. Informacijos autoriui pavedama identifikuoti ir įslaptinti visus informacijos turinčius dokumentus, nepriklausomai nuo to, ar tai spausdintinės kopijos, ar kompiuterinių duomenų saugojimo laikmenos. Kiekvienas spausdintinės kopijos lapas pažymimas puslapio viršuje ir apačioje nurodoma slaptumo žyma. Tiek spausdintinei, tiek kompiuterinių duomenų saugojimo laikmenose laikomai informacijai suteikiama to laipsnio slaptumo žyma, kuria buvo pažymėta aukščiausio slaptumo žymos laipsnio dokumentą sudarant panaudota informacija. SISTEMOS veikimo būdas taip pat gali turėti įtakos ta sistema sudarytos informacijos slaptumo žymos laipsniui.

51. Organizacijai ir jos informacijos turėtojams pavedama apsvarstyti atskirų informacijos elementų sujungimo problemas bei išvadas, darytinas iš susijusių elementų, ir nustatyti, ar informacijos visumai neturėtų būt suteiktas aukštesnis slaptumo žymos laipsnis.

52. Tai, kad informacija gali būti sutrumpinimo kodas, perdavimo kodas arba bet kokios formos binarinė išraiška, nesuteikia jokios saugumo garantijos, todėl neturėtų įtakoti informacijos įslaptinimo.

53. Perduodant informaciją iš vienos SISTEMOS į kitą, perdavimo metu ir priimančiojoje SISTEMOJE ji saugoma originalią informacijos slaptumo žymą ir kategoriją atitinkančiu būdu.

54. Visos kompiuterinių duomenų saugojimo laikmenos tvarkomos saugomos informacijos aukščiausio laipsnio slaptumo žymą arba laikmenų žymėjimą atitinkančiu būdu ir yra visuomet tinkamai saugomos.

55. Pakartotinai užrašyti ES įslaptintą informaciją naudojamos kompiuterinių duomenų saugojimo laikmenos išlaiko aukščiausio laipsnio slaptumo žymą, kuria jos kada nors buvo naudojamos, kol tos informacijos slaptumo žymos laipsnis nėra sumažinamas ar ta informacija nėra išslaptinama, arba kol laikmenų slaptumo žymos laipsnis nėra atitinkamai sumažinamas arba jos nėra išslaptinamos ar sunaikinamos TGS ar valstybės nustatyta tvarka (žr. 61–63 punktus).

INFORMACIJOS KONTROLĖ IR ATSKAITOMYBĖ

56. Naudojimasis ES SLAPTAI ir aukštesnio laipsnio slaptumo žyma pažymėta informacija registruojamas ir protokoluojamas automatiškai (audito takeliai) arba ranka. Protokolai saugomi vadovaujantis šiais saugumo nuostatais.

57. IT aplinkoje laikoma ES įslaptinta informacija gali būti tvarkoma kaip vienas įslaptintas dokumentas ir neturi būti registruojama, jei medžiaga yra identifikuota, pažymėtas jos slaptumo žymos laipsnis bei ji yra tinkamai kontroliuojama.

58. Kai informacija surenkama iš ES įslaptintą informaciją tvarkančios SISTEMOS ir iš IT aplinkos perduodama į nuotolinio terminalo (darbo vietos) aplinką, SAI pritarus nustatomos informacijos kontrolės ir registravimo procedūros. Informacijai su ES SLAPTAI ir aukštesnio laipsnio slaptumo žyma prie tokių procedūrų priskiriami specialūs nurodymai dėl informacijos apskaitomybės.

IŠIMAMŲ KOMPIUTERINIŲ DUOMENŲ SAUGOJIMO LAIKMENŲ TVARKYMAS IR KONTROLĖ

59. Visos išimamos kompiuterinių duomenų saugojimo laikmenos su ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma tvarkomos kaip medžiaga ir joms taikomos bendros taisyklės. Atitinkamus identifikavimo ir įslaptinimo žymenis reikia priderinti prie konkrečios laikmenų fizinės išvaizdos, kad jie būtų aiškiai atpažįstami.

60. Vartotojai atsako už tai, kad ES įslaptinta informacija būtų laikoma atitinkama slaptumo žyma pažymėtose ir tinkamai saugomose laikmenose. Nustatoma tvarka, užtikrinanti, kad visų slaptumo žymos laipsnių ES įslaptinta informacija kompiuterinių duomenų saugojimo laikmenose būtų saugoma pagal šiuos saugumo nuostatus.

KOMPIUTERINIŲ DUOMENŲ SAUGOJIMO LAIKMENŲ IŠSLAPTINIMAS IR NAIKINIMAS

61. TGS arba valstybės patvirtinta tvarka kompiuterinių duomenų saugojimo laikmenų, naudojamų ES įslaptintai informacijai įrašyti, slaptumo žymos laipsnis gali būti sumažintas arba jos gali būti išslaptintos.

62. Kompiuterinių duomenų saugojimo laikmenos, kuriose buvo saugota slaptumo žyma ES VISIŠKAI SLAPTAI pažymėta įslaptinta informacija arba ypatingos kategorijos informacija, neišslaptinamos ir pakartotinai nenaudojamos.

63. Jei kompiuterinių duomenų saugojimo laikmenų negalima išslaptinti arba pakartotinai panaudoti, jos sunaikinamos TGS arba valstybės patvirtinta tvarka.

RYŠIŲ SAUGUMAS

64. Kai ES įslaptinta informacija yra perduodama elektromagnetinio ryšio priemonėmis, taip perduodamos informacijos konfidencialumui, vientisumui ir prieinamumui užtikrinti taikomos specialios priemonės. SAI nustato perdavimų apsaugos nuo pasiklausymo ir perėmimo reikalavimus. Ryšių sistemoje perduodama informacija saugoma laikantis konfidencialumo, vientisumo ir prieinamumo užtikrinimo reikalavimų.

65. Kai konfidencialumui, vientisumui ir prieinamumui užtikrinti yra reikalingi šifravimo metodai, tokius metodus ir su jais susijusias priemones specialiai tam tikslui patvirtina SAI.

66. Perduodant informaciją su ES SLAPTAI ir aukštesnio laipsnio slaptumo žyma konfidencialumas saugomas taikant Tarybos pagal Tarybos Saugumo komiteto rekomendaciją patvirtintus šifravimo metodus arba priemones. Perduodant žymomis ES KONFIDENCIALIAI ar ES RIBOTO NAUDOJIMO pažymėtą informaciją, konfidencialumas saugomas taikant GS-VĮ pagal Tarybos Saugumo komiteto rekomendaciją arba valstybės narės patvirtintus šifravimo metodus arba priemones.

67. ES įslaptintos informacijos perdavimo taisyklės detaliai išdėstomos specialiose Tarybos pagal Tarybos Saugumo komiteto rekomendaciją patvirtintose saugumo instrukcijose.

68. Esant išskirtinėms aplinkybėms, žymomis ES RIBOTO NAUDOJIMO, ES KONFIDENCIALIAI ir ES SLAPTAI pažymėta informacija gali būti perduodama atviru tekstu, kiekvienam tokiam atvejui gavus aiškų leidimą. Tokios išskirtinės aplinkybės yra:

a) gresianti arba esama krizė, konfliktas arba karinė padėtis;

b) kai ypač svarbus yra perdavimo greitis, o šifravimo priemonės nepasiekiamos, ir kai manoma, kad perduodama informacija negalės būti laiku panaudota siekiant pakenkti operacijoms.

69. SISTEMA turi būti pajėgi prireikus neleisti pasinaudoti įslaptinta informacija vienoje ar visose nuotolinėse darbo vietose ar terminaluose arba ją fiziškai išjungiant, arba specialių SAI aprobuotų programinės įrangos funkcijų pagalba.

DIEGIMO IR SPINDULIAVIMO SAUGUMAS

70. Pradinis sistemų instaliavimas ir kiekvienas svarbesnis jų pakeitimas organizuojamas taip, kad jį atliktų tik asmens patikimumo pažymėjimus turintys sistemų instaliavimo specialistai, nuolat prižiūrimi techniškai kvalifikuoto personalo, turinčio patikimumo patikrinimo pažymėjimus, leidžiančius naudotis ES įslaptinta informacija, kuri pagal slaptumo žymos laipsnį atitinka aukščiausią informacijos, kuri bus saugoma ir tvarkoma atitinkama sistema, slaptumo žymos laipsnį.

71. Visa įranga instaliuojama laikantis aktualios Tarybos saugumo politikos.

72. SISTEMOS, kuriose apdorojama ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma pažymėta informacija, saugomos taip, kad jų saugumui negrėstų neteisėto informacijos atskleidimo dėl elektromagnetinio spinduliavimo pavojus, kurio tyrimo ir kontrolės priemonės vadinamos „TEMPEST“.

73. TEMPEST apsaugos priemones TGS ir ES decentralizuotų agentūrų įrangai patikrina ir patvirtina TGS saugumo institucijos paskirta TEMPEST įstaiga. Įslaptintą ES informaciją tvarkančios nacionalinės įrangos patvirtinimo institucija pripažįstama nacionalinė TEMPEST patvirtinimo institucija.

