GENEROLO JONO ŽEMAIČIO LIETUVOS KARO AKADEMIJA

VALSTYBĖS IR TARNYBOS PASLAPČIŲ APSAUGA

NORMINIŲ TEISĖS AKTŲ RINKINYS

Mokomoji knyga

II dalis

Vilnius
2014

UDK 351/354(474.5)(094)
Va227

Leidinys „Valstybės ir tarnybos paslapčių apsauga: norminių teisės aktų rinkinys“ skirtas Generolo Jono Žemaičio Lietuvos karo akademijos kariūnams ir klausytojams, studijuojantiems įslaptintos informacijos apsaugos ir informacijos saugumo studijų dalykus. Leidinys taip pat turėtų būti naudingas krašto apsaugos sistemos ir kitų valstybės institucijų darbuotojams, dirbantiems su įslaptinta informacija, organizuojantiems, koordinuojantiems ir kontroliuojantiems jos apsaugą.

Sudarytojas – Generolo Jono Žemaičio Lietuvos karo akademijos dėstytojas *Andrius TEKORIUS*.

Atsakingoji redaktorė – *doc. dr. Audronė PETRAUSKAITĖ*.

Recenzavo: *prof. dr. Alvydas ŠAKOČIUS* (Mykolo Romerio universitetas);
dr. Gintautas SURGAILIS (Generolo Jono Žemaičio Lietuvos karo akademija).

Norminių teisės aktų rinkinys apsvarstytas, patvirtintas ir rekomenduotas spausdinti Generolo Jono Žemaičio Lietuvos karo akademijos Universitetinių studijų instituto Humanitarinių mokslų katedros posėdyje 2013 m. kovo 20 d., protokolo Nr. VL-134.

ISBN 978-609-8074-21-5

TURINYS

4.1. NACIONALINĖS KOMUNIKACIJŲ APSAUGOS TARNYBOS NUOSTATAI

(Žin., 2010, Nr. 87-4631)

PATVIRTINTA
Vyriausybinių ryšių centro prie Lietuvos Respublikos valstybės saugumo departamento direktoriaus 2010 m. birželio 30 d. įsakymu Nr. 1-22

I. BENDROSIOS NUOSTATOS

1. Nacionalinės komunikacijų apsaugos tarnybos (toliau vadinama – NKAT) nuostatai (toliau vadinama – Nuostatai) nustato NKAT tikslus, uždavinius, funkcijas, teises, darbo organizavimo tvarką ir veiklos kontrolės tvarką.

2. NKAT pagal kompetenciją užtikrina Lietuvos Respublikos, užsienio valstybių, Europos Sąjungos (toliau vadinama – ES) ir tarptautinių organizacijų Lietuvos Respublikai perduotos įslaptintos informacijos, saugomos, apdorojamos ar perduodamos automatizuoto duomenų apdorojimo (toliau vadinama – ADA) sistemose ar tinkluose, apsaugą.

3. NKAT savo veikloje vadovaujasi Lietuvos Respublikos Konstitucija, Lietuvos Respublikos tarptautinėmis sutartimis, Lietuvos Respublikos įstatymais, įstatymus įgyvendinančiais teisės aktais, kitais teisės aktais bei šiais Nuostatais.

4. NKAT funkcijas atlieka Lietuvos Respublikos Vyriausybės 2009 m. lapkričio 18 d. nutarimu Nr. 1545 „Dėl Nacionalinės komunikacijų apsaugos, Saugumo priežiūros, Nacionalinės šifrų paskirstymo tarnybų ir institucijų, užtikrinančių apsaugą nuo informatyviojo elektromagnetinio spinduliavimo, funkcijų atlikimo“ (Žin., 2009, Nr. 144-6363) įgaliota valstybės įstaiga – Vyriausybinių ryšių centras prie Lietuvos Respublikos valstybės saugumo departamento* (toliau vadinama – VRC).

5. VRC vadovo sprendimu NKAT funkcijas vykdo Nacionalinis komunikacijų apsaugos skyrius (toliau vadinama – padalinys, vykdantis NKAT funkcijas), kuris yra tiesiogiai pavaldus VRC direktoriaus pavaduotojui pagal kompetenciją.

6. Padalinio, vykdančio NKAT funkcijas, nuostatai privalo būti parengti vadovaujantis šiais nuostatais, VRC nuostatais bei kitais Lietuvos Respublikos teisės aktais.

---

* **Pastaba:** Nuo 2014 m. sausio 1 d. Vyriausybinių ryšių centras prie Krašto apsaugos ministerijos.

II. NKAT UŽDAVINIAI IR FUNKCIJOS

7. NKAT uždaviniai:

7.1. pagal kompetenciją nustatyti įslaptintos informacijos, tvarkomos ADA sistemose ir tinkluose, apsaugos reikalavimus;

7.2. pagal kompetenciją įgyvendinti Lietuvos Respublikos teisės aktų reikalavimus bei ES, NATO įslaptintos informacijos, tvarkomos ADA sistemose ar tinkluose, apsaugos politikos nuostatas;

7.3. pagal kompetenciją kontroliuoti reikalavimų, nustatytų įslaptintos informacijos, tvarkomos ADA sistemose ar tinkluose, apsaugos srityje laikymąsi paslapčių subjektuose, rangovuose ir/ar subrangovuose.

8. Įgyvendindama nustatytus uždavinius, NKAT atlieka šias funkcijas:

8.1. pagal kompetenciją vertina ADA sistemų ir tinklų atitiktį Lietuvos Respublikos, ES ir kitų tarptautinių organizacijų įslaptintos informacijos apsaugos reikalavimams;

8.2. pagal kompetenciją bendradarbiauja su Lietuvos Respublikos, NATO, ES bei šių organizacijų šalių narių, kitų tarptautinių organizacijų analogiškomis tarnybomis, komercinėmis organizacijomis;

8.3. pagal kompetenciją atstovauja Lietuvos Respublikai įslaptintos informacijos, tvarkomos ADA sistemose ar tinkluose, apsaugos klausimais užsienio valstybėse, NATO, ES bei kitose tarptautinėse organizacijose, dalyvauja renginiuose ir seminaruose;

8.4. rengia, dalyvauja rengiant teisės aktus ir kitus dokumentus, reglamentuojančius Lietuvos Respublikos įslaptintos informacijos ADA sistemose ir tinkluose apsaugą;

8.5. dalyvauja planuojant, organizuojant, diegiant ADA sistemose ir tinkluose įslaptintos informacijos apsaugos priemones, kontroliuoja jų naudojimą;

8.6. pagal kompetenciją konsultuoja apsaugos priemonių taikymo, dokumentacijos parengimo ir kitais, su įslaptintos informacijos apsauga ADA tinkluose ir sistemose susijusiais, klausimais;

8.7. pagal kompetenciją dalyvauja rengiant ir įgyvendinant ADA sistemų ir tinklų projektus;

8.8. teikia siūlymus dėl reikalingų tarptautinių standartų taikymo, formuoja rekomendacijas dėl jų naudojimo Lietuvos Respublikoje;

8.9. rengia, atnaujina ilgalaikes ADA sistemų ir tinklų apsaugos programas;

8.10. formuoja, vysto informacijos saugos įvertinimo, apsaugos techninę bazę;

8.11. organizuoja ir vykdo ar dalyvauja vykdant institucijų, įstaigų ir jų padalinių, kuriuose yra tvarkoma įslaptinta informacija, ADA sistemų ir tinklų apsaugos reikalavimų laikymosi patikrinimus;

8.12. dalyvauja tiriant įslaptintos informacijos atskleidimo ADA sistemose ir tinkluose incidentus, vykdo prevencines priemones;

8.13. analizuoja esamas ir naujai atsirandančias grėsmes ADA sistemų ir tinklų saugumui, vertina jų keliamą riziką, priima sprendimus dėl tikslingumo naudoti specialias priemones siekiant sumažinti riziką;

8.14. vykdo nesankcionuotų pasiklausymo įrenginių paiešką institucijų, įstaigų ir jų padalinių patalpose, kuriose yra įrengtos ADA sistemos ir tinklai bei tvarkoma įslaptinta informacija.

III. NKAT TEISĖS

9. NKAT, įgyvendindama jai pavestus uždavinius, turi teisę:

9.1. teisės aktų nustatyta tvarka neatlygintinai gauti visą reikalingą informaciją iš valstybės, savivaldybės institucijų, paslapčių subjektų, kitų asmenų, būtiną NKAT uždaviniams įgyvendinti ir funkcijoms vykdyti;

9.2. pagal kompetenciją dalyvauti rengiant teisės aktus su įslaptintos informacijos, saugomos, apdorojamos ar perduodamos ADA sistemose ar tinkluose, apsauga susijusiais klausimais;

9.3. kviesti ekspertus (konsultantus) ekspertizės ar konsultacinių darbų įslaptintos informacijos apsaugos klausimais;

9.4. pagal kompetenciją teikti paslapčių subjektams ir/ar jų rangovams (subrangovams) rekomendacijas bei privalomus vykdyti nurodymus dėl ADA sistemų ir tinklų apsaugą reglamentuojančių teisės aktų laikymosi ir taikymo, kontroliuoti minėtų teises aktų vykdymą;

9.5. naudotis kitomis Lietuvos Respublikos įstatymų ir kitų teisės aktų suteiktomis teisėmis.

10. Tarnybos darbuotojų atsakomybę ir teises reglamentuoja jų pareigybių aprašymai.

IV. VEIKLOS ORGANIZAVIMAS IR KONTROLĖ

11. Padaliniui, vykdančiam NKAT funkcijas, vadovauja asmuo, skiriamas į pareigas teisės aktų nustatyta tvarka.

12. Padalinio, vykdančio NKAT funkcijas, veikla planuojama, organizuojama ir vykdoma teisės aktų nustatyta tvarka pagal VRC strateginį veiklos planą.

13. Padalinio, vykdančio NKAT funkcijas, vadovaujančiam asmeniui jo teisės, pareigos, funkcijos, atsakomybė, atskaitomybė nustatoma vadovaujantis šiais Nuostatais, pareigybės aprašymu bei kitais teisės aktais.

14. Padalinio, vykdančio NKAT funkcijas, struktūra, personalo statusas ir sudėtis nustatoma vadovaujantis VRC nuostatais bei VRC vadovo (ar jo įgaliotų asmenų) priimtais teisės aktais.

15. Padalinio, vykdančio NKAT funkcijas, veiklą kontroliuoja teisės aktų nustatyta tvarka įgalioti asmenys.

V. BAIGIAMOSIOS NUOSTATOS

16. Šiuos Nuostatus gali keisti VRC, suderinęs su Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija.

SUDERINTA
Lietuvos Respublikos paslapčių apsaugos
koordinavimo komisijos
2010 m. birželio 28 d. sprendimu Nr. 56-3

4.2. INFORMATIKOS IR RYŠIŲ DEPARTAMENTO PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS DIREKTORIAUS 2010 M. LAPKRIČIO 29 D. ĮSAKYMAS NR. 5V-138 DĖL BENDRŲJŲ (VISIEMS VIENODŲ) ŽINYBINIŲ SAUGUMO PRIEŽIŪROS TARNYBŲ STEIGIMO IR VEIKLOS TAISYKLIŲ, DOKUMENTŲ, REIKALINGŲ LEIDIMUI AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ IŠDUOTI, RENGIMO IR LEIDIMŲ AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ IŠDAVIMO TAISYKLIŲ IR AUTOMATIZUOTO DUOMENŲ APDOROJIMO SISTEMŲ IR TINKLŲ, KURIUOSE BUS SAUGOMA, APDOROJAMA AR KURIAIS BUS PERDUODAMA ĮSLAPTINTA INFORMACIJA, SAUGUMO REIKALAVIMŲ APRAŠO PATVIRTINIMO

(Žin., 2010, Nr. 142-7328; 2013, Nr. 4-158)

Vadovaudamasis Lietuvos Respublikos Vyriausybės 2009 m. lapkričio 18 d. nutarimo Nr. 1545 „Dėl Nacionalinės komunikacijų apsaugos, Saugumo priežiūros, Nacionalinės šifrų paskirstymo tarnybų ir institucijų, užtikrinančių apsaugą nuo informatyviojo elektromagnetinio spinduliavimo, funkcijų atlikimo“ (Žin., 2009, Nr. 144-6363; 2010, Nr. 125-6409) 3.3 punktu,

t v i r t i n u pridedamus:

1. Bendrąsias (visiems vienodas) žinybinių saugumo priežiūros tarnybų steigimo ir veiklos taisykles;

2. Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisykles;

3. Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašą.

PATVIRTINTA
Informatikos ir ryšių departamento
prie Lietuvos Respublikos vidaus reikalų
ministerijos direktoriaus 2010 m. lapkričio
29 d. įsakymu Nr. 5V-138

BENDROSIOS (VISIEMS VIENODOS) ŽINYBINIŲ SAUGUMO PRIEŽIŪROS TARNYBŲ STEIGIMO IR VEIKLOS TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Bendrosios (visiems vienodos) žinybinių saugumo priežiūros tarnybų steigimo ir veiklos taisyklės (toliau – Taisyklės) nustato žinybinių saugumo priežiūros tarnybų (toliau – žinybinė SPT) steigimą, funkcijas, atskaitomybę, veiklos koordinavimą, ir panaikinimą.

2. Taisyklėse vartojamos sąvokos:

Saugumo priežiūros tarnyba (toliau – **SPT**) – Lietuvos Respublikos Vyriausybės įgaliota valstybės institucija, vykdanti leidimų automatizuotai apdoroti ir perduoti įslaptintą informaciją automatizuoto duomenų apdorojimo (toliau vadinama – ADA) sistemomis ir tinklais išdavimo, šių sistemų ir tinklų apsaugos kontrolės paslapčių subjektuose ir kitas teisės aktuose numatytas funkcijas.

Žinybinė SPT – šiose Taisyklėse nustatyta tvarka paslapčių subjekto vadovo ar jo įgalioto asmens sprendimu įsteigtas arba įgaliotas struktūrinis paslapčių subjekto padalinys, institucija ar įstaiga, vykdanti ADA sistemų ir tinklų apsaugos kontrolės ir leidimų automatizuotai apdoroti ir perduoti įslaptintą informaciją paslapčių subjekto ADA sistemomis ir tinklais išdavimo funkcijas.

Kitos taisyklėse vartojamos sąvokos atitinka sąvokas, nustatytas Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) bei kituose teisės aktuose.

3. Žinybinė SPT savo veikloje vadovaujasi Lietuvos Respublikos Konstitucija, Lietuvos Respublikos tarptautinėmis sutartimis, įstatymais, kitais Lietuvos Respublikos teisės aktais, NATO ir Europos Sąjungos (toliau – ES) įslaptintos informacijos apsaugą reglamentuojančiais dokumentais ir šiomis Taisyklėmis.

II. ŽINYBINIŲ SPT FUNKCIJOS

4. Žinybinė SPT atlieka šias funkcijas:

4.1. pagal kompetenciją bendradarbiauja su Lietuvos Respublikos, ES, NATO, kitų šalių bei tarptautinių organizacijų institucijomis, atsakingomis už įslaptintos informacijos apsaugą;

4.2. dalyvauja ir pagal kompetenciją atstovauja Lietuvos Respublikai NATO, ES, tarptautinių organizacijų ir užsienio valstybių organizuojamuose renginiuose, susijusiuose su įslaptintos informacijos apsauga;

4.3. pagal kompetenciją vykdo ADA sistemų ir tinklų atitikties nustatytiems apsaugos reikalavimams vertinimą;

4.4. pagal kompetenciją vykdo ADA sistemos ir tinklų veikimo patikrinimą;

4.5. išduoda leidimus, laikinus leidimus ir ribotus leidimus jos kompetencijai priklausančiam paslapčių subjektui, valdančiam ADA sistemas ir tinklus, automatizuotai apdoroti įslaptintą informaciją (toliau – leidimas);

4.6. atlieka jos kompetencijai priklausančio paslapčių subjekto ADA sistemų ir tinklų ADA sistemų ir tinklų, kuriems buvo išduoti leidimai, saugumo kontrolę;

4.7. teikia privalomus nurodymus ADA sistemų ir tinklų valdytojams, ADA sistemų ir tinklų personalui dėl saugumo incidentų tyrimo, esamos situacijos gerinimo, nuolatinio rizikos valdymo bei priimtinos rizikos lygio nustatymo;

4.8. pagal kompetenciją dalyvauja sujungtų ADA sistemų ir tinklų vertinimo ir patikrinimo tarybos veikloje;

4.9. pagal kompetenciją konsultuoja asmenis, atsakingus už paslapčių subjektų įslaptintos informacijos apsaugą, teikia jiems metodinę pagalbą;

4.10. atlieka kitas Lietuvos Respublikos teisės aktuose numatytas funkcijas.

III. ŽINYBINIŲ SPT STEIGIMAS

5. Paslapčių subjektas, siekiantis įsteigti žinybinę SPT, Lietuvos Respublikos paslapčių koordinavimo komisijai (toliau – komisija) turi pateikti motyvuotą prašymą dėl žinybinės SPT įsteigimo tikslingumo ir dokumentaciją, pagrindžiančią žinybinės SPT būtinumą, kurioje nurodoma paslapčių subjekto valdomų ADA sistemų ir tinklų skaičius, paskirtis, šių ADA sistemų ir tinklų slaptumo žymos, naudotojų kiekis, ADA sistemos ir tinklo aprėptis geografiniu požiūriu. Komisija turi teisę prašyti pateikti papildomą informaciją.

6. Žinybinė SPT gali būti steigiama tik komisijai priėmus sprendimą dėl jos steigimo tikslingumo.

7. Paslapčių subjektas, siekdamas įregistruoti žinybinę SPT, turi pateikti SPT prašymą dėl žinybinės SPT įregistravimo, komisijos sprendimo dėl žinybinės SPT steigimo tikslingumo kopiją, žinybinės SPT nuostatus ir žinybinės SPT darbuotojų pareigybių aprašymus.

8. Žinybinė SPT savo veiklą gali pradėti tik tada, kai šiose Taisyklėse nustatyta tvarka yra įregistruojama SPT.

9. SPT ne vėliau kaip po 10 (dešimt) darbo dienų nuo dokumentų gavimo ir, prireikus atlikto žinybinės SPT patikrinimo, turi priimti vieną iš šių sprendimų:

9.1. įregistruoti žinybinę SPT ir apie tai informuoti šią žinybinę SPT steigiantį paslapčių subjektą ir komisiją;

9.2. atsisakyti įregistruoti žinybinę SPT, jeigu pateiktuose registravimo dokumentuose ir/ar patikrinimo metu buvo nustatyti trūkumai.

10. Jeigu SPT priima taisyklių 9.2 punkte numatytą sprendimą, sprendimo motyvo kopija turi būti pateikta dėl žinybinės SPT įregistravimo besikreipiančiam paslapčių subjektui ir komisijai.

11. Atsisakius įregistruoti žinybinę SPT pakartotinis prašymas dėl žinybinės SPT įregistravimo SPT gali būti pateiktas tik pašalinus sprendimo motyve nurodytus trūkumus.

12. SPT koordinuoja žinybinių saugumo priežiūros tarnybų veiklą, susijusią su ADA sistemų ir tinklų apsaugos kontrolės ir leidimų automatizuotai apdoroti ir perduoti įslaptintą informaciją paslapčių subjekto ADA sistemomis ir tinklais

išdavimo funkcijų vykdymu.

IV. ŽINYBINIŲ SPT VEIKLOS KOORDINAVIMAS

13. Žinybinė SPT privalo nedelsdama, bet ne vėliau kaip per 2 (dvi) darbo dienas, pranešti SPT apie žinybinės SPT išduotus leidimus automatizuotai apdoroti ir perduoti įslaptintą informaciją paslapčių subjekto ADA sistemomis ir tinklais.

14. Žinybinė SPT privalo nedelsdama pranešti SPT apie žinybinės SPT kompetencijai priskirtose ADA sistemose ir tinkluose įvykusius saugumo incidentus, keliančius grėsmę ADA sistemoms ir tinklams ar juose tvarkomai įslaptintai informacijai, ir imasi priemonių šiems incidentams likviduoti.

15. SPT, įregistravus žinybinę SPT arba jos registravimo metu bei kartą per trejus kalendorinius metus, atlieka žinybinės SPT veiklos, susijusios su ADA sistemų ir tinklų apsaugos kontrolės ir leidimų automatizuotai apdoroti ir perduoti įslaptintą informaciją paslapčių subjekto, ADA sistemomis ir tinklais išdavimo funkcijų vykdymu, patikrinimus.

16. Patikrinimo metu konstatavus, kad žinybinės SPT veikla neatitinka teisės aktuose nustatytų reikalavimų, SPT kreipiasi į paslapčių subjektą, kuriame yra įsteigta minėta žinybinė SPT, su prašymu pašalinti nustatytus trūkumus.

17. Laiku, be pateisinamų priežasčių, nepašalinus nurodytų trūkumų ir / ar apie tai nepranešus SPT, SPT inicijuoja žinybinės SPT išregistravimą. Trūkumų šalinimo metu gali būti sustabdyti ar panaikinti minėtos žinybinės SPT išduoti leidimai automatizuotai apdoroti ir perduoti įslaptintą informaciją paslapčių subjekto ADA sistemomis ir tinklais.

V. ŽINYBINIŲ SPT PANAIKINIMAS

18. Įsteigta žinybinė SPT gali būti panaikinta žinybinę SPT įsteigusio paslapčių subjekto sprendimu. Apie žinybinės SPT panaikinimą informuojama SPT ir komisija.

19. Panaikinus ar išregistravus žinybinę SPT visi jos įgaliojimai, teisės, išduoti ADA sistemoms leidimai ir kiti dokumentai atitenka SPT.

VI. BAIGIAMOSIOS NUOSTATOS

20. SPT sprendimai dėl žinybinės SPT veiklos (neregistravimo, išregistravimo, patikrinimų ir kitais klausimais) gali būti skundžiami komisijai.

SUDERINTA
Lietuvos Respublikos paslapčių
apsaugos koordinavimo komisijos
2010 m. lapkričio 12 d. protokoliniu
sprendimu Nr. 56-5

PATVIRTINTA
Informatikos ir ryšių departamento
prie Lietuvos Respublikos vidaus reikalų
ministerijos direktoriaus 2010 m. lapkričio
29 d. įsakymu Nr. 5V-138

DOKUMENTŲ, REIKALINGŲ LEIDIMUI AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ IŠDUOTI, RENGIMO IR LEIDIMŲ AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ IŠDAVIMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės (toliau – taisyklės) nustato dokumentų, kuriuos privalo pateikti automatizuoto duomenų apdorojimo (toliau – ADA) sistemų ir tinklų, kuriuose saugoma, apdorojama ar perduodama įslaptinta informacija, valdytojai, siekdami gauti leidimą automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais arba siekdami sujungti ADA sistemas ir tinklus, turinį, leidimų rūšis ir jų išdavimo procedūrą.

2. Taisyklėse vartojamos sąvokos:

ADA sistemos ar tinklo valdytojas – ADA sistemos ar tinklo nuostatuose nurodytas paslapčių subjektas arba jo įgaliotas struktūrinis padalinys, arba rangovas (subrangovas), kuris valdo ADA sistemą ar tinklą, juos sukūręs ar užsakęs sukurti arba įsigijęs.

Saugumo aplinka – apibrėžta teritorija, patalpa ar erdvė, kurioje išdėstyta įranga, užtikrinanti įslaptintą informaciją tvarkančios ADA sistemos ir tinklo veikimą, kurioje nustatytos atitinkamos saugumo valdymo procedūros arba kurioje tvarkoma įslaptinta informacija.

Saugumo valdymo procedūros – Saugumo valdymo procedūrų apraše aprašytos įslaptintos informacijos apsaugos reikalavimų įgyvendinimo instrukcijos.

Globali saugumo aplinka – perimetro fizinės apsaugos priemonėmis apsaugota saugumo aplinka, kurioje įdiegti ADA sistema ir tinklai ar jų sudėtinės dalys.

Lokali saugumo aplinka – globalios saugumo aplinkos apsuptos I ir (ar) II klasių saugumo zonos, kuriose įdiegti ir arba eksploatuojami ADA sistemos ir tinklai ar jų sudėtinės dalys.

Elektroninė saugumo aplinka – saugumo aplinka, kurioje elektroniniu būdu tvarkoma įslaptinta informacija, kuri yra saugoma techninėmis ir programinėmis ADA sistemų ir tinklų apsaugos priemonėmis.

Grėsmė – vienos ar daugiau įslaptintos informacijos savybių – konfidencialumo, vientisumo ar prieinamumo – praradimo galimybė.

Rizika – grėsmės pasireiškimo per tam tikrą laiko tarpą tikimybė.

Pažeidžiamumas –ADA sistemos ir tinklo savybė, sudaranti galimybę pasireikšti grėsmei.

Kitos taisyklėse vartojamos sąvokos atitinka sąvokas, nustatytas Lietuvos

Respublikos valstybės ir tarnybos paslapčių įstatyme (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) bei kituose teisės aktuose.

3. Leidimų automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais išdavimo procedūra apima:

3.1. dokumentų, reikalingų leidimams automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais gauti, parengimą ir pateikimą;

3.2. ADA sistemų ir tinklų atitikties šių taisyklių 5 punkte nustatytiems reikalavimams vertinimą (toliau – vertinimas);

3.3. ADA sistemos ir tinklų veikimo patikrinimą (toliau – patikrinimas);

3.4. leidimų automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais išdavimą arba patikrinimo metu nustatytų trūkumų nurodymą.

4. Gali būti išduoti trijų rūšių leidimai automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais:

4.1. leidimas ADA sistemose ir tinkluose atlikti visas numatytas funkcijas (toliau – leidimas) (forma pridedama);

4.2. laikinas leidimas ADA sistemose ir tinkluose atlikti visas nustatytas funkcijas (toliau – laikinas leidimas) (forma pridedama);

4.3 leidimas ADA sistemose ir tinkluose atlikti vienkartinius veiksmus (toliau – ribotas leidimas) (forma pridedama).

5. ADA sistemų ir tinklų apsauga užtikrinama vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29), Lietuvos Respublikos paslapčių apsaugos koordinavimo komisijos nustatytais reikalavimais, Saugumo priežiūros tarnybos patvirtintais Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimais, Nacionalinės šifrų paskirstymo tarnybos bei Nacionalinės komunikacijų apsaugos tarnybos nustatytais reikalavimais ir kitais Lietuvos Respublikos, NATO ir Europos Sąjungos įslaptintos informacijos apsaugą reglamentuojančiais dokumentais.

II. DOKUMENTŲ, REIKALINGŲ LEIDIMAMS GAUTI, TURINIO REIKALAVIMAI IR PATEIKIMAS

6. ADA sistemos ar tinklo valdytojas, siekdamas gauti leidimą automatizuotai apdoroti ir perduoti įslaptintą informaciją, turi pateikti paraišką dėl leidimo automatizuotai apdoroti ir perduoti įslaptintą informaciją išdavimo žinybinei saugumo priežiūros tarnybai (toliau – žinybinė SPT) arba, jeigu žinybinė SPT nėra įsteigta, – Saugumo priežiūros tarnybai (toliau – SPT). Kartu su paraiška dėl leidimo automatizuotai apdoroti ir perduoti įslaptintą informaciją išdavimo turi būti pateikti ADA sistemos ar tinklo valdytojo įsakymu patvirtinti ADA sistemos ar tinklo nuostatai bei šie ADA sistemos ar tinklo valdytojo įsakymu patvirtinti saugos dokumentai:

6.1. specifinių saugumo reikalavimų aprašas;

6.2. saugumo valdymo procedūrų aprašas;

6.3. rizikos analizė;

6.4. saugumo reikalavimų įgyvendinimo patikrinimo ataskaita.

6[1]. Rangovo ADA sistemas ir tinklus, kuriuose numatoma automatizuotai

apdoroti įslaptintą informaciją ar kuriais numatoma tokią informaciją perduoti, vertina ir leidimus automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais išduoda žinybinė SPT arba SPT įslaptintų sandorių saugumą užtikrinančios institucijos rašytiniu prašymu.

7. Specifinių saugumo reikalavimų aprašas (toliau – SSRA) – tai ADA sistemos ir tinklo apsaugos organizavimo principų ir detalių saugumo reikalavimų sąvadas. SSRA tikslas yra apibrėžti saugios ADA sistemos ir tinklo būseną, jos saugumui kylančias grėsmes ir reikalavimus, keliamus ADA sistemos ir tinklo apsaugai. SSRA privalomai turi būti pateikta ši informacija:

7.1. ADA sistemos ir tinklo apibūdinimas:

7.1.1. ADA sistemos ir tinklo paskirtis ir funkcijos;

7.1.2. ADA sistemoje ir tinkle naudojamos techninės ir programinės įrangos aprašas (-ai);

7.1.3. Saugomos, apdorojamos bei perduodamos informacijos slaptumo žyma ir įslaptintos informacijos apimtys;

7.1.4. ADA sistemos ir tinklo naudotojai, jų funkcijos;

7.1.5. informacijos, su kuria gali susipažinti atskiri naudotojai ar jų grupės, slaptumo žymos;

7.1.6. sąsajos tarp atskirų ADA sistemų ir tinklų.

7.2. ADA sistemai ir tinklui keliamų saugumo reikalavimų aprašymas. ADA sistemai ir tinklui keliami saugumo reikalavimai aprašomi atsižvelgiant į:

7.2.1. grėsmes, kylančias ADA sistemai ir tinklui;

7.2.2. gaunamos, saugomos, apdorojamos ir perduodamos įslaptintos informacijos ADA sistemoje ir tinkle svarbą;

7.2.3. ADA sistemos ir tinklo pažeidžiamumus;

7.2.4. šių taisyklių 5 p. nustatytus saugumo reikalavimus, keliamus ADA sistemai ir tinklui ir gaunamos, saugomos, apdorojamos ir jais perduodamos įslaptintos informacijos apsaugai.

7.3. Saugumo aplinkų aprašymas. Aprašomos šios ADA sistemos saugumo aplinkos:

7.3.1. globali saugumo aplinka ir joje nustatytos saugumo valdymo procedūros ir už jų vykdymą ir kontrolę atsakingi asmenys;

7.3.2. lokali saugumo aplinka ir joje nustatytos saugumo valdymo procedūros ir už jų vykdymą ir kontrolę atsakingi asmenys;

7.3.3. elektroninė saugumo aplinka.

7.4. Saugumo priemonių aprašymas. Šiame skyriuje išdėstomos priemonės, kurios užtikrina ADA sistemos ir tinklo saugumą (toliau – priemonės). Turi būti išskirtos skirtingose saugumo aplinkose panaudotos prieigos kontrolės, identifikavimo ir autentifikavimo, apskaitos, fizinės, personalo, procedūrinės, ryšio priemonės, taip pat ADA sistemos ir tinklo vientisumą, prieinamumą ir konfidencialumą užtikrinančios priemonės.

7.5. Saugumo valdymo reikalavimų aprašymas. Šiame skyriuje aprašoma:

7.5.1. ADA sistemos ir tinklo veiklos tęstinumas;

7.5.2. ADA sistemos ir tinklo rizikos valdymas;

7.5.3. ADA sistemos ir tinklo pakeitimų valdymas;

7.5.4. ADA sistemos ir tinklo apsaugos dokumentavimas ir mokymai;

7.5.5. ADA sistemos ir tinklo veiklos nutraukimo sąlygos bei procedūros.

8. Saugumo valdymo procedūrų aprašas (toliau – SVPA) – tai dokumentas, kuriame tiksliai aprašomas SSRA įvardytų reikalavimų įgyvendinimas ir ADA sistemos ir tinklo apsaugos organizavimo užtikrinimo procedūros.

9. SVPA privalomai turi būti nurodyta:

9.1. ADA sistemos ir tinklo saugumo administravimo ir valdymo procedūros:

9.1.1. trumpas ADA sistemos ir tinklo aprašymas, paminint ADA sistemos ir tinklo ryšius su kitomis sistemomis ir tinklais bei ADA sistemos ir tinklo funkcijas;

9.1.2. asmenys, atsakingi už ADA sistemos ir tinklo saugumo užtikrinimą, jų atsakomybės apibrėžimas;

9.1.3. teisių autorizuotiems naudotojams naudotis ADA sistema ir tinklu suteikimo, pakeitimo ar panaikinimo procedūrų apibrėžimas;

9.1.4. pranešimo apie pastebėtus ADA sistemos ar tinklo saugumo pažeidimus ADA sistemos ar tinklo valdytojui bei žinybinei SPT ar SPT procedūrų aprašymas;

9.1.5. procedūrų, užtikrinančių viso personalo, dirbančio su ADA sistema ir tinklu, supažindinimą su saugumą užtikrinančiomis procedūromis, nustatymas;

9.1.6. kita informacija, susijusi su ADA sistemos ir tinklo saugumo administravimo ir valdymo procedūromis.

9.2. ADA sistemos ir tinklo fizinės apsaugos procedūros:

9.2.1. ADA sistemų ir tinklų tarnybinių stočių ir darbo vietų patalpų, elektroninių dokumentų, kriptografinių duomenų saugojimo ir kitų ADA sistemos ir tinklo veikimui būtinų patalpų apibūdinimas;

9.2.2. spynų, kodų ir raktų saugojimo ir išdavimo procedūrų aprašymas, atsakingų asmenų identifikavimas;

9.2.3. procedūrų, užtikrinančių ADA sistemos ir tinklo fizinę apsaugą pasibaigus darbo valandoms, aprašymas;

9.2.4. procedūrų, užtikrinančių patalpų, kur įdiegta ADA sistemos ir tinklo sudėtinės dalys, lankytojų kontrolę, aprašymas;

9.2.5. leidimų lankytojams patekti į ADA sistemos ir tinklo tarnybines patalpas išdavimo procedūrų aprašymas, atsakingų asmenų identifikavimas;

9.2.6. naujos įrangos įdiegimo, saugojimo ir pašalinimo iš ADA sistemos ir tinklo procedūrų aprašymas;

9.2.7. fizinės apsaugos sistemų, signalizacijų testavimo procedūrų bei veiksmų pavojaus atveju aprašymas;

9.2.8. kita informacija, susijusi su ADA sistemos ir tinklo fizinės apsaugos procedūromis.

9.3. ADA sistemos ir tinklo personalo saugumo procedūros:

9.3.1. ADA sistemos ir tinklo personalo pareigos, funkcijos, leidime dirbti ar susipažinti su įslaptinta informacija nurodyta mažiausia slaptumo žyma;

9.3.2. naudotojų paskyrimo, jų grupių sudarymo, teisių ir prieigos prie ADA sistemos ir tinklo paslaugų ir išteklių valdymo principai;

9.3.3. būtiniausio ADA sistemos ir tinklo personalo sąrašas, jų pareigos, funkcijos, prieinamos informacijos apsaugos lygis;

9.3.4. personalo mokymo ir švietimo saugumo klausimais aprašymas;

9.3.5. informacija apie pagalbinio personalo veiklą ADA sistemų ir tinklų tarnybinėse ar pagalbinėse patalpose;

9.3.6. kita informacija, susijusi su ADA sistemos ir tinklo personalo saugumo procedūromis.

9.4. Įslaptintos informacijos (nepriklausomai nuo fiksavimo būdo ir formos) administravimo procedūros. Šiame skyriuje aprašoma:

9.4.1. naudojamos dokumentų saugojimo terpės, taikomos slaptumo žymos;

9.4.2. procedūros, apibrėžiančios įslaptintų dokumentų registravimą, valdymą, saugojimą, šių procesų patikrinimą ir kontrolę ir už jų įgyvendinimą atsakingus asmenis;

9.4.3. procedūros, apibrėžiančios įslaptintų dokumentų gavimą, platinimą, slaptumo žymų panaikinimą, įslaptintų dokumentų sunaikinimą ir už šiuos procesus atsakingus asmenis.

9.5. ADA sistemos ir tinklo informacijos saugumo procedūros:

9.5.1. techninės įrangos saugumą užtikrinančios procedūros. Kompiuterinės įrangos eksploatavimo procedūros ir dokumentacija, specifiniai nustatymai, kompiuterinės įrangos gedimo metu atliekamos procedūros, darbo vietų prijungimo, atjungimo nuo ADA sistemos ir tinklo procedūros ir už šių procedūrų įgyvendinimą atsakingi asmenys;

9.5.2. programinės įrangos saugumą užtikrinančios procedūros. Naujų naudotojų sąskaitų sukūrimo, panaikinimo, slaptažodžių ir kriptografinių raktų valdymo procedūros, atsargumo priemonės, kurių turi būti imtasi atliekant tam tikrus darbus, operacinių sistemų ir kitos programinės įrangos valdymo procedūros ir už šių procedūrų įgyvendinimą atsakingi asmenys;

9.5.3. apsaugos nuo kompiuterinių virusų procedūros. Kompiuterinių virusų paieškos kompiuteriuose ir kitose kompiuterinėse terpėse, rastų kompiuterinių virusų sunaikinimo, kompiuterinių virusų aptikimo įvykių pranešimo procedūros ir už šių procedūrų įgyvendinimą atsakingi asmenys;

9.5.4. automatizuoto saugumo valdymo procedūros. ADA sistemos ir tinklo automatizuoto saugumo valdymo procedūros ir naudojama programinė įranga, gautų ataskaitų (apimant ir veiklos įrašus) saugojimo, peržiūrėjimo, sunaikinimo procedūros, veiksmai atliekami automatizuoto saugumo valdymo programinės įrangos gedimo metu ir už šių procedūrų įgyvendinimą atsakingi asmenys;

9.5.5. šifravimo procedūros ir už šių procedūrų įgyvendinimą atsakingi asmenys;

9.5.6. apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) procedūros. Techninės įrangos pajungimo, išdėstymo patalpose ir periodinių patikrinimų procedūros bei už šių procedūrų įgyvendinimą atsakingi asmenys. Šio punkto nuostatos netaikomos ADA sistemoms ir tinklams, kuriuose saugoma, apdorojama ar perduodama įslaptinta informacija, žymima slaptumo žyma „Riboto naudojimo“;

9.5.7. saugaus duomenų perdavimo procedūros ir už šių procedūrų įgyvendinimą atsakingi asmenys.

9.5.8. įslaptintai informacijai įrašyti skirtų laikmenų administravimo ir naudojimo procedūros bei už šių procedūrų įgyvendinimą atsakingi asmenys.

9.6. ADA sistemos ir tinklo veiklos tęstinumo valdymo planas turi kompleksiškai apimti nenumatytų situacijų, likviduojamų avarijų padarinių valdymo, saugumo incidentų tyrimo, įstaigos veiklos atkūrimo nuostatas. ADA sistemos

ir tinklo veiklos tęstinumo valdymo plane privalomai turi būti nurodyta:

9.6.1. atsarginių ADA sistemos ir tinklo duomenų kopijų darymo dažniu, jų saugojimo, perdavimo, bandomojo atkūrimo ir panaudojimo procedūromis;

9.6.2. veiksmų planu kompiuterinės, programinės įrangos gedimo, ADA sistemos sugadinimo, įsilaužimo, užpuolimo, telekomunikacinių ryšių praradimo, elektros dingimo, stichinių nelaimių atvejais;

9.6.3. ADA sistemos ir tinklo personalo gyvybės ir sveikatos apsauga;

9.6.4. ADA sistemos ir tinklo veiklos atkūrimu;

9.6.5. ADA sistemos ir tinklo naudotojų mokymu ir nenumatytų situacijų metu vykdomų veiksmų lavinimu;

9.6.6. reguliariu šio plano veiksmingumo išbandymu.

9.7. ADA sistemos ir tinklo programinės ir techninės įrangos (toliau – įranga) pakeitimų valdymas. Šiame skyriuje išdėstoma informacija yra susijusi su:

9.7.1. personalu, atsakingu už ADA sistemos ir tinklo įrangos atnaujinimo organizavimą ir valdymą;

9.7.2. dokumentacija, apibrėžiančia ADA sistemos ir tinklo įrangos pakeitimų procesą;

9.7.3. procedūromis, užtikrinančiomis saugų ADA sistemos ir tinklo įrangos pakeitimų įgyvendinimo procesą. Pakeitimai, galintys turėti neigiamos įtakos ADA sistemos ir tinklo ar saugomos, apdorojamos bei šiais tinklais perduodamos įslaptintos informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti išbandyti bandomojoje aplinkoje, kurioje nėra įslaptintų duomenų ir ji atskirta nuo eksploatuojamos ADA sistemos ir tinklo:

9.7.4. kreipimosi procedūromis dėl ADA sistemos ir tinklo įrangos pakeitimų organizavimo;

9.7.5. ADA sistemos sąrankos dokumentacija, atspindinčia esamą ADA sistemos ir tinklo sąrankos būklę.

10. Rizikos analizės tikslas yra išsiaiškinti rizikos valdymo principus, galimas ADA sistemos ir tinklo grėsmes, pažeidžiamumus, įgyvendintas ir galimas įgyvendinti saugos priemones, taip pat priimtiną rizikos lygį ir liekamosios rizikos veiksnius. Rengiant rizikos analizę rekomenduojama vadovautis Vidaus reikalų ministerijos parengtu ir išleistu Rizikos analizės vadovu.

11. Rizikos analizė turi būti atliekama ADA sistemos ar tinklo valdytojo sudarytos ekspertų grupės. Rizikos analizėje turi būti pateikiama ši informacija:

11.1. identifikuojama ADA sistemos ir tinklo galimos rizikos aplinka ir pažeidžiamumai. Tam tikslui pasinaudojama GSA, LSA ir ESA aprašymuose pateikta informacija;

11.2. įvertinamas ADA sistemos ir tinklo fizinis ir informacinis turtas;

11.3. įvairiais įslaptintos informacijos apsaugos aspektais (fizinė apsauga, personalo patikimumas, įslaptintos informacijos administravimas, ADA sistemų ir tinklų apsauga ir kt.) įvertinamos ADA sistemoje ir tinkle įgyvendintos saugumo priemonės;

11.4. identifikuojamos ADA sistemai ir tinklui siūlomos diegti apsaugos priemonės, nustatomi rizikos mažinimo ir valdymo principai;

11.5. įvertinama liekamoji ADA sistemos ar tinklo rizika bei nurodoma, kad ADA sistemos ar tinklo valdytojas suvokia ir prisiima šią riziką.

12. Saugumo reikalavimų įgyvendinimo patikrinimo ataskaitos tikslas – pa-

tikrinti informaciją apie SSRA ir SVPA nurodytų apsaugos priemonių įgyvendinimą ADA sistemoje ar tinkle. Saugumo reikalavimų įgyvendinimo patikrinimo ataskaitoje turi būti pateikiama ši informacija:

12.1. saugumo reikalavimų patikrinimo apimtis (būtini ir pageidautini patikrinti ADA sistemos ar tinklo elementai, ADA sistemos ar tinklo veiklos ir saugumo aspektai ir kt.);“;

12.2. saugumo reikalavimų patikrinimo struktūra (patikrinime dalyvaujantys subjektai, patikrinimo prioritetai, saugumo reikalavimų atitikties ir atskirų saugumo reikalavimų ar jų grupių priimtinumo kriterijai ir kt.);

12.3. saugumo reikalavimų patikrinimo detalus aprašas (saugumo reikalavimų sąrašas, saugumo reikalavimų patikrinimo metodika ir kt.);

12.4. saugumo reikalavimų patikrinimo rezultatai ir saugumo reikalavimų atitikties aktas.

13. Visi taisyklių 6 punkte nurodyti dokumentai gali būti papildyti kita, su ADA sistemos ar tinklo saugumu susijusia informacija. Tuo atveju, jei II skyriuje reikalaujamos nurodyti nuostatos yra išdėstytos kituose teisės aktuose, turi būti pateikti šie teisės aktai, o taisyklių 6 punkte nustatytuose dokumentuose turi būti pateiktos nuorodos į minėtus teisės aktus.

III. ADA SISTEMŲ IR TINKLŲ IR SUJUNGTŲ ADA SISTEMŲ VERTINIMAS IR PATIKRINIMAS, LEIDIMŲ ADA SISTEMOMS IR TINKLAMS IŠDAVIMAS

14. Sprendimą dėl leidimo, laikino leidimo ar riboto leidimo išdavimo, neišdavimo, galiojimo sustabdymo, anuliavimo ar atsisakymo vertinti ADA sistemą ir tinklus priima žinybinė saugumo priežiūros tarnyba (toliau – žinybinė SPT) ar saugumo priežiūros tarnyba (toliau – SPT).

14. ADA sistemos ar tinklo vertinimo ir patikrinimo metu įvertinama, ar parengti ir pateikti visi būtini ADA sistemos ar tinklo saugos dokumentai, ar saugos dokumentų nuostatos atitinka taisyklių 5 punkte nurodytų teisės aktų nuostatas ir reikalavimus, taip pat patikrinama, kaip ADA sistemoje ar tinkle įgyvendinti saugumo reikalavimai, atsižvelgiant į pateiktą ADA sistemos ar tinklo saugumo reikalavimų įgyvendinimo patikrinimo ataskaitą. Žinybinė SPT ar SPT nepriklausomai patikrina ir įvertina ADA sistemos ar tinklo atitiktį minėtiems reikalavimams. Žinybinė SPT ar SPT turi teisę pasitelkti Nacionalinės komunikacijų apsaugos tarnybos, Nacionalinės šifrų paskirstymo tarnybos ar institucijos, užtikrinančios apsaugą nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST), atstovus dėl saugumo reikalavimų, susijusių su šių institucijų kompetencija, patikrinimo.

15. Leidimas gali būti išduodamas tik vertinimo ir patikrinimo metu nustačius ADA sistemų ir tinklų atitiktį taisyklių 5 punkte nustatytiems reikalavimams. Leidimas turi būti išduodamas ne vėliau kaip per 3 mėnesius nuo ADA sistemos ar tinklo valdytojo paraiškos dėl leidimo automatizuotai apdoroti ir perduoti įslaptintą informaciją išdavimo gavimo žinybinėje SPT ar SPT dienos. ADA sistema ar tinklu leidžiamų atlikti funkcijų apimtis, atitiktis nustatytiems reikalavimams nurodoma ADA sistemos ar tinklo vertinimo ir patikrinimo išvadoje.

16. Laikinas leidimas išduodamas per taisyklių 15 punkte nustatytą terminą

vertinimo metu nustačius ADA sistemų ir tinklų atitiktį taisyklių 5 punkte nustatytiems reikalavimams, tačiau dėl objektyvių priežasčių nesant galimybės atlikti patikrinimą, arba vertinimo ir patikrinimo metu nustačius ADA sistemų ir tinklų atitikties nustatytiems reikalavimams trūkumus, kurie nekelia kritinės grėsmės ADA sistemų ir tinklų saugumui, yra žinomi ADA sistemos ar tinklo valdytojui ir yra sudarytas ADA sistemos ar tinklo valdytojo vadovo įsakymu patvirtintas ADA sistemos ar tinklo atitikties nustatytiems reikalavimams trūkumų šalinimo planas. ADA sistema ar tinklu leidžiamų atlikti funkcijų apimtis, atitiktis nustatytiems reikalavimams, nustatyti trūkumai, kurie nekelia kritinės grėsmės ADA sistemos ar tinklo saugumui, bei jų pašalinimo terminai nurodomi ADA sistemos ar tinklo vertinimo ir patikrinimo išvadoje.

17. Ribotas leidimas išduodamas per taisyklių 15 punkte nustatytą terminą vertinimo ir patikrinimo metu nustačius ADA sistemų ir tinklų atitiktį taisyklių 5 punkte nustatytiems reikalavimams, atsižvelgiant į ADA sistemos ar tinklo valdytojo prašomų leisti atlikti vienkartinių veiksmų pobūdį, arba vertinimo ir patikrinimo metu nustačius ADA sistemų ir tinklų atitikties nustatytiems reikalavimams trūkumus, kurie nekelia kritinės grėsmės ADA sistemų ir tinklų saugumui ir yra žinomi ADA sistemos ar tinklo valdytojui. ADA sistema ar tinklu leidžiamų atlikti funkcijų (vienkartinių veiksmų) apimtis nurodoma ADA sistemos ar tinklo vertinimo ir patikrinimo išvadoje.

18. Prireikus vertinti ir patikrinti ADA sistemą ir tinklą, žinybinė SPT ar SPT teisės aktų nustatyta tvarka gali inicijuoti vertinimo ir patikrinimo darbo grupės sudarymą ar inicijuoti kreipimąsi į nepriklausomus ekspertus.

19. Žinybinė SPT ar SPT turi teisę bet kuriuo ADA sistemos ar tinklo vertinimo ar patikrinimo momentu reikalauti iš ADA sistemos ar tinklo valdytojo papildomų dokumentų, o per nustatytą terminą negavusi reikalaujamų dokumentų,– atsisakyti išduoti prašomą leidimą, laikiną leidimą ar ribotą leidimą.

20. Žinybinė SPT ar SPT per taisyklių 15–17 punktuose nustatytą terminą priima sprendimą:

20.1. išduoti leidimą, laikiną leidimą ar ribotą leidimą ir ADA sistemos ar tinklo valdytojui pateikia jį kartu su ADA sistemos ar tinklo vertinimo ir patikrinimo išvados, kurioje nurodomi ir nustatyti trūkumai, nekeliantys kritinės grėsmės ADA sistemos ar tinklo saugumui bei jų pašalinimo terminai, kopija;

20.2. neišduoti leidimo, laikino leidimo ar riboto leidimo ir ADA sistemos ar tinklo valdytojui pateikia ADA sistemos ar tinklo vertinimo ir patikrinimo išvados, kurioje nurodomi nustatyti trūkumai, keliantys kritinę grėsmę ADA sistemos ar tinklo saugumui, kopiją.

21. Leidimų, laikinų leidimų ir ribotų leidimų geografiškai nutolusiomis, priklausančiomis skirtingoms institucijoms ar valstybėms ADA sistemomis ir tinklais automatizuotai apdoroti įslaptintą informaciją, išdavimui turi būti sukurta sujungtų ADA sistemų ir tinklų vertinimo ir patikrinimo taryba (toliau – akreditavimo taryba). Akreditavimo tarybą gali sudaryti žinybinės (-ių) SPT, SPT, institucijų, atliekančių Nacionalinės komunikacijų apsaugos tarnybos, Nacionalinės šifrų paskirstymo tarnybos, apsaugos nuo elektromagnetinio spinduliavimo tarnybų funkcijas, Paslapčių apsaugos koordinavimo komisijos, asmenys, atsakingi už ADA sistemos ir tinklo saugumą (toliau – akreditavimo tarybos nariai). Akreditavimo tarybos veikla remiasi tarp akreditavimo tarybos

narių pasirašytu susitarimu, kuriame nusakoma akreditavimo tarybos narių įgaliojimai, akreditavimo tarybos funkcijos. Akreditavimo taryba ADA sistemos ir tinklo vertinime ir patikrinime turi vadovautis šiomis taisyklėmis ir kitais Lietuvos Respublikos teisės aktais.

22. Akreditavimo taryba turi būti sudaryta prieš pradedant sujungtų ADA sistemų ir tinklų vertinimą ir patikrinimą, o panaikinta panaikinus ADA sistemų ir tinklų sujungimą. Akreditavimo taryba turi būti suburta, kuomet įvykdomi esminiai pakeitimai ADA sistemose ir tinkluose, veikiantys sujungtų ADA sistemų ir tinklų saugumą, arba likus iki leidimo galiojimo pabaigos ne mažiau kaip 4 mėnesiams.

23. ADA sistemų ir tinklų valdytojai, siekiantys gauti leidimą sujungtomis ADA sistemomis ir tinklais apdoroti ir perduoti įslaptintą informaciją, ADA sistemų vertinimo ir patikrinimo tarybai pateikia šių taisyklių 6 punkte nurodytus dokumentus ir papildo juos ADA sistemų ir tinklų ribų apsaugos mechanizmų reikalavimais, numatytais institucijos, atliekančios Nacionalinės komunikacijų apsaugos tarnybos funkcijas, nustatyta tvarka. Leidimo sujungtai ADA sistemai ir tinklui išdavimo procesas gali būti pradėtas tik ADA sistemoms ir tinklams, kurie jau turi leidimus, laikinus leidimus ar ribotus leidimus ir pateikus šių leidimų kopijas akreditavimo tarybai.

24. Sujungtų ADA sistemų vertinimas ir patikrinimas vykdomas šių taisyklių nustatyta bendra ADA sistemų ir tinklų vertinimo ir patikrinimo tvarka.

25. Jei leidimas, laikinas leidimas ar ribotas leidimas yra išduotas žinybinės SPT sprendimu, atitinkamo leidimo kopija per 2 darbo dienas nuo leidimo įregistravimo turi būti nusiųsta SPT.

26. Priėmus sprendimą neišduoti leidimo, laikino leidimo ar riboto leidimo arba anuliavus leidimo, laikino leidimo ar riboto leidimo išdavimą, pakartotinai paraiška gali būti teikiama ne anksčiau kaip po 3 mėnesių nuo šiame punkte nurodyto sprendimo priėmimo ir tik pašalinus motyvuotoje išvadoje ar sprendime dėl leidimo, laikino leidimo ar riboto leidimo anuliavimo nurodytus trūkumus.

27. Leidimas išduodamas ne ilgesniam nei 3 metų terminui. Laikinas leidimas gali būti išduodamas ne ilgesniam kaip 1 metų terminui. Riboto leidimo trukmė nustatoma priklausomai nuo funkcijų svarbos ir apimties, kurias leidžiama atlikti ADA sistema ir tinklu, tačiau negali būti ilgesnė nei 3 mėnesiai.

27. Jeigu rangovas (subrangovas) jau turi išduotą galiojantį įmonės patikimumą patvirtinantį pažymėjimą (juridinio asmens) arba rangovo (subrangovo) leidimą dirbti ar susipažinti su įslaptinta informacija (fizinio asmens), leidimas, laikinas leidimas ar ribotas leidimas įsigalioja nuo jo išdavimo dienos ir galioja terminą, nurodytą taisyklių 27 punkte, bet ne ilgiau nei įmonės patikimumą patvirtinantis pažymėjimas arba rangovo (subrangovo) leidimas dirbti ar susipažinti su įslaptinta informacija ir netenka galios nuo įmonės patikimumą patvirtinančio pažymėjimo arba rangovo (subrangovo) leidimo dirbti ar susipažinti su įslaptinta informacija baigimo galioti arba panaikinimo dienos.

Jeigu rangovas (subrangovas) neturi išduoto galiojančio įmonės patikimumą patvirtinančio pažymėjimo (juridinio asmens) arba rangovo (subrangovo) leidimo dirbti ar susipažinti su įslaptinta informacija (fizinio asmens), leidimas, laikinas leidimas ar ribotas leidimas įsigalioja nuo įmonės patikimumą patvirtinančio pažymėjimo arba rangovo (subrangovo) leidimo dirbti ar susipažinti su

įslaptinta informacija išdavimo dienos ir galioja terminą, nurodytą taisyklių 27 punkte, bet ne ilgiau nei įmonės patikimumą patvirtinantis pažymėjimas arba rangovo (subrangovo) leidimas dirbti ar susipažinti su įslaptinta informacija ir netenka galios nuo įmonės patikimumą patvirtinančio pažymėjimo arba rangovo (subrangovo) leidimo dirbti ar susipažinti su įslaptinta informacija baigimo galioti arba panaikinimo dienos.

IV. PAKARTOTINIS LEIDIMŲ ADA SISTEMOMS IR TINKLAMS IŠDAVIMAS

28. ADA sistemos ir tinklų valdytojas privalo kreiptis pakartotinai dėl leidimo ar laikino leidimo išdavimo:

28.1. jeigu ADA sistemoje ir tinkluose įvykdyti reikšmingi pakeitimai, kurie pagal Saugumo reikalavimų įgyvendinimo patikrinimo ataskaitos ir (arba) ADA sistemos ar tinklo valdytojo atlikto rizikos ir (ar) atitikties vertinimo rezultatus žinybinės SPT ar SPT sprendimu daro įtaką visos ADA sistemos ir tinklų ar sujungtų ADA sistemų ir tinklų saugumui;

28.2. likus iki leidimo ar laikino leidimo galiojimo pabaigos ne mažiau kaip 3 mėnesiams. Ši nuostata nėra taikoma riboto leidimo atveju.

29. Šių taisyklių 28 punkte nurodytais atvejais valdytojas žinybinei SPT (jei tokios nėra įsteigta – SPT) siunčia taisyklių 6 punkte nurodytą paraišką su leidimui ar laikinam leidimui gauti reikalingais dokumentais.

V. BAIGIAMOSIOS NUOSTATOS

30. Leidimų, laikinų leidimų ar ribotų leidimų ADA sistemoms ir tinklams, ir sujungtoms ADA sistemoms ir tinklams dirbti su įslaptinta informacija apskaitą tvarko žinybinė SPT (jei tokios nėra įsteigta – SPT).

31. SPT ir žinybinė SPT pildo išduotų leidimų, laikinų leidimų ar ribotų leidimų žurnalus bei saugo leidimų, laikinų leidimų ar ribotų leidimų kopijas kartu su leidimui, laikinam leidimui ar ribotam leidimui gauti pateiktais dokumentais.

32. SPT saugo žinybinių SPT išduotų leidimų, laikinų leidimų ar ribotų leidimų ADA sistemoms ir tinklams, ir sujungtoms ADA sistemoms ir tinklams kopijas.

33. SPT ar žinybinės SPT sprendimai dėl leidimo, laikino leidimo ar riboto leidimo ADA sistemoms ir tinklams išdavimo, neišdavimo ar panaikinimo gali būti skundžiami Lietuvos Respublikos paslapčių apsaugos koordinavimo komisijai.

SUDERINTA
Lietuvos Respublikos paslapčių
apsaugos koordinavimo komisijos
2010 m. lapkričio 12 d. protokoliniu
sprendimu Nr. 56-5

PATVIRTINTA
Informatikos ir ryšių departamento
prie Lietuvos Respublikos vidaus reikalų
ministerijos direktoriaus 2010 m. lapkričio
29 d. įsakymu Nr. 5V-138

AUTOMATIZUOTO DUOMENŲ APDOROJIMO SISTEMŲ IR TINKLŲ, KURIUOSE BUS SAUGOMA, APDOROJAMA AR KURIAIS BUS PERDUODAMA ĮSLAPTINTA INFORMACIJA, SAUGUMO REIKALAVIMŲ APRAŠAS

I. BENDROSIOS NUOSTATOS

1. Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas (toliau – aprašas) nustato reikalavimus automatizuoto duomenų apdorojimo (toliau – ADA) sistemoms ir tinklams, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, siekiant užtikrinti ADA sistemose saugomos, apdorojamos ir ADA tinklais perduodamos įslaptintos informacijos slaptumą (konfidencialumą), šios informacijos bei ADA sistemų ir tinklų paslaugų ir išteklių vientisumą ir prieinamumą viso ADA sistemų ir tinklų gyvavimo ciklo metu.

2. Apraše vartojamos sąvokos:

ADA sistemos ar tinklo valdytojas – ADA sistemos ar tinklo nuostatuose nurodytas paslapčių subjektas arba jo įgaliotas struktūrinis padalinys, arba rangovas (subrangovas), kuris valdo ADA sistemą ar tinklą, juos sukūręs ar užsakęs sukurti arba įsigijęs.

ADA sistemos ar tinklo tvarkytojas – ADA sistemos ar tinklo nuostatuose nurodytas paslapčių subjektas arba jo įgaliotas struktūrinis padalinys, arba rangovas (subrangovas), kuris pagal ADA sistemos ar tinklo nuostatus įgaliotas tvarkyti ADA sistemą ar tinklą, jų duomenis.

ADA sistemos ar tinklo naudotojas – asmuo, kuriam ADA sistemos ar tinklo valdytojas arba tvarkytojas, pagal ADA sistemos ar tinklo nuostatuose apibrėžtą kompetenciją, suteikė teisę naudotis ADA sistema ar tinklu.

ADA sistemos ar tinklo slaptumo žyma – aukščiausia slaptumo žyma, kuria pažymėta įslaptinta informacija gali būti saugoma, apdorojama ADA sistemoje ar perduodama ADA tinklu.

Įgaliotoji institucija – institucija, kuriai teisės aktais pavesta atlikti Nacionalinės komunikacijų apsaugos tarnybos arba Nacionalinės šifrų paskirstymo tarnybos, arba Saugumo priežiūros tarnybos, arba apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) funkcijas.

RN sistema ar tinklas – ADA sistema, kurioje saugoma, apdorojama įslaptinta informacija, žymima slaptumo žyma „Riboto naudojimo“, ar tinklas, kuriuo tokia informacija yra perduodama.

KF sistema ar tinklas – ADA sistema, kurioje saugoma, apdorojama įslap-

tinta informacija, žymima slaptumo žyma „Konfidencialiai“, ar tinklas, kuriuo tokia informacija yra perduodama.

S sistema ar tinklas – ADA sistema, kurioje saugoma, apdorojama įslaptinta informacija, žymima slaptumo žyma „Slaptai“, ar tinklas, kuriuo tokia informacija yra perduodama.

VS sistema ar tinklas – ADA sistema, kurioje saugoma, apdorojama įslaptinta informacija, žymima slaptumo žyma „Visiškai slaptai“, ar tinklas, kuriuo tokia informacija yra perduodama.

Saugos dokumentai – ADA sistemos ar tinklo valdytojo įsakymu patvirtinti teisės aktai, reglamentuojantys ADA sistemos ar tinklo saugą, nurodyti Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklėse.

Saugumo incidentas – įvykis, veiksmas ar neveikimas, kuris sudaro ar gali sudaryti sąlygas neteisėtai prisijungti prie ADA sistemos ar tinklo, sutrikdyti ar pakeisti (įskaitant valdymo perėmimą) ADA sistemos ar tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti įslaptintą informaciją, elektroninius duomenis, panaikinti ar apriboti galimybę naudotis įslaptinta informacija, elektroniniais duomenimis, taip pat sudaryti sąlygas pasisavinti, paskelbti, platinti ar kitaip neteisėtai naudoti įslaptintą informaciją, elektroniniais duomenimis.

Kitos apraše vartojamos sąvokos atitinka sąvokas, nustatytas Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme ir kituose teisės aktuose.

3. Aprašas skirtas užtikrinti:

3.1. efektyvų ir racionalų ADA sistemų ir tinklų saugos valdymą;

3.2. efektyvų prieigos teisių prie ADA sistemų ir tinklų valdymą ir kontrolę;

3.3. galimybę nustatyti ADA sistemos ar tinklo naudotojų tapatybę ir patikrinti jos autentiškumą;

3.4. galimybę fiksuoti veiksmus ir įvykius ADA sistemoje ar tinkle;

3.5. tyčinių ar atsitiktinių ADA sistemoje tvarkomos ir tinklais perduodamos įslaptintos informacijos, ADA sistemos ar tinklo paslaugų ir išteklių konfidencialumo, vientisumo ir prieinamumo pažeidimų fiksavimą;

3.6. galimybę greitai atkurti ADA sistemos ar tinklo veikimą ir pasiekti svarbius išteklius ar paslaugas sugedus vienam ar keliems ADA sistemos ar tinklo komponentams arba praradus jų kontrolę;

3.7. operatyvią įslaptintos informacijos ir svarbių ADA sistemos ar tinklo komponentų evakuaciją arba naikinimą ekstremalių situacijų metu.

4. Užsienio valstybių, Europos Sąjungos ir tarptautinių organizacijų įslaptintos informacijos, ADA sistemų ir tinklų saugumui šis aprašas taikomas tiek, kiek neprieštarauja Lietuvos Respublikos tarptautinėms sutartims ir šiomis sutartimis grindžiamiems bei jas įgyvendinantiems tarptautinių organizacijų sprendimams ir Europos Sąjungos teisės aktams.

II. REIKALAVIMAI ADA SISTEMŲ IR TINKLŲ SAUGOS VALDYMO ORGANIZAVIMUI

5. Turi būti paskirtas ADA sistemos ar tinklo saugos įgaliotinis (toliau – saugos įgaliotinis), kuris atsako už ADA sistemos ar tinklo saugos reikalavimų įgyvendinimo organizavimą ir kontrolę. Esant poreikiui, gali būti skiriami saugos įgaliotiniai struktūriniuose ADA sistemos ar tinklo tvarkytojo padaliniuose (toliau – tvarkytojo saugos įgaliotinis), kurie atlieka saugos įgaliotinio funkcijas saugos įgaliotinio nustatytos kompetencijos ribose ir yra jam atskaitingi.

6. Turi būti paskirtas ADA sistemos ar tinklo administratorius (toliau – administratorius). Administratoriai yra atskaitingi saugos įgaliotiniui. Saugos įgaliotinį skirti administratoriumi draudžiama. Administratoriaus funkcijas gali būti pavesta vykdyti ADA sistemos ar tinklo valdytojo struktūriniam padaliniui.

7. Jeigu ADA sistemoje ar tinkle naudojamos kriptografinės priemonės, turi būti paskirtas ADA sistemos ar tinklo kriptografinių priemonių administratorius (administratorius) (toliau – kriptografinių priemonių administratorius). Kriptografinių priemonių administratoriai yra atskaitingi saugos įgaliotiniui. Saugos įgaliotinį skirti kriptografinių priemonių administratoriumi draudžiama.

8. Saugos įgaliotinis, administratorius ir kriptografinių priemonių administratorius gali turėti pavaduotojus.

9. Saugos įgaliotinis, administratorius ir kriptografinių priemonių administratorius įgyvendina atsakingo asmens funkcijas organizuojant ADA sistemų ir tinklų apsaugą ADA sistemos ar tinklo valdytojo institucijoje nustatytas Valstybės ir tarnybos paslapčių įstatyme.

10. ADA sistemos ar tinklo valdytojo funkcijos ir atsakomybė:

10.1. skiria saugos įgaliotinį, administratorių ir, esant poreikiui, kriptografinių priemonių administratorių ar jų pavaduotojus;

10.2. skiria ADA sistemos ar tinklo tvarkytoją (tvarkytojus) ir nustato jo (jų) kompetencijos ribas tvarkant ADA sistemą ar tinklą;

10.3. tvirtina saugos dokumentus;

10.4. atsako už ADA sistemos ar tinklo saugos reikalavimų įgyvendinimą;

10.5. atsako už dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, pateikimą laiku;

10.6. atsako už ADA sistemos ar tinklo saugos užtikrinimui reikalingų finansinių ir kitų išteklių skyrimą laiku.

11. ADA sistemos ar tinklo valdytojas turi teisę įgalioti ADA sistemos ar tinklo tvarkytoją atlikti tam tikras savo funkcijas.

12. Saugos įgaliotinio funkcijos ir atsakomybė:

12.1. teikia ADA sistemos ar tinklo valdytojo vadovui arba jo įgaliotiems asmenims siūlymus dėl:

12.1.1. administratoriaus ir (ar) kriptografinių priemonių administratoriaus skyrimo;

12.1.2. ADA sistemos ar tinklo saugos dokumentų priėmimo, keitimo ar panaikinimo;

12.1.3. ADA sistemos ar tinklo rizikos vertinimo ir atitikties įslaptintos informacijos saugumo reikalavimams vertinimo (toliau – atitikties vertinimas) atlikimo;

12.1.4. ADA sistemos ar tinklo saugos tobulinimo, saugumo priemonių diegimo;

12.1.5. ADA sistemos ar tinklo valdytojo ar tvarkytojo personalo kvalifikacijos kėlimo;

12.2. rengia ADA sistemos ar tinklo saugos dokumentus;

12.3. organizuoja ADA sistemos ar tinklo rizikos analizės ir (ar) atitikties vertinimo atlikimą;

12.4. organizuoja ADA sistemos ar tinklo naudotojų pasirašytiną supažindinimą su ADA sistemos ar tinklo saugos dokumentais ir teisės aktais bei su atsakomybe už nustatytų reikalavimų nesilaikymą;

12.5. organizuoja ADA sistemos ar tinklo naudotojų apmokymus, susijusius su ADA sistemos ar tinklo naudojama techninе bei programine įranga;

12.6. atsako už ADA sistemos ar tinklo saugumo reikalavimų įgyvendinimą;

12.7. atsako už tinkamą ADA sistemos ar tinklo saugumą užtikrinančių procedūrų vykdymo kontrolę;

12.8. informuoja ADA sistemos ar tinklo valdytojo vadovą arba jo įgaliotus asmenis apie saugumo incidentus, koordinuoja jų tyrimą ir dalyvauja jame;

12.9. inicijuoja ir koordinuoja reguliarius ADA sistemos ir tinklo veiklos tęstinumo valdymo plano bandymus;

12.10. teikia administratoriams, kriptografinių priemonių administratoriams ir ADA sistemos ar tinklo valdytojo darbuotojams, užtikrinantiems ADA sistemos ar tinklo funkcionavimą, privalomus vykdyti nurodymus ir pavedimus;

12.11. koordinuoja ir kontroliuoja tvarkytojo saugos įgaliotinių veiklą jiems priskirtos kompetencijos ribose;

12.12. atlieka kitas ADA sistemos ar tinklo valdytojo vadovo ar jo įgaliotų asmenų pavestas ir jam priskirtas funkcijas.

13. Administratoriaus atsakomybė ir funkcijos:

13.1. atsako už ADA sistemos ar tinklo funkcionavimą ir užtikrina tinkamą ir saugų jo darbą;

13.2. apmoko ADA sistemos ar tinklo naudotojus naudotis ADA sistema ar tinklu;

13.3. įvertina ADA sistemos ar tinklo naudotojų pasirengimą dirbti su ADA sistemos ar tinklo įranga ir suteikia naudotojams prieigos prie ADA sistemos ar tinklo teisę;

13.4. teikia saugos įgaliotiniui informaciją, reikalingą 12.2, 12.3, 12.6, 12.7, 12.9 ir 12.10 punktuose nurodytoms funkcijoms atlikti;

13.5. teikia siūlymus ADA sistemos ar tinklo funkcionavimo užtikrinimo, plėtimo, priežiūros ir įslaptintos informacijos saugos klausimais;

13.6. administruoja ADA sistemos ar tinklo techninę ir programinę įrangą, juos žymi informacinėmis užklijomis, nurodančiomis aukščiausią leistiną tvarkyti šia įranga įslaptintos informacijos slaptumo žymą;

13.7. registruoja įvykusius saugumo incidentus, informuoja apie juos saugos įgaliotinį, dalyvauja jų tyrime ir šalinime;

13.8. koordinuoja ADA sistemos ar tinklo valdytojo darbuotojų, užtikrinančių ADA sistemos ar tinklo funkcionavimą, veiklą.

14. Reikalavimai kriptografinių priemonių administratoriui, jo funkcijos ir

atsakomybė nustatomi Bendrosiose įslaptintos informacijos kriptografinės apsaugos taisyklėse.

15. ADA sistemos ar tinklo rizikos valdymas turi būti sudėtinė ADA sistemos ar tinklo valdymo proceso dalis viso ADA sistemos ar tinklo gyvavimo ciklo metu.

16. ADA sistemos ar tinklo eksploatavimo metu rizikos vertinimas turi būti atliekamas:

16.1. RN ir KF sistemų ir tinklų – ne rečiau kaip kartą per 2 metus;

16.2. S ir VS sistemų ir tinklų – ne rečiau kaip kartą per 1 metus.

17. ADA sistemos ar tinklo eksploatavimo metu atitikties saugos reikalavimams vertinimas (toliau – atitikties vertinimas) turi būti atliekamas:

17.1. RN ir KF sistemų ir tinklų – ne rečiau kaip kartą per 2 metus;

17.2. S ir VS sistemų ir tinklų – ne rečiau kaip kartą per 1 metus.

18. Neeilinis rizikos ir (ar) atitikties vertinimas turi būti vykdomas:

18.1. po saugumo incidento ADA sistemoje ir tinkle, kuris parodė saugumo užtikrinimo priemonių nustatymo, įgyvendinimo ir eksploatavimo trūkumus;

18.2. atlikus pakeitimus ADA sistemos ar tinklo specifinių saugumo reikalavimų apraše ar saugumo valdymo procedūrų apraše;

18.3. paaiškėjus naujoms grėsmėms, pažeidžiamumams arba nustačius papildomas aplinkybes, į kurias prieš tai nebuvo atsižvelgta arba kurių rizika labai pasikeitė;

18.4. ADA sistemos ir tinklo valdytojo vadovybės pavedimu;

18.5. kitais žinybinės SPT ar SPT nustatytais atvejais.

19. Po rizikos ir (ar) atitikties vertinimo saugos įgaliotinis organizuoja rizikos valdymo ir (ar) neatitikčių šalinimo plano sudarymą, kurį teikia tvirtinti ADA sistemos ar tinklo valdytojui. Planas (planai) ir rizikos ir (ar) atitikties vertinimo dokumentacija pateikiami žinybinei Saugumo priežiūros tarnybai, o jeigu tokia neįsteigta – Saugumo priežiūros tarnybai.

20. ADA sistemose ir tinkluose taikomos techninės apsaugos priemonės ir mechanizmai turi atitikti reikalavimus, keliamus įslaptintos informacijos, žymimos atitinkama slaptumo žyma, apsaugai. Taikomų techninių apsaugos priemonių ir mechanizmų tinkamumas įslaptintos informacijos apsaugai teisės aktų nustatyta tvarka turi būti patvirtintas įgaliotųjų institucijų.

21. ADA sistemų ir tinklų sudėtinės dalys ir tvarkomos įslaptintos informacijos apsaugos mechanizmai turi būti diegiami ir eksploatuojami vadovaujantis įgaliotųjų institucijų reikalavimais.