VI poskyris

Saugumas tvarkant įslaptintą informaciją

OPERACINĖS SAUGUMO PRIEMONĖS

74. OSP apibrėžia saugumo principus, kuriais turi būti vadovaujamasi saugumo reikalais, operacines procedūras, kurių turi būti laikomasi, ir darbuotojų pareigas. Už OSP parengimą atsako ITSOI.

PROGRAMINĖS ĮRANGOS APSAUGOS/KONFIGŪRACIJOS TVARKYMAS

75. Taikomųjų programų saugumas įvertinamas remiantis pačios programos įslaptinimo įvertinimu, o ne pagal informacijos, kurią ji turi apdoroti, įslaptinimą. Naudojamos programinės įrangos versijos reguliariai tikrinamos siekiant užtikrinti jų vientisumą ir tinkamą veikimą.

76. Naujos ar pakeistos programinės įrangos versijos ES įslaptintai informacijai apdoroti nenaudojamos tol, kol jų nepatikrina ITSOI.

TIKRINIMAS, AR NĖRA KENKSMINGOS PROGRAMINĖS ĮRANGOS AR KOMPIUTERIŲ VIRUSŲ

77. Pagal SAI reikalavimus reguliariai tikrinama, ar neatsirado kenksmingos programinės įrangos ar kompiuterių virusų.

78. Visos į TGS, ES decentralizuotas agentūras ar valstybes nares patenkančios kompiuterinių duomenų saugojimo laikmenos prieš jas instaliuojant į kurią nors SISTEMĄ patikrinamos, kad būtų įsitikinta, jog jose nėra kenksmingos programinės įrangos ar kompiuterių virusų.

APTARNAVIMAS

79. Planinio ir neplaninio sistemų, kurioms yra parengtas SSRS, aptarnavimo sutartys ir tvarka tiksliai apibrėžia reikalavimus ir priemones jo į IT aplinką patenkančiam aptarnavimo personalui ir įsinešamai įrangai.

80. Reikalavimai aiškiai išdėstomi SSSRA, o procedūros – OSP. Rangovo aptarnavimo paslaugos, kai reikia pasinaudoti nuotolinėmis diagnostinėmis procedūromis, leistinos ypatingais atvejais, esant griežtai saugumo kontrolei ir tik turint SAI leidimą.

VII poskyris

Tiekimas

81. Bet koks įgyjamas SISTEMOJE naudojamas saugumo produktas turi būti jau įvertintas ir sertifikuotas arba tuo metu vertinamas ar sertifikuojamas. Tai pagal tarptautiniu mastu pripažintus kriterijus (pvz., Bendrieji informacinių technologijų saugumo vertinimo kriterijai, žr. ISO 15 408) turi atlikti atitinkama vertinimo ar sertifikavimo įstaiga.

82. Sprendžiant, ar įranga, ypač kompiuterinių duomenų saugojimo laikmenos, turėtų būti nuomojamos, o ne perkamos, reikia turėti omenyje, kad tokia įranga, kartą panaudota tvarkant įslaptintą ES informaciją, negali būti vėl išnuomota už tam tikros saugios aplinkos ribų, prieš tai SAI sutikimu jos neišslaptinus, kuris galimas tik leidus SAI, o ši ne visada duos tokį leidimą.

AKREDITACIJA

83. Visas SISTEMAS, kurioms turi būti parengtas SSSRA, prieš pradedant jomis tvarkyti ES įslaptintą informaciją turi akredituoti SAI, remdamasi SSSRA, OSP ir kituose susijusiuose dokumentuose pateikta informacija. Posistemės ir nuotoliniai terminalai (darbo vietos) akredituojami kaip visų SISTEMŲ, su kuriomis jie yra sujungti, dalis. Kai SISTEMĄ naudoja ir Taryba, ir kitos organizacijos, TGS ir atitinkamos saugumo institucijos tarpusavyje susitaria dėl akreditacijos.

84. Akreditacija gali būti vykdoma pagal konkrečiai SISTEMAI pritaikytą ir SAI apibrėžtą akreditacijos strategiją.

VERTINIMAS IR SERTIFIKAVIMAS

85. Tam tikrais atvejais prieš akreditaciją SISTEMOS techninės įrangos, mikroprogramų ir programinės įrangos saugumo savybės įvertinamos ir sertifikuojamos kaip tinkamos reikiamo slaptumo žymos laipsnio informacijai saugoti.

86. Reikalavimai įvertinimui ir sertifikavimui yra sistemos planavimo dalis ir turi būti aiškiai išdėstyti SSSRA.

87. Vertinimą ir sertifikavimą pagal patvirtintas rekomendacijas ITSOI vardu atlieka techniškai kvalifikuotas ir tinkamus patikimumo pažymėjimus turintis personalas.

88. Atitinkamą personalą gali skirti valstybės narės paskirta vertinimo ir sertifikavimo institucija arba jos paskirti atstovai, pvz., kompetentingi ir patikrinti rangovai.

89. Vertinimas ir sertifikavimas gali būti supaprastinamas (pvz., vertinami tik integravimo aspektai), jei sistemos yra pagrįstos nacionaliniu lygiu įvertintais ir sertifikuotais kompiuterio saugumo produktais.

ĮPRASTAS SAUGUMO SAVYBIŲ TIKRINIMAS TĘSTINIAM AKREDITAVIMUI

90. ITSOI nustato įprastos kontrolės procedūras, užtikrinančias, kad visos SISTEMOS saugumo savybės ir toliau būtų veiksmingos.

91. Pokyčių, dėl kurių būtų reikalinga pakartotinė akreditacija arba išankstinis SAI pritarimas, tipai aiškiai nurodomi ir suformuluoti SSSRA. Po kiekvieno pakeitimo, remonto ar gedimo, galinčio paveikti SISTEMOS saugumo savybes, ITSOI pasirūpina, kad būtų atliktas patikrinimas, užtikrinantis tinkamą saugumo savybių veikimą. SISTEMOS akreditacijos pratęsimas paprastai priklauso nuo teigiamų patikrinimų rezultatų.

92. Visas SISTEMAS, kuriose yra įdiegtos saugumo savybės, reguliariai tikrina arba kontroliuoja SAI. Slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtą informaciją apdorojančios SISTEMOS tikrinamos ne rečiau kaip kartą per metus.

VIII poskyris

Laikinas ar atsitiktinis naudojimas

MIKROKOMPIUTERIŲ AR ASMENINIŲ KOMPIUTERIŲ SAUGUMAS

93. Mikrokompiuteriai ar asmeniniai kompiuteriai (AK) su fiksuotais diskais (ar kitokiomis pastoviomis laikmenomis), veikiantys atskirai arba sujungti į tinklą, bei nešiojamoji kompiuterinė įranga (pvz., nešiojamieji AK ir elektroninės „užrašų knygutės“) su fiksuotais kietaisiais diskais, laikomi informacijos laikmenomis ta pačia prasme, kaip ir lankstieji diskeliai arba kitos išimamos kompiuterinių duomenų saugojimo laikmenos.

94. Šiai įrangai suteikiamos apsaugos – prieigos, apdorojimo, saugojimo ir gabenimo atžvilgiu – lygmuo turi atitikti bet kada joje laikytos arba apdorotos informacijos aukščiausią slaptumo žymos laipsnį (tol, kol tas laipsnis nebus nustatyta tvarka sumažintas arba informacija nebus išslaptinta).

NUOSAVOS IT ĮRANGOS NAUDOJIMAS ATLIEKANT TARNYBINES PAREIGAS TARYBOJE

95. Dirbant su įslaptinta ES informacija draudžiama naudoti nuosavas išimamas kompiuterinių duomenų saugojimo laikmenas, programinę įrangą ir ir IT techninę įrangą (pvz., asmeninius kompiuterius ir nešiojamąją kompiuterinę įrangą), galinčius saugoti informaciją.

96. Nuosava techninė įranga, programinė įranga ir laikmenos negali būti įnešamos į I ir II klasės zonas, kuriose dirbama su įslaptinta ES informacija, be TGS Saugumo biuro, valstybės narės institucijos ar atitinkamos ES decentralizuotos agentūros vadovo leidimo.

RANGOVUI PRIKLAUSANČIOS ARBA VALSTYBIŲ NARIŲ PATIEKTOS IT ĮRANGOS NAUDOJIMAS ATLIEKANT TARNYBINES PAREIGAS TARYBOJE

97. Prie oficialios Tarybos veiklos prisidedančiose organizacijose naudoti rangovui priklausančią IT ir programinę įrangą gali leisti TGS Saugumo biuro, valstybės narės institucijos ar atitinkamos ES decentralizuotos agentūros vadovas. TGS ar ES decentralizuotų agentūrų darbuotojams taip pat gali būti leista naudoti valstybių narių patiektą IT ir programinę įrangą; tokiu atveju IT įranga perduodama atitinkamai TGS inventoriaus kontrolei. Bet kuriuo atveju, jei IT įranga naudojama ES įslaptintai informacijai apdoroti, konsultuojamasi su SAI, kad būtų tinkamai apsvarstyti ir įgyvendinti naudojant tą įrangą taikytini INFOSEC elementai.

XII SKYRIUS

ĮSLAPTINTOS ES INFORMACIJOS PERDAVIMAS TREČIOSIOMS ŠALIMS ARBA TARPTAUTINĖMS ORGANIZACIJOMS

ĮSLAPTINTOS ES INFORMACIJOS PERDAVIMĄ REGLAMENTUOJANTYS PRINCIPAI

1. Taryba priima sprendimą dėl įslaptintos ES informacijos perdavimo trečiosioms šalims arba tarptautinėms organizacijoms, atsižvelgdama į:

   — tokios informacijos pobūdį ir turinį,

   — gavėjui taikomą „būtina žinoti“ principą,

   — naudos Europos Sąjungai įvertinimą.

   Prašoma rengiamą perduoti įslaptintą ES informaciją rengusios valstybės narės sutikimo.

2. Sprendimai kiekvienu atveju priimami atskirai, atsižvelgiant į:

   — siekiamą bendradarbiavimo su atitinkamomis trečiosiomis šalimis arba tarptautinėmis organizacijomis laipsnį,

   — jų patikimumą, priklausantį nuo saugumo lygio, kuris būtų užtikrintas toms valstybėms ar organizacijoms patikėtai įslaptintai ES informacijai, ir į jose taikomų saugumo taisyklių atitiktį ES taisyklėms; Tarybos Saugumo komitetas šiuo klausimu pateikia Tarybai savo techninę išvadą.

3. Priimdamos ES įslaptintą informaciją, trečiosios šalys arba tarptautinės organizacijos garantuoja, kad perduota informacija nebus naudojama jokiems kitiems tikslams, išskyrus tuos, dėl kurių informacija yra perduodama arba ja yra keičiamasi, ir kad užtikrins Tarybos reikalaujamą apsaugą.

LYGIAI

4. Nusprendusi, kad įslaptinta informacija gali būti perduodama tam tikrai valstybei ar tarptautinei organizacijai arba su ja gali būti keičiamasi ta informacija, Taryba priima sprendimą dėl galimo bendradarbiavimo lygio. Jis ypač priklauso nuo tos valstybės ar tarptautinės organizacijos taikomos saugumo politikos ir nuostatų.

5. Yra trys bendradarbiavimo lygiai:

   1 lygis

   Bendradarbiavimas su trečiosiomis šalimis ar tarptautinėmis organizacijomis, kurių saugumo politika ir nuostatai yra labai artimos ES saugumo politikai ir nuostatoms.

   2 lygis

   Bendradarbiavimas su trečiosiomis šalimis ar tarptautinėmis organizacijomis, kurių saugumo politika ir nuostatai žymiai skiriasi nuo ES saugumo politikos ir nuostatų.

   3 lygis

   Bendradarbiavimas retkarčiais su trečiosiomis šalimis ar tarptautinėmis organizacijomis, kurių saugumo politikos ir nuostatų negalima įvertinti.

6. Kiekvienas bendradarbiavimo lygis nulemia saugumo nuostatas, parengiamas atskirai kiekvienam konkrečiam atvejui atsižvelgiant į Tarybos Saugumo komiteto techninę nuomonę, kurias taikyti bus prašoma gavėjų, siekiant apsaugoti jiems perduotą įslaptintą informaciją. Šios procedūros ir saugumo nuostatos išdėstytos 4, 5 ir 6 priedėliuose.

SUTARTYS

7. Nusprendusi, kad yra nuolatinis arba ilgalaikis poreikis keistis įslaptinta informacija su trečiosiomis šalimis ar kitomis tarptautinėmis organizacijomis, Taryba su jomis sudaro „Susitarimus dėl saugumo keičiantis įslaptinta informacija tvarkos“, kuriuose apibrėžiami bendradarbiavimo tikslai ir abipusės informacijos, kuria keičiamasi, apsaugos taisyklės.

8. Esant 3 lygio bendradarbiavimui, kurį apibrėžimas apriboja laiko ir tikslo atžvilgiu, vietoje „Susitarimo dėl saugumo keičiantis įslaptinta informacija tvarkos“ gali pakakti paprasto supratimo memorandumo, apibrėžiančio įslaptintos informacijos, kuria bus keičiamasi, pobūdį ir abipusius įsipareigojimus dėl tos informacijos, jei jos slaptumo žymos laipsnis ne aukštesnis už ES RIBOTO NAUDOJIMO.

9. Prieš pateikiant susitarimų dėl saugumo tvarkos ir supratimo memorandumų projektus Tarybai sprendimui priimti, juos patvirtina Saugumo komitetas.

10. NSI teiks Generaliniam sekretoriui – vyriausiajam įgaliotiniui visą reikalingą pagalbą, kad būtų užtikrinta, jog perduodama informacija bus naudojama ir saugoma laikantis susitarimų dėl saugumo priemonių ar supratimo memorandumų sąlygų.

1 priedėlis

Nacionalinių saugumo institucijų sąrašas

BELGIJA

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
Tel. (32-2) 501 85 14
Faks. (32-2) 501 80 58
Teleksas 21376
Telegrafo adresas: Direction de Sécurité A01 – MINAFET

DANIJA

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
Tel. (45-33) 14 88 88
Faks. (45-38) 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø
Tel. (45-33) 32 55 66
Faks. (45-33) 93 13 20

VOKIETIJA

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
Tel. (49-30) 39 81 15 28
Faks. (49-30) 39 81 16 10

GRAIKIJA

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR./SEC.)
STG 1020 Holargos – Athens
Greece
Tel.: (30-1) 655 22 03 (darbo valandomis)
(30-1) 655 22 05 (visą parą)
Faks. (30-1) 642 69 40

ISPANIJA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8 500
E-28023 Madrid
Tel. (34-91) 372 57 07
Faks. (34-91) 372 58 08
el. paštas: nsa-sp@areatec.com

PRANCŪZIJA

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Tel. (33-0) 144 18 81 80
Faks. (33-0) 144 18 82 00
Teleksas: SEGEDEFNAT 200019
Telegrafo adresas: SEGEDEFNAT PARIS

AIRIJA

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Tel. (353-1) 478 08 22
Faks. (353-1) 478 14 84

ITALIJA

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Tel. (39-06) 627 47 75
Faks. (39-06) 614 33 97
Teleksas: 623876 AQUILA 1
Telegrafo adresas: PCM-ANS-UCSI-ROMA

LIUKSEMBURGAS

Autorité Nationale de Sécurité
Ministère d'État
Boîte Postale 2379
L-1023 Luxembourg
Tel.: (352) 478 22 10 (pagrindinis)
(352) 478 22 35 (tiesioginis)
Faks.: (352) 478 22 43
352–478 22 71
Teleksas: 3481 SERET LU
Telegrafo adresas: MIN D'ETAT – ANS

NYDERLANDAI

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
Tel. (31-70) 320 44 00
Faks. (31-70) 320 07 33
Teleksas: 32166 SYTH NL

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL-2500 ES Den Haag
Tel. (31-70) 318 70 60
Faks. (31-70) 318 79 51

AUSTRIJA

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A-1014 Wien
Tel. (43-1) 531 15 34 64
Faks. (43-1) 53 18 52 19

PORTUGALIJA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449–004 Lisboa
Tel.: (351-21) 301 55 10
(351-21) 301 00 01, papildomas 20 45 37
Faks. (351-21) 302 03 50

SUOMIJA

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

ŠVEDIJA

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Tel. (46-8) 405 54 44
Faks. (46-8) 723 11 76

JUNGTINĖ KARALYSTĖ

The Secretary (for DIR/5)
PO Box 5656
London EC1A 1AH
Tel. (44-20) 72 70 87 51
Faks. (44-20) 76 30 14 28
Telegrafo adresas: UK Delegation to Security Policy Dept FCO, marked (in Box 5656 for DIR/5).

2 priedėlis

Nacionalinių įslaptintos informacijos slaptumo žymų palyginimas

ES kategorija	ES visiškai slaptai	ES slaptai	ES konfidencialiai	ES riboto naudojimo
NATO kategorija (1)				
VES kategorija	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted
Belgija	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Danija	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Vokietija	Streng Geheim	Geheim	VS (2) – Vertraulich	VS – Nur für den Dienstgebrauch
Graikija	Ακρως Απορρητο	Απορρητο	Εηπιστευτικο	Περιορισμενης χρησης
Ispanija	Secreto	Reservado	Confidencial	Difusion Limitada
Prancūzija	Très Secret Défense (3)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Airija	Top Secret	Secret	Confidential	Restricted
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Liuksemburgas	Très Secret	Secret	Confidentiel	Diffusion restreinte
Nyderlandai	STG Zeer Geheim	STG Geheim	STG Confidentieel	
Austrija	Streng Geheim	Geheim	Vertraulich	Eigeschränkt
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado
Suomija	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Švedija	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Jungtinė Karalystė	Top Secret	Secret	Confidential	Restricted

(1) NATO: atitiktis NATO slaptumo žymų laipsniams bus nustatyta derantis dėl Europos Sąjungos ir NATO susitarimo dėl saugumo.

(2) Vokietija: VS = Verschlusssache.

(3) Prancūzija: slaptumo žyma „Très Secret Défense“, apimanti prioritetinius Vyriausybės klausimus, gali būti pakeista tik Ministrui Pirmininkui leidus.

3 priedėlis

Praktinis slaptumo žymų vadovas

Šis vadovas yra informacinis ir negali būti aiškinamas kaip keičiantis esmines II ir III skyrių nuostatas.