22. KF, S ir VS sistemų ir tinklų sudėtinės dalys, išskyrus teisės aktų nustatytas išimtis, turi būti įrengiamos ne žemesnėje kaip II klasės saugumo zonoje. Tokių ADA sistemų ir tinklų tarnybinės stotys, kriptografinė ryšio apsaugos įranga ir kiti kritiniai ADA sistemos ir tinklo komponentai turi būti įrengiami I klasės saugumo zonoje. KF ir S sistemų kriptografinę įrangą, kuri naudojama tik darbo valandomis ir aktyvuojama specialiomis lustinėmis kortelėmis arba raktais, leidžiama įrengti II klasės saugumo zonoje. RN sistemų ir tinklų sudėtinės dalys, išskyrus teisės aktų nustatytas išimtis, turi būti įrengiamos ne žemesnėje kaip administracinėje saugumo zonoje, o tokių ADA sistemų ir tinklų tarnybinės stotys ir kiti kritiniai ADA sistemos ir tinklo komponentai turi būti įrengiami ne žemesnėje kaip II klasės saugumo zonoje.

III. REIKALAVIMAI ADA SISTEMŲ IR TINKLŲ PRIEIGOS TEISIŲ VALDYMUI

23. Prieigos prie ADA sistemos ar tinklo teisė suteikiama ADA sistemos ar tinklo valdytojo sprendimu, vadovaujantis principu „būtina žinoti“. ADA sistemos ar tinklo naudotojas privalo turėti galiojantį leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma, atitinkančia ADA sistemos ar tinklo slaptumo žymą arba aukštesne. Kiekvienas ADA sistemos ar tinklo naudotojas privalo turėti unikalų identifikatorių. ADA sistemos ar tinklo saugos įgaliotinis ir administratorius privalo turėti galiojantį leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma, atitinkančia ADA sistemos ar tinklo slaptumo žymą arba aukštesne.

24. ADA sistemos ar tinklo priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus identifikatorių, kuriuo naudojantis nebūtų galima modifikuoti, naikinti ar kitaip keisti ADA sistemos ar tinklo sisteminiuose įvykių žurnaluose saugomos informacijos ir keisti sisteminių įvykių žurnalų pildymo nustatymų. Atlikti ADA sistemos ar tinklo naudotojo funkcijas, naudojantis šiuo identifikatoriumi, draudžiama.

25. ADA sistemos ar tinklo naudotojas privalo užtikrinti „Būtina žinoti“ principo laikymąsi ir neleisti bei nesudaryti sąlygų asmenims susipažinti su jiems neskirta įslaptinta informacija.

26. ADA sistemos ar tinklo naudotojui neatliekant jokių veiksmų (RN ir KF sistemoje ar tinkle – 15 min., S ir VS sistemoje ar tinkle – 10 min.), ADA sistema ar tinklas turi užtikrinti, kad toliau naudotis ADA sistema ar tinklu galima būtų tik pakartojus tapatybės nustatymo ir patvirtinimo veiksmus.

27. ADA sistemos ar tinklo naudotojo prieiga turi būti blokuojama, jei žinoma, kad šis naudotojas nesinaudos (atostogauja, išvykęs į komandiruotę, serga ir pan.) RN ir KF sistema ar tinklu – daugiau kaip 2 mėnesius, S ir VS sistema ar tinklu – daugiau kaip 1 mėnesį.

28. Jeigu ADA sistemos ar tinklo naudotojas nesilaiko įslaptintos informacijos apsaugos reikalavimų, piktnaudžiauja jam suteiktais įgaliojimais, yra nušalintas nuo pareigų, ADA sistemos ar tinklo valdytojo ar tvarkytojo sprendimu ADA sistemos ar tinklo naudotojo prieiga prie ADA sistemos ar tinklo turi būti blokuojama nedelsiant, iki aplinkybių išsiaiškinimo.

29. Asmenų, netekusių 23 p. nurodytų leidimų, arba asmenų, kurie nebeatitinka principo „Būtina žinoti“, prieiga prie atitinkamos įslaptintos informacijos ir (ar) ADA sistemos ar tinklo turi būti nedelsiant panaikinama.

30. Reikalavimus tapatybės patvirtinimo priemonėms nustato Nacionalinė komunikacijų apsaugos tarnyba.

IV. REIKALAVIMAI ADA SISTEMŲ IR TINKLŲ ĮVYKIŲ REGISTRAVIMUI

31. ADA sistemose ir tinkluose turi būti užtikrintas nuolatinis įvykių (ADA sistemos ar tinklo veiklos įrašų) registravimas, nurodant laiką ir susijusį naudotojo identifikatorių. Reikalaujamų registruoti įvykių sąrašą nustato Nacionalinė komunikacijų apsaugos tarnyba. ADA sistemos ar tinklo valdytojas, vadovau-

damasis rizikos analize, gali savo sprendimu papildyti minėtą sąrašą. Įvykiai turi būti registruojami pagrindiniame ir rezerviniame (jei leidžia ADA sistemos ar tinklo funkcionalumas – nutolusiame) įvykių žurnaluose. Laikrodžiai, pagal kuriuos nustatomas įvykių laikas, turi būti sinchronizuoti, išskyrus ADA sistemas, kurias sudaro pavieniai, nesujungti kompiuteriai. Turi būti priemonės, leidžiančios nustatyti su įvykiais susijusius asmenis visą įvykių žurnalų saugojimo laiką.

32. VS sistemose papildomai turi būti užtikrintas registravimas sėkmingų ir nesėkmingų bandymų prieiti prie kiekvienos informacijos rinkmenos, pažymėtos slaptumo žyma „Visiškai slaptai“.

33. ADA sistemos ar tinklo įvykių žurnalų pildymo nustatymų keitimas ir žurnalų kopijų darymas turi būti atliekamas naudojant atskirą tik tam skirtą identifikatorių. Minėti veiksmai turi būti atliekami tik užtikrinus ADA sistemos ar tinklo valdytojo vadovo, saugos įgaliotinio ir administratoriaus dalyvavimą ir kontrolę.

34. ADA sistemos ar tinklo įvykių žurnalų įrašai turi būti saugomi S sistemose ir tinkluose – 5 metus, VS sistemose ir tinkluose – 10 metų, RN ir KF sistemoms ir tinklams reikalavimas netaikomas. Jeigu ADA sistema ar tinklas likviduojami, įvykių žurnalas turi būti saugomas atitinkamai 5 metus arba 10 metų nuo likvidavimo dienos.

V. KITI REIKALAVIMAI

35. Patalpos, kuriose įrengta ADA sistemos ar tinklo įranga, turi atitikti reikalavimus, keliamus patalpoms, kuriose saugoma ar kuriose dirbama su atitinkama žyma pažymėta įslaptinta informacija.

36. ADA sistemos ar tinklo ranga (taip pat ir nešiojamieji kompiuteriai, kiti mobilieji įrenginiai), kurioje saugoma įslaptinta informacija, turi būti gabenama laikantis įslaptintos informacijos, gaminių ir kitų objektų, žymimų slaptumo žyma, atitinkančia ADA sistemos ar tinklo slaptumo žymą, gabenimo reikalavimų.

37. ADA sistemos ar tinklo įrenginiai turi būti pažymėti ADA sistemos ar tinklo slaptumo žymą nurodančia informacine užklija (užklijomis).

38. ADA sistemos ar tinklo įrenginiai turi būti apsaugoti apsauginėmis užklijomis. Apsauginių užklijų turi būti tiek ir jos turi būti tokio dydžio, kad neleistų atidaryti įrenginio korpuso, jų nepažeidžiant. Jeigu leidžia įrenginio konstrukcija ir (ar) funkcinės galimybės, turi būti įjungta įrenginio apsauga nuo korpuso atidarymo. Prieš pradėdamas darbą su ADA sistema ar tinklu, ADA sistemos ar tinklo naudotojas privalo įsitikinti, kad apsauginės užklijos nepažeistos.

39. ADA sistemoje ir tinkle saugomos ir apdorojamos informacijos atsarginės kopijas rekomenduojama užšifruoti. Metodines rekomendacijas atsarginių kopijų šifravimui nustato Nacionalinė komunikacijų apsaugos tarnyba.

40. ADA sistemos ar tinklo valdytojas turi nustatyti atsarginių ADA sistemos ir tinklo duomenų kopijų darymo dažnį, jų saugojimo, perdavimo, bandomojo atkūrimo ir panaudojimo procedūras, o atsarginių kopijų bandomasis atkūrimas turi būti vykdomas:

40.1. RN ir KF sistemų ir tinklų – ne rečiau kaip kartą per 1 metus;

40.2. S ir VS sistemų ir tinklų – ne rečiau kaip kartą per 6 mėnesius.

41. ADA sistemoje saugomos ir apdorojamos informacijos atsarginės kopijos turi būti daromos, administruojamos ir saugomos vadovaujantis kompiuterių laikmenų apsaugos reikalavimais, taikomais laikmenoms su ADA sistemos slaptumo žyma pažymėta įslaptinta informacija.

42. Laikmenos, kurios ADA sistemos ar tinklo naudotojų prijungiamos prie ADA sistemos ar tinklo kompiuterio ar įdedamos į ADA sistemos ar tinklo kompiuteryje esantį nuskaitymo įrenginį, turi būti įregistruotos Lietuvos Respublikos Vyriausybės nustatyta tvarka Įslaptintai informacijai įrašyti skirtų laikmenų registre. ADA sistemos ar tinklo kompiuteriuose turi būti išjungta automatinė laikmenų paleistis (angl. *autorun*). Rekomenduojama naudoti programinę įrangą, skirtą USB laikmenų kontrolei. Prieš prijungiant ar įdedant tokią laikmeną, ji turi būti patikrinta kenkėjiškos programinės įrangos aptikimo priemonėmis atskirame tam skirtame neprijungtame prie ADA sistemos ar tinklo kompiuteryje. Jungti laikmenas prie S ir VS sistemų ar tinklų šių sistemų ar tinklų naudotojams leidžiama tik įslaptintų dokumentų administravimo punktuose įrengtose darbo vietose.

43. Turi būti užtikrinta visų ADA sistemos ar tinklo kompiuterių apsauga nuo kenkėjiškos programinės įrangos. Programinės įrangos, skirtos apsaugai nuo kenkėjiškos programinės įrangos, sąrašą tvirtina Nacionalinė komunikacijų apsaugos tarnyba. ADA sistemos ar tinklo kompiuterių, prijungtų prie vietinio kompiuterių tinklo, apsauga nuo kenkėjiškos programinės įrangos turi būti valdoma ir atnaujinama centralizuotai. Išjungti ar pašalinti šią apsaugą leidžiama tik ADA sistemos administravimo tikslu. Ši apsauga turi būti atnaujinama gamintojo rekomenduojamu periodiškumu. Neprijungtų prie vietinio kompiuterių tinklo kompiuterių apsauga turi būti atnaujinama rankiniu būdu, naudojant tik tam skirtas laikmenas. Jeigu toks kompiuteris naudojamas rečiau, nei apsaugos gamintojo rekomenduojamas atnaujinimo periodas, apsauga turi būti atnaujinama nedelsiant po šio kompiuterio įjungimo ir naudotojo tapatybės nustatymo operacinėje sistemoje.

44. Diegti, atkurti arba atnaujinti ADA sistemos ar tinklo programinę įrangą naudojant laikmenas leidžiama tik iš gamintojo pateiktų arba iš įrašytų vienkartinio įrašymo laikmenų.

45. ADA sistemoje ar tinkle naudojamos techninės ir programinės įrangos sąrašus tvirtina ADA sistemos ar tinklo valdytojas, prieš tai suderinęs juos su žinybine Saugumo priežiūros tarnyba, o jei tokia neįsteigta – Saugumo priežiūros tarnyba.

46. ADA sistemos ar tinklo įranga turi būti prižiūrima laikantis gamintojo rekomendacijų.

47. ADA sistemos ar tinklo įrangos gedimų šalinimas, jeigu to negali atlikti saugos įgaliotinis, administratorius ir (ar) kitas įgaliotas ADA sistemos ar tinklo valdytojo personalas, turi būti atliekamas laikantis įslaptintų sandorių saugumo reikalavimų. Gedimų šalinimą turi atlikti atitinkamą kvalifikaciją turintis specialistas, gedimų šalinimas pagal galimybes turi būti atliekamas vietoje, prižiūrint saugos įgaliotiniui ar administratoriui.

48. ADA sistemos ar tinklo testavimas turi būti atliekamas naudojant atskirą tam skirtą testavimo aplinką, nenaudojant įslaptintos informacijos arba naudo-

jant ją fiktyvią.

49. ADA sistemos ar tinklo naudotojas turi nedelsdamas informuoti saugos įgaliotinį, o jeigu jo nėra – administratorių apie neveikiančią ar netinkamai veikiančią ADA sistemą ar tinklą, pažeistas įrenginių apsaugines užklijas, saugos reikalavimų nesilaikančius ADA sistemos ar tinklo naudotojus, bet kokią veiklą, skirtą įslaptintai informacijai atskleisti ir (ar) ADA sistemos ar tinklo veiklai sutrikdyti. Tuo atveju, kai tokią veiklą vykdo saugos įgaliotinis ir (ar) administratorius, ADA naudotojas privalo informuoti ADA sistemos ar tinklo valdytojo vadovą, Lietuvos Respublikos valstybės saugumo departamentą ir žinybinę Saugumo priežiūros tarnybą, o jei tokia neįsteigta – Saugumo priežiūros tarnybą.

50. Jei dėl ADA sistemos ar tinklo ypatumų nėra galimas ar tikslingas atskirų šiame apraše išdėstytų reikalavimų įgyvendinimas, ADA sistemos ar tinklo valdytojas privalo atskirai įvertinti kiekvieno tokio reikalavimo neįgyvendinimo riziką ir šią informaciją pateikti žinybinei Saugumo priežiūros tarnybai, o jei tokia neįsteigta – Saugumo priežiūros tarnybai, kuri sprendžia dėl atitinkamo reikalavimo netaikymo ir apie priimtą sprendimą informuoja ADA sistemos ar tinklo valdytoją.

SUDERINTA
Lietuvos Respublikos paslapčių
apsaugos koordinavimo komisijos
2010 m. lapkričio 12 d.
protokoliniu sprendimu Nr. 56-5

Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklių
1 priedas

(LEIDIMO AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ FORMA)

20 m. d. Nr.

Vilnius

Šis leidimas išduotas

_____
(paslapčių subjekto pavadinimas arba rangovo (subrangovo) pavadinimas)

ir patvirtina, kad automatizuoto duomenų apdorojimo sistema ar tinklas

_____,
(automatizuoto duomenų apdorojimo sistemos ar tinklo pavadinimas)

valdoma (-as) _____
(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo pavadinimas)

_____,
(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo adresas)

turi teisę atlikti visas teisės aktų nustatytas funkcijas ir automatizuotai apdoroti įslaptintą informaciją, žymimą slaptumo žyma (žymomis)

_____ ir žemesne (žemesnėmis).
(slaptumo žyma ar žymos)

Leidimas išduotas vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) 40 str. 3 d. ir šiais teisės aktais:

1. _____
(SPT ar žinybinės SPT funkcijas atliekančios institucijos, surašiusios išvadą dėl leidimo išdavimo, pavadinimas, išvados data ir numeris)

2. _____
(Specifinių saugumo reikalavimų aprašo pavadinimas, teisės aktą, kuriuo jis patvirtintas, priėmusios institucijos pavadinimas, teisės akto rūšis, numeris, priėmimo data)

3. _____
(Saugumo valdymo procedūrų aprašo pavadinimas, teisės aktą, kuriuo jis patvirtintas, priėmusios institucijos pavadinimas, teisės akto rūšis, numeris, priėmimo data)

4. _____
(Rizikos analizės pavadinimas, teisės aktą, kuriuo jis patvirtintas, priėmusios institucijos pavadinimas, teisės akto rūšis, numeris, priėmimo data)

5. _____
(kiti teisės aktai)

Leidimas galioja: _____
(leidimo galiojimo terminas)

_____ _____ _____
(leidimą išdavusios SPT ar žinybinės SPT vadovo pareigos) (parašas) (vardas, pavardė)

Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklių
2 priedas

(LAIKINO LEIDIMO AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ FORMA)

20 m. d. Nr.

Vilnius

Šis laikinas leidimas išduotas

_____
(paslapčių subjekto pavadinimas arba rangovo (subrangovo) pavadinimas)

ir patvirtina, kad automatizuoto duomenų apdorojimo sistema ar tinklas

_____,
(automatizuoto duomenų apdorojimo sistemos ar tinklo pavadinimas)

valdoma (-as) _____
(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo pavadinimas)

_____,
(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo adresas)

turi teisę atlikti šio leidimo 1 p. nurodytoje išvadoje nustatytas funkcijas nurodyta apimtimi ir sąlygomis ir automatizuotai apdoroti įslaptintą informaciją, žymimą slaptumo žyma (žymomis)

_____ ir žemesne (žemesnėmis).
(slaptumo žyma ar žymos)

Laikinas leidimas išduotas vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) 40 str. 3 d. ir šiais teisės aktais:

1. _____
(ŠPT ar žinybinės ŠPT funkcijas atliekančios institucijos, surašiusios išvadą dėl laikino leidimo išdavimo, pavadinimas, išvados data ir numeris)

2. _____
(Specifinių saugumo reikalavimų aprašo pavadinimas, teisės aktą, kuriuo jis patvirtintas, priėmusios institucijos pavadinimas, teisės akto rūšis, numeris, priėmimo data)

3. _____
(Saugumo valdymo procedūrų aprašo pavadinimas, teisės aktą, kuriuo jis patvirtintas, priėmusios institucijos pavadinimas, teisės akto rūšis, numeris, priėmimo data)

4. _____
(Rizikos analizės pavadinimas, teisės aktą, kuriuo jis patvirtintas, priėmusios institucijos pavadinimas, teisės akto rūšis, numeris, priėmimo data)

5. _____
(kiti teisės aktai)

Laikinas leidimas galioja: _____
(laikino leidimo galiojimo terminas)

_____	_____	_____
(laikiną leidimą išdavusios ŠPT ar žinybinės ŠPT vadovo pareigos)	(parašas)	(vardas, pavardė)

Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklių
3 priedas

(RIBOTO LEIDIMO AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ FORMA)

20 m. d. Nr.

Vilnius

Šis ribotas leidimas išduotas

_____
(paslapčių subjekto pavadinimas arba rangovo (subrangovo) pavadinimas)

ir patvirtina, kad automatizuoto duomenų apdorojimo sistema ar tinklas

_____,
(automatizuoto duomenų apdorojimo sistemos ar tinklo pavadinimas)

valdoma (-as)

_____
(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo pavadinimas)

_____,
(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo adresas)

turi teisę atlikti šio leidimo 1 p. nurodytoje išvadoje nustatytus vienkartinius veiksmus nurodyta apimtimi ir sąlygomis ir automatizuotai apdoroti įslaptintą informaciją, žymimą slaptumo žyma (žymomis)

_____ ir žemesne (žemesnėmis).
(slaptumo žyma ar žymos)

Ribotas leidimas išduotas vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) 40 str. 3 d. ir šiais teisės aktais:

1. _____
(SPT ar žinybinės SPT funkcijas atliekančios institucijos, surašiusios išvadą dėl riboto leidimo išdavimo, pavadinimas, išvados data ir numeris)
2. _____
(Specifinių saugumo reikalavimų aprašo pavadinimas, teisės aktą, kuriuo jis patvirtintas, priėmusios institucijos pavadinimas, teisės akto rūšis, numeris, priėmimo data)
3. _____
(Saugumo valdymo procedūrų aprašo pavadinimas, teisės aktą, kuriuo jis patvirtintas, priėmusios institucijos pavadinimas, teisės akto rūšis, numeris, priėmimo data)
4. _____
(Rizikos analizės pavadinimas, teisės aktą, kuriuo jis patvirtintas, priėmusios institucijos pavadinimas, teisės akto rūšis, numeris, priėmimo data)
5. _____
(kiti teisės aktai)

Ribotas leidimas galioja: _____
(riboto leidimo galiojimo terminas)

_____	_____	_____
(ribotą leidimą išdavusios SPT ar žinybinės SPT vadovo pareigos)	(parašas)	(vardas, pavardė)

4.3. KRAŠTO APSAUGOS MINISTRO 2005 M. GRUODŽIO 29 D. ĮSAKYMAS NR. V-1706 „DĖL ĮSLAPTINTŲ DOKUMENTŲ, ŽYMIMŲ SLAPTUMO ŽYMA „RIBOTO NAUDOJIMO“, ADMINISTRAVIMO TVARKOS APRAŠO PATVIRTINIMO“

Vadovaudamasis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) ir Lietuvos Respublikos Vyriausybės 2005 m. gruodžio 5 d. nutarimu Nr. 1307 „Dėl įslaptintos informacijos administravimo taisyklių patvirtinimo“ (Žin., 2005, Nr. 143-5193) :

1. T v i r t i n u Įslaptintų dokumentų, žymimų slaptumo žyma „Riboto naudojimo“, administravimo tvarkos aprašą (pridedama).

2. S u t e i k i u krašto apsaugos sistemos institucijų ir įstaigų, kuriose dirbama su įslaptinta informacija ar saugoma įslaptinta informacija, žymima slaptumo žyma „Riboto naudojimo“, vadovams teisę vadovaujantis šiuo įsakymu patvirtintu tvarkos aprašu organizuoti įslaptintų dokumentų, žymimų slaptumo žyma „Riboto naudojimo“, administravimą administracinėje saugumo zonoje.

3. L a i k a u netekusiu galios Krašto apsaugos ministro 2003 m. sausio 30 d. įsakymą Nr. V-121 „Dėl įslaptintų dokumentų, žymimų slaptumo žymomis „Konfidencialiai“ ir „Riboto naudojimo“ administravimo krašto apsaugos sistemoje laikinosios tvarkos patvirtinimo“.

4. S u t e i k i u įsakymo 2 punkte išvardytų institucijų ir įstaigų vadovams, vadovaujantis principu „Būtina žinoti“, teisę leisti su disponuojamais įslaptintais dokumentais, pažymėtais slaptumo žyma „Riboto naudojimo“, susipažinti kitų paslapčių subjektų asmenims, pateikusiems institucijos, kurioje jie dirba, vadovo pasirašytą prašymą.

PATVIRTINTA
Lietuvos Respublikos krašto apsaugos ministro 2005 m. gruodžio 29 d.
įsakymu Nr. V- 1706

ĮSLAPTINTŲ DOKUMENTŲ, ŽYMIMŲ SLAPTUMO ŽYMA „RIBOTO NAUDOJIMO“, ADMINISTRAVIMO TVARKOS APRAŠAS

I. BENDROSIOS NUOSTATOS

1. Įslaptintų dokumentų, žymimų slaptumo žyma „Riboto naudojimo“, administravimo tvarkos aprašas (toliau – tvarka) nustato Lietuvos Respublikos įslaptintų dokumentų, žymimų slaptumo žyma „Riboto naudojimo“ (toliau – dokumentai) saugojimo vietą, apskaitos sistemų funkcionavimą, platinimo, dauginimo, kitų asmenų supažindinimo, vertimų, išslaptinimo, naikinimo procedūras krašto apsaugos sistemos institucijose ir įstaigose.

2. Šia tvarka privalo vadovautis krašto apsaugos sistemos institucijos ir įstaigos, kuriose dirbama su įslaptinta informacija ar saugoma įslaptinta informacija, žymima slaptumo žyma „Riboto naudojimo“.

3. Dokumentai krašto apsaugos sistemos institucijose ir įstaigose rengiami ir įforminami pagal Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės (toliau – Lietuvos archyvų departamentas) nustatytus bendruosius dokumentų rengimo, tvarkymo ir apskaitos reikalavimus ir Lietuvos Respublikos Vyriausybės patvirtintų Įslaptintos informacijos administravimo taisyklių reikalavimus.

4. Tvarka parengta vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29), Lietuvos Respublikos Vyriausybės 2005 m. gruodžio 5 d nutarimu Nr. 1307 „Dėl įslaptintų dokumentų administravimo taisyklių patvirtinimo“ (Žin., 2005, Nr. 143-5193) ir kitais teisės aktais.

II. ĮSLAPTINTŲ DOKUMENTŲ ADMINISTRAVIMO ORGANIZAVIMAS

5. Už dokumentų administravimo reikalavimų vykdymą krašto apsaugos sistemos institucijose, įstaigose ir jos struktūriniuose padaliniuose (kuriuose įslaptinti dokumentai rengiami, įforminami, registruojami, siunčiami, gabenami, gaunami, dauginami, saugomi, apskaitomi, tvarkomi ir naikinami) atsakingi šių institucijų, įstaigų ir jų struktūrinių padalinių vadovai, jų įgalioti asmenys, taip pat asmenys, kuriems šie dokumentai yra patikėti.

6. Su dokumentais dirbama, dokumentai ir sudarytos bylos saugomos administracinėje arba aukštesnėje saugumo klasės zonoje. Administracinėje saugumo zonoje dokumentai ar sudarytos bylos turi būti saugomos rakinamose me-

talinėse spintose.

7. Krašto apsaugos sistemos institucijos ar įstaigos vadovas, atsižvelgdamas į tai, kurioje saugumo zonoje administruojami dokumentai:

7.1. paskiria atsakingą asmenį, asmenis ar padalinius dokumentų administravimo funkcijoms atlikti (toliau – atsakingas asmuo), nustato jo kompetenciją ir atsakomybę;

7.2. tvirtina dokumentų registrų sąrašą ir nustato, kokie registrai turi būti naudojami;

7.3. nustato darbo su dokumentais, dokumentų registrų, bylų sudarymo ir dokumentų saugojimo vietas ir jų apsaugos priemones.

8. Paslapčių subjekto dokumentų administravimo priežiūra vykdoma Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo, kitų įstatymų ir norminių teisės aktų nustatyta tvarka.

III. ATSAKINGAS ASMUO

9. Už dokumentų administravimą atsakingas asmuo tvarko dokumentų apskaitą, juos registruoja, kontroliuoja apyvartą, perduoda dokumentus ar jų kopijas vykdytojams ir kitiems paslapčių subjektams, atrenka dokumentus naikinti, išslaptinti arba pratęsti jų įslaptinimo terminą, informuoja paslapčių subjektus apie įslaptintų dokumentų išslaptinimą ar įslaptinimo termino pratęsimą, naikina dokumentus, tikrina juos, užtikrina, kad administruojant dokumentus būtų laikomasi principo „Būtina žinoti“.

10. Atsakingo asmens kompetencija, funkcijos ir atsakomybė apibrėžiami atsakingo asmens pareigybės aprašyme, pareiginiuose nuostatuose ar padalinio nuostatuose.

11. Atsakingas asmuo turi būti pasirašytinai supažindintas su Detaliuoju įslaptintos informacijos, susijusios su krašto apsaugos sistemos veikla, sąrašu, įstatymų nustatyta atsakomybe už neteisėtą disponavimą įslaptinta informacija, įslaptintos informacijos atskleidimą, praradimą, pagrobimą ar kitokį neteisėtą įgijimą, įslaptintos informacijos apsaugą reglamentuojančių teisės aktų reikalavimais.

IV. ĮSLAPTINTŲ DOKUMENTŲ REGISTRAVIMAS

12. Parengti ir gauti dokumentai registruojami elektroniniuose ar įprastuose dokumentų registruose, vadovaujantis Įslaptintos informacijos administravimo taisyklių reikalavimais.

13. Tvarkomieji dokumentai (nutarimai, sprendimai, įsakymai, potvarkiai ir kita) gali būti registruojami dokumentų registruose kartu su neįslaptintais tvarkomaisiais dokumentais, jei jų pavadinimuose nėra tarnybos paslaptį sudarančios informacijos.

14. Dokumentų registrai įrašomi į krašto apsaugos sistemos institucijos ar įstaigos įslaptintų dokumentų registrų sąrašą arba, jeigu dokumentų registrų pavadinimuose nėra tarnybos paslaptį sudarančios informacijos, į bendrą paslapčių subjekto dokumentų registrų sąrašą ir atskiras įslaptintų dokumentų registrų sąrašas nesudaromas.

15. Dokumentų registrų sąrašas sudaromas pagal Lietuvos archyvų departamento nustatytus bendruosius dokumentų rengimo, tvarkymo ir apskaitos reikalavimus.

16. NATO, Europos Sąjungos Lietuvai perduoti dokumentai, pažymėti žymomis „NATO Restricted“ ir „EU Restreint“, gauti su nacionaliniais lydraščiais, registruojami vadovaujantis NATO, Europos Sąjungos Lietuvai perduotų įslaptintų dokumentų administravimo taisyklių reikalavimais antrinėse subregistratūrose arba kontrolės punktuose.

V. DOKUMENTŲ GABENIMAS IR SIUNTIMAS

17. Dokumentai adresatams gabenami ar siunčiami laikantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo 24 straipsnyje, Įslaptintų dokumentų administravimo taisyklių nustatytų reikalavimų.

18. Dokumentai adresatams siunčiami šifruotojo ryšio priemonėmis, gabenami diplomatinių, karinių, kurjerių pašto tarnybų kurjerių, krašto apsaugos sistemos institucijų ir įstaigų vadovų įgaliotų asmenų, dokumentų rengėjų arba užduočių vykdytojų taip, kad būtų užtikrintas gabenamų dokumentų saugumas.

VI. GAUTŲ DOKUMENTŲ PERDAVIMAS, KOPIJŲ (IŠRAŠŲ) PLATINIMAS

19. Gauti ir užregistruoti dokumentų originalai perduodami institucijos ar įstaigos, kuriai adresuoti dokumentai, vadovui. Jis susipažįsta su dokumentais ir, jei reikia vykdyti užduotį, rašo rezoliucijas, t. y. paskiria vykdytojus ir užduočių vykdymo terminus.

20. Dokumentai su rezoliucijomis grąžinami atsakingam asmeniui, kuris rezoliucijas surašo į dokumentų registrą ir dokumentų kopijas perduoda užduočių vykdytojams.

21. Skubiais atvejais vykdytojai, kuriems buvo persiųsti dokumentai, turi teisę perduoti kitiems darbuotojams dokumentų originalus ar duoti nurodymą daryti jų kopijas negrąžindami dokumentų atsakingam asmeniui. Dokumentai grąžinami įvykdžius užduotį.

22. Vykdytojas, gavęs dokumentų kopijas (išrašus), gali padaryti papildomų kopijų (išrašų) (ar perduoti turimas) susipažinti kitiems skyriaus (institucijos ar įstaigos) darbuotojams, laikydamasis principo „Būtina žinoti“, jeigu dokumente nėra nuorodos „Būtinas informacijos rengėjo sutikimas“.

VII. DOKUMENTŲ TVARKYMAS IR PATIKRINIMAS

23. Dokumentai tvarkomi, jų bylos sudaromos ir įforminamos pagal Lietuvos archyvų departamento nustatytus bendruosius dokumentų rengimo, tvarkymo ir apskaitos reikalavimus, Įslaptintos informacijos administravimo taisyklių reikalavimus.

24. Dokumentų bylos, jei jų antraštėse nėra tarnybos paslaptį susarančios informacijos, gali būti įrašomos į kiekvienais metais sudaromo bendro dokumentacijos plano įslaptintų bylų skyrių.

25. Kartą per 5 metus atliekamas dokumentų patikrinimas, kurio metu tikri-

nama ar įslaptintų dokumentų registruose įrašyti dokumentai saugomi nurodytose bylose.

VIII. BYLŲ APSKAITA IR SAUGOJIMAS

26. Bylų apskaita tvarkoma laikantis Įslaptinto informacijos administravimo taisyklių reikalavimų.

IX. DOKUMENTŲ IŠSLAPTINIMAS IR NAIKINIMAS

27. Dokumentai išslaptinami, įslaptinimo terminai keičiami laikantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo 10 straipsnio ir Įslaptintos informacijos administravimo taisyklėse nustatytų reikalavimų.

28. Dokumentų kopijos (išrašai) naikinami asmens, kuris jais disponuoja, sprendimu, kai jos tampa nebereikalingos ar užduotis įvykdyta.

29. Dokumentai, jų kopijos (išrašai), vertimai turi būti sunaikinti taip, kad būtų neįmanoma atkurti paties dokumento ar jo dalies turinio.

4.4. KRAŠTO APSAUGOS MINISTRO 2006 M. LAPKRIČIO 22 D. ĮSAKYMAS NR. V-1184 „DĖL KRAŠTO APSAUGOS SISTEMOS ĮSLAPTINTŲ DOKUMENTŲ, GAMINIŲ IR KITŲ OBJEKTŲ GABENIMO TVARKOS APRAŠO PATVIRTINIMO“

Vadovaudamasis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) 24 straipsniu, Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatymo (Žin., 1998, Nr. 49-1325; 1999, Nr. 64-2069; 2003, Nr. 32-1308, Nr. 91(1)-4106; 2004, Nr. 169-6215) 10 straipsnio 2 dalies 5 punktu, Lietuvos Respublikos įstatymo „Dėl Šiaurės Atlanto sutarties šalių susitarimo dėl informacijos saugumo, NATO susitarimo dėl su gynyba susijusių išradimų, dėl kurių paduotos patento paraiškos, abipusės slaptumo apsaugos bei NATO susitarimo dėl techninės informacijos perdavimo gynybos tikslais ratifikavimo“ (Žin., 2004, Nr. 127-4556) 3 straipsniu ir siekdamas užtikrinti įslaptintos informacijos apsaugą krašto apsaugos sistemoje:

1. T v i r t i n u Krašto apsaugos sistemos įslaptintų dokumentų, gaminių ir kitų objektų gabenimo tvarkos aprašą (pridedama).

2. Į s a k a u krašto apsaugos sistemos institucijų vadovams vadovautis patvirtintu tvarkos aprašu organizuojant įslaptintų dokumentų, gaminių ir kitų objektų gabenimą.

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2006 m. lapkričio 22 d.
įsakymu Nr. V-1184

KRAŠTO APSAUGOS SISTEMOS ĮSLAPTINTŲ DOKUMENTŲ, GAMINIŲ IR KITŲ OBJEKTŲ GABENIMO TVARKOS APRAŠAS

I. BENDROSIOS NUOSTATOS

1. Krašto apsaugos sistemos įslaptintų dokumentų, gaminių ir kitų objektų gabenimo tvarkos aprašas (toliau – tvarkos aprašas) nustato bendruosius krašto apsaugos sistemos institucijų ir joms perduotų kitų Lietuvos Respublikos paslapčių subjektų, užsienio valstybių, Europos Sąjungos ar kitų tarptautinių organizacijų įslaptintų dokumentų, gaminių ir kitų objektų gabenimo Lietuvos Respublikoje, į užsienio valstybes ir iš jų reikalavimus.

2. Užsienio valstybių, Europos Sąjungos ar kitų tarptautinių organizacijų įslaptinti dokumentai, gaminiai ir kiti objektai, perduoti krašto apsaugos sistemos institucijoms, gabenami vadovaujantis Lietuvos Respublikos tarptautinėmis sutartimis, Lietuvos Respublikos įstatymais, kitais Lietuvos Respublikos teisės aktais bei šiuo tvarkos aprašu.

3. Gabenant įslaptintus dokumentus, gaminius ir kitus objektus, taikomi visi įslaptintos informacijos apsaugos reikalavimai, nustatyti Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) ir kitų teisės aktų, reglamentuojančių įslaptintos informacijos apsaugą.

4. Šio tvarkos aprašo reikalavimų privalo laikytis krašto apsaugos ministro ar jo įgalioto asmens paskirti asmenys, taip pat Karo policijos Kurjerių skyriaus, kurjerių pašto tarnybų, su kuriomis Krašto apsaugos ministerija yra sudariusi įslaptintų dokumentų, gaminių ir kitų objektų gabenimo sutartį, asmenys, gabendami įslaptintus dokumentus, gaminius ir kitus objektus.

5. Sudarant sutartis su kurjerių pašto tarnybomis, į sutartis privalo būti įtraukti šiame tvarkos apraše numatyti įslaptintos informacijos gabenimo saugumo reikalavimai.

6. Šio tvarkos aprašo nuostatos netaikomos gabenant įslaptintus dokumentus, žymimus slaptumo žyma „Riboto naudojimo“, ir kriptografines priemones.

7. Aprašas parengtas vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu, Šiaurės Atlanto Sutarties Organizacijos (toliau – NATO) 2006 m. gegužės 11 d. direktyva 15-25, dokumentu C-M(2002)49 „NATO saugumo politika“ bei papildomomis direktyvomis.

8. Šiame tvarkos apraše vartojamos sąvokos:

Kariniai kurjeriai – Karo policijos Kurjerių skyriaus asmenys, įgalioti gabenti įslaptintą informaciją, ir turintys šios tarnybos išduotus karinio kurjerio pažymėjimus.

Gabenimas – dokumentų, gaminių ar kitų objektų pristatymas įslaptintos informacijos gavėjui.

Kitos šiame tvarkos apraše vartojamos sąvokos atitinka Lietuvos Respubli-

kos valstybės ir tarnybos paslapčių įstatyme vartojamas sąvokas.

II. ĮSLAPTINTŲ DOKUMENTŲ, GAMINIŲ IR KITŲ OBJEKTŲ GABENIMO LIETUVOS RESPUBLIKOJE TVARKA

9. Dokumentus, gaminius ir kitus objektus krašto apsaugos sistemoje gali gabenti:

9.1. krašto apsaugos sistemos institucijų, įstaigų ar padalinių vadovų įgalioti asmenys.

9.2. Karo policijos Kurjerių skyrius (toliau – kariniai kurjeriai);

9.3. kurjerių pašto tarnybų, su kuriomis krašto apsaugos sistemos institucijos yra sudariusios įslaptintų dokumentų, gaminių ir kitų objektų gabenimo sutartis, asmenys.

9.4. Neteko galios.

10. Įslaptintus dokumentus, gaminius ir kitus objektus, žymimus slaptumo žyma „Visiškai slaptai“, Lietuvos Respublikos teritorijoje turi gabenti ne mažiau kaip du kariniai kurjeriai arba krašto apsaugos ministro ar jo įgalioto asmens paskirti atsakingieji asmenys, kurių vienas turi būti ginkluotas šaunamuoju ginklu.

11. Įslaptintus dokumentus, gaminius ir kitus objektus, žymimus slaptumo žyma „Slaptai“, Lietuvos Respublikos teritorijoje turi gabenti vienas šaunamuoju ginklu ginkluotas asmuo arba ne mažiau kaip du neginkluoti kariniai ar kurjerių pašto tarnybų kurjeriai, arba krašto apsaugos ministro ar jo įgalioto asmens paskirti atsakingieji asmenys.

12. Asmenys, gabenantys įslaptintus dokumentus, gaminius ir kitus objektus, privalo turėti Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka išduotą leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą.

13. Dokumentus, gaminius ir kitus objektus gabenantys asmenys privalo turėti ryšio priemones, kad esant reikalui būtų galima išsikviesti pagalbą.

14. Gabenti įslaptintus dokumentus, žymimus slaptumo žymomis „Visiškai slaptai“ ir „Slaptai“, turi ne mažiau kaip 2 (du) asmenys, o įslaptintus dokumentus, žymimus slaptumo žyma „Konfidencialiai“, gali gabenti vienas 9 punkte įvardytas asmuo.

III. ĮSLAPTINTŲ DOKUMENTŲ, GAMINIŲ IR KITŲ OBJEKTŲ PARUOŠIMO GABENTI TVARKA

15. Siuntėjas yra atsakingas už įslaptintų dokumentų, gaminių ir kitų objektų paruošimą gabenti.

16. Keliami šie dokumentų, gaminių ir kitų objektų pakavimo reikalavimai:

16.1. supakuota turi būti taip, kad neįmanoma būtų nustatyti gaminio pobūdžio ar savybių (jeigu pobūdis ar savybės sudaro paslaptį);

16.2. pakuojama į vidinę ir išorinę pakuotę taip, kad būtų užtikrintas ne tik gaminio ar kito objekto įslaptintos informacijos saugumas, bet ir apsauga nuo mechaninių pažeidimų gabenant;

16.3. vidinė pakuotė turi būti plombuojama (klijuojama lipnia juosta ar kitu būdu). Plomba turi būti uždėta taip, kad bandant atidaryti pakuotę

(išpakuoti), plomba būtų pažeidžiama ir pažeidimo faktą būtų įmanoma nustatyti;

16.4. ant vidinės pakuotės privalo būti:

- slaptumo žyma;
- atsakingojo asmens, pakavusio gaminį, vardas ir pavardė, parašas, taip pat atsakingojo asmens ar paslapčių subjekto spaudas;
- gaminio registracijos numeris;
- gaminio inventorinis numeris, jei toks yra;
- adresatas;
- siuntėjas.

17. Išorinė pakuotė privalo nesiskirti nuo paprastiems siuntiniams gabenti skirtų pakuočių.

18. Ant išorinės pakuotės privalo būti nurodyta:

- gavėjo adresas;
- siuntų registro numeris;
- žyma „Tik kurjeris“.

19. Ant išorinės pakuotės gali būti pateikta gabenimo skubumo žyma. Skubumo žymos yra:

19.1. „PRISTATYTI IKI _____ (data) “ – privalu pristatyti iki nurodytos datos;

19.2. „NEDELSIANT“ – privalu pristatyti per 48 val.;

19.3. „PIRMUMO TVARKA“ – siuntinys pristatomas pirmiau nei paprasti (nepažymėti gabenimo skubumo žyma) siuntiniai.

20. Siuntų gabenimo svoriai, matmenys:

20.1. atskiro siunčiamo daikto svoris negali viršyti 15 kg;

20.2. 50 kg yra maksimalus vieno supakuoto siuntinio, kurį galima išsiųsti be išankstinio siuntėjo pranešimo, svoris;

20.3. dėžėje negalima pakuoti keleto siuntinių, jeigu jų bendras svoris viršija 50 kg; siuntėjas, išsiųsdamas vieną ar keletą dėžių, kurių kiekviena viršija 50 kg, privalo užtikrinti, kad siuntos turinys būtų vientisas ir negalėtų būti susmulkintas į keletą mažesnių dalių;

20.4. maksimalus siuntinio dydis – 105x70x60 cm;

20.5. siuntiniai, kuriems reikalingos medinės dėžės, neturi viršyti šių matmenų – 100x100x100 cm;

20.6. jei siuntiniai viršija nurodytus matmenis, siuntėjas apie tai privalo pranešti siuntinius gabenančiai institucijai likus ne mažiau kaip 24 val. iki išsiuntimo.

IV. ĮSLAPTINTŲ DOKUMENTŲ, GAMINIŲ BEI KITŲ OBJEKTŲ PERDAVIMO IR PRIĖMIMO TVARKA

21. Prireikus persiųsti dokumentus, gaminius ar kitus objektus, siuntėjas:

21.1. užpildo siuntų sąrašą (Lietuvos Respublikos Vyriausybės 2005 m. gruodžio 5 d. nutarimu Nr. 1307 patvirtintų Įslaptintos informacijos administravimo taisyklių 6 priedas), jame nurodo adresatą, siunčiamų įslaptintų dokumentų registracijos numerius, išsiuntimo datą ir laiką;

21.2. siųsdamas įslaptintus dokumentus, žymimus slaptumo žymomis „Vi-

siškai slaptai“ ar „Slaptai“, pildo 3 (tris) siuntų sąrašo egzempliorius, vienas sąrašo egzempliorius, pasirašytas kurjerio, paliekamas įslaptintų dokumentų siuntėjui, kitas įdedamas į siuntą (adresatui), trečias atiduodamas kurjeriui;

21.3. siųsdamas įslaptintus dokumentus, žymimus slaptumo žymomis „Konfidencialiai“ ar „Riboto naudojimo“, pildo 2 (du) siuntų sąrašo egzempliorius, vienas egzempliorius, pasirašytas kurjerio, paliekamas įslaptintų dokumentų siuntėjui, kitas atiduodamas kurjeriui;

21.4. siųsdamas įslaptintus dokumentus, gaminius ir kitus objektus per karinį kurjerį ar krašto apsaugos sistemos institucijų ar įstaigų vadovų įgaliotus asmenis, apsauginių vokų nenaudoja, siuntų sąrašų nepildo. Išsiuntimo datą, adresatą, siuntų skaičių, įslaptintų dokumentų registracijos numerius nurodo Siuntų su įslaptintais dokumentais įteikimo žurnale (Lietuvos Respublikos Vyriausybės 2005 m. gruodžio 5 d. nutarimu Nr. 1307 patvirtintų Įslaptintos informacijos administravimo taisyklių 7 priedas), kuris pateikiamas pasirašyti pristačius siuntą.

V. ĮSLAPTINTŲ DOKUMENTŲ, GAMINIŲ IR KITŲ OBJEKTŲ GABENIMO, PERDAVIMO TVARKA

22. Kurjeris, gabendamas siuntinį, privalo:

22.1. parinkti saugiausią gabenimo būdą ir maršrutą pagal iš anksto sudarytą ir kurjerių tarnybos patvirtintą maršrutų sąrašą;

22.2. užtikrinti gabenamų dokumentų, gaminių ir kitų objektų saugumą;

22.3. gabenti taip, kad atsitiktiniai asmenys negalėtų nustatyti, jog gabenama informacija yra įslaptinta, ir susipažinti su tokia informacija;

22.4. įslaptintus dokumentus, gaminius ir kitus objektus gabenantis asmuo privalo užtikrinti jų apsaugą nuo praradimo panaudodamas visas priemones – kovinius veiksmus, turimas specialiąsias priemones ar šaunamąjį ginklą. Šios priemonės turi būti naudojamos proporcingai pradėtam ar tiesiogiai gresiančiam pavojingam kėsinimuisi užvaldyti įslaptintą informaciją. Šaunamasis ginklas gali būti naudojamas jeigu kyla pavojus užpultojo gyvybei ar sveikatai.

23. Pristačius siuntinį adresu, nurodytu ant pakuotės, reikia perduoti jį gavėjo atsakingajam asmeniui ir duoti pasirašyti siuntų sąraše. Šį sąrašą būtina saugoti kaip dokumentą, patvirtinantį siuntinio pristatymą. Gavimo faktą patvirtinančiuose dokumentuose turi būti nurodytas siuntinio paketo numeris.

24. Gavimo faktą patvirtinantis dokumentas turi būti įdėtas į siuntinio paketo vidų. Gavimo faktą patvirtinantis dokumentas ir perduodami dokumentai turi būti užregistruoti.

25. Gavimo faktą patvirtinančiame dokumente, nurodžius datą ir pasirašius, jis turi būti nedelsiant grąžinamas siuntėjui.

26. Jeigu siuntinio pakuotė pažeista:

26.1. siuntinys neišpakuojamas;

26.2. rengiama pažyma apie pakuotės pažeidimus, ją pasirašo nurodytus pažeidimus nustatęs asmuo ir siuntą pristatęs įgaliotasis asmuo;

26.3. įgaliotojo asmens pateiktame siuntų sąraše pateikiama pažymos nuoroda;

26.4. apie siuntinio pažeidimus nedelsiant informuojamas siuntinio siuntėjas.

VI. ĮSLAPTINTŲ DOKUMENTŲ, GAMINIŲ IR KITŲ OBJEKTŲ GABENIMO Į (IŠ) UŽSIENIO VALSTYBIŲ, EUROPOS SĄJUNGOS AR KITŲ TARPTAUTINIŲ ORGANIZACIJŲ TVARKA

27. Gabenti dokumentus, turinčius slaptumo žymą „Visiškai slaptai“ (COSMIC TOP SECRET), tarp valstybių draudžiama. Informacija, pažymėta slaptumo žyma „Visiškai slaptai“, platinama COSMIC registratūros kanalais.

28. Įslaptintų dokumentų, gaminių ar kitų objektų muitinis tikrinimas ir įforminimas atliekamas vadovaujantis Europos Bendrijos teisės aktų, Lietuvos Respublikos tarptautinių sutarčių, Lietuvos Respublikos įstatymų bei kitų teisės aktų nustatyta tvarka.

29. Įslaptintus dokumentus, gaminius ir kitus objektus turi teisę gabenti neginkluoti, bet ne mažiau kaip du:

29.1. krašto apsaugos ministro ar jo įgalioto asmens paskirti atsakingieji asmenys;

29.2. kariniai kurjeriai;

29.3. kurjerių pašto tarnybų, su kuriomis Krašto apsaugos ministerija yra sudariusi įslaptintų dokumentų, gaminių ir kitų objektų gabenimo sutartį, asmenys. Jie privalo turėti Valstybės saugumo departamento vadovybės leidimą;

29.4. diplomatiniai kurjeriai

30. Įslaptintą NATO informaciją gabenti asmeniniu bagažu NATO valstybėje gali būti leidžiama laikantis tokių pat griežtų reikalavimų, kaip ir gabenant atitinkamą slaptumo žymą turinčią nacionalinę informaciją. Taip pat reikalinga atsižvelgti į šiuos reikalavimus:

30.1. visą gabenamą informaciją, įtrauktą į apskaitą, būtina registruoti atitinkamoje registratūroje, kontrolės punkte ar įstaigoje;

30.2. įslaptinta informacija turi būti supakuota pagal 35 punkte nurodytus reikalavimus, o rakinamasis lagaminas turi būti tokio dydžio ir svorio, kad asmuo jį galėtų nuolat nešiotis su savimi;

30.3. įslaptintos informacijos gabentojas neturi niekam jos palikti, išskyrus tam skirtas vietas, įslaptinta informacija neturi būti paliekama be priežiūros, o jos pakuotė gabenimo metu neturi būti atidaroma;

30.4. įslaptinta informacija neturi būti skaitoma viešose vietose;

30.5. asmuo turi būti supažindintas su funkcijomis, atliekamomis gabenant įslaptintą medžiagą, ir su savimi turėti raštiškus įgaliojimus gabenti tokią medžiagą; gabenant įslaptintą NATO informaciją, pažymėtą „NATO Konfidencialiai“ (NATO CONFIDENTIAL) ir aukštesnėmis slaptumo žymomis, asmuo privalo turėti visose NATO valstybėse pripažįstamą kurjerio pažymėjimą, įgaliojantį jį gabenti nurodytus dokumentus.

31. Įslaptinti dokumentai, gaminiai ar kiti objektai gabenami vadovaujantis Lietuvos Respublikos tarptautinių sutarčių ir šiomis sutartimis grindžiamų bei jas įgyvendinančių tarptautinių organizacijų sprendimų, Europos Sąjungos teisės aktų bei Lietuvos Respublikos Valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka.

32. Neteko galios.

33. Įslaptinta informacija, pažymėta žyma „NATO Konfidencialiai“ (NATO CONFIDENTIAL) ir aukštesnėmis slaptumo žymomis, gabenama tarp objektų

ar įstaigų, turi būti supakuota taip, kad neturintys tam teisės asmenys negalėtų su ja susipažinti. Taikomi šie pakavimo reikalavimai:

33.1. dokumentai turi būti įdėti į dvigubus nepermatomus ir tvirtus vokus. Rakinamasis lagaminas ar kita plombuojama tara gali būti laikomi viršutiniu voku;

33.2. vidinis vokas turi būti apsaugotas, ant jo turi būti atitinkamos NATO slaptumo žymos spaudas, gavėjo adresas;

33.3. ant viršutinio voko turi būti nurodytas gavėjas (institucija, bet ne konkretus asmuo) ir jo adresas, taip pat paketo numeris, kad būtų galima užpildyti dokumento gavimo kvitą;

33.4. ant viršutinio voko neturi būti jokios nuorodos, iš kurios būtų galima suprasti, kokia yra informacijos, esančios voke, slaptumo žyma ar kad voke apskritai esama įslaptintos informacijos;

33.5. jei dokumentai perduodami dvigubame voke per kurjerį, ant viršutinio voko turi būti pateikta nuoroda „Tik per kurjerį“.

34. Gabenant dokumentus turi būti laikomasi šių principų:

34.1. apsauga turi būti užtikrinama visais gabenimo etapais ir visomis aplinkybėmis, nuo pradinio punkto iki adresato;

34.2. nustatytas krovinio apsaugos lygis turi atitikti aukščiausią jame esančios medžiagos slaptumo laipsnį;

34.3. kelionės maršrutas turi būti (kiek įmanoma) tiesioginis ir kelionė turi trukti kaip įmanoma trumpiau;

34.4. būtina pasirūpinti, kad kelionės maršrutas eitų tik per NATO valstybių teritorijas. Maršrutais per NATO nepriklausančias valstybes turi būti keliaujama tik Valstybės saugumo departamentui leidus.

35. Asmenys, gabenantys įslaptintus Europos Sąjungos dokumentus, žymimus slaptumo žymomis „ES Slaptai“, „ES Konfidencialiai“, taip pat asmenys, gabenantys įslaptintus NATO dokumentus, žymimus slaptumo žymomis „NATO Slaptai“, „NATO Konfidencialiai“, privalo turėti atitinkamą Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka išduotą asmens patikimumo pažymėjimą.

36. Kurjeriai bei apsaugos darbuotojai ir krovinį lydintys asmenys turi būti supažindinti su NATO, ES saugumo procedūromis ir funkcijomis saugant patikėtą įslaptintą NATO, ES informaciją.

VII. KURJERIŲ IR KITŲ ASMENŲ, ĮGALIOTŲ GABENTI SIUNTINIUS, VEIKSMŲ APRIBOJIMAI

37. Kurjeriui ar kitam asmeniui, įgaliotam gabenti įslaptintą informaciją, draudžiama:

37.1. atlikti kitas užduotis ar pavedimus, nesusijusius su įslaptintos informacijos gabenimu;

37.2. asmenis, nesusijusius su šios informacijos gabenimu ir apsauga, vežti transportu, skirtu įslaptintai informacijai gabenti;

37.3. kartu su įslaptinta informacija gabenti kitus krovinius;

37.4. pažeisti siuntinio pakuotę;

37.5. susipažinti su įslaptinta informacija.

VIII. ATSAKOMYBĖ

38. Asmuo už šio tvarkos aprašo nuostatų nesilaikymą, neteisėtą įslaptintos informacijos rinkimą, naudojimą, perdavimą ar praradimą ir kitus padarytus darbo su įslaptinta informacija reikalavimų pažeidimus atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

IX. BAIGIAMOSIOS NUOSTATOS

(NETEKO GALIOS)

4.5. KRAŠTO APSAUGOS MINISTRO 2006 M. LAPKRIČIO 27 D. ĮSAKYMAS NR. V-1217 „DĖL SAUGUMO ZONŲ REGLAMENTO PATVIRTINIMO“ *

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2006 m. lapkričio 27 d.
įsakymu Nr. V-1217

SAUGUMO ZONŲ REGLAMENTAS

I. BENDROSIOS NUOSTATOS

1. Saugumo zonų reglamentas (toliau – Reglamentas) nustato krašto apsaugos sistemos institucijų ir įstaigų valdomų ar naudojamų karinių teritorijų, pastatų ar patalpų, skirtų dirbti su įslaptinta informacija ar šiai informacijai saugoti, priskyrimo I, II klasės ar administracinei saugumo zonai tvarką.

2. Reglamentas netaikomas Nuolatinės atstovybės prie Šiaurės Atlanto Sutarties Organizacijos kariniam atstovui, Gynybos reikalų skyriui, Lietuvos nacionalinio karinio atstovo biurui Vyriausiojoje jungtinių pajėgų Europoje vadavietėje, Lietuvos Respublikos gynybos atašė ir tarptautinėse operacijose dalyvaujantiems padaliniams.

3. Reglamente vartojamos sąvokos atitinka Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) ir Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatyme (Žin., 1998, Nr. 49-1325; 1999, Nr. 64-2069; 2003, Nr. 32-1308, Nr. 91(1)-4106; 2004, Nr. 169-6215) vartojamas sąvokas.

4. Reglamentas parengtas vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29), Šiaurės Atlanto Sutarties Šalių susitarimu dėl informacijos saugumo (Žin., 2004, Nr. 127-4558), Europos Sąjungos Tarybos 2001 m. kovo 19 d. sprendimu Nr. 264 „Dėl Tarybos saugumo nuostatų“ ir kitais teisės aktais.

II. SAUGUMO ZONŲ NUSTATYMO TVARKA

5. Nustatant saugumo zonas, būtina atsižvelgti į turimos įslaptintos informacijos slaptumo žymas, apimtį, formą (įslaptinti dokumentai, gaminiai, kiti objektai), personalo turimus leidimus dirbti ar susipažinti su įslaptinta informacija, informacijos saugojimo būdą (informacija bus saugoma metalinėse spintose, seifuose ar prie jos bus galima prieiti tiesiogiai) ir įvertinti užsienio valstybių ar organizacijų žvalgybos tarnybų, sabotažo, terorizmo bei kitos nusikalstamos veikos riziką.

* **Pastaba**: Į rinkinį šis Krašto apsaugos ministro įsakymas neįtrauktas.

6. Saugumo zonos, kuriose saugoma įslaptinta informacija, žymima slaptumo žyma „Konfidencialiai“ ar aukštesne, nerekomenduojama nustatyti šalia zonų, kurias sunku arba visiškai neįmanoma kontroliuoti (pvz., automobilių stovėjimo aikštelių, išorinių pirmo ir paskutinio aukšto sienų, nekontroliuojamų pastatų ar kabinetų).

7. Saugumo zonų fizinės apsaugos priemonės turi užtikrinti Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo ir kitų teisės aktų nustatytų fizinės apsaugos reikalavimų vykdymą.

8. Karinės teritorijos, pastatų, patalpų suskirstymo į I, II klasės ar administracinę saugumo zonas planus tvirtina ir keičia karines teritorijas, pastatus, patalpas valdančių ar naudojančių institucijų, įstaigų ar jų struktūrinių padalinių vadovai (ar jų įgalioti asmenys), suderinę su:

8.1. Krašto apsaugos ministerijos specialiąja ekspertų komisija, kai tvirtinama Krašto apsaugos ministerijos ir tiesiogiai jai pavaldžios institucijos, įstaigos ar jos struktūrinio padalinio valdomos karinės teritorijos, pastato ar patalpos suskirstymo į I, II klasės ar administracinę saugumo zonas schema;

8.2. Gynybos štabo viršininko pavaduotoju žvalgybai (J2), kai tvirtinama tiesiogiai kariuomenės vadui pavaldaus karinio vieneto, neturinčio specialiosios ekspertų komisijos, valdomos karinės teritorijos, pastato ar patalpos suskirstymo į I, II klasės ar administracinę saugumo zonas schema;

8.3. pajėgų (valdybos) specialiąja ekspertų komisija, kai tvirtinama pajėgų (valdybos) ir joms pavaldžios institucijos, įstaigos ar struktūrinio padalinio valdomos karinės teritorijos, pastato ar patalpos suskirstymo į I, II klasės ar administracinę saugumo zonas schema.

9. Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos valdomos karinės teritorijos, pastato ar patalpos suskirstymo į I, II klasės ar administracinę saugumo zonas schemas tvirtina ir keičia Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos direktorius arba jo įgaliotas asmuo.

10. Karinių mokymų ir pratybų metu karinės teritorijos, pastatų ir patalpų, kuriose numatoma dirbti su įslaptinta informacija, žymima slaptumo žyma „Riboto naudojimo“, ar šią informaciją saugoti, priskyrimo administracinei saugumo zonai schemą tvirtina karinius mokymus ar pratybas organizuojančios institucijos, įstaigos ar jos struktūrinio padalinio vadovas (ar jo įgaliotas asmuo).

III. FIZINĖS APSAUGOS PROCEDŪRŲ REGLAMENTAVIMAS IR REIKALAVIMŲ VYKDYMAS

11. Institucijų, įstaigų ar jų struktūrinių padalinių vadovai (ar jų įgalioti asmenys) įslaptintos informacijos fizinei apsaugai užtikrinti privalo nustatyti fizinės apsaugos procedūras, kuriomis būtų reglamentuojama karinės teritorijos, pastatų ir patalpų apsaugos organizavimo, patekimo į saugumo zonas, patalpų atrakinimo ir užrakinimo, apsaugos signalizacijos įjungimo ir išjungimo, taip pat patekimo į seifus ir metalines spintas, kuriose saugoma įslaptinta informacija, raktų ir kodų (skaičių ar simbolių) apskaitos ir apsaugos, kodų keitimo tvarka bei remonto darbų saugumo zonose vykdymo tvarka ir kitos fizinės apsaugos

procedūros.

12. Fizinės apsaugos procedūros privalo būti suderintos su krašto apsaugos sistemos veiklos apsaugos ir vidaus saugumo reikalavimus reglamentuojančiais dokumentais.

13. Fizinės apsaugos reikalavimų vykdymui užtikrinti institucijų, įstaigų ar jų struktūrinių padalinių vadovai (ar jų įgalioti asmenys) privalo paskirti atsakinguosius asmenis.

IV. BAIGIAMOSIOS NUOSTATOS

14. Asmenys, nevykdantys šio Reglamento reikalavimų, atsako teisės aktų nustatyta tvarka.

4.6. KRAŠTO APSAUGOS MINISTRO 2006 M. GRUODŽIO 29 D. ĮSAKYMAS NR. V-1334 „DĖL KRAŠTO APSAUGOS SISTEMOS SAUGUMO SPECIALISTŲ PAREIGYBIŲ“

Vadovaudamasis Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatymo (Žin., 1998, Nr. 49-1325; 1999, Nr. 64-2069; 2003, Nr. 32-1308, Nr. 91(1)-4106; 2004, Nr. 169-6215) 10 straipsnio 2 dalies 5 punktu bei atsižvelgdamas į 2006 m. lapkričio 22 d. krašto apsaugos ministro įsakymą Nr.V-1188 „Dėl krašto apsaugos sistemos vidaus saugumo organizavimo“:

1. T v i r t i n u pridedamą Krašto apsaugos sistemos institucijų, įstaigų ir jų struktūrinių padalinių, kuriuose turi būti įsteigtos saugumo specialistų pareigybės, sąrašą (toliau – sąrašas).

2. N u r o d a u, kad jei sąraše nenurodyta kitaip, už institucijų, įstaigų ar struktūrinių padalinių (išskyrus Antrąjį operatyvinių tarnybų departamentą), įsikūrusių kitų krašto apsaugos institucijų, įstaigų ar struktūrinių padalinių valdomose arba naudojamose karinėse teritorijose, pastatuose ar patalpose, fizinės apsaugos organizavimą atsako pastarųjų saugumo specialistai.

3. P a v e d u Ministerijos valstybės sekretoriui kontroliuoti, kaip vykdomas šis įsakymas.

PATVIRTINTA
Lietuvos Respublikos krašto apsaugos
ministro 2006 m. gruodžio 29 d.
įsakymu Nr. V-1334

KRAŠTO APSAUGOS SISTEMOS INSTITUCIJŲ, ĮSTAIGŲ IR JŲ STRUKTŪRINIŲ PADALINIŲ, KURIUOSE TURI BŪTI ĮSTEIGTOS SAUGUMO SPECIALISTŲ PAREIGYBĖS, SĄRAŠAS

Eil. Nr.	Institucijos, įstaigos, struktūriniai padaliniai, kuriuose turi būti įsteigtos saugumo specialistų pareigybės	Institucijos, įstaigos, struktūriniai padaliniai, už kurių valdomų ar naudojamų karinių teritorijų, pastatų ar patalpų fizinės apsaugos organizavimą atsako saugumo specialistai
1.	Gynybos štabas	Krašto apsaugos ministerija ir jos struktūriniai padaliniai, įstaigos prie Ministerijos, įsikūrusios Ministerijos ir Gynybos štabo rūmų komplekse (Totorių 25/3 ir Šv. Ignoto 8/29, Vilnius).
2.	Karo prievolės administravimo tarnyba	Karo prievolės administravimo tarnyba, Karo prievolės centrai
3.	Infrastruktūros plėtros departamentas	Infrastruktūros plėtros departamentas

4.	Mobilizacijos departamentas	Mobilizacijos departamentas
5.	Krizių valdymo centras	Krizių valdymo centras
6.	Lauko (sausumos) pajėgų štabas	Lauko (sausumos) pajėgų štabo patalpos
7.	Motorizuotosios pėstininkų brigados „Geležinis Vilkas“ štabas	Motorizuotosios pėstininkų brigados „Geležinis Vilkas“ štabas
8.	Algirdo batalionas	Algirdo batalionas
9.	Kęstučio batalionas	Kęstučio batalionas
10.	Mindaugo batalionas	Mindaugo batalionas
11.	Birutės batalionas	Birutės batalionas
12.	Artilerijos batalionas	Artilerijos batalionas
13.	Krašto apsaugos savanorių pajėgų štabas	Krašto apsaugos savanorių pajėgų štabas ir pastatas (Viršuliškių g. 36, Vilnius), Aviacijos rinktinė
14.	KASP 1-oji rinktinė	KASP 1-oji rinktinė
15.	KASP 2-oji rinktinė	KASP 2-oji rinktinė
16.	KASP 3-oji rinktinė	KASP 3-oji rinktinė
17.	KASP 5-oji rinktinė	KASP 5-oji rinktinė
18.	KASP 8-oji rinktinė	KASP 8-oji rinktinė
19.	Butigeidžio batalionas	Butigeidžio batalionas
20.	Inžinerijos batalionas	Inžinerijos batalionas
21.	Karinių oro pajėgų štabas	Karinių oro pajėgų štabas
22.	Aviacijos bazė	Aviacijos bazė
23.	Oro erdvės stebėjimo ir kontrolės valdyba	Oro erdvės stebėjimo ir kontrolės valdyba
24.	Oro erdvės kontrolės centras	Oro erdvės kontrolės centras
25.	Oro gynybos batalionas	Oro gynybos batalionas
26.	Karinių jūrų pajėgų štabas	Karinių jūrų pajėgų štabas, Jūros ir pakrančių stebėjimo tarnyba
27.	Karo laivų flotilė	Karo laivų flotilė, laivai
28.	Logistikos valdyba	Logistikos valdyba, Materialinių resursų departamentas, Sandėlių tarnyba
29.	Karo medicinos tarnyba	Karo medicinos tarnyba
30.	Arsenalas	Arsenalas
31.	Judėjimo kontrolės centras	Judėjimo kontrolės centras
32.	Karo kartografijos centras	Karo kartografijos centras
33.	Vytenio bendrosios paramos logistikos batalionas	Vytenio bendrosios paramos logistikos batalionas
34.	Vaidoto tiesioginės paramos logistikos batalionas	Vaidoto tiesioginės paramos logistikos batalionas
35.	Mokymo ir doktrinų valdyba	Mokymo ir doktrinų valdyba
36.	Jonušo Radvilos mokomasis pulkas	Jonušo Radvilos mokomasis pulkas
37.	Puskarininkių mokykla	Puskarininkių mokykla
38.	Centrinis poligonas	Centrinis poligonas
39.	Lietuvos karo akademija	Lietuvos karo akademija
40.	Adolfo Ramanausko kovinio rengimo centras	Adolfo Ramanausko kovinio rengimo centras
41.	Specialiųjų operacijų junginio štabas	Specialiųjų operacijų junginio štabas
42.	Vytauto Didžiojo jėgerių batalionas	Vytauto Didžiojo jėgerių batalionas
43.	Ypatingos paskirties tarnyba	Ypatingos paskirties tarnyba
44.	Štabo batalionas	Štabo batalionas
45.	Karo policija	Karo policijos štabas

4.7. KRAŠTO APSAUGOS MINISTRO 2007 M. VASARIO 5 D. ĮSAKYMAS NR. V-137 „DĖL NETIKĖTŲ (KONTROLINIŲ) ĮSLAPTINTOS INFORMACIJOS APSAUGOS PATIKRINIMŲ KRAŠTO APSAUGOS SISTEMOJE“

Vadovaudamasis Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatymo (Žin., 1998, Nr. 49-1325; 1999, Nr. 64-2069; Nr. 91(1)-4106; 2004, Nr. 169-6215; 2006, Nr. 72-2679) 10 straipsnio 2 dalies 5 punktu ir įgyvendindamas Įslaptintos informacijos apsaugos būklės tikrinimo tvarkos aprašo, patvirtinto krašto apsaugos ministro 2006 m. birželio 2 d. įsakymu Nr. V-581 „Dėl Įslaptintos informacijos apsaugos būklės tikrinimo tvarkos aprašo patvirtinimo“, 13 punktą:

1. N u s t a t a u šią netikėtų (kontrolinių) patikrinimų tvarką:

1.1. netikėtus (kontrolinius) patikrinimus krašto apsaugos sistemoje (toliau - KAS) vykdo Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos (toliau – AOTD) direktoriaus įsakymu sudaryta AOTD komisija ar darbo grupė;

1.2. patikrinimai vykdomi pagal AOTD direktoriaus patvirtintą tikrinimų planą-grafiką iš anksto neinformuojant krašto apsaugos sistemos institucijų vadovų;

1.3. tikrinamos (pasirinktinai) visos įslaptintos informacijos apsaugos sritys, vertinant, ar galėjo būti įslaptintos informacijos praradimo ar neteisėto atskleidimo atvejų bei įslaptintos informacijos apsaugos pažeidimo faktų;

1.4. apie galimus įslaptintos informacijos praradimo ar neteisėto atskleidimo atvejus komisija ar darbo grupė informuoja mane, o apie įslaptintos informacijos apsaugos pažeidimus - KAM Specialiąją ekspertų komisiją.

2. Į s a k a u krašto apsaugos sistemos institucijų vadovams netikėtus (kontrolinius) patikrinimus atliekančiai AOTD komisijai ar darbo grupei suteikti visą būtiną patikrinimams atlikti informaciją.

4.8. KRAŠTO APSAUGOS MINISTRO 2007 M. VASARIO 23 D. ĮSAKYMAS NR. V-192 „DĖL ASMENŲ, ATSAKINGŲ UŽ ĮSLAPTINTOS INFORMACIJOS APSAUGĄ, TIPINIO FUNKCIJŲ SĄRAŠO“

Vadovaudamasis Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatymo (Žin., 1998, Nr. 49-1325; 1999, Nr. 64-2069; 2003, Nr. 32-1308, Nr. 91(1)-4106; 2004, Nr. 169-6215) 10 straipsnio 2 dalies 5 punktu, Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) 3 straipsnio 7 dalimi, 12 straipsnio 1 dalimi, 14 straipsniu, Lietuvos Respublikos įstatymo „Dėl Šiaurės Atlanto sutarties šalių susitarimo dėl informacijos saugumo, NATO susitarimo dėl su gynyba susijusių išradimų, dėl kurių paduotos patento paraiškos, abipusės slaptumo apsaugos bei NATO susitarimo dėl techninės informacijos perdavimo gynybos tikslais ratifikavimo“ (Žin., 2004, Nr. 127-4556) 3 straipsniu, Lietuvos Respublikos įstatymo „Dėl Šiaurės Atlanto sutarties šalių susitarimo dėl bendradarbiavimo, susijusio su atomine informacija, ratifikavimo“ (Žin., 2004, Nr. 174-6432) 2 straipsniu ir siekdamas užtikrinti įslaptintos informacijos apsaugą krašto apsaugos sistemoje:

1. T v i r t i n u Asmenų, atsakingų už įslaptintos informacijos apsaugos organizavimą ir vykdymą, tipinį funkcijų sąrašą (pridedama).

2. Į s a k a u krašto apsaugos sistemos institucijų, įstaigų ir jų struktūrinių padalinių, vadovams:

2.1. paskirti atsakingus asmenis, organizuojančius ir vykdančius įslaptintos informacijos administravimą, apsaugą ir kontrolę:

2.1.1. personalo patikimumo srityje, jei institucijoje, įstaigoje ar jos struktūriniame padalinyje yra darbuotojų, turinčių teisę dirbti ar susipažinti su įslaptinta informacija;

2.1.2. informacijos administravimo srityje, jei institucijoje, įstaigoje ar jos struktūriniame padalinyje yra administruojama įslaptinta informacija;

2.1.3 įslaptintos informacijos fizinės apsaugos srityje, jei institucijoje, įstaigoje ar jos struktūriniame padalinyje dirbama su įslaptinta informacija ar ji saugoma;

2.1.4. įslaptintų sandorių saugumo srityje, institucijose ir įstaigose, kurioms pavedama vykdyti pirkimus, vykdant įslaptintą sandorį, susijusį su įstatymų nustatyta valstybės ar tarnybos paslaptimi, vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) 7 skirsniu;

2.1.5. automatizuotų duomenų apdorojimo (toliau – ADA) sistemų ir tinklų apsaugos srityje, jei institucijoje, įstaigoje ar jos struktūriniame padalinyje yra įdiegtos ADA sistemos ir tinklai;

2.2. paskirti institucijoje, įstaigoje ar struktūriniame padalinyje kontrolės pareigūnus, jei administruojama NATO, Europos Sąjungos Lietuvai perduota įslaptinta informacija, žymima slaptumo žyma VISIŠKAI SLAPTAI;

2.3. paskirti institucijoje, įstaigoje ar struktūriniame padalinyje kontrolės pareigūnus, jei administruojama ATOMAL informacija;

2.4. užtikrinti, kad iki 2007 m. liepos 2 d. asmenų, atsakingų už įslaptintos informacijos administravimą, apsaugą ir kontrolę (išskyrus vykdančių funkcijas įslaptintų sandorių saugumo srityje), pareigybių aprašymai ar pareiginiai nuostatai būtų papildyti patvirtintame sąraše nustatytomis funkcijomis.

3. P a v e d u:

3.1. Krašto apsaugos ministerijos Administracijos departamentui iki 2007 m. kovo 30 d. organizuoti seminarą dėl asmenų, atsakingų už įslaptintos informacijos apsaugos organizavimą ir vykdymą, paskyrimo struktūriniuose padaliniuose;

3.2. Krašto apsaugos ministerijos valstybės sekretoriui kontroliuoti, kaip vykdomas šis įsakymas.

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2007 m. vasario 23 d.
įsakymu Nr. V-192

ASMENŲ, ATSAKINGŲ UŽ ĮSLAPTINTOS INFORMACIJOS APSAUGĄ, TIPINIS FUNKCIJŲ SĄRAŠAS

I. BENDROSIOS NUOSTATOS

1. Asmenų, atsakingų už įslaptintos informacijos apsaugą (toliau – Atsakingųjų asmenų), tipinis funkcijų sąrašas (toliau – Funkcijų sąrašas) nustato institucijų, įstaigų ar jų struktūrinių padalinių atsakingųjų asmenų funkcijas, organizuojant ir vykdant įslaptintos informacijos administravimą, apsaugą ir kontrolę.

2. Funkcijų sąrašu privalo vadovautis krašto apsaugos sistemos institucijos, įstaigos ir jų struktūriniai padaliniai, kuriuose dirbama su įslaptinta informacija ar tokia informacija saugoma.

3. Šiame Funkcijų sąraše vartojamos sąvokos:

3.1. NATO VS kontrolės pareigūnas (angl. *COSMIC Control Officer*) – Šiaurės Atlanto Sutarties Organizacijos (toliau – NATO) Lietuvai perduotos įslaptintos informacijos, žymimos slaptumo žyma VISIŠKAI SLAPTAI (angl. *COSMIC TOP SECRET*), administravimą, apsaugą ir kontrolę vykdantis asmuo.

3.2. NATO VS kontrolės pareigūną pavaduojantis asmuo (angl. *Alternate COSMIC Control Officer*) – nesant NATO VS kontrolės pareigūno, jo funkcijas vykdantis asmuo.

3.3. ES VS kontrolės pareigūnas (angl. *EU TOP SECRET Control Officer*) –

Europos Sąjungos (toliau – ES) Lietuvai perduotos įslaptintos informacijos, žymimos slaptumo žyma VISIŠKAI SLAPTAI (angl. *TRES SECRET UE/EU TOP SECRET*), administravimą, apsaugą ir kontrolę vykdantis asmuo.

3.4. ES VS kontrolės pareigūną pavaduojantis asmuo (angl. *Alternate EU TOP SECRET Control Office*) – nesant ES VS kontrolės pareigūno, jo funkcijas vykdantis asmuo.

3.5. atominė informacija (ATOMAL), Jungtinių Amerikos Valstijų Vyriausybės teikiama pagal Šiaurės Atlanto Sutarties Šalių susitarimą dėl bendradarbiavimo, susijusio su atomine informacija – tai informacija, Jungtinių Amerikos Valstijų Vyriausybės pažymėta kaip „Riboto naudojimo duomenys“ (*Restricted Data*) arba „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*).

3.6. ATOMAL kontrolės pareigūnas (angl. *ATOMAL Control Officer*) – ATOMAL informacijos administravimą, apsaugą ir kontrolę vykdantis asmuo.

3.7. ATOMAL kontrolės pareigūną pavaduojantis asmuo (angl. *Alternate ATOMAL Control Officer*) – nesant ATOMAL kontrolės pareigūno, jo funkcijas vykdantis asmuo.

3.8. Kitos šiame Funkcijų sąraše vartojamos sąvokos atitinka Valstybės ir tarnybos paslapčių įstatyme (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) ir Šiaurės Atlanto Sutarties Šalių susitarime dėl bendradarbiavimo, susijusio su atomine informacija (Žin., 2004, Nr. 174-6436), vartojamas sąvokas.

4. Funkcijų sąrašas parengtas vadovaujantis Valstybės ir tarnybos paslapčių įstatymu, Šiaurės Atlanto Sutarties Šalių susitarimu dėl informacijos saugumo (Žin., 2004, Nr. 127-4558), Šiaurės Atlanto Sutarties Šalių susitarimu dėl bendradarbiavimo, susijusio su atomine informacija (ATOMAL), Europos Sąjungos Tarybos 2001 m. kovo 19 d. sprendimu Nr. 264 „Dėl Tarybos saugumo nuostatų“ ir kitais teisės aktais.

II. ATSAKINGŲJŲ ASMENŲ PASKYRIMAS

5. Įslaptintos informacijos apsaugos organizavimą ir vykdymo funkcijas atsakingiesiems asmenims paskirsto ir pavaduojančius asmenis paskiria institucijos, įstaigos ar jos struktūrinio padalinio vadovas arba jo įgaliotas asmuo.

6. Atsižvelgiant į atliekamo darbo apimtį, Atsakingųjų asmenų funkcijos gali būti paskirstomos keliems asmenims arba priskiriamos vienam asmeniui.

7. NATO VS kontrolės pareigūno, ATOMAL kontrolės pareigūno ir ES VS kontrolės pareigūno funkcijos, atsižvelgiant į atliekamo darbo apimtį, gali būti priskiriamos vienai pareigybei. Vieno kontrolės pareigūno funkcijos negali būti paskirstomos kelioms pareigybėms.

8. Pareigybių kvalifikaciniai reikalavimai rengiami vadovaujantis krašto apsaugos ministro 2003 m. rugsėjo 17 d. įsakymu Nr. V-1011 patvirtintų Pareiginių nuostatų rengimo rekomendacijų, 2005 m. birželio 13 d. įsakymu Nr. V-737 patvirtinto Krašto apsaugos sistemos karinių specialybių sąrašo, 2005 m. vasario 28 d. įsakymu Nr. V-223 patvirtinto Leidimų dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimų išdavimo ir apskaitos organizavimo krašto apsaugos sistemoje tvarkos aprašo bei kitų teisės aktų reikalavimais ir įtraukiami į institucijos, įstaigos ar jos struktūrinio padalinio pareigybių ap-

rašymus ar pareiginius nuostatus.

9. Atsižvelgiant į darbo krūvį pareigybėms gali būti priskirtos ir kitos nesietinos su šiomis pareigomis funkcijos.

III. ATSAKINGŲJŲ ASMENŲ FUNKCIJOS

10. Valstybės ir tarnybos paslapčių įstatyme nustatytos Atsakingųjų asmenų funkcijos:

10.1. personalo patikimumo srityje turi būti vykdomos institucijoje, įstaigoje ar jos struktūriniame padalinyje, kuriame yra darbuotojų, turinčių teisę dirbti ar susipažinti su įslaptinta informacija;

10.2. informacijos administravimo srityje turi būti vykdomos institucijoje, įstaigoje ar jos struktūriniame padalinyje, kuriame yra administruojama įslaptinta informacija;

10.3. vykdant įslaptintos informacijos fizinę apsaugą turi būti atliekamos institucijoje, įstaigoje ar jos struktūriniame padalinyje, kuriame dirbama su įslaptinta informacija ar saugoma įslaptinta informacija;

10.4. sudarant ir vykdant įslaptintus sandorius turi būti vykdomos institucijose ir įstaigose, kurioms pavedama vykdyti pirkimus, susijusius su įstatymų nustatyta valstybės ar tarnybos paslaptimi, vadovaujantis krašto apsaugos ministro 2006 m. rugsėjo 15 d. įsakymu Nr. V-918 patvirtintu Įsigijimų, susijusių su valstybės ar tarnybos paslaptimi, organizavimo krašto apsaugos sistemoje tvarkos aprašu.

10.5. organizuojant automatizuotų duomenų apdorojimo sistemų ir tinklų apsaugą turi būti vykdomos institucijose, įstaigose ir jų struktūriniuose padaliniuose, kuriuose yra įdiegtos automatizuotų duomenų apdorojimo sistemos ir tinklai.

11. Subregistratūroje, antrinėse subregistratūrose ir kontrolės punktuose, kuriuose administruojama (numatoma administruoti) NATO Lietuvai perduota įslaptinta informacija, žymima slaptumo žyma VISIŠKAI SLAPTAI, turi būti paskirtas NATO VS kontrolės pareigūnas.

12. NATO VS kontrolės pareigūno funkcijos:

12.1. užtikrina, kad teritorijose ir patalpose, kuriose dirbama su NATO Lietuvai perduota įslaptinta informacija, žymima slaptumo žyma VISIŠKAI SLAPTAI, ar kuriose ji saugoma, būtų įdiegtos ir tinkamai veiktų reikiamos fizinės apsaugos priemonės;

12.2. vykdo NATO Lietuvai perduotos įslaptintos informacijos, žymimos slaptumo žyma VISIŠKAI SLAPTAI, apskaitą, kontroliuoja jos apyvartą ir tvarko jos registraciją;

12.3. atrenka NATO Lietuvai perduotą įslaptintą informaciją, žymimą slaptumo žyma VISIŠKAI SLAPTAI, naikinti ir organizuoja jos sunaikinimą;

12.4. surenka ir nuolat atnaujina pavaldžių antrinių subregistratūrų ar kontrolės punktų NATO VS kontrolės pareigūnų parašų pavyzdžius;

12.5. paskirsto NATO Lietuvai perduotą įslaptintą informaciją, žymimą slaptumo žyma VISIŠKAI SLAPTAI, vykdytojams, antrinėms registratūroms ar kontrolės punktams;

12.6. atlieka NATO Lietuvai perduotos įslaptintos informacijos, žymimos slaptumo žyma VISIŠKAI SLAPTAI, patikrinimą.

13. ATOMAL centrinėje registratūroje turi būti paskirtas ATOMAL kontrolės pareigūnas.

14. ATOMAL kontrolės pareigūno funkcijos:

14.1. užtikrina, kad teritorijose ir patalpose, kuriose dirbama su ATOMAL informacija ar kuriose ji saugoma, būtų įdiegtos ir tinkamai veiktų reikiamos fizinės apsaugos priemonės;

14.2. vykdo ATOMAL informacijos apskaitą, kontroliuoja jos apyvartą ir tvarko jos registraciją;

14.3. perduoda ATOMAL informaciją vykdytojams;

14.4. organizuoja ATOMAL informacijos apsaugos būklės patikrinimus.

15. Subregistratūroje, antrinėse subregistratūrose ir kontrolės punktuose, kuriuose administruojama (numatoma administruoti) ES Lietuvai perduota įslaptinta informacija, žymima slaptumo žyma VISIŠKAI SLAPTAI, turi būti paskirtas ES VS kontrolės pareigūnas.

16. ES VS kontrolės pareigūno funkcijos:

16.1. užtikrina, kad teritorijose ir patalpose, kuriose dirbama su ES Lietuvai perduota įslaptinta informacija, žymima slaptumo žyma VISIŠKAI SLAPTAI, ar kuriose ji saugoma, būtų įdiegtos ir tinkamai veiktų reikiamos fizinės apsaugos priemonės;

16.2. vykdo ES Lietuvai perduotos įslaptintos informacijos, žymimos slaptumo žyma VISIŠKAI SLAPTAI, apskaitą, kontroliuoja jos apyvartą ir tvarko jos registraciją;

16.3. atrenka ES Lietuvai perduotą įslaptintą informaciją, žymimą slaptumo žyma VISIŠKAI SLAPTAI, naikinti ir organizuoja jos sunaikinimą;

16.4. surenka ir nuolat atnaujina pavaldžių antrinių subregistratūrų ar kontrolės punktų ES VS kontrolės pareigūnų parašų pavyzdžius;

16.5. paskirsto ES Lietuvai perduotą įslaptintą informaciją, žymimą slaptumo žyma VISIŠKAI SLAPTAI, vykdytojams, antrinėms registratūroms ar kontrolės punktams;

16.6. atlieka ES Lietuvai perduotos įslaptintos informacijos, žymimos slaptumo žyma VISIŠKAI SLAPTAI, patikrinimą.

IV. BAIGIAMOSIOS NUOSTATOS

17. Funkcijų sąrašo keitimą gali inicijuoti Krašto apsaugos ministerijos Administracijos departamentas ir Gynybos štabo J2.

18. Šį Funkcijų sąrašą tvirtina ir jo keitimo teisę turi krašto apsaugos ministras.

4.9. KRAŠTO APSAUGOS MINISTRO 2007 M. LAPKRIČIO 10 D. ĮSAKYMAS NR. V-1109 „DĖL REKOMENDACIJŲ ĮSLAPTINTOS INFORMACIJOS EVAKUACIJOS ARBA SUNAIKINIMO PLANUI PARENGTI PATVIRTINIMO“

Vadovaudamasis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) 26 straipsniu:

1. T v i r t i n u Rekomendacijas įslaptintos informacijos evakuacijos arba sunaikinimo planui parengti (pridedama).

2. N u r o d a u krašto apsaugos sistemos institucijų, įstaigų ir jų padalinių, kuriuose administruojama įslaptinta informacija, vadovams, vadovaujantis 1 punktu patvirtintomis rekomendacijomis, parengti (patikslinti) ir patvirtinti:

2.1. Įslaptintos informacijos evakuacijos arba sunaikinimo planą;

2.2. Įslaptintos informacijos evakuacijos ar sunaikinimo prioritetų sąrašą.

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2007 m. lapkričio 10 d.
įsakymu Nr. V-1109

REKOMENDACIJOS ĮSLAPTINTOS INFORMACIJOS EVAKUACIJOS ARBA SUNAIKINIMO PLANUI PARENGTI

I. BENDROSIOS NUOSTATOS

1. Rekomendacijos įslaptintos informacijos evakuacijos arba sunaikinimo planui parengti (toliau – rekomendacijos) nustato įslaptintos informacijos, kuria disponuoja krašto apsaugos sistemos institucijos, įstaigos ir jų padaliniai (toliau – institucijos), evakuacijos arba sunaikinimo karo padėties ar ekstremalių situacijų atveju tikslą, objektą, priežastis, vykdymo ir planų derinimo procedūras.

2. Rekomendacijos netaikomos rengiant kriptografinių priemonių evakuacijos arba sunaikinimo planus.

3. Šiose rekomendacijose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) vartojamas sąvokas.

4. Rekomendacijos parengtos vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu, Šiaurės Atlanto Sutarties šalių susitarimu

dėl informacijos saugumo (Žin., 2004, Nr. 127-4558), Europos Sąjungos Tarybos 2001 m. kovo 19 d. sprendimu Nr. 264 „Dėl Tarybos saugumo nuostatų“ (2001/264/EB) ir kitais teisės aktais.

II. TIKSLAS, OBJEKTAS IR VYKDYMO PRIEŽASTYS

5. Įslaptintos informacijos evakuacijos arba sunaikinimo tikslas yra išvengti galimybės prarasti ar neteisėtai atskleisti įslaptintą informaciją, kuria disponuoja institucijos.

6. Įslaptintos informacijos evakuacijos arba sunaikinimo objektas (toliau – objektas) – institucijų, įstaigų ir jų padalinių administruojama įslaptinta informacija.

7. Objektai evakuojami, kai kyla grėsmė prarasti ar neteisėtai atskleisti įslaptintą informaciją, karo padėties, terorizmo grėsmės, radioaktyviojo ar cheminio užteršimo, inžinerinių tinklų avarijų, gaisro ir kitų ekstremalių situacijų atvejais, kai nėra galimybės papildomomis informacijos apsaugos priemonėmis sumažinti įslaptintos informacijos praradimo ar atskleidimo riziką.

8. Objektai naikinami, kai iškyla atskleidimo ar praradimo grėsmė ir kai nėra galimybės jų evakuoti.

III. REKOMENDACIJOS PLANUI PARENGTI

9. Įslaptintos informacijos evakuacijos arba sunaikinimo planą (toliau – planas) turi parengti kiekviena institucija, kuri administruoja įslaptintą informaciją.

10. Planus rengia, prireikus juos keičia, derina ir teikia tvirtinti institucijos vadovo paskirti asmenys ar padaliniai. Parengtas planas derinamas su jame nurodytais atsakingais už plane nustatytų funkcijų vykdymą asmenimis ar institucijos padaliniais.

11. Planuose pareigybėms, institucijos padaliniams ar, iš anksto suderinus, kitoms institucijoms turi būti paskirstytos sprendimo priėmimo, vadovavimo evakuacijos procesui, objektų paruošimo gabenti, gabenimo, naikinimo ir kitos būtinos funkcijos, numatytos priemonės joms atlikti.

12. Planas tvirtinamas institucijos vadovo tvarkomuoju dokumentu.

13. Sprendimą dėl įslaptintos informacijos evakuacijos (evakavimo vietų, evakuotos informacijos saugojimo) arba sunaikinimo priima institucijų vadovai, remdamiesi turima informacija apie 7 ir 8 punktuose išvardytas aplinkybes. Vadovauti evakuacijos ir naikinimo procesui skiriami už įslaptintos informacijos apsaugą atsakingi arba kiti asmenys. Objektų gabenimo maršrutas, gabenimo būdas ir priemonės turi būti parenkamos taip, kad atsitiktiniai asmenys negalėtų nustatyti, jog gabenama įslaptinta informacija.

14. Objektai gabenti paruošiami sudedant juos į tam tikslui iš anksto paruoštus ir saugyklose laikomus konteinerius pagal Įslaptintos informacijos evakuacijos ar sunaikinimo prioritetų sąrašą (toliau – sąrašas). Objektai sąraše išdėstomi grupėmis eilės tvarka taip, kad pirmiausia būtų numatyta evakuoti arba naikinti naujausią aukštesnę slaptumo žymą turinčią informaciją. Į sąrašą įrašyti objektai pažymimi žyma, nurodančią evakavimo arba sunaikinimo eilę. Sąrašą rengia, kasmet arba prireikus tikslina, institucijos vadovui tvirtinti pateikia,

objektus pažymi, evakuacijos metu objektus į konteinerius pagal sąrašą sudeda, juos užrakina ir antspauduoja už įslaptintos informacijos administravimą atsakingi arba kiti vadovo paskirti asmenys.

15. Objektus konteineriuose turi gabenti kariniai kurjeriai arba institucijos vadovo paskirti asmenys (padaliniai).

16. Objektams naikinti iš anksto paruošiama naudoti arba numatoma įranga ar priemonės, kuriomis informacija būtų sunaikinta taip, kad nebūtų įmanoma atkurti viso ar dalies jos turinio. Informacija naikinama sąraše numatyta eilės tvarka, o ją naikina už įslaptintos informacijos administravimą atsakingi arba kiti vadovo paskirti asmenys.

IV. BAIGIAMOSIOS NUOSTATOS

17. Šios rekomendacijos pildomos ir keičiamos Lietuvos Respublikos krašto apsaugos ministro įsakymu.

4.10. KRAŠTO APSAUGOS MINISTRO 2008 M. RUGSĖJO 4 D. ĮSAKYMAS NR. V-839 „DĖL PATALPŲ, SEIFŲ IR METALINIŲ SPINTŲ RAKTŲ, KODINIŲ UŽRAKTŲ IR APSAUGOS SISTEMŲ SKAIČIŲ KOMBINACIJŲ APSAUGOS ORGANIZAVIMO, SKAIČIŲ KOMBINACIJŲ KEITIMO IR PATALPŲ ANTSPAUDAVIMO TAISYKLIŲ PATVIRTINIMO“

Vadovaudamasis Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatymo (Žin., 1998, Nr. 49-1325; 1999, Nr. 64-2069; 2003, Nr. 32-1308, Nr. 91(1)-4106; 2004, Nr. 169-6215) 10 straipsnio 2 dalies 5 punktu ir siekdamas įgyvendinti Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) 30 straipsnio 1 dalies ir 4 dalies 6 punkto nuostatas:

1. T v i r t i n u Patalpų, seifų ir metalinių spintų raktų, kodinių užraktų ir apsaugos sistemų skaičių kombinacijų apsaugos organizavimo, skaičių kombinacijų keitimo ir patalpų antspaudavimo taisykles (toliau – Taisyklės) (pridedama).

2. Į s a k a u krašto apsaugos sistemos institucijų, įstaigų ir struktūrinių padalinių vadovams vadovaujantis Taisyklėmis nustatyti patalpų, seifų ir metalinių spintų raktų, kodinių užraktų, taip pat apsaugos sistemų skaičių kombinacijų apsaugos organizavimo, skaičių kombinacijų keitimo ir patalpų antspaudavimo procedūras pastatuose ar patalpose, už kurias jie atsakingi.

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2008 m. rugsėjo 4 d.
įsakymu Nr. V-839

PATALPŲ, SEIFŲ IR METALINIŲ SPINTŲ RAKTŲ, KODINIŲ UŽRAKTŲ IR APSAUGOS SISTEMŲ SKAIČIŲ KOMBINACIJŲ APSAUGOS ORGANIZAVIMO, SKAIČIŲ KOMBINACIJŲ KEITIMO IR PATALPŲ ANTSPAUDAVIMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Patalpų, seifų ir metalinių spintų raktų, kodinių užraktų ir apsaugos sistemų skaičių kombinacijų apsaugos organizavimo, skaičių kombinacijų keitimo ir patalpų antspaudavimo taisyklės (toliau – Taisyklės) nustato patalpų, kurios priskiriamos administracinei, I ir II klasės saugumo zonai, seifų ir metalinių spintų, kuriose saugoma įslaptinta informacija, raktų išdavimo, saugojimo ir apskaitos, kodinių užraktų ir apsaugos nuo įsilaužimo signalizacijos skaičių kombinacijų sudarymo, apsaugos ir keitimo, patalpų antspaudavimo procedūras.

2. Taisyklėse vartojamos sąvokos atitinka Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) vartojamas sąvokas.

3. Taisyklės parengtos vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29), Šiaurės Atlanto Sutarties šalių susitarimu dėl informacijos saugumo (Žin., 2004, Nr. 127-4558), Europos Sąjungos Tarybos 2001 m. kovo 19 d. sprendimu Nr. 264 „Dėl Tarybos saugumo nuostatų“ ir kitais teisės aktais.

II. PATALPŲ, SEIFŲ IR METALINIŲ SPINTŲ RAKTŲ IŠDAVIMAS, SAUGOJIMAS IR APSKAITA

4. Raktai nuo spynų, įrengtų duryse į saugumo zonoje esančias patalpas, taip pat seifų ir metalinių spintų, kuriose saugoma įslaptinta informacija, duryse, darbuotojams išduodami tik jiems pasirašius apskaitos žurnale. Apskaitos žurnale privalo būti nurodyti patalpos durų, seifo ar metalinės spintos identifikavimo numeriai, išdavimo data, asmens, kuriam išduoti raktai, vardas ir pavardė, pareigos.

5. Raktai nuo spynų, įrengtų duryse į I klasės saugumo zonos patalpas, taip pat seifų ir metalinių spintų, kuriuose saugoma įslaptinta informacija, žymima slaptumo žymomis „Konfidencialiai“ ir aukštesnėmis, negali būti išnešami už administracinės saugumo zonos ribų. Darbo dienos pabaigoje jie užrakinami I ar II klasės saugumo zonoje esančiuose seifuose (spintose) su kodinėmis spynomis arba pasirašytinai perduodami apsaugos darbuotojams antspauduotose raktinėse. Raktai nuo spynų, įrengtų duryse į administracinės, II klasės saugumo

zonos patalpas, taip pat seifų ir metalinių spintų, kuriuose saugoma įslaptinta informacija, žymima slaptumo žymomis „Riboto naudojimo“, gali būti išnešami, tačiau jie negali turėti jokių identifikavimo žymų.

6. Atsarginių raktų komplektus privalo saugoti, vadovo paskirtas atsakingas asmuo (toliau – atsakingas asmuo). Jų išdavimo priežastys registruojamos apskaitos žurnale. Atsarginiai raktai saugomi antspauduotuose konteineriuose ar seife. Konteinerius antspauduoja asmenys, kurie atsako už patalpoje, seife ir metalinėje spintoje saugomą įslaptintą informaciją.

7. I ir II saugumo zonų patalpų, seifų ir metalinių spintų atsarginiai raktai išduodami tik atsakingo už įslaptintos informacijos apsaugos reikalavimų vykdymą institucijos, įstaigos ar struktūrinio padalinio vadovo arba jo įgalioto asmens sprendimu. Atsakingas asmuo šių raktų komplektus tikrina ne rečiau kaip kas 3 mėnesiai. Tikrinamas raktų kiekis, konteinerių antspaudai ir pasirinktinai raktų tinkamumas užraktams.

Administracinės saugumo zonos patalpų, seifų ir metalinių spintų atsarginiai raktai išduodami padalinio vadovo sprendimu.

8. Kai nėra asmens, kuriam buvo patikėta įslaptinta informacija, atidaryti patalpas, seifus ar metalines spintas galima tik atsakingo už įslaptintos informacijos apsaugos reikalavimų vykdymą institucijos, įstaigos ar struktūrinio padalinio vadovo arba jo įgalioto asmens sprendimu. Atidarymo faktas ir atsarginių raktų panaudojimas registruojami apskaitos žurnale. Asmuo, susipažinęs su skaičių kombinacija, pasirašo registre.

III. SKAIČIŲ KOMBINACIJŲ SUDARYMAS, APSAUGA IR KEITIMAS

9. Patalpų, seifų ir metalinių spintų kodinių užraktų skaičių kombinacijas sudaro ir keičia darbuotojai, atsakingi už patalpoje, seife ar metalinėje spintoje saugomą įslaptintą informaciją.

10. Apsaugos nuo įsilaužimo signalizacijos administratoriaus, instaliuotojo kodus (skaičių kombinacijas), leidžiančius įjungti ir išjungti apsaugos sistemą sudaro ir keičia darbuotojai, atsakingi už šių sistemų priežiūrą.

11. Apsaugos nuo įsilaužimo signalizacijos naudotojų kodus sudaro šių sistemų naudotojai. Naudotojų kodams netaikomi šių Taisyklių 14 ir 15 punktuose nustatyti reikalavimai. Kodą naudojančiam darbuotojui, išėjus iš darbo ar perėjus į kitas, nesusijusias su tos patalpos naudojimu, pareigas, kodas panaikinamas.

12. Skaičių kombinacijoms sudaryti negalima naudoti derinių, kurie būtų susiję su informacija apie vartotoją, pvz., gimimo datų, telefono numerių ar kitų nuspėjamų skaičių sekos**.**

13. Kiekvienas darbuotojas privalo žinoti (įsiminti) apsaugos nuo įsilaužimo signalizacijos, patalpų, seifų ar metalinių spintų, už kurias jis yra atsakingas, kodinių užraktų skaičių kombinacijas.

14. Skaičių kombinacijos saugomos antspauduotuose vokuose. Vokus antspauduoja įslaptintą informaciją administruojantis padalinys. Skaičių kombinaciją pakeitęs asmuo ant voko užrašo apsaugos nuo įsilaužimo signalizacijos, patalpos durų, seifo ar metalinės spintos identifikavimo numerį, skaičių kom-

binacijos keitimo datą, kito numatomo keitimo datą, savo pareigas, vardą, pavardę ir pasirašo. Vadovaujantis įslaptinamos informacijos, susijusios su krašto apsaugos sistemos veikla, detaliuoju sąrašu, ant voko užrašoma slaptumo žyma su nuoroda „sunaikinti pakeitus skaičių kombinaciją“ ir vokas registruojamas laikino saugojimo įslaptintų administravimo dokumentų registre. Vokui su skaičių kombinacija suteikiama slaptumo žyma pagal aukščiausią informacijos, saugomos seife ar metalinėje spintoje, slaptumo žymą.

15. Skaičių kombinacijų fizinei apsaugai taikomos apsaugos priemonės negali būti mažesnės nei reikalavimai, taikomi tos slaptumo žymos informacijai, kuriai apsaugoti jos skirtos.

16. Skaičių kombinacijos keičiamos:

16.1. gavus naują įrangą;

16.2. patalpų, seifų ir metalinių spintų kodinių užraktų – periodiškai, kartą per 6 mėnesius;

16.3. apsaugos sistemų skaičių kombinacijos, leidžiančios įjungti ir išjungti apsaugos sistemas – kartą per metus;

16.4. jei skaičių kombinaciją sužinojo ar įtariama, kad galėjo sužinoti, pašalinis asmuo;

16.5. perdavus seifą ar metalinę spintą su kodiniu užraktu kitam darbuotojui;

16.6. jei darbuotojas, žinantis patalpų kodinių užraktų skaičių kombinaciją, išeina iš darbo ar pereina į kitas, nesusijusias su tos patalpos naudojimu, pareigas.

IV. PATALPŲ ANTSPAUDAVIMAS

17. Patalpos, kuriose neįrengta apsaugos nuo įsilaužimo signalizacija, seifai ir metalinės spintos, gali būti antspauduojamos institucijos ar jos struktūrinio padalinio vadovo nustatyta tvarka.

18. Spaudai darbuotojams išduodami pasirašytinai.

4.11. KRAŠTO APSAUGOS MINISTRO 2008 M. LAPKRIČIO 20 D. ĮSAKYMAS NR. V-1133 „INFORMAVIMO APIE KRAŠTO APSAUGOS SISTEMOS PROFESINĖS KARO TARNYBOS KARIŲ, VALSTYBĖS TARNAUTOJŲ IR ASMENŲ, DIRBANČIŲ PAGAL DARBO SUTARTIS, IŠVYKAS Į UŽSIENĮ TVARKOS APRAŠO“ *

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2008 m. lapkričio 20 d.
įsakymu Nr. V-1133

INFORMAVIMO APIE KRAŠTO APSAUGOS SISTEMOS PROFESINĖS KARO TARNYBOS KARIŲ, VALSTYBĖS TARNAUTOJŲ IR ASMENŲ, DIRBANČIŲ PAGAL DARBO SUTARTIS, IŠVYKAS Į UŽSIENĮ TVARKOS APRAŠAS

I. BENDROSIOS NUOSTATOS

1. Informavimo apie krašto apsaugos sistemos profesinės karo tarnybos karių, valstybės tarnautojų ir asmenų, dirbančių pagal darbo sutartis, išvykas į užsienį tvarkos aprašas (toliau – aprašas) nustato profesinės karo tarnybos karių (toliau – kariai), valstybės tarnautojų (toliau – tarnautojai) ir asmenų, dirbančių pagal darbo sutartis (toliau – darbuotojai), pranešimo apie išvykas į užsienio valstybes ne tarnybos tikslais tvarką.

2. Šis aprašas netaikomas kariams, tarnautojams ir darbuotojams, į užsienio valstybes vykstantiems tarnybos tikslais (mokymosi, kvalifikacijos kėlimo, gydymosi ir kt.) krašto apsaugos sistemos siuntimu.

II. INFORMAVIMAS APIE IŠVYKĄ Į UŽSIENĮ

3. Kariai, tarnautojai ir darbuotojai, ne tarnybos tikslais vykstantys į užsienio valstybes, neįeinančias į NATO, ES ir Šengeno erdvės valstybių sąrašą, prieš 14 kalendorinių dienų apie išvyką privalo informuoti struktūrinio padalinio vadą ir Antrąjį operatyvinių tarnybų departamentą prie KAM (toliau – AOTD), užpildydami nustatytos formos anketą (1 priedas). Anketos kopija išsiunčiama AOTD elektroniniu paštu KZT@aotd.kam.lt arba faksu (8 5) 273 8972.

4. Artimųjų mirties, ligos arba kitais ypatingais atvejais, kai neįmanoma apie išvyką informuoti aprašo 3 punkte nurodytu būdu, vykstantysis prieš išvykdamas informuoja AOTD arba žodžiu savo tiesioginį vadą (vadovą), kuris nedelsdamas praneša AOTD aprašo 5 punkte nurodytais telefono numeriais.

* **Pastaba:** Į rinkinį šis Krašto apsaugos ministro įsakymas ir Aprašo priedai neįtraukti.

5. Grįžę iš aprašo 3 punkte nurodytų valstybių asmenys per 5 kalendorines dienas privalo užpildyti nustatytos formos anketą (2 priedas ,,Kelionės į užsienį klausimynas“). Apie šios anketos užpildymą asmuo privalo nedelsdamas informuoti AOTD KATT tel. 202 09, TEO tel. (8 5) 273 8972, (8 5) 264 1292 ir perduoti šią anketą į dalinį atvykusiam AOTD pareigūnui. Jei asmens atostogos po grįžimo iš šių užsienio valstybių dienos trunka ilgiau nei 5 kalendorines dienas, asmuo anketą užpildo ir pateikia pirmąją po atostogų darbo dieną.

6. Kariai, tarnautojai ir darbuotojai, ne tarnybos tikslais vykę į užsienio valstybes (įskaitant įeinančias į NATO, ES ir Šengeno erdvės valstybių sąrašą) ir patyrę incidentų dėl saugumo, neplanuotų susitikimų su įtartinais asmenimis ir kitų išskirtinių, su asmeniniu ar įslaptintos informacijos saugumu susijusių įvykių, per 5 punkte nurodytą terminą privalo užpildyti nustatytos formos anketą (2 priedas „Kelionės į užsienį klausimynas“) ir pateikti AOTD aprašo 5 punkte nurodytu būdu.

III. BAIGIAMOSIOS NUOSTATOS

7. Kariai, tarnautojai ir darbuotojai, pažeidę šio tvarkos aprašo nuostatas, atsako teisės aktų nustatyta tvarka.

4.12. KRAŠTO APSAUGOS MINISTRO 2010 M. VASARIO 10 D. ĮSAKYMAS NR. V-122 „DĖL ELEKTROMAGNETINIO SPINDULIAVIMO ŠALTINIŲ, INFORMACIJOS FIKSAVIMO AR PERDAVIMO ĮRENGINIŲ, ELEKTRONINIŲ LAIKMENŲ NAUDOJIMO“

Vadovaudamasis Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatymo (Žin., 1998, Nr. 49-1325) 3 straipsnio 3 dalimi, krašto ministro 2009 m. spalio 5 d. įsakymo Nr. V-949 „Dėl teisių perdavimo krašto apsaugos viceministrams ir Ministerijos kancleriui“ 1 punktu, siekdamas įgyvendinti Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29) 30 straipsnio 2 dalies 2 punkto ir 31 straipsnio 6 dalies 5 punkto nuostatas ir atsižvelgdamas į Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos 2009 m. gruodžio 3 d. rašte Nr. S-010-4251RN „Dėl asmeninės kompiuterinės įrangos naudojimo darbo vietose“ pateiktus siūlymus:

1. N u s t a t a u, kad:

1.1. į krašto apsaugos sistemos institucijų teritorijas, pastatus ar patalpas, priskirtas I klasės saugumo zonai, draudžiama įnešti pašalinius (su darbo ar tarnybos funkcijų teritorijoje, pastate ar patalpoje vykdymu nesusijusius, ar krašto apsaugos sistemai nepriklausančius ar panaudos pagrindais neperduotus valdyti ar naudoti) elektromagnetinio spinduliavimo šaltinius (buitinius elektros prietaisus, ryšio priemones (radijo imtuvus ir siųstuvus, telefonus), informacinių technologijų pagrindu veikiančius įrenginius ir pan.), kitus informacijos fiksavimo ar perdavimo įrenginius, kurie nėra elektromagnetinio spinduliavimo šaltiniai, elektronines laikmenas;

1.2. į krašto apsaugos sistemos institucijų teritorijas, pastatus ar patalpas, priskirtas II klasės saugumo zonai, draudžiama įnešti krašto apsaugos sistemai nepriklausančius ar panaudos pagrindais neperduotus valdyti ar naudoti informacijos fiksavimo ar perdavimo įrenginius (fotoaparatus, vaizdo kameras, radijo siųstuvus, telefonus ir pan.), elektronines laikmenas;

1.3. draudžiama tarnybinę informaciją apdoroti ar ją saugoti krašto apsaugos sistemai nepriklausančiose ar panaudos pagrindais neperduotose valdyti ar naudoti laikmenose (kino ar fotografijos negatyve, pozityve, standžiajame ar keičiamajame diske, kompaktinėje plokštelėje, lanksčiajame diskelyje, atminties ar magnetinėje kortelėje ir pan.);

1.4. tais atvejais, kai teritorijoje, pastate ar patalpoje, priskirtoje I ar II klasės saugumo zonai, atliekamiems darbams būtina naudoti krašto apsaugos sistemai nepriklausančius ar panaudos pagrindais neperduotus valdyti ar naudoti prietaisus, leidimą tokius prietaisus naudoti suteikia institucijos, struktūrinio padalinio vadovas ar jų įgaliotas asmuo, kuris valdo ar naudoja I ar II klasės saugumo zoną;

1.5. institucijos, struktūrinio padalinio vadovas ar jų įgaliotas asmuo informacijos apsaugai užtikrinti gali nustatyti papildomas, jų valdomas ar naudojamas teritorijas, pastatus ar patalpas, kuriose taikomi 1.1, 1.2 ir 1.4 punktuose nustatyti reikalavimai.

2. Į s a k a u krašto apsaugos sistemos institucijų, įstaigų ir jų padalinių vadovams papildyti įstaigų, struktūrinių padalinių vidaus tvarkos taisykles ar karinių vienetų standartines veiklos procedūras šio įsakymo 1 punkte nustatytais reikalavimais.

4.13. KRAŠTO APSAUGOS MINISTRO 2012 M. LAPKRIČIO 29 D. ĮSAKYMAS NR. V-1332 „DĖL ELEKTRONINIŲ APSAUGOS SISTEMŲ, SUSIJUSIŲ SU TARNYBOS PASLAPTIMI, ĮRENGIMO ORGANIZAVIMO KRAŠTO APSAUGOS SISTEMOJE TVARKOS APRAŠO PATVIRTINIMO“

Vadovaudamasi Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatymo (Žin., 1998, Nr. 49-1325; 1999, Nr. 64-2069; 2003, Nr. 91(1)-4106; 2004, Nr. 169-6215; 2006, Nr. 72-2679; 2008, Nr. 38-1377; 2010, Nr. 63-3099; 2011, Nr. 46-2155, Nr. 86-4151) 10 straipsnio 2 dalies 4 punktu ir 3 dalimi:

1. T v i r t i n u Elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, įrengimo organizavimo krašto apsaugos sistemoje tvarkos aprašą (pridedama).

2. P r i p a ž į s t u netekusiais galios:

2.1. Lietuvos Respublikos krašto apsaugos ministro 2007 m. rugpjūčio 27 d. įsakymą Nr. V-844 „Dėl Elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, projektavimo ir įrengimo darbų bei priežiūros paslaugų įsigijimo krašto apsaugos sistemoje tvarkos aprašo tvirtinimo“;

2.2. Lietuvos Respublikos krašto apsaugos ministro 2008 m. gegužės 23 d. įsakymą Nr. V-464 „Dėl Lietuvos Respublikos krašto apsaugos ministro 2007 m. rugpjūčio 27 d. įsakymo Nr. V-844 „Dėl Elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, projektavimo ir įrengimo darbų bei priežiūros paslaugų įsigijimo krašto apsaugos sistemoje tvarkos aprašo tvirtinimo“ pakeitimo“;

2.3. Lietuvos Respublikos krašto apsaugos ministro 2008 m. gruodžio 23 d. įsakymą Nr. V-1240 „Dėl Lietuvos Respublikos krašto apsaugos ministro 2007 m. rugpjūčio 27 d. įsakymo Nr. V-844 „Dėl Elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, projektavimo ir įrengimo darbų bei priežiūros paslaugų įsigijimo krašto apsaugos sistemoje tvarkos aprašo tvirtinimo“ pakeitimo“;

2.4. Lietuvos Respublikos krašto apsaugos ministro 2009 m. birželio 30 d. įsakymą Nr. V-633 „Dėl Lietuvos Respublikos krašto apsaugos ministro 2007 m. rugpjūčio 27 d. įsakymo Nr. V-844 „Dėl Elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, projektavimo ir įrengimo darbų bei priežiūros paslaugų įsigijimo krašto apsaugos sistemoje tvarkos aprašo tvirtinimo“ pakeitimo“;

2.5. Lietuvos Respublikos krašto apsaugos ministro 2010 m. spalio 27 d. įsakymą Nr. V-1158 „Dėl Lietuvos Respublikos krašto apsaugos ministro 2007 m. rugpjūčio 27 d. įsakymo Nr. V-844 „Dėl Elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, projektavimo ir įrengimo darbų bei priežiūros paslaugų įsigijimo krašto apsaugos sistemoje tvarkos aprašo tvirtinimo“ pakeitimo“;

2.6. Lietuvos Respublikos krašto apsaugos ministro 2011 m. gegužės 18 d. įsakymą Nr. V-575 „Dėl Lietuvos Respublikos krašto apsaugos ministro 2007 m. rugpjūčio 27 d. įsakymo Nr. V-844 „Dėl Elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, projektavimo ir įrengimo darbų bei priežiūros paslaugų įsigijimo krašto apsaugos sistemoje tvarkos aprašo tvirtinimo“ pakeitimo“.

3. N u s t a t a u, kad Infrastruktūros plėtros departamento prie Krašto apsaugos ministerijos direktoriaus vadovaujantis šio įsakymo 2.1 punkte nurodytu įsakymu 2012 m. patvirtintos elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, techninės specifikacijos galioja elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, centralizuotiems pirkimams, o šių techninių specifikacijų pakeitimai turi būti rengiami, derinami ir tvirtinami pagal šio įsakymo 1 punktu patvirtintą tvarkos aprašą

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2012 m. lapkričio 29 d.
įsakymu Nr. V-1332

ELEKTRONINIŲ APSAUGOS SISTEMŲ, SUSIJUSIŲ SU TARNYBOS PASLAPTIMI, ĮRENGIMO ORGANIZAVIMO KRAŠTO APSAUGOS SISTEMOJE TVARKOS APRAŠAS

I. BENDROSIOS NUOSTATOS

1. Elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, įrengimo organizavimo krašto apsaugos sistemoje tvarkos aprašas (toliau – Aprašas) reglamentuoja apsauginės užpuolimo signalizacijos, apsauginės įsilaužimo signalizacijos, elektroninės įeigos kontrolės sistemos, uždarosios vaizdo stebėjimo sistemos (toliau – apsaugos sistemos) įrengimo planavimo, dokumentų rengimo ir darbų organizavimo tvarką, įrengtų apsaugos sistemų priežiūros reikalavimus.

2. Aprašu privalo vadovautis krašto apsaugos sistemos (toliau – KAS) institucijos ir jų padaliniai, dalyvaujantys apsaugos sistemų įrengimo planavimo, dokumentų rengimo, darbų organizavimo ir įrengtų apsaugos sistemų priežiūros veikloje. Aprašas netaikomas Antrajam operatyvinių tarnybų departamentui prie Krašto apsaugos ministerijos (toliau – AOTD), kai dėl AOTD veiklos specifikos iškyla neplanuota būtinybė skubiai įrengti arba rekonstruoti apsaugos sistemas AOTD naudojamose patalpose ar teritorijose.

3. Apsaugos sistemų projektavimo, įrengimo, garantinės priežiūros ir remonto paslaugų arba priežiūros ir remonto paslaugų, pasibaigus garantiniam terminui, pirkimai organizuojami vadovaujantis Pirkimų organizavimo krašto

apsaugos sistemoje tvarkos Aprašu, patvirtintu Lietuvos Respublikos krašto apsaugos ministro 2007 m. liepos 30 d. įsakymu Nr. V-768.

4. Aprašo nuostatos taikomos tik Lietuvos Respublikoje įrengiamoms ir prižiūrimoms apsaugos sistemoms.

5. Apraše vartojamos sąvokos:

Elektroninių apsaugos sistemų įrengimo projektinė užduotis – dokumentas, nusakantis apsaugos sistemų rūšį, išdėstymo ir veikimo pricipus ir skirtas techninėms specifikacijoms rengti.

Objektas – patalpa, pastatas ar teritorija, kurioje numatoma įrengti apsaugos sistemą.

5[1]. Kitos apraše vartojamos sąvokos atitinka Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29), Lietuvos Respublikos viešųjų pirkimų įstatyme (Žin., 1996, Nr. 84-2000; 2006, Nr. 4-102), Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatyme (Žin., 2011, Nr. 85-4135) ir šių įstatymų įgyvendinamuosiuose teisės aktuose vartojamas sąvokas.

II. APSAUGOS SISTEMŲ ĮRENGIMO PLANAVIMAS

6. Bendras apsaugos sistemų įrengimo KAS poreikis, apimantis tiek naujas įrengiamas apsaugos sistemas, tiek išplečiamas, modernizuojamas ar rekonstruojamas jau esamas, numatomas KAS planavimo vadove, metų apimtis nurodant KAS metų investicijų plane.

7. Apsaugos sistemų įrengimo poreikį nustato ir sistemų įrengimo plano projektą (KAS planavimo vadovo priedas Nr. 3, C priedėlis) rengia Lietuvos kariuomenės Logistikos valdyba (toliau – LK LV) pagal iš KAS institucijų ar jų padalinių gautą informaciją apie objektus, kuriuose reikia įrengti, išplėsti, modernizuoti ar rekonstruoti apsaugos sistemas.

8. Planuojant įrengti apsaugos sistemas, turi būti gautos išvados dėl šių sistemų įrengimo darbų pirkimo procedūrų ir (arba) sutarčių vykdymo metu ketinamos panaudoti, perduoti tiekėjams ar sukurti informacijos įslaptinimo pagrįstumo (toliau – išvados dėl informacijos įslaptinimo pagrįstumo):

8.1. dėl išvadų dėl informacijos įslaptinimo pagrįstumo, pirmaisiais ir antraisiais metais KAS (išskyrus Krašto apsaugos ministeriją) valdomuose objektuose planuojant įrengti apsaugos sistemas, į Lietuvos Respublikos krašto apsaugos ministro sudarytą Krašto apsaugos ministerijos specialiąją ekspertų komisiją (toliau – KAM SEK) užpildžiusi kreipimosi formą (priedas) ir surinkusi visus KAM SEK reikalingus pateikti dokumentus ir informaciją, nurodytus Pirkimų organizavimo krašto apsaugos sistemoje tvarkos apraše, kreipiasi LK LV;

8.2. dėl išvadų dėl informacijos įslaptinimo pagrįstumo, Krašto apsaugos ministerijos valdomuose objektuose planuojant įrengti apsaugos sistemas, į KAM SEK, užpildžiusi kreipimosi formą (priedas) ir surinkusi visus KAM SEK reikalingus pateikti dokumentus ir informaciją, nurodytus Pirkimų organizavimo krašto apsaugos sistemoje tvarkos apraše, kreipiasi Lietuvos kariuomenės Karo policija (toliau – LK KP) ir gautas išvadas pateikia LK LV;

8.3. išvadas dėl informacijos, susijusios su AOTD valdomuose objektuose planuojamomis įrengti apsaugos sistemomis, įslaptinimo pagrįstumo teikia

AOTD specialioji ekspertų komisija (toliau – AOTD SEK). AOTD SEK išvadą AOTD pateikia LK LV;

8.4. planuojant jau įrengtų apsaugos sistemų išplėtimą, modernizavimą, rekonstrukciją arba naujų įrengimą, kai apsaugos sistemos prijungiamos prie jau įrengtų ir neketinama keisti jų įslaptinimo lygmens, vadovaujamasi KAM SEK arba AOTD SEK pateiktomis išvadomis dėl įrengtų apsaugos sistemų informacijos įslaptinimo pagrįstumo.

9. LK LV apsaugos sistemų įrengimo plano projektą, KAM SEK ir AOTD SEK išvadas pateikia Krašto apsaugos ministerijos Pajėgumų planavimo departamentui (toliau – PPD). PPD, atsižvelgęs į KAM SEK ar AOTD SEK išvadas, analizuoja apsaugos sistemų įrengimo plano projekte nurodytą apsaugos sistemų įrengimo poreikį ir rengia (tikslina) apsaugos sistemų įrengimo investicinį projektą ir infrastruktūros plėtros investicinius projektus, kuriuose yra numatomas apsaugos sistemų įrengimas. Apsaugos sistemų įrengimo investicinis projektas ir infrastruktūros plėtros investiciniai projektai, kuriuose yra numatomas apsaugos sistemų įrengimas, derinami ir tvirtinami KAS planavimo vadove nustatyta tvarka.

III. APSAUGOS SISTEMOMS ĮRENGTI IR JŲ GARANTINEI PRIEŽIŪRAI VYKDYTI REIKALINGŲ DOKUMENTŲ RENGIMAS

9^{1}. Elektroninių apsaugos sistemų įrengimo projektinę užduotį parengia KAS institucijos ar jos padalinio, kuriame planuojama įrengti apsaugos sistemą, vado (viršininko) įsakymu sudaryta komisija arba įgalioti asmenys.

9^{2}. KAS institucijos, kurioje planuojama įrengti apsaugos sistemą, vado (viršininko) ar jo įgalioto asmens parašu patvirtinta elektroninių apsaugos sistemų įrengimo projektinė užduotis (tvirtinimo žymos, kai tvirtinama parašu, reikalavimai nustatyti Dokumentų rengimo taisyklių, patvirtintų Lietuvos vyriausiojo archyvaro 2011 m. liepos 4 d. įsakymu Nr. V-117 (Žin., 2011, Nr. 88-4229), 33.4 punkte) teikiama PPD. AOTD patvirtinta elektroninių apsaugos sistemų įrengimo projektinė užduotis PPD neteikiama.

9^{3}. Elektroninių apsaugos sistemų įrengimo projektinėje užduotyje turi būti nurodoma:

9^{3}.1. statinio (patalpų), kuriame bus įrengiama apsaugos sistema, pavadinimas, inventorinis ar unikalus numeris, tikslus adresas;

9^{3}.2. pageidaujamos įrengti apsaugos sistemos rūšis (elektroninė užpuolimo ir įsilaužimo apsauginė signalizacija, elektroninė įeigos kontrolės sistema, vaizdo stebėjimo sistema ir t. t.);

9^{3}.3. detalus aprašymas, kaip ir kokia teritorija ar jos ruožai, pastatai ar patalpos (nurodant pastatų ar patalpų numerius, teritorijos ir patalpų saugumo zonas) turi būti apsaugoti;

9^{3}.4. tikslūs saugomos teritorijos ir statinių aukštų planai. Planuose turi būti pažymėti perimetro, statinių, aukštų, patalpų ir t.t. ruožai, būtini apsaugoti apsaugos, vaizdo stebėjimo sistemomis, elektronine įeigos kontrolės sistema kontroliuojami patekimai į teritorijas ar patalpas, esami silpnų srovių komunikacijų kanalai.

10. PPD pagal elektroninių apsaugos sistemų įrengimo projektinę užduotį rengia apsaugos sistemų technines specifikacijas (techninius reikalavimus), ku-

rias, suderinęs su AOTD, tvirtina PPD direktorius. AOTD valdomų objektų apsaugos sistemų technines specifikacijas (techninius reikalavimus) rengia AOTD ir tvirtina AOTD direktorius. Patvirtintų techninių specifikacijų (techninių reikalavimų) kopijas PPD ir AOTD perduoda LK LV.

11. Apsaugos sistemų projektavimo, įrengimo darbų ir garantinės priežiūros paslaugų pirkimams organizuoti technines specifikacijas (techninius reikalavimus), KAM SEK ar AOTD SEK išvadų dėl informacijos įslaptinimo pagrįstumo kopijas ir kitus su pirkimu susijusius dokumentus KAM Įsigijimų departamentui pateikia LK LV. Sudarytų sutarčių kopijas su visais priedais LK LV perduoda Infrastruktūros plėtros departamentui prie KAM (toliau – IPD), kuris kontroliuoja sutartinių įsipareigojimų vykdymą.

12. IPD, įvertinęs parengto apsaugos sistemų įrengimo projekto atitiktį techninėms specifikacijoms (techniniams reikalavimams), teikia jį derinti KAS statinio valdytojui ir (ar) naudotojui ir AOTD.

13. Apsaugos sistemų įrengimo projektą derinantys asmenys informaciją apie pastebėtus trūkumus pateikia IPD. Sprendimus dėl derinant ar rengiant apsaugos sistemų įrengimo projektą iškilusių probleminių klausimų priima krašto apsaugos viceministras resursams, finansams, įsigijimams ir infrastruktūrai, atsižvelgdamas į krašto apsaugos ministro įsakymu sudarytos Infrastruktūros plėtros projektų derinimo komisijos pasiūlymus.

IV. APSAUGOS SISTEMŲ ĮRENGIMO DARBŲ ORGANIZAVIMAS

14. KAS statinių valdytojai ir (arba) naudotojai iki apsaugos sistemų įrengimo darbų pradžios privalo pagal IPD pateiktus sąrašus išduoti leidimus įeiti į objektą apsaugos sistemų įrengimo darbus atliksiančios įmonės darbuotojams ir specialiosios statinio statybos techninės priežiūros vadovui.

15. Apsaugos sistemų įrengimo darbų techninę priežiūrą organizuoja IPD direktoriaus iš IPD specialistų paskirtas specialiosios statinio techninės priežiūros vadovas. Specialiosios statinio techninės priežiūros vadovas, tik įsitikinęs, kad atliktų darbų kokybė atitinka technines specifikacijas (techninius reikalavimus), darbų apimtys atitinka numatytas sutartyje, priima darbus (pasirašo atliktų darbų aktus ir vizuoja PVM sąskaitas faktūras bei pažymas apie atliktų darbų vertę ir išlaidas). Kai apsaugos sistemų įrengimo darbus atlikusi įmonė informuoja IPD apie baigtus darbus, IPD, patikrinęs pateiktą informaciją, nedelsdamas, bet ne vėliau kaip per 3 darbo dienas, raštu apie tai informuoja LK LV.

16. Sprendimai dėl papildomų apsaugos sistemų įrengimo darbų ir sutartyje numatytų darbų dalies atsisakymo priimami vadovaujantis Sprendimų dėl papildomų ir nevykdomų statybos darbų priėmimo krašto apsaugos sistemoje tvarkos aprašu, patvirtintu krašto apsaugos ministro 2011 m. vasario 23 d. įsakymu Nr. V-226.

17. Įmonei atlikus sutartyje numatytus apsaugos sistemų įrengimo darbus, elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, pripažinimas baigtomis įrengti ir tinkamomis naudoti organizuojamas vadovaujantis Statinių pripažinimo baigtais statyti ir elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, pripažinimo baigtomis įrengti ir tinkamomis naudoti krašto apsaugos sistemoje tvarkos aprašu, patvirtintu krašto apsaugos ministro 2010 m.

birželio 15 d. įsakymu Nr. V-644. KAS statinio valdytojas ir (arba) naudotojas pagal LK LV pateiktus elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, pripažinimo baigtomis įrengti ir tinkamomis naudoti komisijos narių sąrašus, iki pradedant apsaugos sistemų pripažinimo baigtomis įrengti ir tinkamomis naudoti procedūras, turi išduoti komisijos nariams leidimus patekti į objektą.

18. IPD per 10 darbo dienų nuo apsaugos sistemų pripažinimo baigtomis įrengti ir tinkamomis naudoti akto pasirašymo dienos:

18.1. surašydamas dokumentų priėmimo perdavimo aktą, perduoda KAS statinio valdytojui ir (ar) naudotojui, o KAM statinių – LK KP, įrengtų apsaugos sistemų techninius dokumentus, instaliavimo kodus ir techninės priežiūros instrukciją, kurioje nurodomi būtini apsaugos sistemos ir jos elementų techninės priežiūros (patikrinimo) darbai (reglamentiniai darbai), jų periodiškumas, išskiriant darbus, atliekamus sistemos naudotojo, ir garantinius darbus, atliekamus sistemos tiekėjo, o pasibaigus garantiniam laikui – parinkto paslaugos teikėjo.

18.2. Statinių statybos, nematerialiojo ir ilgalaikio materialiojo turto vertės įrašymo į apskaitos registrus krašto apsaugos sistemoje tvarkos aprašo, patvirtinto krašto apsaugos ministro 2012 m. rugpjūčio 3 d. įsakymu Nr. V-881, nustatyta tvarka parengia apsaugos sistemų įrengimo vertės perdavimo pažymą ir pateikia ją LK LV.

19. Aprašo 18.2 punkte nurodyto teisės akto nustatyta tvarka LK LV organizuoja įrengtų apsaugos sistemų vertės perdavimą.

20. KAS statinio valdytojas ir (ar) naudotojas apsaugos sistemų įrengimo sutartyje nurodytu laiku privalo pateikti IPD sąrašus atsakingų darbuotojų, kurie turės būti išmokyti eksploatuoti įrengtas apsaugos sistemas, ir užtikrinti jų dalyvavimą mokyme.

V. ĮRENGTŲ APSAUGOS SISTEMŲ PRIEŽIŪRA

21. Įrengtų apsaugos sistemų tiekėjo garantinių įsipareigojimų vykdymą kontroliuoja apsaugos sistemų techninę priežiūrą vykdantis asmuo (LK LV Įgulų aptarnavimo tarnyba arba kitas KAS statinio valdytojas ir (arba) naudotojas).

22. Siekdamas užtikrinti apsaugos sistemų funkcionavimą, likus ne mažiau kaip 6 mėnesiams iki garantinio laiko pabaigos, apsaugos sistemų techninę priežiūrą vykdantis asmuo (LK LV Įgulų aptarnavimo tarnyba arba kitas KAS statinio valdytojas ir (arba) naudotojas) vadovaudamasis Aprašo 3 punkte nurodytu teisės aktu organizuoja techninės priežiūros pasibaigus garantiniam laikui paslaugų ir apsaugos sistemos remonto darbų pirkimą.

23. Technines specifikacijas (techninius reikalavimus) techninės priežiūros paslaugoms pasibaigus garantiniam laikui arba remonto darbams pirkti rengia apsaugos sistemų techninę priežiūrą vykdantis asmuo (LK LV Įgulų aptarnavimo tarnyba arba kitas KAS statinio valdytojas ir (arba) naudotojas) vadovaudamasis Aprašo 3 punkte nurodytu teisės aktu, įrengtų apsaugos sistemų techniniais dokumentais ir techninės priežiūros instrukcija.

Elektroninių apsaugos sistemų, susijusių su tarnybos paslaptimi, įrengimo organizavimo krašto apsaugos sistemoje tvarkos aprašo priedas

(Kreipimosi forma)

_____

(krašto apsaugos sistemos institucijos pavadinimas)

_____

Lietuvos Respublikos krašto apsaugos ministerijos specialiajai ekspertų komisijai

_____ Nr. _____
(data)

KREIPIMASIS DĖL INFORMACIJOS, SUSIJUSIOS SU ELEKTRONINĖMIS APSAUGOS SISTEMOMIS, ĮSLAPTINIMO PAGRĮSTUMO

_____,

(kreipimosi teisinis pagrindas)

prašome Krašto apsaugos ministerijos specialiosios ekspertų komisijos pateikti išvadą dėl

_____

(objekto pavadinimas, adresas, statinį identifikuojantis numeris)

informacijos, naudojamos elektroninių apsaugos sistemų **projektavimo, įrengimo, remonto darbų ir garantinės priežiūros paslaugų įsigijimo ar remonto darbų ir priežiūros paslaugų įsigijimo, pasibaigus garantiniam terminui**, metu, įslaptinimo (suteikiant žymas **RIBOTO NAUDOJIMO** ar **KONFIDENCIALIAI**) pagrįstumo.

Informacija apie objektą ir ketinamas įrengti arba eksploatuoti objekto apsaugos sistemas:

Eil. Nr.	Informacija	Pastabos
1.	Apsaugos sistemos **projektavimo, įrengimo, remonto darbų ir garantinės priežiūros paslaugų teikimas, remonto darbų ir priežiūros paslaugų teikimas, pasibaigus garantiniam terminui**, numatomas patalpose, priskirtose **I, II klasių ar Administracinei** saugumo klasės zonai (zonoms)	
2.	Objektui* Svarbių karinių objektų sąraše, patvirtintame *(įrašyti galiojančio dokumento datą, numerį, pavadinimą)* , priskirtas (nepriskirtas) Nr. _____	
3.	Objekto technologiniai (projektiniai) apsaugos sistemų sprendinių aprašymai ir schemos atitinka Detaliojo įslaptinamos informacijos sąrašo, patvirtinto *(įrašyti galiojančio dokumento datą, numerį, pavadinimą)*, _____ punktą	
4.	Informacijos, su kuria numatoma dirbti ar ją saugoti objekte, aukščiausia slaptumo žyma **VISIŠKAI SLAPTAI, SLAPTAI, KONFIDENCIALIAI, RIBOTO NAUDOJIMO, neįslaptinta**	

5.	Objekte **yra**/**nėra** įrengta **įslaptinta**/**neįslaptinta** apsaugos sistema, jos slaptumo žyma _____	
6.	Objektui apsaugoti numatoma **suprojektuoti, įrengti** elektroninę apsaugos sistemą, **pirkti elektroninės apsaugos sistemos garantinės priežiūros paslaugas ir remonto darbus arba priežiūros paslaugas ir remonto darbus, pasibaigus garantiniam terminui:**	
6.1.	**apsauginė įsilaužimo signalizacija**	
6.2.	**apsauginė užpuolimo signalizacija**	
6.3.	**įeigos kontrolės sistema**	
6.4.	**uždaroji vaizdo stebėjimo sistema**	
7.	**Tiekėjams ketinama perduoti įslaptinta informacija, jos slaptumo žymos ir įslaptinimo pagrindas**	
8.	**Numatoma sukurti įslaptinta informacija, jos slaptumo žymos ir įslaptinimo pagrindas**	

Pastaba. Paryškintus nereikalingus žodžius išbraukite. Stulpelyje „Pastabos“ įrašykite kitą reikalingą informaciją.

*** Objektas – patalpa, pastatas ar teritorija, kurioje numatoma įrengti apsaugos sistemą.**

Papildoma informacija:

_____

_____

_____

PRIDEDAMA:

1._____

(brėžiniai ir schemos (statinio teritorijos planas, statinio aukštų planai, kita))

_____

_____

_____	_____	_____
(krašto apsaugos sistemos institucijos vado (vadovo) pareigų pavadinimas)	(parašas)	(vardas ir pavardė)

5.1. LIETUVOS RESPUBLIKOS TARPTAUTINĖS SUTARTYS DĖL ĮSLAPTINTOS INFORMACIJOS APSAUGOS

Eil. Nr.	Tarptautinė organizacija, valstybė, su kuria pasirašyta sutartis	Sutarties pavadinimas	Ratifikavimo data
1.	Europos Sąjunga	Taryboje posėdžiavusių ES valstybių narių susitarimas dėl įslaptintos informacijos, kuria keičiamasi ES interesais, apsaugos	2012-11-06
2.	Šiaurės Atlanto Sutarties Organizacija	Šiaurės Atlanto Sutarties Šalių susitarimas dėl informacijos saugumo	2004-07-15
3.	Šiaurės Atlanto Sutarties Organizacija	NATO susitarimas dėl techninės informacijos perdavimo gynybos tikslais	2004-07-15
4.	Šiaurės Atlanto Sutarties Organizacija	Šiaurės Atlanto Sutarties Šalių susitarimas dėl bendradarbiavimo, susijusio su atomine informacija	2004-11-11
5.	Šiaurės Atlanto Sutarties Organizacija	NATO susitarimas dėl su gynyba susijusių išradimų, dėl kurių paduotos patento paraiškos, abipusės slaptumo apsaugos	2004-07-15
6.	Lietuvos Respublikos ir Vakarų Europos Sąjungos	Saugumo susitarimas	1997-05-22
7.	Lietuvos Respublikos ir Šiaurės Atlanto Sutarties Organizacijos	Saugumo susitarimas	1994-06-13
8.	Lietuvos Respublikos Vyriausybės ir Norvegijos Karalystės Vyriausybės	Susitarimas dėl įslaptintos informacijos abipusės apsaugos	2012-04-12
9.	Lietuvos Respublikos Vyriausybės ir Izraelio Valstybės Vyriausybės įgaliotos Gynybos ministerijos	Susitarimas dėl įslaptintos karinės ir su gynyba susijusios informacijos abipusės apsaugos	2012-04-12
10.	Lietuvos Respublikos Vyriausybės ir Ispanijos Karalystės	Susitarimas dėl įslaptintos informacijos abipusės apsaugos	2011-11-03
11.	Lietuvos Respublikos Vyriausybės ir Gruzijos Vyriausybės	Susitarimas dėl keitimosi įslaptinta informacija ir įslaptintos informacijos abipusės apsaugos	2010- 04-08

12.	Lietuvos Respublikos Vyriausybės ir Prancūzijos Respublikos Vyriausybės	Bendrasis saugumo susitarimas dėl keitimosi įslaptinta informacija ir įslaptintos informacijos apsaugos	2010-04-08
13.	Lietuvos Respublikos Vyriausybės ir Lenkijos Respublikos Vyriausybės	Susitarimas dėl įslaptintos informacijos abipusės apsaugos	2009-05-21
14.	Lietuvos Respublikos Vyriausybės ir Italijos Respublikos Vyriausybės	Susitarimas dėl įslaptintos informacijos abipusės apsaugos	2009-01-12
15.	Lietuvos Respublikos Vyriausybės ir Slovakijos Respublikos Vyriausybės	Susitarimas dėl įslaptintos informacijos abipusės apsaugos	2009-01-12
16.	Lietuvos Respublikos Vyriausybės ir Bulgarijos Respublikos Vyriausybės	Susitarimas dėl įslaptintos informacijos abipusės apsaugos	2007-11-20
17.	Lietuvos Respublikos Vyriausybės ir Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės Vyriausybės	Susitarimas dėl įslaptintos informacijos abipusės apsaugos	2006-12-05
18.	Lietuvos Respublikos Vyriausybės ir Ukrainos Respublikos Ministrų Tarybos	Susitarimas dėl įslaptintos informacijos abipusės apsaugos	2003-12-16
19.	Lietuvos Respublikos Vyriausybės ir Švedijos Karalystės Vyriausybės	Bendroji saugumo sutartis dėl įslaptintos informacijos abipusės apsaugos	2002-09-19
20.	Lietuvos Respublikos Vyriausybės ir Rumunijos Vyriausybės	Sutartis dėl įslaptintos karinės informacijos apsaugos	2002-06-25
21.	Lietuvos Respublikos Vyriausybės ir Čekijos Respublikos Vyriausybės	Sutartis dėl įslaptintos informacijos abipusės apsaugos	2001-03-27
22.	Lietuvos Respublikos Vyriausybės ir Latvijos Respublikos Vyriausybės	Sutartis dėl įslaptintos informacijos abipusės apsaugos	2000-10-12
23.	Lietuvos Respublikos Vyriausybės ir Estijos Respublikos Vyriausybės	Sutartis dėl abipusės įslaptintos informacijos apsaugos	2000-10-12
24.	Lietuvos Respublikos Vyriausybės ir Vokietijos Federacinės Respublikos Vyriausybės	Sutartis dėl įslaptintos informacijos abipusės apsaugos	1999-04-20
25.	Lietuvos Respublikos Vyriausybės ir Jungtinių Amerikos Valstijų Vyriausybės	Sutartis dėl saugumo priemonių slaptajai karinei informacijai apsaugoti	1995-11-21

5.2. ŠIAURĖS ATLANTO SUTARTIES ŠALIŲ SUSITARIMAS DĖL INFORMACIJOS SAUGUMO

(Žin., 2004, Nr. 127-4558)

1949 m. balandžio 4 d. Vašingtone pasirašytos Šiaurės Atlanto Sutarties Šalys,

patvirtindamos, kad veiksmingos politinės konsultacijos, bendradarbiavimas ir gynybos planavimas siekiant Sutarties tikslų lemia poreikį Šalims keistis įslaptinta informacija;

manydamos, kad Šiaurės Atlanto Sutarties Šalių vyriausybėms būtinos nuostatos dėl įslaptintos informacijos, kuria jos gali keistis, abipusės apsaugos;

suvokdamos, kad būtini bendri saugumo standartų ir procedūrų pagrindai;

veikdamos savo ir Šiaurės Atlanto Sutarties Organizacijos vardu,

s u s i t a r ė:

1 straipsnis

Šalys:

i) saugo:

a) atitinkamai pažymėtą įslaptintą informaciją (žr. I priedą), kurią parengė NATO (žr. II priedą) arba kurią valstybė narė pateikė NATO;

b) atitinkamai pažymėtą įslaptintą valstybių narių informaciją, pateiktą kitai valstybei narei pradedant vykdyti kurią nors NATO programą, projektą ar sutartį;

ii) išsaugo šio straipsnio i punkte nurodytos informacijos slaptumo žymas ir visokeriopai stengiasi ją atitinkamai apsaugoti;

iii) nenaudoja šio straipsnio i punkte nurodytos įslaptintos informacijos kitokiems tikslams, nei nustatytieji Šiaurės Atlanto Sutartyje arba su ja susijusiuose sprendimuose ir rezoliucijose;

iv) neatskleidžia šio straipsnio i punkte nurodytos informacijos ne NATO Šalims be informacijos rengėjo sutikimo.

2 straipsnis

Vykdydamos šio Susitarimo 1 straipsnį, Šalys užtikrina, kad būtų įsteigta Nacionalinė saugumo institucija NATO veiklai, kuri įgyvendintų prevencines apsaugos priemones. Šalys nustato ir įgyvendina saugumo standartus, kurie užtikrina vienodą įslaptintos informacijos apsaugos laipsnį.

3 straipsnis

1) Šalys užtikrina, kad būtų atliktas tinkamas visų jų pilietybę turinčių asmenų, kurie, vykdydami tarnybines pareigas, turi arba gali susipažinti su informacija, žymima slaptumo žyma „Konfidencialiai“ ir aukštesnio laipsnio slaptumo žymomis, patikimumo patikrinimas prieš jiems pradedant eiti tokias pareigas.

2) Asmens patikimumo patikrinimo procedūros turi būti tokios, kad pagal jas būtų galima nustatyti, ar asmuo, atsižvelgiant į jo lojalumą ir patikimumą,

gali susipažinti su įslaptinta informacija, tuo nesukeldamas nepriimtino pavojaus saugumui.

3) Bet kurios iš Šalių prašymu visos Šalys bendradarbiauja, atlikdamos atitinkamas asmens patikimumo patikrinimo procedūras.

4 straipsnis

Generalinis Sekretorius užtikrina, kad NATO taikytų atitinkamas šio Susitarimo nuostatas (žr. III priedą).

5 straipsnis

Šis Susitarimas netrukdo Šalims sudaryti kitų susitarimų dėl keitimosi jų parengta įslaptinta informacija, neturinčių įtakos šio Susitarimo dalykui.

6 straipsnis

a) Šį Susitarimą gali pasirašyti Šiaurės Atlanto Sutarties Šalys ir jis turi būti ratifikuojamas, priimamas arba patvirtinamas. Ratifikavimo, priėmimo arba patvirtinimo dokumentai deponuojami Jungtinių Amerikos Valstijų Vyriausybei.

b) Šis Susitarimas įsigalioja praėjus trisdešimčiai dienų nuo tos dienos, kai dvi jį pasirašiusios valstybės deponuoja savo ratifikavimo, priėmimo arba patvirtinimo dokumentus. Kiekvienai kitai šį Susitarimą pasirašiusiai valstybei jis įsigalioja praėjus trisdešimčiai dienų nuo tos dienos, kai ji deponuoja savo ratifikavimo, priėmimo arba patvirtinimo dokumentą.

c) Šalims, kurioms šis Susitarimas jau įsigaliojo, jis pakeičia Šiaurės Atlanto Sutarties Organizacijos Šalių saugumo susitarimą, kurį 1952 m. balandžio 19 d. Šiaurės Atlanto Taryba patvirtino dokumentą D.C. 2/7 papildančio dokumento priedėlio A priedu (1 punktas) ir vėliau įtraukė į 1955 m. kovo 2 d. Šiaurės Atlanto Tarybos patvirtinto dokumento C-M(55)15 (galutinė redakcija) A priedėlį (1 punktas).

7 straipsnis

Bet kuri nauja Šiaurės Atlanto Sutarties Šalis gali prisijungti prie šio Susitarimo pagal savo konstitucines procedūras. Jos prisijungimo dokumentas deponuojamas Jungtinių Amerikos Valstijų Vyriausybei. Kiekvienai prisijungusiai valstybei šis Susitarimas įsigalioja praėjus trisdešimčiai dienų nuo tos dienos, kai deponuojamas jos prisijungimo dokumentas.

8 straipsnis

Jungtinių Amerikos Valstijų Vyriausybė kitų Šalių vyriausybėms praneša apie kiekvieno ratifikavimo, priėmimo, patvirtinimo arba prisijungimo dokumento deponavimą.

9 straipsnis

Bet kuri Šalis gali denonsuoti šį Susitarimą raštu pranešdama apie tai depozitarui, kuris apie tokį pranešimą informuoja visas kitas Šalis. Toks denon-

savimas įsigalioja praėjus vieneriems metams po to, kai depozitaras gauna tokį pranešimą. Tačiau denonsavimas nekeičia Šalių pagal šio Susitarimo nuostatas anksčiau prisiimtų įsipareigojimų ir įgytų teisių.

Tai patvirtindami, toliau nurodyti tinkamai savo vyriausybių įgalioti asmenys pasirašė šį Susitarimą.

Pasirašyta 1997 m. kovo 6 d. Briuselyje anglų ir prancūzų kalbomis, vienu egzemplioriumi, kuris deponuojamas Junginių Amerikos Valstijų Vyriausybės archyvuose. Abu tekstai yra autentiški. Jungtinių Amerikos Valstijų Vyriausybė perduoda patvirtintas Susitarimo kopijas visoms kitoms jį pasirašiusioms valstybėms.

I PRIEDAS

Šis priedas yra Susitarimo sudėtinė dalis.