Slaptumo žyma	Kada	Kas	Žymos dėjimas	Slaptumo žymos laipsnio sumažinimas/išslaptinimas/sunaikinimas	
				Kas	Kada
ES VISIŠKAI SLAPTAI: Ši žyma taikoma tik tai informacijai ir medžiagai, kurią atskleidus be leidimo galėtų būti padaryta ypač didelė žala svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams (II skyriaus 1 punktas).	Tikėtina, kad atskleidus ES VISIŠKAI SLAPTAI pažymėtą medžiagą: — iškiltų tiesioginė grėsmė ES, vienos iš jos valstybių narių arba draugiškų valstybių vidaus stabilumui; — būtų ypač smarkiai pakenkta santykiams su draugiškomis Vyriausybėmis; — būtų tiesiogiai sukelta masiška žūtis; — būtų ypač pakenkta valstybių narių ar kitų prisidedančių šalių pajėgų operacijų veiksmingumui ar saugumui arba pastoviam ypač svarbių saugumo ar žvalgybos operacijų veiksmingumui; — būtų padaryta didelė ilgalaikė žala ES ar valstybių narių ekonomikai.	Valstybės narės: tinkamai įgalioti asmenys (autoriai) (III skyriaus 4 punktas); TGS: tinkamai įgalioti asmenys (autoriai) (III skyriaus 4 punktas), GS-VĮ ir GSP. Autoriai nurodo datą ir terminą, kada turinio slaptumo žymos laipsnis gali būti sumažintas ar informacija išslaptinta. Kitais atvejais jie peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad užtikrintų, jog pradinis įslaptinimas yra būtinas (III skyriaus 10 punktas).	Slaptumo žyma ES VISIŠKAI SLAPTAI ant ES VISIŠKAI SLAPTAI dokumentų bei, kai reikia, gynybos kvalifikacinė žyma ESDP, dedama mechaninėmis priemonėmis ir ranka (II skyriaus 8 punktas). ES slaptumo žymos dedamos centre kiekvieno puslapio viršuje ir apačioje, puslapiai numeruojami. Ant kiekvieno dokumento yra registracijos numeris ir data, registracijos numeris rašomas kiekviename puslapyje. Jei turi būti išplatintos kelios tokių dokumentų kopijos, ant kiekvienos kopijos pirmajame jos puslapyje užrašomas kopijos numeris kartu su bendru puslapių skaičiumi. Visi priedai ir pridedami dokumentai išvardijami pirmajame puslapyje (VII skyriaus 1 punktas).	Išslaptinimas ar slaptumo žymos laipsnio sumažinimas yra išimtinė autoriaus arba GS-VĮ ar GSP kompetencija. Jie apie pakeitimą informuoja visus kitus adresatus, kuriems dokumentas buvo nusiųstas ar nukopijuotas (III skyriaus 9 punktas). Slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtus dokumentus sunaikina už juos atsakinga centrinė registratūra arba subregistratūra. Kiekvienas sunaikintas dokumentas įrašomas į sunaikinimo aktą, kurį pasirašo dokumentų su slaptumo žyma ES VISIŠKAI SLAPTAI kontrolės pareigūnas ir naikinimą stebėjęs pareigūnas, turintis dirbti su slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtais dokumentais tinkamą asmens patikimumo pažymėjimą. Apie tai padaromas įrašas registre. Sunaikinimo aktai kartu su platinimo žiniaraščiais 10 metų saugomi registratūroje (VII skyriaus 31 punktas).	Perteklinės kopijos ir nebereikalingi dokumentai turi būti sunaikinti (VII skyriaus 31 punktas). Slaptumo žyma ES VISIŠKAI SLAPTAI pažymėti dokumentai, įskaitant visas rengiant slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtus dokumentus susikaupusias atliekas, pvz., sugadintas kopijas, juodraščius, spausdintines pastabas, nuorašams naudotą kalkinį popierių, stebint slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtų dokumentų registro kontrolės pareigūnui sunaikinami sudeginant, paverčiant popieriaus mase, supjaustant ar kitaip susmulkinant, kad taptų neatgaminamais ir neatkuriamos formos (VII skyriaus 31 punktas).

Slaptumo žyma	Kada	Kas	Žymos dėjimas	Slaptumo žymos laipsnio sumažinimas/išslaptinimas/sunaikinimas	
				Kas	Kada
ES SLAPTAI: Ši žyma taikoma tik tai informacijai ir medžiagai, kurią atskleidus be leidimo galėtų būti būti labai pakenkta svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams (II skyriaus 2 punktas).	Tikėtina, kad atskleidus slaptumo žyma ES SLAPTAI pažymėtą medžiagą: — būtų sukelta tarptautinė įtampa; — būtų padaryta didelė žala santykiams su draugiškomis Vyriausybėmis; — būtų sukelta tiesioginė grėsmė gyvybei arba labai pakenkta viešajai tvarkai arba asmens saugumui ar laisvei; — būtų padaryta didelė žala valstybių narių ar kitų prisidedančių šalių pajėgų operacijų veiksmingumui ar saugumui arba pastoviam ypač svarbių saugumo ar žvalgybos operacijų veiksmingumui; — būtų padaryta didelė materialinė žala ES ar vienos iš jos valstybių narių finansiniams, monetariniams, ekonominiams ir prekybiniams interesams.	Valstybės narės: įgalioti asmenys (autoriai) (III skyriaus 2 punktas); TGS ir ES decentralizuotos agentūros: įgalioti asmenys (autoriai) (III skyriaus 2 punktas), generaliniai direktoriai, GS-VĮ ir GSP. Autoriai nurodo datą ir terminą, kada turinio slaptumo žymos laipsnis gali būti sumažintas ar informacija išslaptinta. Kitais atvejas jie peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad užtikrintų, jog pradinis įslaptinimas yra būtinas (VII skyriaus 1 punktas).	Slaptumo žyma ES SLAPTAI ant ES SLAPTAI dokumentų bei, kai reikia, gynybos kvalifikacinė žyma ESDP, dedama mechaninėmis priemonėmis ir ranka (III skyriaus 8 punktas). ES slaptumo žymos dedamos centre kiekvieno puslapio viršuje ir apačioje, puslapiai numeruojami. Ant kiekvieno dokumento yra registracijos numeris ir data, registracijos numeris rašomas kiekviename puslapyje. Jei turi būti išplatintos kelios tokių dokumentų kopijos, ant kiekvienos kopijos pirmajame jos puslapyje užrašomas kopijos numeris kartu su bendru puslapių skaičiumi. Visi priedai ir pridedami dokumentai išvardijami pirmajame puslapyje (VII skyriaus 1 punktas).	Išslaptinimas ar slaptumo žymos laipsnio sumažinimas yra išimtinė autoriaus arba GS-VĮ ar GSP kompetencija. Jie apie pakeitimą informuoja visus kitus adresatus, kuriems dokumentas buvo nusiųstas ar nukopijuotas (VII skyriaus 9 punktas). Slaptumo žyma ES SLAPTAI pažymėtus dokumentus sunaikina už juos atsakinga registratūra, stebint asmens patikimumo pažymėjimą turinčiam asmeniui. Naikinami ES SLAPTAI dokumentai įrašomi į pasirašytus sunaikinimo aktus, kurie kartu su sunaikinimo formomis ne mažiau kaip trejus metus saugomi registratūroje (VII skyriaus 32 punktas).	Perteklinės kopijos ir nebereikalingi dokumentai turi būti sunaikinti (VII skyriaus 31 punktas). Slaptumo žyma ES SLAPTAI pažymėti dokumentai, įskaitant visas juos rengiant susikaupusias atliekas, pvz., sugadintas kopijas, juodraščius, spausdintines pastabas, nuorašams naudotą kalkinį popierių, sunaikinami sudeginant, paverčiant popieriaus mase, supjaustant ar kitaip susmulkinant, kad taptų neatgaminamais ir neatkuriamos formos (VII skyriaus 31, 32 punktai).