Įslaptinta NATO informacija apibrėžiama taip:

a) „informacija“ – tai žinios, kurias galima perduoti bet kokia forma;

b) „įslaptinta informacija“ – tai informacija arba medžiaga, kurią reikia saugoti nuo neteisėto atskleidimo ir todėl jai suteikta slaptumo žyma;

c) „medžiaga“ – tai dokumentai, taip pat bet kokia pagaminta ar gaminama mechanizmo, įrangos ar ginklo dalis;

d) „dokumentas“ – tai bet kokia fiksuota informacija, nesvarbu, kokia jos fizinė forma ir savybės, kuri, be kita ko, apima rašytinę ir spausdintinę medžiagą, duomenų apdorojimo korteles ir juostas, žemėlapius, schemas, fotografijas, piešinius, brėžinius, graviūras, eskizus, darbo užrašus ir raštus, kalkinius egzempliorius ir rašalines juosteles arba bet kuria kita priemone ar procesu padarytas kopijas, taip pat garso, balso, magnetinius, elektroninius, optinius ar vaizdo įrašus bet kuria forma, nešiojamąją ADA (automatizuoto duomenų apdorojimo) įrangą su stacionariomis kompiuterinėmis laikmenomis ir išimamas kompiuterines laikmenas.

II PRIEDAS

Šis priedas yra Susitarimo sudėtinė dalis.

Šiame Susitarime „NATO“ – tai Šiaurės Atlanto Sutarties Organizacija ir institucijos, kurioms taikomas Susitarimas dėl Šiaurės Atlanto Sutarties Organizacijos, valstybių atstovų ir tarptautinio personalo statuso, pasirašytas 1951 m. rugsėjo 20 d. Otavoje, arba Protokolas dėl tarptautinių karinių vadaviečių, įsteigtų įgyvendinant Šiaurės Atlanto Sutartį, statuso, pasirašytas 1952 m. rugpjūčio 28 d. Paryžiuje.

III PRIEDAS

Šis priedas yra Susitarimo sudėtinė dalis.

Siekiant gerbti išimtines karinių vadų teises, su jais turi būti konsultuojamasi.

5.3. ŠIAURĖS ATLANTO SUTARTIES ŠALIŲ SUSITARIMAS DĖL BENDRADARBIAVIMO, SUSIJUSIO SU ATOMINE INFORMACIJA

(Žin., 2004, Nr. 174-6436; 2007, Nr. 9-351)

Preambulė

1949 m. balandžio 4 d. Vašingtone pasirašytos Šiaurės Atlanto Sutarties Šalys,

pripažindamos, kad jų bendras saugumas ir gynyba reikalauja būti pasirengusioms netikėtam atominiam karui;

pripažindamos, kad su tuo susijusios informacijos teikimas Šiaurės Atlanto Sutarties Organizacijai ir jos valstybėms narėms tarnauja jų bendriems interesams;

atsižvelgdamos į šiais tikslais parengtą Jungtinių Amerikos Valstijų 1954 m. Atominės energijos aktą, su pakeitimais;

veikdamos savo ir Šiaurės Atlanto Sutarties Organizacijos vardu,

s u s i t a r ė :

I straipsnis

Kol Šiaurės Atlanto Sutarties Organizacija iš esmės ir konkrečiai prisidės prie bendros gynybos ir saugumo, Jungtinių Amerikos Valstijų Vyriausybė, taikydama Jungtinių Valstijų 1954 m. Atominės energijos akto (su pakeitimais) reikalavimus ir jų laikydamasi, bendradarbiaus, prireikus pagal šio Susitarimo nuostatas perduodama tokiu būdu prisidedančiai Šiaurės Atlanto Sutarties Organizacijai ir jos valstybėms narėms atominę informaciją, jeigu Jungtinių Amerikos Valstijų Vyriausybė nuspręs, kad toks bendradarbiavimas stiprins šalies gynybą bei saugumą ir nesukels jiems nepagrįsto pavojaus.

II straipsnis

Panašiai į Jungtinių Amerikos Valstijų Vyriausybės įsipareigojimus pagal šį Susitarimą, kitos valstybės, Šiaurės Atlanto Sutarties Organizacijos narės, tokiu mastu, kokiu mano esant būtina, perduos Šiaurės Atlanto Sutarties Organizacijai, įskaitant jos karines ir civilines institucijas, bei jos valstybėms narėms savo parengtą šiame Susitarime numatyto pobūdžio atominę informaciją. Kitų valstybių narių tokios informacijos perdavimą reglamentuojančias sąlygas ir tvarką nustatys tolesni susitarimai, tačiau jos bus tokios pačios arba panašios į šiame Susitarime išdėstytas sąlygas ir tvarką.

III straipsnis

Jungtinių Amerikos Valstijų Vyriausybė perduos Šiaurės Atlanto Sutarties Organizacijai, įskaitant jos karines ir civilines institucijas, bei Šiaurės Atlanto Sutarties Organizacijos valstybėms narėms, kurioms atominės informacijos reikia vykdant su NATO užduotimis susijusias funkcijas, tokią atominę informaci-

ją, kurią Jungtinių Amerikos Valstijų Vyriausybė laiko būtina:

a) plėtoti gynybos planus;

b) mokyti personalą, kaip naudoti atominius ginklus ir gintis nuo jų bei kitaip panaudoti atominę energiją kariniais tikslais;

c) įvertinti potencialių priešų pajėgumus naudoti atominius ginklus ir kitaip panaudoti atominę energiją kariniais tikslais;

d) sukurti pristatymo sistemas, pritaikytas gabenamiems atominiams ginklams.

IV straipsnis

1. Jungtinių Amerikos Valstijų Vyriausybė bendradarbiaus pagal šį Susitarimą, remdamasi savo šioje srityje taikytinais įstatymais.

2. Pagal šį Susitarimą Jungtinių Amerikos Valstijų Vyriausybė neperduos jokių atominių ginklų, atominių ginklų nebranduolinių dalių ar atominių ginklų sistemų nebranduolinių dalių, kuriose naudojami riboto naudojimo duomenys.

3. Atominė informacija, kurią Jungtinių Amerikos Valstijų Vyriausybė perduoda pagal šį Susitarimą, turi būti naudojama tik NATO gynybos planams ir veiklai rengti ar įgyvendinti, taip pat pristatymo sistemoms sukurti bendrų Šiaurės Atlanto Sutarties Organizacijos interesų labui.

V straipsnis

1. Pagal šį Susitarimą perduodamos atominės informacijos saugumui užtikrinti taikomos visos atitinkamų NATO taisyklių ir tvarkos, sutartų saugumo priemonių ir nacionalinių įstatymų bei kitų teisės aktų numatytos apsaugos priemonės. Jokiais atvejais Šiaurės Atlanto Sutarties Organizacija ar jos valstybės narės atominės informacijos apsaugai netaiko žemesnio laipsnio saugumo standartų, negu nustatytieji šio Susitarimo įsigaliojimo dieną galiojančiomis atitinkamomis NATO saugumo taisyklėmis bei kitomis sutartomis saugumo priemonėmis.

2. Visose NATO karinėse ir civilinėse institucijose saugumo programa bus kuriama ir koordinuojama sutartų saugumo priemonių nustatyta tvarka, vadovaujant Šiaurės Atlanto Tarybai.

3. Jungtinių Amerikos Valstijų Vyriausybės pagal šį Susitarimą perduodama atominė informacija bus perduodama esamais ar vėliau sutartais atominės informacijos perdavimo kanalais.

4. Šiaurės Atlanto Sutarties Organizacija ar jos jurisdikcijai priklausantys asmenys neperduoda atominės informacijos, kuri yra perduota arba kuria pasikeista pagal šį Susitarimą, neįgaliotiems asmenims arba, išskyrus šio straipsnio 5 dalyje numatytus atvejus, už Organizacijos jurisdikcijos ribų, ir nesikeičia su jais šia informacija.

5. Jeigu Jungtinių Amerikos Valstijų Vyriausybė nenustato kitaip, Šiaurės Atlanto Sutarties Organizacija gautą Jungtinių Valstijų atominę informaciją gali perduoti savo valstybėms narėms, kai tai būtina su NATO užduotimis susijusioms funkcijoms atlikti, jeigu tokios atominės informacijos platinimas tokiose valstybėse narėse yra apribotas tik konkrečiais asmenimis, susijusiais su NATO užduotimis, kurioms atlikti ši informacija reikalinga. Valstybės narės sutinka,

kad tokiu būdu iš Šiaurės Atlanto Sutarties Organizacijos ar kitaip pagal šį Susitarimą gauta atominė informacija negali būti perduota neįgaliotiems asmenims arba už informaciją gavusios valstybės narės jurisdikcijos ribų; tačiau tokia informacija gali būti perduota Šiaurės Atlanto Sutarties Organizacijai arba, Jungtinių Amerikos Valstijų Vyriausybei leidus, kitoms valstybėms narėms, kurioms ši informacija reikalinga su NATO užduotimis susijusioms funkcijoms atlikti.

VI straipsnis

Nepaisant kitų šio Susitarimo nuostatų, Jungtinių Amerikos Valstijų Vyriausybė gali nustatyti Šiaurės Atlanto Sutarties Organizacijai ar jos valstybėms narėms perduotos atominės informacijos platinimo mastą, nurodyti asmenų, kurie gali susipažinti su tokia informacija, kategorijas ir taikyti kitus, jos manymu, būtinus informacijos platinimo apribojimus.

VII straipsnis

1. Šalis, gaunanti atominę informaciją pagal šį Susitarimą, ją naudoja tik jame nurodytais tikslais. Bet kokie išradimai ar atradimai, informaciją gavusios Šalies arba jos jurisdikcijai priklausančių asmenų padaryti remiantis tokia informacija, pagal galimus susitarimus gynybos tikslais neatlygintinai perduodami Jungtinių Amerikos Valstijų Vyriausybei ir saugomi pagal šio Susitarimo V straipsnio nuostatas.

2. Už bet kokios pagal šį Susitarimą perduotos informacijos taikymą arba naudojimą atsako ją gaunanti Šalis; informaciją perduodanti Šalis neteikia jokių kompensacijų ar garantijų dėl informacijos pritaikymo ar naudojimo.

VIII straipsnis

Jokia šio Susitarimo nuostata nepakeičia šio Susitarimo Šalių dvišalių susitarimų dėl bendradarbiavimo keičiantis atomine informacija ir neturi jiems jokios įtakos.

IX straipsnis

Šiame Susitarime:

a) „atominis ginklas“ – tai bet koks įtaisas, naudojantis atominę energiją, išskyrus jo transportavimo ar varomąsias priemones (kai tokios priemonės yra atskiriamosios šio įtaiso dalys), kurio pagrindinė paskirtis – naudoti arba tobulinti jį kaip ginklą, ginklo eksperimentinį pavyzdį ar ginklo bandymo įtaisą;

b) „atominė informacija“, Jungtinių Amerikos Valstijų Vyriausybės teikiama pagal šį Susitarimą – tai informacija, Jungtinių Amerikos Valstijų Vyriausybės pažymėta kaip „Riboto naudojimo duomenys“ (*Restricted Data*) arba „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*).

X straipsnis

1. Šis Susitarimas įsigalioja, kai Jungtinių Amerikos Valstijų Vyriausybė gauna visų Šiaurės Atlanto Sutarties Šalių pranešimus, kad jos sutinka būti įpa-

reigotos šio Susitarimo sąlygų.

2. Jungtinių Amerikos Valstijų Vyriausybė informuos visas Šiaurės Atlanto Sutarties Šalis ir Šiaurės Atlanto Sutarties Organizaciją apie kiekvieną tokį pranešimą ir apie šio Susitarimo įsigaliojimą.

3. Šis Susitarimas galioja tol, kol jis nutraukiamas vieningu sutarimu arba pakeičiamas kitu susitarimu; tačiau susitariama, kad viso šio Susitarimo nutraukimas neatleidžia nė vienos Šalies nuo šio Susitarimo reikalavimų saugoti pagal jį perduotą informaciją.

XI straipsnis

Nepaisant 1955 m. birželio 22 d. Paryžiuje pasirašyto Šiaurės Atlanto Sutarties Šalių susitarimo dėl bendradarbiavimo, susijusio su atomine informacija, VI straipsnio 4 dalies, įsigaliojus šiam Susitarimui, jis pakeičia minėtą susitarimą. Tačiau susitariama, kad pagal tą susitarimą perduota informacija visais atvejais laikoma informacija, perduota pagal šio Susitarimo nuostatas.

XII straipsnis

Šio Susitarimo data yra jo pateikimo pasirašyti data; jį galima pasirašyti tol, kol jį pasirašo visos Šiaurės Atlanto Sutarties Šalys.

Tai patvirtindami, toliau nurodyti atstovai pasirašė šį Susitarimą savo valstybių, Šiaurės Atlanto Sutarties Organizacijos narių, ir Šiaurės Atlanto Sutarties Organizacijos vardu.

Pasirašyta 1964 m. birželio 18 d. Paryžiuje anglų ir prancūzų kalbomis vienu egzemplioriumi, kuris deponuojamas Jungtinių Amerikos Valstijų Vyriausybės archyvuose. Abu tekstai yra autentiški.

Jungtinių Amerikos Valstijų Vyriausybė perduoda patvirtintas Susitarimo kopijas visoms jį pasirašiusioms ir prie jo prisijungiančioms valstybėms.

ŠIAURĖS ATLANTO SUTARTIES ŠALIŲ SUSITARIMO DĖL BENDRADARBIAVIMO, SUSIJUSIO SU ATOMINE INFORMACIJA, SAUGUMO PRIEDAS

Šiame Priede išdėstytos saugumo priemonės, kurių Šiaurės Atlanto Sutarties Organizacija ir jos valstybės narės imasi, kad būtų apsaugota atominė informacija, kurią Jungtinių Amerikos Valstijų Vyriausybė perdavė Šiaurės Atlanto Sutarties Organizacijai ir jos valstybėms narėms pagal 1964 m. birželio 18 d. Paryžiuje pasirašytą Susitarimą dėl bendradarbiavimo, susijusio su atomine informacija (toliau – Susitarimas); šis Priedas yra neatskiriama Susitarimo dalis. Jei Šiaurės Atlanto Sutarties Organizacijos narė, išskyrus Jungtinių Amerikos Valstijų Vyriausybę, perduoda atominę informaciją pagal Susitarimo II straipsnį, jos saugumui užtikrinti imamasi ne mažesnių apsaugos priemonių, negu numatyta šiame Priede.

I SKYRIUS
BENDROSIOS NUOSTATOS

A. NATO karinės ir civilinės institucijos bei valstybės narės užtikrina pagal Susitarimą perduotos atominės informacijos saugumą taikydamos ne mažiau griežtas NATO saugumo taisykles negu tos, kurios yra išdėstytos Dokumente C–M(55)15(Final) ir jo 1961 m. sausio 1 d. Priedėlyje, pažymėtame slaptumo žyma „Konfidencialiai“, taip pat šiame Priede išdėstytas saugumo priemones.

B. Visų NATO karinių ir civilinių institucijų bei valstybių narių, pagal Susitarimą gaunančių atominę informaciją, vykdoma saugumo programa numato visas šiame Priede nustatytų saugumo reikalavimų įgyvendinimui būtinas priemones.

C. Generalinis Sekretorius, veikiantis Šiaurės Atlanto Tarybos vardu ir jos vadovaujamas, atsako už NATO saugumo programos dėl atominės informacijos, perduotos pagal Susitarimą, apsaugos taikymo priežiūrą. Šio Priedo X skyriuje nustatyta tvarka jis užtikrina, kad NATO civilinėse ir karinėse institucijose bei nacionalinėse civilinėse ir karinėse struktūrose yra taikomos visos NATO saugumo programoje numatytos būtinos priemonės informacijai, kuria keičiamasi pagal Susitarimą, apsaugoti.

D. Asmens turimas laipsnis, pareigos ar asmens patikimumo pažymėjimas savaime nesuteikia teisės susipažinti su atomine informacija.

E. Susipažinti su Šiaurės Atlanto Sutarties Organizacijai perduota atomine informacija gali tik Šiaurės Atlanto Sutarties Organizacijos valstybių narių piliečiai, kuriems yra išduotas asmens patikimumo pažymėjimas pagal šio Priedo II skyrių ir kuriems pagal einamas pareigas būtina susipažinti su tokia informacija.

F. Susipažinti su atomine informacija, perduota valstybei narei pagal Susitarimą, gali tik jos piliečiai, kuriems yra išduotas asmens patikimumo pažymėjimas pagal šio Priedo II skyrių ir kuriems pagal einamas pareigas būtina susipažinti su tokia informacija, kad tokia valstybė narė galėtų vykdyti savo pareigas ir įsipareigojimus Šiaurės Atlanto Sutarties Organizacijai.

II SKYRIUS
PERSONALO PATIKIMUMAS

A. Asmens patikimumo pažymėjimas susipažinti su atomine informacija asmeniui išduodamas tik įsitikinus, kad tokios teisės suteikimas nesukels pavojaus Šiaurės Atlanto Sutarties Organizacijos saugumui arba Šiaurės Atlanto Sutarties Organizacijos valstybių narių nacionaliniam saugumui.

B. Prieš suteikdama teisę susipažinti su atomine informacija, atitinkamo asmens šalies vyriausybės atsakinga institucija nustato asmens, kuriam turi būti suteikta tokia teisė, patikimumą (priima sprendimą išduoti asmens patikimumo pažymėjimą).

C. Sprendimas, ar asmens patikimumo pažymėjimo išdavimas tikrai atitinka saugumo interesus, priimamas remiantis visa turima informacija. Prieš nustatydama asmens patikimumą, atsakinga valstybės institucija atlieka tyrimą ir visa

surinkta informacija įvertinama pagal neigiamos informacijos, kuri galėtų kelti abejonių dėl asmens patikimumo, pagrindines rūšis, nurodytas 1961 m. sausio 1 d. dokumento C–M(55)15 (Final) Priedėlio, pažymėto slaptumo žyma „Konfidencialiai“, III skyriuje.

D. Minimalus tyrimo mastas ir lygis turi atitikti dokumento C–M(55)15 (Final) Priedėlio, pažymėto slaptumo žyma „Konfidencialiai“, III skyriuje išdėstytus standartus, tačiau prieš leidžiant susipažinti su atomine informacija, žymima slaptumo žyma „Slaptai“, asmenims, kurie netarnauja valstybių narių ginkluotosiose pajėgose arba nepriklauso jų karinių institucijų civiliniam personalui, būtina atlikti biografijos tikrinimą.

E. Kiekviena institucija, disponuojanti atomine informacija, tvarko joje dirbantiems asmenims išduotų asmens patikimumo pažymėjimų, patvirtinančių teisę susipažinti su tokia informacija, apskaitą. Kai reikalinga, kiekvieno asmens patikimumo pažymėjimo klausimas apsvarstomas iš naujo, kad būtų užtikrintas jo ir galiojančių reikalavimų, taikomų asmens užimamoms pareigoms, atitikimas, ir pakartotinai apsvarstomas skubos tvarka, kai gaunama informacijos, nurodančios, kad tolesnis darbas einant pareigas, susijusias su atomine informacija, gali būti nesuderinamas su saugumo interesais.

F. Kiekvienoje valstybėje nacionalinės institucijos, atsakingos už nacionalinį saugumą, palaiko veiksmingus ryšius su institucija, priimančia sprendimus dėl asmens patikimumo pažymėjimų išdavimo, kad būtų užtikrintas neigiamos informacijos, gautos po to, kai buvo išduotas asmens patikimumo pažymėjimas, greitas perdavimas.

III SKYRIUS
FIZINĖ APSAUGA

A. Atominė informacija apsaugoma fizinėmis priemonėmis nuo šnipinėjimo, sabotažo, neteisėto naudojimo ar bet kokios kitos priešiškos veiklos. Tokios apsaugos lygis taikomas pagal saugomos įslaptintos informacijos svarbą.

B. Turi būti parengtos atominės informacijos fizinės apsaugos programos, kad būtų:

1) užtikrinta tinkama darbo vietose naudojamos, saugyklose laikomos arba perduodamos atominės informacijos apsauga;

2) nustatytos saugumo zonos ir įėjimo į jas kontrolė, kai tai būtina dėl įslaptintos atominės informacijos slaptumo žymos, pobūdžio, apimties ar naudojimo ir atitinkamo pastato (pastatų) ypatybių ir vietos;

3) įdiegta įėjimo kontrolės sistema, apimanti procedūras, kuriomis vadovaudamasi kompetentinga institucija leistų patekti į saugumo zoną, tikslius personalo asmens tapatybės nustatymo bei atpažinimo įrengimų apskaitos metodus ir judėjimo saugumo zonose bei įėjimo į jas ribojančių priemonių įgyvendinimo būdus.

C. B dalyje išdėstytos nuostatos taikomos kartu su dokumento C–M(55)15 (Final) IV skyriuje nurodytomis procedūromis.

IV SKYRIUS
ATOMINĖS INFORMACIJOS KONTROLĖ

A. Turi būti vykdomos informacijos kontrolės programos, kurių pagrindinis tikslas:

1) kontroliuoti prieigą;

2) parengti informacijos slaptumo žymą atitinkančią apskaitą;

3) sunaikinti informaciją, kai ji nebereikalinga.

B. Visuomet būtina laikytis slaptumo žymų, kurias pagal Susitarimą perduodamai atominei informacijai taiko Jungtinių Amerikos Valstijų Vyriausybė. Keisti informacijos slaptumo žymą žemesne žyma arba ją išslaptinti galima tik gavus Jungtinių Amerikos Valstijų Vyriausybės sutikimą.

C. Dokumentai, kuriuose yra pagal Susitarimą Jungtinių Amerikos Valstijų Vyriausybės perduotos atominės informacijos, žymimi NATO žymomis ir įslaptinami tuo pačiu lygiu, kokį nustatė Jungtinių Amerikos Valstijų Vyriausybė, papildomai įrašant žymą „ATOMAL“. Be to, dokumente ta kalba, kuria parašytas dokumentas, užrašomas toks sakinys:

„Šiame dokumente esanti Jungtinių Amerikos Valstijų atominė informacija („Riboto naudojimo duomenys“ (*Restricted Data*) arba „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*) yra perduota pagal 1964 m. birželio 18 d. pasirašytą NATO susitarimą dėl bendradarbiavimo, susijusio su atomine informacija, ir turi būti atitinkamai saugoma.“

D. Visi dokumentai, pažymėti slaptumo žymomis „Visiškai slaptai“ ir „Slaptai“, taip pat visi dokumentai, kuriems pagal Susitarimo VI straipsnį nustatyti specialūs apribojimai, registruojami apskaitos dokumentuose. Tokiuose apskaitos dokumentuose įrašomi visų asmenų, gaunančių dokumentus, kuriems taikomi specialūs apribojimai, duomenys.

E. Dokumentus, kuriuose yra Jungtinių Amerikos Valstijų atominės informacijos, pažymėtos šio skyriaus C dalyje nurodytomis žymomis, galima atgaminti, įskaitant jų ištraukas ir vertimus, laikantis tokių taisyklių:

1) dokumentus, pažymėtus slaptumo žymomis „Visiškai slaptai“ ir „Slaptai“, galima atgaminti tik gavus išankstinį Jungtinių Amerikos Valstijų Vyriausybės sutikimą. Tokiuose dokumentuose įrašoma atitinkama žyma. Kai ypač skubiu atveju neįmanoma laiku gauti išankstinį sutikimą, šios taisyklės galima nesilaikyti, tačiau Jungtinių Amerikos Valstijų Vyriausybei apie tai pranešama ypatingos skubos tvarka;

2) dokumentus, pažymėtus slaptumo žyma „Konfidencialiai“, galima atgaminti tik esant būtinam poreikiui;

3) atgaminiai, įskaitant ištraukas ir vertimus, žymimi visomis dokumento originalo slaptumo žymomis (įskaitant C dalyje nurodytas žymas), ir apskaitomi pagal dokumento originalui taikomas kontrolės taisykles. Kai dalys turi skirtingas slaptumo žymas, dokumentai, kuriuose yra atominės informacijos ištraukų, žymimi aukščiausia dalies, kurios ištrauka buvo padaryta, slaptumo žyma ir prireikus – C dalyje nurodytomis žymomis. Atominės informacijos ištraukos apskaitomos pagal šio skyriaus D dalies nuostatų reikalavimus. Be to,

dokumentams, kuriuose yra ištraukų, taikomi dokumento originalui nustatyti specialūs apribojimai.

F. Dokumentai, parengti pagal Susitarimą perduodamai atominei informacijai užrašyti žodinės ir vaizdinės informacijos užrašymo priemonėmis, žymimi šio skyriaus C dalyje nurodytomis žymomis ir apskaitomi bei kontroliuojami pagal jų slaptumo žymas.

V SKYRIUS
PERDAVIMO KANALAI

Jungtinių Amerikos Valstijų Vyriausybė pagal Susitarimą teikiamą atominę informaciją, įskaitant žodinę ir vaizdinę medžiagą, perduoda esamais ar vėliau sutartais kanalais. Siekdama padėti Generaliniam Sekretoriui vykdyti šio Priedo I skyriaus C dalyje jam nustatytas informacijos apsaugos funkcijas, Jungtinių Amerikos Valstijų Vyriausybė Generaliniam Sekretoriui pateikia pakankamai informacijos, kad būtų galima atpažinti kiekvieną Jungtinių Amerikos Valstijų Vyriausybės rašytinį atominės informacijos pranešimą ir kiekvieną pranešimą, kurį Jungtinių Amerikos Valstijų Vyriausybė leido perduoti pagal Susitarimą. Tokia informacija taip pat perduodama nuolatinei grupei, atsakingai už visų pranešimų perdavimą karinėms institucijoms.

VI SKYRIUS
ATASKAITOS

A. Iki kiekvienų metų kovo 31 d. kiekviena valstybė narė ir NATO karinė bei civilinė institucija, gaunanti pagal Susitarimą perduodamą Jungtinių Amerikos Valstijų atominę informaciją, per Generalinį Sekretorių Jungtinių Amerikos Valstijų Vyriausybei perduoda esamais ar vėliau sutartais kanalais ataskaitą, kurioje pateikiama:

1) visų atominės informacijos dokumentų, gautų iš Jungtinių Amerikos Valstijų Vyriausybės per dvylika mėnesių iki praėjusių metų gruodžio 31 d., sąrašas;

2) 1 punkte nurodytų dokumentų platinimo apskaitos dokumentas;

3) pažyma, patvirtinanti, kad buvo fiziškai patikrinti visi atominės informacijos dokumentai, už kuriuos valstybė narė arba NATO karinė ar civilinė institucija yra atskaitinga pagal Susitarimą. Pažymoje pateikiamas visų dingusių dokumentų sąrašas ir dokumentų praradimo tyrimo rezultatų bei ištaisomųjų veiksmų, kurių imtasi, kad būtų išvengta panašių įvykių ateityje, ataskaita.

B. Jei pagal Susitarimą perduotos Jungtinių Amerikos Valstijų atominės informacijos saugumas yra pažeidžiamas dėl dokumento praradimo ar kitu būdu, Generaliniam Sekretoriui ir Jungtinių Amerikos Valstijų Vyriausybei esamais ar vėliau sutartais kanalais nedelsiant perduodama ataskaita, kurioje nurodoma visa informacija, susijusi su informacijos saugumo pažeidimu.

VII SKYRIUS
SAUGUMO MOKYMAS

Valstybės narės bei NATO karinės ir civilinės institucijos, gaunančios informaciją pagal Susitarimą, įgyvendina atitinkamą programą, užtikrinančią, kad visi asmenys, turintys teisę susipažinti su atomine informacija, būtų informuoti apie jų pareigą saugoti tokią informaciją. Programa apima specialųjį pradinį mokymą ir supažindinimą su saugumo reikalavimais, reguliarų kartotinį instruktažą apie asmeninę atsakomybę ir, asmeniui baigiant eiti pareigas, – pokalbį, kurio metu būtų pabrėžiama jo tolesnė atsakomybė už atominės informacijos apsaugą.

VIII SKYRIUS
ĮSLAPTINTŲ SANDORIŲ SAUGUMAS

Susitarimo Šalys, sudarydamos kiekvieną įslaptintą sandorį, subsandorį arba susitarimą dėl konsultacijų ar kitokį susitarimą, kurio vykdymas susijęs su susipažinimu su pagal Susitarimą perduodama atomine informacija, įtraukia į jį atitinkamas nuostatas, įpareigojančias susijusius privačius asmenis laikytis šiame Priede nustatytų saugumo reikalavimų.

IX SKYRIUS
NUOLATINĖ SAUGUMO SISTEMOS PERŽIŪRA

A. Reguliariai per laikotarpį, kurį nustato Šiaurės Atlanto Taryba, NATO Saugumo komitetui rekomendavus, atliekamas visų NATO karinių ir civilinių institucijų bei valstybių narių, kurios pagal Susitarimą gauna atominę informaciją, išsamus saugumo tikrinimas, vadovaujantis šio Priedo I skyriaus A dalyje nustatytais kriterijais. Susitariama toliau nuolat keistis nuomonėmis dėl saugumo politikos, standartų bei procedūrų ir leisti Jungtinių Amerikos Valstijų darbo grupėms saugumo klausimais tikrinti bei tiesiogiai susipažinti su Šiaurės Atlanto Sutarties Organizacijos agentūrų ir valstybių narių institucijų, atsakingų už pagal Susitarimą perduodamų dokumentų ir informacijos apsaugą, procedūromis ir praktika. Tokie vizitai reikalingi, kad būtų išsiaiškinta, ar atitinkamos saugumo sistemos yra tinkamos, bei būtų galima jas tinkamai palyginti.

B. Apie tokius vizitus pranešama Generaliniam Sekretoriui, o vykstant į karines institucijas – ir nuolatinei grupei, ir po kiekvieno tokio apsilankymo Jungtinių Amerikos Valstijų darbo grupės jiems pateikia atitinkamų rezultatų ataskaitą. Visi apsilankymai nacionalinėse institucijose rengiami bendradarbiaujant su atitinkamos šalies nacionalinio saugumo institucijomis.

X SKYRIUS
SAUGUMO TIKRINIMAS

A. Reguliariai, tačiau ne rečiau kaip kartą kas dvylika mėnesių, atliekamas visų NATO karinių ir civilinių institucijų bei valstybių narių, kurios gauna pagal Susitarimą atominę informaciją, išsamus saugumo tikrinimas, vadovaujantis šio Priedo I skyriaus A dalyje nustatytais kriterijais. Tokį tikrinimą atlieka NATO agentūrų, atsakingų už NATO saugumo programos įgyvendinimą, kvalifikuoti pareigūnai. Taryba, jei ji priima sprendimą, kad reikia arba pageidautina, gali duoti nurodymą organizuoti specialų tikrinimą ir paskirti *ad hoc* tikrinimo grupę, kurią sudaro NATO karinių ir civilinių institucijų ar kiti kvalifikuoti pareigūnai. Apsilankymai valstybių narių karinėse ir civilinėse institucijose organizuojami bendradarbiaujant su atitinkamomis nacionalinėmis institucijomis.

B. Tikrinant įvertinami visi saugumo programos aspektai ir per trisdešimt dienų nuo tikrinimo pabaigos Generaliniam Sekretoriui išsiunčiama rašytinė ataskaita, kurioje nurodyti saugumo taisyklių įgyvendinimo trūkumai.

C. Generalinis Sekretorius pagal Susitarimą pateikia šių tikrinimų ataskaitų kopijas Jungtinėms Amerikos Valstijoms ir, vadovaudamasis kitomis Susitarimo nuostatomis bei prireikus – tikrintoms įstaigoms, atitinkamoms nacionalinėms saugumo institucijoms bei karinėms vadavietėms.

D. Per trisdešimt dienų nuo tikrinimo ataskaitos gavimo dienos atitinkamos tikrintos NATO arba nacionalinės institucijos Generaliniam Sekretoriui išsiunčia ataskaitą apie priemones, kurių imtasi tikrinimo ataskaitoje nurodytiems trūkumams ištaisyti. Išnagrinėjęs tikrinimo ataskaitą bei ataskaitą apie ištaisomąsias priemones, Generalinis Sekretorius, veikdamas Tarybos vardu, atitinkamai nurodo susijusioms nacionalinėms institucijoms, nuolatinei grupei ar civilinei institucijai, kokie tolesni veiksmai būtų reikalingi, kad būtų įgyvendinti NATO saugumo kriterijai ir šio Susitarimo nuostatos. Ataskaitų apie ištaisomąsias priemones kopijos bei pagal šią dalį Generalinio Sekretoriaus atsiųstų bet kokių pastabų kopijos platinamos laikantis tokios tvarkos, kuri pagal šio skyriaus C dalį nustatyta tikrinimų ataskaitoms.

E. Jei, įgyvendinus šio skyriaus D dalyje nurodytas priemones problema, dėl kurios būtini ištaisomieji veiksmai tikrinimo metu išaiškėjusiems trūkumams pašalinti, neišsprendžiama, Generalinis Sekretorius klausimą perduoda Tarybai ir jai rekomenduoja paskirti *ad hoc* tikrinimo grupę, kuri išnagrinėtų problemą ir pateiktų ataskaitą Tarybai, kad pastaroji po to galėtų imtis atitinkamų veiksmų.

ŠIAURĖS ATLANTO SUTARTIES ŠALIŲ SUSITARIMO DĖL BENDRADARBIAVIMO, SUSIJUSIO SU ATOMINE INFORMACIJA, ĮGYVENDINIMO ADMINISTRACINĖS PRIEMONĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

Tikslas

1. Šis dokumentas nustato Šiaurės Atlanto Sutarties Šalių susitarimo dėl bendradarbiavimo, susijusio su atomine informacija (toliau – Susitarimas), sudaryto 1964 m. birželio 18 d. Paryžiuje ir paskelbto dokumentu C–M(64)39, bei jo Techninio ir Saugumo priedų įgyvendinimo priemones. Šių priemonių negalima aiškinti taip, kad jos prieštarautų Susitarimui. Šiuo dokumentu panaikinamas dokumentas C–M(65)11, kuriame išdėstytos Susitarimo taikymo priemonės, ir dokumentas C–M(65)135, kuriame išdėstyti laikini detalesni nurodymai.

2. Jungtinės Karalystės Vyriausybė sutinka, kad atominė informacija, kurią Jungtinė Karalystė perduoda Šiaurės Atlanto Sutarties Organizacijai ir jos karinėms bei civilinėms institucijoms ir valstybėms narėms, būtų pranešama pagal šį Susitarimą. Kadangi tokia informacija perduodama retai, Jungtinės Karalystės Vyriausybė nusprendė nesiderėti dėl specialaus susitarimo, kaip numatoma Susitarimo II straipsnyje, ir sutinka, kad Jungtinės Karalystės parengtos atominės informacijos perdavimui būtų taikomos tos pačios sąlygos ir reikalavimai, kurie nurodyti Susitarime. Todėl Jungtinės Karalystės atominė informacija, kurią jos Vyriausybė praneša NATO, žymima ATOMAL, vadinama „JK atomine informacija“ (*UK ATOMIC Information*) ir apibūdinama užrašu, kaip nustatyta šio dokumento 38 punkto b papunkčio 2 dalyje. Ji saugoma ir kontroliuojama laikantis saugumo taisyklių ir reikalavimų, nustatytų dokumente C–M(64)39 ir šiame dokumente.

3. Šio dokumento tikslai:

a) palengvinti ATOMAL informacijos teikimą ir naudojimą, taikant atitinkamas saugumo priemones;

b) numatyti informacijos apie atominius ginklus įslaptinimo gaires;

c) nustatyti NATO struktūrų darbo tvarką, funkcijas ir atsakomybę tvarkant ir saugant ATOMAL informaciją.

4. Bet kuriems su ATOMAL informacija susijusiems klausimams, kurie šiame dokumente nėra konkrečiai aptariami, taikomos Susitarimo ir dokumento C–M(55)15(Final) nuostatos bei jo Priedėlis, pažymėtas slaptumo žyma „Konfidencialiai“.

5. Šiame dokumente nurodytos priemonės taikomos ir karo veiksmų metu, kiek tai yra praktiškai įmanoma, jei tos priemonės nedaro neigiamo poveikio NATO pajėgų operacinei galiai.

Sąvokos

6. **ATOMAL informacija** – tai informacija, pažymėta žyma „Riboto naudojimo duomenys“ (*Restricted Data*) arba žyma „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*), kurią Jungtinių Amerikos Valstijų Vyriausybė pagal Susitarimą arba pagal 1955 metų susitarimą, kurį jis pakeitė, teikia kitoms NATO struktūroms;

arba kaip „JK atominė informacija“ (*UK ATOMIC Information*), kurią Jungtinės Karalystės Vyriausybė pagal galiojančius susitarimus teikia kitoms NATO struktūroms.

7. **Griežtos apskaitos ATOMAL dokumentas** – tai dokumentas, pažymėtas slaptumo žyma „Visuotinės reikšmės visiškai slaptai ATOMAL“ (*COSMIC TOP SECRET ATOMAL*), „NATO Slaptai ATOMAL“ (*NATO SECRET ATOMAL*) arba „NATO Konfidencialiai ATOMAL“ (*NATO CONFIDENTIAL ATOMAL*), kuriam taikomi specialūs apribojimai pagal Susitarimo VI straipsnį ir kuris dėl to tampa griežtos apskaitos dokumentu pagal Saugumo priedo IV skyriaus D dalies nuostatas (šių dokumentų atgaminiai ir jais naudojantis parengti antriniai dokumentai taip pat yra griežtos apskaitos dokumentai).

8. **Atgaminys** – tai ATOMAL dokumento kopija arba vertimas, arba ištrauka, kurią sudaro viena ar kelios ištisinės pastraipos, diagramos ar lentelės, kuriose yra ATOMAL informacijos.

9. **Antrinis dokumentas** – tai dokumentas, kuriame yra ATOMAL informacijos, gautos iš vieno ar kelių ATOMAL dokumentų ar kitų šaltinių, ir kuris nėra atgaminys, kaip apibrėžta 8 punkte, nes jame netiesiogiai naudojama ATOMAL informacija. Šiame dokumente užrašai, daromi konferencijų, vizitų ar mokymo kursų metu, laikomi antriniais dokumentais.

10. **NATO struktūros:** NATO valstybės narės; Šiaurės Atlanto Taryba; Karinis komitetas; Sąjungininkų pajėgų Europoje vadavietė; Sąjungininkų pajėgų Lamanše vadavietė; Sąjungininkų pajėgų Atlante vadavietė; taip pat Kanados ir Jungtinių Amerikos Valstijų regioninė planavimo grupė.

11. **Saugumo institucija:** valstybės narės Nacionalinė saugumo institucija, įsteigta pagal dokumento C–M(55)15(Final) C priedėlio I skyriaus reikalavimus; Generalinis Sekretorius, veikiantis Šiaurės Atlanto Tarybos vardu ir jos vadovaujamas, taip pat santykiuose su Šiaurės Atlanto Taryba; Karinio komiteto pirmininkas; NATO vyriausieji vadai; taip pat Kanados ir Jungtinių Amerikos Valstijų regioninės planavimo grupės pirmininkas.

12. **ATOMAL centrinė registratūra:** centrinė kontroliuojanti įstaiga, kiekvienoje NATO struktūroje paskirta prašyti, gauti, registruoti, tvarkyti ir platinti ATOMAL dokumentus.

13. **ATOMAL antrinė registratūra:** kontroliuojanti įstaiga, atsakinga už ATOMAL dokumentų gavimą, registravimą, tvarkymą ir platinimą tam tikroje NATO struktūros dalyje.

14. **ATOMAL kontrolės punktas:** žemesnio už antrinę registratūrą lygio kontroliuojanti įstaiga, atsakinga už ATOMAL dokumentų gavimą, registravimą, tvarkymą ir platinimą įstaigos, kurią ji aptarnauja, personalui.

II skyrius

INFORMACIJOS PERDAVIMAS NATO STRUKTŪROMS IR ORGANIZACIJOS VIDUJE

Jungtinių Amerikos Valstijų informacijos, pažymėtos žyma „Riboto naudojimo duomenys“ (Restricted Data) arba „Buvę riboto naudojimo duomenys“ (Formerly Restricted Data), ir Jungtinės Karalystės atominės informacijos pirmasis perdavimas

15. Jungtinių Amerikos Valstijų Vyriausybė perduos NATO struktūroms Jungtinių Amerikos Valstijų informaciją, pažymėtą žyma „Riboto naudojimo duomenys“ (*Restricted Data*) arba „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*) ir NATO ATOMAL žymomis Jungtinių Amerikos Valstijų Vyriausybės ir atitinkamos NATO struktūros sutartais kanalais. Šis principas bus taikomas ir perduodant NATO struktūroms JK atominę informaciją. NATO struktūrų prašymai gauti Jungtinių Amerikos Valstijų informaciją, pažymėtą žyma „Riboto naudojimo duomenys“ (*Restricted Data*) arba „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*), arba Jungtinės Karalystės atominę informaciją, nustatytais kanalais perduodami atitinkamai Jungtinių Amerikos Valstijų arba Jungtinės Karalystės Vyriausybei. Atsižvelgiant į informacijos rengėją, Jungtinių Amerikos Valstijų arba Jungtinės Karalystės Vyriausybė informuos NATO saugumo biurą apie konkrečią informaciją, pažymėtą žyma „Riboto naudojimo duomenys“ (*Restricted Data*) arba „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*), arba JK atominę informaciją, nurodydama išsamią informaciją apie NATO struktūroms perduotus dokumentus. Kai NATO struktūroms perduodami dokumentai, kuriems taikomi specialūs apribojimai, NATO saugumo biurui pranešama apie kiekvieną perduotą dokumentą ir jam taikomus specialius apribojimus.

Generalinio Sekretoriaus atsakomybė

16. Generalinis Sekretorius, veikdamas Šiaurės Atlanto Tarybos vardu ir jos vadovaujamas, atsako už NATO saugumo programos dėl ATOMAL informacijos, perduotos pagal Susitarimą, apsaugos taikymo priežiūrą. Susitarimo saugumo priedo X skyriuje nustatyta tvarka jis užtikrina, kad NATO civilinėse ir karinėse institucijose bei nacionalinėse civilinėse ir karinėse institucijose būtų taikomos visos NATO saugumo programoje numatytos būtinos priemonės ATOMAL informacijai, kurią šios institucijos turi arba joms leidžiama turėti pagal Susitarimą, apsaugoti.

Saugumo institucijų atsakomybė

17. Kiekvienos NATO struktūros saugumo institucija atsako už ATOMAL saugumo programos įgyvendinimą atitinkamoje struktūroje. Vyriausiųjų NATO vadaviečių saugumo institucija atsako už šios programos įgyvendinimą visose pavaldžiose tarptautinėse vadavietėse ir agentūrose. Valstybės narės saugumo institucija atsako už ATOMAL saugumo programos įgyvendinimą visose nacio-

nalinėse civilinėse ir karinėse institucijose šalies viduje bei užsienyje[1].

Informacijos platinimas NATO struktūros viduje

18. Jei nėra specialių platinimą draudžiančių apribojimų, bet kuri iš NATO struktūrų, gavusi ATOMAL informaciją dokumentų forma, žodžiu arba naudojant vaizdines priemones, gali struktūros viduje perduoti tą informaciją asmenims (įskaitant personalą, kuriam dėl administracinių priežasčių leidžiama teikti šią informaciją), kuriems pagal šio dokumento III skyriaus 39 punkto nuostatas yra išduotas asmens patikimumo pažymėjimas ir kuriems įstaigos, kurioje jie tarnauja, įgalioto asmens sprendimu tokia informacija yra būtina jų pareigoms vykdyti (pagal principą „būtina žinoti“ (*need-to-know*).

19. Kiekvienoje NATO struktūroje ATOMAL informaciją kontroliuoja centrinė registratūra, antrinės registratūros ir kontrolės punktai, kaip nustatyta šiame dokumente. Centrinėms registratūroms, antrinėms registratūroms ir kontrolės punktams gali būti priskirtos dvigubos funkcijos – kontroliuoti ir ATOMAL dokumentus, ir dokumentus, pažymėtus žyma „Visuotinės reikšmės“ (COSMIC). Tačiau jei NATO struktūra mano, kad tai tikslinga, ji gali įsteigti atskiras ATOMAL ir COSMIC centrines registratūras, antrines registratūras ir kontrolės punktus. Bet kuriuo atveju ATOMAL dokumentai turi būti registruojami atskirai ir saugomi taip, kad jie būtų prieinami tik turinčiam tam teisę personalui.

Informacijos platinimas tarp NATO struktūrų

20. Jei nėra specialių tokį platinimą draudžiančių apribojimų, ATOMAL informacija keičiamasi per ATOMAL centrines registratūras, o gaunančių ir perduodančių struktūrų atitinkamos vadovybės leidimu tokia informacija gali būti keičiamasi ir per antrines registratūras bei kontrolės punktus. ATOMAL centrinių registratūrų, kurios veikia kaip centrinės kontroliuojančios įstaigos kiekvienoje NATO struktūroje, sąrašas pateikiamas II priede.

21. Kiekviena NATO struktūra nuolat teikia NATO saugumo biurui naujausią informaciją apie visas savo ATOMAL antrines registratūras ir kontrolės punktus, nurodydama, kurias antrines registratūras ir kontrolės punktus ji yra įgaliojusi prašyti, perduoti ir gauti ATOMAL informaciją tiesiai iš kitų NATO struktūrų. Kiekviena NATO struktūra kitoms atitinkamoms struktūroms praneša apie suteiktus tokius įgaliojimus. Visos centrinės registratūros ir tokius įgaliojimus turinčios antrinės registratūros bei kontrolės punktai keičiasi parašų pavyzdžiais.

22. NATO saugumo biuras tvarko ATOMAL centrinių registratūrų ir ATOMAL antrinių registratūrų bei kontrolės punktų, kurie yra įgalioti gauti, prašyti ar perduoti ATOMAL informaciją iš kitų NATO institucijų, naujausius sąrašus. Kasmet atnaujinamą centrinių registratūrų ir įgaliotų keistis ATOMAL informacija antrinių registratūrų bei kontrolės punktų sąrašą NATO saugumo biuras perduoda gavęs prašymą.

23. Vyriausiųjų NATO vadaviečių padaliniai įgaliojami keistis ATOMAL

[1] Žr. dokumento C–M(55)15(Final) C priedėlio I skyrių.

informacija su nacionalinėmis karinėmis institucijomis, kurios yra priskirtos ar numatytos priskirti jų vadovavimui. Vyriausieji NATO vadai, gavę atitinkamus prašymus, tokią informaciją perduoda jiems priskirtų ar numatytų priskirti institucijų vyriausiems vadams[2]. Vyriausiųjų NATO vadaviečių padaliniai valstybėms narėms praneša, kokios jų vadovavimui priklausančios nacionalinės karinės institucijos gali atlikti ATOMAL registratūros funkcijas. Valstybės narės, patikrinusios, ar nurodytos institucijos gali tinkamai taikyti saugumo priemones ATOMAL informacijai apsaugoti, paskiria šias institucijas ATOMAL antrinėmis registratūromis arba kontrolės punktais[3].

24. Perduodamas informaciją kitos NATO struktūros ATOMAL antrinei registratūrai ar kontrolės punktui, siuntėjas tuo pačiu metu arba kuo greičiau po to, bet ne vėliau kaip po 30 dienų gaunančios struktūros ATOMAL centrinei registratūrai pagal konkretų atitinkamų NATO struktūrų susitarimą pateikia perduotą informaciją, jei jos prašoma, arba registracijos numerius, kurie leidžia teisingai identifikuoti dokumentus, kuriuose yra ši informacija. ATOMAL informacija keičiamasi tarp NATO struktūrų tik tais atvejais, kai siuntėjas įsitikina, kad gavėjui ji būtina NATO uždaviniams vykdyti (pagal principą „būtina žinoti“ (*need-to-know*). Tokią informaciją gaunanti NATO struktūra atsako už jos saugojimą, kontrolę, apskaitą ir ataskaitas pagal šį dokumentą. (Prašymus gauti ATOMAL informaciją, kurią turi kita struktūra, NATO struktūros pateikia pagal šio dokumento I priede nustatytus reikalavimus.)

Specialūs apribojimai

25. Vadovaujantis Susitarimo VI straipsniu, Jungtinės Amerikos Valstijos savo perduodamai žodinei, vaizdinei ar rašytinei ATOMAL informacijai gali nustatyti specialius apribojimus. Tokie apribojimai pažymimi atitinkamomis žymomis dokumento tituliniame lape. Kai Jungtinių Amerikos Valstijų perduota informacija su specialiais apribojimais yra naudojama atgaminiuose ar antriniuose dokumentuose arba platinama žodžiu ar raštu, jai turi būti taikomi tie patys specialūs apribojimai. Bet kuri iš NATO struktūrų Jungtinių Amerikos Valstijų Vyriausybei gali paduoti prašymus leisti platinti ATOMAL informaciją netaikant specialių apribojimų (žr. IV priedą).

26. Jungtinės Karalystės Vyriausybė savo perduodamai žodinei, vaizdinei ar rašytinei JK atominei informacijai taip pat gali nustatyti specialius apribojimus.

[2] Valstybė narė, paskyrusi karines pajėgas, galinčias gauti ATOMAL informaciją, gali prašyti, kad tokios toms pajėgoms siunčiamos informacijos kopijos reguliariai tuo pačiu metu būtų siunčiamos jos paskirtai aukštesniajai nacionalinei institucijai tol, kol ji nenurodys kitaip.

[3] Turkijos valdžios institucijos pareiškia, kad dėl organizacinių priežasčių jos negali priimti 23 punkto. Turkijos valdžios institucijos yra paskyrusios Turkijos generalinį štabą (TGS) vienintele institucija, galinčia gauti, kontroliuoti ir platinti visą iš kitų NATO struktūrų gautą ATOMAL informaciją. Perduoti ATOMAL informaciją iš kurios nors NATO struktūros tiesiogiai Turkijos antrinėms registratūroms ir (arba) kontrolės punktams paprastai neleidžiama. Vykdydamas savo pareigas, TGS įsteigė Turkijos centrinę registratūrą (MUSAT), kuri yra vienintelė Turkijos registratūra, įgaliota gauti ATOMAL informaciją iš kitų NATO struktūrų ir joms tokią informaciją perduoti. Visas nurodytos tvarkos išimtis ir nukrypimus nuo jos dėl operacinių priežasčių atitinkama NATO struktūra turi derinti su Turkijos valdžios institucijomis.

Tokie apribojimai pažymimi atitinkamomis žymomis dokumento tituliniame lape. Kai Jungtinės Karalystės perduota informacija su specialiais apribojimais yra naudojama atgaminiuose ar antriniuose dokumentuose arba platinama žodžiu ar raštu, jai turi būti taikomi tie patys specialūs apribojimai. Bet kuri iš NATO struktūrų Jungtinės Karalystės Vyriausybei gali paduoti prašymus leisti platinti JK atominę informaciją netaikant specialių apribojimų.

ATOMAL registracijos sistema

27. Kiekvienai ATOMAL centrinei registratūrai, antrinėms registratūroms ir kontrolės punktams vadovauja ATOMAL kontrolės pareigūnas ir prireikus jo pavaduotojai.

28. **ATOMAL centrinės registratūros:** ATOMAL centrinė registratūra įsteigiama kiekvienoje NATO struktūroje ir apie ją pranešama NATO saugumo biurui. NATO struktūra savo ATOMAL centrinę registratūrą gali keisti bet kuriuo metu, apie tai pranešusi NATO saugumo biurui ir visoms kitoms ATOMAL centrinėms registratūroms.

29. ATOMAL centrinė registratūra atlieka, *inter alia*, šias funkcijas:

a) teikia prašymus ir gauna ATOMAL dokumentus iš Jungtinių Amerikos Valstijų ir iš kitų ATOMAL centrinių registratūrų, antrinių registratūrų ir kontrolės punktų;

b) kontroliuoja prieigą prie savo saugomos ATOMAL informacijos;

c) tvarko griežtos apskaitos ATOMAL dokumentų apskaitą;

d) perduoda ATOMAL dokumentus tos pačios NATO struktūros ATOMAL antrinėms registratūroms ir kontrolės punktams;

e) perduoda ATOMAL dokumentus kitų NATO struktūrų ATOMAL centrinėms registratūroms ir įgaliotoms ATOMAL antrinėms registratūroms bei kontrolėms punktams;

f) tvarko tiesiogiai aptarnaujamų institucijų (t. y. institucijų, kurių tiesiogiai neaptarnauja antrinė registratūra ar kontrolės punktas) asmenų, kuriems leidžiama susipažinti su ATOMAL informacija, naujausius sąrašus;

g) teikia patarimus atitinkamoms nurodytoms institucijoms dėl tiesiogiai jai pavaldžių antrinių registratūrų ir kontrolės punktų įsteigimo ar likvidavimo;

h) tvarko jai tiesiogiai pavaldžių ATOMAL antrinių registratūrų ir kontrolės punktų sąrašą;

i) tvarko kitų NATO struktūrų ATOMAL antrinių registratūrų ir kontrolės punktų, su kuriais ji ar jai pavaldžios įstaigos yra įgaliotos keistis ATOMAL informacija, sąrašą;

j) atlieka III skyriaus 48 ir 49 punktuose nurodytas koordinavimo funkcijas, susijusias su žodiniais ir vaizdiniais ATOMAL informacijos pranešimais.

30. **ATOMAL antrinės registratūros:** ATOMAL antrines registratūras prireikus steigia ATOMAL centrinės registratūros, atsižvelgdamos į šiuos veiksnius:

a) ATOMAL dokumentų kiekį;

b) saugojimo reikalavimus;

c) geografines ir ryšių problemas.

31. ATOMAL antrinė registratūra atlieka, *inter alia*, šias funkcijas:

a) gauna ATOMAL dokumentus iš ją įsteigusios ATOMAL centrinės registratūros ir, jei turi tokius įgaliojimus, iš kitų tos pačios NATO struktūros ATOMAL antrinių registratūrų bei kontrolės punktų bei, jei turi tokius įgaliojimus, teikia prašymus ir gauna tokius dokumentus iš Jungtinių Amerikos Valstijų ir iš kitų NATO struktūrų ATOMAL centrinių registratūrų, antrinių registratūrų bei kontrolės punktų;

b) kontroliuoja prieigą prie savo saugomos ATOMAL informacijos;

c) tvarko griežtos apskaitos ATOMAL dokumentų apskaitą;

d) perduoda ATOMAL dokumentus ją įsteigusiai ATOMAL centrinei registratūrai ir, jei turi tokius įgaliojimus, tos pačios NATO struktūros ATOMAL antrinėms registratūroms bei kontrolės punktams;

e) jei turi tokius įgaliojimus, perduoda ATOMAL dokumentus kitų NATO struktūrų įgaliotoms ATOMAL centrinėms registratūroms, antrinėms registratūroms ir kontrolės punktams;

f) tvarko tiesiogiai aptarnaujamų institucijų (t. y. institucijų, kurių tiesiogiai neaptarnauja kontrolės punktas) asmenų, kuriems leidžiama susipažinti su ATOMAL informacija, naujausius sąrašus;

g) jei turi tokius įgaliojimus, teikia patarimus atitinkamoms nurodytoms institucijoms dėl tiesiogiai jai pavaldžių kontrolės punktų įsteigimo ar likvidavimo;

h) tvarko kitų NATO struktūrų ATOMAL antrinių registratūrų ir kontrolės punktų, su kuriais ji ar jai pavaldžios įstaigos yra įgaliotos tiesiogiai keistis ATOMAL informacija, sąrašą, kartu saugodama kontrolės personalo parašų pavyzdžius;

i) atlieka III skyriaus 48 ir 49 punktuose nurodytas koordinavimo funkcijas, susijusias su žodiniais ir vaizdiniais ATOMAL informacijos pranešimais.

32. **ATOMAL kontrolės punktai:** ATOMAL kontrolės punktus galima steigti aptarnauti institucijoms, kurių ATOMAL centrinė registratūra arba antrinė registratūra tiesiogiai neaptarnauja. Nedažnam ir trumpam susipažinimui su ATOMAL dokumentais nebūtina steigti ATOMAL kontrolės punktą, jei taikoma tvarka užtikrina, kad dokumentus ir toliau kontroliuoja atitinkama ATOMAL centrinė registratūra, antrinė registratūra ar įsteigtas kontrolės punktas.

33. ATOMAL kontrolės punktas atlieka, *inter alia*, šias funkcijas:

a) gauna ATOMAL dokumentus iš jį įsteigusios ATOMAL centrinės registratūros arba antrinės registratūros ir, jei turi tokius įgaliojimus, teikia prašymus ir gauna tokius dokumentus iš kitų ATOMAL centrinių registratūrų, antrinių registratūrų ir kontrolės punktų;

b) kontroliuoja prieigą prie savo saugomos ATOMAL informacijos;

c) tvarko griežtos apskaitos ATOMAL dokumentų apskaitą;

d) perduoda ATOMAL dokumentus jį įsteigusiai ATOMAL centrinei registratūrai arba antrinei registratūrai ir, jei turi tokius įgaliojimus, kitoms ATOMAL centrinėms registratūroms, antrinėms registratūroms ir kontrolės punktams;

e) tvarko tiesiogiai aptarnaujamų institucijų asmenų, kuriems leidžiama susipažinti su ATOMAL informacija, naujausius sąrašus;

f) persiunčia nebereikalingus ATOMAL dokumentus jį įsteigusiai ATOMAL centrinei registratūrai arba antrinei registratūrai;

g) tvarko kitų NATO struktūrų ATOMAL antrinių registratūrų ir kontrolės

punktų, su kuriais jis yra įgaliotas tiesiogiai keistis ATOMAL informacija, sąrašą, kartu saugodamas kontrolės personalo parašų pavyzdžius;

h) tvarko nacionalinių antrinių registratūrų ir kontrolės punktų, su kuriais yra įgaliotas tiesiogiai keistis ATOMAL informacija, sąrašą, kartu saugodamas kontrolės personalo parašų pavyzdžius;

i) jei turi tokius įgaliojimus, atlieka III skyriaus 48 ir 49 punktuose nurodytas koordinavimo funkcijas, susijusias su žodiniais ir vaizdiniais ATOMAL informacijos pranešimais toje pačioje struktūroje arba santykiuose su kitomis NATO struktūromis.

III SKYRIUS
IŠSAMIOS PROCEDŪROS

ATOMAL informacijos įslaptinimas

34. Visuomet būtina laikytis įslaptinimo, kurį pagal Susitarimą perduodamai ATOMAL informacijai, atsižvelgiant į jos rengėją, taiko Jungtinių Amerikos Valstijų arba Jungtinės Karalystės Vyriausybė. Informacijos apie atominius ginklus įslaptinimo gairės pateikiamos III priede.

35. Atgaminių įslaptinimo lygis turi būti toks pat kaip ir dokumento originalo arba atskirų atgamintų dalių įslaptinimo lygis, jei Jungtinių Amerikos Valstijų arba Jungtinės Karalystės Vyriausybė nenumato kitaip.

36. Jei nėra Jungtinių Amerikos Valstijų ir (arba) Jungtinės Karalystės Vyriausybės nustatytų konkrečių įslaptinimo gairių, antrinių dokumentų įslaptinimo lygis turi būti bent toks pat, kaip ir dokumentų (arba atskirų įslaptintų dalių), kuriuose esanti informacija naudojama antriniame dokumente.

37. Klausimai, susiję su informacijos įslaptinimu, pateikiami Jungtinių Amerikos Valstijų ir (arba) Jungtinės Karalystės Vyriausybei, atsižvelgiant į informacijos rengėją.

Dokumentų žymėjimas

38. Visi dokumentai, kuriuose yra ATOMAL informacijos, žymimi taip:

a) kiekvieno puslapio viršuje ir apačioje įrašomos žymos: „Visuotinės reikšmės visiškai slaptai ATOMAL“ (*COSMIC TOP SECRET ATOMAL*), „NATO Slaptai ATOMAL“ (*NATO SECRET ATOMAL*) arba „NATO Konfidencialiai ATOMAL“ (*NATO CONFIDENTIAL ATOMAL*);

b) įrašomas vienas iš šių teiginių:

1) „Šiame dokumente esanti Jungtinių Amerikos Valstijų atominė informacija („Riboto naudojimo duomenys“ (*Restricted Data*) arba „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*) yra perduota pagal 1964 m. birželio 18 d. pasirašytą NATO susitarimą dėl bendradarbiavimo, susijusio su atomine informacija, ir turi būti atitinkamai saugoma“[4] ; arba

2) „Šiame dokumente yra JK atominės informacijos. Ši informacija yra per-

[4] Dokumentams, perduotiems pagal 1955 m. NATO susitarimą, dabar taikomos 1964 m. Susitarimo nuostatos.

duota Šiaurės Atlanto Sutarties Organizacijai, įskaitant jos karines bei civilines institucijas ir valstybes nares, su sąlyga, kad gaunanti institucija jos neperduos jokiai kitos šalies institucijai, vyriausybei ar piliečiui ir jokios kitos organizacijos narei be Jos Didenybės Vyriausybės Jungtinėje Karalystėje leidimo“; arba

3) antrinių dokumentų, kuriuose yra ir Jungtinių Amerikos Valstijų, ir Jungtinės Karalystės parengtos atominės informacijos, atveju dokumento tituliniame lape įrašomi abu teiginiai, nurodyti 38 punkto b papunkčio 1 dalyje ir b papunkčio 2 dalyje;

c) dokumentai, perduoti su specialiais apribojimais, atitinkamai pažymimi dokumento tituliniame lape, nurodant, atitinkamai, Jungtinių Amerikos Valstijų ir (arba) Jungtinės Karalystės Vyriausybės nustatytą apribojimą;

d) jei draudžiama daryti ATOMAL dokumento atgaminius ar naudoti jį rengiant antrinius dokumentus, dokumentas yra atitinkamai pažymimas;

e) apskaitos tikslais kiekvienas griežtos apskaitos ATOMAL dokumentas privalo turėti registracijos numerį, datą, ir jo egzemplioriai turi būti sunumeruoti. Prireikus apskaitos tikslais galima taikyti papildomą žymėjimą;

f) perduodant dokumentus elektroniniu būdu, atitinkami žodžiai „Visuotinės reikšmės visiškai slaptai ATOMAL“ (*COSMIC TOP SECRET ATOMAL*), „NATO Slaptai ATOMAL“ (*NATO SECRET ATOMAL*) arba „NATO Konfidencialiai ATOMAL“ (*NATO CONFIDENTIAL ATOMAL*) perduodami kiekvieno pranešimo pradžioje, po jų nurodant taikytinus specialius apribojimus. Kai pranešimo tekstas yra perduodamas dokumento forma, jis žymimas taip pat, kaip kiti ATOMAL dokumentai;

g) dokumentų su ATOMAL informacija, kurie buvo išleisti be jokių ATOMAL žymų, turėtojai privalo šiuos dokumentus pažymėti pirmiau nurodytais būdais, kai jiems yra pranešama, kad tai yra ATOMAL dokumentai. Gavus tokį pranešimą, patikrinama, ar yra padaryta šių dokumentų atgaminių ir ar yra remiantis juose esančia ATOMAL informacija parengtų antrinių dokumentų; jei tokių dokumentų yra, jie pažymimi pirmiau nurodytu būdu;

h) turėtojas, kuris mano, kad jo saugomame NATO dokumente be ATOMAL žymos yra ATOMAL informacijos, saugo tą dokumentą kaip ATOMAL dokumentą ir paprašo dokumento rengėjo paaiškinimo ir rekomendacijų;

i) kai dokumentų rengėjai nustato, kad dokumentai su ATOMAL informacija nėra tinkamai pažymėti, jie taiko tokiems dokumentams šiame dokumente nustatytas kontrolės priemones, pažymi ATOMAL dokumentus tinkamu būdu ir atitinkamai praneša visiems gavėjams, kam buvo išsiųstos tokių dokumentų kopijos. Gavusi tokius pranešimus, kiekviena centrinė registratūra, antrinė registratūra ar kontrolės punktas imasi tokių pat veiksmų ir savo ruožtu praneša kitiems gavėjams;

j) klausimai dėl dokumentuose esančios ATOMAL informacijos pateikiami Jungtinių Amerikos Valstijų ir (arba) Jungtinės Karalystės Vyriausybei, atsižvelgiant į juose esančios informacijos rengėją.

Asmens patikimumo pažymėjimai

39. Asmens patikimumo pažymėjimą (kuris patvirtina asmens teisę gauti ATOMAL informaciją) išduoda ir informacijos, su kuria asmuo turi teisę susipažinti, slaptumo lygį nustato atitinkamo asmens valstybės vyriausybės atsakinga institucija. Asmens patikimumo pažymėjimus galima išduoti tik ištyrus ir patikrinus informaciją pagal Susitarimo Saugumo priedo II skyrių. Priimdama sprendimą dėl asmens patikimumo, atsakinga institucija, gavusi atitinkamą asmenį įdarbinusios įstaigos prašymą, jeigu šiam asmeniui reikia arba tikėtina, kad reikės, susipažinti su ATOMAL informacija, privalo išduoti asmens patikimumo pažymėjimą, kuriame patvirtinama teisė susipažinti su ATOMAL informacija ir informacijos, su kuria leidžiama susipažinti, įslaptinimo lygis. Tokių pažymėjimų kopijas saugo už jų išdavimą atsakinga institucija ir įstaiga, kurioje asmuo dirba.

Galimybė susipažinti su informacija

40. Galimybė susipažinti su tam tikra ATOMAL informacija priklauso nuo vyriausybės išduotame asmens patikimumo pažymėjime nurodyto informacijos, su kuria leidžiama susipažinti, įslaptinimo lygio, įstaigos, kurioje asmuo dirba, įgalioto asmens sprendimo, ar jam reikia su ta informacija susipažinti pagal principą „būtina žinoti“ (*need-to-know*), ir galimų specialių informacijos platinimo apribojimų. Atsižvelgiant į veiklos sritį, ATOMAL centrinė registratūra, antrinė registratūra arba kontrolės punktas tvarko naujausią asmenų, kuriems buvo suteikta teisė susipažinti su ATOMAL informacija, sąrašą. Tokiuose sąrašuose taip pat nurodomi tie asmenys, kuriems leista susipažinti su ATOMAL informacija, perduota taikant specialius apribojimus.

Susipažinimo su informacija registravimas

41. Gavęs bet kurį dokumentą, pažymėtą slaptumo žyma „Visuotinės reikšmės visiškai slaptai ATOMAL“ (*COSMIC TOP SECRET ATOMAL*), dokumento gavėjas prideda susipažinimo su informacija registracijos lapą. Toks pat susipažinimo su ATOMAL informacija lapas taip pat pridedamas prie visų dokumentų, pažymėtų slaptumo žymomis „NATO Slaptai ATOMAL“ (*NATO SECRET ATOMAL*) ir „NATO Konfidencialiai ATOMAL“ (*NATO CONFIDENTIAL ATOMAL*), kuriems taikomi specialūs apribojimai. Visi asmenys, kuriems buvo suteikta galimybė susipažinti su tokių dokumentų turiniu, pasirašo susipažinimo su informacija registracijos lape.

Apskaita

42. ATOMAL centrinės registratūros, antrinės registratūros ir kontrolės punktai tvarko įrašus apie visų griežtos apskaitos ATOMAL dokumentų gavimą, atgaminius, antrinius dokumentus, perdavimą, slaptumo žymų pakeitimus ir sunaikinimą. ATOMAL dokumentų apskaitos įrašai tvarkomi atskirai nuo kitų įslaptintų dokumentų kontrolės įrašų. Tokie įrašai taip pat aiškiai nurodo tuos ATOMAL dokumentus, kuriuose yra JK atominės informacijos.

Atgaminiai

43. NATO struktūra prireikus gali atgaminti Jungtinių Amerikos Valstijų jai perduotus dokumentus, pažymėtus slaptumo žymomis „NATO Slaptai ATOMAL“ (*NATO SECRET ATOMAL*) ir „NATO Konfidencialiai ATOMAL“ (*NATO CONFIDENTIAL ATOMAL*), jei nėra konkrečių priešingų Jungtinių Amerikos Valstijų Vyriausybės nurodymų[5] . NATO struktūros parengtus antrinius ATOMAL dokumentus, pažymėtus slaptumo žymomis „NATO Slaptai ATOMAL“ (*NATO SECRET ATOMAL*) ir „NATO Konfidencialiai ATOMAL“ (*NATO CONFIDENTIAL ATOMAL*), prireikus galima atgaminti, jei juos parengusi NATO struktūra nėra nustačiusi konkrečių priešingų nurodymų. Dokumentus, pažymėtus slaptumo žyma „Visuotinės reikšmės visiškai slaptai ATOMAL“ (*COSMIC TOP SECRET ATOMAL*), galima atgaminti tik tokiu mastu, kokiu leidžia juos parengusi struktūra. Tačiau NATO struktūroms leidžiama daryti vertimus tiek, kiek reikia kitiems atgaminimo poreikiams nustatyti, jei tokių poreikių yra.

44. ATOMAL dokumentų, kuriuose yra JK atominės informacijos, negalima atgaminti, jei Jungtinės Karalystės Vyriausybė nėra nurodžiusi kitaip.

45. Visais atvejais ATOMAL dokumentų atgaminiai žymimi tokiomis pat žymomis, kaip dokumento originalas arba atgaminta dalis, kaip nurodyta 38 punkte, ir apskaitomi, kaip nurodyta 42 punkte.

Antriniai dokumentai

46. Kiekviena NATO struktūra prireikus gali ATOMAL informaciją įtraukti į antrinius dokumentus, jei Jungtinių Amerikos Valstijų ir (arba) Jungtinės Karalystės Vyriausybė netaiko specialių apribojimų dėl ATOMAL informacijos naudojimo antriniams dokumentams. Dokumentai, kurių negalima naudoti antriniams dokumentams, turi būti atitinkamai pažymėti.

47. Visais atvejais antriniai dokumentai žymimi, kaip nurodyta 38 punkte, ir apskaitomi, kaip nurodyta 42 punkte.

Žodiniai ir vaizdiniai pranešimai

48. Asmenys, įtraukti į tos pačios ar kitos NATO struktūros įgaliotų ATOMAL centrinių registratūrų, antrinių registratūrų ir kontrolės punktų asmenų, turinčių teisę susipažinti su tokia informacija, sąrašus, gali perduoti vienas kitam žodinę ir vaizdinę ATOMAL informaciją, kuriai netaikomi specialūs tokį platinimą draudžiantys apribojimai, jei atitinkamos ATOMAL centrinės registratūros ir, jei turi tokius įgaliojimus, antrinės registratūros bei kontrolės punktai tinkamai koordinuoja savo veiklą informacijos apsaugos tikslais ir užtikrina, kad informacijos gavėjams yra tinkamai suteikta teisė susipažinti su atitinkama informacija (žr. I priedą dėl prašymų dėl vizitų tvarkos).

49. Po kiekvieno tokio NATO struktūrų informacijos perdavimo informaciją

[5] Jungtinės Amerikos Valstijos pagal Susitarimo Saugumo priedo IV skyriaus E dalį patvirtino galimybę atgaminti dokumentus, pažymėtus slaptumo žymomis „NATO Slaptai ATOMAL“ (*NATO SECRET ATOMAL*) ir „NATO Konfidencialiai ATOMAL“ (*NATO CONFIDENTIAL ATOMAL*), išskyrus dokumentus, kuriems taikomi specialūs apribojimai, kurie atgaminti draudžia.

perduodančios NATO struktūros raštu parengia naują informaciją, kuria pasikeista, bei jos gavėjų pavardžių sąrašą ir šių dokumentų kopijas per 30 dienų pateikia gaunančioms struktūroms. Gaunančioms struktūroms skirtos kopijos siunčiamos į ATOMAL centrines registratūras arba antrines registratūras ar kontrolės punktus, aptarnaujančius įstaigą, kurioje dirba gaunantis informaciją asmuo. Tokie dokumentai kontroliuojami ir apskaitomi šiame dokumente nustatyta tvarka.

ATOMAL pratybų dokumentai

50. ATOMAL informacija, perduota pratybų tikslais, tvarkoma, žymima ir kontroliuojama vadovaujantis ATOMAL dokumentams nustatytais reikalavimais. Tačiau apskaitos įrašai turi būti saugomi atskirai.

51. Pratybų dokumentai paprastai sunaikinami ne vėliau kaip po 30 dienų nuo pratybų pabaigos. Visi kontrolės įrašai, sunaikinimo liudijimai, žurnalai, rodyklės kortelės ir kiti susiję dokumentai paliekami saugoti ATOMAL kontroliuojančioje įstaigoje.

52. Pratybų dokumentai, kurie nesunaikinami per 30 dienų nuo pratybų pabaigos, apskaitomi kaip visi kiti ATOMAL dokumentai.

Saugumo mokymas

53. Kiekvienoje NATO struktūroje sudaroma saugumo mokymo programa, kuria siekiama užtikrinti, kad visi turintys teisę susipažinti su ATOMAL informacija asmenys:

a) prieš gaudami informaciją, būtų specialiai instruktuojami apie taikytinus ATOMAL informacijos saugumo reikalavimus bei nuostatus ir pasirašytų atitinkamą dokumentą;

b) būtų reguliariai pakartotinai instruktuojami ir pasirašytų atitinkamą dokumentą;

c) baigę eiti su ATOMAL informacija susijusias pareigas, dalyvautų pokalbyje, kuriame būtų pabrėžiama, kad jų tolesnė atsakomybė už ATOMAL informacijos apsaugą ir saugumą nesibaigia, ir pasirašytų dokumentą, kuriuo patvirtintų, kad dalyvavo tokiame pokalbyje ir suprato savo tolesnę atsakomybę.