Slaptumo žyma	Kada	Kas	Žymos dėjimas	Slaptumo žymos laipsnio sumažinimas/išslaptinimas/sunaikinimas	
				Kas	Kada
ES KONFIDENCIALIAI: Ši žyma taikoma tai informacijai ir medžiagai, kurią atskleidus be leidimo, galėtų būti būti pakenkta Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams (II skyriaus 3 punktas).	Tikėtina, kad atskleidus slaptumo žyma ES KONFIDENCIALIAI pažymėtą medžiagą: — būtų padaryta konkreti žala diplomatiniams santykiams, t. y. būtų sukeltas oficialus protestas ar kitokios sankcijos; — būtų pažeistas asmens saugumas ar laisvė; — būtų padaryta žala valstybių narių ar kitų prisidedančių šalių pajėgų operacijų veiksmingumui ar saugumui arba svarbių saugumo ar žvalgybos operacijų veiksmingumui; — būtų iš esmės pakenkta svarbių organizacijų finansiniam gyvybingumui; — būtų trukdoma tyrimui arba padedama padaryti sunkų nusikaltimą; — būtų iš esmės veikiama prieš ES arba valstybių narių finansinius, monetarinius, ekonominius ir prekybinius interesams; — būtų rimtai trukdoma plėtoti ar vykdyti pagrindines ES politikos kryptis; — būtų sustabdyta ar kitaip realiai sutrikdyta svarbi ES veikla.	Valstybės narės: įgalioti asmenys (autoriai) (III skyriaus 2 punktas); TGS ir ES decentralizuotos agentūros: įgalioti asmenys (autoriai) (III skyriaus 2 punktas), generaliniai direktoriai, GS-VĮ ir GSP. Autoriai nurodo datą ir terminą, kada turinio slaptumo žymos laipsnis gali būti sumažintas ar informacija išslaptinta. Kitais atvejas jie peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad užtikrintų, jog pradinis įslaptinimas yra būtinas (III skyriaus 10 punktas).	Slaptumo žyma ES KONFIDENCIALIAI ant ES KONFIDENCIALIAI dokumentų bei, kai reikia, gynybos kvalifikacinė žyma ESDP, dedama mechaninėmis priemonėmis ir ranka arba spausdinant ant iš anksto antspauduoto ir registruoto popieriaus (II skyriaus 8 punktas). ES slaptumo žymos dedamos centre kiekvieno puslapio viršuje ir apačioje, puslapiai numeruojami. Ant kiekvieno dokumento yra registracijos numeris ir data. Visi priedai ir pridedami dokumentai išvardijami pirmajame puslapyje (VII skyriaus 1 punktas).	Išslaptinimas ar slaptumo žymos laipsnio sumažinimas yra išimtinė autoriaus arba GS-VĮ ar GSP kompetencija. Jie apie pakeitimą informuoja visus kitus adresatus, kuriems dokumentas buvo nusiųstas ar nukopijuotas (VII skyriaus 31 punktas). Slaptumo žyma ES KONFIDENCIALIAI pažymėtus dokumentus sunaikina už juos atsakinga registratūra, stebint asmens patikimumo pažymėjimą turinčiam asmeniui. Jų sunaikinimas užregistruojamas pagal nacionalinius teisės aktus, o TGS ir ES decentralizuotose agentūrose – pagal GS-VĮ arba GSP instrukcijas (VII skyriaus 33 punktas).	Perteklinės kopijos ir nebereikalingi dokumentai turi būti sunaikinti (VII skyriaus 31 punktas). Slaptumo žyma ES KONFIDENCIALIAI pažymėti dokumentai, įskaitant visas juos rengiant susikaupusias atliekas, pvz., sugadintas kopijas, juodraščius, spausdintines pastabas, nuorašams naudotą kalkinį popierių, sunaikinami sudeginant, paverčiant popieriaus mase, supjaustant ar kitaip susmulkinant, kad taptų neatgaminamais ir neatkuriamos formos (VII skyriaus 31, 33 punktai).

Slaptumo žyma	Kada	Kas	Žymos dėjimas	Slaptumo žymos laipsnio sumažinimas/išslaptinimas/sunaikinimas	
				Kas	Kada
ES RIBOTO NAUDOJIMO: Ši žyma taikoma tai informacijai ir medžiagai, kurios atskleidimas be leidimo būtų nenaudingas ES arba vienos ar daugiau jos valstybių narių interesams (II skyriaus 4 punktas).	Tikėtina, kad atskleidus slaptumo žyma ES RIBOTO NAUDOJIMO pažymėtą medžiagą: — būtų neigiamai paveikti diplomatiniai santykiai; — būtų sukelti dideli nemalonumai atskiriems asmenims; — būtų sunkiau palaikyti valstybių narių ar kitų prisidedančių šalių pajėgų operacijų veiksmingumą ar saugumą; — asmenims arba įmonėms būtų padaryta finansinių nuostolių arba padėta neteisėtai pasipelnyti ar gauti naudos; — būtų pažeisti įsipareigojimai išlaikyti trečiųjų šalių suteiktos informacijos konfidencialumą; — būtų pažeisti įstatymu nustatyti informacijos atskleidimo apribojimai; — būtų trukdoma tyrimui arba padedama padaryti nusikaltimą; — būtų susilpnintos ES arba valstybių narių pozicijos komercinėse ar politinėse derybose su kitomis šalimis; — būtų trukdoma plėtoti ar vykdyti ES politikos kryptis; — būtų pakenkta ES ir jos veiklos tinkamam valdymui.	Valstybės narės: įgalioti asmenys (autoriai) (III skyriaus 2 punktas); TGS ir ES decentralizuotos agentūros: įgalioti asmenys (autoriai) (III skyriaus 2 punktas), generaliniai direktoriai, GS-VĮ ir GSP. Autoriai nurodo datą ir terminą, kada turinio slaptumo žymos laipsnis gali būti sumažintas ar informacija išslaptinta. Kitais atvejais jie peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad užtikrintų, jog pradinis įslaptinimas yra būtinas (III skyriaus 10 punktas).	Slaptumo žyma ES RIBOTO NAUDOJIMO ant ES RIBOTO NAUDOJIMO dokumentų bei, kai reikia, gynybos kvalifikacinė žyma ESDP, dedama mechaninėmis ar elektroninėmis priemonėmis (II skyriaus 8 punktas). ES slaptumo žymos dedamos centre kiekvieno puslapio viršuje ir apačioje, puslapiai numeruojami. Ant kiekvieno dokumento yra registracijos numeris ir data (VII skyriaus 1 punktas).	Išslaptinimas ar slaptumo žymos laipsnio sumažinimas yra išimtinė autoriaus arba GS-VĮ ar GSP kompetencija. Jie apie pakeitimą informuoja visus kitus adresatus, kuriems dokumentas buvo nusiųstas ar nukopijuotas (III skyriaus 9 punktas). Slaptumo žyma ES RIBOTO NAUDOJIMO pažymėtus dokumentus sunaikina už juos atsakinga registratūra pagal nacionalinius teisės aktus, o TGS ir ES decentralizuotose agentūrose – pagal GS-VĮ arba GSP instrukcijas (VII skyriaus 34 punktas).	Perteklinės kopijos ir nebereikalingi dokumentai turi būti sunaikinti (VII skyriaus 31 punktas).

4 priedėlis

ES įslaptintos informacijos perdavimo trečiosioms šalims arba tarptautinėms organizacijoms vadovas

1 lygio bendradarbiavimas

TVARKA

1. Teisę teikti įslaptintą ES informaciją valstybėms, kurios nėra pasirašiusios Europos Sąjungos sutarties, arba kitoms tarptautinėms organizacijoms, kurių saugumo politika ir nuostatos panašios į ES politiką ir nuostatas, turi Taryba.

2. Taryba gali deleguoti teisę priimti sprendimą dėl įslaptintos informacijos perdavimo. Tai darydama, Taryba nurodo galimos perduoti informacijos pobūdį ir slaptumo žymos laipsnį, kuris paprastai nėra aukštesnis už ES KONFIDENCIALIAI.

3. Sudarius susitarimą dėl saugumo, prašymus perduoti ES įslaptintą informaciją suinteresuotų valstybių arba tarptautinių organizacijų saugumo įstaigos pateikia Generaliniam sekretoriui – vyriausiajam įgaliotiniui, nurodydamos informacijos perdavimo tikslus ir įslaptintos informacijos, kurią prašoma perduoti, pobūdį.

   Prašymą taip pat gali pateikti valstybė narė arba ES decentralizuota agentūra, mananti, kad ES įslaptintos informacijos perdavimas būtų tikslingas; jos nurodo informacijos perdavimo tikslus bei jo naudą ES, taip pat prašomos perduoti informacijos pobūdį bei slaptumo žymos laipsnį.

4. Prašymą svarsto TGS, kuris:

   — atsiklausia perduotinos informacijos autore esančios valstybės narės arba, atitinkamais atvejais, ES decentralizuotos agentūros nuomonės,

   — užmezga reikalingus ryšius su informaciją gaunančių valstybių arba tarptautinių organizacijų saugumo įstaigomis, kad patikrintų, ar jų saugumo politika ir nuostatos užtikrina, jog perduota įslaptinta informacija būtų saugoma pagal šiuos saugumo nuostatus,

   — paprašo valstybių narių nacionalinių saugumo institucijų techninės nuomonės dėl informaciją gaunančių valstybių arba tarptautinių organizacijų patikimumo.

5. TGS prašymą ir Saugumo biuro rekomendaciją pateikia Tarybai sprendimui priimti.

SAUGUMO NUOSTATOS, KURIAS TURI TAIKYTI GAVĖJAI

6. Apie Tarybos sprendimą leisti perduoti įslaptintą ES informaciją Generalinis sekretorius – vyriausiasis įgaliotinis praneša informaciją gaunančioms valstybėms arba tarptautinėms organizacijoms, kartu nusiųsdamas tiek šių saugumo nuostatų kopijų, kiek, jo manymu, yra reikalinga. Jeigu prašymą yra pateikusi valstybė narė, ji ir praneša gavėjui apie gautą leidimą.

   Sprendimas teikti informaciją įsigalioja tik gavėjams raštu patvirtinus, kad jie:

   — nenaudos informacijos jokiems kitiems tikslams, išskyrus tuos, dėl kurių susitarta,

   — saugos informaciją pagal šiuos saugumo nuostatus, ypač pagal specialias toliau išdėstytas nuostatas.