Ataskaitos

54. Iki kovo 31 d. kiekvienos NATO struktūros ATOMAL centrinė registratūra pateikia metinę ataskaitą NATO saugumo biurui, kuris ją išnagrinėjęs teikia Jungtinėms Amerikos Valstijoms. NATO saugumo biuras išnagrinėja ataskaitas ir imasi, jo nuomone, tinkamų veiksmų. Tokioje ataskaitoje turi būti:

a) centrinės registratūros, antrinės registratūros ir kontrolės punkto sudaryti visų gruodžio 31 d. turėtų dokumentų, pažymėtų slaptumo žyma „Visuotinės reikšmės visiškai slaptai ATOMAL“ (*COSMIC TOP SECRET ATOMAL*), visų dokumentų, pažymėtų slaptumo žyma „NATO Slaptai ATOMAL“ (*NATO SECRET ATOMAL*), ir visų dokumentų, pažymėtų slaptumo žyma „NATO Konfidencialiai ATOMAL“ (*NATO CONFIDENTIAL ATOMAL*) su specialiais apribojimais, sąrašai ir visų per ataskaitinį laikotarpį gautų dokumentų kiekiai

pagal slaptumo žymas, nesvarbu, ar jie yra dar turimi ar išplatinti, ar sunaikinti. Skaičiuojant dokumentus, įskaičiuojama kiekviena dokumento kopija;

b) pažyma, patvirtinanti, kad yra atliktas visų griežtai apskaitomų ATOMAL dokumentų, kuriuos turi NATO institucija, fizinis patikrinimas;

c) visų dingusių ATOMAL dokumentų sąrašas su datomis, kada apie juos buvo skubiai pranešta, kaip reikalaujama 61 punkte.

Tikrinimai

55. Tikrinimo programa – pagrindinė priemonė, kuria nustatoma, ar tinkamai yra laikomasi ATOMAL informacijos saugumo priemonių.

56. **NATO struktūros saugumo institucijų tikrinimai:** kiekvienoje NATO struktūroje sudaroma tikrinimų programa, siekiant užtikrinti, kad visos ATOMAL centrinės registratūros, antrinės registratūros ir kontrolės punktai, turintys ATOMAL informacijos, būtų reguliariai tikrinami, ne rečiau kaip kartą per 12 mėnesių. Toms institucijoms, kurios yra įgaliotos saugoti ATOMAL informaciją, bet tokios informacijos neturi, tikrinimų dažnumą nustato kiekviena NATO struktūra, atsižvelgdama į reguliaraus NATO įslaptintos informacijos apsaugos tikrinimo programas (žr. dokumento C–M(55)(Final) C priedėlio 12 punktą ir 20 punkto d papunktį). Tačiau tam, kad veiklos reikalavimai būtų vykdomi realiu laiku, atitinkamos institucijos (tais metais, kai jos nėra tikrinamos) kiekvienos NATO struktūros saugumo instituciją kasmet užtikrina, kad būtinos ATOMAL informacijos saugumo priemonės tebėra veiksmingos. Tikrinimus atlieka kvalifikuoti pareigūnai, ir prireikus imamasi veiksmingų bei skubių ištaisomųjų priemonių. Už tikrinimus atsako:

a) valstybių narių saugumo institucijos, atsakingos už visų nacionalinių civilinių ir karinių institucijų šalies viduje ir užsienyje tikrinimą;

b) NATO karinių institucijų vadai, atsakingi už visas savo pavaldžias tarptautines vadavietes ir institucijas.

57. Tikrintojų grupės parengia tikrinimų rašytines ataskaitas ir kiekvieną ataskaitą nedelsdamos nustatytais kanalais išsiunčia NATO struktūrų saugumo institucijoms, kad per 30 dienų nuo tikrinimo pabaigos ataskaitos kopija būtų persiųsta NATO saugumo biurui. Tų institucijų, kurios gautų ATOMAL informaciją tik nenumatytu atveju, tikrinimo ataskaitas reikia parengti, bet NATO saugumo biurui siųsti nereikia. Institucijų, saugančių JK atominę informaciją, atskiros tikrinimo ataskaitos rengti nereikia. Prireikus rašytinėje ATOMAL tikrinimo ataskaitoje nurodomi turimi dokumentai, kuriuose yra tokios informacijos.

58. NATO saugumo biurui siunčiamos tikrinimų ataskaitos turėtų būti parengtos viena iš oficialiųjų NATO kalbų. Jei dėl kalbos kyla sunkumų, NATO struktūros 50 proc. ataskaitų gali siųsti anglų arba prancūzų kalba, o 50 proc. – originalo kalba, tačiau jos turi užtikrinti, kad ataskaita dėl kiekvienos tikrintos institucijos NATO oficialiąja kalba būtų parengiama kas antri metai.

59. Tikrinimas nelaikomas baigtu tol, kol tikrinimo grupė nepateikia ataskaitos. Tačiau visais atvejais ataskaita turi būti baigta ir pateikta NATO saugumo biurui per 90 dienų nuo tikrinimo pradžios. Per 30 dienų nuo ataskaitos gavimo dienos tikrintos institucijos arba aukštesnės institucijos atitinkami įgalioti asmenys išsiunčia atitinkamos NATO struktūros saugumo institucijai ataskaitą apie

tai, kokių priemonių imtasi tikrinimo ataskaitoje nurodytiems trūkumams ištaisyti. Ataskaitos apie ištaisomąsias priemones kopija siunčiama NATO saugumo biurui. NATO saugumo biuras išnagrinėja ir įvertina šias ataskaitas dėl atitikimo šiam dokumentui ir bendriems NATO saugumo tikslams. Jei NATO saugumo biuras mano, kad tikrinimas ar ištaisomosios priemonės yra nepakankamos arba kad didelė dalis kitų saugumo reikalavimų yra neįvykdyta, jis nedelsdamas konsultuojasi su atitinkama NATO struktūra, siekdamas nustatyti, kokie tolesni veiksmai būtų reikalingi.

60. **NATO saugumo biuro tikrinimai:** NATO saugumo biuras tikrina NATO struktūras, turinčias ATOMAL informacijos, ne rečiau kaip kartą per 12 mėnesių tokiu mastu, kokio reikia siekiant nustatyti, ar tos struktūros taiko pakankamas vykdymo ir įgyvendinimo priemones. NATO saugumo biuro tikrinimo programoje numatomi atrankiniai tikrinimai, derinant su atitinkamomis NATO struktūrų įvairaus lygio saugumo institucijomis, kad nustatytus rezultatus būtų galima patvirtinti. NATO saugumo biuras taip pat atlieka tikrinimus Tarybos nurodymu. NATO saugumo biuro tikrinimų ataskaitos siunčiamos atitinkamų NATO struktūrų saugumo institucijoms, kurios turi laiku pateikti ataskaitas apie ištaisomąsias priemones.

Informacijos saugumo pažeidimai ir neteisėtas atskleidimas

61. Jei ATOMAL neteisėtai atskleidžiama praradus dokumentus ar kokiu nors kitu būdu arba jei manoma, kad ji yra neteisėtai atskleista, NATO struktūros atitinkama institucija nedelsdama praneša NATO saugumo biurui. Išsamios procedūros ir dalyvaujančių institucijų pareigos nustatytos V priede.

I PRIEDAS

Prašymai gauti ATOMAL informaciją

1. Prašymai gauti ATOMAL informaciją Jungtinėms Amerikos Valstijoms arba kitoms NATO struktūroms pateikiami raštu, laikantis II skyriaus 24 punkto ir III skyriaus 48 punkto reikalavimų. Juose nurodoma ši informacija:

a) prašomos informacijos apibūdinimas;

b) tikslas, kuriam reikalinga informacija, ir pageidaujamas jos platinimo mastas;

c) prašomas kopijų skaičius;

d) bet kuri kita informacija, kuri gali būti naudinga nagrinėjant prašymą.

2. Prašymai gauti JK atominę informaciją raštu pateikiami adresu: *AD/Sc(Nuc)2/ATOMIC CONTROL OFFICE, Ministry of Defence, Main Building, Whitehall, London*, per oficialų JK atstovą NATO civilinėse ir karinėse institucijose; juose turi būti šio Priedo 1 punkte nurodyta informacija.

Vizitai

3. Prieš vizitus į NATO struktūras, susijusius su ATOMAL informacija, būtina atitinkamai NATO struktūrai raštu pateikti prašymą dėl vizito laikantis II skyriaus 24 punkto ir III skyriaus 48 punkto reikalavimų. Prašyme nurodoma ši informacija:

a) pavadinimas ir veiklos vieta, kurią norima aplankyti, ir, jei žinoma, konkretus asmuo, su kuriuo pageidaujama susitikti;

b) siūlomos vizito datos;

c) vizito tikslas;

d) kiekvieno atvykstančiojo pavardė ir asmens patikimumo pažymėjimas;

e) pareiškimas, kad kiekvienam atvykstančiajam būtina atitinkama informacija (pagal principą „būtina žinoti“ (*need-to-know*).

II PRIEDAS

ATOMAL centrinių registratūrų, kurios NATO struktūrose veikia kaip centrinės ATOMAL programos kontroliuojančios įstaigos, sąrašas

1. ATOMAL informacijos suteikimą kiekvienoje valstybėje narėje administruoja toliau nurodytos institucijos:

Belgija

Office de Coordination Atomique Belgique (Bruxelles),
Etat-major général,
Quartier Reine Elisabeth,
rue d'Evere, 1140 Bruxelles
Telegrafo adresas: MOD BELGIUM – OCABE(B)

Kanada

Department of National Defence,
ATOMAL Control Officer,
National Defence Headquarters,
Ottawa, Ontario, Canada K1A OK2
Telegrafo adresas: NDHQ – OTTAVA

Danija

Ministry of Defence,
7th Office,
ATOMAL Control Office,
Slotshomsgade 10, DK-1216, Copenhagen K.
Telegrafo adresas: MOD DENMARK

Prancūzija

Chef du Bureau central COSMIC/ATOMAL,
Service de Sécurité de Défense,
Secrétariat Général de la Défense nationale,
51 Bd de Latour-Maubourg, 75700 Paris – France
Telegrafo adresas: MOD FRANCE

Vokietija

Federal Minister of Defence,
COSMIC and ATOMAL Central Agency,
Attn. Control Officer,
53 Bonn
Telegrafo adresas: MOD BONN – COSMIC and ATOMAL Central Registry

Graikija

ATOMAL Central Registry,
Supreme Hellenic Armed Forces Command,
SHAFC Building, Holargos, Athens
Telegrafo adresas: ATOMAL Central Registry – SHAFC

Islandija

Ministry of Foreign Affairs,
Reykjavik

Italija

Presidency of Council of Ministers,
National Security Authority,
Central Security Office,
ATOMAL Central Registry,
Rome
Telegrafo adresas: MOD ITALY – ANS-UCS I

Liuksemburgas

Bureau d'ordre central ATOMAL au
Haut-Commissariat de la Protection nationale,
5 rue Auguste Lumlčre, Luxembourg

Nyderlandai

Ministry of Defence,
Chief Defence Staff,
Room A 210, Plein 4, the Hague
Telegrafo adresas: MOD NETHERLANDS – CDS

Norvegija

Ministry of Defence,
ATOMAL Central Registry,
Oslo Department,
Oslo 1, Norway
Telegrafo adresas: MOD NORWAY

Portugalija

Estado Major General das Forēas Armadas (EMGFA)
Registo Cenral NATO, Lisboa – Rastelo

Turkija

ATOMAL Central Regisry,
TGS, MUSAT,

Ankara
Telegrafo adresas: MOD TURKEY

Jungtinė Karalystė

1) UK ATOMAL Control Officer,
Room 0302, Ministry of Defence, Main Building, London SW1A 2HB;

2) Jungtinės Karalystės institucija, atsakinga už bendrą JK atominės informacijos kontrolę ir perdavimą, taip pat praktinių klausimų ir prašymų pateikimo punktas:
AD/Sc(Nuc)2/ATOMIC CONTROL OFFICE,
Ministry of Defence, Main Building, Whitehall, London
AD/Sc(Nuc)2/ATOMIC CONTROL OFFICE taip pat pateikiami šie specifiniai klausimai ir prašymai:

a) prašymai gauti JK atominę informaciją;

b) klausimai apie dokumentų, kuriuose yra JK atominės informacijos, turinį ir įslaptinimą;

c) dėl specialių apribojimų pakeitimo;

d) pranešimai apie JK atominės informacijos neteisėtą atskleidimą.

Jungtinės Amerikos Valstijos

1) Central ATOMAL Registry,
Central US Registry, Room 1B 889, The Pentagon, Washington, D.C. 20310
Telegrafo adresas: SECDEF WASHINGTON;

2) Jungtinių Amerikos Valstijų punktas ryšiams palaikyti visais klausimais dėl Jungtinių Amerikos Valstijų politikos, susijusios su 1964 m. ATOMAL susitarimu ir ATOMAL administracinėmis priemonėmis, ir metinių ataskaitų, siunčiamų Jungtinėms Amerikos Valstijoms, gavėjas (ATOMAL administracinių priemonių III skyriaus 54 punktas):
JAV misija prie NATO;

3) JAV įstaiga, atsakinga už pirmąjį ATOMAL informacijos perdavimą, ir punktas ryšiams palaikyti dėl praktinių klausimų ir prašymų, susijusių su ATOMAL administracinėmis priemonėmis:
Joint ATOMAL Information Exchange Group (JAIEG),
Washington, D. C. 20305
(kiekvieno pranešimo JAIEG kopija turi būti pateikiama susipažinti JAV Delegacijai NATO būstinėje).
JAIEG taip pat pateikiami šie specifiniai klausimai ir prašymai:

I) dėl specialiųjų apribojimų pakeitimo (ATOMAL administracinių priemonių II skyriaus 25 punktas);

II) dėl dokumentų atgaminimo (ATOMAL administracinių priemonių III skyriaus 43 ir 45 punktai);

III) prašymai dėl informacijos, pažymėtos žyma „Riboto naudojimo duomenys“ (*Restricted Data*) arba „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*), pateikimo (ATOMAL administracinių priemonių II skyriaus 15 punktas);

4) JAV institucija, atsakinga už ATOMAL turinį ir ATOMAL informacijos įslaptinimą (ATOMAL administracinių priemonių III skyriaus 34–38 punktai):
United States Security Authority for NATO Affairs,
Director, Security Plans and Programs,
ODUSD (Policy), Room 3C–277, Washington, D.C. 20301–2200.
Kiekvienos korespondencijos kopija siunčiama:
Director,
Office of Classification,
US Department of Energy, DP–32, Washington, D.C. 20545.

2. Už NATO tarptautines civilines ir karines institucijas yra atsakingos toliau nurodytos institucijos:
a) Šiaurės Atlanto Taryba
ATOMAL Central Registry,
NATO Headquarters, 1110 Brussels;
b) Karinis komitetas:
ATOMAL Central Registry,
International Military Staff – Military Committee (IMS–MC),
NATO Headquarters,1110 Brussels;
c) Sąjungininkų pajėgų Europoje vadavietė SHAPE,
Attn. COSMIC and ATOMAL Control Officer,
B–7010 Casteau, Belgium;
d) Sąjungininkų pajėgų Atlante vadavietė SACLANT,
Attn. ATOMAL Control Officer,
Norfolk, Virginia 23511, USA;
e) Sąjungininkų pajėgų Lamanše vadavietė CINCHAN,
Attn. ATOMAL Control Officer,
Northwood, Middlesex, HA6 3KR, England.

3. NATO struktūra gali pakeisti savo administracinę įstaigą, apie tai pranešusi NATO saugumo biurui ir visoms kitoms ATOMAL centrinėms registratūroms, išvardytoms šio Priedo 1 ir 2 punktuose.

IV PRIEDAS

Specialūs apribojimai NATO branduolinio planavimo dokumentams gauti

1. Kaip numatyta Šiaurės Atlanto Sutarties Šalių susitarimo dėl bendradarbiavimo, susijusio su atomine informacija (dokumentas C–M(64)39), VI straipsnyje ir ATOMAL administracinių priemonių (dokumentas C–M(68)41(5th revise) II skyriaus 25 punkte, tam tikra ypatingos apsaugos reikalaujanti ATOMAL informacija pranešama NATO taikant Jungtinių Amerikos Valstijų nustatytus specialius apribojimus. Tokie nustatyti specialūs apribojimai nurodomi kiekvieno pateikiamo dokumento tituliniame lape. Jungtinės Amerikos Valstijos nusprendė, kad tam tikrai informacijai, kuri suteikiama naudoti NATO branduolinio planavimo veiklai, apribojimai nustatomi iš anksto.

2. Siekiant lengvai identifikuoti tokius dokumentus, užtikrinti jų nuolatinį

saugumą ir kad jie netyčia nebūtų sumaišyti su kitais dokumentais bei visuomet būtų registruojami tokios informacijos gavėjai, NATO branduolinio planavimo dokumentams parengiamas dokumento lydraštis, kuriame taip pat įrašomi visi asmenys, kurie yra gavę šią informaciją.

3. Dokumento lydraščio pavyzdys pridedamas. Lydraštyje taip pat nurodomi iš anksto nustatyti specialūs apribojimai, taikomi gauti ypatingos apsaugos reikalaujančią informaciją NATO branduolinio planavimo veiklai. Visi asmenys, kurie susipažino su dokumente esančia informacija, kuriai taikomi specialūs apribojimai, įrašomi antroje lydraščio pusėje. Neužpildyta lydraščio forma nėra įslaptintas dokumentas.

4. NATO struktūros gali viena kitai perduoti dokumentus, kuriems taikomi specialūs apribojimai, jei nustatytuose apribojimuose toks perdavimas nėra konkrečiai draudžiamas.

5. Bet kuri informaciją gaunanti NATO struktūra gali pagal dokumento C–M(68)41(5th revise) II skyrių pateikti Jungtinėms Amerikos Valstijoms prašymus platinti informaciją, kuriai taikomi specialūs apribojimai, netaikant nustatytų apribojimų.

6. Šiuo metu egzistuojančius NATO branduolinio planavimo dokumentus jų turėtojams nurodo Jungtinės Amerikos Valstijos. Prie kiekvieno tokio egzistuojančio dokumento, vadovaujantis gautais Jungtinių Amerikos Valstijų nurodymais, pridedamas naujas lydraštis.

7. Įrašuose apie susipažinimą su informacija taip pat nurodomos asmenų, kurie yra gavę informaciją vaizdinių ar žodinių pranešimų būdu, pavardės ir tai patvirtinantys tokių asmenų parašai.

8. Užpildžius informaciją, kuriai taikomi specialūs apribojimai, gavusių asmenų sąrašo puslapį, jei reikia, pridedami papildomi lydraščio puslapiai. Kiekvienas puslapis numeruojamas iš eilės, kad būtų nuosekliai registruojami asmenys, susipažinę su informacija.

9. NATO parengti branduolinio planavimo dokumentai pažymimi kaip turintys informacijos, kuriai taikomi specialūs apribojimai, pirmame dokumento puslapyje ir, juos rengiant, taip pat pridedamas lydraštis. Panašiai elgiamasi ir su nesunaikintais projektais bei darbo dokumentais, kuriuose yra tokios pačios informacijos.

10. Dokumentai, kuriems taikomi specialūs apribojimai, atskirai nesaugomi. Tačiau privalu užtikrinti, kad tokius dokumentus, juos saugant, vežant ar pan., gautų tik asmenys, kurie atitinka specialių apribojimų nustatytas sąlygas.

11. Susipažinimo su ATOMAL informacija registracijos lapuose, kurių reikalauja dokumentas C-M(68)41(5th revise), turėtų būti nurodyti tie turintys teisę susipažinti su ATOMAL informacija asmenys, kuriems buvo leista susipažinti su informacija, kuriai taikomi specialūs apribojimai.

12. Pakankamą lydraščių formų skaičių kiekvienai NATO struktūrai jos prašymu ir pagal poreikius pateikia NATO saugumo biuras.

(Slaptumo žyma)

LYDRAŠTIS

<table>
<tr><td colspan="2"></td><td>Kontrolinis numeris (-iai)</td><td>Pridedami dokumentai</td></tr>
<tr><td colspan="4">Pridedamame dokumente yra informacijos, kurios apsauga yra ypač svarbi ir kurios neteisėtas atskleidimas turėtų rimtų pasekmių NATO; tvarkant ir saugant pridedamą informaciją, būtina griežtai laikytis NATO ATOMAL saugumo reikalavimų. Šis lydraštis – tai ne DOKUMENTAS, PATVIRTINANTIS, KAD INFORMACIJA GAUTA, o asmenų, kurie yra susipažinę su pirmiau nurodyto numerio dokumentu (-ais) registracijos sąrašas.</td></tr>
<tr><td colspan="4">Kiekvienas asmuo, gavęs pridedamą dokumentą, pasirašo lape ir nurodo toliau reikalaujamus duomenis.</td></tr>
<tr><td rowspan="2">Eil. Nr.</td><td rowspan="2">PAVARDĖ</td><td>DATA</td><td rowspan="2">PASTABOS (Nurodykite, ar skaitytas visas dokumentas ar tam tikros konkrečios jo dalys)</td></tr>
<tr><td>GAUTA PERDUOTA</td></tr>
<tr><td>1.</td><td></td><td></td><td></td></tr>
<tr><td>2.</td><td></td><td></td><td></td></tr>
<tr><td>3.</td><td></td><td></td><td></td></tr>
<tr><td>4.</td><td></td><td></td><td></td></tr>
<tr><td>5.</td><td></td><td></td><td></td></tr>
<tr><td>6.</td><td></td><td></td><td></td></tr>
<tr><td>7.</td><td></td><td></td><td></td></tr>
<tr><td>8.</td><td></td><td></td><td></td></tr>
<tr><td>9.</td><td></td><td></td><td></td></tr>
<tr><td>10.</td><td></td><td></td><td></td></tr>
<tr><td>11.</td><td></td><td></td><td></td></tr>
<tr><td>12.</td><td></td><td></td><td></td></tr>
<tr><td>13.</td><td></td><td></td><td></td></tr>
<tr><td>14.</td><td></td><td></td><td></td></tr>
<tr><td>15.</td><td></td><td></td><td></td></tr>
</table>

Šio lydraščio negalima atskirti nuo jo priedo (-ų), kol šis priedas (-ai) nebus sunaikinti; tuomet šis lydraštis bus pažymėtas slaptumo žyma „NATO Konfidencialiai“ (*NATO CONFIDENTIAL*) ir bus saugomas dar trejus metus.

(Slaptumo žyma)

(Slaptumo žyma)

INFORMACIJOS, KURIOS PLATINIMUI JUNGTINĖS AMERIKOS VALSTIJOS TAIKO SPECIALIUS APRIBOJIMUS, LYDRAŠTIS

Kaip nurodyta Šiaurės Atlanto Sutarties Šalių susitarime dėl bendradarbiavimo, susijusio su atomine informacija, ir ATOMAL administracinėse priemonėse, ATOMAL informacijos perdavimui Jungtinės Amerikos Valstijos gali nustatyti specialius apribojimus. Jungtinių Amerikos Valstijų Vyriausybė nusprendė, kad tam tikrai informacijai, suteiktai naudoti NATO branduolinio planavimo veiklai, be priemonių, nurodytų ATOMAL administracinėse priemonėse, taip pat taikomi šie specialūs apribojimai.

A. Susipažinimas su informacija

Susipažinti su atitinkamai pažymėtais dokumentais gali tik personalas, kuris atitinka visus toliau nurodytus reikalavimus:

1) jiems yra išduotas atitinkamas asmens patikimumo pažymėjimas, patvirtinantis asmens teisę susipažinti su ATOMAL informacija;

2) NATO struktūros atsakingas pareigūnas nustatė, kad pagal principą „būtina žinoti“ (*need-to-know*) jiems reikia informacijos, susijusios su NATO branduolinio planavimo veikla, t. y. veikla tokiose institucijose, kaip Branduolinio planavimo grupė (NPC) arba Branduolinės gynybos reikalų komitete (NDAC);

3) atitinkama NATO struktūros saugumo institucija yra juos individualiai patikrinusi ir jų pavardes įtraukusi į savo patikrintų tokios informacijos gavėjų sąrašą[*1];

4) eina vienas iš šių pareigų:

a) valstybių vadovai, vyriausybių vadovai arba ministrai ir vyriausybės departamentų ar įstaigų, atsakančių už NATO branduolinio planavimo klausimus, vadovai, taip pat ribotas skaičius šių pareigūnų patarėjų tokiais klausimais;

b) nuolatiniai atstovai Šiaurės Atlanto Taryboje ir tų jų delegacijų nariai, kurie atsako už NATO branduolinio planavimo klausimus, pareigas;

c) NATO Generalinis Sekretorius ir kiti Tarptautinio sekretoriato nariai, kurie atsako už NATO branduolinio planavimo klausimus, pareigas;

d) Karinio komiteto nariai, taip pat ribotas skaičius štabo pareigūnų, kurie Komitetui pataria NATO branduolinio planavimo klausimais;

e) NATO gynybos planavimo komitetas; NATO branduolinės gynybos reikalų komitetas; NATO branduolinio planavimo grupė; taip pat ribotas skaičius sekretoriato tarnautojų, kurie pataria šiems komitetams tokiais klausimais; ir tie šių komitetų darbo grupių ir techninių specialistų grupių nariai, kuriems reikia susipažinti su tokia informacija;

f) vyriausiųjų NATO karinių vadaviečių vadai (SACEUR, SACLANT ir

[1] NATO struktūros saugumo institucijos vadovas savo nuožiūra gali įgalioti kurį nors aukšto rango pareigūną (arba jo nesant pavaduoti paskirtą asmenį) saugumo institucijos vardu tvirtinti asmenis, kuriems leidžiama susipažinti su informacija.

ACCHAN), taip pat ribotas skaičius tokio vado štabo pareigūnų, kurie pataria NATO branduolinio planavimo klausimais;

g) Kanados ir Jungtinių Amerikos Valstijų regioninės planavimo grupės pirmininkas bei nariai, taip pat ribotas skaičius šios grupės sekretoriato tarnautojų, kurie pataria NATO branduolinio planavimo klausimais;

h) valstybių narių ir NATO karinių vadaviečių personalas, kuris dalyvauja branduolinio planavimo arba Šiaurės Atlanto Tarybos įsteigto komiteto ar grupių veikloje ir kuriam dėl tokio dalyvavimo reikia susipažinti su informacija;

i) ATOMAL kontrolės pareigūnai ir jų pavaduotojai, taip pat minimalus administracinis personalas, kuriam reikia tvarkyti informaciją padedant paskirtam atlikti tikrinimą personalui.

INFORMACIJA, KURIOS PLATINIMUI JUNGTINĖS AMERIKOS VALSTIJOS TAIKO SPECIALIUS APRIBOJIMUS

(Slaptumo žyma)

V PRIEDAS
ATOMAL INFORMACIJOS SAUGUMO PAŽEIDIMAI IR NETEISĖTO JOS ATSKLEIDIMO ATVEJAI

Bendrosios nuostatos

1. Dokumento C–M(64)39 B priedo VI skyriaus B dalis reikalauja, kad NATO Generaliniam Sekretoriui ir Jungtinių Amerikos Valstijų Vyriausybei būtų nedelsiant pranešama apie visus JAV atominės informacijos neteisėto atskleidimo atvejus, praradus dokumentus arba kokiu nors kitu būdu. Apie visus JK atominės informacijos neteisėto atskleidimo atvejus taip pat turi būti nedelsiant pranešama NATO Generaliniam Sekretoriui ir Jungtinės Karalystės Vyriausybei. Toliau pateikiamos administracinės priemonės, kurių imamasi pranešant apie ATOMAL informacijos saugumo pažeidimo ir neteisėto atskleidimo atvejus.

Sąvokos

2. **Informacijos saugumo pažeidimas:** šiame priede informacijos saugumo pažeidimas – tai veiksmas arba neveikimas, prieštaraujantis galiojantiems NATO bendrosioms ar vietinėms saugumo taisyklėms, dėl kurio ATOMAL informacijos saugumui gali kilti pavojus arba ji gali būti neteisėtai atskleista.

3. **Neteisėtas informacijos atskleidimas:** ATOMAL informacija yra neteisėtai atskleista, kai ją visą ar kurią nors jos dalį sužino tokios teisės neturintys asmenys, t. y. asmenys, neturintys atitinkamo NATO patikimumo pažymėjimo ar įgaliojimo susipažinti su tokia informacija, taip pat kai iškyla tokio ATOMAL informacijos perdavimo pavojus[1].

Veiksmai informacijos saugumo pažeidimų atveju

4. Apie visus pastebėtus ATOMAL informacijos saugumo pažeidimus nedelsiant pranešama atitinkamai saugumo institucijai. Pradinės ataskaitos apie tokius informacijos saugumo pažeidimus, kai negalima tuoj pat pašalinti ATOMAL informacijos neteisėto atskleidimo galimybės, taip pat nedelsiant pateikiamos NATO saugumo biurui.

5. Visas ATOMAL informacijos saugumo pažeidimo aplinkybes tiria asme-

[1] Pastabos:
a) ATOMAL informacija, kuri prarandama, nors ir trumpam jai patekus už saugumo zonos ribų, yra laikoma neteisėtai atskleista;
b) ATOMAL informacija, kuri prarandama, nors ir trumpam jai dingus saugumo zonoje (įskaitant esančią dokumentuose, kurie nerandami atliekant eilinę inventorizaciją), yra laikoma neteisėtai atskleista tol, kol tyrimo metu neįrodoma kitaip.

nys, kurie, jei įmanoma, turi įslaptintos informacijos apsaugos ir jos saugumo pažeidimų tyrimo patirties, ir kurie yra nepriklausomi nuo asmenų, tiesiogiai susijusių su tiriamu informacijos saugumo pažeidimu; informacijos saugumo pažeidimą tiriantys asmenys, *inter alia*, nustato:

a) ar ATOMAL informacija buvo neteisėtai atskleista;

b) jei taip, kurie asmenys galėjo neteisėtai gauti ATOMAL informaciją ir kuriems iš tokių asmenų išduotas NATO patikimumo pažymėjimas ir jie pagal turimus duomenis turi teisę bei yra nacionalinių institucijų įgalioti susipažinti su ATOMAL informacija;

c) kokios ištaisomosios, drausminės (įskaitant teisines) ir vėlesnės priemonės yra rekomenduojamos.

6. Visus asmenis, kuriuos tyrėjas nustato kaip neteisėtai gavusius ATOMAL informaciją, administracinė institucija instruktuoja apie atitinkamą informacijos, su kuria jie netyčia susipažino, įslaptinimą bei kategoriją.

Neteisėto informacijos atskleidimo registravimas

7. NATO struktūrų saugumo institucijos imasi priemonių, kad ataskaitų apie ATOMAL informacijos neteisėtą atskleidimą, įskaitant ataskaitas apie tyrimą ir ištaisomąsias priemones, kopijos būtų saugomos ir su jomis būtų galima susipažinti atliekant saugumo tikrinimus padaliniuose, kuriuose buvo padarytas informacijos saugumo pažeidimas.

Pranešimas apie informacijos neteisėtą atskleidimą

8. Visais atvejais, kai ATOMAL informacija yra neteisėtai atskleista, kaip apibrėžta šio Priedo 3 punkte (įskaitant 1 išnašą), ataskaitos apie neteisėtą informacijos atskleidimą NATO saugumo biurui teikiamos per nacionalinę saugumo instituciją, NATO vadavietės vadą arba kitą suinteresuotą NATO instituciją.

9. Pradinėse ataskaitose nurodoma ši informacija:

a) atitinkamos ATOMAL informacijos aprašymas, įskaitant jos dalyką, apimtį, įslaptinimą ir slaptumo žymas, registracijos ir kopijos numerį, datą ir to dokumento rengėją;

b) labai trumpas informacijos neteisėto atskleidimo aplinkybių apibūdinimas, įskaitant datą, laikotarpį, kurio metu ATOMAL informacija galėjo būti neteisėtai atskleista, ir, jei žinoma, informacija, nurodyta 5 punkto b papunktyje;

c) ar dokumento rengėjui buvo pranešta apie informacijos neteisėtą atskleidimą, ar buvo paprašyta, kad tai padarytų NATO saugumo biuras.

10. Pateikiant pradinę ataskaitą, atitinkamais ATOMAL registratūros kanalais NATO saugumo biurui kartu siunčiama kiekvieno neteisėtai atskleisto ATOMAL dokumento kopija arba, jei tokio dokumento nėra, atitinkamos neteisėtai atskleistos ATOMAL informacijos santrauka.

11. Atsižvelgiant į tolesnį tyrimą po pradinės ataskaitos rengiamos kitos ataskaitos. Visais atvejais NATO saugumo biuras turi gauti baigiamąją ataskaitą arba tyrimo pažangos ataskaitą per 90 dienų nuo pradinės ataskaitos.

12. Ataskaitą siunčianti institucija taip pat pateikia ataskaitą apie taikomas ištaisomąsias priemones, kurios neleistų pažeidimams pasikartoti, ir tolesnes prie-

mones, patvirtinančias tyrimo ataskaitoje rekomenduotų priemonių įgyvendinimą.

Informaciją parengusios NATO struktūros veiksmai

13. Pagrindinis ataskaitų apie ATOMAL informacijos neteisėtą atskleidimą informacijos rengėjui tikslas yra tai, kad informaciją parengusi NATO struktūra galėtų įvertinti NATO padarytą žalą ir imtis visų tikslingų ir praktinių priemonių tai žalai sumažinti. Žalos įvertinimo ir taikomų ar planuojamų taikyti žalos mažinimo priemonių ataskaitos siunčiamos NATO saugumo biurui.

NATO saugumo biuro veiksmai

4. NATO saugumo biuras:

a) informuoja Jungtinių Amerikos Valstijų ir (arba) Jungtinės Karalystės institucijas (atsižvelgiant į atitinkamos informacijos rengėją) apie visus praneštus ATOMAL informacijos saugumo pažeidimus;

b) imasi priemonių, kad dokumento, kuriame yra neteisėtai atskleistos ATOMAL informacijos, kopijos, jei jos yra, arba šios informacijos santrauka būtų nusiųsta Jungtinių Amerikos Valstijų ir (arba) Jungtinės Karalystės institucijoms;

c) koordinuoja tyrimus, kuriuose dalyvauja daugiau kaip viena saugumo institucija;

d) prireikus koordinuoja su informacijos rengėjais ir atitinkamomis saugumo institucijomis galutinį NATO padarytos žalos įvertinimą ir taikomas žalos mažinimo priemones;

e) apsvarsto visas ataskaitas prieš jas pateikiant Jungtinių Amerikos Valstijų ir (arba) Jungtinės Karalystės institucijoms;

f) rekomenduoja ir (arba) susitarus su atitinkama saugumo institucija atlieka tolesnį tyrimą, jei mano, kad tai reikalinga;

g) praneša NATO Generaliniam Sekretoriui visais atvejais, kai to reikalauja Aljansui padarytos žalos rimtumas.

NATO Generalinio Sekretoriaus veiksmai

15. NATO Generalinis Sekretorius gali prašyti atitinkamų institucijų atlikti tolesnį tyrimą ir pateikti jo ataskaitą.

ATOMAL informacijos neteisėto atskleidimo tyrimo pabaiga

16. ATOMAL informacijos neteisėto atskleidimo tyrimas baigiamas tik tuomet, kai apie tai praneša atitinkamos Jungtinių Amerikos Valstijų ir (arba) Jungtinės Karalystės institucijos. Jei tam tikras dokumentas yra galutinai prarastas, atitinkama NATO struktūra gali jį išbraukti iš apskaitos.

5.4. TARYBOJE POSĖDŽIAVUSIŲ EUROPOS SĄJUNGOS VALSTYBIŲ NARIŲ SUSITARIMAS DĖL ĮSLAPTINTOS INFORMACIJOS, KURIA KEIČIAMASI EUROPOS SĄJUNGOS INTERESAIS, APSAUGOS

(Priimta: 2011-05-25, ratifikuota 2012-11-06)

TARYBOJE POSĖDŽIAVĘ EUROPOS SĄJUNGOS VALSTYBIŲ NARIŲ VYRIAUSYBIŲ ATSTOVAI,

Kadangi:

(1) Europos Sąjungos valstybės narės (toliau – Šalys) pripažįsta, jog siekiant visapusiškai ir veiksmingai konsultuotis ir bendradarbiauti, gali prireikti tarpusavyje su Europos Sąjungos institucijomis ar Europos Sąjungos įsteigtomis agentūromis, įstaigomis ar biurais keistis įslaptinta informacija Europos Sąjungos interesais.

(2) Šalys turi bendrą norą – prisidėti prie nuoseklios ir išsamios bendros sistemos, skirtos įslaptintos informacijos, gaunamos iš Šalių, iš Europos Sąjungos institucijų ar Europos Sąjungos įsteigtų agentūrų, įstaigų arba biurų, bei iš trečiųjų šalių ar tarptautinių organizacijų, apsaugai Europos Sąjungos interesais, įdiegimo.

(3) Šalys supranta, kad būtina nustatyti tinkamas prieigos prie tokios įslaptintos informacijos ir keitimosi ja saugumo priemones, siekiant tą informaciją apsaugoti,

SUSITARĖ:

1 STRAIPSNIS

Šio Susitarimo tikslas – užtikrinti, kad Šalys apsaugotų įslaptintą informaciją:

kuri yra gaunama iš Europos Sąjungos institucijų ar Europos Sąjungos įsteigtų agentūrų, įstaigų ar biurų, ir kuri pateikiama Šalims arba kuria su Šalimis keičiamasi;

kuri yra gaunama iš Šalių ir pateikiama Europos Sąjungos institucijoms ar Europos Sąjungos įsteigtoms agentūroms, įstaigoms ar biurams arba kuria su jomis keičiamasi;

kuri yra gaunama iš Šalių, siekiant pateikti ją kitoms Šalims arba su Šalimis

ja keistis Europos Sąjungos interesais, ir kuri yra pažymėta, siekiant nurodyti, kad jai taikomas šis Susitarimas;

kurią iš trečiųjų valstybių ar tarptautinių organizacijų yra gavusios Europos Sąjungos institucijos ar Europos Sąjungos įsteigtos agentūros, įstaigos ar biurai ir kuri yra pateikiama Šalims arba su Šalimis keičiamasi.

2 STRAIPSNIS

Šiame Susitarime „įslaptinta informacija“ – bet kokia forma esanti informacija ir medžiaga, kurios neteisėtas atskleidimas padarytų įvairaus dydžio žalos Europos Sąjungos arba vienos ar kelių valstybių narių interesams, ir kuri pažymėta viena iš ES slaptumo žymų arba priede nurodyta ją atitinkančia slaptumo žyma:

- „TRES SECRET UE/EU TOP SECRET“. Ši šyma žymima informacija ir medžiaga, kurios neteisėtas atskleidimas padarytų ypatingai didelės žalos esminiams Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

- „SECRET UE/EU SECRET“. Šia žyma žymima informacija ir medžiaga, kurios neteisėtas atskleidimas rimtai pakenktų esminiams Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

- „CONFIDENTIEL UE/EU CONFIDENTIAL“. Šia žyma žymima informacija ir medžiaga, kurios neteisėtas atskleidimas pakenktų esminiams Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

- RESTREINT UE/EU RESTRICTED“. Šia žyma žymima informacija ir medžiaga, kurios neteisėtas atskleidimas būtų nepalankus Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

3 STRAIPSNIS

1. Vadovaudamosi savo atitinkamais nacionaliniais įstatymais ir kitais teisės katais Šalys imasi visų tinkamų priemonių užtikrinti, kad įslaptintai informacijai, kuriai taikomas šis Susitarimas, suteikiamos apsaugos lygis būtų lygiavertis apsaugos lygiui, kuris pagal Europos Sąjungos Tarybos saugumo taisykles suteikiamas ES įslaptintai informacijai, pažymėtai viena iš priede nurodytų atitinkamų slaptumo žymų.

2. Nė viena šio Susitarimo nuostata nedaro poveikio Šalių nacionaliniams įstatymams ar kitiems teisės aktams, susijusiems su galimybe visuomenei susipažinti su dokumentais, taip pat su asmens duomenų apsauga arba įslaptintos informacijos apsauga.

3. Šalys informuoja šio Susitarimo depozitarą apie priede pateiktų slaptumo klasifikacijų pasikeitimus. 11 straipsnis tokiems pranešimams netaikomas.

4 STRAIPSNIS

1. Kiekviena Šalis užtikrina, kad įslaptinta informacija, kuri pateikiama arba kuria keičiamasi pagal šį Susitarimą nebūtų:

a) išslaptinta ir nebūtų sumažintos jos slaptumo žymos laipsnis be išankstinio rašytinio įslaptintos informacijos rengėjo sutikimo;

b) panaudota kitiems nei įslaptintos informacijos rengėjo nustatytiems tikslams;

c) atskleista jokiai trečiajai valstybei ar tarptautinei organizacijai be išankstinio rašytinio įslaptintos informacijos rengėjo sutikimo ir be tinkamo susitarimo ar administracinio susitarimo su ta trečiąja valstybe ar tarptautine organizacija dėl įslaptintos informacijos apsaugos.

2. Vadovaudamasi savo konstitucinėmis normomis, nacionaliniais įstatymais ir kitais teisės aktais, kiekviena Šalis laikosi įslaptintos informacijos rengėjo sutikimo principo.

5 STRAIPSNIS

1. Kiekviena Šalis užtikrina, kad prieiga prie įslaptintos informacijos būtų suteikiama laikantis principo „būtina žinoti“.

2. Šalys garantuoja, kad priega prie įslaptintos informacijos, kuri pažymėta CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma ar priede nurodyta jas atitinkančia slaptumo žyma, yra suteikiam tik asmenims, kurie turi tinkamą darbo su įslaptinta informacija leidimą arba kurie dėl jų vykdomų funkcijų yra kitu būdu pagal nacionalinius įstatymus ir kitus teisės aktus tinkamai įgalioti.

3. Kiekviena Šalis užtikrina, kad visi asmenys, kuriems suteikta prieiga prie įslaptintos informacijos, būtų informuojami apie jų pareigą pagal atitinkamas saugumo taisykles apsaugoti tokią informaciją.

4. Gavusios prašymą, Šalys, laikydamosi savo atitinkamų nacionalinių įstatymų ir kitų teisės aktų, teikia abipusę pagalbą vykdant asmenų, kuriems reikia išduoti leidimus dirbti su įslaptinta informacija, kandidatūrų tikrinimą.

5. Laikydamasi savo nacionalinių įstatymų ir kitų teisės aktų, kiekviena Šalis užtikrina, kad bet kuris jos jurisdikcijai priklausantis subjektas, kuris gali gauti ar rengti įslaptintą informaciją, turi tinkamą leidimą dirbti su įslaptinta informacija, ir kad tokie subjektai yra pajėgūs užtikrinti tinkamą apsaugą tinkamu saugumo lygiu, kaip numatyta 3 straipsnio 1 dalyje.

6. Šio susitarimo taikymo srityje Šalys gali pripažinti kitos Šalies išduotus personalui ir patalpoms leidimus dirbti su slapta informacija.

6 STRAIPSNIS

Šalys užtikrina, kad visa įslaptinta informacija, kuriai taikomas šis Susitarimas ir kurią Šalys persiunčia, kuria keičiasi ar perduoda savo teritorijoje ar tarpusavyje, būtų tinkamai apsaugota, kaip numatyta 3 straipsnio 1 dalyje.

7 STRAIPSNIS

Kiekviena Šalis užtikrina, kad būtų įgyvendintos tinkamos priemonės, skirtos įslaptintos informacijos, kuri yra tvarkoma, saugoma ar perduodama ryšių ir informacinėse sistemose, apsaugai, kaip numatyta 3 straipsnio 1 dalyje. Tokios priemonės turi užtikrinti įslaptintos informacijos konfidencialumą, integralumą, prieinamumą, ir, atitinkamais atvejais, atsakomybės už informaciją prisiėmimą bei autentiškumą, taip pat tinkamo lygio su ta informacija susijusių veiksmų apskaitą ir atsekamumą.

8 STRAIPSNIS

Šalys viena kitai teikia, pateikus prašymą, reikiamą informaciją apie savo atitinkamas saugumo taisykles ir teisės aktus.

9 STRAIPSNIS

1. Vadovaudamosi atitinkamais nacionaliniais įstatymais ir kitais teisės aktais, Šalys imasi visų tinkamų priemonių, siekdamos ištirti atvejus, kai žinoma arba kai esama pagrįstų priežasčių įtarti, kad įslaptinta infomacija, kuriai taikomas šis Susitarimas, buvo neteisėtai atskleista arba prarasta.

2. Šalis, kuri nustato, kad įslaptinta informacija buvo neteisėtai atskleista arba prarasta, atitinkamais kanalais nedelsdama informuoja įslaptintos informacijos rengėją apie tokį įvykį ir vėliau informuoja įslaptintos informacijos rengėją apie galutinius tyrimo rezultatus bei ištaisomąsias priemones, kurių buvo imtasi, siekiant užkirsti kelią tokių įvykių pasikartojimui. Gavusi prašymą bet kuri kitą susijusi Šalis gali teikti paramą tyrimui atlikti.

10 STRAIPSNIS

1. Šis susitarimas nedaro poveikio galiojantiems bet kurios Šalies sudarytiems susitarimams ar administraciniams susitarimams dėl įslaptintos informacijos apsaugos ar keitimosi ja.

2. Šis Susitarimas neužkerta kelio Šalims sudaryti kitus susitarimus ar administracinius susitarimus, susijusius su jų pateiktos įslaptintos informacijos apsauga ar keitimusi ja, su sąlyga, kad tokie susitarimai neprieštarauja šiam Susitarimui.

11 STRAIPSNIS

Šį susitarimą galima iš dalies keisti Šalims dėl to susitarus tarpusavyje raštu. Visi pakeitimai įsigalioja apie juos pranešus pagal 13 straipsnio 2 dalį.

12 STRAIPSNIS

Visi dviejų ar daugiau Šalių ginčai dėl šio Susitarimo aiškinimo ar taikymo sprendžiami atitinkamų Šalių tarpusavio konsultacijomis.

13 STRAIPSNIS

1. Šalys praneša Europos Sąjungos generaliniam sekretoriui apie šio Susitarimo įsigaliojimui būtinų vidaus procedūrų užbaigimą.

2. Šis Susitarimas įsigalioja antro mėnesio, einančio po to, kai Šalis pranešė Europos Sąjungos generaliniam sekretoriui apie šio Susitarimo įsigaliojimui būtinų vidaus procedūrų užbaigimą, pirmą dieną.

3. Europos Sąjungos generalinis sekretorius yra šio Susitarimo, skelbiamo *Europos Sąjungos oficialiame leidinyje*, depozitaras.

14 STRAIPSNIS

Šis Susitarimas sudarytas vienu originalo egzemplioriumi airių, anglų, bulgarų, čekų, danų, estų, graikų, ispanų, italų, latvių, lenkų, lietuvių, maltiečių, olandų, portugalų, prancūzų, rumunų, slovakų, slovėnų, suomių, švedų, vengrų ir vokiečių kalbomis; visi dvidešimt trys tekstai yra vienodo autentiškumo.

TAI PALIUDYDAMI, tinkamai įgalioti Taryboje posėdžiavę valstybių narių vyriausybių atstovai pasirašė šį Susitarimą.

Priimta du tūkstančiai vienuoliktų metų gegužės dvidešimt penktą dieną Briuselyje.

PRIEDAS

Saugumo klasifikacijų atitikmenys

ES	TRES SECRET UE/EU TOP SECRET	SECRET UE/ EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/ EU RESTRICTED
Belgija	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.199)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	*pastaba toliau* [1]
Bulgarija	Строго секретно	Секретно	Поверително	За служебно ползване
Čekija	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danija	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Vokietija	STRENG GEHEIM	GEHEIM	VS [2] - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Estija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Airija	Top Secret	Secret	Confidential	Restricted
Graikija	Άκρως Απόρρητο Santrumpa: (ΑΑΠ)	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Ispanija	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Prancūzija	Très Secret Défense	Secret Défense	Confidentiel Défense	*pastaba toliau* [3]
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipras	Άκρως Απόρρητο Santrumpa: (ΑΑΠ)	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Liuksemburgas	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Vengrija	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nyderlandai	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK

[1] *Diffusion Restreinte / Beperkte Versreiding* Belgijoje nėra saugumo žyma.

[2] Vokietija: VS – *Verschlussache*.

[3] Prancūzijos nacionalinėje sistemoje žyma „RESTREINT“ nenaudojama. „RESTREINT UE/EU RESTRICTED“ žyma pažymėtą informaciją Prancūzija tvarko ir saugo taip pat griežtai, kaip nustatyta Europos Sąjungos Tarybos saugumo taisyklėse aprašytais standartais ir procedūromis.

Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lenkija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado
Rumunija	Strict secret de importanţă deosebită	Strict secret	Secret	Secret de serviciu
Slovėnija	Strogo tajno	Tajno	Zaupno	Interno
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomija	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTA-MUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedija [4]	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/ SECRET HEMLIG	HEMLIG/ CONFIDENTIAL HEMLIG	HEMLIG/ RESTRICTED HEMLIG
Jungtinė Karalystė	Top Secret	Secret	Confidential	Restricted

[4] Švedija: viršutinėje eilutėje nurodytas saugumo klasifikacijos žymas naudoja gynybos institucijos, o nurodytas apatinėje eilutėje – kitos institucijos.

5.5. LIETUVOS RESPUBLIKOS IR ŠIAURĖS ATLANTO SUTARTIES ORGANIZACIJOS SAUGUMO SUSITARIMAS

(Žin., 2001, Nr. 73-2574)

Lietuvos Respublikos Vyriausybė, atstovaujama Jo Ekscelencijos Adolfo VENSKAUS, Lietuvos Respublikos ambasadoriaus prie Europos Sąjungos Briuselyje, ir Šiaurės Atlanto Sutarties Organizacija, atstovaujama dr. Manfredo VERNERIO (Manfred WÖRNER), Šiaurės Atlanto Sutarties Organizacijos Generalinio Sekretoriaus,

atsižvelgdamos į tai, kad Lietuvos Respublika yra Šiaurės Atlanto Bendradarbiavimo Tarybos (NACC) ir programos „Partnerystė taikos labui“ (PTL) dalyvė;

sutikusios konsultuotis politiniais ir su saugumu susijusiais klausimais, plėtoti ir stiprinti politinį bei karinį bendradarbiavimą Europoje;

suprasdamos, kad efektyviai bendradarbiaujant šiais klausimais šalims reikia keistis svarbia ir (arba) konfidencialia informacija,

s u s i t a r ė:

1 straipsnis

Šalys:

i) gins ir saugos kitos Šalies suteiktą informaciją ir medžiagą;

ii) stengsis užtikrinti, jei tokia informacija ir medžiaga būtų įslaptinta, kad Šalies pateiktai informacijai ir medžiagai būtų suteikta tą informaciją ir medžiagą pateikusios Šalies nustatyta slaptumo žyma, ir saugos tokią informaciją ir medžiagą pagal sutartus bendrus standartus;

iii) nesinaudos pasikeista informacija ir medžiaga kitais tikslais, negu išdėstyta atitinkamose programose bei su šiomis programomis susijusiuose nutarimuose ir rezoliucijose;

iv) neatskleis šios informacijos ir medžiagos trečiosioms šalims be ją perdavusios Šalies sutikimo.

2 straipsnis

i) Lietuvos Respublikos Vyriausybė, prieš suteikdama asmenims teisę naudotis tokia informacija ir medžiaga, įsipareigoja patikrinti visus savo valstybės piliečius, kuriems einant tarnybines pareigas reikia ar kurie gali naudotis pagal NACC ar PTL programas pasikeista informacija ar medžiaga.

ii) Turi būti parengta tikrinimo tvarka, kad atsižvelgiant į asmens lojalumą ir patikimumą būtų nustatyta, ar gali jis susipažinti su įslaptinta informacija nesudarydamas pavojaus jos saugumui.

3 straipsnis

Generalinio Sekretoriaus ir NATO Karinio komiteto pirmininko vadovaujamas ir jiems atstovaujantis NATO Saugumo skyrius (NOS), veikiantis Šiaurės Atlanto Tarybos ir NATO Karinio komiteto vardu ir pagal jų įgaliojimus, yra atsakingas už saugumo priemones, taikomas įslaptintos informacijos, kuria keičiamasi dirbant Šiaurės Atlanto Bendradarbiavimo Taryboje ir pagal programą „Partnerystė taikos labui“, apsaugai.

4 straipsnis

Lietuvos Respublikos Vyriausybė praneš NOS apie saugumo tarnybą, atliekančią panašias funkcijas Lietuvoje. Lietuvos Respublikos Vyriausybės ir NATO administraciniai susitarimai dėl, be kita ko, informacijos, kuria bus keičiamasi, abipusės apsaugos standartų ir Lietuvos Respublikos saugumo tarnybos ir NOS ryšių bus parengti atskirai.

5 straipsnis

Prieš pasikeičiant bet kokia įslaptinta informacija tarp Lietuvos Respublikos Vyriausybės ir NATO, atsakingos saugumo tarnybos turi abipusiškai įsitikinti, kad informaciją gaunanti šalis yra pasiruošusi apsaugoti gautą informaciją, kaip reikalauja informaciją perdavusi šalis.

Tai patvirtindami, pirmiau nurodyti atstovai pasirašė šį Susitarimą.

Sudarytas 1994 m. birželio 13 d. Briuselyje dviem egzemplioriais anglų ir prancūzų kalbomis, abu tekstai turi vienodą teisinę galią.

5.6. LIETUVOS RESPUBLIKOS VYRIAUSYBĖS IR NORVEGIJOS KARALYSTĖS VYRIAUSYBĖS SUSITARIMAS DĖL ĮSLAPTINTOS INFORMACIJOS ABIPUSĖS APSAUGOS*

(Žin., 2012, Nr. 54-2669)

Lietuvos Respublikos Vyriausybė ir Norvegijos Karalystės Vyriausybė, toliau – Šalys,

siekdamos apsaugoti įslaptintą informaciją, kuria jos keičiasi tiesiogiai arba per kitas Šalių jurisdikcijai priklausančias valdymo institucijas ar rangovus, kurie pagal nacionalinę teisę turi teisę dirbti su įslaptinta informacija,

s u s i t a r ė :

1 straipsnis

Taikymo sritis

1. Šis Susitarimas taikomas visiems įslaptintiems sandoriams arba susitarimams, kurių vykdymo metu keičiamasi įslaptinta informacija ir kurie bus sudaryti dėl šių dalykų:

1) Šalių valdymo institucijų bendradarbiavimo;

2) Šalių valdymo institucijų ir (arba) rangovų bendradarbiavimo, keitimosi įslaptinta informacija, bendros veiklos, įslaptintų sandorių ar kitų jų tarpusavio santykių.

2. Šiuo Susitarimu negalima naudotis siekiant gauti įslaptintą informaciją, kurią kita Šalis gavo iš trečiosios šalies.

2 straipsnis

Apibrėžtys

Šiame Susitarime:

1) įslaptinta informacija – bet kokio pavidalo, pobūdžio ar bet kuriomis priemonėmis perduodama parengta arba rengiama informacija, kuri pagal nacionalinę teisę yra įslaptinta;

2) sandoris – dviejų ar daugiau šalių susitarimas, kuriame nustatomos šalių teisės ir prievolės;

3) įslaptintas sandoris – sandoris, kuriame yra įslaptintos informacijos, kuris yra su ja susijęs arba kurio pagrindu įslaptinta informacija parengiama;

4) valdymo institucijos – valstybės ar savivaldybių institucijos ir šių institucijų steigiamos įmonės, kurių veikla susijusi su įslaptinta informacija ir jos apsauga ir kurios pagal nacionalinę teisę turi teisę informaciją įslaptinti ir išslaptinti;

* **Pastaba:** Susitarimas pateikiamas kaip tarptautinio susitarimo dėl įslaptintos informacijos apsaugos su NATO šalimi pavyzdys

5) kompetentinga saugumo institucija – valdymo institucija, kuri pagal nacionalinę teisę atsako už įslaptintos informacijos, kuria keičiamasi pagal šį Susitarimą, apsaugos priežiūrą;

6) rangovas – fizinis arba juridinis asmuo, turintis teisę sudaryti įslaptintus sandorius;

7) saugumo pažeidimas – nacionalinėms saugumo nuostatoms prieštaraujantis veiksmas arba neveikimas, galintis kelti pavojų įslaptintai informacijai arba pažeisti jos apsaugos reikalavimus;

8) informaciją parengusi Šalis – Šalis, kurios jurisdikcijoje įslaptinta informacija yra parengta;

9) informaciją gaunanti Šalis – Šalis, kurios jurisdikcijai įslaptinta informacija yra perduodama;

10) apsaugos reikalavimų pažeidimas – įslaptintos informacijos arba jos dalies patekimas trečiajai šaliai arba pavojus, kad taip atsitiks;

11) trečioji šalis – valstybė arba tarptautinė organizacija, kuri nėra šio Susitarimo šalis, arba fizinis ar juridinis asmuo, kuris neatitinka nacionalinių reikalavimų dėl teisės susipažinti su įslaptinta informacija, įskaitant „būtina žinoti“ principą;

12) asmens patikimumo pažymėjimas – atlikus Šalies nacionalines asmens patikrinimo saugumo požiūriu procedūras asmens atžvilgiu priimtas teigiamas sprendimas, kurio pagrindu šiam asmeniui suteikiama teisė susipažinti bei dirbti su tam tikra slaptumo žyma pažymėta įslaptinta informacija;

13) įmonės patikimumo pažymėjimas – atlikus Šalies nacionalines patikrinimo saugumo požiūriu procedūras įmonės atžvilgiu priimtas teigiamas sprendimas, kurio pagrindu šiai įmonei suteikiama teisė gauti tam tikra slaptumo žyma pažymėtą įslaptintą informaciją, su ja dirbti, ją apdoroti ir saugoti;

14) saugumo patvirtinimas – pagal nacionalinę teisę valdymo institucijos išduotas patvirtinimas, kad RIBOTO NAUDOJIMO įslaptinta informacija bus saugoma pagal jos nacionalinės teisės norminių aktų reikalavimus;

15) principas „būtina žinoti“ – teisė susipažinti su įslaptinta informacija gali būti suteikta tik tuo atveju, jei yra patvirtinta, kad asmeniui, kuriam ji reikalinga, yra būtina ją žinoti, kad galėtų eiti tarnybines pareigas, dėl kurių ši informacija buvo perduota informaciją gaunančiai Šaliai.

3 straipsnis

Slaptumo žymos

1. Įslaptinta informacija žymima šiomis slaptumo žymomis. Jos laikomos atitinkančiomis viena kitą:

LIETUVOS	Atitikmuo anglų kalba	NORVEGIJOS
VISIŠKAI SLAPTAI	TOP SECRET	STRENGT HEMMELIG
SLAPTAI	SECRET	HEMMELIG
KONFIDENCIALIAI	CONFIDENTIAL	KONFIDENSIELT
RIBOTO NAUDOJIMO	RESTRICTED	BEGRENSET

2. Informaciją gaunanti Šalis ir (arba) jos jurisdikcijai priklausančios valdymo institucijos be išankstinio rašytinio kompetentingos saugumo institucijos arba informaciją įslaptinusios valdymo institucijos leidimo negali gautai įslaptintai informacijai priskirti žemesnio lygio slaptumo žymos arba jos išslaptinti. Informaciją parengusios Šalies kompetentinga saugumo institucija arba valdymo institucija nedelsdamos raštu praneša informaciją gaunančiai Šaliai apie visus apsikeistos informacijos slaptumo žymų pasikeitimus.

3. Informaciją gaunanti Šalis ir (arba) jos jurisdikcijai priklausančios valdymo institucijos gautą įslaptintą informaciją pažymi savo slaptumo žymomis, atitinkančiomis gautos įslaptintos informacijos slaptumo žymas. Vertimai ir kopijos pažymimos ta pačia slaptumo žyma kaip ir originalas.

4 straipsnis

Abipusės apsaugos principai

1. Vadovaudamosi savo nacionaliniais įstatymais, kitais teisės norminiais aktais ir praktika, abi Šalys imasi atitinkamų priemonių įslaptintai informacijai, kuri buvo perduota, gauta, pagaminta arba parengta vykdant kokį nors Šalių susitarimą arba joms bendradarbiaujant tarpusavyje, apsaugoti. Šalys visai perduotai, gautai, pagamintai arba parengtai įslaptintai informacijai užtikrina tokią pačią apsaugą, kokia yra suteikiama jų tokia pačia slaptumo žyma žymimai įslaptintai informacijai.

2. Teisė susipažinti su įslaptinta informacija ir patekti į vietas ar įmones, kur vykdoma įslaptinta veikla arba kur laikoma įslaptinta informacija, suteikiama tik tiems, kam buvo išduotas asmens patikimumo pažymėjimas ir kas, dėl savo vykdomų funkcijų ar darbo, atitinka principą „būtina žinoti“.

3. Pagal joms priklausančią jurisdikciją Šalys prižiūri, kaip laikomasi nacionalinių įstatymų, kitų teisės norminių aktų ir praktikos reikalavimų, keliamų įslaptintos informacijos apsaugai.

4. Šalys pagal savo nacionalinę teisę saugo intelektinės nuosavybės teises ir komercines paslaptis (praktinę patirtį – angl. *know-how*), kurios buvo perduotos kartu su įslaptinta informacija.

5. Šalia slaptumo žymos gali būti nurodomi ir kiti darbo su perduota įslaptinta informacija reikalavimai, detalizuojantys įslaptintos informacijos panaudojimą. Papildomus darbo su įslaptinta informacija reikalavimus Šalys viena kitai perduoda per savo kompetentingas saugumo institucijas.

6. Kai gauta įslaptinta informacija tampa nereikalinga, ji, gavus išankstinį rašytinį informaciją parengusios Šalies kompetentingos saugumo institucijos sutikimą, gali būti sunaikinta.

5 straipsnis

Įslaptintos informacijos atskleidimas

Be išankstinio rašytinio informaciją parengusios Šalies sutikimo Šalys pagal šį Susitarimą gautos įslaptintos informacijos neatskleidžia trečiajai šaliai. Gauta įslaptinta informacija naudojama tik tiems tikslams, kuriems ji buvo perduota.

6 straipsnis

Kompetentingos saugumo institucijos

1. Šalys paskiria ir informuoja viena kitą apie kompetentingas saugumo institucijas, kurios prižiūri visų šio Susitarimo 1 straipsnyje minėtų susitarimų dėl įslaptintos informacijos apsaugos įgyvendinimą. Paprašius kompetentingos saugumo institucijos keičiasi informacija apie šio Susitarimo įgyvendinimą, taip pat apie valdymo institucijas, atsakingas už tam tikrus įslaptintos informacijos apsaugos aspektus.

2. Šalys įsipareigoja užtikrinti, kad jų kompetentingos saugumo institucijos tinkamai laikytųsi šio Susitarimo nuostatų.

3. Prireikus abiejų Šalių kompetentingos saugumo institucijos pagal jų valstybėms priklausančią jurisdikciją rengia ir platina įslaptintos informacijos, kuria keičiamasi pagal bet kokį kitą Šalių susitarimą, apsaugos reikalavimus ir procedūras ir prižiūri, kaip jų laikomasi.

4. Vienos kompetentingos saugumo institucijos prašymu kita kompetentinga saugumo institucija pateikia informaciją apie savo saugumo organizavimą ir procedūras, kad būtų galima jas palyginti ir laikytis analogiškų saugumo standartų bei rengti bendrus įgaliotų pareigūnų vizitus abiejose valstybėse. Tokie vizitai turi būti abiejų Šalių suderinti.

7 straipsnis

Vizitai

1. Viena Šalis leidžia kitos Šalies atstovams atvykti į vietas, kur rengiama, tvarkoma ar saugoma įslaptinta informacija arba kur vykdomi įslaptinti projektai siekiant pasikeisti įslaptinta informacija, tik tuo atveju, jei prieš tai buvo gautas rašytinis priimančiosios Šalies kompetentingos saugumo institucijos leidimas. Šis leidimas suteikiamas asmenims, kurie turi asmens patikimumo pažymėjimą, kurie atitinka principą „būtina žinoti“ ir kuriems atitinkamos Šalies kompetentinga saugumo institucija arba valdymo institucijos, nurodytos pagal 6 straipsnį, suteikė leidimą atvykti vizito ar vizitų.

2. Prašančios leisti apsilankyti Šalies kompetentinga saugumo institucija arba valdymo institucija, nurodyta pagal 6 straipsnį, pagal šio straipsnio nuostatas praneša valstybės, į kurią ketinama atvykti vizito, kompetentingai saugumo institucijai arba valdymo institucijai, nurodytai pagal 6 straipsnį, apie planuojamą vizitą ir užtikrina, kad ši kompetentinga saugumo institucija arba valdymo institucija prašymą dėl vizito gautų prieš tris savaites iki vizito ar vizitų.

3. Prašyme dėl vizito nurodoma:

1) atvykstančio asmens pavardė, vardas, gimimo vieta ir data, pilietybė ir darbdavys, paso arba kito asmens tapatybės dokumento duomenys;

2) patvirtinimas, kad atvykstantis asmuo turi asmens patikimumo pažymėjimą, atitinkantį vizito tikslą;

3) vizito ar vizitų objektą ir tikslą; (Ši informacija turi būti tiksli ir pakankamai išsami. Patariama nevartoti bendrybių ir santrumpų);

4) numatoma prašomo vizito ar vizitų data ir trukmė;

5) asmuo ryšiams palaikyti įmonėje (ar objekte), kuriuose bus lankomasi,

buvę kontaktai ir visa kita informacija, galinti padėti nustatyti vizito ar vizitų pagrįstumą.

4. Prašymas pateikiamas:

1) per Lietuvos ambasadą Osle – kai prašoma leisti Lietuvos Respublikos piliečiams atvykti į Norvegiją;

2) per Norvegijos ambasadą Vilniuje – kai prašoma leisti Norvegijos Karalystės piliečiams atvykti į Lietuvą;

3) abiejų Šalių kompetentingų saugumo institucijų susitarimu gali būti taikoma kita tvarka.

5. Leidimai atvykti vizito galioja ne ilgiau kaip dvylika mėnesių.

6. Vizito metu gautai įslaptintai informacijai turi būti užtikrinamas toks pat įslaptinimo ir apsaugos lygis, kokį užtikrina informaciją parengusi Šalis.

8 straipsnis

Sandoriai

1. Kai kuri nors Šalis ir (arba) jos jurisdikcijai priklausančios valdymo institucijos ketina sudaryti įslaptintą sandorį, kuris turi būti vykdomas kitos Šalies valstybės teritorijoje, Šalis, kurios valstybės teritorijoje šis sandoris pagal šį Susitarimą turi būti vykdomas, prisiima atsakomybę už įslaptintos informacijos tvarkymą pagal savo nacionalinę teisę. Šiuo atveju turi būti gautas išankstinis rašytinis numatomo rangovo Šalies kompetentingos saugumo institucijos užtikrinimas. Jame turi būti patvirtinta, kad numatomas rangovas turi atitinkamo lygio įmonės patikimumo pažymėjimą ir priemones to paties lygio įslaptintai informacijai tvarkyti ir saugoti. RIBOTO NAUDOJIMO įslaptintai informacijai išduodamas saugumo patvirtinimas.

2. Visuose įslaptintuose sandoriuose turi būti atitinkamas skyrius apie saugumą ir įslaptinimo žinynas pagal šio Susitarimo sąlygas.

3. Valstybės, kurioje bus vykdomas įslaptintas sandoris, kompetentinga saugumo institucija prisiima atsakomybę už įslaptintos informacijos saugumo priemonių nustatymą ir administravimą pagal tokius pačius standartus ir reikalavimus kaip ir tie, kurie taikomi jos pačios įslaptintų sandorių apsaugai.

4. Rangovas praneša kompetentingai saugumo institucijai apie visus subrangovus, norinčius vykdyti įslaptintų sandorių dalis, kad ši juos patvirtintų. Patvirtinti subrangovai turi įvykdyti tas pačias saugumo prievoles, kokios yra nustatytos rangovui.

5. Valstybės, kurioje ketinama vykdyti įslaptintą projektą, susitarimą, sandorį ar sandorio dalį, kompetentingai saugumo institucijai turi būti iš anksto apie tai pranešta ir pateikta tokio projekto, susitarimo, sandorio ar sandorio dalies kopija.

6. Informaciją gaunanti Šalis, perduodama iš kitos Šalies gautą įslaptintą informaciją savo esamiems arba numatomiems rangovams, prieš tai turi:

1) užtikrinti, kad šie esami arba numatomi rangovai ir jų įmonės yra pajėgūs tinkamai saugoti įslaptintą informaciją;

2) atitinkamiems rangovams suteikti atitinkamą įmonės patikimumo pažymėjimą;

3) visiems darbuotojams, kurie dėl savo pareigų privalo susipažinti su įslaptinta informacija, suteikti atitinkamus asmens patikimumo pažymėjimus;

4) užtikrinti, kad visi asmenys, turintys teisę susipažinti su įslaptinta informacija, būtų supažindinti su jų pareigomis saugoti įslaptintą informaciją pagal galiojančius įstatymus;

5) periodiškai tikrinti, kaip užtikrinamas įslaptintos informacijos saugumas.

9 straipsnis

Pranešimai ir jų perdavimas

1. Paprastai įslaptinta informacija fiziškai perduodama Šalių diplomatiniais kanalais.

2. Įslaptinta informacija gali būti keičiamasi ir per atstovus, oficialiai paskirtus pagal nacionalinę teisę.

3. Dėl didelio įslaptintos informacijos kiekio perdavimo kompetentingos saugumo institucijos tariasi kiekvienu atveju atskirai.

4. Kompetentingų saugumo institucijų susitarimu gali būti naudojami kiti patvirtinti informacijos perdavimo ar pasikeitimo būdai.

10 straipsnis

Saugumo pažeidimas

Kai pažeidžiamas kitos Šalies parengtos arba iš kitos Šalies gautos įslaptintos informacijos saugumas arba kai tai yra susiję su bendrais interesais, valstybės, kurioje buvo pažeisti įslaptintos informacijos apsaugos reikalavimai, kompetentinga saugumo institucija kuo greičiau praneša apie tai kitos valstybės kompetentingai saugumo institucijai ir pradeda atitinkamą tyrimą. Prireikus kita Šalis bendradarbiauja atliekant šį tyrimą. Bet kuriuo atveju kita Šalis turi būti informuojama apie tyrimo rezultatus ir jai turi būti pateikta galutinė saugumo pažeidimo priežasčių ir masto ataskaita.

11 straipsnis

Išlaidos

Nė viena Šalis neatlygina kitos Šalies išlaidų, susijusių su šio Susitarimo vykdymu.

12 straipsnis

Ginčų sprendimas

Visi ginčai dėl šio Susitarimo aiškinimo ar taikymo sprendžiami Šalims tarpusavyje konsultuojantis ir į jokį nacionalinį ar tarptautinį teismą ar trečiąją šalį nesikreipiama.

13 straipsnis

Baigiamosios nuostatos

1. Šis Susitarimas įsigalioja tą dieną, kai gaunamas paskutinis pranešimas, kuriuo Šalys patvirtino viena kitai, kad įvykdė visus nacionalinės teisės reikalavimus, būtinus šiam Susitarimui įsigalioti. Susitarimas sudaromas neapibrėžtam laikotarpiui.

2. Bet kuri Šalis gali bet kada nutraukti šį Susitarimą, apie tai diplomatiniais kanalais raštu pranešdama kitai Šaliai. Tokiu atveju Susitarimas nustoja galioti praėjus šešiems mėnesiams nuo tos dienos, kai ta kita Šalis gavo pranešimą apie jo nutraukimą.

3. Šis Susitarimas gali būti bet kada persvarstomas, keičiamas ar iš dalies keičiamas abiejų Šalių rašytiniu susitarimu.

4. Šį Susitarimą nutraukus, visa pagal jį perduoda įslaptinta medžiaga ir (arba) informacija kuo greičiau grąžinama kitai Šaliai. Negrąžinta įslaptinta informacija ir (arba) medžiaga saugoma pagal šio Susitarimo nuostatas.

Sudaryta 2011 m. kovo 24 d. Vilniuje dviem autentiškais egzemplioriais lietuvių, norvegų ir anglų kalbomis. Kilus nesutarimų dėl Susitarimo aiškinimo, vadovaujamasi tekstu anglų kalba.

5.7. LIETUVOS RESPUBLIKOS VYRIAUSYBĖS IR GRUZIJOS VYRIAUSYBĖS SUSITARIMAS DĖL KEITIMOSI ĮSLAPTINTA INFORMACIJA IR ĮSLAPTINTOS INFORMACIJOS ABIPUSĖS APSAUGOS*

(Žin., 2010-04-27, Nr. 48-2311)

Lietuvos Respublikos Vyriausybė ir Gruzijos Vyriausybė (toliau – Šalys),

nutarusios konsultuotis politiniais ir su saugumu susijusiais klausimais ir plėsti bei stiprinti politinį, teisinį, karinį ir ekonominį bendradarbiavimą;

suvokdamos politinės padėties pasaulyje pokyčius ir pripažindamos svarbų savo abipusio bendradarbiavimo vaidmenį taikos įtvirtinimui, tarptautiniam saugumui ir abipusiam pasitikėjimui;

suprasdamos, kad patikimam bendradarbiavimui gali reikėti tarpusavyje keistis įslaptinta informacija;

norėdamos nustatyti įslaptintos informacijos abipusę apsaugą reglamentuojančias taisykles, taikytinas būsimiems bendradarbiavimo susitarimams ir įslaptintiems sandoriams, kuriuose gali būti įslaptintos informacijos, ar su ja susijusiems bendradarbiavimo susitarimams ir įslaptintiems sandoriams, kuriuos tarpusavyje vykdys Šalys,

s u s i t a r ė:

1 straipsnis

Tikslas ir taikymo sritis

1. Šio Susitarimo tikslas – užtikrinti įslaptintos informacijos, kuria Šalys keičiasi arba kurią parengia tarpusavyje bendradarbiaudamos, apsaugą.

2. Šis Susitarimas taikomas bet kokiai su įslaptinta informacija susijusiai veiklai, sandoriams ar susitarimams, kuriuos Šalys vykdys ar sudarys ateityje arba kuriuos jos vykdė ar sudarė iki šio Susitarimo įsigaliojimo.

2 straipsnis

Apibrėžtys

Šiame Susitarime:

1) **įslaptinta informacija** – bet kokio pavidalo ir pobūdžio tarnybos arba valstybės paslaptimi pripažįstama informacija, dokumentai ir medžiaga, kuriai suteikiama slaptumo žyma ir kuri nacionalinio saugumo interesais ir pagal nacionalinės teisės aktus turi būti saugoma nuo neteisėtos prieigos prie įslaptintos informacijos arba saugumo pažeidimo;

2) **neteisėta prieiga prie įslaptintos informacijos arba saugumo pažei-**

* **Pastaba:** Susitarimas pateikiamas kaip tarptautinio susitarimo dėl įslaptintos informacijos apsaugos su ne NATO šalimi pavyzdys

dimas – nacionalinės teisės aktams prieštaraujantis veiksmas arba neveikimas, dėl kurio atskleidžiama įslaptinta informacija, įskaitant, bet neapsiribojant, jos praradimu, netinkamu naudojimu, sugadinimu, neteisėtu sunaikinimu arba bet kuriuo kitu veiksmu ar neveikimu, dėl kurių įslaptinta informacija tapo arba gali tapti žinoma neturinčiam teisės su ja susipažinti asmeniui;

3) **slaptumo žyma** – įslaptintos informacijos žyma, rodanti jos įslaptinimo lygį, kuris atspindi jos svarbą, prieigos prie jos apribojimo lygį ir jos apsaugos lygį;

4) **patikimumo pažymėjimas** – atlikus nacionalines patikrinimo procedūras priimtas teigiamas sprendimas, kuriuo patvirtinamas fizinio ar juridinio asmens lojalumas ir patikimumas, taip pat kiti saugumo aspektai pagal nacionalinės teisės aktus, ir suteikiantis tam fiziniam ar juridiniam asmeniui teisę susipažinti ir dirbti su tam tikra slaptumo žyma žymima įslaptinta informacija;

5) **informaciją parengusi Šalis** – Šalies valstybės valdymo / kompetentinga institucija, kuri parengė įslaptintą informaciją;

6) **informaciją gaunanti Šalis** – Šalies valstybės valdymo / kompetentinga institucija arba rangovas, kuriems perduodama įslaptinta informacija;

7) **valdymo institucija** – valstybės ar savivaldybės institucija ir jos įsteigta įmonė, kurios veikla yra susijusi su įslaptinta informacija ir kuriai pagal nacionalinės teisės aktus suteikiama teisė informaciją įslaptinti ir išslaptinti;

8) **kompetentinga institucija** – valstybės institucija, kuri pagal atitinkamos Šalies valstybės nacionalinės teisės aktus įgyvendina tos valstybės įslaptintos informacijos apsaugos politiką, vykdo bendrą šios srities kontrolę, taip pat prižiūri, kaip įgyvendinamas šis Susitarimas. Šios institucijos išvardytos šio Susitarimo 5 straipsnyje;

9) **rangovas** – fizinis ar juridinis asmuo, turintis teisę sudaryti įslaptintus sandorius pagal šio Susitarimo ir nacionalinės teisės aktų nuostatas;

10) **įslaptintas sandoris** – bet kokios derybos iki sandorio sudarymo, sandoriai, jų pagrindu sudaryti sandoriai ar kiti patvirtinti susitarimai su rangovais arba tarp rangovų, priklausančių kurios nors Šalies valstybės jurisdikcijai, dėl prekių tiekimo, darbų atlikimo ar paslaugų teikimo, kuriuos vykdant reikia susipažinti su įslaptinta informacija arba kurių vykdymo metu tokia informacija yra sukuriama;

11) **principas „būtina žinoti“** reiškia, kad teisė susipažinti su įslaptinta informacija gali būti patikėta tik asmenims, kurie pagal nacionalinės teisės aktus turi teisę susipažinti su įslaptinta informacija ir kuriems dėl einamų tarnybinių pareigų atlikimo ir (arba) dėl konkrečios tarnybinės užduoties vykdymo reikia susipažinti su įslaptinta informacija;

12) **trečioji šalis** – valstybė arba tarptautinė organizacija, kuri nėra šio Susitarimo šalis;

13) **įslaptintos informacijos išslaptinimas** – įslaptintos informacijos įslaptinimo lygio panaikinimas.

3 straipsnis

Informacijos slaptumo žymos

1. Šalys susitaria, kad toliau nurodytos informacijos slaptumo žymos atitinka viena kitą ir informacijos slaptumo žymas, nurodytas atitinkamos valstybės nacionalinės teisės aktuose.

Lietuvos Respublikoje	Atitikmuo anglų kalba	Gruzijoje
VISIŠKAI SLAPTAI	TOP SECRET	განსაქუთრებული მნიშვნელობის
SLAPTAI	SECRET	სრულიად საიდუმლო
KONFIDENCIALIAI	CONFIDENTIAL	საიდუმლო
RIBOTO NAUDOJIMO	RESTRICTED	შეზღუდული სარგებლობისთვის

2. Informaciją gaunanti Šalis privalo pažymėti gautą įslaptintą informaciją atitinkama slaptumo žyma.

3. Informaciją gaunanti Šalis be išankstinio rašytinio informaciją parengusios Šalies sutikimo negali gautos įslaptintos informacijos išslaptinti arba priskirti jai žemesnio lygio slaptumo žymą.

4 straipsnis

Nacionalinės priemonės

1. Vadovaudamosi savo nacionalinės teisės aktais, Šalys imasi visų reikiamų priemonių, kad būtų apsaugota pagal šį Susitarimą kartu parengta įslaptinta informacija arba įslaptinta informacija, kuria pagal šį Susitarimą buvo tiesiogiai ar netiesiogiai pasikeista. Tokiai įslaptintai informacijai turi būti užtikrinamas toks pats apsaugos lygis, koks yra suteikiamas nacionalinei to paties įslaptinimo lygio įslaptintai informacijai.

2. Teisė susipažinti su įslaptinta informacija nė vienam asmeniui neturi būti suteikiama tik dėl jo rango, einamų tarnybinių pareigų ar dėl to, kad jis turi patikimumo pažymėjimą. Teisė susipažinti su įslaptinta informacija suteikiama tik tiems asmenims, kuriems išduotas atitinkamas patikimumo pažymėjimas arba kuriems vadovaujantis nacionalinės teisės aktais buvo suteikta tokia teisė ir kurie atitinka principą „būtina žinoti“.

3. Informaciją gaunanti Šalis įsipareigoja:

a) neatskleisti įslaptintos informacijos trečiajai šaliai be išankstinio rašytinio informaciją parengusios Šalies kompetentingos institucijos sutikimo;

b) nenaudoti įslaptintos informacijos kitiems tikslams, nei tiems, kuriems ji buvo perduota;

c) garantuoti tokias su įslaptinta informacija susijusias privatines teises, kaip patentų teisė, autorių teisė ar komercinės paslaptys.

4. Jei kurio nors kito Šalių tarpusavyje sudaryto susitarimo nuostatos dėl keitimosi įslaptinta informacija ar jos apsaugos yra griežtesnės, taikomos to susitarimo nuostatos.

5 straipsnis

Kompetentingos institucijos

1. Šalių kompetentingos institucijos yra šios:
Lietuvos Respublikoje:
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija;
Gruzijoje:
Gruzijos vidaus reikalų ministerija.

2. Kompetentingos institucijos informuoja viena kitą apie galiojančius nacionalinės teisės aktus, reglamentuojančius įslaptintos informacijos apsaugą, ir apie visus tokių teisės aktų pasikeitimus, turinčius reikšmės įslaptintos informacijos apsaugai pagal šį Susitarimą.

3. Siekdamos užtikrinti glaudų bendradarbiavimą įgyvendinant šį Susitarimą, kompetentingos institucijos vienos iš jų prašymu gali rengti konsultacijas.

4. Siekdamos panašių saugumo standartų ir stengdamosi juos palaikyti, kompetentingos institucijos gali teikti viena kitai informaciją apie atitinkamos Šalies įslaptintos informacijos apsaugai taikomus saugumo standartus, procedūras ir praktiką.

5. Kompetentingos institucijos gali sudaryti su šiuo Susitarimu susijusius įgyvendinimo susitarimus.

6 straipsnis

Įslaptintos informacijos perdavimas

1. Paprastai įslaptinta informacija perduodama per diplomatinius ar karinius kurjerius arba kitomis, abiejų Šalių valstybių kompetentingų institucijų iš anksto patvirtintomis priemonėmis, atitinkančiomis nacionalinės teisės aktų reikalavimus.

2. Informaciją gaunanti Šalis kuo skubiau patvirtina, kad gavo įslaptintą informaciją.

3. Jei perduodama įslaptinta informacija pažymėta slaptumo žyma VISIŠKAI SLAPTAI / TOP SECRET / განსაქუთრებული მნიშვნელობის arba SLAPTAI / SECRET / სრულიად საიდუმლო, informaciją gaunanti Šalis raštu patvirtina, kad gavo įslaptintą informaciją.

4. Įslaptinta informacija gali būti perduodama saugiomis elektroninių ryšių sistemomis, tinklais ar kitomis kompetentingų institucijų patvirtintomis elektromagnetinėmis priemonėmis tik užšifruota, panaudojant abiejų kompetentingų institucijų patvirtintus šifravimo būdus ir priemones.

5. Jei reikia perduoti didelį įslaptintos informacijos kiekį, Šalių kompetentingos institucijos kiekvieną kartą priima atskirą sprendimą, kuriuo patvirtinamos transporto priemonės, maršrutas ir saugumo priemonės.

6. Informaciją parengusi Šalis informaciją gaunančiai Šaliai perduoda įslaptintą informaciją tokia forma, kuri atitinka perdavimo tikslą.

7 straipsnis

Vertimas, kopijavimas, naikinimas

1. Įslaptinta informacija, pažymėta slaptumo žyma VISIŠKAI SLAPTAI / TOP SECRET / განსაქუთრებული მნიშვნელობის arba SLAPTAI / SECRET / სრულიად საიდუმლო, verčiama ir kopijuojama tik gavus rašytinį informaciją parengusios Šalies leidimą.

2. Įslaptintą informaciją kopijuoja ir verčia asmenys, turintys atitinkamą patikimumo pažymėjimą.

3. Kiekviena įslaptintos informacijos kopija ar vertimas, kai ji verčiama arba kopijuojama, pažymimas visomis originalo slaptumo žymomis ir nurodomi papildomi naudojimo reikalavimai. Tokiems įslaptintos informacijos vertimams ar jos kopijoms taikoma tokia pati kontrolė kaip ir originalams. Kopijų daroma tik tiek, kiek reikia tarnybinėms reikmėms.

4. Įslaptinta informacija gali būti sunaikinta gavus išankstinį rašytinį informaciją parengusios Šalies sutikimą. Įslaptinta informacija sunaikinama arba pakeičiama taip, kad jos – nei visos, nei dalies – nebūtų galima atkurti.

5. Įslaptinta informacija, žymima slaptumo žyma VISIŠKAI SLAPTAI / TOP SECRET / განსაქუთრებული მნიშვნელობის, nenaikinama, išskyrus 7 straipsnio 6 ir 7 dalyse nurodytus atvejus. Ji grąžinama informaciją parengusiai Šaliai.

6. Susidarius padėčiai, kai pagal šį Susitarimą parengtos ar perduotos įslaptintos informacijos neįmanoma apsaugoti ir (arba) grąžinti, įslaptinta informacija sunaikinama nedelsiant. Apie įslaptintos informacijos sunaikinimą informaciją gaunanti Šalis kuo skubiau praneša informaciją parengusiai Šaliai.

7. Informaciją parengusi Šalis prie slaptumo žymos gali pateikti ir kitus išsamius darbo su perduota įslaptinta informacija nurodymus. Įslaptinta informacija, kurią sunaikinti draudžiama, grąžinama informaciją parengusiai Šaliai.

8 straipsnis

Įslaptinti sandoriai

1. Valdymo institucija, kuri ketina sudaryti įslaptintą sandorį su kitos Šalies valstybės teritorijoje įregistruotu rangovu arba kuri ketina leisti vienam savo rangovų sudaryti įslaptintą sandorį kitos Šalies valstybėje, privalo iš anksto gauti kompetentingos institucijos rašytinį patikinimą, kad siūlomam rangovui yra išduotas atitinkamo lygio patikimumo pažymėjimas. Jei numatomas rangovas neturi atitinkamo patikimumo pažymėjimo, kompetentinga institucija reikiamu lygiu pradeda patikrinimo procedūrą. Įslaptintas sandoris gali būti sudaromas tik su tuo rangovu, kuriam išduotas atitinkamas patikimumo pažymėjimas.

2. Šalies, kurios valstybės teritorijoje bus vykdomas įslaptintas sandoris, kompetentinga institucija prisiima atsakomybę už įslaptintos informacijos saugumo priemonių nustatymą ir administravimą pagal tokius pačius standartus ir reikalavimus kaip ir tie, kurie taikomi jos pačios įslaptintų sandorių apsaugai.

3. Prie kiekvieno įslaptinto sandorio pridedamas įslaptinimo priedas, kuris yra įslaptinto sandorio sudedamoji dalis. Įslaptintą informaciją parengusi Šalis šiame priede nurodo, kokia įslaptinta informacija bus teikiama informaciją gau-

nančiai Šaliai ar bus jos parengta ir koks atitinkamas informacijos įslaptinimo lygis yra nustatytas šiai informacijai. Įslaptinimo priedo kopija siunčiama kompetentingoms institucijoms.

4. Rangovo įsipareigojimas saugoti įslaptintą informaciją visais atvejais visų pirma apima:

a) rangovo įsipareigojimą įslaptintą informaciją atskleisti tik tam asmeniui, kuris turi atitinkamą patikimumo pažymėjimą ir kuris atitinka principą „būtina žinoti“;

b) priemones, kurios bus naudojamos įslaptintai informacijai perduoti;

c) pranešimo apie galimus pakeitimus, susijusius su įslaptinta informacija, dėl to, kad keičiamas jos įslaptinimo lygis, arba dėl to, kad apsauga nebereikalinga, procedūras ir priemones;

d) įslaptintame sandoryje numatytų vienos Šalies valstybės personalo vizitų į kitos Šalies valstybės objektus, patekimo į juos ar jų apžiūrėjimo patvirtinimo tvarką;

e) įsipareigojimą laiku pranešti rangovo kompetentingai institucijai apie visus įvykusius, mėgintus ar įtariamus neteisėtos prieigos prie įslaptintos informacijos arba saugumo pažeidimo atvejus;

f) su įslaptintu sandoriu susijusios įslaptintos informacijos naudojimą tik su įslaptinto sandorio dalyku susijusiems tikslams;

g) griežtą įslaptintos informacijos sunaikinimo procedūrų laikymąsi.

5. Įslaptintos informacijos apsaugai reikalingos priemonės, taip pat dėl neteisėtos prieigos prie įslaptintos informacijos arba saugumo pažeidimo informaciją parengusiai Šaliai padarytų galimų nuostolių įvertinimas ir kompensavimo tvarka išsamiau išdėstoma atitinkamame įslaptintame sandoryje.

6. Į sandorius, susijusius su informacija, pažymėta slaptumo žyma RIBOTO NAUDOJIMO / RESTRICTED / შეზღუდული სარგებლობისთვის, įtraukiamas atitinkamas straipsnis, kuriuo nustatomos minimalios priemonės, taikytinos tokios įslaptintos informacijos apsaugai. Kompetentingos institucijos informuojamos apie tokius sandorius.

9 straipsnis

Vizitai

1. Atvykstantys asmenys gauna išankstinį priimančios valstybės valdymo / kompetentingos institucijos leidimą, išduotą pagal jos nacionalinės teisės aktus, tik jei jie turi teisę susipažinti su įslaptinta informacija pagal jų nacionalinės teisės aktus ir jei jiems būtina susipažinti su įslaptinta informacija ar patekti į patalpas, kuriose įslaptinta informacija yra rengiama, tvarkoma ar saugoma.

2. Prašyme leisti atvykti su vizitu pateikiama ši informacija:

a) visas atvykstančio asmens vardas ir pavardė, gimimo data ir vieta, asmens kodas ir (arba) paso (arba asmens tapatybės kortelės) numeris;

b) atvykstančio asmens pilietybė;

c) atvykstančio asmens pareigos ir organizacijos, kuriai jis atstovauja, pavadinimas;

d) informacija apie atvykstančiam asmeniui išduotą asmens patikimumo pa-

žymėjimą;

e) vizito tikslas, siūloma darbo programa ir numatoma vizito data;

f) organizacijų ir objektų, kuriuose bus lankomasi, pavadinimai.

3. Kiekviena Šalis pagal atitinkamus nacionalinės teisės aktus užtikrina atvykstančių asmenų asmens duomenų apsaugą.

10 straipsnis

Neteisėta prieiga prie įslaptintos informacijos arba saugumo pažeidimas

1. Neteisėtos prieigos prie įslaptintos informacijos arba saugumo pažeidimo atveju, valstybės, kurioje buvo neteisėtai pasinaudota prieiga prie įslaptintos informacijos arba buvo pažeistas saugumas, kompetentinga institucija kuo skubiau apie tai praneša kitai kompetentingai institucijai ir užtikrina atitinkamą tyrimą. Prireikus Šalys bendradarbiauja atliekant tyrimą.

2. Kitai Šaliai pranešami neteisėtos prieigos prie įslaptintos informacijos arba saugumo pažeidimo tyrimo rezultatai ir pateikiama galutinė išvada dėl priežasčių ir padarytos žalos masto.

11 straipsnis

Išlaidos

Kiekviena Šalis apmoka savo išlaidas, susijusias su jos įsipareigojimų pagal šį Susitarimą vykdymu.

12 straipsnis

Ginčų sprendimas

Visi ginčai, kilę dėl šio Susitarimo aiškinimo ar taikymo, draugiškai sprendžiami rengiant Šalių konsultacijas.

13 straipsnis

Pakeitimai

Šis Susitarimas gali būti keičiamas abipusiu rašytiniu Šalių sutarimu. Pakeitimai įforminami protokolais, kurie tampa sudedamąja šio Susitarimo dalimi. Pakeitimai įsigalioja šio Susitarimo 14 straipsnio 1 dalyje nustatyta tvarka.

14 straipsnis

Baigiamosios nuostatos

1. Šis Susitarimas sudaromas neapibrėžtam laikui ir įsigalioja nuo tos dienos, kai gaunamas paskutinis pranešimas, kuriuo Šalys praneša viena kitai, kad įvykdytos visos vidaus teisinės procedūros, būtinos šiam Susitarimui įsigalioti.

2. Šalis gali nutraukti šį Susitarimą apie tai raštu pranešdama kitai Šaliai. Nutraukimas įsigalioja praėjus šešiems mėnesiams nuo pranešimo apie nutraukimą gavimo dienos. Nutraukus Susitarimą visa įslaptinta informacija, kuria buvo pasikeista, kuo skubiau grąžinama kitai Šaliai. Įslaptinta informacija, kuri negrą-

žinama, yra saugoma vadovaujantis šio Susitarimo nuostatomis tol, kol informaciją parengusi Šalis atleidžia informaciją gaunančią Šalį nuo šio įsipareigojimo.

Sudaryta Briuselyje, 2009 m. birželio 11 d. dviem egzemplioriais lietuvių, gruzinų ir anglų kalbomis. Visi tekstai yra autentiški. Kilus nesutarimų dėl aiškinimo, vadovaujamasi tekstu anglų kalba.

6.1. PAGRINDINIŲ EUROPOS SĄJUNGOS NORMINIŲ TEISĖS AKTŲ, REGLAMENTUOJANČIŲ ĮSLAPTINTOS INFORMACIJOS APSAUGĄ, SĄRAŠAS

Eil. Nr.	Dokumento numeris	Data	Dokumento pavadinimas
1.	OJ L 141	27 May 2011	Council Security Rules
2.	OJ L 202	8 July 2011	Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information echxanged in the interests of the European Union
3.	14845/11	28 September 2011	Guidelines on downgranding and declassifying Council documents
4.	10873/11	23 August 2011	Guidelines on marking EUCI
5.	14035/07 REV 1	22 October 2007	Guidelines on the physical protection of EU classified information (EUCI)
6.	CSC MD 22/2007	20 April 2007	Legal protection of EU classified information in EU Member States

6.2. TARYBOS SPRENDIMAS 2011 M. KOVO 31 D. DĖL ES ĮSLAPTINTOS INFORMACIJOS APSAUGAI UŽTIKRINTI SKIRTŲ SAUGUMO TAISYKLIŲ (2011/292/ES)

Numeris: 2011/292

CELEX numeris: 32011D0292

Publikavimas: Oficialusis leidinys L, 2011-05-27, Nr. 141

2011-03-31 Priėmė - ES Ministrų Taryba

EUROPOS SĄJUNGOS TARYBA, atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 240 straipsnio 3 dalį, atsižvelgdama į 2009 m. gruodžio 1 d. Tarybos sprendimą 2009/937/ES, patvirtinantį Tarybos darbo tvarkos taisykles (1), ypač į jo 24 straipsnį, kadangi:

(1) Siekiant plėtoti Tarybos veiklą visose srityse, kuriose reikia tvarkyti įslaptintą informaciją, tikslinga sukurti Tarybą, jos generalinį sekretoriatą ir valstybes nares apimančią įslaptintos informacijos apsaugą užtikrinančią visapusišką saugumo sistemą.

(2) Šis sprendimas turėtų būti taikomas tais atvejais, kai Taryba, jos parengiamieji organai ir Tarybos generalinis sekretoriatas (TGS) tvarko ES įslaptintą informaciją (ESĮI).

(3) Vadovaudamosi savo nacionaliniais įstatymais ir kitais teisės aktais ir tiek, kiek reikia Tarybos veiklai užtikrinti, valstybės narės turėtų laikytis šio sprendimo, kai jų kompetentingos institucijos, personalas ir rangovai tvarko ESĮI, kad visi būtų tikri, jog yra užtikrinta lygiavertė ESĮI apsauga.

(4) Taryba ir Komisija yra įsipareigojusios taikyti lygiaverčius ESĮI apsaugą užtikrinančius saugumo standartus.

(5) Taryba pabrėžia, jog svarbu, kad Europos Parlamentas ir kitos ES institucijos, agentūros, įstaigos ar tarnybos atitinkamais atvejais prisidėtų prie įslaptintos informacijos apsaugos principų, standartų ir taisyklių, būtinų siekiant apsaugoti Sąjungos ir jos valstybių narių interesus, įgyvendinimo.

(6) Pagal Europos Sąjungos sutarties V antraštines dalies 2 skyrių įsteigtos ES agentūros ir įstaigos, Europolas ir Eurojustas vykdydami savo vidaus darbo organizavimą, taiko šiame sprendime nustatytus ESĮI apsaugai užtikrinti skirtus pagrindinius principus ir būtiniausius standartus, kaip numatyta atitinkamuose jų įsteigimo teisės aktuose.

(7) Pagal ES sutarties V antraštinės dalies 2 skyrių vykdomų krizių valdymo operacijų metu taikomos Tarybos patvirtintos ESĮI apsaugai užtikrinti skirtos saugumo taisyklės, jas taiko ir jose dalyvaujantis personalas.

(8) ES specialieji įgaliotiniai ir jų darbuotojų grupių nariai taiko Tarybos patvirtintas ESĮI apsaugai užtikrinti skirtas saugumo taisykles.

(9) Šis sprendimas priimamas nepažeidžiant Sutarties dėl Europos Sąjungos veikimo (SESV) 15 ir 16 straipsnių ir jų įgyvendinamųjų aktų.

(10) Šis sprendimas priimamas nedarant poveikio dabartinei valstybių narių praktikai, susijusiai su nacionalinių parlamentų informavimu apie Sąjungos veiklą,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis. Tikslas, taikymo sritis ir sąvokų apibrėžtys

1. Šis sprendimas nustato pagrindinius ESĮI apsaugai užtikrinti skirtus saugumo principus ir būtiniausius standartus.

2. Šie pagrindiniai saugumo principai ir būtiniausi standartai taikomi Tarybai bei TGS ir jų privalo laikytis valstybės narės, vadovaudamosi savo atitinkamais nacionaliniais įstatymais ir kitais teisės aktais, kad visi būtų tikri, jog yra užtikrinta lygiavertė ESĮI apsauga.

3. Šio sprendimo taikymo tikslais, taikomos A priedėlyje pateiktos sąvokų apibrėžtys.

2 straipsnis. ESĮI sąvokos apibrėžtis, slaptumo žymos ir kitos žymos

1. ES įslaptinta informacija (ESĮI) – bet kuri informacija arba medžiaga, kuriai suteikta ES slaptumo žyma ir kurią neteisėtai atskleidus galėtų būti padaryta tam tikro dydžio žala Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

2. ESĮI žymima viena iš šių slaptumo žymų:

a) TRÉS SECRET UE/EU TOP SECRET : informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti padaryta ypatingai didelė žala Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

b) SECRET UE/EU SECRET : informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti rimtai pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

c) CONFIDENTIEL UE/EU CONFIDENTIAL : informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

d) RESTREINT UE/EU RESTRICTED : informacija ir medžiaga, kurios neteisėtas atskleidimas galėtų būti nepalankus Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

3. ESĮI žymima slaptumo žyma pagal 2 dalį. Ji gali būti pažymėta papildoma žyma, skirta nurodyti veiklos sritį, su kuria ji yra susijusi, nurodyti įslaptintos informacijos rengėją, apriboti jos platinimą, naudojimą ar suteikimą.

3 straipsnis. Įslaptinimo administravimas

1. Kompetentingos institucijos užtikrina, kad ESĮI būtų žymima tinkama slaptumo žyma, būtų aiškiai nurodoma, kad tai yra įslaptinta informacija, ir jai būtų suteikta slaptumo žyma tik tokiam laikotarpiui, kuris yra būtinas.

2. ESĮI slaptumo žymos laipsnis nesumažinamas arba ji neišslaptinama ir nekeičiamos arba nepanaikinamos 2 straipsnio 3 dalyje nurodytos žymos be išankstinio įslaptintos informacijos rengėjo rašytinio sutikimo.

3. Taryba patvirtina ESĮI rengimo saugumo politiką, kuri apima praktinį žymų vadovą.

4 straipsnis. Įslaptintos informacijos apsauga

1. ESĮI apsaugoma laikantis šio sprendimo.

2. Bet kokios ESĮI turėtojas yra atsakingas už jos apsaugą pagal šį sprendimą.

3. Valstybėms narėms nacionaline slaptumo žyma pažymėtą įslaptintą informaciją įtraukus į Europos Sąjungos struktūras ar tinklus Taryba ir TGS tą informaciją apsaugo laikydamasi reikalavimų, taikomų lygiaverčio slaptumo žymos laipsnio ESĮI, kaip nustatyta B priedėlyje pateiktoje slaptumo žymų atitikmenų lentelėje.

4. Didelio ESĮI kiekio ar ESĮI rinkinio atveju gali būti reikalaujama užtikrinti tokio lygio apsaugą, kuri taikoma aukštesnio laipsnio slaptumo žyma pažymėtai informacijai.

5 straipsnis. Saugumo rizikos valdymas

1. ESĮI kylančios rizikos valdymas yra procesas. Šio proceso tikslas – nustatyti žinomą saugumo riziką, apibrėžti saugumo priemones tokiai rizikai sumažinti iki priimtino lygio pagal šiame sprendime išdėstytus pagrindinius principus ir būtiniausius standartus ir taikyti šias priemones laikantis nuodugnios apsaugos sąvokos, kaip apibrėžta A priedėlyje. Reguliariai atliekamas tokių priemonių efektyvumo vertinimas.

2. ESĮI apsaugai užtikrinti skirtos saugumo priemonės visą savo gyvavimo ciklą turi atitikti jos slaptumo žymos laipsnį, informacijos ar medžiagos formą ir kiekį, patalpų, kuriose laikoma ESĮI, vietos ir konstrukcijos reikalavimus ir turi būti parenkamos atsižvelgiant į vietos lygiu įvertintą piktavališkos ir (arba) nusikalstamos veiklos, įskaitant šnipinėjimą, sabotažą ar terorizmą, keliamą grėsmę.

3. Nenumatytų atvejų planuose turi būti atsižvelgiama į poreikį apsaugoti ESĮI nepaprastosios padėties atvejais siekiant užkirsti kelią galimybei neteisėtai susipažinti su šia informacija, ją atskleisti ar prarasti jos vientisumą arba galimybę ja naudotis.

4. Veiklos tęstinumo planuose numatomos prevencinės ir atstatymo priemonės siekiant sumažinti didelių klaidų ar incidentų poveikį ESĮI administravimui ir saugojimui.

6 straipsnis. Šio sprendimo įgyvendinimas

1. Remdamasi Saugumo komiteto rekomendacija, Taryba prireikus patvirtina saugumo politiką, kuria nustatomos šio sprendimo įgyvendinimo priemonės.

2. Saugumo komitetas savo lygiu gali susitarti dėl saugumo gairių, kurios skirtos papildyti ar sustiprinti šį sprendimą, ir pritarti Tarybos patvirtintai saugumo politikai.

7 straipsnis. Personalo patikimumas

1. Personalo patikimumas – priemonių taikymas, siekiant užtikrinti, kad galimybė susipažinti su ESĮI, būtų suteikta tik asmenims, kurie:

- atitinka principą „būtina žinoti“,

- atitinkamais atvejais turi atitinkamo slaptumo žymos laipsnio asmens patikimumo pažymėjimus, ir

- informuoti apie jų pareigas.

2. Personalo patikimumo tikrinimo procedūrų tikslas – nustatyti, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti suESĮI.

3. Prieš TGS dirbantiems asmenims, kuriems dėl jų pareigų gali reikėti susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ESĮI, leidžiant susipažinti su tokia ESĮI, jų visų patikimumas turi būti patikrintas atitinkamu lygiu. Asmens patikimumo pažymėjimo išdavimo tvarka, taikoma TGS pareigūnams ir kitiems tarnautojams, išdėstyta I priede.

4. Prieš 14 straipsnio 3 dalyje nurodytiems valstybių narių darbuotojams, kuriems dėl jų pareigų gali reikėti susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ESĮI, leidžiant susipažinti su tokia ESĮI, jų patikimumas turi būti patikrintas atitinkamu lygiu arba jie turi turėti kitus tinkamus leidimus atsižvelgiant į jų atliekamas funkcijas pagal nacionalinius įstatymus ir kitus teisės aktus.

5. Visi asmenys, prieš jiems suteikiant leidimą susipažinti su ESĮI, o vėliau – reguliariai, informuojami apie pareigą saugoti ESĮI pagal šį sprendimą ir jie ją patvirtina.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos I priede.

8 straipsnis. Fizinis saugumas

1. Fizinis saugumas yra fizinių ir techninių apsaugos priemonių taikymas siekiant užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI.

2. Fizinės saugumo priemonės skirtos sutrukdyti įsibrauti slaptai arba įsiveržti jėga, atgrasyti nuo neteisėtų veiksmų, sutrukdyti jiems bei juos nustatyti, ir sudaryti sąlygas suskirstyti personalą pagal tai, kas gali susipažinti su ESĮI, vadovaujantis principu „būtina žinoti“. Tokios priemonės grindžiamos rizikos valdymo procesu.

3. Fizinio saugumo priemonės taikomos visose patalpose, pastatuose, kabinetuose, salėse ir kitose zonose, kuriose tvarkoma arba saugoma ESĮI, įskaitant zonas, kuriose įrengtos ryšių ir informacinės sistemos, kaip apibrėžta 10 straipsnio 2 dalyje.

4. Zonos, kuriose saugoma CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ESĮI, įrengiamos kaip saugumo zonos pagal II priedo nuostatas ir patvirtinamos kompetentingos saugumo institucijos.

5. CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėtos ESĮI apsaugai naudojama tik patvirtinta įranga ar prietaisai.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos II priede.

9 straipsnis. Įslaptintos informacijos administravimas

1. Įslaptintos informacijos administravimas – administracinių ESĮI kontrolės visą jos gyvavimo ciklą priemonių taikymas siekiant papildyti 7, 8 ir 10 straipsniuose numatytas priemones ir tokiu būdu atgrasyti nuo tokios informacijos sąmoningo ar tikslingo atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius. Tokios priemonės visų pirma yra susijusios su ESĮI rengimu, registravimu, kopijavimu, vertimu, gabenimu ir naikinimu.

2. CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija saugumo tikslais registruojama prieš ją platinant ir ją gavus. TGS kompetentingos tarnybos ir valstybių narių kompetentingos institucijos šiuo tikslu sukuria registratūrų sistemą. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija registruojama tam skirtuose registruose.

3. Tarnybas ir patalpas, kuriose ESĮI tvarkoma arba saugoma, reguliariai tikrina kompetentinga saugumo institucija.

4. Už fiziškai apsaugotų zonų ribų ESĮI iš vienos tarnybos į kitą ir iš vienų patalpų į kitas perduodama šiais būdais:

a) paprastai ESĮI perduodama elektroninėmis priemonėmis apsaugant informaciją pagal 10 straipsnio 6 dalį patvirtintomis šifravimo priemonėmis;

b) kai nenaudojamos a punkte nurodytos priemonės, ESĮI gabenama:

i) elektroninėse laikmenose (pvz., USB atmintinėse, kompaktiniuose diskuose, kietuosiuose diskuose), informaciją apsaugant pagal 10 straipsnio 6 dalį patvirtintomis šifravimo priemonėmis; arba

ii) visais kitais atvejais, kompetentingos saugumo institucijos nurodytu būdu, laikantis atitinkamų III priede nustatytų apsaugos priemonių.

5. Šio straipsnio įgyvendinimo nuostatos išdėstytos III priede.

10 straipsnis. ESĮI, tvarkomos naudojantis ryšių ir informacinėmis sistemomis, apsauga

1. Informacijos saugumo užtikrinimas (ISU) ryšių ir informacinių sistemų srityje – užtikrinimas, kad tokiose sistemose tvarkoma informacija bus apsaugota ir kad, valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti, ir tada, kada turi veikti. Veiksmingas ISU užtikrina tinkamą konfidencialumo, vientisumo, prieinamumo, atsakomybės už veiksmus prisiėmimo ir autentiškumo lygį. ISU grindžiamas rizikos valdymo procesu.

2. Ryšių ir informacinė sistema – tai sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu. Ryšių ir informacinė sistema apima visas sistemos dalis, kurių reikia jos veikimui, įskaitant infrastruktūrą, organizavimą, personalą ir informacijos šaltinius. Šis sprendimas taikomas ryšių ir informacinėmis sistemoms, kuriose tvarkoma ESĮI (RIS).

3. ESĮI RIS tvarkoma laikantis ISU principo.

4. Visa RIS turi būti akredituojama. Akreditavimo tikslas – įsitikinti, kad įgyvendintos visos atitinkamos saugumo priemonės ir kad pasiektas pakankamas ESĮI ir RIS apsaugos lygis, vadovaujantis šiuo sprendimu. Pareiškime dėl akreditavimo nurodomas aukščiausias informacijos, kuri gali būti tvarkoma

RIS, slaptumo žymos laipsnis ir atitinkami reikalavimai bei sąlygos.

5. RIS, kurioje tvarkoma CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, apsaugoma tokiu būdu, kad informacija negalėtų būti neteisėtai atskleista dėl netyčinio elektromagnetinio spinduliavimo (TEMPEST apsaugos priemonės).

6. Kai ESĮI apsauga užtikrinama šifravimo priemonėmis, tokios priemonės patvirtinamos taip:

a) SECRET UE/EU SECRET ir aukštesnio laipsnio slaptumo žyma pažymėtos informacijos konfidencialumas užtikrinamas taikant šifravimo priemones, kurias remdamasi Saugumo komiteto rekomendacija patvirtina Taryba, vykdydama Kriptografijos patvirtinimo institucijos (KPI) funkcijas;

b) CONFIDENTIEL UE/EU CONFIDENTIAL arba RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtos informacijos konfidencialumas užtikrinamas taikant šifravimo priemones, kurias remdamasis Saugumo komiteto rekomendacija patvirtina Tarybos generalinis sekretorius (toliau – generalinis sekretorius), vykdydamas KPI funkcijas.

Nepažeidžiant b punkto, valstybių narių nacionalinėse sistemose CONFIDENTIEL UE/EU CONFIDENTIAL arba RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtos ESĮI konfidencialumas gali būti apsaugomas taikant šifravimo priemones, kurias patvirtina valstybės narės KPI.

7. Perduodant ESĮI elektroninėmis priemonėmis naudojamos patvirtintos šifravimo priemonės. Nepaisant šio reikalavimo, esant nepaprastosios padėties sąlygoms arba specifinių techninių konfigūracijų atvejais, kaip nurodyta IV priede, gali būti taikomos specialios procedūros.

8. TGS kompetentingos tarnybos ir valstybių narių kompetentingos institucijos atitinkamai nustato šias ISU funkcijas vykdančias struktūras:

a) ISU instituciją (ISUI);

b) TEMPEST instituciją (TEI);

c) Kriptografijos patvirtinimo instituciją (KPI);

d) Kriptografijos platinimo instituciją (KPLI).

9. TGS kompetentingos tarnybos ir valstybių narių kompetentingos institucijos kiekvienai sistemai atitinkamai nustato:

a) Saugumo akreditavimo instituciją (SAI);

b) ISU operacinę instituciją.

10. Šio straipsnio įgyvendinimo nuostatos išdėstytos IV priede.

11 straipsnis. Pramoninis saugumas

1. Pramoninis saugumas – priemonių, kurias rangovai arba subrangovai taiko derybų dėl sutarčių sudarymo metu ir visą įslaptintų sutarčių gyvavimo ciklą siekdami užtikrinti ESĮI apsaugą, taikymas. Tokiose sutartyse nenumatoma galimybė susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija.

2. TGS sutartimi gali patikėti pramonės arba kitiems subjektams, registruotiems valstybėje narėje arba trečiojoje valstybėje, kuri yra sudariusi susitarimą arba administracinį susitarimą pagal 12 straipsnio 2 dalies a arba b punktą, užduotis, kurioms atlikti reikia arba reikės susipažinti su ESĮI arba ją tvarkyti ar

laikyti.

3. TGS, kaip perkančioji institucija, užtikrina, kad sudarant įslaptintas sutartis su pramonės ar kitais subjektais būtų laikomasi šiame sprendime išdėstytų ir sutartyje nurodytų būtiniausių pramoninio saugumo standartų.

4. Kiekvienos valstybės narės nacionalinė saugumo institucija (NSI), paskirtoji saugumo institucija (PSI) ar bet kuri kita kompetentinga institucija, kiek tai įmanoma pagal nacionalinius įstatymus ir kitus teisės aktus, užtikrina, kad jų teritorijoje įregistruoti rangovai ir subrangovai derybų dėl sutarčių sudarymo metu arba vykdydami įslaptintą sutartį imtųsi visų tinkamų ESĮI apsaugos priemonių.

5. Kiekvienos valstybės narės NSI, PSI ar kita kompetentinga saugumo institucija, laikydamosi nacionalinių įstatymų ir kitų teisės aktų, užtikrina, kad minėtoje valstybėje narėje įregistruoti rangovai ar subrangovai, dalyvaujantys įslaptintose sutartyse arba subrangos sutartyse, pagal kurias jas vykdant arba prieš jas sudarant turi būti suteikta galimybė savo patalpose susipažinti su įslaptinta informacija, pažymėta slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET, turėtų reikiamą slaptumo žymos laipsnį atitinkantį Įmonės patikimumą patvirtinantį pažymėjimą (ĮPPP).

6. Rangovo ar subrangovo darbuotojams, kuriems vykdant įslaptintą sutartį reikia susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija, atitinkama NSI, PSI ar kita kompetentinga saugumo institucija laikydamasi nacionalinių įstatymų ir kitų teisės aktų bei I priede nustatytų būtiniausių saugumo standartų suteikia asmens patikimumo pažymėjimą (APP).

7. Šio straipsnio įgyvendinimo nuostatos išdėstytos V priede.

12 straipsnis. Keitimasis įslaptinta informacija su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

1. Tarybai nusprendus, kad reikia keistis ESĮI su trečiąja valstybe arba tarptautine organizacija, šiuo tikslu nustatoma tinkama tvarka.

2. Siekdama nustatyti tokią tvarką ir apibrėžti abipusiškumo taisykles dėl įslaptintos informacijos, kuria keičiamasi, apsaugos

a) Taryba sudaro susitarimus dėl keitimuisi ESĮI ir jos apsaugai užtikrinti skirtų saugumo procedūrų (toliau – susitarimai dėl informacijos saugumo); arba

b) generalinis sekretorius gali pagal VI priedo 17 punktą sudaryti administracinius susitarimus tuomet, kai ESĮI, kuri turi būti suteikta, slaptumo žymos laipsnis paprastai nėra aukštesnis nei RESTREINT UE/EU RESTRICTED.

3. 2 dalyje nurodytuose susitarimuose dėl informacijos saugumo arba administraciniuose susitarimuose numatomos nuostatos, kuriomis užtikrinama, jog trečiosioms valstybėms arba tarptautinėms organizacijoms gavus ESĮI tai informacijai užtikrinama jos slaptumo žymos laipsnį atitinkanti apsauga, remiantis būtiniausiais standartais, kurie yra ne mažiau griežti nei šiame sprendime nustatyti standartai.

4. Sprendimą suteikti Tarybos parengtą ESĮI trečiajai valstybei arba tarptautinei organizacijai priima Taryba atskirai kiekvienu konkrečiu atveju atsižvelgdama į tokios informacijos pobūdį ir turinį bei gavėjo atitiktį principui „būtina žinoti“ ir įvertinusi naudą ES. Jeigu Taryba nėra įslaptintos informacijos, kurią

prašoma suteikti, rengėja, TGS pirmiausia bando gauti jos įslaptintos informacijos rengėjo raštišką sutikimą suteikti tą informaciją. Jei įslaptintos informacijos rengėjo neįmanoma nustatyti, jo pareigą prisiima Taryba.

5. Įvertinimo vizitai rengiami siekiant įsitikinti, kad trečiojoje valstybėje arba tarptautinėje organizacijoje taikomos ESĮI arba įslaptintos informacijos, kuri suteikta ar kuria keičiamasi, apsaugos priemonės yra veiksmingos.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos VI priede.

13 straipsnis. ESĮI saugumo pažeidimai ir neteisėtas atskleidimas

1. Saugumo pažeidimu laikomas šiame sprendime nustatytoms saugumo taisyklėms priešingas asmens veiksmas arba neveikimas.

2. Laikoma, kad ESĮI neteisėtai atskleista, jeigu pažeidus saugumo taisykles ji visa arba jos dalis yra atskleista leidimo neturintiems asmenims.

3. Apie visus saugumo pažeidimus arba įtariamus saugumo pažeidimus nedelsiant pranešama kompetentingai saugumo institucijai.

4. Tai atvejais, kai žinoma arba yra pagrįstų priežasčių manyti, kad ESĮI buvo neteisėtai atskleista arba prarasta, kompetentinga saugumo institucija, vadovaudamasi atitinkamais įstatymais ir kitais teisės aktais, imasi visų atitinkamų priemonių:

a) informuoti įslaptintos informacijos rengėją;

b) užtikrinti, kad siekiant nustatyti faktus tokį atvejį nagrinėtų su pažeidimu tiesiogiai nesusijęs personalas;

c) įvertinti galimą ES ar valstybių narių interesams padarytą žalą;

d) imtis atitinkamų priemonių, kad būtų užkirstas kelias pažeidimui pasikartoti; ir

e) kad atitinkamos institucijos būtų informuotos apie atliktus veiksmus.

5. Bet kuriam asmeniui, kuris pažeidė šiame sprendime nustatytas saugumo taisykles, gali būti taikomos drausminės priemonės vadovaujantis taikomomis taisyklėmis. Asmeniui, kuris neteisėtai atskleidė ar pametė ESĮI, taikomos drausminės ir (arba) teisinės priemonės vadovaujantis taikomais įstatymais, taisyklėmis ir kitais teisės aktais.

14 straipsnis. Atsakomybė už įgyvendinimą

1. Taryba imasi visų priemonių, būtinų siekiant užtikrinti bendrą šio sprendimo taikymo nuoseklumą.

2. Generalinis sekretorius imasi visų priemonių, būtinų užtikrinti, kad TGS pareigūnai ir kiti tarnautojai, į TGS komandiruoti darbuotojai ir TGS samdyti rangovai, tvarkydami arba saugodami ESĮI arba kitą įslaptintą informaciją Tarybos naudojamose patalpose ir TGS, įskaitant trečiosiose valstybėse esančias ryšių palaikymo tarnybas, laikytųsi šio sprendimo.

3. Vadovaudamosi savo atitinkamais nacionaliniais įstatymais ir kitais teisės aktais, valstybės narės imasi visų atitinkamų priemonių siekdamos užtikrinti, kad tvarkydami ar saugodami ESĮI šio sprendimo laikytųsi:

a) valstybių narių nuolatinių atstovybių Europos Sąjungoje darbuotojai ir Tarybos arba jos parengiamųjų organų posėdžiuose ar kitoje Tarybos veikloje

dalyvaujantys nacionalinių delegacijų nariai;

b) kiti valstybių narių nacionalinių administracinių įstaigų darbuotojai, įskaitant į tas administracines įstaigas komandiruotus darbuotojus, dirbantys tiek valstybėse narėse, tiek užsienyje;

c) kiti asmenys, kuriems valstybėse narėse dėl jų funkcijų yra suteiktas tinkamas leidimas susipažinti su ESĮI; ir

d) valstybių narių rangovai, dirbantys tiek valstybėse narėse, tiek užsienyje.

15 straipsnis. Saugumo organizavimas Taryboje

1. Atlikdama savo vaidmenį užtikrinti bendrą šio sprendimo taikymo nuoseklumą, Taryba tvirtina:

a) 12 straipsnio 2 dalies a punkte nurodytus susitarimus;

b) sprendimus dėl ESĮI suteikimo trečiosioms valstybėms ir tarptautinėms organizacijoms;

c) metinę tikrinimo programą, kurią siūlo generalinis sekretorius bei rekomenduoja Saugumo komitetas ir kuri yra skirta valstybių narių tarnybų bei patalpų ir ES agentūrų bei įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, taip pat ir Europolo ir Eurojusto tikrinimams ir įvertinimo vizitams į trečiąsias valstybes bei tarptautines organizacijas siekiant įsitikinti priemonių, įgyvendintų siekiant apsaugoti ESĮI, veiksmingumu; ir

d) saugumo politiką, kaip numatyta 6 straipsnio 1 dalyje.

2. Generalinis sekretorius vykdo TGS saugumo tarnybos funkcijas. Vykdydamas tas funkcijas generalinis sekretorius:

a) įgyvendina Tarybos saugumo politiką ir ją nuolat peržiūri;

b) bendradarbiauja su valstybių narių NSI visais su Tarybos veikla susijusiais saugumo klausimais dėl įslaptintos informacijos apsaugos;

c) išduoda ES APP TGS pareigūnams ir kitiems tarnautojams pagal 7 straipsnio 3 dalį, prieš jiems suteikiant leidimą susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija;

d) atitinkamais atvejais nurodo ištirti Tarybos turimos ar parengtos įslaptintos informacijos faktinio ar įtariamo neteisėto atskleidimo arba praradimo atvejus ir prašo atitinkamų saugumo institucijų padėti atlikti šiuos tyrimus;

e) reguliariai tikrina įslaptintos informacijos apsaugai užtikrinti skirtas saugumo priemones TGS patalpose;

f) reguliariai tikrina ESĮI apsaugai užtikrinti skirtas ES agentūrose ir įstaigose, įsteigtose pagal ES sutarties V antraštinės dalies 2 skyrių, Europole ir Eurojuste, taip pat ir pagal ES sutarties V antraštinės dalies 2 skyrių vykdomų krizių valdymo operacijų metu ir ES specialiųjų įgaliotinių (ESSĮ) bei jų darbuotojų grupių narių taikomas saugumo priemones;

g) kartu su atitinkama NSI ir suderinęs su ja reguliariai tikrina ESĮI apsaugai užtikrinti skirtas saugumo priemones valstybių narių tarnybose ir patalpose;

h) derina saugumo priemones su valstybių narių kompetentingomis institucijomis, kurios yra atsakingos už įslaptintos informacijos apsaugą, ir atitinkamai su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis, įskaitant dėl grėsmių ESĮI saugumui pobūdžio ir apsaugos nuo jų priemonių;

i) sudaro administracinius susitarimus, nurodytus 12 straipsnio 2 dalies b punkte; ir

j) rengia pradinį ir reguliarius įvertinimo vizitus į trečiąsias valstybes bei tarptautines organizacijas siekdamas įsitikinti priemonių, įgyvendintų siekiant apsaugoti ESĮI, kuri teikiama arba kuria keičiamasi, veiksmingumu.TGS saugumo tarnyba padeda generaliniam sekretoriui vykdyti šias užduotis.

3. Įgyvendindamos 14 straipsnio 3 dalį valstybės narės turėtų:

a) paskirti už ESĮI apsaugai užtikrinti skirtas saugumo priemones atsakingą NSI tam, kad:

i) viešosiose ar privačiose nacionalinėse institucijose, įstaigose ar agentūrose, esančiose valstybės teritorijoje arba užsienyje, laikoma ESĮI būtų apsaugota pagal šį sprendimą;

ii) būtų užtikrintas ESĮI apsaugai skirtų saugumo priemonių reguliarus tikrinimas;

iii) dėl jų atliekamų funkcijų visų nacionalinėse administracinėse įstaigose dirbančių asmenų ir rangovo pasamdytų asmenų, kuriems gali būti leista susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, patikimumas būtų tinkamai patikrintas arba jie turėtų kitus tinkamus leidimus pagal nacionalinius įstatymus ir kitus teisės aktus;

iv) siekiant iki minimumo sumažinti ESĮI neteisėto atskleidimo ar praradimo pavojų būtų įdiegtos būtinos saugumo programos;

v) su ESĮI apsauga susijusių saugumo klausimų derinimą su kitomis kompetentingomis nacionalinėmis institucijomis, įskaitant su nurodytąsias šiame sprendime; ir

vi) būtų atsakyta į atitinkamus ES agentūrų ir įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, Europolo ir Eurojusto, taip pat pagal ES sutarties V antraštinės dalies 2 skyrių vykdomų krizių valdymo operacijų personalo bei ESSĮ ir jų darbuotojų grupių narių prašymus išduoti asmens patikimumo pažymėjimus. NSI yra išvardytos C priedėlyje;

b) užtikrinti, kad jų kompetentingos institucijos vyriausybėms, o per jas Tarybai, teiktų informaciją apie ESĮI saugumui kylančių grėsmių pobūdį ir apsaugos nuo jų priemones bei patarti šiais klausimais.

16 straipsnis. Saugumo komitetas

1. Įsteigiamas Saugumo komitetas. Jis nagrinėja ir vertina saugumo klausimus, kuriems taikomas šis sprendimas, ir atitinkamai teikia rekomendacijas Tarybai.

2. Saugumo komitetą sudaro valstybių narių NSI atstovai, o jo posėdžiuose dalyvauja Komisijos ir Europos išorės veiksmų tarnybos atstovas. Jam pirmininkauja generalinis sekretorius arba jo paskirtas atstovas. Jo posėdžiai rengiami pagal Tarybos nurodymus arba generalinio sekretoriaus ar NSI prašymu.ES agentūrų ir įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, taip pat ir Europolo ir Eurojusto atstovai gali būti kviečiami dalyvauti posėdžiuose svarstant jiems svarbius klausimus.

3. Saugumo komitetas savo veiklą organizuoja taip, kad galėtų teikti reko-

mendacijas konkrečių saugumo sričių klausimais. Jis įsteigia ekspertų pogrupį ISU klausimais ir prireikus kitus ekspertų pogrupius. Šis komitetas parengia tokių ekspertų pogrupių įgaliojimus, o šie pogrupiai teikia jam savo veiklos ataskaitas, įskaitant prireikus bet kurias rekomendacijas Tarybai.

17 straipsnis. Ankstesnio sprendimo pakeitimas

1. Šis sprendimas panaikina ir pakeičia 2001 m. kovo 19 d. Tarybos sprendimą 2001/264/EB dėl Tarybos saugumo nuostatų patvirtinimo (2).

2. Visa ESĮI, įslaptinta pagal Sprendimą 2001/264/EB, toliau saugoma pagal šio sprendimo atitinkamas nuostatas.

18 straipsnis. Įsigaliojimas

Šis sprendimas įsigalioja jo paskelbimo Europos Sąjungos oficialiajame leidinyje dieną.

Priimta Briuselyje 2011 m. kovo 31 d.

(1) OL L 325, 2009 12 11, p. 35.
(2) OL L 101, 2001 4 11, p. 1.

PRIEDAI

I PRIEDAS
Personalo patikimumas

II PRIEDAS
Fizinis saugumas

III PRIEDAS
Įslaptintos informacijos administravimas

IV PRIEDAS
RIS tvarkomos ESĮI apsauga

V PRIEDAS
Pramoninis saugumas

VI PRIEDAS
Keitimasis įslaptinta informacija su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

I PRIEDAS
PERSONALO PATIKIMUMAS

I. ĮVADAS

1. Šiame priede nustatytos 7 straipsnio įgyvendinimo nuostatos. Jame nustatomi kriterijai, kuriais remiantis nustatoma, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESĮI, ir šiuo tikslu taikytinos tikrinimo bei administracinės procedūros.

2. Šiame priede, išskyrus atvejus, kai yra svarbu atskirti, terminas „asmens patikimumo pažymėjimas“ reiškia nacionalinį asmens patikimumo pažymėjimą (nacionalinį APP) ir (arba) ES asmens patikimumo pažymėjimą (ES APP), kaip apibrėžta A priedėlyje.

II. LEIDIMAS SUSIPAŽINTI SU ESĮI

3. Asmeniui leidžiama susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ES įslaptinta informacija tik tuo atveju, kai:

a) nustatoma, kad jis atitinka principą „būtina žinoti“;

b) dėl jo atliekamų funkcijų jam buvo išduotas atitinkamo slaptumo žymos laipsnio APP arba kiti tinkami leidimai pagal nacionalinius įstatymus ir kitus teisės aktus; ir

c) jis buvo informuotas apie ESĮI apsaugai užtikrinti skirtas saugumo taisykles bei procedūras ir patvirtino savo pareigą saugoti tokią informaciją.

4. Kiekviena valstybė narė ir TGS savo struktūrose nustato tas pareigybes, kurias užimantiems asmenims reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija ir todėl jie turi turėti atitinkamo slaptumo žymos laipsnio APP.

III. ASMENS PATIKIMUMO PAŽYMĖJIMUI TAIKOMI REIKALAVIMAI

5. NSI ir kitos kompetentingos nacionalinės institucijos, gavusios pagal tinkamus įgaliojimus pateiktą prašymą, privalo užtikrinti, kad būtų vykdomas jų piliečių, kuriems turi būti sudaryta galimybė susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, patikimumo tikrinimas. Tikrinimo standartai turi atitikti nacionalinius įstatymus ir kitus teisės aktus.

6. Jeigu atitinkamas asmuo nuolat gyvena kitos valstybės narės ar trečiosios valstybės teritorijoje, kompetentingos nacionalinės institucijos prašo gyvenamosios vietos valstybės kompetentingos institucijos pagalbos laikydamosi nacionalinių įstatymų ir kitų teisės aktų. Valstybės narės padeda viena kitai vykdyti patikimumo tikrinimą pagal nacionalinius įstatymus ir kitus teisės aktus.

7. Jei leidžiama pagal nacionalinius įstatymus ir kitus teisės aktus, NSI arba kitos kompetentingos nacionalinės institucijos gali vykdyti asmenų, kurie nėra

jų šalies piliečiai ir kuriems reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, patikimo tikrinimą. Tikrinimo standartai turi atitikti nacionalinius įstatymus ir kitus teisės aktus.

Patikimumo tikrinimo kriterijai

8. Asmens lojalumas ir patikimumas, kad jam būtų galima išduoti APP susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, nustatomas vykdant patikimumo tikrinimą. Kompetentinga nacionalinė institucija atlieka bendrą vertinimą, remdamasi tokio patikimumo tikrinimo išvadomis. Nepalanki išvada nebūtinai reiškia, kad bus atsisakyta išduoti APP. Šiuo tikslu taikomi pagrindiniai kriterijai turėtų apimti, atsižvelgiant į nacionalinius įstatymus ir kitus teisės aktus, nagrinėjimą, ar asmuo:

a) įvykdė ar bandė, susitarė su kitais asmenimis arba padėjo kitiems asmenims įvykdyti šnipinėjimo, terorizmo, sabotažo, išdavystės ar kurstymo aktą;

b) yra ar buvo šnipų, teroristų, sabotuotojų ar asmenų, pagrįstai tuo įtariamų, bendrininkas arba yra ar buvo organizacijų ar užsienio valstybių, įskaitant užsienio valstybių žvalgybos tarnybas, kurios gali kelti grėsmę ES ir (arba) valstybių narių saugumui, atstovų bendrininkas, išskyrus atvejus, kai tokiam bendrininkavimui buvo suteiktas leidimas jam vykdant oficialias pareigas;

c) yra ar buvo bet kurios organizacijos, kuri smurtinėmis, ardomosiomis ar kitomis neteisėtomis priemonėmis siekia, inter alia, nuversti valstybės narės vyriausybę, pakeisti valstybės narės konstitucinę tvarką arba pakeisti jos valdymo formą ar politiką, narys;

d) yra ar buvo c punkte apibūdintos bet kurios organizacijos rėmėjas arba yra ar buvo glaudžiai susijęs su tokių organizacijų nariais;

e) tyčia nuslėpė, iškreipė ar suklastojo svarbią, ypač susijusią su saugumo aspektais, informaciją arba tyčia melavo pildydamas asmens patikimumo tikrinimo klausimyną ar dalyvaudamas patikimumo tikrinimo pokalbyje;

f) buvo nuteistas už nusikalstamą veiką ar nusikalstamas veikas;

g) piktnaudžiauja alkoholiu, vartoja nelegalius narkotikus ir (arba) piktnaudžiauja legaliomis narkotinėmis medžiagomis;

h) atlieka ar atliko veiksmus, dėl kurių jį galima šantažuoti ar daryti jam spaudimą;

i) savo elgesiu ar žodžiais pasirodė esąs nesąžiningas, nelojalus ar nepatikimas;

j) rimtai ar pakartotinai pažeidė saugumo nuostatus; arba bandė atlikti ar sėkmingai atliko neteisėtus veiksmus, susijusius su ryšių ir informacinėmis sistemomis;

k) gali patirti spaudimą (pvz., dėl vienos ar kelių ne ES pilietybių turėjimo arba dėl giminaičių ar artimų asmenų, kurie galėtų būti pažeidžiami dėl užsienio žvalgybos tarnybų, teroristų grupių ar kitų ardomojo pobūdžio organizacijų ar asmenų, kurių siekiai gali kelti grėsmę ES ir (arba) valstybių narių saugumo interesams, poveikio).

9. Vykdant patikimumo tikrinimą, atitinkamais atvejais, vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, taip pat gali būti svarbi informacija apie asmens finansinę padėtį ir sveikatą.

10. Vykdant patikimumo tikrinimą, atitinkamais atvejais, vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, taip pat gali būti svarbūs sutuoktinio, sugyventinio ar artimo šeimos nario charakteris, elgesys ir gyvenimo aplinkybės.

Susipažinimui su ESĮI taikomi tikrinimo reikalavimai APP išdavimas pirmą kartą

11. Pradinis APP, leidžiantis susipažinti su slaptumo žymomis CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET pažymėta informacija, grindžiamas patikimumo

patikrinimu, apimančiu bent 5 paskutinių metų laikotarpį arba laikotarpį nuo 18 metų amžiaus iki patikrinimo datos, pasirenkant trumpesnį laikotarpį; patikrinimas apima šiuos aspektus:

a) užpildomas nacionalinis asmens patikimumo tikrinimo klausimynas, atsižvelgiant į ESĮI, su kuria asmeniui gali reikėti susipažinti, slaptumo žymos laipsnį; užpildytas klausimynas perduodamas kompetentingai saugumo institucijai;

b) patikrinta asmens tapatybė / pilietybė / nacionalinė priklausomybė – tikrinama asmens gimimo data bei vieta ir jo tapatybė. Nustatoma buvusi ir dabartinė asmens pilietybė / nacionalinė priklausomybė; taip pat įvertinamas bet kuris asmens pažeidžiamumas, susijęs su galimu užsienio subjektų spaudimu, pavyzdžiui, dėl ankstesnės gyvenamosios vietos ar buvusių ryšių atsirandantis pažeidžiamumas; ir

c) patikrinami nacionaliniai ir vietiniai duomenys – tikrinamas nacionalinio saugumo registras ir centrinis nuosprendžių registras, jei tokie egzistuoja, ir (arba) kiti palyginami vyriausybės ir policijos registrai. Tikrinami teisėsaugos įstaigų, kurių teisinei jurisdikcijai priklausė asmens gyvenamoji arba darbo vieta registrai.

12. Pradinis APP, leidžiantis susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija, grindžiamas patikimumo patikrinimu, apimančiu bent dešimt paskutinių metų laikotarpį arba laikotarpį nuo 18 metų amžiaus iki patikrinimo datos, pasirenkant trumpesnį laikotarpį. Jei organizuojami pokalbiai, kaip toliau nurodyta e punkte, patikrinimas apima bent septynių paskutinių metų laikotarpį arba laikotarpį nuo 18 metų amžiaus iki patikrinimo datos, pasirenkant trumpesnį laikotarpį. Patikimumo pažymėjimų, leidžiančių susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija, išdavimui, atsižvelgiant į nacionalinius įstatymus ir kitus teisės aktus, taikomi ne tik pirmiau 8 punkte nurodyti kriterijai, bet ir tikrinami toliau išvardyti aspektai; jie taip pat gali būti tikrinami prieš išduodant asmens patikimumo pažymėjimus, leidžiančius susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija, jei tai privaloma pagal nacionalinius įstatymus ir kitus teisės aktus:

a) finansinė padėtis – renkama informacija apie asmens finansinę padėtį, kad būtų galima įvertinti dėl rimtų finansinių sunkumų galintį atsirasti pažeidžiamumą užsienio ar šalies vidaus subjektų spaudimo atveju arba kad būtų nustatytas nepaaiškinamas turto padidėjimas;

b) išsilavinimas – renkama informacija siekiant sužinoti apie asmens įgytą išsilavinimą mokyklose, universitetuose ir kitose švietimo įstaigose nuo jo aštuonioliktojo gimtadienio ar per kitą, patikimumo tikrinimą atliekančios institucijos manymu, tinkamą laikotarpį;

c) darbovietės – renkama informacija apie dabartinę ir ankstesnes darbovietes, remiantis tokiais šaltiniais kaip darbo charakteristika, veiklos ar efektyvumo ataskaitos, taip pat darbdavių ar viršininkų informacija;

d) karo tarnyba – jei taikoma, tikrinama, ar asmuo tarnavo ginkluotosiose pajėgose ir kokiu būdu buvo išleistas į atsargą; ir

e) pokalbiai – kai tai numatyta ir leidžiama pagal nacionalinę teisę, organizuojamas (-i) pokalbis (-iai) su asmeniu. Į pokalbį taip pat kviečiami kiti asmenys, kurie gali nešališkai įvertinti asmens biografijos faktus, veiklą, lojalumą ir patikimumą. Kai pagal nacionalinę praktiką tikrinamo asmens prašoma pateikti rekomendacijas, turi būti apklausiami rekomendacijas pateikę asmenys,

išskyrus atvejus, kai yra pagrįstų priežasčių to nedaryti.

13. Prireikus vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais gali būti atliekami papildomi patikrinimai, kad būtų surinkta visa svarbi informacija apie asmenį ir kad būtų pagrįsta arba paneigta nepalanki informacija.

APP atnaujinimas

14. Po to, kai pirmą kartą išduotas APP ir jeigu asmuo nuolat dirbo nacionalinėje administracinėje įstaigoje ar TGS bei jam nuolat reikia dirbti su ESĮI, APP peržiūrimas siekiant jį atnaujinti ne rečiau kaip kas penkerius metus pažymėjimų, leidžiančių susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija, atveju ir ne rečiau kaip kas dešimt metų pažymėjimų, leidžiančių susipažinti su slaptumo žymomis SECRET UE/EU SECRET ir CONFIDENTIEL UE/EU CONFIDENTIAL pažymėta informacija, atveju, skaičiuojant nuo paskutinio patikimumo patikrinimo, kuriuo remiantis buvo išduotas pažymėjimas, rezultatų pranešimo datos. Visuose dėl APP atnaujinimo atliekamuose patikimumo patikrinimuose tikrinamas laikotarpis nuo ankstesnio tikrinimo datos.

15. Siekiant atnaujinti APP tikrinami 11 ir 12 punktuose apibūdinti aspektai.

16. Prašymai dėl atnaujinimo teikiami laiku, atsižvelgiant į tokiam patikimumo tikrinimui atlikti reikiamą laiką. Tačiau atitinkamai NSI ar kitai kompetentingai nacionalinei institucijai gavus atitinkamą prašymą dėl atnaujinimo ir atitinkamą asmens patikimumo tikrinimo klausimyną nepasibaigus APP galiojimo laikotarpiui ir dar neužbaigus būtino patikimumo patikrinimo, kompetentinga nacionalinė institucija gali pratęsti turimo APP galiojimo laikotarpį ne ilgiau kaip 12 mėnesių, jeigu leidžia nacionaliniai įstatymai ir kiti teisės aktai. Jeigu pasibaigus šiam 12 mėnesių laikotarpiui patikimumo patikrinimas dar nebaigtas, asmeniui skiriamos tokios užduotys, kurioms atlikti nereikia turėti APP.

TGS taikoma APP išdavimo procedūra

17. TGS pareigūnų ir kitų tarnautojų atveju TGS saugumo tarnyba nusiunčia užpildytą asmens patikimumo tikrinimo klausimyną valstybės narės, kurios pilietis asmuo yra, NSI, prašydama atlikti patikimumo patikrinimą, skirtą gauti leidimą naudotis tam tikro slaptumo žymos laipsnio ESĮI, su kuria asmeniui reikės susipažinti.

18. Jei TGS sužino patikimumo patikrinimui svarbios informacijos apie asmenį, kuris pateikė prašymą dėl ES APP, TGS, laikydamasis atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI.

19. Užbaigusi patikimumo patikrinimą atitinkama NSI praneša TGS saugumo tarnybai tokio patikrinimo rezultatus, naudodama Saugumo komiteto nustatytą korespondencijai skirtą standartinę formą.

a) Jei patikimumo tikrinimo rezultatai užtikrinamai rodo, kad neturima jokios nepalankios informacijos, kuri leistų abejoti asmens lojalumu ir patikimumu, TGS paskyrimų tarnyba gali asmeniui išduoti ES APP ir leisti susipažinti su iki tam tikro laipsnio slaptumo žyma pažymėta ESĮI iki nustatytos datos;

b) Jei patikimumo tikrinimo rezultatai nėra tokie užtikrinantys, TGS paskyrimų tarnyba apie tai praneša atitinkamam asmeniui, kuris gali prašyti, kad Paskyrimų tarnyba jį išklausytų. Paskyrimų tarnyba gali prašyti kompetentingos NSI pateikti daugiau paaiškinimų, kuriuos ji gali pateikti pagal savo nacionalinius įstatymus ir kitus teisės aktus. Jei rezultatai pasitvirtina, ES APP neišduodamas.

20. Patikimumo tikrinimui bei gautiems rezultatams taikomi atitinkamoje valstybėje narėje galiojantys įstatymai ir kiti teisės aktai, įskaitant su apskundimu susijusius įstatymus ir kitus teisės aktus. TGS paskyrimų tarnybos sprendimai gali būtų apskųsti pagal Europos Sąjungos pareigūnų tarnybos nuostatus ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygas, nustatytus Reglamente (EEB, Euratomas, EAPB) Nr. 259/68 [1] (toliau – Tarnybos nuostatai ir įdarbinimo sąlygos).

21. ES APP galioja visoms užduotims, kurias tas asmuo vykdo TGS ar Europos Komisijoje, su sąlyga, kad tebegalioja jo išdavimą pagrindžiančios aplinkybės.

22. Jeigu asmens tarnyba neprasideda per 12 mėnesių nuo patikimumo patikrinimo rezultatų pranešimo TGS paskyrimų tarnybai arba jeigu asmens tarnyboje daroma 12 mėnesių pertrauka ir tuo laikotarpiu jis nėra priimtas į pareigybę TGS ar valstybės narės nacionalinėje administracinėje įstaigoje, atitinkamos NSI prašoma patvirtinti, kad rezultatai tebegalioja bei yra tinkami.

23. Jei TGS sužino informacijos apie tai, kad galiojantį ES APP turintis asmuo kelia pavojų saugumui, TGS, laikydamasis atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI. Kai NSI informuoja TGS apie tai, kad pagal 19 punkto a papunktį suteiktas užtikrinimas dėl galiojantį ES APP turinčio asmens panaikinamas, TGS paskyrimų tarnyba gali paprašyti pateikti paaiškinimą, kurį NSI gali pateikti pagal nacionalinius įstatymus ir kitus teisės aktus. Jei nepalanki informacija patvirtinama, ES APP panaikinamas, o asmeniui neleidžiama susipažinti su ESĮI ir eiti pareigų, kurias einant jis galėtų susipažinti su ta informacija arba sukelti pavojų saugumui.

24. Apie bet kurį sprendimą panaikinti TGS pareigūno ar kito tarnautojo ES APP ir, atitinkamais atvejais, tokio panaikinimo priežastis pranešama atitinkamam pareigūnui, kuris gali prašyti, kad TGS paskyrimų tarnyba jį išklausytų. NSI teikiamą informaciją reglamentuoja atitinkamoje valstybėje narėje galiojantys įstatymai ir kiti teisės aktai, įskaitant su apeliacijomis susijusius įstatymus ir kitus teisės aktus. TGS paskyrimų tarnybos sprendimai gali būtų apskųsti pagal Tarnybos nuostatus ir įdarbinimo sąlygas.

25. Į TGS komandiruoti nacionaliniai ekspertai, siekiantys eiti pareigas, kurioms reikia ES APP, TGS saugumo tarnybai prieš pradėdami tarnybą pateikia galiojantį nacionalinį APP, leidžiantį susipažinti su ESĮI.

APP registrai

26. Nacionalinių APP ir ES APP, leidžiančių susipažinti su ESĮI, registrus tvarko atitinkamai kiekviena valstybė narė ir TGS. Šiuose registruose bent jau nurodoma ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos laipsnis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma), APP išdavimo data ir jo galiojimo laikas.

27. Kompetentinga saugumo institucija gali išduoti asmens patikimumo pažymėjimą patvirtinančią pažymą (APPP), kurioje nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos laipsnis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma), atitinkamo nacionalinio APP, leidžiančio susipažinti su ESĮI, ar ES APP galiojimo laikas ir pačios pažymos galiojimo laikas.

Reikalavimo turėti APP taikymo išimtys

28. Teisė susipažinti su ESĮI asmenims, kuriems dėl jų atliekamų funkcijų suteiktas tinkamas leidimas, valstybėse narėse nustatoma pagal nacionalinius įstatymus ir kitus teisės aktus; tokie asmenys informuojami apie jų saugumo įsipareigojimus ESĮI apsaugos srityje.

IV. ŠVIETIMAS SAUGUMO KLAUSIMAIS IR SAUGUMO SUPRATIMAS

29. Visi asmenys, kuriems išduotas APP, raštu patvirtina, kad jie supranta savo įsipareigojimus saugoti ESSĮ ir padarinius, jei ESĮI būtų neteisėtai atskleista. Atitinkamai valstybė narė ir TGS registruoja tokius rašytinius patvirtinimus.

30. Visi asmenys, kuriems leidžiama susipažinti su ESĮI arba kurie turi dirbti su ESĮI, yra iš pat pradžių informuojami ir paskui reguliariai informuojami apie grėsmes saugumui ir jie turi nedelsdami pranešti atitinkamoms saugumo tarnyboms apie bet kokius bandymus užmegzti kontaktą ar veiklą, kurie, jų nuomone, yra įtartini ar neįprasti.