7. *Personalas*

   a) Galimybė naudotis ES įslaptinta informacija yra griežtai ribojama ir pagal „būtina žinoti“ principą suteikiama tik pareigūnams, kurie turi ja naudotis, kad atliktų tarnybines pareigas;

b) visi pareigūnai arba atitinkamos valstybės piliečiai, kuriems bus leista naudotis ES KONFIDENCIALIAI arba aukštesnio slaptumo žymos laipsnio įslaptinta informacija, turi turėti jų valstybės Vyriausybės išduotą slaptumo žymos laipsnį atitinkantį asmens patikimumo pažymėjimą arba kitą lygiavertį leidimą.

8. *Dokumentų perdavimas*

a) Praktinė dokumentų perdavimo tvarka nustatoma susitarimu, remiantis Tarybos saugumo nuostatų VII skyriaus nuostatomis. Visų pirma nurodomos registratūros, kurioms turi būti siunčiama įslaptinta ES informacija;

b) jeigu tarp įslaptintos informacijos, kurią Taryba leido perduoti, yra slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtos informacijos, ją gaunanti valstybė arba tarptautinė organizacija įsteigia centrinę ES registratūrą, o prireikus – ES subregistratūras. Šios registratūros vadovaujasi šių saugumo nuostatų VIII skyriaus nuostatomis.

9. *Registracija*

Registratūrai gavus ES KONFIDENCIALIAI arba aukštesnio laipsnio slaptumo žyma pažymėtą ES dokumentą, jis įrašomas į specialų šios organizacijos tvarkomą registrą, kuriame yra skiltys gavimo datai, informacijai apie dokumentą (datai, registracijos ir kopijos numeriams), slaptumo žymai, pavadinimui, gavėjo pavardei ar pareigoms, kvito grąžinimo datai ir dokumento grąžinimo ES autoriui arba sunaikinimo datai.

10. *Sunaikinimas*

a) Įslaptinti ES dokumentai sunaikinami pagal šių saugumo nuostatų VI skyriuje išdėstytus nurodymus. Įslaptintų dokumentų, pažymėtų slaptumo žymomis ES SLAPTAI ir ES VISIŠKAI SLAPTAI sunaikinimo aktų kopijos nusiunčiamos tuos dokumentus atsiuntusiai ES registratūrai;

b) įslaptinti ES dokumentai įtraukiami į juos gaunančių įstaigų įslaptintų dokumentų sunaikinimo nenumatytais atvejais planus.

11. *Dokumentų apsauga*

Imamasi visų priemonių, kad leidimo neturintys asmenys negalėtų pasinaudoti įslaptinta ES informacija.

12. *Kopijos, vertimai ir išrašai*

Slaptumo žyma ES KONFIDENCIALIAI arba ES SLAPTAI pažymėto dokumento kopijos, vertimai ar išrašai negali būti daromi be atitinkamos saugumo organizacijos vadovo leidimo; šios organizacijos vadovas kopijas, vertimus ar išrašus patikrina, registruoja ir prireikus antspauduoja.

Leidimą kopijuoti arba versti slaptumo žyma ES VISIŠKAI SLAPTAI pažymėtą dokumentą suteikia tik jį sukūrusi institucija, kuri nurodo, kiek kopijų leidžiama padaryti; jeigu dokumentą sukūrusios institucijos negalima nustatyti, prašymas perduodamas TGS Saugumo biurui.

13. *Saugumo pažeidimai*

Kai yra pažeistas ES įslaptinto dokumento saugumas arba įtariama, kad tai padaryta, su sąlyga, kad yra sudarytas susitarimas dėl saugumo, nedelsiant imamasi šių veiksmų:

a) atliekamas tyrimas, kad būtų nustatytos saugumo pažeidimo aplinkybės;

b) pranešama TGS Saugumo biurui, nacionalinei saugumo institucijai ir dokumentą sukūrusiai institucijai arba, to nepadarius, aiškiai konstatuojama, kad ši institucija nebuvo informuota;

c) imamasi veiksmų, kad būtų kuo labiau sumažinti saugumo pažeidimo padariniai;

d) apsvarstomos ir įgyvendinamos priemonės, kurios užkirstų kelią pakartotiniam pažeidimui;

e) įgyvendinamos TGS Saugumo biuro rekomenduotos priemonės, turinčios užkirsti kelią pakartotiniam pažeidimui.

14. *Tikrinimai*

TGS Saugumo biurui leidžiama, susitarus su suinteresuotomis valstybėmis arba tarptautinėmis organizacijomis, įvertinti perduotos įslaptintos ES informacijos apsaugos priemonių veiksmingumą.

15. *Ataskaitos*

Jei yra sudarytas susitarimas dėl saugumo, valstybė arba tarptautinė organizacija tol, kol laiko įslaptintą ES informaciją, per išduodant leidimą perduoti informaciją nurodytą terminą pateikia metų ataskaitą, patvirtinančią, kad buvo laikomasi šių saugumo nuostatų.

5 priedėlis

Įslaptintos ES informacijos perdavimo trečiosioms šalims arba tarptautinėms organizacijoms vadovas

2 lygio bendradarbiavimas

TVARKA

1. Teisę perduoti įslaptintą ES informaciją trečiosioms šalims arba tarptautinėms organizacijoms, kurių saugumo politika ir nuostatos žymiai skiriasi nuo ES politikos ir nuostatų, turi Taryba. Iš esmės gali būti perduodama ne aukštesnio kaip ES SLAPTAI laipsnio slaptumo žyma pažymėta informacija, neperduodama nacionalinė, specialiai valstybėms narėms rezervuota informacija bei informacijos kategorijos, pažymėtos specialiomis kvalifikacinėmis žymomis.

2. Taryba gali deleguoti teisę priimti sprendimą. Deleguodama ji, laikydamasi 1 punkte nurodytų apribojimų, nurodo galimos perduoti informacijos pobūdį ir slaptumo žymos laipsnį, kuris paprastai nėra aukštesnis už ES RIBOTO NAUDOJIMO.

3. Sudarius susitarimą dėl saugumo, prašymus perduoti ES įslaptintą informaciją suinteresuotų valstybių arba tarptautinių organizacijų saugumo įstaigos pateikia Generaliniam sekretoriui – vyriausiajam įgaliotiniui, nurodydamos informacijos perdavimo tikslus ir įslaptintos informacijos, kurią prašoma perduoti, pobūdį.

   Prašymą taip pat gali pateikti valstybė narė arba ES decentralizuota agentūra, mananti, kad ES įslaptintos informacijos perdavimas būtų tikslingas; jos nurodo informacijos perdavimo tikslus bei jo naudą ES, taip pat prašomos perduoti informacijos pobūdį bei slaptumo žymos laipsnį.

4. Prašymą svarsto TGS, kuris:

   — atsiklausia perduotinos informacijos autore esančios valstybės narės arba, atitinkamais atvejais, ES decentralizuotos agentūros nuomonės,

   — užmezga preliminarius ryšius su informaciją gaunančių valstybių arba tarptautinių organizacijų saugumo įstaigomis, kad gautų informacijos apie jų saugumo politiką ir nuostatas, ir ypač kad sudarytų įslaptintos informacijos slaptumo žymų, taikomų ES ir atitinkamoje valstybėje arba tarptautinėje organizacijoje, palyginamąją lentelę,

   — surengia Tarybos Saugumo komiteto posėdį arba prireikus pasinaudodamas supaprastinta rašytine (nutylėjimo) procedūra, apklausia valstybių narių nacionalines saugumo institucijas, kad gautų Saugumo komiteto techninę nuomonę.

5. Tarybos Saugumo komitetas pareiškia techninę nuomonę dėl:

   — informaciją gaunančių valstybių arba tarptautinių organizacijų patikimumo, įvertinant saugumo riziką ES ar jos valstybėms narėms,

   — informacijos gavėjų gebėjimo apsaugoti ES perduotą įslaptintą informaciją įvertinimo,

   — pasiūlymų dėl praktinių procedūrų tvarkant ES įslaptintą informaciją (pvz., išbraukyto teksto versijų pateikimas) ir perduotus dokumentus (ES įslaptintos informacijos antraščių, specialių kvalifikacinių žymų palikimas ar pašalinimas ir t. t.),

   — informaciją sukūrusios institucijos atliekamo informacijos slaptumo žymos laipsnio sumažinimo arba jos išslaptinimo iki jos perdavimo ją gaunančioms šalims arba tarptautinėms organizacijoms ([1]).

([1]) Tai reiškia, kad, jei visos kopijos platinamos ES, informaciją sukūrusi institucija taikys III skyriaus 9 punkte nustatytą tvarką.

6. Generalinis sekretorius – vyriausiasis įgaliotinis prašymą ir TGS Saugumo biuro gautą Tarybos Saugumo komiteto techninę nuomonę perduoda Tarybai sprendimui priimti.

SAUGUMO NUOSTATOS, KURIAS TURI TAIKYTI GAVĖJAI

7. Apie Tarybos sprendimą leisti perduoti įslaptintą ES informaciją Generalinis sekretorius – vyriausiasis įgaliotinis praneša informaciją gaunančioms valstybėms arba tarptautinėms organizacijoms, kartu pateikdamas ES ir atitinkamų valstybių ar organizacijų naudojamų slaptumo žymų palyginamąją lentelę. Jeigu prašymą yra pateikusi valstybė narė, ji ir praneša gavėjui apie gautą leidimą.