31. Visi asmenys, kurie nebeeina pareigų, kurias einant jiems reikia susipažinti su ESĮI, yra informuojami apie jų įsipareigojimus toliau saugoti ESĮI slaptumą ir atitinkamais atvejais jie tai patvirtina raštu.

V. IŠSKIRTINĖS APLINKYBĖS

32. Kai leidžia nacionaliniai įstatymai ir kiti teisės aktai, valstybės narės kompetentingos nacionalinės institucijos išduotas asmens patikimumo pažymėjimas, kuriuo leidžiama susipažinti su nacionaliniu lygiu įslaptinta informacija, gali laikinai, kol bus išduotas nacionalinis APP susipažinti su ESĮI, suteikti teisę nacionaliniams pareigūnams susipažinti su ne aukštesne nei lygiaverčio slaptumo žymos laipsnio ESĮI, kaip nustatyta B priedėlyje pateiktoje atitikmenų lentelėje, kai ES interesais būtina suteikti tokią laikiną teisę susipažinti su informacija. NSI informuoja Saugumo komitetą, kai pagal nacionalinius įstatymus ir kitus teisės aktus tokia laikina teisės susipažinti su ESĮI negali būti suteikta.

33. Dėl skubos priežasčių, kurios pagrįstos tarnybos interesais, laukiant išsamaus patikimumo patikrinimo pabaigos, TGS paskyrimų tarnyba, pasikonsultavusi su valstybės narės, kurios pilietis yra atitinkamas asmuo, NSI ir atsižvelgusi į preliminaraus patikrinimo, skirto patikrinti, ar nėra žinomos nepalankios informacijos apie asmenį, rezultatus, gali TGS pareigūnams ir kitiems tarnautojams išduoti laikiną leidimą susipažinti su ESĮI konkrečiai funkcijai atlikti. Tokie laikini leidimai galioja ne ilgiau kaip šešis mėnesius ir nesuteikia teisės susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija. Visi asmenys, kuriems išduotas laikinas leidimas, raštu patvirtina, kad jie supranta savo įsipareigojimus saugoti ESSĮ ir ESĮI neteisėto atskleidimo pasekmes. TGS registruoja tokius rašytinius patvirtinimus.

34. Kai asmuo turi būti paskirtas į pareigybę, kuriai užimti reikalingas vienu laipsniu aukštesnis nei turimas APP, jis gali būti paskirtas į tą pareigybę laikinai, jeigu:

a) asmens vadovas raštu įtikinamai pagrindžia, kad būtina susipažinti su aukštesnio laipsnio ESĮI;

b) suteikiama teisė susipažinti tik su konkrečia ESĮI, kurios reikia užduočiai atlikti;

c) asmeniui išduotas nacionalinis APP arba ES APP tebegalioja;

d) imtasi veiksmų pareigybei reikiamo laipsnio leidimui gauti;

e) kompetentinga institucija atliko pakankamus patikrinimus, kad asmuo nėra rimtai ar pakartotinai pažeidęs saugumo nuostatų;

f) asmens paskyrimą patvirtino kompetentinga institucija; ir

g) išimtys, įskaitant informacijos, su kuria leista susipažinti, aprašymą, registruojamos atsakingame registre ar subregistre.

35. Pirmiau nurodytos procedūros laikomasi, kai reikia suteikti leidimą vieną kartą susipažinti su vienu laipsniu aukštesne slaptumo žyma pažymėta ESĮI nei ta, su kuria susipažinti jiems buvo leista atlikus patikimumo patikrinimą. Tokia procedūra neturi būti naudojama pakartotinai.

36. Itin išskirtinėmis aplinkybėmis, tokiomis kaip vykdant užduotis priešiškoje aplinkoje arba kylant tarptautinei įtampai, kai to reikia imantis neatidėliotinų priemonių, visų pirma siekiant išsaugoti žmonių gyvybes, valstybės narės ir generalinis sekretorius arba generalinio sekretoriaus pavaduotojas gali, kai įmanoma – raštu, suteikti galimybę susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija asmenims, kuriems nėra išduotas reikiamas APP, jeigu tokio leidimo

tikrai reikia ir jeigu nėra pagrįstų abejonių dėl atitinkamo asmens lojalumo ir patikimumo. Toks leidimas registruojamas, kartu aprašant informaciją, su kuria leista susipažinti.

37. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtos informacijos atveju toks leidimo suteikimas skubos tvarka taikomas tik tiems asmenims, kuriems buvo leista susipažinti su nacionaline informacija, atitinkančia TRES SECRET UE/EU TOP SECRET slaptumo laipsnį, arba su slaptumo žyma SECRET UE/EU SECRET pažymėta informacija.

38. Saugumo komitetas informuojamas apie atvejus, kai naudojamasi 36 ir 37 punktuose išdėstyta procedūra.

39. Kai valstybės narės nacionaliniai įstatymai ir kiti teisės aktai nustato griežtesnes taisykles dėl laikinų leidimų, laikinų paskyrimų, asmenims susipažinti su įslaptinta informacija vieną kartą ar skubos tvarka leidžiama ir šiame skirsnyje numatytos procedūros taikomos tik nepažeidžiant atitinkamuose įstatymuose ir kituose teisės aktuose nustatytų apribojimų.

40. Saugumo komitetui pateikiama šiame skirsnyje numatytų procedūrų taikymo metinė ataskaita.

VI. DALYVAVIMAS TARYBOJE VYKSTANČIUOSE POSĖDŽIUOSE

41. Vadovaujantis 28 punktu, asmenys, paskirti dalyvauti Tarybos arba Tarybos parengiamųjų organų posėdžiuose, kuriuose aptariama CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, gali tai daryti tik patvirtinus jų APP turėtojo statusą. Deleguotų asmenų APPPP ar kitus asmens patikimumo patikrinimo įrodymus atitinkamos institucijos siunčia TGS saugumo tarnybai arba išimtiniais atvejais ją pateikia atitinkamas deleguotas asmuo. Jei taikoma, gali būti naudojamas suvestinis pavardžių sąrašas, kuriame pateikiami atitinkami įrodymai apie APP.

42. Kai asmens, kuris eidamas savo pareigas turi dalyvauti Tarybos ir Tarybos parengiamųjų organų posėdžiuose, nacionalinis APP susipažinti su ESĮI panaikinamas saugumo sumetimais, kompetentinga institucija apie tai informuoja TGS.

VII. GALIMA PRIEIGA PRIE ESĮI

43. Kai asmenys turi būti įdarbinti tokioje aplinkoje, kurioje jie gali turėti prieigą prie CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėtos informacijos, jų patikimumas turi būti tinkamai patikrintas arba jie turi būti visą laiką lydimi.

44. Kurjerių, apsaugos darbuotojų ir lydinčių asmenų patikimumas turi būti patikrintas atitinkamu lygiu, arba jie turi būti kitaip deramai patikrinti vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, jie yra supažindinami su ESĮI apsaugai užtikrinti skirtomis saugumo procedūromis ir jiems išdėstomos jų pareigos jiems patikėtos tokios informacijos apsaugos srityje.

(1) OL L 56, 1968 3 4, p. 1.

II PRIEDAS

FIZINIS SAUGUMAS

I. ĮVADAS

1. Šiame priede nustatytos 8 straipsnio įgyvendinimo nuostatos. Jame išdėstyti būtiniausi reikalavimai, taikomi patalpų, pastatų, kabinetų, salių ir kitų zonų, kuriose tvarkoma ir saugoma ESĮI, įskaitant zonas, kuriose yra RIS, fizinei apsaugai.

2. Fizinio saugumo priemonės yra skirtos užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI:

a) užtikrinant, kad ESĮI būtų tinkamai tvarkoma ir saugoma;

b) sudarant sąlygas suskirstyti personalą pagal tai, kas gali susipažinti su ESĮI, remiantis principu "būtina žinoti" ir atitinkamais atvejais – personalo narių patikimumo pažymėjimais;

c) atgrasant nuo neteisėtų veiksmų, sutrukdant jiems bei juos nustatant; ir

d) sutrukdant asmenims įsibrauti slaptai arba įsiveržti jėga arba juos užlaikant.

II. FIZINIO SAUGUMO REIKALAVIMAI IR PRIEMONĖS

3. Fizinio saugumo priemonės parenkamos remiantis grėsmių įvertinimu, kurį atlieka kompetentingos institucijos. ESĮI apsaugai užtikrinti savo patalpose TGS ir valstybės narės taiko rizikos valdymo procesą, kad užtikrintų, jog, atsižvelgiant į įvertintą riziką, būtų taikoma atitinkamo lygio fizinė apsauga.

Rizikos valdymo procese atsižvelgiama į visus svarbius veiksnius, visų pirma:

a) ESĮI slaptumo žymos laipsnį;

b) ESĮI formą ir kiekį, atsižvelgiant į tai, kad dideliam ESĮI kiekiui ar rinkiniui apsaugoti gali reikėti taikyti griežtesnes apsaugos priemones;

c) pastatus ar zonas, kuriose laikoma ESĮI, supančią aplinką ir jų struktūrą; ir

d) įvertintą žvalgybos tarnybų, kurių veikla nukreipta prieš ES arba jos valstybes nares, keliamą grėsmę ir grėsmę dėl sabotažo, terorizmo, ardomosios arba kitų rūšių nusikalstamos veiklos.

4. Kompetentinga saugumo tarnyba, taikydama nuodugnios apsaugos sąvoką, nustato tinkamas įgyvendintinas fizinio saugumo priemones. Tai gali būti viena (ar daugiau) iš šių priemonių:

a) perimetro barjeras: fizinis barjeras, kuris skirtas zonos, kurioje reikalinga apsauga, ribos apsaugai užtikrinti;

b) įsibrovimo aptikimo sistemos (ĮAS): ĮAS gali būti naudojama siekiant padidinti perimetro barjero teikiamo saugumo lygį arba patalpose ir pastatuose vietoj apsaugos personalo ar jam padėti;

c) patekimo kontrolė: gali būti kontroliuojamas patekimas į objektą, pastatą ar pastatus objekte arba į zonas ar patalpas pastate. Kontrolė gali būti vykdoma elektroninėmis arba elektroninėmis-mechaninėmis priemonėmis, ją gali vykdyti apsaugos personalas ir (arba) priimamojo darbuotojas, arba ji gali būti vykdoma kitomis fizinėmis priemonėmis;

d) apsaugos personalas: siekiant atgrasyti slaptą įsibrovimą planuojančius asmenis, galima įdarbinti apmokytą ir prižiūrimą apsaugos personalą, inter alia, prireikus tinkamai patikrinant jų patikimumą;

e) apsauginės vaizdo stebėjimo sistemos (AVSS): apsaugos personalas gali naudotis AVSS, kad patikrintų incidentus ir ĮAS pavojaus signalus dideliuose objektuose ar ties perimetru;

f) apsauginis apšvietimas: apsauginis apšvietimas ne tik skleidžia šviesą, būtiną veiksmingam stebėjimui, kurį tiesiogiai atlieka apsaugos personalas arba kuris netiesiogiai atliekamas per AVSS sistemą, bet jį taip pat galima naudoti siekiant atgrasyti potencialų įsibrovėlį; ir

g) kitos tinkamos fizinės priemonės, skirtos atgrasyti asmenis be leidimo naudotis ESĮI, nustatyti tokio naudojimo atvejus, arba užkirsti kelią tam, kad ESĮI būtų prarasta ar jai būtų padaryta žala.

5. Kompetentinga institucija gali būti įgaliojama apieškoti įeinančius ir išeinančius asmenis siekiant atgrasyti nuo neleistino medžiagos įnešimo arba neleistino ESĮI išnešimo iš patalpų ar pastatų.

6. Iškilus pavojui, kad ESĮI bus pamatyta, netgi atsitiktinai, imamasi tinkamų priemonių siekiant išvengti šio pavojaus.

7. Naujos infrastruktūros atveju infrastruktūros planavimo ir projektavimo metu apibrėžiami fizinio saugumo reikalavimai ir jos funkcinės specifikacijos. Esamos infrastruktūros atveju kiek įmanoma įgyvendinami fizinio saugumo reikalavimai.

III. ESĮI FIZINEI APSAUGAI SKIRTA ĮRANGA

8. Įsigydama ESĮI fizinei apsaugai užtikrinti skirtą įrangą (pavyzdžiui, apsaugines talpyklas, naikiklius, durų užraktus, elektronines patekimo kontrolės sistemas, įsibrovimo aptikimo sistemas, signalizacijos sistemas), kompetentinga saugumo institucija užtikrina, kad įranga atitiktų patvirtintus techninius standartus ir būtiniausius reikalavimus.

9. ESĮI fizinei apsaugai užtikrinti naudotinos įrangos techninės specifikacijos išdėstomos saugumo gairėse, kurias turi patvirtinti Saugumo komitetas.

10. Saugumo sistemos reguliariai tikrinamos ir reguliariai atliekama įrangos priežiūra. Atliekant priežiūrą atsižvelgiama į patikrinimų rezultatus, kad būtų užtikrinta, jog įrenginiai toliau veiktų optimaliai.

11. Kiekvieno patikrinimo metu iš naujo vertinamas individualių saugumo priemonių ir visos saugumo sistemos veiksmingumas.

IV. FIZIŠKAI APSAUGOTOS ZONOS

12. ESĮI fizinės apsaugos tikslais nustatomos dviejų tipų fiziškai apsaugotos zonos arba nacionalinės lygiavertės zonos:

a) administracinės zonos; ir

b) saugumo zonos (įskaitant techniniu požiūriu saugias saugumo zonas).

Šiame sprendime visos nuorodos į administracines zonas ir saugumo zonas, įskaitant techniniu požiūriu saugias saugumo zonas, laikomos ir nuorodomis į nacionalines lygiavertes zonas.

13. Kompetentinga saugumo institucija nustato, kad zona atitinka reikalavimus, jog būtų klasifikuojama kaip administracinė zona, saugumo zona ar techniniu požiūriu saugi saugumo zona.

14. Administracinių zonų atveju:

a) nustatoma aiškiai apibrėžta išorinė riba, kad būtų galima tikrinti asmenis ir, jei įmanoma, transporto priemones;

b) į šias zonas įeiti nelydimiems leidžiama tik tiems asmenims, kuriems kompetentinga institucija suteikė tinkamą leidimą; ir

c) visi kiti asmenys turi būti visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

15. Saugumo zonų atveju:

a) nustatoma aiškiai apibrėžta ir saugoma išorinė riba, per kurią kiekvienas įėjimas ir išėjimas yra kontroliuojamas naudojantis leidimų arba asmens atpažinimo sistema;

b) į zoną įeiti nelydimiems leidžiama tik tiems asmenims, kurių patikimumas patikrintas ir kurie turi specialų leidimą įeiti į zoną, vadovaujantis principu „būtina žinoti“;

c) visi kiti asmenys turi būti visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

16. Tais atvejais, kai įėjus į saugumo zoną galima visais praktiniais tikslais tiesiogiai susipažinti su joje laikoma įslaptinta informacija, taikomi tokie papildomi reikalavimai:

a) turi būti aiškiai nurodyta paprastai zonoje laikomos informacijos aukščiausio slaptumo žymos laipsnio specifikacija;

b) visi lankytojai privalo turėti specialų leidimą, suteikiantį teisę įeiti į zoną, turi būti visą laiką lydimi ir jų patikimumas turi būti tinkamai patikrintas, nebent imtasi priemonių užtikrinti, kad nebūtų įmanoma susipažinti su ESĮI.

17. Saugumo zonos, kurios turi būti apsaugotos nuo pasiklausymo, klasifikuojamos kaip techniniu požiūriu saugios saugumo zonos. Taikomi šie papildomi reikalavimai:

a) tokiose zonose turi būti įdiegta ĮAS, ir kai jose nedirbama, jos turi būti rakinamos, o kai dirbama – saugomos. Visi raktai apskaitomi ir saugomi vadovaujantis VI skirsniu;

b) visi į tokias zonas įeinantys asmenys ar įnešamos medžiagos turi būti kontroliuojami;

c) tokios zonos reguliariai fiziškai ir (arba) techniškai tikrinamos, kaip reikalauja kompetentinga saugumo institucija. Tokie patikrinimai atliekami, kai į zoną buvo įeita be leidimo ar įtariama apie tokį patekimą; ir

d) tokiose zonose negali būti ryšių linijų, kurioms nesuteiktas leidimas, telefonų, kuriems nesuteiktas leidimas, ar kitų ryšių prietaisų bei elektros ar elektroninės įrangos, kuriems nesuteiktas leidimas.

18. Nepaisant 17 punkto d papunkčio, prieš naudojantis ryšių prietaisais ir elektros ar elektronine įranga zonose, kuriose rengiami susitikimai ar atliekamas darbas, susijęs su SECRET UE/EU SECRET arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, taip pat, kai grėsmė ESĮI vertinama kaip didelė, tokius prietaisus ir įrangą visų pirma ištiria kompetentinga saugumo ins-

titucija, siekdama užtikrinti, kad naudojantis šia įranga nebūtų galima perduoti jokios suprantamos informacijos per neapdairumą ar neteisėtai už saugumo zonos perimetro.

19. Saugumo zonos, kuriose nėra visą parą budinčio personalo, atitinkamais atvejais tikrinamos pasibaigus įprastai darbo dienai ir atsitiktiniais intervalais ne įprastomis darbo valandomis, išskyrus atvejus, kai įdiegta ĮAS.

20. Siekiant surengti susitikimą, kuriame naudojama įslaptinta informacija arba bet kokiu kitu panašiu tikslu administracinėje zonoje gali būti laikinai įrengtos saugumo zonos ir techniniu požiūriu saugios saugumo zonos.

21. Saugios eksploatacijos taisyklės rengiamos kiekvienai saugumo zonai ir jose nustatoma:

a) ESĮI, kuri gali būti tvarkoma ir saugoma toje zonoje, slaptumo žymos laipsnis;

b) įdiegtinos stebėjimo ir apsaugos priemonės;

c) kokie asmenys turi leidimą nelydimi patekti į zoną, vadovaujantis principu „būtina žinoti“ ir asmens patikimumo pažymėjimu;

d) atitinkamais atvejais, palydos tvarka ir ESĮI apsaugos tvarka, kai kitiems asmenims leidžiama patekti į zoną;

e) bet kurios kitos atitinkamos priemonės ir procedūros.

22. Saugumo zonose įrengiamos saugyklos. Sienos, grindys, lubos, langai ir durys su užraktais turi būti kompetentingos saugumo institucijos patvirtintos ir užtikrinti apsaugą, kurią užtikrina apsauginės talpyklos, patvirtintos to paties laipsnio slaptumo žymos ESĮI saugoti.

V. FIZINĖS APSAUGOS PRIEMONĖS TVARKANT IR SAUGANT ESĮI

23. Slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėta ESĮI gali būti tvarkoma:

a) saugumo zonose;

b) administracinėse zonose, jeigu ta ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys; arba

c) ne saugumo zonose ar administracinėse zonose, jeigu turėtojas gabena ESĮI pagal III priedo 28–40 punktus ir yra įsipareigojęs taikyti kompensacines priemones, nustatytas kompetentingos saugumo institucijos parengtose saugumo instrukcijose, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys.

24. Slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėta ESĮI saugoma tinkamuose rakinamuose biuro balduose administracinėse zonose arba saugumo zonose. Laikinai ji gali būti saugoma ne saugumo zonose ar administracinėse zonose, jeigu turėtojas yra įsipareigojęs taikyti kompensacines priemones, nustatytas kompetentingos saugumo institucijos parengtose saugumo instrukcijose.

25. Slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta ESĮI gali būti tvarkoma:

a) saugumo zonose;

b) administracinėse zonose, jeigu ta ESĮI yra apsaugota taip, kad su ja nega-

lėtų susipažinti leidimo neturintys asmenys; arba

c) ne saugumo zonose ar administracinėse zonose, jeigu turėtojas:

i) gabena ESĮI pagal III priedo 28–40 punktus;

ii) yra įsipareigojęs taikyti kompensacines priemones, nustatytas kompetentingos saugumo institucijos parengtose saugumo instrukcijose, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;

iii) visą laiką asmeniškai kontroliuoja šią ESĮI; ir

iv) jei dokumentai yra popieriniu pavidalu, apie tai pranešė atitinkamai registratūrai.

26. Slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET pažymėta ESĮI saugoma saugumo zonose esančiose apsauginėse talpyklose arba saugyklose.

27. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta ESĮI tvarkoma saugumo zonose.

28. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta ESĮI saugoma saugumo zonose laikantis kurios nors iš toliau nurodytų sąlygų:

a) apsauginėje talpykloje laikantis 8 punkto reikalavimų, taikant vieną ar kelias iš toliau nurodytų kontrolės priemonių:

i) nuolatinė apsauga arba tikrinimas, kurį vykdo apsaugos personalas arba budintis personalas, kurio patikimumas patikrintas;

ii) patvirtinta ĮAS kartu veikiant reagavimo apsaugos personalui;

arba

b) saugykloje su įrengta ĮAS kartu veikiant reagavimo apsaugos personalui.

29. ESĮI gabenimą už fiziškai apsaugotų zonų ribų reglamentuojančios taisyklės išdėstytos III priede.

VI. ESĮI APSAUGAI UŽTIKRINTI NAUDOJAMŲ RAKTŲ IR KODŲ KONTROLĖ

30. Kompetentinga saugumo institucija nustato kabinetų, patalpų, saugyklų ir apsauginių talpyklų raktų bei kodų valdymo procedūras. Tokios procedūros apsaugo nuo neleistino susipažinimo su informacija.

31. Kodai patikimi kuo mažesniam asmenų skaičiui ir tik tiems asmenims, kuriems reikia juos naudoti; šie asmenys kodus įsimena. Apsauginių talpyklų ir saugyklų, kuriose saugoma ESĮI, kodai keičiami:

a) pasikeitus kodus žinančiam personalui;

b) iškilus pavojui ar įtarimui;

c) po spynos techninio patikrinimo ar remonto; ir

d) bent kas 12 mėnesių.

III PRIEDAS

ĮSLAPTINTOS INFORMACIJOS ADMINISTRAVIMAS

I. ĮVADAS

1. Šiame priede nustatytos 9 straipsnio įgyvendinimo nuostatos. Jame išdėstytos administracinės ESĮI kontrolės visą jos gyvavimo ciklą priemonės siekiant atgrasyti nuo tokios informacijos sąmoningo ar atsitiktinio neteisėto atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius.

II. ĮSLAPTINIMO ADMINISTRAVIMAS

Slaptumo žymos ir kitos žymos

2. Informacija įslaptinama tuo atveju, jei dėl jos konfidencialumo reikia ją apsaugoti.

3. ESĮI rengėjas atsako už slaptumo žymos laipsnio nustatymą pagal atitinkamas įslaptinimo gaires ir už pirminį informacijos platinimą.

4. ESĮI slaptumo žymos laipsnis nustatomas vadovaujantis 2 straipsnio 2 dalimi ir remiantis saugumo politika, kuri turi būti tvirtinama pagal 3 straipsnio 3 dalį.

5. Slaptumo žyma nurodoma aiškiai ir teisingai, neatsižvelgiant į tai, ar ESĮI yra pateikiama popieriuje, žodžiu, elektronine ar bet kuria kita forma.

6. Atskiroms dokumento dalims (t. y. puslapiams, dalims, skirsniams, priedams ir priedėliams) gali būti suteikiamos skirtingos slaptumo žymos ir jos atitinkamai pažymimos, taip pat tais atvejais, kai jos saugomos elektronine forma.

7. Dokumento ar dokumentų bylos bendras slaptumo žymos laipsnis nustatomas pagal aukščiausią slaptumo žymos laipsnį turinčią jo dalį. Kai renkama informacija iš įvairių šaltinių, galutinis dokumentas peržiūrimas siekiant nustatyti jo bendrą slaptumo žymos laipsnį, nes gali paaiškėti, kad jam turi būti suteiktas aukštesnis slaptumo žymos laipsnis nei jo dalims.

8. Kiek įmanoma, dokumentams, kurių dalys pažymėtos skirtingo laipsnio slaptumo žymomis, suteikiama tokia struktūra, kad skirtingo laipsnio slaptumo žymomis pažymėtas dalis būtų galima lengvai nustatyti ir prireikus atskirti.

9. Pridedamų dokumentų lydinčiųjų dokumentų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymas. Jei tokie dokumentai pateikiami atskirai nuo priedų, įslaptintos informacijos rengėjas turi aiškiai nurodyti, koks slaptumo žymos laipsnis jiems suteikiamas, naudodamas atitinkamą žymą, pavyzdžiui:

CONFIDENTIEL UE/EU CONFIDENTIAL

Be priedo (-ų) RESTREINT UE/EU RESTRICTED

Žymos

10. Be vienos iš slaptumo žymų, nurodytų 2 straipsnio 2 dalyje, ESĮI gali būti pažymėta papildomomis žymomis, pavyzdžiui:

a) identifikatoriumi, kuriuo nurodomas įslaptintos informacijos rengėjas;

b) bet kuriais apribojimais, kodiniais žodžiais ar santrumpomis, kuriais nurodoma veiklos sritis, su kuria dokumentas yra susijęs, jo specialus platinimas vadovaujantis principu „būtina žinoti“ arba naudojimo apribojimai;

c) paskirstymo žymomis;

d) jei taikoma, nurodant datą ar konkretų įvykį, po kurio informacijos slaptumo žymos laipsnis gali būti sumažintas arba ji gali būti išslaptinta.

Žymų santrumpos

11. Siekiant nurodyti atskirų teksto pastraipų slaptumo žymos laipsnį, gali būti naudojamos standartinės slaptumo žymų santrumpos. Santrumpos nepakeičia pilnų slaptumo žymų.

12. ES įslaptintuose dokumentuose gali būti naudojamos šios standartinės santrumpos, kuriomis nurodomas skirsnių arba teksto dalių, užimančių mažiau nei vieną puslapį, slaptumo žymos laipsnis:

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

ESĮI rengimas

13. Rengiant ES įslaptintą dokumentą:

a) kiekvienas puslapis aiškiai pažymimas slaptumo žyma;

b) kiekvienas puslapis numeruojamas;

c) dokumente nurodomas jo numeris ir dalykas, kurie nėra įslaptinta informacija, išskyrus tuo atveju, kai jie pažymėti kaip įslaptinta informacija;

d) dokumente nurodoma data;

e) jei platinamos kelios dokumentų, pažymėtų SECRET UE/EU SECRET ir aukštesnio laipsnio slaptumo žyma, kopijos, kiekvienos iš jų kiekviename puslapyje nurodomas kopijos numeris.

14. Kai rengiant ESĮI neįmanoma taikyti 13 punkte išdėstytų reikalavimų, taikomos kitos atitinkamos priemonės vadovaujantis saugumo gairėmis, parengtomis remiantis 6 straipsnio 2 dalimi.

ESĮI slaptumo žymos laipsnio sumažinimas ir ESĮI išslaptinimas

15. Įslaptintos informacijos rengėjas, kai įmanoma, rengdamas ESĮI, ypač RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtą informaciją, nurodo, ar tam tikrą dieną arba po tam tikro įvykio galima sumažinti ESĮI slaptumo žymos laipsnį arba ją išslaptinti.

16. TGS reguliariai peržiūri jo turimą ESĮI, siekdamas įsitikinti, ar slaptumo žymos lygis vis dar taikomas. TGS sukuria sistemą, skirtą peržiūrėti registruotos ESĮI, kurią jis parengė, slaptumo žymos laipsnį ne rečiau kaip kas penkeri metai. Tokia peržiūra nėra reikalinga, jeigu įslaptintos informacijos rengėjas iš pat pradžių nurodo, kad informacijos slaptumo žymos laipsnis bus sumažintas arba informacija išslaptinta automatiškai, o informacija buvo atitinkamai pažymėta.

III. ESĮI REGISTRAVIMAS SAUGUMO TIKSLAIS

17. Kiekviename TGS ir valstybių narių nacionalinių administracinių įstaigų organizaciniame vienete, kuriame tvarkoma ESĮI, steigiamos atsakingos registratūros, siekiant užtikrinti, kad ESĮI būtų administruojama pagal šį sprendimą. Registratūros steigiamos kaip II priede apibrėžtos saugumo zonos.

18. Šiame sprendime registravimas saugumo tikslais (toliau – registravimas) – procedūrų, kuriomis užregistruojamas dokumento gyvavimo ciklas, įskaitant jo platinimą ir sunaikinimą, taikymas.

19. Kai organizacinis vienetas gauna CONFIDENTIEL UE/EU CONFIDENTIAL ir aukštesnio laipsnio slaptumo žyma pažymėtą medžiagą ir kai ją išsiunčia, visa ši medžiaga registruojama tam skirtose registratūrose.

20. Centrinis TGS registratūra registruoja visą įslaptintą informaciją, kurią Taryba ir TGS suteikė trečiosioms valstybėms ir tarptautinėms organizacijoms, bei visą įslaptintą informaciją, gautą iš trečiųjų valstybių ir tarptautinių organizacijų.

21. RIS atveju registravimo procedūros gali būti atliekamos vykdant procesus pačioje RIS.

22. Taryba patvirtina ESĮI registravimo saugumo tikslais saugumo politiką.

TRES SECRET UE/EU TOP SECRET registratūros

23. Valstybėse narėse ir TGS paskiriama registratūra, kuri veikia kaip centrinė slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtą informaciją gaunanti ir siunčianti tarnyba. Prireikus gali būti paskirtos antrinės registratūros, kurios tvarko tokią informaciją jos registravimo tikslais.

24. Tokios antrinės registratūros negali perduoti slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtų dokumentų tiesiogiai kitoms tos pačios centrinės TRES SECRET UE/EU TOP SECRET registratūros antrinėms registratūroms arba į išorę be aiškaus rašytinio tos registratūros leidimo.

IV. ES ĮSLAPTINTŲ DOKUMENTŲ KOPIJAVIMAS IR VERTIMAS

25. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėti dokumentai kopijuojami arba verčiami tik gavus išankstinį rašytinį įslaptintos informacijos rengėjo sutikimą.

26. Jeigu SECRET UE/EU SECRET arba žemesnio laipsnio slaptumo žyma pažymėtų dokumentų įslaptintos informacijos rengėjas nenustatė apribojimų dėl jų kopijavimo ar vertimo, dokumento turėtojo nurodymu tokius dokumentus galima kopijuoti arba versti.

27. Dokumento kopijoms ir vertimams taikomos tos pačios saugumo priemonės, kaip ir dokumento originalui.

V. ESĮI GABENIMAS

28. Gabenant ESĮI taikomos 30–40 punktuose išdėstytos apsaugos priemonės. Kai ESĮI gabenama elektroninėje laikmenoje ir nepaisant 9 straipsnio 4 dalies, toliau išvardytas apsaugos priemones gali papildyti kompetentingos saugumo institucijos nurodytos atitinkamos techninės kontrpriemonės, kad būtų sumažinta rizika, jog informacija bus prarasta ar atskleista.

29. TGS ir valstybių narių kompetentingos saugumo institucijos parengia ESĮI gabenimo instrukcijas remdamosi šiuo sprendimu.

Pastate arba uždaroje pastatų grupėje

30. Pastate arba uždaroje pastatų grupėje gabenama informacija turi būti uždengta, kad nebūtų galima stebėti jos turinio.

31. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija pastate arba uždaroje pastatų grupėje turi būti gabenama apsaugotame voke, ant kurio nurodytas tik gavėjo vardas ir pavardė.

Europos Sąjungoje

32. ESĮI, gabenama iš vieno pastato ar patalpos į kitą Europos Sąjungoje, turi būti supakuota taip, kad ji būtų apsaugota nuo neteisėto atskleidimo.

33. SECRET UE/EU SECRET ir žemesnio laipsnio slaptumo žyma pažymėtą informaciją Europos Sąjungoje gabena:

a) atitinkamai karinis, vyriausybinis ar diplomatinis kurjeris;

b) kurjeris su sąlyga, kad:

i) ESĮI nepaliekama be ją gabenančio asmens priežiūros, išskyrus tuo atveju, kai ji saugoma laikantis II priede nustatytų reikalavimų;

ii) paketas su ESĮI neatidaromas gabenimo metu, o ESĮI neskaitoma viešose vietose;

iii) asmenys informuojami apie jų pareigas, susijusias su saugumu;

iv) prireikus asmenims suteikiamas kurjerio pažymėjimas;

c) pašto tarnybos arba komercinės kurjerių pašto tarnybos su sąlyga, kad:

i) jos yra patvirtintos atitinkamos NSI vadovaujantis nacionaliniais įstatymais

ir kitais teisės aktais;

ii) jos taiko atitinkamas apsaugos priemones laikydamosi būtiniausių reikalavimų, kurie turi būti nustatyti saugumo gairėse pagal 6 straipsnio 2 dalį.

Gabenimo iš vienos valstybės narės į kitą atveju c punkto nuostatos taikomos tik gabenant informaciją, pažymėtą slaptumo žyma iki CONFIDENTIEL UE/EU CONFIDENTIAL.

34. CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET slaptumo žyma pažymėtą medžiagą (pavyzdžiui, įrangą ar įrenginius), kurios negalima gabenti 33 punkte nurodytomis priemonėmis, kaip krovinį pagal V priedą gabena komercinės vežėjų bendrovės.

35. TRES SECRET UE/EU TOP SECRET slaptumo žyma pažymėtą informaciją iš vieno pastato ar patalpos į kitą Europos Sąjungoje gabena atitinkamai karinis, vyriausybinis ar diplomatinis kurjeris.

Iš ES į trečiosios valstybės teritoriją

36. ESĮI, gabenama iš ES į trečiosios valstybės teritoriją, turi būti supakuota taip, kad ji būtų apsaugota nuo neteisėto atskleidimo.

37. CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET slaptumo žyma pažymėtą informaciją iš ES į trečiosios valstybės terito-

riją gabena:

a) karinis ar diplomatinis kurjeris;

b) kurjeris su sąlyga, kad:

i) ant paketo yra oficialus spaudas arba ESĮI supakuota aiškiai nurodant, kad tai yra oficiali siunta ir jai neturėtų būti taikomas muitinės ar saugumo patikrinimas;

ii) asmenys turi kurjerio pažymėjimą, kuriame nurodytas paketas ir kuris suteikia jiems teisę gabenti paketą;

iii) ESĮI nepaliekama be ją gabenančio asmens priežiūros, išskyrus tuo atveju, kai ji saugoma laikantis II priede nustatytų reikalavimų;

iv) paketas su ESĮI neatidaromas gabenimo metu arba ESĮI neskaitoma viešose vietose; ir

v) asmenys informuojami apie jų pareigas, susijusias su saugumu.

38. Gabenant ES parengtą trečiajai šaliai ar tarptautinei organizacijai skirtą slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET pažymėtą informaciją laikomasi atitinkamų nuostatų, numatytų susitarime dėl informacijos saugumo arba administraciniame susitarime pagal 12 straipsnio 2 dalies a arba b punktus.

39. Slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėtą informaciją taip pat gali gabenti pašto tarnybos ar komercinės kurjerių pašto tarnybos.

40. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtą informaciją iš ES į trečiosios šalies teritoriją gabena karinis ar diplomatinis kurjeris.

VI. ESĮI NAIKINIMAS

41. Nebereikalingi ES įslaptinti dokumentai gali būti sunaikinti nepažeidžiant atitinkamų taisyklių ir nuostatų dėl archyvavimo.

42. Dokumentus, kurie turi būti registruojami pagal 9 straipsnio 2 dalį, turėtojo arba kompetentingos institucijos nurodymu sunaikina atsakinga registratūra. Registracijos knygos ir kita registravimo informacija atitinkamai atnaujinama.

43. Dokumentai, pažymėti SECRET UE/EU SECRET arba TRES SECRET UE/EU TOP SECRET slaptumo žyma, naikinami dalyvaujant liudytojui, kuris turi leidimą susipažinti su ne žemesnio už naikinamo dokumento slaptumo žymos laipsnio įslaptinta informacija.

44. Atsakingas registratūros darbuotojas ir liudytojas, kai pastarojo dalyvavimas privalomas, pasirašo sunaikinimo aktą, kuris registruojamas atitinkamame registre. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtų dokumentų sunaikinimo aktai registre saugomi bent dešimt metų, o CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET slaptumo žyma pažymėtų dokumentų – bent penkerius metus.

45. Įslaptinti dokumentai, įskaitant pažymėtus slaptumo žyma RESTREINT UE/EU RESTRICTED, sunaikinami tokiais būdais, kurie atitinka atitinkamus ES arba lygiaverčius standartus arba kuriuos valstybės narės patvirtino laikydamosi nacionalinių techninių standartų, kad jų nebūtų galima visiškai ar iš dalies atkurti.

46. Kompiuterinių duomenų saugojimo laikmenos, naudotos ESĮI, sunaikinamos vadovaujantis IV priedo 36 punkto nuostatomis.

VII. PATIKRINIMAI IR ĮVERTINIMO VIZITAI

47. Sąvoka „patikrinimas“ toliau vartojama nurodant a) patikrinimą pagal 9 straipsnio 3 dalį, 15 straipsnio 2 dalies e, f ir g punktus; arba b) įvertinimo vizitą pagal 12 straipsnio 5 dalį,kurių metu vertinamas priemonių, įgyvendintų siekiant apsaugoti ESĮI, veiksmingumas.

48. Patikrinimai atliekami, inter alia, siekiant:

a) užtikrinti, kad būtų laikomasi šiame sprendime nustatytų būtiniausių ESĮI apsaugos standartų;

b) tikrinamuose subjektuose pabrėžti saugumo ir veiksmingo rizikos valdymo svarbą;

c) rekomenduoti atsakomąsias priemones konkrečiam įslaptintos informacijos konfidencialumo praradimo, jos vientisumo ar prieinamumo netekimo poveikiui sušvelninti; ir

d) sustiprinti saugumo institucijų vykdomas švietimo saugumo klausimais ir sąmoningumo ugdymo programas.

49. Iki kiekvienų kalendorinių metų pabaigos Taryba patvirtina kitų metų tikrinimo programą, kaip numatyta 15 straipsnio 1 dalies c punkte. Faktinės kiekvieno patikrinimo datos nustatomos suderinus su ES agentūra ar įstaiga, valstybe nare, trečiąja valstybe ar atitinkama tarptautine organizacija.

Patikrinimų vykdymas

50. Patikrinimai atliekami siekiant patikrinti tikrinamo subjekto atitinkamas taisykles, reglamentus ir procedūras, taip pat patikrinti, ar subjekto praktika atitinka šiame sprendime nustatytus pagrindinius principus ir būtiniausius standartus ir keitimąsi įslaptinta informacija su tuo subjektu reglamentuojančias nuostatas.

51. Patikrinimai atliekami dviem etapais. Prieš patikrinimą prireikus organizuojamas parengiamasis susitikimas su atitinkamu subjektu. Po šio parengiamojo susitikimo patikrinimo grupė, suderinusi su minėtu subjektu, sudaro išsamią tikrinimo programą, apimančią visas saugumo sritis. Patikrinimo grupei leidžiama patekti į visas vietas, kuriose tvarkoma ESĮI, visų pirma registratūras ir RIS įrengimo vietas.

52. Už valstybių narių nacionalinėse administracinėse įstaigose atliekamus patikrinimus atsako bendra TGS ir Komisijos patikrinimo grupė, visapusiškai bendradarbiaudama su tikrinamo subjekto pareigūnais.

53. Už trečiųjų valstybių ir tarptautinių organizacijų patikrinimus atsako bendra TGS ir Komisijos patikrinimo grupė, visapusiškai bendradarbiaudama su trečiosios valstybės ar tarptautinės organizacijos pareigūnais.

54. ES agentūrų ir įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, taip pat Europolo ir Eurojusto patikrinimus atlieka TGS saugumo tarnyba, padedama NSI, kurios teritorijoje yra įsikūrusi agentūra ar įstaiga, ekspertų. Gali dalyvauti Europos Komisijos saugumo direktoratas (EKSD), jei jis reguliariai keičiasi ESĮI su atitinkama agentūra ar įstaiga.

55. ES agentūrų bei įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, taip pat Europolo ir Eurojusto ir trečiųjų valstybių bei tarptautinių organizacijų patikrinimų atveju NSI ekspertų pagalbos prašoma laikantis išsamios tvarkos, dėl kurios turi susitarti Saugumo komitetas.

Patikrinimo ataskaitos

56. Pabaigus patikrinimą tikrinamam subjektui pateikiamos pagrindinės išvados ir rekomendacijos. Po to parengiama patikrinimo ataskaita, už kurios parengimą atsako TGS saugumo tarnyba. Jei buvo pasiūlyti taisomieji veiksmai ir pateiktos rekomendacijos, ataskaitoje padarytos išvados turėtų būti pakankamai išsamiai pagrįstos. Ataskaita pateikiama atitinkamai patikrinto subjekto tarnybai.

57. Jei patikrinimai atliekami valstybių narių nacionalinėse administracinėse įstaigose:

a) patikrinimo ataskaitos projektas nusiunčiamas atitinkamai NSI, kad ši patikrintų jame pateikiamų faktų teisingumą, taip pat ar jame nėra jokios informacijos, pažymėtos aukštesnio laipsnio nei RESTREINT UE/EU RESTRICTED slaptumo žyma;

b) išskyrus atvejus, kai atitinkamos valstybės narės NSI paprašo, kad patikrinimų ataskaitos nebūtų platinamos, jos išplatinamos Saugumo komiteto nariams ir EKSD; ataskaita įslaptinama pažymint slaptumo žyma RESTREINT UE/EU RESTRICTED;

TGS saugumo tarnyba atsako už tai, kad būtų rengiama reguliari ataskaita, kurioje būtų akcentuojama nurodytu laikotarpiu valstybėse narėse atliktų patikrinimų metu įgyta patirtis ir kurią išnagrinėtų Saugumo komitetas.

58. Trečiųjų valstybių ir tarptautinių organizacijų įvertinimo vizitų atveju ataskaita išplatinama Saugumo komitetui ir EKSD. Ataskaita pažymima ne žemesnio laipsnio nei RESTREINT UE/EU RESTRICTED slaptumo žyma. Taisomieji veiksmai patikrinami kito vizito metu ir apie juos pranešama Saugumo komitetui.

59. ES agentūrų ir įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, taip pat Europolo ir Eurojusto patikrinimo vizitų atveju patikrinimo ataskaitos išplatinamos Saugumo komiteto nariams ir EKSD. Patikrinimo ataskaitos projektas nusiunčiamas atitinkamai agentūrai ar įstaigai, kad ši patikrintų jame pateikiamų faktų teisingumą, taip pat ar jame nėra jokios informacijos, pažymėtos aukštesnio laipsnio nei RESTREINT UE/EU RESTRICTED slaptumo žyma. Taisomieji veiksmai patikrinami kito vizito metu ir apie juos pranešama Saugumo komitetui.

60. TGS saugumo tarnyba vykdo reguliarius TGS organizacinių vienetų patikrinimus 48 punkte nustatytais tikslais.

Patikrinimų kontrolinis sąrašas

61. TGS saugumo tarnyba parengia ir atnaujina dalykų, tikrintinų vykdant patikrinimą, saugumo patikrinimo kontrolinį sąrašą. Šis kontrolinis sąrašas pateikiamas Saugumo komitetui.

62. Kontroliniam sąrašui užpildyti būtina informacija gaunama visų pirma patikrinimo metu iš tikrinamo subjekto saugumo valdymo tarnybų. Išsamiai užpildžius kontrolinį sąrašą, susitarus su tikrinamu subjektu, sąrašas įslaptinamas. Jis negali būti patikrinimo ataskaitos sudedamoji dalis.

IV PRIEDAS

RIS TVARKOMOS ESĮI APSAUGA

I. ĮVADAS

1. Šiame priede nustatytos 10 straipsnio įgyvendinimo nuostatos.

2. Toliau išdėstytos ISU savybės ir sąvokos yra būtinos saugumui ir tinkamam RIS

operacijų vykdymui užtikrinti:

Autentiškumas: užtikrinimas, kad informacija yra tikra ir gauta iš bona fide šaltinių;

Prieinamumas: galimybė leidimą turinčiam subjektui pateikus prašymą gauti informaciją ir ja naudotis;

Konfidencialumas : savybė, kuri reiškia, kad informacija nėra atskleidžiama neturintiems leidimo asmenims, subjektams ar procesams;

Vientisumas: savybė, kuri reiškia, kad apsaugomas informacijos tikslumas ir išsamumas bei turtas;

Atsakomybės už veiksmus prisiėmimas : galimybė įrodyti, kad veiksmas buvo atliktas ar įvykis įvyko, kad šio įvykio ar veiksmo po to negalima būtų išsižadėti.

II. INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI

3. Toliau išdėstytos nuostatos yra RIS, kurioje tvarkoma ESĮI, saugumo užtikrinimo pagrindas. Išsamūs šių nuostatų įgyvendinimo reikalavimai nustatyti ISU saugumo politikoje ir saugumo gairėse.

Saugumo rizikos valdymas

4. Saugumo rizikos valdymas yra neatsiejama RIS apibrėžties, kūrimo, veikimo ir priežiūros dalis. Rizikos valdymą (įvertinimą, traktavimą, pripažinimą ir informavimą) kaip kartotinį procesą kartu vykdo sistemos savininkų, projekto institucijų, vykdančiųjų institucijų ir saugumo patvirtinimo institucijų atstovai, taikydami pavirtintą, skaidrų ir visiškai suprantamą rizikos įvertinimo procesą. RIS ir jos turinio taikymo sritis aiškiai apibrėžiama rizikos valdymo proceso pradžioje.

5. Kompetentingos institucijos peržiūri pavojus, kurie gali kilti RIS, ir nuolat vykdo naujausiais duomenimis grindžiamus ir tikslius pavojų įvertinimus, kurie atspindi esamą sistemos operacinę aplinką. Jos nuolat atnaujina savo žinias pažeidžiamumo klausimais ir reguliariai peržiūri pažeidžiamumo įvertinimą, neatsilikdamos nuo informacinių technologijų (IT) aplinkos pokyčių.

6. Tvarkant saugumo riziką siekiama taikyti apsaugos priemonių rinkinį, kuris užtikrina tinkamą vartotojų reikalavimų, sąnaudų ir likutinės rizikos, susijusios su saugumu, pusiausvyrą.

7. RIS akreditavimui taikomi konkretūs reikalavimai, reikalavimai dėl informacijos apimties ir išsamumo, kuriuos nustato atitinkama SAI, turi atitikti įvertintą riziką, atsižvelgiant į visus svarbius veiksnius, įskaitant ESĮI, kuri tvarkoma RIS, slaptumo žymos laipsnį. Akreditavimas apima atsakingos institucijos oficialų pareiškimą dėl likutinės rizikos ir likutinės rizikos pripažinimą.

Saugumas viso RIS gyvavimo ciklo metu

8. Saugumas turi būti užtikrintas viso RIS gyvavimo ciklo metu – nuo pradžios iki naudojimosi pabaigos.

9. Kiekvienu gyvavimo ciklo etapu nustatomas kiekvieno RIS dalyvio ir jo sąveikos su kitais dalyviais vaidmuo saugumo požiūriu.

10. RIS, įskaitant technines ir netechnines saugumo priemones, bandomos saugumo požiūriu akreditavimo proceso metu siekiant užtikrinti tinkamą saugumo užtikrinimo lygį ir patikrinti, ar jos teisingai įdiegtos, integruotos ir sukonfigūruotos.

11. Saugumo įvertinimai, patikrinimai ir peržiūros atliekami reguliariai RIS veikimo ir techninės priežiūros metu bei susidarius išskirtinėms aplinkybėms.

12. RIS saugumo dokumentų atnaujinimas viso jos gyvavimo ciklo metu vykdomas kaip neatsiejama pakeitimų atlikimo ir konfigūracijos tvarkymo proceso dalis.

Geriausios praktikos pavyzdžiai

13. TGS ir valstybės narės bendradarbiauja rengdami geriausios praktikos pavyzdžius RIS tvarkomai ESĮI apsaugoti. Geriausios praktikos gairėse išdėstomos RIS skirtos techninės, fizinės, organizacinės ir procedūrinės saugumo priemonės, kurių veiksmingumas apsisaugant nuo konkrečių grėsmių ir pažeidžiamumo buvo įrodytas.

14. RIS tvarkomos ESĮI apsauga grindžiama ir ES, ir už jos ribų ISU srityje dirbančių subjektų įgyta patirtimi.

15. Geriausios praktikos pavyzdžių platinimu ir jų įgyvendinimu prisidedama prie siekio užtikrinti lygiavertį įvairių TGS ir valstybių narių naudojamų RIS, kuriose tvarkoma ESĮI, saugumo užtikrinimo lygį.

Nuodugni apsauga

16. Siekiant sušvelninti pavojų RIS, įgyvendinama daug techninių ir netechninių saugumo priemonių, kurios grupuojamos kaip kelios gynybinės linijos. Jos apima:

a) atgrasymą: saugumo priemones, skirtas įtikinti nerengti priešiškų planų pulti RIS;

b) prevenciją: saugumo priemones, skirtas apsunkinti RIS puolimą arba jam sutrukdyti;

c) aptikimą: saugumo priemones, skirtas aptikti RIS puolimo atvejį;

d) atsparumą: saugumo priemones, skirtas apriboti puolimo poveikį iki mažiausio informacijos rinkinio ar RIS dalių grupės bei užkirsti kelią tolesnei žalai; ir

e) atstatymą: saugumo priemones, skirtas RIS saugiai padėčiai atkurti.

Tokių saugumo priemonių griežtumo lygis nustatomas atsižvelgiant į rizikos įvertinimą.

17. Kompetentingos institucijos užtikrina savo gebėjimus reaguoti į incidentus, kurie gali apimti kelias organizacijas ar valstybes, kad galėtų derinti reagavimo veiksmus ir dalytis informacija apie šiuos incidentus bei susijusią

riziką (kompiuterinių incidentų tyrimo gebėjimai).

Minimalumo ir mažiausių privilegijų principas

18. Įdiegiamos tik atsižvelgiant į operacinius reikalavimus būtinos funkcijos, prietaisai ir paslaugos siekiant išvengti bereikalingos rizikos.

19. RIS naudotojams ir automatizuotiems procesams suteikiama tik tokia prieiga, privilegijos ar leidimai, kokios jiems reikia savo užduotims atlikti siekiant apriboti žalą, kuri padaroma dėl avarijų, klaidų ar RIS išteklių naudojimo be leidimo.

20. RIS atliekamos registravimo procedūros prireikus patikrinamos akreditavimo proceso metu.

Informuotumas informacijos saugumo užtikrinimo srityje

21. Informuotumas apie riziką ir turimas saugumo priemones yra pirmoji RIS saugumo gynybos linija. Visų pirma visi personalo nariai, susiję su RIS gyvavimo ciklu, įskaitant naudotojus, suvokia:

a) kad saugumo spragos gali labai pakenkti RIS;

b) galimą žalą kitiems, kuri gali kilti dėl tarpusavio sujungimo ir tarpusavio priklausomybės; ir

c) savo asmeninę atsakomybę ir atsakingumą už RIS saugumą atsižvelgdami į savo vaidmenį naudojant sistemas ir procesus.

22. Siekiant užtikrinti, kad būtų suvokiama atsakomybė už saugumą visam dalyvaujančiam personalui, įskaitant aukštesniąją vadovybę ir RIS naudotojus, yra privalomi ISU švietimo ir informuotumo mokymai.

IT saugumo priemonių vertinimas ir patvirtinimas

23. Reikiamas saugumo priemonių patikimumo lygis, apibrėžiamas kaip saugumo užtikrinimo lygis, nustatomas remiantis rizikos valdymo proceso rezultatais ir laikantis atitinkamos saugumo politikos bei saugumo gairių.

24. Saugumo užtikrinimo lygis patikrinamas naudojant tarptautiniu arba nacionaliniu lygiu patvirtintus procesus ir metodus. Tai apima pirminį įvertinimą, kontrolę ir auditą.

25. ESĮI apsaugai skirtas šifravimo priemones įvertina ir patvirtina valstybės narės nacionalinė KPI.

26. Prieš rekomenduojant, kad pagal 10 straipsnio 6 dalį jas pavirtintų Taryba arba generalinis sekretorius, tokias šifravimo priemones turi būti įvertinusi antra šalis, t. y. valstybės narės Tinkamos kvalifikacijos institucija (TKI), kuri nesusijusi su įrangos projektavimu arba gamyba. Reikalaujamas antros šalies įvertinimo išsamumo lygis priklauso nuo numatomo didžiausio ESĮI, kuri bus apsaugoma šiomis priemonėmis, slaptumo žymos laipsnio. Taryba patvirtina šifravimo priemonių vertinimo ir patvirtinimo saugumo politiką.

27. Atitinkamai Taryba arba generalinis sekretorius, remdamiesi Saugumo komiteto rekomendacija, gali netaikyti 25 arba 26 punkte nustatytų reikalavimų ir tam tikram laikotarpiui suteikti laikiną patvirtinimą laikydamiesi 10 straipsnio 6 dalyje nustatytos tvarkos, kai tai pateisinama dėl konkrečių su veikla su-

sijusių priežasčių.

28. TKI yra valstybės narės KPI, kuri buvo akredituota remiantis Tarybos nustatytais kriterijais antram ESĮI apsaugai skirtų šifravimo priemonių įvertinimui atlikti.

29. Taryba patvirtina ne šifravimo IT saugumo priemonių reikalavimų atitikimo ir patvirtinimo saugumo politiką.

Perdavimas saugumo zonose

30. Nepaisant šio sprendimo nuostatų, kai ESĮI perdavimas vykdomas saugumo zonose, remiantis rizikos valdymo proceso rezultatais ir SAI pritarus gali būti naudojamas nešifruotas platinimas arba šifravimas žemesniu lygiu.

Saugus RIS tarpusavio sujungimas

31. Šiame sprendime sistemų tarpusavio sujungimas reiškia tiesioginį dviejų ar daugiau IT sistemų sujungimą siekiant dalytis duomenimis ir kitais informacijos šaltiniais (pavyzdžiui, ryšiais) vienakrypčiu arba daugiakrypčiu būdu.

32. RIS kiekviena tarpusavyje sujungta IT sistema pirmiausia yra traktuojama kaip nepatikima ir sistemoje įdiegiamos apsaugos priemonės keitimuisi įslaptinta informacija kontroliuoti.

33. Bet kokio RIS ir kitos IT sistemos tarpusavio sujungimo atveju laikomasi toliau išdėstytų pagrindinių reikalavimų:

a) tokiems tarpusavio sujungimams taikomus veiklos arba operacinius reikalavimus nurodo ir patvirtina atsakingos institucijos;

b) tarpusavio sujungimui taikomas rizikos valdymas ir akreditavimo procesas bei yra reikalingas kompetentingų SAI pavirtinimas; ir

c) ribų apsaugos priemonės (RAP) įdiegiamos visų RIS perimetre.

34. Akredituota RIS ir neapsaugotas arba viešas tinklas negali būti tarpusavyje sujungiami, išskyrus atvejus, kai tarp RIS ir neapsaugoto arba viešo tinklo yra šiuo tikslu įdiegtos patvirtintos ribų apsaugos priemonės. Tokiems tarpusavio sujungimams taikytinas saugumo priemones peržiūri kompetentinga ISUI ir patvirtina kompetentinga SAI.

Kai duomenys, perduodami neapsaugotu arba viešu tinklu, yra užšifruojami pagal 10 straipsnį patvirtinta šifravimo priemone, toks sujungimas nelaikomas tarpusavio sujungimu.

35. Draudžiamas tiesioginis arba pakopinis RIS, akredituotos tvarkyti slaptumo žyma TRES SECFRET UE/EU TOP SECRET pažymėtą informaciją, ir neapsaugoto arba viešo tinklo tarpusavio sujungimas.

Kompiuterinių duomenų saugojimo laikmenos

36. Kompiuterinių duomenų saugojimo laikmenos sunaikinamos laikantis kompetentingos saugumo institucijos patvirtintų procedūrų.

37. Kompiuterinių duomenų saugojimo laikmenos gali būti naudojamos pakartotinai, gali būti sumažintas jų slaptumo žymos laipsnis arba jos gali būti išslaptinamos laikantis saugumo politikos, kuri turi būti nustatyta pagal 6 straipsnio 1 dalį.

Nepaprastosios padėties sąlygos

38. Nepaisant šio sprendimo nuostatų, toliau apibūdintos specialios procedūros gali būti taikomos esant nepaprastajai padėčiai, pavyzdžiui, gresiant ar esant krizei, konfliktui ar karinei padėčiai arba susidarius išskirtinėms su eksploatavimu susijusioms sąlygoms.

39. ESĮI gali būti perduodama naudojant šifravimo priemones, kurios buvo patvirtintos žemesnio įslaptinimo laipsnio informacijai, arba nešifruota kompetentingai institucijai pritarus, jei vėlavimas padarytų aiškiai didesnę žalą, negu įslaptintos medžiagos atskleidimas, ir jei:

a) siuntėjas ir gavėjas neturi reikiamos šifravimo įrangos arba jokios šifravimo įrangos; ir

b) įslaptinta medžiaga negali būti laiku perduota kitomis priemonėmis.

40. 38 punkte išdėstytomis aplinkybėmis perduodama įslaptinta informacija nėra pažymėta jokiomis žymomis arba nuorodomis, kurios sudarytų sąlygas ją atskirti nuo neįslaptintos informacijos arba kurią galima apsaugoti naudojant turimas šifravimo priemones. Gavėjams kitomis priemonėmis nedelsiant pranešama apie informacijos slaptumo laipsnį.

41. Jeigu taikomas 38 punktas, kompetentingai institucijai ir Saugumo komitetui vėliau pateikiama ataskaita.

III. SU INFORMACIJOS SAUGUMO UŽTIKRINIMU SUSIJUSIOS FUNKCIJOS IR INSTITUCIJOS

42. Valstybėse narėse ir TGS nustatomos toliau išdėstytos su informacijos saugumo užtikrinimu susijusios funkcijos. Šioms funkcijoms nereikalingas vienas bendras organizacinis subjektas. Joms suteikiami atskiri įgaliojimai. Tačiau šios funkcijos ir su jomis susijusi atsakomybė gali būti sujungtos arba integruotos viename organizaciniame vienete arba padalytos skirtingiems organizaciniams vienetams, jei išvengiama vidaus interesų arba užduočių konfliktų.

Informacijos saugumo užtikrinimo institucija

43. ISUI atsako už šias sritis:

a) ISU srities saugumo politikos formavimą ir saugumo gairių rengimą bei jų veiksmingumo bei tinkamumo stebėseną;

b) su šifravimo priemonėmis susijusios techninės informacijos apsaugą ir administravimą;

c) užtikrinimą, kad ESĮI apsaugai parinktos ISU priemonės atitiktų atitinkamą jų tinkamumo nustatymo ir atrankos politiką;

d) užtikrinimą, kad šifravimo priemonės būtų pasirenkamos laikantis jų tinkamumo nustatymo ir atrankos politikos;

e) mokymo ir informuotumo ISU srityje derinimą;

f) konsultavimąsi su sistemos tiekėju, saugumo srities subjektais ir vartotojų atstovais ISU saugumo politikos ir saugumo gairių klausimais; ir

g) užtikrinimą, kad Saugumo komiteto ISU klausimais ekspertų pogrupis turėtų atitinkamas žinias.

TEI

44. TEI užtikrina, kad RIS atitiktų TEMPEST politiką ir gaires. Ji patvirtina TEMPEST kontrpriemones, skirtas įrenginiams ir priemonėms, siekiant apsaugoti ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje.

Kriptografijos patvirtinimo institucija

45. Kriptografijos patvirtinimo institucijos (KPI) pareiga – užtikrinti, kad šifravimo priemonės atitiktų nacionalinę šifravimo politiką arba Tarybos šifravimo politiką. Ji suteikia leidimą naudoti šifravimo priemonę siekiant apsaugoti ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje. Valstybėse narėse KPI papildomai atsako už šifravimo priemonių įvertinimą.

Kriptografijos platinimo institucija

46. Kriptografijos platinimo institucija (KPI) atsako už šias sritis:

a) ES šifravimo medžiagos valdymą ir apskaitą;

b) užtikrinimą, kad visos ES šifravimo medžiagos apskaitai, saugiam tvarkymui, saugojimui ir platinimui būtų taikomos tinkamos procedūros ir nustatyti tinkami kanalai; ir

c) ES šifravimo medžiagos perdavimo ją naudojantiems asmenims ir tarnyboms arba priėmimo iš jų užtikrinimą.

Saugumo akreditavimo institucija

47. Kiekvienai sistemai skirta SAI atsako už šias sritis:

a) užtikrinimą, kad RIS atitiktų atitinkamą saugumo politiką ir saugumo gaires, pareiškimo dėl RIS patvirtinimo, leidžiant jas naudoti tvarkant ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje, pateikimą, nurodant akreditavimo reikalavimus ir sąlygas bei kriterijus, kuriais remiantis sprendžiama, kad reikia iš naujo patvirtinti arba akredituoti RIS;

b) saugumo akreditavimo proceso nustatymą vadovaujantis atitinkama politika, aiškiai nurodant patvirtinimo sąlygas, nustatytas jos priežiūrai pavestoms RIS;

c) saugumo akreditavimo strategijos, kurioje išdėstytas akreditavimo proceso išsamumo lygis, atitinkantis reikiamą saugumo užtikrinimo lygį, nustatymą;

d) su saugumu susijusių dokumentų, įskaitant pareiškimus dėl rizikos valdymo ir likutinės rizikos, sistemos saugumo reikmių aktus (toliau – SSRA), saugumo įgyvendinimo patikrinimo dokumentus ir saugios eksploatacijos taisykles (toliau – SecOPs), nagrinėjimą ir patvirtinimą bei užtikrinimą, kad jie atitiktų Tarybos saugumo taisykles ir politiką;

e) su RIS susijusių saugumo priemonių įgyvendinimo patikrinimą vykdant saugumo įvertinimus, patikrinimus ar peržiūras arba juos finansuojant;

f) saugumo reikalavimų (pavyzdžiui, susijusių su personalo patikimumo laipsniais), taikomų svarbiausioms, susijusioms su RIS apsauga pareigybėms, nustatymą;

g) patvirtintų šifravimo ir TEMPEST priemonių, naudojamų siekiant užtikrinti RIS saugumą, parinkimo patvirtinimą;

h) RIS tarpusavio sujungimo su kitomis RIS patvirtinimą arba prireikus dalyvavimą bendrame patvirtinime; ir

i) sistemos tiekėjo, saugumo srities subjektų ir vartotojų atstovų konsultavimą saugumo rizikos valdymo, visų pirma likutinės rizikos, ir pareiškimo dėl patvirtinimo reikalavimų ir sąlygų klausimais.

48. TGS SAI atsako už visų TGS kompetencijai priklausančių RIS akreditavimą.

49. Atitinkama valstybės narės SAI atsako už tos valstybės narės kompetencijai priklausančių RIS ir jų sisteminių komponentų akreditavimą.

50. Jungtinė saugumo akreditacijos valdyba (SAV) yra atsakinga tiek už TGS SAI žinioje, tiek už valstybių narių SAI žinioje esančių RIS akreditavimą. Ją sudaro po vieną kiekvienos valstybės narės SAI atstovą, o jos posėdžiuose dalyvauja Europos Komisijos atstovas SAI klausimais. Kiti subjektai, turintys prijungimo prie RIS mazgus, kviečiami dalyvauti posėdžiuose, kai svarstomi su ta sistema susiję klausimai.

SAV pirmininkauja TGS SAI atstovas. Ji sprendimus priima institucijų, valstybių narių ir kitų subjektų, turinčių prijungimo prie RIS mazgus, SAI atstovų sutarimu. SAV reguliariai teikia savo veiklos ataskaitas Saugumo komitetui ir jam praneša apie visus pareiškimus dėl akreditavimo.

Informacijos saugumo užtikrinimo operacinė institucija

51. Kiekvienai sistemai skirta ISU operacinė institucija atsako už šias sritis:

a) saugumo dokumentų, atitinkančių saugumo politiką ir saugumo gaires, rengimą, visų pirma SSRA, įskaitant pareiškimą dėl likutinės rizikos, SecOPs ir šifravimo planą vykdant RIS akreditavimo procesą, rengimą;

b) dalyvavimą atrenkant ir bandant konkrečioms sistemoms skirtas techninio saugumo priemones, prietaisus ir programinę įrangą, jų įgyvendinimo priežiūrą ir užtikrinimą, kad jie būtų saugiai įdiegti, sukonfigūruoti bei eksploatuojami pagal atitinkamus saugumo dokumentus;

c) dalyvavimą parenkant TEMPEST saugumo priemones ir prietaisus, jei reikia pagal SSRA, ir užtikrinimą, kad jie būtų saugiai įdiegti ir eksploatuojami bendradarbiaujant su TEI;

d) SecOps įgyvendinimo ir taikymo stebėseną; prireikus atsakomybę už eksploatavimo saugumą deleguojant sistemos savininkui;

e) šifravimo priemonių valdymą ir tvarkymą užtikrinant šifravimo ir kontroliuojamų objektų saugojimą ir prireikus užtikrinant šifravimo kintamųjų generavimą;

f) saugumo analizės peržiūros ir bandymų atlikimą, visų pirma siekiant parengti atitinkamas rizikos ataskaitas, kurių reikalauja SAI;

g) mokymo konkrečioms RIS skirto ISU klausimais rengimą;

h) konkrečioms RIS skirtų apsaugos priemonių įgyvendinimą ir vykdymą.

V PRIEDAS
PRAMONINIS SAUGUMAS

I. ĮVADAS

1. Šiame priede nustatytos 11 straipsnio įgyvendinimo nuostatos. Jame išdėstytos bendros saugumo nuostatos, taikomos pramonės ar kitiems subjektams derybų dėl sutarčių sudarymo metu arba visą TGS sudarytų įslaptintų sutarčių gyvavimo ciklą.

2. Taryba patvirtina pramoninio saugumo politiką, kurioje visų pirma apibrėžiami išsamūs reikalavimai susiję su ĮPPP, saugumo aspektų paaiškinimais (SAP), vizitais, ESĮI perdavimu ir gabenimu.

II. SAUGUMO ASPEKTAI ĮSLAPTINTOSE SUTARTYSE

Slaptumo žymų vadovas (SŽV)

3. Prieš paskelbdamas kvietimą teikti pasiūlymus įslaptintai sutarčiai sudaryti arba prieš sudarydamas įslaptintą sutartį, TGS, kaip perkančioji institucija, nustato visos informacijos, kuri turi būti suteikta konkurso dalyviams ir rangovams, slaptumo žymą, taip pat visos informacijos, kurią turi parengti rangovas, slaptumo žymą. Šiuo tikslu TGS parengia SŽV, kuris turi būti naudojamas vykdant sutartį.

4. Siekiant nustatyti skirtingų įslaptintos sutarties dalių slaptumo žymą, taikomi toliau nurodyti principai:

a) rengdamas SŽV, TGS atsižvelgia į visus svarbius saugumo aspektus, įskaitant slaptumo žymą, kurią informacijai priskyrė jos įslaptintos informacijos rengėjas ir kurią jis patvirtino kaip naudotiną tai sutarčiai;

b) bendras sutarties slaptumo žymos laipsnis negali būti žemesnis nei aukščiausia bet kurios jos dalies slaptumo žyma; ir

c) atitinkamais atvejais, jei daromi pakeitimai, susiję su slaptumo žymų suteikimu informacijai, parengtai rangovų ar jiems suteiktai vykdant sutartį, ir jei daromi vėlesni SŽV pakeitimai, TGS palaiko ryšius su valstybių narių NSI/PSI ar kitomis atitinkamomis kompetentingomis saugumo institucijomis.

Saugumo aspektų paaiškinimas (SAP)

5. Konkrečioms sutartims skirti saugumo reikalavimai aprašomi SAP. Prireikus į SAP įtraukiamas SŽV; SAP yra neatsiejama įslaptintos sutarties ar subrangos sutarties dalis.

6. SAP nustatomos nuostatos, pagal kurias reikalaujama, kad rangovas ir (arba) subrangovas laikytųsi būtiniausių šiame sprendime nustatytų standartų. Šių būtiniausių standartų nesilaikymas gali būti pakankamas pagrindas sutarčiai nutraukti.

Programos / projekto saugumo instrukcijos (PSI)

7. Atsižvelgiant į programų ar projektų, kuriuos vykdant reikia susipažinti su ESĮI arba ją tvarkyti ar saugoti, apimtį, programą ar projektą valdyti paskirta perkančioji institucija gali parengti konkrečios programos / projekto saugumo instrukcijas (PSI). PSI turi patvirtinti valstybių narių NSI/PSI ar kita programoje / projekte dalyvaujanti kompetentinga saugumo institucija; jose gali būti nustatyti papildomi saugumo reikalavimai.

III. ĮMONĖS PATIKIMUMĄ PATVIRTINANTIS PAŽYMĖJIMAS (ĮPPP)

8. ĮPPP išduoda valstybės narės NSI arba PSI ar kita kompetentinga saugumo institucija ir jame pagal nacionalinius įstatymus ir kitus teisės aktus nurodoma, kad pramonės arba kitas subjektas savo patalpose gali apsaugoti atitinkamo slaptumo žymos (CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET) laipsnio ESĮI. Prieš rangovui ar subrangovui arba potenciaIiam rangovui ar subrangovui suteikiant ESĮI arba galimybę susipažinti su ESĮI, TGS, kaip perkančiajai institucijai, turi būti pateikiamas ĮPPP.

9. Išduodama ĮPPP atitinkama NSI ar PSI, mažų mažiausiai:

a) įvertina pramonės ar kitų subjektų patikimumą;

b) įvertina nuosavybę, kontrolę ar nederamos įtakos tikimybę, kurie gali būti laikomi saugumo rizika;

c) įsitikina, kad pramonės arba kitas subjektas patalpose yra sukūręs saugumo sistemą, kuri apima visas atitinkamas saugumo priemones, būtinas, kad būtų apsaugota informacija ar medžiaga, pažymėta CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma, laikantis šiame sprendime nustatytų reikalavimų;

d) įsitikina, kad vadovybės, savininkų ir darbuotojų, kurie turi turėti galimybę susipažinti su informacija, pažymėta CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma, asmens patikimumo statusas yra nustatytas laikantis šiame sprendime nustatytų reikalavimų;

e) įsitikina, kad pramonės arba kitas subjektas yra paskyręs patalpų saugumo pareigūną, kuris yra atsakingas vadovybei už saugumo įsipareigojimų tokiame subjekte vykdymo užtikrinimą.

10. Atitinkamais atvejais TGS, kaip perkančioji institucija, praneša atitinkamai NSI/PSI ar kitai kompetentingai saugumo institucijai, kad prieš sudarant sutartį arba sutarties vykdymui reikalingas ĮPPP. ĮPPP arba APP reikalaujama prieš sudarant sutartį, tais atvejais, kai ESĮI, pažymėta CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma, turi būti suteikta paraiškų teikimo proceso metu.

11. Perkančioji institucija nesudaro įslaptintos sutarties su pasirinktu dalyviu prieš tai negavusi valstybės narės, kurioje yra registruotas atitinkamas rangovas ar subrangovas, NSI/PSI ar kitos kompetentingos saugumo institucijos patvirtinimo, kad reikiamais atvejais yra išduotas tinkamas ĮPPP.

12. ĮPPP išdavusi NSI/PSI ar kita kompetentinga saugumo institucija praneša TGS, kaip perkančiajai institucijai, apie pasikeitimus, turinčius įtakos ĮPPP.

Subrangos sutarties atveju atitinkamai informuojama NSI/PSI ar kita kompetentinga saugumo institucija.

13. Jeigu atitinkama NSI/PSI ar kita kompetentinga saugumo institucija panaikina ĮPPP, tai yra pakankamas pagrindas TGS, kaip perkančiajai institucijai, nutraukti įslaptintą sutartį arba pašalinti dalyvį iš konkurso.

IV. ĮSLAPTINTOS SUTARTYS IR SUBRANGOS SUTARTYS

14. Tais atvejais, kai ESĮI suteikiama dalyviui prieš sudarant sutartį, kvietime teikti paraiškas numatoma nuostata, kuria paraiškos nepateikęs dalyvis arba dalyvis, kuris nebuvo atrinktas, įpareigojamas per nurodytą laiką grąžinti visus įslaptintus dokumentus.

15. Sudarius įslaptintą sutartį ar subrangos sutartį, TGS, kaip perkančioji institucija, praneša rangovo ar subrangovo NSI/PSI ar kitai kompetentingai saugumo institucijai tos įslaptintos sutarties saugumo nuostatas.

16. Nutraukus tokią sutartį, TGS, kaip perkančioji institucija (ir (arba) atitinkamai NSI/PSI ar kita kompetentinga saugumo institucija subrangos sutarties atveju) skubiai apie tai praneša valstybės narės, kurioje registruotas rangovas arba subrangovas, NSI/PSI ar kitai kompetentingai saugumo institucijai.

17. Paprastai reikalaujama, kad nutraukus įslaptintą sutartį ar subrangos sutartį rangovas arba subrangovas perkančiajai institucijai grąžintų visą turimą ESĮI.