Sprendimas teikti informaciją įsigalioja tik gavėjams raštu patvirtinus, kad jie:

— nenaudos informacijos jokiems kitiems tikslams, išskyrus tuos, dėl kurių susitarta,

— saugos informaciją pagal šiuos saugumo nuostatus, ypač pagal specialias toliau išdėstytas nuostatas.

8. Nustatomos šios apsaugos taisyklės, nebent Taryba, gavusi Tarybos Saugumo komiteto techninę nuomonę, nuspręstų nustatyti specialią įslaptintų ES dokumentų tvarkymo procedūrą (ES slaptumo žymų, kvalifikacinių žymų pašalinimas ir kt.).

Tokiu atveju taisyklės bus atitinkamai pakoreguotos.

9. *Personalas*

a) Galimybė naudotis ES įslaptinta informacija yra griežtai ribojama ir pagal „būtina žinoti“ principą suteikiama tik pareigūnams, kurie turi ja naudotis, kad atliktų tarnybines pareigas;

b) visi pareigūnai arba atitinkamos valstybės piliečiai, kuriems bus leista naudotis ES įslaptinta informacija, turi turėti nacionalinį asmens patikimumo pažymėjimą arba kitą lygiavertį leidimą, atitinkantį pagal palyginamosios lentelės apibrėžimus ES slaptumo žymai lygiavertį nacionalinės slaptumo žymos laipsnį;

c) šie nacionaliniai asmens patikimumo pažymėjimai ar leidimai nusiunčiami Generaliniam sekretoriui – vyriausiajam įgaliotiniui susipažinti.

10. *Dokumentų perdavimas*

a) Praktinė dokumentų perdavimo tvarka nustatoma TGS Saugumo biuro ir gaunančiųjų valstybių arba tarptautinių organizacijų saugumo įstaigų susitarimu, remiantis Tarybos saugumo nuostatų VII skyriaus nuostatomis. Visų pirma nurodomi tikslūs adresai, kuriais dokumentai turi būti nusiųsti, taip pat ES įslaptintai informacijai perduoti naudojamos kurjerių ir pašto tarnybos;

b) ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma pažymėti dokumentai siunčiami dvigubame voke. Vidinis vokas pažymimas raidėmis „ES“ ir slaptumo žyma. Kiekvienam įslaptintam dokumentui įdedamas gavimo kvitas. Kvite, kuris neįslaptinamas, įrašomi tik dokumento rekvizitai (registracijos ir kopijos numeriai, data) ir jo kalba, bet ne pavadinimas;

c) vidinis vokas įdedamas į išorinį voką, ant kurio užrašomas pakvitavimui reikalingas paketo numeris. Ant išorinio voko slaptumo žyma nededama;

d) kvitas su paketo numeriu visada įteikiamas kurjeriams.

11. *Gautų dokumentų registravimas gavimo vietoje*

Adresato valstybės NSI arba ją atitinkanti institucija, savo Vyriausybės vardu priimanti ES persiunčiamą įslaptintą informaciją, arba informaciją gaunančios tarptautinės organizacijos saugumo biuras užveda specialų registrą įslaptintai ES informacijai registruoti. Registre yra skiltys gavimo datai, dokumento rekvizitams (datai, registracijos ir kopijos numeriams), slaptumo žymai, pavadinimui, gavėjo pavardei ar pareigoms, kvito grąžinimo datai ir dokumento grąžinimo ES arba jo sunaikinimo datai įrašyti.

12. *Dokumentų grąžinimas*

Grąžindamas įslaptintą dokumentą Tarybai arba jį perdavusiai valstybei narei, gavėjas laikosi 10 punkte nustatytos tvarkos.

13. *Apsauga*

a) Nenaudojami dokumentai yra saugomi nacionalinei įslaptintai medžiagai su tokia pat slaptumo žyma saugoti aprobuotame apsaugos konteineryje. Ant konteinerio neturi būti nuorodų apie jo turinį, su kuriuo gali susipažinti tik leidimą tvarkyti ES įslaptintą informaciją turintys asmenys. Kai naudojami kodiniai užraktai, kodus žino tik tie valstybės arba tarptautinės organizacijos pareigūnai, kurie turi leidimus naudotis konteineryje saugoma ES įslaptinta informacija, o kodai keičiami kas šešis mėnesius arba dažniau, jei keičiamas pareigūnas, panaikinamas nors vieno kodą žinančio pareigūno asmens patikimumo pažymėjimas arba gresia neteisėtas atskleidimas;

b) ES įslaptintus dokumentus iš apsaugos konteinerių išima tik leidžiantį naudotis ES įslaptinta informacija patikimumo pažymėjimą turintys ir „būtina žinoti“ principą atitinkantys pareigūnai. Kol dokumentai yra jų žinioje, jie atsako už saugią tų dokumentų priežiūrą, o ypač už tai, kad dokumentais nepasinaudotų joks leidimo neturintis asmuo. Jie taip pat užtikrina, kad dokumentai baigus jais naudotis bei po darbo valandų būtų saugomi apsaugos konteineriuose;

c) draudžiama be TGS Saugumo biuro leidimo daryti dokumentų su ES KONFIDENCIALIAI arba aukštesnio laipsnio slaptumo žyma fotokopijas ar išrašus;

d) nustatoma ir su TGS Saugumo biuru suderinama skubaus ir visiško dokumentų sunaikinimo nenumatytais atvejais tvarka.

14. *Fizinis saugumas*

a) Nenaudojami apsaugos konteineriai, skirti ES įslaptintiems dokumentams saugoti, visą laiką laikomi užrakinti;

b) kai techninės priežiūros darbuotojams ar valytojams reikia patekti į patalpą, kurioje laikomi tokie apsaugos konteineriai, arba joje dirbti, juos visada lydi valstybės arba organizacijos saugumo tarnybos narys arba už patalpos saugumo priežiūrą tiesiogiai atsakingas pareigūnas;

c) po įprastinių darbo valandų (naktimis, savaitgaliais ir švenčių dienomis) apsaugos konteinerius, kuriuose laikomi ES įslaptinti dokumentai, saugo arba apsauga, arba automatinė signalizacijos sistema.

15. *Saugumo pažeidimai*

Kai yra pažeistas ES įslaptinto dokumento saugumas arba įtariama, kad tai padaryta, nedelsiant yra imamasi šių veiksmų:

a) nedelsiant nusiunčiamas pranešimas TGS Saugumo biurui arba valstybės narės, kuri ėmėsi iniciatyvos persiųsti dokumentus, NSI (su kopija TGS Saugumo biurui);

b) atliekamas tyrimas, kurį baigus saugumo įstaigai (žr. a papunktį) nusiunčiama išsami ataskaita. Tuomet imamasi reikalingų priemonių padėčiai ištaisyti.

16. *Tikrinimai*

TGS Saugumo biurui leidžiama, susitarus su suinteresuotomis valstybėmis ar tarptautinėmis organizacijomis, įvertinti perduotos įslaptintos ES informacijos apsaugos priemonių veiksmingumą.

17. *Ataskaitos*

Tol, kol laiko įslaptintą ES informaciją, valstybė arba tarptautinė organizacija per išduodant leidimą perduoti informaciją nurodytą terminą pateikia metų ataskaitą, patvirtinančią, kad buvo laikomasi šių saugumo nuostatų.

6 priedėlis

Įslaptintos ES informacijos teikimo trečiosioms šalims arba tarptautinėms organizacijoms vadovas

3 lygio bendradarbiavimas

TVARKA

1. Retkarčiais Taryba tam tikromis ypatingomis aplinkybėmis gali pageidauti bendradarbiauti su valstybėmis arba organizacijomis, kurios negali suteikti pagal šiuos saugumo nuostatus reikalaujamų garantijų, nors taip bendradarbiaujant gali prireikti perduoti ES įslaptintą informaciją. Neperduodama nacionalinė, specialiai valstybėms narėms rezervuota informacija.

2. Tokiomis ypatingomis aplinkybėmis prašymus bendradarbiauti su ES, gautus iš trečiųjų valstybių arba tarptautinių organizacijų, taip pat ir tais atvejais, kai taip bendradarbiauti siūlo valstybės narės arba tam tikrais atvejais – ES decentralizuotos agentūros, pirmiausia iš esmės svarsto Taryba, kuri prireikus paklausia informaciją sukūrusios valstybės narės ar decentralizuotos agentūros nuomonės. Taryba apsvarsto, ar išmintinga perduoti įslaptintą informaciją, įvertina, kiek gavėjams būtina ją žinoti, ir nusprendžia, kokio pobūdžio įslaptinta informacija gali būti perduota.

3. Jei Taryba pritaria, Generalinis sekretorius – vyriausiasis įgaliotinis sušaukia Tarybos Saugumo komiteto posėdį arba, prireikus pasinaudodamas supaprastinta rašytine (nutylėjimo) procedūra, apklausia valstybių narių nacionalines saugumo institucijas, kad gautų Saugumo komiteto techninę nuomonę.

4. Tarybos Saugumo komitetas pateikia techninę nuomonę dėl:

   a) ES arba valstybėms narėms egzistuojančios saugumo rizikos įvertinimo;

   b) perduotinos informacijos slaptumo žymos laipsnio, kur reikia, atsižvelgiant į jos pobūdį;

   c) informaciją sukūrusios institucijos atliekamo informacijos slaptumo žymos laipsnio sumažinimo arba jos išslaptinimo iki jos perdavimo ją gaunančioms šalims arba tarptautinėms organizacijoms ([1]);

   d) perduodamų dokumentų tvarkymo procedūrų (žr. 5 punktą);

   e) galimų perdavimo būdų (naudojimosi viešosiomis pašto paslaugomis, viešosiomis ar saugiomis telekomunikacijų sistemomis, diplomatiniu paštu, patikimumo pažymėjimus turinčiais kurjeriais ir kt.).

5. Šiame priedėlyje nurodytoms valstybėms arba organizacijoms perduodami dokumentai iš esmės parengiami be nuorodos į šaltinį ar ES įslaptinimą. Tarybos Saugumo komitetas gali rekomenduoti:

   — naudoti specialias kvalifikacines žymas ar kodinius pavadinimus,

   — naudoti specialią įslaptinimo sistemą, susiejančią informacijos slaptumą su reikalavimais dėl kontrolės priemonių, keliamais gavėjo naudojamiems dokumentų perdavimo būdams (žr. pavyzdžius 14 punkte).

6. TGS Saugumo biuras pateikia Saugumo komiteto techninę nuomonę Tarybai, prireikus pridėdamas pasiūlymus dėl įgaliojimų, kurių reikia vykdant užduotį, delegavimo, ypač kai aplinkybės reikalauja skubiai veikti.

7. Tarybai aprobavus įslaptintos ES informacijos perdavimą ir praktines jo įgyvendinimo procedūras, TGS Saugumo biuras užmezga reikalingus ryšius su atitinkamos valstybės ar organizacijos saugumo įstaiga, kad būtų lengviau taikyti numatytas saugumo priemones.

([1]) Tai reiškia, kad, jei visos kopijos platinamos ES, informaciją sukūrusi institucija taikys III skyriaus 9 punkte apibrėžtą tvarką.

8. Kaip nuorodą, kuria reikėtų remtis, TGS Saugumo biuras visoms valstybėms narėms ir, prireikus, suinteresuotoms ES decentralizuotoms agentūroms išplatina lentelę, kurioje yra apibendrinti informacijos pobūdis bei slaptumo žymos ir išvardytos organizacijos bei šalys, kurioms Tarybos sprendimu ji gali būti perduodama.

9. Informaciją perduodančios valstybės narės NSI arba TGS Saugumo biuras imasi visų reikalingų priemonių, padedančių įvertinti atsiradusią žalą ir iš naujo apsvarstyti procedūras.

10. Pasikeitus bendradarbiavimo sąlygoms, klausimas perduodamas svarstyti Tarybai.

SAUGUMO NUOSTATOS, KURIAS TURI TAIKYTI GAVĖJAI

11. Apie Tarybos sprendimą leisti perduoti įslaptintą ES informaciją Generalinis sekretorius – vyriausiasis įgaliotinis praneša informaciją gaunančioms valstybėms arba tarptautinėms organizacijoms, kartu pateikdamas Tarybos Saugumo komiteto pasiūlytas bei Tarybos patvirtintas išsamias apsaugos taisykles. Jeigu prašymą yra pateikusi valstybė narė, ji ir praneša gavėjui apie gautą leidimą.

Sprendimas teikti informaciją įsigalioja tik gavėjams raštu patvirtinus, kad jie:

— naudos informaciją tik bendradarbiavimo, dėl kurio Taryba yra priėmusi sprendimą, tikslams,

— saugos informaciją pagal Tarybos reikalavimus.

12. *Dokumentų perdavimas*

a) Dėl praktinės dokumentų perdavimo tvarkos susitaria TGS Saugumo biuras ir informaciją gaunančių valstybių arba tarptautinių organizacijų saugumo įstaigos. Jie tiksliai nurodo adresus, kuriais reikia siųsti dokumentus;

b) dokumentai su ES KONFIDENCIALIAI ir aukštesnio laipsnio slaptumo žyma perduodami dvigubame voke. Vidinis vokas pažymimas specialiu spaudu arba patvirtintu kodiniu pavadinimu bei šiam dokumentui patvirtinta specialia slaptumo žyma. Kiekvienam įslaptintam dokumentui pridedamas kvitas. Kvite, kuris nežymimas slaptumo žyma, įrašomi tik dokumento rekvizitai (registracijos ir kopijos numeriai, data) ir kalba, bet ne pavadinimas;

c) vidinis vokas įdedamas į išorinį voką, ant kurio yra užrašytas pakvitavimui reikalingas paketo numeris. Ant išorinio voko slaptumo žyma nededama;

d) kvitas su paketo numeriu visada įteikiamas kurjeriams.

13. *Gautų dokumentų registravimas gavimo vietoje*

Adresato valstybės NSI arba ją atitinkanti institucija, savo Vyriausybės vardu priimanti ES persiunčiamą įslaptintą informaciją, arba informaciją gaunančios tarptautinės organizacijos saugumo biuras užveda specialų registrą įslaptintai ES informacijai registruoti. Registre yra skiltys gavimo datai, dokumento rekvizitams (datai, registracijos ir kopijos numeriams), slaptumo žymai, pavadinimui, gavėjo pavardei ar pareigoms, kvito grąžinimo datai ir dokumento grąžinimo ES arba jo sunaikinimo datai įrašyti.

14. *Įslaptintos informacijos, kuria keičiamasi, naudojimas ir apsauga*

a) Su informacija, pažymėta slaptumo žyma ES SLAPTAI, dirba specialiai paskirti pareigūnai, turintys leidimą naudotis tokio slaptumo žymos laipsnio informacija. Ji saugoma kokybiškose apsaugos spintose, kurias gali atidaryti tik pareigūnai, turintys leidimą naudotis jose laikoma informacija. Zonos, kuriose tokios spintos yra, nuolat saugomos, be to, įrengiama tikrinimo sistema, užtikrinanti, kad į jas patektų tik tinkamus leidimus turintys asmenys. Slaptumo žyma ES SLAPTAI pažymėta informacija siunčiama diplomatiniu paštu, per saugaus pašto tarnybas arba saugiomis telekomunikacijos priemonėmis. Slaptumo žyma ES SLAPTAI pažymėtų dokumentų kopijos daromos tik turint tą dokumentą sukūrusios institucijos raštišką sutikimą. Visos kopijos registruojamos ir kontroliuojamos. Visoms operacijoms, susijusioms su dokumentais, pažymėtais slaptumo žyma ES SLAPTAI, išrašomi kvitai;

b) slaptumo žyma ES KONFIDENCIALIAI pažymėtus dokumentus tvarko tinkamai įgalioti susipažinti su atitinkamu klausimu pareigūnai. Dokumentai saugomi saugomose zonose esančiose užrakinamose apsaugos spintose.

Slaptumo žyma ES KONFIDENCIALIAI pažymėta informacija siunčiama diplomatiniu paštu, per karinio pašto tarnybas ir saugiomis telekomunikacijų priemonėmis. Kopijas daro gaunančioji įstaiga, jų kiekis ir platinimo adresatai registruojami specialiuose registruose.

c) Su slaptumo žyma ES RIBOTO NAUDOJIMO pažymėta informacija dirbama patalpose, į kurias negali patekti leidimų neturintis personalas; ji saugoma užrakintuose konteineriuose. Dokumentai registruotu paštu dvigubuose vokuose gali būti siunčiami pasinaudojant viešojo pašto paslaugomis, o nenumatytais atvejais operacijų metu – neapsaugotomis viešųjų telekomunikacijų sistemomis. Gavėjai gali daryti kopijas;

d) neįslaptintai informacijai specialiosios apsaugos priemonės nereikalingos, ji gali būti siunčiama paštu ir viešųjų telekomunikacijų sistemomis. Adresatai gali ją kopijuoti.

15. *Naikinimas*

Nebereikalingi dokumentai turi būti sunaikinti. Naikinant ES RIBOTO NAUDOJIMO ir ES KONFIDENCIALIAI slaptumo žymomis pažymėtus dokumentus, specialiuose registruose padaromas atitinkamas įrašas. Naikinant ES SLAPTAI slaptumo žyma pažymėtus dokumentus, surašomi sunaikinimo aktai, pasirašomi dviejų naikinimą stebinčių asmenų.

16. *Saugumo pažeidimai*

Jei ES KONFIDENCIALIAI arba ES SLAPTAI slaptumo žymomis pažymėta informacija pasinaudoja leidimo tam neturintys asmenys arba įtariama, kad tai padaryta, valstybės NSI arba organizacijos saugumo vadovas atlieka neteisėto pasinaudojimo informacija aplinkybių tyrimą. Jeigu tyrimo rezultatai teigiami, pranešama informaciją sukūrusiai institucijai. Imamasi priemonių netinkamoms procedūroms arba saugojimo būdams patobulinti, jei dėl jų buvo neteisėtai pasinaudota informacija. Tarybos Generalinis Sekretorius – vyriausiasis įgaliotinis arba be leidimo atskleistą informaciją perdavusios valstybės narės NSI gali paprašyti gavėjo pateikti išsamią informaciją apie tyrimą.