18. Konkrečios nuostatos dėl ESĮI sunaikinimo vykdant sutartį arba ją nutraukus nustatomos SAP.

19. Tais atvejais, kai rangovui arba subrangovui duotas leidimas nutraukus sutartį pasilikti ESĮI, rangovas ir subrangovas toliau laikosi šiame sprendime nustatytų būtiniausių standartų bei užtikrina ESĮI konfidencialumą.

20. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, nurodomos kvietime teikti paraiškas ir sutartyje.

21. Prieš sudarydamas subrangos sutartis dėl įslaptintos sutarties dalių, rangovas turi gauti TGS, kaip perkančiosios institucijos, leidimą. Su pramonės arba kitais subjektais, registruotais valstybėje, kuri nėra ES valstybė narė ir nėra sudariusi susitarimo dėl informacijos saugumo su ES, subrangos sutartys negali būti sudaromos.

22. Rangovas atsako už tai, kad visa subrangos veikla būtų vykdoma laikantis šiame sprendime nustatytų būtiniausių standartų, ir negali suteikti subrangovui ESĮI be išankstinio rašytinio perkančiosios institucijos sutikimo.

23. ESĮI, kurią parengė ar tvarko rangovas arba subrangovas, atžvilgiu įslaptintos informacijos rengėjo teisėmis naudojasi perkančioji institucija.

V. SU ĮSLAPTINTOMIS SUTARTIMIS SUSIJĘ VIZITAI

24. Jei TGS, rangovams ar subrangovams vykdant įslaptintą sutartį jiems priklausančiose patalpose reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma pažymėta informacija, dėl jų vizitų susitariama palaikant ryšius su NSI/PSI arba kita susijusia

kompetentinga saugumo institucija. Tačiau atsižvelgiant į tam tikrus projektus NSI/PSI gali taip pat susitarti dėl tvarkos, pagal kurią dėl tokių vizitų gali būti susitariama tiesiogiai.

25. Tam, kad būtų leista susipažinti su ESĮI, susijusia su TGS sutartimi, visi lankytojai turi turėti atitinkamą APP ir turi būti vadovaujamasi principu „būtina žinoti“.

26. Lankytojams leidžiama susipažinti tik su ta ESĮI, kuri yra susijusi su vizito tikslu.

VI. ESĮI PERDAVIMAS IR GABENIMAS

27. Perduodant ESĮI elektroninėmis priemonėmis taikomos atitinkamos 10 straipsnio ir IV priedo nuostatos.

28. Gabenant ESĮI taikomos atitinkamos III priedo nuostatos, laikantis nacionalinių įstatymų ir kitų teisės aktų.

29. Nustatant įslaptintos medžiagos kaip krovinio gabenimui taikomą saugumo tvarką taikomi toliau nurodyti principai:

a) saugumas užtikrinamas visuose gabenimo etapuose nuo gabenimo pradžios vietos iki galutinės paskirties vietos;

b) siuntai suteikiamas apsaugos lygis nustatomas pagal joje esančios medžiagos aukščiausią slaptumo žymos laipsnį;

c) gabenimą užtikrinančios bendrovės turi gauti atitinkamos slaptumo žymos ĮPPP. Tokiais atvejais laikantis I priedo turi būti patikrintas siuntą gabenančio personalo patikimumas;

d) prieš gabenant per valstybių sienas medžiagą, pažymėtą CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma, siuntėjas parengia, o atitinkamos NSI/PSI ar kitos kompetentingos saugumo institucijos patvirtina gabenimo planą;

e) stengiamasi, kad kelionės vyktų be sustojimo ir būtų užbaigtos kuo greičiau, atsižvelgiant į aplinkybes;

f) kai galima, turėtų būti pasirenkami maršrutai tik per valstybių narių teritorijas. Maršrutais per valstybes, kurios nėra valstybės narės, turėtų būti gabenama tik gavus siuntėjo ir gavėjo valstybių NSI/PSI ar kitos kompetentingos saugumo institucijos leidimą.

VII. ESĮI PERDAVIMAS TREČIOSIOSE VALSTYBĖSE ĮSIKŪRUSIEMS RANGOVAMS

30. ESĮI trečiosiose valstybėse įsikūrusiems rangovams ir subrangovams perduodama laikantis saugumo priemonių, dėl kurių susitarė TGS, kaip perkančioji institucija, ir atitinkamos trečiosios valstybės, kurioje registruotas rangovas, NSI/PSI.

VIII. RESTREINT UE/EU RESTRICTED SLAPTUMO ŽYMA PAŽYMĖTOS INFORMACIJOS TVARKYMAS IR SAUGOJIMAS

31. Palaikydamas ryšius su valstybės narės NSI/PSI TGS, kaip perkančioji institucija, prireikus turi teisę remiantis sutarties nuostatomis rengti vizitus į rangovo / subrangovo patalpas, kad patikrintų, ar įgyvendintos pagal sutartį reikalaujamos tinkamos saugumo priemonės, skirtos apsaugoti RESTREINT UE/EU RESTRICTED laipsnio slaptumo žyma pažymėtą ESĮI.

32. Kiek būtina pagal nacionalinius įstatymus ir kitus teisės aktus, NSI/PSI ar kitoms kompetentingoms saugumo institucijoms TGS, kaip perkančioji institucija, praneša apie sutartis arba subrangos sutartis, kuriose yra RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtos informacijos.

33. TGS sudarytų sutarčių, kuriose yra RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtos informacijos, atveju rangovai ar subrangovai ir jų personalas neprivalo turėti ĮPPP ar APP.

34. TGS, kaip perkančioji institucija, išnagrinėja atsakymus į kvietimus dalyvauti konkurse dėl sutarčių, pagal kurias turi būti suteikta galimybė susipažinti su RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėta informacija, neatsižvelgdama į reikalavimus, susijusius su ĮPPP ar APP, kurie gali būti numatyti nacionaliniuose įstatymuose ir kituose teisės aktuose.

35. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, turi atitikti 21 punkto reikalavimus.

36. Kai pagal sutartį numatytas informacijos, pažymėtos RESTREINT UE/EU RESTRICTED slaptumo žyma, tvarkymas rangovo naudojamoje RIS, TGS, kaip perkančioji institucija, užtikrina, kad sutartyje arba subrangos sutartyje būtų nustatyti su RIS akreditavimu susiję būtini techniniai ir administraciniai reikalavimai, kurie atitiktų įvertintą riziką, atsižvelgiant į visus svarbius veiksnius. Perkančioji institucija ir atitinkama NSI/PSI susitaria dėl tokio RIS akreditavimo masto.

VI PRIEDAS

KEITIMASIS ĮSLAPTINTA INFORMACIJA SU TREČIOSIOMIS ŠALIMIS IR TARPTAUTINĖMIS ORGANIZACIJOMIS

I. ĮVADAS

1. Šiame priede nustatytos 12 straipsnio įgyvendinimo nuostatos.

II. TVARKA, REGLAMENTUOJANTI KEITIMĄSI ĮSLAPTINTA INFORMACIJA

2. Tarybai nustačius, kad yra ilgalaikis poreikis keistis įslaptinta informacija, sudaromas:

- susitarimas dėl informacijos saugumo, arba
- administracinis susitarimas, vadovaujantis 12 straipsnio 2 dalimi ir III bei IV skirsniais bei remiantis saugumo komiteto rekomendacija.

3. Tais atvejais, kai BSGP operacijos vykdymui surinkta ESĮI gali būti suteikiama tokioje operacijoje dalyvaujančioms trečiosioms valstybėms ar tarptautinėms organizacijoms, ir jeigu nėra nustatyta 2 dalyje nurodyta tvarka, keitimasis ESĮI su dalyvaujančiąja trečiąja valstybe arba tarptautine organizacija vadovaujantis V skirsniu reglamentuojamas:

- susitarimu dėl dalyvavimo bendrųjų sąlygų,
- ad hoc susitarimu dėl dalyvavimo, arba
- jeigu nėra sudarytas nė vienas iš pirmiau nurodytų susitarimų – ad hoc administraciniu susitarimu.

4. Jeigu nėra nustatyta 2 ir 3 dalyse nurodyta tvarka ir jeigu priimamas sprendimas vadovaujantis VI skirsniu suteikti ESĮI trečiajai valstybei ar tarptautinei organizacijai išimtine ad hoc tvarka, iš atitinkamos trečiosios valstybės ar tarptautinės organizacijos turi būti gautas raštiškas patvirtinimas, kad ji saugos bet kokią jai suteiktą ESĮI laikydamasi šiame sprendime nustatytų pagrindinių principų ir būtiniausių standartų.

III. SUSITARIMAI DĖL INFORMACIJOS SAUGUMO

5. Susitarimais dėl informacijos saugumo nustatomi pagrindiniai principai ir būtiniausi standartai, reglamentuojantys ES ir trečiosios valstybės ar tarptautinės organizacijos keitimąsi įslaptinta informacija.

6. Susitarimuose dėl informacijos saugumo numatomi techniniai įgyvendinimo susitarimai, dėl kurių turi susitarti TGS saugumo tarnyba, EKSD ir kompetentinga atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo institucija. Tokiuose susitarimuose atsižvelgiama į atitinkamoje trečiojoje valstybėje ar tarptautinėje organizacijoje galiojančiais saugumo nuostatais ir esamomis struktūromis bei procedūromis užtikrinamą apsaugos lygį. Šiuos susitarimus patvirtina Saugumo komitetas.

7. Keistis ESĮI elektroninėmis priemonėmis neleidžiama, jei tai nėra aiškiai numatyta susitarime dėl informacijos saugumo arba techniniuose įgyvendinimo susitarimuose.

8. Susitarimuose dėl informacijos saugumo numatoma, kad prieš keičiantis įslaptinta informacija pagal susitarimą, TGS saugumo tarnyba ir EKSD susitaria, kad gaunančioji šalis atitinkamu būdu gali apsaugoti ir saugoti jai teikiamą informaciją.

9. Kai Taryba sudaro susitarimą dėl informacijos saugumo, kiekvienoje šalyje paskiriama po vieną registratūrą, kuri yra pagrindinis įslaptintos informacijos gavimo ir išsiuntimo punktas.

10. Siekiant įvertinti atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo nuostatus, struktūras ir procedūras, abipusiu susitarimu su atitinkama trečiąja valstybe ar tarptautine organizacija TGS Saugumo tarnyba kartu su EKSD rengia įvertinimo vizitus. Tokie įvertinimo vizitai rengiami laikantis atitinkamų III priedo nuostatų ir jų metu įvertinama:

a) įslaptintai informacijai apsaugoti taikoma reglamentavimo sistema;

b) bet kurie konkretūs saugumo politikos ypatumai ir saugumo organizavimo tvarka trečiojoje valstybėje arba tarptautinėje organizacijoje, kurie galėtų daryti poveikį įslaptintos informacijos, kuria gali būti keičiamasi, slaptumo žymos laipsniui;

c) faktiškai taikomos saugumo priemonės ir procedūros; ir

d) patikimumo patikrinimo procedūros, susijusios su numatomos suteikti ESĮI slaptumo žymos laipsniu.

11. ES vardu įvertinimo vizitą atliekanti grupė įvertina, ar atitinkamoje trečiojoje valstybėje arba tarptautinėje organizacijoje saugumo nuostatai ir procedūros yra tinkami, kad būtų apsaugota atitinkamo slaptumo žymos laipsnio ESĮI.

12. Šių vizitų rezultatai pateikiami ataskaitoje, kuria remdamasis Saugumo komitetas nustato, koks gali būti aukščiausias ESĮI, kuria gali būti keičiamasi su atitinkama trečiąja šalimi popieriuje ir prireikus elektroninėmis priemonėmis, slaptumo žymos laipsnis, bei konkrečias sąlygas, reglamentuojančias keitimąsi šia informacija su ta šalimi.

13. Būtina dėti visas pastangas, kad būtų surengtas vizitas į atitinkamą trečiąją valstybę arba tarptautinę organizaciją saugumui visapusiškai įvertinti prieš tai, kai Saugumo komitetas patvirtina įgyvendinamuosius susitarimus, siekiant nustatyti taikomos saugumo sistemos pobūdį ir veiksmingumą. Tačiau jei tai nėra įmanoma, TGS saugumo tarnyba Saugumo komitetui pateikia kuo išsamesnę ataskaitą, pagrįstą turima informacija, informuodama Saugumo komitetą apie taikomus saugumo nuostatus ir saugumo organizavimo tvarką atitinkamoje trečiojoje valstybėje arba tarptautinėje organizacijoje.

14. Saugumo komitetas gali nuspręsti, kad laukiant įvertinimo vizito rezultatų negalima suteikti ESĮI arba galima suteikti ESĮI, kurios slaptumo žymos laipsnis ne aukštesnis nei nurodytas, arba jis gali nustatyti kitas specialias sąlygas, kurios taikomos ESĮI suteikimui atitinkamai trečiajai valstybei arba tarptautinei organizacijai. Apie tai TGS saugumo tarnyba praneša atitinkamai trečiajai valstybei arba tarptautinei organizacijai.

15. Remdamasi tarpusavio susitarimu su atitinkama trečiąja valstybe arba tarptautine organizacija, TGS saugumo tarnyba reguliariai rengia tolesnius įvertinimo vizitus, siekdama patikrinti, ar įdiegtos priemonės ir toliau atitinka iš pradžių sutartus būtiniausius standartus.

16. Kai susitarimas dėl informacijos saugumo įsigalioja ir keičiamasi įslap-

tinta informacija su atitinkama trečiąja valstybe ar tarptautine organizacija, Saugumo komitetas gali nuspręsti pakeisti ESĮI, kuria gali būti keičiamasi popieriniu pavidalu ar elektroninėmis priemonėmis, aukščiausią slaptumo žymos laipsnį, visų pirma atsižvelgdamas į tolesnių įvertinimo vizitų rezultatus.

IV. ADMINISTRACINIAI SUSITARIMAI

17. Esant ilgalaikiam poreikiui su trečiąja valstybe ar tarptautine organizacija keistis įslaptinta informacija, kurios slaptumo žymos laipsnis paprastai nėra aukštesnis nei RESTREINT UE/EU RESTRICTED, ir Saugumo komitetui nustačius, kad atitinkama šalis neturi pakankamai išplėtotos tokiai informacijai skirtos saugumo sistemos, kad ta šalis galėtų sudaryti susitarimą dėl informacijos saugumo, generalinis sekretorius gali, pritarus Tarybai, sudaryti administracinį susitarimą su atitinkamos trečiosios valstybės ar tarptautinės organizacijos atitinkamomis institucijomis.

18. Tais atvejais, kai dėl skubių operatyvinių priežasčių reikia greitai nustatyti keitimosi įslaptinta informacija tvarką, tik Taryba gali nuspręsti, kad būtų sudarytas administracinis susitarimas siekiant keistis aukštesnio slaptumo žymos laipsnio informacija.

19. Administraciniai susitarimai paprastai sudaromi pasikeičiant laiškais.

20. Prieš faktiškai suteikiant ESĮI atitinkamai trečiajai valstybei ar tarptautinei organizacijai rengiamas 10 punkte nurodytas įvertinimo vizitas, o šio vizito ataskaita siunčiama Saugumo komitetui ir jo tvirtinama kaip patenkinama. Tačiau, jei esama išskirtinių priežasčių skubiai pasikeisti įslaptinta informacija, apie kurias pranešta Tarybai, ESĮI gali būti suteikta, su sąlyga, kad dedamos visos pastangos kuo greičiau surengti tokį įvertinimo vizitą.

21. Keistis ESĮI elektroninėmis priemonėmis neleidžiama, jei tai nėra aiškiai numatyta administraciniame susitarime.

V. KEITIMASIS ĮSLAPTINTA INFORMACIJA VYKDANT BSGP OPERACIJAS

22. Trečiųjų valstybių ar tarptautinių organizacijų dalyvavimą BSGP operacijose reglamentuoja susitarimai dėl dalyvavimo bendrųjų sąlygų. Tokiuose susitarimuose nustatomos nuostatos dėl BSGP operacijų vykdymui surinktos ESĮI suteikimo jose dalyvaujančiosioms trečiosioms valstybėms ar tarptautinėms organizacijoms. Aukščiausias ESĮI, kuria gali būti keičiamasi, slaptumo žymos laipsnis yra RESTREINT UE/EU RESTRICTED BSGP civilinėms operacijoms ir CONFIDENTIEL UE/EU CONFIDENTIAL BSGP karinėms operacijoms, išskyrus atvejus, kai nustatyta kitaip sprendime, kuriuo įsteigiama kiekviena BSGP operacija.

23. Ad hoc susitarimuose dėl dalyvavimo, sudarytuose dėl konkrečios BSGP operacijos, nustatomos nuostatos dėl tos operacijos vykdymui surinktos ESĮI suteikimo joje dalyvaujančiajai trečiajai valstybei ar tarptautinei organizacijai. Aukščiausias ESĮI, kuria gali būti keičiamasi, slaptumo žymos laipsnis yra RESTREINT UE/EU RESTRICTED BSGP civilinėms operacijoms ir CONFIDENTIEL UE/EU CONFIDENTIAL BSGP karinėms operacijoms, išskyrus atvejus, kai nustatyta kitaip sprendime, kuriuo įsteigiama kiekviena BSGP operacija.

24. *Ad hoc* administraciniuose susitarimuose dėl trečiosios valstybės ar tarptautinės organizacijos dalyvavimo konkrečioje BSGP operacijoje gali būti nu-

matytas, inter alia, operacijos vykdymui surinktos ESĮI suteikimas tai trečiajai valstybei ar tarptautinei organizacijai. Tokie ad hoc administraciniai susitarimai sudaromi vadovaujantis IV skirsnio 17 ir 18 punktuose nustatyta tvarka. Aukščiausias ESĮI, kuria gali būti keičiamasi, slaptumo žymos laipsnis yra RESTREINT UE/EU RESTRICTED BSGP civilinėms operacijoms ir CONFIDENTIEL UE/EU CONFIDENTIAL BSGP karinėms operacijoms, išskyrus atvejus, kai nustatyta kitaip sprendime, kuriuo įsteigiama kiekviena BSGP operacija.

25. Prieš įgyvendinant nuostatas dėl ESĮI suteikimo pagal 22, 23 ir 24 punktus, nėra būtina sudaryti įgyvendinimo susitarimus ar rengti įvertinimo vizitus.

26. Jei priimančioji valstybė, kurios teritorijoje vykdoma BSGP operacija, nėra sudariusi su ES susitarimo dėl informacijos saugumo arba administracinio susitarimo dėl keitimosi įslaptinta informacija, iškilus konkrečiai neatidėliotinai su operatyvine veikla susijusiai būtinybei gali būti sudarytas ad hoc administracinis susitarimas. Ši galimybė numatoma sprendime, kuriuo įsteigiama BSGP operacija. Tokiomis aplinkybėmis suteikiama tik ta ESĮI, kuri buvo surinkta BSGP operacijai vykdyti ir kurios slaptumo žymos laipsnis nėra aukštesnis nei RESTREINT UE/EU RESTRICTED. Pagal tokį ad hoc administracinį susitarimą priimančioji valstybė įsipareigoja saugoti ESĮI laikydamasi būtiniausių standartų, kurie turi būti ne mažiau griežti nei yra nustatyti šiame sprendime.

27. Nuostatose dėl įslaptintos informacijos, kurios turi būti įtrauktos į susitarimus dėl dalyvavimo bendrųjų sąlygų ir į 22–24 punktuose nurodytus ad hoc administracinius susitarimus, nustatoma, kad atitinkama trečioji valstybė ar tarptautinė organizacija užtikrina, kad jos personalas, komandiruotas į bet kokią operaciją, saugos ESĮI pagal Tarybos saugumo taisykles ir vadovaudamasis tolesniais kompetentingų institucijų, įskaitant operacijos vadovavimo grandinės pareigūnus, pateiktais nurodymais.

28. Jeigu vėliau sudaromas ES ir dalyvaujančiosios trečiosios valstybės ar tarptautinės organizacijos susitarimas dėl informacijos saugumo, šio susitarimo dėl informacijos saugumo nuostatos yra viršesnės už bet kokių susitarimų dėl dalyvavimo bendrųjų sąlygų, ad hoc susitarimų dėl dalyvavimo ir ad hoc administracinių susitarimų nuostatas dėl keitimosi ESĮI bei jos apdorojimo.

29. Keistis ESĮI elektroninėmis priemonėmis pagal susitarimą dėl dalyvavimo bendrųjų sąlygų, ad hoc susitarimą dėl dalyvavimo ar ad hoc administracinį susitarimą su trečiąja valstybe ar tarptautine organizacija neleidžiama, jei tai nėra aiškiai numatyta atitinkamame susitarime arba administraciniame susitarime.

30. BSGP operacijos vykdymui surinkta ESĮI gali būti atskleidžiama trečiųjų valstybių ar tarptautinių organizacijų į tą operaciją komandiruotam personalui, vadovaujantis 22–29 punktų nuostatomis. Kai tokiam personalui leidžiama susipažinti su ESĮI BSGP operacijos patalpose ar RIS, turi būti imamasi priemonių (įskaitant atskleistos ESĮI registravimą), kad būtų sumažinta rizika, jog informacija bus prarasta ar atskleista. Tokios priemonės nurodomos atitinkamuose planavimo ar misijos dokumentuose.

VI. ESĮI AD HOC SUTEIKIMAS IŠIMTINE TVARKA

31. Jei nėra nustatyta galiojančios tvarkos pagal III–V skirsnius, ir Tarybai ar vienam iš jos parengiamųjų organų nusprendus, kad išimtiniu atveju reikia

suteikti ESĮI trečiajai valstybei ar tarptautinei organizacijai, TGS:

a) kiek įmanoma, patikrina atitinkamas trečiosios valstybės ar tarptautinės organizacijos saugumo institucijas, ar jų saugumo nuostatai, struktūros bei procedūros yra pakankami, kad užtikrintų, jog joms suteikta ESĮI būtų apsaugota pagal ne mažiau griežtus standartus nei yra nustatyti šiame sprendime;

b) prašo Saugumo komiteto, remiantis turima informacija, pateikti rekomendaciją, kiek galima pasitikėti atitinkamos trečiosios valstybės ar tarptautinės organizacijos, kuriai bus suteikta ESĮI, saugumo nuostatais, struktūromis bei procedūromis.

32. Jeigu Saugumo komitetas pateikia rekomendaciją, kuria pritaria ESĮI suteikimui, klausimas perduodamas Nuolatinių atstovų komitetui (COREPER), kuris priima sprendimą dėl šios ESĮI suteikimo.

33. Jeigu Saugumo komiteto rekomendacijoje nepritariama ESĮI suteikimui:

a) su BUSP/BSGP susijusiose srityse Politinis ir saugumo komitetas aptaria šį klausimą ir suformuluoja rekomendaciją dėl Nuolatinių atstovų komiteto sprendimo;

b) visose kitose srityse Nuolatinių atstovų komitetas aptarią šį klausimą ir priima sprendimą.

34. Jei manoma, kad tikslinga, ir iš anksto gavus rašytinį įslaptintos informacijos rengėjo sutikimą, Nuolatinių atstovų komitetas gali nuspręsti, kad įslaptinta informacija gali būti suteikta tik iš dalies ir tik tuo atveju, jei prieš tai jos slaptumo žymos laipsnis sumažinamas arba ji išslaptinama, arba kad informacija, kurią suteikti numatyta, turi būti parengta nenurodant šaltinio ar pirminio ES slaptumo žymos laipsnio.

35. Priėmus sprendimą suteikti ESĮI, TGS perduoda atitinkamą dokumentą, pažymėtą leidimo suteikti informaciją žyma, nurodant trečiąją valstybę ar tarptautinę organizaciją, kuriai ji buvo suteikta. Prieš suteikiant tokią informaciją arba faktinio jos suteikimo metu atitinkama trečioji šalis raštu įsipareigoja apsaugoti ESĮI, kurią ji gauna, pagal šiame sprendime nustatytus pagrindinius principus ir būtiniausius standartus.

VII. LEIDIMAS SUTEIKTI ESĮI TREČIOSIOMS VALSTYBĖMS ARBA TARPTAUTINĖMS ORGANIZACIJOMS

36. Kai yra nustatyta 2 dalyje nurodyta tvarka, reglamentuojanti keitimąsi įslaptinta informacija su trečiąja valstybe ar tarptautine organizacija, Taryba priima sprendimą suteikti leidimą generaliniam sekretoriui suteikti ESĮI atitinkamai trečiajai valstybei ar tarptautinei organizacijai, laikantis principo, kad su tuo turi sutikti įslaptintos informacijos rengėjas.

37. Kai yra nustatyta 3 dalyje nurodyta tvarka, reglamentuojanti keitimąsi įslaptinta informacija su trečiąja valstybe ar tarptautine organizacija, generaliniam sekretoriui suteikiamas leidimas suteikti ESĮI, vadovaujantis tuo sprendimu, kuriuo įsteigiama BSGP operacija, ir laikantis principo, kad su tuo turi sutikti įslaptintos informacijos rengėjas.

38. Generalinis sekretorius gali perduoti šią teisę vyresniesiems TGS pareigūnams ar kitiems jam pavaldiems asmenims.

Priedėliai

A Priedėlis
Sąvokų apibrėžtys

B Priedėlis
Slaptumo žymų atitikmenys

C Priedėlis
Nacionalinių saugumo institucijų (NSI) sąrašas

D Priedėlis
Santrumpų sąrašas

A priedėlis

SĄVOKŲ APIBRĖŽTYS

Šiame sprendime vartojamos tokios sąvokų apibrėžtys:

Akreditavimas – procesas, po kurio Saugumo akreditavimo institucija (SAI) pateikia oficialų pareiškimą, patvirtinantį kad sistemai yra leista veikti taikant nustatytą slaptumo žymos laipsnį, konkrečiu slaptumo režimu jos operacinėje aplinkoje ir priimtinu rizikos lygiu, laikantis prielaidos, kad įgyvendintas patvirtintas techninių, fizinių, organizacinių ir procedūrinių saugumo priemonių rinkinys;

Asmens patikimumo pažymėjimas (APP) - ES asmens patikimumo pažymėjimas (ES APP) – TGS paskyrimo tarnybos leidimas susipažinti su ESĮI, išduodamas pagal šį sprendimą valstybės narės kompetentingoms institucijoms užbaigus patikimumo tikrinimo procedūras ir patvirtinantis, kad asmeniui gali būti leidžiama susipažinti su iki tam tikro laipsnio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI iki nustatytos datos, jei nustatyta, kad asmuo atitinka principą „būtina žinoti“; taigi laikoma, kad nurodyto asmens patikimumas yra patikrintas;

Nacionalinis asmens patikimumo pažymėjimas (nacionalinis APP) – valstybės narės kompetentingos institucijos pažyma, leidžianti susipažinti su ESĮI ir išduota valstybės narės kompetentingoms institucijoms užbaigus patikimumo tikrinimo procedūras ir patvirtinanti, kad asmeniui gali būti leidžiama susipažinti su iki tam tikro laipsnio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI iki nustatytos datos, jei nustatyta, kad asmuo atitinka principą „būtina žinoti“; taigi laikoma, kad nurodyto asmens patikimumas yra patikrintas, asmens patikimumo pažymėjimą patvirtinanti pažyma (APPPP) kompetentingos institucijos išduota pažyma, kurioje nurodoma, kad asmens patikimumas yra patikrintas ir kad jis turi galiojantį nacionalinį arba ES APP, ir nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos laipsnis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma), atitinkamo APP galiojimo laikas ir pačios pažymos galiojimo laikas;

BSGP operacija – karinio ar civilinio krizių valdymo operacija – vadovaujantis ES sutarties V antraštinės dalies 2 skyriumi;

Sąlygų, kuriomis veikia RIS, apibrėžtis, pagrįsta apdorojamos informacijos slaptumo žyma ir patikimumo laipsniais, oficialiais prieigos patvirtinimais ir naudotojams taikomu principu “būtina žinoti”. Įslaptintos informacijos apdorojimui arba perdavimui gali būti taikomi keturi darbo režimai: skirtinis režimas, aukšto lygio sistemos režimas, patalpų atskyrimo pertvaromis režimas ir daugialaipsnis režimas:

- darbo saugumo režimas – skirtinis režimas – toks darbo režimas, kai visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo žymos laipsnio informacija ir pagal bendrą principą „būtina žinoti“ turi susipažinti su visa RIS tvarkoma informacija,

- **aukšto lygio sistemos režimas** – toks darbo režimas, kai visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo

žymos laipsnio informacija, tačiau ne visi galintys naudotis RIS asmenys turi pagal bendrą principą „būtina žinoti“ susipažinti su RIS tvarkoma informacija; patvirtinimas apie teisės susipažinti su informacija suteikimą gali būti išduodamas asmens,

- **patalpų atskyrimo pertvaromis režimas** – toks darbo režimas, kai visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo žymos laipsnio informacija, tačiau ne visi galintys naudotis RIS asmenys turi oficialų leidimą susipažinti su visa RIS tvarkoma informacija; oficialus leidimas reiškia oficialų patekimo į objektą centrinį valdymą, kuris yra atskirtas nuo leidimo asmeniui savo nuožiūra suteikti prieigą,

- **daugialaipsnis režimas** – toks darbo režimas, kai ne visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo žymos laipsnio informacija ir ne visi galintys naudotis RIS asmenys turi pagal bendrą principą „būtina žinoti“ susipažinti su RIS tvarkoma informacija; dokumentas fiksuota informacija, neatsižvelgiant į jos fizinę formą ar charakteristikas;

ES įslaptinta informacija (ESĮI) – žr. 2 straipsnio 1 dalį;

ESĮI administravimas – visi galimi veiksmai, kurie gali būti atliekami su ESĮI per visą jos gyvavimo ciklą. Tai apima ESĮI parengimą, apdorojimą, gabenimą, slaptumo žymos laipsnio sumažinimą, išslaptinimą ir sunaikinimą. RIS atžvilgiu tai taip pat apima ESĮI rinkimą, skelbimą, perdavimą ir saugojimą;

Fizinis saugumas – žr. 8 straipsnio 1 dalį;

Grėsmė – galimas nepageidaujamas atvejis, dėl kurio gali būti padaryta žala organizacijai ar jos naudojamoms sistemoms; tokios grėsmės gali būti atsitiktinės arba tyčinės (piktybinės); jas apibūdina pavojingi elementai, galimi taikiniai ir puolimo būdai;

Įmonės patikimumą patvirtinantis pažymėjimas (ĮPPP) – NSI ar PSI administracinis patvirtinimas, kad saugumo požiūriu patalpose gali būti užtikrinta nurodyto slaptumo žymos laipsnio ESĮI tinkamo lygio apsauga ir kad buvo tinkamai patikrintas jose dirbančio personalo narių, kuriems reikia susipažinti su ESĮI, patikimumas bei jie buvo informuoti apie atitinkamus saugumo reikalavimus, būtinus norint susipažinti su ESĮI ir ją apsaugoti;

Informacijos saugumo užtikrinimas – žr. 10 straipsnio 1 dalį;

Įslaptintos informacijos administravimas – žr. 9 straipsnio 1 dalį;

Įslaptintos informacijos rengėjas – ES institucija, agentūra ar įstaiga, valstybė narė, trečioji valstybė ar tarptautinė organizacija, kurios atsakomybe įslaptinta informacija buvo parengta ir (arba) pateikta naudoti ES struktūrose;

Įslaptinta subrangos sutartis – TGS rangovo ir kito rangovo (t. y. subrangovo) sudaryta prekių tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia susipažinti su ESĮI ar ją rengti arba suteikiama galimybė su ja susipažinti ar ją rengti;

Įslaptinta sutartis – TGS ir rangovo sudaryta prekių tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia susipažinti su ESĮI ar ją rengti arba suteikiama galimybė su ja susipažinti ar ją rengti;

Išslaptinimas – bet kokios slaptumo žymos panaikinimas;

Likutinė rizika – rizika, kuri lieka po to, kai buvo įgyvendintos saugumo priemonės, atsižvelgiant į tai, kad ne nuo visų grėsmių apsisaugoma ir ne visi

pažeidžiamumo aspektai gali būti pašalinti;

Medžiaga – dokumentas arba bet kokie pagaminti ar gaminami įrenginiai ar įranga;

Nuodugni apsauga – saugumo priemonių, kurios grupuojamos į kelis apsaugos lygius, taikymas;

Paskirtoji saugumo institucija (PSI) – valstybės narės nacionalinei saugumo institucijai (NSI) atsakinga institucija, kuri atsako už pramonės ir kitų subjektų informavimą apie nacionalinę politiką visais pramoninio saugumo klausimais ir duoda nurodymus bei padeda ją įgyvendinti. PSI funkciją gali vykdyti NSI arba kita kompetentinga institucija;

Patikimumo tikrinimas – tikrinimo procedūros, kurias, vadovaudamasi valstybėje narėje galiojančiais įstatymais ir kitais teisės aktais, atlieka kompetentinga institucija siekdama gauti užtikrinimą, kad nėra jokios nepalankios informacijos, kuri neleistų asmeniui išduoti nacionalinio arba ES asmens patikimumo pažymėjimo, suteikiančio galimybę susipažinti su tam tikro lygio ESĮI (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija);

Pažeidžiamumas – bet kokio pobūdžio silpnumas, kuriuo gali būti naudojamasi vienos ar daugiau grėsmių atveju. Pažeidžiamumas gali atsirasti dėl neveikimo arba gali būti susijęs su kontrolės stiprumo, išsamumo ar nuoseklumo trūkumu ir gali būti techninio, procedūrinio, fizinio, organizacinio ar veiklos pobūdžio;

Personalo patikimumas – žr. 7 straipsnio 1 dalį;

Pramonės arba kitas subjektas – subjektas, tiekiantis prekes, vykdantis darbus arba teikiantis paslaugas; tai gali būti pramonės, prekybos, paslaugų, mokslo, mokslinių tyrimų, švietimo ar vystymo subjektas arba savarankiškai dirbantis asmuo;

Pramoninis saugumas – žr. 11 straipsnio 1 dalį;

Programos / projekto saugumo instrukcijos (PSI) – saugumo procedūrų, kurios yra taikomos konkrečiai programai / projektui siekiant standartizuoti saugumo procedūras, sąrašas. Jos gali būti tikslinamos įgyvendinant programą / projektą;

Rangovas – fizinis arba juridinis asmuo, turintis teisnumą ir veiksnumą sudaryti sutartis;

Registravimas – žr. III priedo 18 punktą;

RIS gyvavimo ciklas – visa RIS egzistavimo trukmė, įskaitant inicijavimą, koncepciją, planavimą, reikalavimų analizę, projektavimą, sukūrimą, bandymą, įdiegimą, veikimą ir priežiūrą bei naudojimo nutraukimą;

Ryšių ir informacinė sistema (RIS) – žr. 10 straipsnio 2 dalį;

Galimybė, kad tam tikros grėsmės atveju bus pasinaudota organizacijos ar sistemų vidiniu ir išoriniu pažeidžiamumu ir taip bus padaryta žala organizacijai ir jos materialiajam ar nematerialiajam turtui. Ji įvertinama atsižvelgiant į kylančios grėsmės tikimybę ir į jos poveikį;

Rizika:

- rizikos pripažinimas – sprendimas atlikus rizikos tvarkymą pripažinti, kad vis dar yra likutinė rizika,

- **rizikos įvertinimas** – grėsmių ir pažeidžiamų sričių nustatymas bei susijusios rizikos analizės, t. y. galimumo ir poveikio analizės, atlikimas,

- **informavimas apie riziką** – RIS vartotojų bendruomenės informuotumo apie riziką didinimas, patvirtinimo institucijų informavimas apie tokią riziką ir pranešimų vykdančiosioms institucijoms teikimas;

Rizikos tvarkymas – rizikos silpninimas, šalinimas, mažinimas (taikant tinkamas technines, fizines, valdymo ar procedūrines priemones), perkėlimas arba stebėsena;

Saugumo aspektų paaiškinimas (SAP) – specialių sutartinių sąlygų rinkinys, kurį parengia perkančioji institucija ir kuris yra įslaptintos sutarties, pagal kurią gali būti susipažįstama su ESĮI arba tokia informacija gali būti rengiama, sudėtinė dalis – jame nurodomi saugumo reikalavimai arba sutarties dalys, kurių saugumą būtina užtikrinti;

Saugumo rizikos valdymo procesas – visas nebūtinai galinčių įvykti atvejų, kurie gali paveikti organizacijos arba jos naudojamų sistemų saugumą, nustatymo, kontrolės ir mažinimo procesas. Jis apima visą su rizika susijusią veiklą, įskaitant jos įvertinimą, tvarkymą, pripažinimą ir informavimą apie ją;

Slaptumo žymos laipsnio sumažinimas – slaptumo žymos lygio sumažinimas;

Slaptumo žymų vadovas (SŽV) – dokumentas, kuriame aprašomi programos arba sutarties įslaptintos dalys, nurodant taikomus slaptumo žymų laipsnius. SŽV gali būti papildomas programos arba sutarties vykdymo laikotarpiu, o informacijos dalims gali būti suteiktos naujos slaptumo žymos arba jų slaptumo žymos laipsnis gali būti sumažintas; tais atvejais, kai yra parengtas SŽV, jis yra SAP dalis;

Šifravimo priemonės – šifravimo algoritmai, šifravimo techninės ir programinės įrangos moduliai, priemonės, apimančios vykdymo informaciją bei susijusius dokumentus ir raktų duomenis;

Tarpusavio sujungimas – žr. IV priedo 31 punktą;

TEMPEST – elektromagnetinio spinduliavimo, dėl kurio neteisėtai atskleidžiama informacija, tikrinimas, tyrimas bei kontrolė ir jo šalinimo priemonės;

Turėtojas – tinkamą leidimą turintis asmuo, kuris atitinka principą „būtina žinoti“ ir turi ESĮI dalį bei yra atitinkamai atsakingas už jos apsaugą;

Turtas – viskas, kas turi tam tikrą vertę organizacijai, jos veiklos operacijoms bei jų tęstinumui, įskaitant informacijos išteklius, padedančius vykdyti organizacijos misiją.

B priedėlis

SLAPTUMO ŽYMŲ ATITIKMENYS

ES	TRES SECRET UE / EU TOP SECRET	SECRET UE / EU SECRET	CONFI-DENTIEL UE / EU CONFI-DENTIAL	RESTREINT UE / EU RESTRICTED
Belgija	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.199)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	(1) pastaba
Bulgarija	Строго секретно	Секретно	Поверително	За служебно ползване
Čekija	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danija	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Vokietija	STRENG GEHEIM	GEHEIM	VS (2) - VERTRAULICH	VS - NUR FÜR DEN DIENST-GEBRAUCH
Estija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Airija	Top Secret	Secret	Confidential	Restricted
Graikija	Άκρως Απόρρητο Santrumpa: (ΑΑΠ)	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Ispanija	SECRETO	RESERVADO	CONFI-DENCIAL	DIFUSIÓN LIMITADA
Prancūzija	Très Secret Défense	Secret Défense	Confidentiel Défense	(3) pastaba
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipras	Άκρως Απόρρητο Santrumpa: (ΑΑΠ)	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Liuksem-burgas	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux

Vengrija	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nyder-landai	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFI-DENTIEEL	Dep. VERT-ROUWELIJK
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lenkija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado
Rumunija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovėnija	Strogo tajno	Tajno	Zaupno	Interno
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomija	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUK-SELLINEN KONFI-DENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedija (4)	HEMLIG/ TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/ SECRET HEMLIG	HEMLIG/ CONFI-DENTIAL HEMLIG	HEMLIG/ REST-RICTED HEMLIG
Jungtinė Karalystė	Top Secret	Secret	Confidential	Restricted

(1) Diffusion Restreinte/Beperkte Verspreiding nėra slaptumo žyma Belgijoje. Žyma „RESTREINT UE/EU RESTRICTED“ pažymėtą informaciją Belgija tvarko ir saugo taip pat griežtai, kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

(2) Vokietija: VS = Verschlusssache.

(3) Prancūzijos nacionalinėje sistemoje slaptumo žyma „RESTREINT“ nenaudojama. Žyma „RESTREINT UE/EU RESTRICTED“ pažymėtą informaciją Prancūzija tvarko ir saugo taip pat griežtai, kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

(4) Švedija: viršutinėje eilutėje nurodytas slaptumo žymas naudoja gynybos institucijos, o nurodytas apatinėje eilutėje – kitos institucijos.

C Priedėlis

NACIONALINIŲ SAUGUMO INSTITUCIJŲ (NSI) SĄRAŠAS

BELGIJA
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
B-1000 Bruxelles
Sekretoriato telefonas: + 32/2/501 45 42
Faksas: + 32/2/501 45 96
El. paštas: nvo-ans@diplobel.fed.be

DANIJA
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Telefonas: + 45/33/14 88 88
Faksas: + 45/33/43 01 90

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 Copenhagen Ø
Telefonas: + 45/33/32 55 66
Faksas: + 45/33/93 13 20

BULGARIJA
State Commission on Information Security
90 Cherkovna Str.
BG-1505 Sofia
Telefonas: + 359/2/921 5911
Faksas: + 359/2/987 3750
El. paštas: dksi@government.bg
Tinklavietė: www.dksi.bg

VOKIETIJA
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Telefonas: + 49/30/18 681 0
Faksas: + 49/30/18 681 1441
El. paštas: oesIII3@bmi.bund.de

ČEKIJA
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
CZ-150 06 Praha 56
Telefonas: + 420/257 28 33 35
Faksas: + 420/257 28 31 10
El. paštas: czech.nsa@nbu.cz
Tinklavietė: www.nbu.cz

ESTIJA
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
EE-15094 Tallinn
Telefonas: +372/7170 113, +372/7170 117
Faksas: +372/7170 213
El. paštas: nsa@kmin.ee

AIRIJA
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2 Ireland
Telefonas: + 353/1/ 478 08 22
Faksas: + 353/1/ 408 29 59

ISPANIJA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
E-28023 Madrid
Telefonas: + 34/91/372 50 00
Faksas: + 34/91/372 58 08
El. paštas: nsa-sp@areatec.com

GRAIKIJA
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλέφωνα: + 30/210/657 20 45 (ώρες γραφείου)
+ 30/210/657 20 09 (ώρες γραφείου)
Φαξ: + 30/210/653 62 79
+ 30/210/657 76 12

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens
Telefonas: + 30/210/657 20 45
+ 30/210/657 20 09
Faksas: + 30/210/653 62 79
+ 30/210/657 76 12

PRANCŪZIJA
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telefonas: + 33/1/71 75 81 77
Faksas: + 33/1/71 75 82 00

ITALIJA
Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
I-00187 Roma
Telefonas: + 39/06/611 742 66
Faksas: + 39/06/488 52 73

LATVIJA
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Telefonas: +371/6702 54 18
Faksas: +371/6702 54 54
El. paštas: ndi@sab.gov.lv

KIPRAS
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: + 357/22/80 75 69, + 357/22/80 76 43, + 357/22/80 77 64
Τηλεομοιότυπο: + 357/22/30 23 51

Ministry of Defence
Minister‘s Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
CY-1432 Nicosia
Telefonas: + 357/22/80 75 69, + 357/22/80 76 43, +357 /22/80 77 64
Faksas: + 357/22/30 23 51
El. paštas: cynsa@mod.gov.cy

LIETUVA
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)
Gedimino pr. 40/1
LT-01110 Vilnius
Telefonai: +370 52663201, +370 5266 32 02
Faksas + 370 52663200
El. paštas nsa@vsd.lt

LIUKSEMBURGAS
Autorité nationale de Sécurité
Boîte postale 2379
L-1023 Luxembourg
Telefonas: + 352/2478 22 10 centrinis
+ 352/2478 22 53 tiesioginis
Faksas: + 352/2478 22 43

NYDERLANDAI
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
NL-2500 EA Den Haag
Telefonas: + 31/70/320 44 00
Faksas: + 31/70/320 07 33
Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
NL-2500 ES Den Haag
Telefonas: + 31/70/318 70 60
Faksas: + 31/70/318 75 22

VENGRIJA
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
HU-1357 Budapest
Telefonas: + 361/346 96 52
Faksas: + 361/346 96 58
El. paštas: nbf@nbf.hu
Tinklavietė: www.nbf.hu

MALTA
Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta
Telefonas: + 356/21 24 98 44
Faksas: + 356/25 69 53 21

AUSTRIJA
Informationssicherheitskommission Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telefonas: + 43/1/531 15 25 94
Faksas: + 43/1/531 15 26 15
El. paštas: ISK@bka.gv.at

LENKIJA
Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2A Rakowiecka St.
PL-00-993 Warszawa
Telefonas: + 48/22/585 73 60
Faksas: + 48/22/585 85 09
El. paštas: nsa@abw.gov.pl
Tinklavietė: www.abw.gov.pl

Służba Kontrwywiadu Wojskowego
(Military Counter-Intelligence Service)
Classified Information Protection Bureau
Oczki 1
PL-02-007 Warszawa
Telefonas: + 48/22/684 12 47
Faksas: + 48/22/684 10 76
El. paštas: skw@skw.gov.pl

RUMUNIJA
Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS National Registry Office for Classified Information)
4 Mures Street
RO-012275 Bucharest
Telefonas: + 40/21/ 224 58 30
Faksas: + 40/21/ 224 07 14
El. paštas: nsa.romania@nsa.ro
Tinklavietė: www.orniss.ro

PORTUGALIJA
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
P-1300-342 Lisboa
Telefonas: +351/ 213 031 710
Faksas: +351/ 213 031 711

SLOVĖNIJA
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SVN-1000 Ljubljana
Telefonas: + 386/1/478 13 90
Faksas: + 386/1/478 13 99

SLOVAKIJA
Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
SVK-850 07 Bratislava
Telefonas: + 421/2/68 69 23 14
Faksas: + 421/2/63 82 40 05
Tinklavietė: www.nbusr.sk

ŠVEDIJA
Utrikesdepartementet
(Ministry of Foreign Affairs)
SSSB
S-103 39 Stockholm
Telefonas: + 46/8/405 10 00
Faksas: + 46/8/723 11 76
El. paštas: ud-nsa@foreign.ministry.se

SUOMIJA
National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Telefonas 1: + 358/9/160 56487
Telefonas 2: +358/9/160 56484
Faksas: + 358/9/160 55140
El. paštas: NSA@formin.fi

JUNGTINĖ KARALYSTĖ
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Telefonas 1: + 44/20/7276 5649
Telefonas 2: + 44/20/7276 5497
Faksas: + 44/20/7276 5651
El. paštas: UK-NSA@cabinet-office.x.gsi.gov.uk

D priedėlis

SANTRUMPŲ SĄRAŠAS

Santrumpa	Reikšmė
APP	Asmens patikimumo pažymėjimas
APPPP	Asmens patikimumo pažymėjimą patvirtinanti pažyma
AVSS	Apsauginės vaizdo stebėjimo sistemos
BSGP	Bendra saugumo ir gynybos politika
BUSP	Bendra užsienio ir saugumo politika
COREPER	Nuolatinių atstovų komitetas
EKSD	Komisijos saugumo direktoratas
ESĮI	ES įslaptinta informacija
ESSĮ	ES specialusis įgaliotinis
ĮAS	Įsibrovimo aptikimo sistemos
ĮPPP	Įmonės patikimumą patvirtinantis pažymėjimas
ISU	Informacijos saugumo užtikrinimas
ISUI	ISU institucija
IT	Informacinės technologijos
KPI	Kriptografijos patvirtinimo institucijos
KPI	Kriptografijos platinimo institucija
NSI	Nacionalinė saugumo institucija
PSI	Paskirtoji saugumo institucija
PSI	Programos / projekto saugumo instrukcijos
RAP	Ribų apsaugos priemonės
RIS	Ryšių ir informacinės sistemos, kuriose tvarkoma ESĮI
SAI	Saugumo akreditavimo institucija
SAP	Saugumo aspektų paaiškinimai
SAV	Jungtinė saugumo akreditacijos valdyba
SecOPs	Saugumo įgyvendinimo patikrinimo dokumentai ir saugios eksploatacijos taisyklės
SSRA	Sistemos saugumo reikmių aktai
SŽV	Slaptumo žymų vadovas
TEI	TEMPEST institucija
TGS	Tarybos generalinis sekretoriatas
TKI	Tinkamos kvalifikacijos institucija

7.1. PAGRINDINIŲ NATO NORMINIŲ TEISĖS AKTŲ, REGLAMENTUOJANČIŲ ĮSLAPTINTOS INFORMACIJOS APSAUGĄ, SĄRAŠAS

Eil. Nr.	Dokumento numeris	Data	Dokumento pavadinimas
1.	C-M(2002)49*	17 June 2002	Security Within the North Atlantic Treaty Organisation Corrigendum 1 dated 9 January 2004 Corrigendum 2 dated 11 May 2005 Corrigendum 3 dated 5 December 2006 Corrigendum 4 dated 5 December 2006 Corrigendum 5 dated 3 July 2007 Corrigendum 6 dated 9 December 2008 Corrigendum 7 dated 19 August 2009 Corrigendum 8 dated 9 April 2010 Corrigendum 9 dated 5 February 2013
2.	C-M(2002)60	11 July 2002	The Management of Non-Classified Information
3.	C-M (64)39 – Second Issue	31 March 2010	Agreement Between the Parties to the North Atlantic Treaty for Cooperation Regarding Atomic Information
4.	C-M(2007)0118	11 December 2007	NATO Information Management Policy
5.	C-M(2008)0113 (INV)	27 November 2008	The Primary Directive on Information Management
6.	C-M(2008)0116 (INV)	12 November 2008	Public Disclosure of NATO Information – Policy and Directive

7.	C-M(2009)0021 (INV)	6 February 2009	Policy on the Retention and Disposition of NATO Information
8.	C-M(2011)0043	17 June 2011	NATO Records Policy
9.	AC/35-D/2000-REV7**	7 January 2013	Directive on Personnel Security
10.	AC/35-D/2001-REV2	7 January 2008	Directive on Physical Security
11.	AC/35-D/2002-REV4	17 January 2012	Directive on Security Information
12.	AC/35-D/2003-REV4	8 September 2009	Directive on Industrial Security
13.	AC/35-D/2004-REV2 AC/35-D/0052-REV2	6 December 2010	Primary Directive on INFOSEC
14.	AC/35-D/2005-REV2	18 October 2010	INFOSEC Management Directive for Communication and Information Systems (CIS)

Pastabos:

* North Atlantic Council (NAC) – Council Memoranda (C-M)

** Security Commity Directives – AC/35-D/2000 series

8.1. IŠTRAUKOS IŠ LIETUVOS RESPUBLIKOS KONSTITUCINIO TEISMO 1996 M. GRUODŽIO 19 D. NUTARIMO „DĖL LIETUVOS RESPUBLIKOS VALSTYBĖS PASLAPČIŲ IR JŲ APSAUGOS ĮSTATYMO 5 IR 10 STRAIPSNIŲ ATITIKIMO LIETUVOS RESPUBLIKOS KONSTITUCIJAI, TAIP PAT DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 1996 M. KOVO 6 D. NUTARIMŲ NR. 309 IR NR. 310 ATITIKIMO LIETUVOS RESPUBLIKOS KONSTITUCIJAI IR LIETUVOS RESPUBLIKOS CIVILINIO PROCESO KODEKSO NORMOMS“

(Žin., 1996, Nr. 126-2962)

<...>
Konstitucinis Teismas
konstatuoja:

Konstitucijos 25 straipsnyje žmogui yra laiduojama įsitikinimų išraiškos ir informacijos laisvė. Šio straipsnio antrojoje dalyje nustatyta: “Žmogui neturi būti kliudoma ieškoti, gauti ir skleisti informaciją bei idėjas.”

Visuotinai pripažįstama, kad šiuolaikinėje visuomenėje informacija yra žmogaus poreikis, jo žinojimo matas. Ji šalina nežinojimą, daro žmogaus elgesį prasmingą. Žmogaus teisių ir laisvių įgyvendinimas yra tiesiogiai susijęs su žmogaus galimybe gauti iš įvairių šaltinių informaciją ir ja naudotis. Tai yra vienas iš pliuralistinės demokratijos laimėjimų, užtikrinančių visuomenės raidą.

Kartu pažymėtina, kad žmogaus teisė ieškoti informacijos, ją gauti ir skleisti nėra absoliuti. Teisės į informaciją apribojimus lemia šios konstitucinės vertybės santykis su kitomis teisinėmis vertybėmis, išreiškiančiomis kitų asmenų teises ir laisves bei visuomenės būtinus poreikius. Vienas tokių poreikių – būtinybė visuomenės ar individo interesų labui apsaugoti tam tikras žinias. Tai yra valstybės, komercinės, profesinės, technologijos paslaptys ar žinios apie žmogaus privatų gyvenimą. Valstybė ypač svarbias karines, ekonomines, politines ar kitokias žinias, kurių atskleidimas ar praradimas gali pakenkti nacionaliniams interesams, skelbia esant valstybės paslaptis. Siekiant užkirsti kelią tokių žinių pagarsinimui, įstatymu nustatoma jų apsauga, apribojamas naudojimasis jomis. Tačiau bendrų interesų apsauga demokratinėje valstybėje negali paneigti žmogaus teisės į informaciją apskritai. Šios problemos sprendimą žmogaus teisių ir laisvių doktrina ir ja besiremianti tarptautinė ir nacionalinė teisė sieja

su teisinių vertybių racionaliu santykiu, laiduojančiu, kad apribojimais nebus pažeista atitinkamos žmogaus teisės esmė. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 10 straipsnis, laiduojantis žmogui teisę laisvai laikytis savo nuomonės, gauti ir skleisti informaciją bei idėjas, numato galimybę riboti šią teisę laikantis šių sąlygų: 1) jeigu tai būtina demokratinėje visuomenėje, 2) numatyta nacionaliniuose įstatymuose ir 3) apribojimais siekiama ginti tokias vertybes kaip valstybės saugumas, teritorijos vientisumas, viešosios tvarkos interesai, kelio teisės pažeidimams ir nusikaltimams užkirtimas, žmogaus sveikatos ir moralės apsauga ir kt. Šių standartų laikosi daugelis valstybių. Konstitucijos 25 straipsnio trečiojoje ir ketvirtojoje dalyse nustatyta:

“Laisvė reikšti įsitikinimus, gauti ir skleisti informaciją negali būti ribojama kitaip, kaip tik įstatymu, jei tai būtina apsaugoti žmogaus sveikatai, garbei ir orumui, privačiam gyvenimui, dorovei ar ginti konstitucinei santvarkai.

Laisvė reikšti įsitikinimus ir skleisti informaciją nesuderinama su nusikalstamais veiksmais – tautinės, rasinės, religinės ar socialinės neapykantos, prievartos bei diskriminacijos kurstymu, šmeižtu ir dezinformacija.”

Šiomis Konstitucijos nuostatomis apibrėžti žmogaus teisės į informaciją apribojimai yra pagrindinis kriterijus teisiškai reguliuojant žinių, sudarančių valstybės paslaptį, įslaptinimo, naudojimo, išslaptinimo bei apsaugos santykius. Įstatymų leidėjas, sprendžiantis, kaip apsaugoti valstybės paslaptį sudarančias žinias, yra įpareigojamas parinkti tokias teisines priemones, kuriomis nebūtų galima nepagrįstai apriboti asmens teisės į informaciją.

Konstitucijos 145 straipsnyje taip pat yra numatyti ir išimtiniai teisės į informaciją laikino apribojimo pagrindai karo ar nepaprastosios padėties atvejais.

<...>

Iš Konstitucijos 25 straipsnio turinio aišku, kad ribojant žmogaus teises ieškoti informacijos, ją gauti ir skleisti reikia laikytis dviejų sąlygų: jas apriboti galima tik įstatymu ir tuomet, kai tai būtina Konstitucijos 25 straipsnio trečiojoje dalyje išvardytoms vertybėms apsaugoti ar ginti.

<...>

Žmogaus teisės ir laisvės yra didžiausia teisinė vertybė, todėl įstatymų leidėjas paprastai nustato tokius valstybės paslapties apsaugos būdus ir priemones, kurie nesudarytų sąlygų nepagrįstai apriboti žmogaus teisę į informaciją. Įstatymo kaip teisės šaltinio forma ir jo priėmimo būdas geriausiai laiduoja, kad konstitucinės santvarkos sąlygojami bendri interesai apsaugoti valstybės paslaptį bus suderinti su žmogaus teisės ieškoti informacijos, gauti ir skleisti ją užtikrinimu. Tiek tokios žmogaus teisės ir laisvės, tiek jas ribojančio įstatymo tarpusavio sąveikos principo laikymasis yra reikšminga žmogaus teisių ir laisvių įgyvendinimo garantija.

<...>

1. 4. Įgyvendinant piliečių teisę ieškoti informacijos, ją gauti ir skleisti ne mažiau svarbi yra Konstitucijos 25 straipsnio penktosios dalies nuostata: „Pilietis turi teisę įstatymo nustatyta tvarka gauti valstybės įstaigų turimą informaciją apie jį.“ Taip įstatymų leidėjas yra tiesiogiai įpareigojamas įstatymu nustatyti, kokia tvarka valstybės įstaigos privalo suteikti piliečiui apie jį turimas žinias.

Konstitucijos 25 straipsnio atskirų dalių normos sudaro vieningą visumą.

Šio straipsnio trečiojoje dalyje yra numatyta galimybė ginant atitinkamas konstitucines vertybes įstatymu riboti žmogaus teisę gauti informaciją. Valstybės paslapčių ir jų apsaugos įstatymas yra vienas iš tokių įstatymų. Šio įstatymo normas vertinti Konstitucijos 25 straipsnio penktosios dalies požiūriu galima tik atsižvelgus į to paties Konstitucijos straipsnio trečiosios dalies normos turinį, todėl piliečio teisė įstatymo nustatyta tvarka gauti valstybės įstaigų turimą informaciją apie jį gali būti ribojama siekiant apsaugoti valstybės paslaptį.

<...>

2.4.

<...>

Konstitucijos 29 straipsnio pirmojoje dalyje asmenų lygybė apibrėžiama nurodant, kad „įstatymui, teismui ir kitoms valstybės institucijoms ar pareigūnams visi asmenys lygūs“. Ši nuostata yra susijusi su to paties straipsnio antrosios dalies nuostatomis, nustatančiomis, kad žmogaus teisių negalima varžyti ir teikti jam privilegijų dėl jo lyties, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų pagrindu.

<...>

Minėtas universalus teisės principas civiliniame procese pasireiškia šalių procesiniu lygiateisiškumu. Šalių procesinės teisės yra lygios. Vienos šalies teisės atitinka kitos šalies teises, pvz., ieškovas turi teisę pareikšti ieškinį, atsakovas turi teisę gintis nuo pareikšto ieškinio pateikdamas atsikirtimus į ieškovo reikalavimą arba pareikšdamas priešieškinį ir t. t. Šis principas yra labai svarbus, nes tik lygiateisės ginčo šalys gali lygiais pagrindais tarpusavyje rungtis. Svarbu, kad šalių procesinio lygiateisiškumo principo būtų laikomasi visose proceso stadijose, nes nuo jo įgyvendinimo priklauso ir kitų proceso principų įgyvendinimas.

Procesiniuose santykiuose sąvoka „teismas“ vartojama bendriausia prasme, turint omenyje teismą ne vien kaip kolegialų organą, bet ir kaip teisėją. Teismas – ypatingas procesinių teisinių santykių subjektas. Kaip valstybės valdžios institucijai, jam vieninteliam yra pavesta vykdyti teisingumą. Įgyvendindamas šią funkciją, teismas veikia valstybės vardu, jis nepriklauso nuo byloje dalyvaujančių asmenų ir klauso tik įstatymo.

Taigi byloje dalyvaujančių asmenų teisinio lygiateisiškumo esmė – asmenų lygybė teismui, bet ne ginčą sprendžiančio teismo (teisėjo) ir byloje dalyvaujančių asmenų lygybė. Kitaip būtų paneigta teismo kaip teisingumą vykdančios institucijos esmė.

<...>

2.5.

<...>

Valstybės paslapties apsaugos teismo procese pagrindai yra numatyti Konstitucijos 117 straipsnyje, nustatančiame, kad teismo posėdis gali būti uždaras, jeigu viešai nagrinėjama byla gali atskleisti valstybės paslaptį. Ši konstitucinė nuostata iš esmės yra pakartota Civilinio proceso kodekso 10 straipsnyje. <...>

8.2. IŠTRAUKOS IŠ LIETUVOS RESPUBLIKOS KONSTITUCINIO TEISMO 2007 M. GEGUŽĖS 15 D. NUTARIMO „DĖL LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ BYLŲ TEISENOS ĮSTATYMO 57 STRAIPSNIO 3 DALIES (2000 M. RUGSĖJO 19 D. REDAKCIJA), LIETUVOS RESPUBLIKOS VALSTYBĖS IR TARNYBOS PASLAPČIŲ ĮSTATYMO 10 STRAIPSNIO 4 DALIES (1999 M. LAPKRIČIO 25 D. REDAKCIJA), 11 STRAIPSNIO (1999 M. LAPKRIČIO 25 D. REDAKCIJA) 1, 2 DALIŲ ATITIKTIES LIETUVOS RESPUBLIKOS KONSTITUCIJAI“

Byla Nr. 7/04-8/04

(Žin., 2007-05-17, Nr. 54-2097)

<...>

Konstitucinis Teismas

k o n s t a t u o j a:

<...>

III

1. Valstybės paslaptis – konstitucinis institutas. Sąvoka „valstybinė paslaptis“ *expressis verbis* vartojama Konstitucijoje (117 straipsnio 1 dalis). Valstybės paslaptis – tai tokia neskelbtina, neskleistina informacija, kurios atskleidimas galėtų padaryti žalos valstybei, kaip bendram visos visuomenės gėriui, visos visuomenės politinei organizacijai, kurios paskirtis – užtikrinti žmogaus teises ir laisves, garantuoti viešąjį interesą.

2. Konstitucinis Teismas savo aktuose ne kartą yra konstatavęs, kad informacijos laisvė nėra absoliuti, taip pat kad Konstitucija neleidžia nustatyti tokio teisinio reguliavimo, kuriuo, įstatymais įtvirtinus informacijos laisvės įgyvendinimo garantijas, būtų sudaromos prielaidos pažeisti kitas konstitucines vertybes, jų pusiausvyrą. Pažymėtina, kad pagal Konstituciją valstybė turi pareigą garantuoti ne tik valstybės paslaptį sudarančios informacijos slaptumą, bet ir tam tikros kitos informacijos slaptumo apsaugą, būtent tai, kad nebūtų savavališkai, neteisėtai kėsinamasi sužinoti ar paskleisti tokią informaciją, kurios atskleidimas galėtų padaryti žalos asmens teisėms ir laisvėms bei teisėtiems interesams, kitoms Konstitucijoje įtvirtintoms, jos ginamoms ir saugomoms vertybėms; antai Konstitucijos 117 straipsnio 1 dalyje, be „valstybinės paslapties“, yra nurodyta „profesinė paslaptis“, „komercinė paslaptis“, taip pat „žmogaus asmeninio ar šeimyninio gyvenimo slaptumas“; Konstitucijos 22 straipsnyje yra įvirtintas *inter alia* asmens privataus gyvenimo, susirašinėjimo, pokalbių telefonu, telegrafo pranešimų ir kitokio susižinojimo neliečiamumas, taip pat draudimas rinkti informaciją apie privatų asmens gyvenimą kitaip nei tik motyvuotu

teismo sprendimu ir tik pagal įstatymą; įvairiuose Konstitucijos straipsniuose (jų dalyse) yra įtvirtintas balsavimo rinkimuose slaptumo principas; pažymėtina, kad ne visa šitaip saugotina informacija yra eksplicitiškai paminėta Konstitucijos tekste. Konstitucinis Teismas yra konstatavęs, kad įstatymų leidėjas turi įstatymu apibrėžti informacijos, kurią skleisti yra draudžiama arba kurios skleidimas yra ribojamas, turinį, taip pat būdus, kuriais tam tikros informacijos neleidžiama skleisti, bei kitas atitinkamos informacijos skleidimo sąlygas, jeigu tai bent kaip riboja informacijos laisvę; jis taip pat turi įstatymu nustatyti: atsakomybę už minėtų draudimų ir ribojimų nepaisymą, įskaitant atsakomybę už informacijos, kurią skleisti draudžiama, skleidimą; subjektus, turinčius įgaliojimus prižiūrėti, kaip laikomasi įstatymų nustatytų draudimų ir (arba) ribojimų skleisti tam tikrą informaciją; subjektus, taikančius atsakomybę už įstatymų nustatytų draudimų ir (arba) ribojimų skleisti tam tikrą informaciją nepaisymą; veiksmingas informacijos laisvės teisminio gynimo priemones; Konstitucija neužkerta kelio kai kurių su informacijos gavimu ir skleidimu susijusių santykių, įskaitant ir santykius, susijusius su įstatymų nustatytų draudimų skleisti informaciją ir (arba) informacijos skleidimo ribojimų laikymosi priežiūra ir kontrole, reguliuoti ir poįstatyminiais teisės aktais, *inter alia* Vyriausybės nutarimais, bet tais poįstatyminiais teisės aktais negalima nustatyti tokio teisinio reguliavimo, kuris nebūtų grindžiamas Konstitucija ir įstatymais, taip pat tokio teisinio reguliavimo, kuris konkuruotų su įstatymų nustatytuoju (Konstitucinio Teismo 2005 m. rugsėjo 19 d. nutarimas).

3. Konstitucinis Teismas savo aktuose ne kartą yra konstatavęs ir tai, kad Konstitucijos negalima aiškinti vien pažodžiui, vien taikant lingvistinį (verbalinį) metodą; tas pats pasakytina ir apie visų žemesnės galios teisės aktų aiškinimą. Konstitucinio Teismo 2006 m. sausio 16 d., 2006 m. rugpjūčio 19 d. nutarimuose yra konstatuota, kad Konstitucija neužkerta kelio įstatymuose, kituose teisės aktuose tiems patiems reiškiniams apibūdinti vartoti kitus žodžius ar formuluotes negu vartojami Konstitucijos tekste.

4. Sistemiškai aiškinant įvairias Konstitucijos nuostatas, iš kurių valstybei kyla pareiga garantuoti valstybės paslaptį sudarančios informacijos slaptumo apsaugą, taip pat užtikrinti, kad nebūtų savavališkai, neteisėtai kėsinamasi sužinoti ar paskleisti tokią informaciją, kurios atskleidimas galėtų padaryti žalos asmens teisėms ir laisvėms bei teisėtiems interesams, kitoms Konstitucijoje įtvirtintoms, jos ginamoms ir saugomoms vertybėms, konstatuotina, kad konstitucinė sąvoka „valstybinė paslaptis“ yra bendrinė. Įstatymų leidėjas, įstatymu apibrėždamas informacijos, kurią skleisti yra draudžiama arba kurios skleidimas yra ribojamas, turinį, taip pat būdus, kuriais tam tikros informacijos neleidžiama skleisti, bei kitas atitinkamos informacijos skleidimo sąlygas (jeigu tai riboja informacijos laisvę), gali vartoti ir kitokias sąvokas (*inter alia* įvairioms konstituciškai saugomų paslapčių rūšims (kategorijoms) įvardyti); jis taip pat gali sąvoką „valstybės paslaptis“ vartoti ir kitokia – ne bendrine (kaip Konstitucijos tekste), bet siauresne – prasme.

Tačiau visais atvejais būtina paisyti valstybės paslapties, kaip neskelbtinos, neatskleistinos informacijos, kurios atskleidimas padarytų žalos valstybei, kaip bendram visos visuomenės gėriui, visos visuomenės politinei organizacijai, tu-

rinčiai užtikrinti žmogaus teises ir laisves, garantuoti viešąjį interesą, konstitucinės sampratos.

5. Asmeniui, kuriam suteikiama teisė susipažinti su valstybės paslaptį sudarančia informacija, keliami tam tikri reikalavimai, susiję su jo patikimumu bei lojalumu Lietuvos valstybei, kurie yra sietini su valstybės pasitikėjimu tuo asmeniu; valstybės nepasitikėjimą tam tikru asmeniu gali lemti paties to asmens veikla, *inter alia* padaryti teisės pažeidimai, taip pat to asmens savybės, ryšiai, kitos svarbios aplinkybės; su valstybės paslaptimis gali būti leidžiama susipažinti tik tokiam asmeniui, kurio veikla, savybės, ryšiai ir kt. negali duoti pagrindo nuogąstauti, kad, jam sužinojus valstybės paslaptį, kils grėsmė, juo labiau bus padaryta žalos valstybės suverenitetui, teritorijos vientisumui, konstitucinei santvarkai, gynybinei galiai, kitiems itin svarbiems valstybės interesams, visuomenės ir valstybės gyvenimo pagrindams, bus pažeisti svarbiausi Konstitucijos reguliuojami, ginami ir saugomi santykiai, kuriuos kaip tik ir turi padėti apsaugoti ir apginti tai, kad tam tikra informacija pagal įstatymus yra įslaptinama; asmeniui, praradusiam valstybės pasitikėjimą, teisė susipažinti ar dirbti su informacija, sudarančia valstybės paslaptį, turi būti atimama.

6. Valstybės paslapties atskleidimas gali sukelti grėsmę ar net padaryti žalos valstybės suverenitetui, teritorijos vientisumui, konstitucinei santvarkai, gynybinei galiai, kitiems itin svarbiems valstybės interesams, visuomenės ir valstybės gyvenimo pagrindams; jeigu valstybės paslaptį sudarančios informacijos atskleidimui (sužinojimui, paskleidimui) nebūtų užkertama kelio, jeigu toks atskleidimas nebūtų teisiškai persekiojamas, būtų sudarytos prielaidos pažeisti net svarbiausius Konstitucijos reguliuojamus, ginamus ir saugomus santykius, taigi tam tikro asmens ar asmenų interesą žinoti ar skleisti tam tikrą informaciją iškelti aukščiau viešojo intereso.

Šiame kontekste paminėtina, kad viešojo intereso „įtvirtinimas ir užtikrinimas, gynimas ir apsauga yra konstituciškai motyvuoti“, nes kiekvienas viešasis interesas „atspindi ir išreiškia pamatines visuomenės vertybes, kurias įtvirtina, saugo ir gina Konstitucija“, tokias kaip visuomenės atvirumas ir darna, teisingumas, asmens teisės ir laisvės, teisės viešpatavimas ir kt. (Konstitucinio Teismo 2006 m. rugsėjo 21 d. nutarimas); viešojo intereso, kaip valstybės pripažinto ir teisės ginamo visuomeninio intereso, įgyvendinimas – viena svarbiausių pačios visuomenės egzistavimo ir raidos sąlygų (Konstitucinio Teismo 1997 m. gegužės 6 d., 2005 m. gegužės 13 d., 2006 m. rugsėjo 21 d. nutarimai). Garantuoti viešąjį interesą – valstybės priedermė.

Konstitucinis Teismas yra konstatavęs ir tai, kad individo autonominiai interesai ir viešasis interesas negali būti priešpriešinami, juos būtina derinti (nes ir asmens teisės, ir viešasis interesas yra konstitucinės vertybės), čia turi būti užtikrinta teisinga pusiausvyra (Konstitucinio Teismo 1997 m. gegužės 6 d., 2004 m. gruodžio 13 d., 2006 m. rugsėjo 21 d. nutarimai).

7. Įstatymais reguliuojant su valstybės paslaptimis (ar kita įslaptinta informacija) ir jų apsauga susijusius santykius, privalu nustatyti ne tik tai, kokia informacija yra valstybės paslaptis (ar sudaro kitą įslaptintą informaciją) ir kokia yra atsakomybė už jos atskleidimą, bet ir tai, kokie asmenys, kokia tvarka ir kokiomis sąlygomis gali disponuoti (taip pat netekti teisės disponuoti) valstybės

paslaptimis (ar kita įslaptinta informacija), taip pat tai, kokiais atvejais, kokia tvarka bei kokiomis sąlygomis valstybės paslaptį sudaranti (ar kita įslaptinta) informacija gali būti išslaptinta ir kas turi įgaliojimus tai padaryti. Šie asmenys, tvarka ir sąlygos gali būti diferencijuojama *inter alia* pagal įstatymų leidėjo nustatytas valstybės paslapčių (ar kitos įslaptintos informacijos) rūšis (kategorijas).

8. Atskleidžiant konstitucinio valstybės paslapties instituto turinį taip pat pažymėtina, kad konstitucinė priedermė saugoti valstybės paslaptis (ar kitą įslaptintą informaciją) kyla ir iš Seimo ratifikuotų tarptautinių sutarčių, kurios yra sudedamoji Lietuvos Respublikos teisinės sistemos dalis (Konstitucijos 138 straipsnio 3 dalis), kurių laikytis yra Lietuvos valstybės konstitucinis įsipareigojimas ir kurios, kaip savo 2006 m. kovo 14 d. nutarime yra konstatavęs Konstitucinis Teismas, pagal Konstituciją turi būti taikomos tada, kai nacionalinės teisės aktas nustato teisinį reguliavimą, konkuruojantį su nustatytuoju tarptautinėje sutartyje, *inter alia* tarptautinėse sutartyse, kuriomis grindžiama Lietuvos Respublikos narystė tarptautinėse organizacijose (kuriose ji gali dalyvauti, jeigu tai neprieštarauja jos interesams ir nepriklausomybei (Konstitucijos 136 straipsnis)). Seimo ratifikuotos tarptautinės sutartys, taip pat jomis grindžiama Lietuvos Respublikos narystė tarptautinėse organizacijose suponuoja tai, kad Lietuvos Respublika (jos institucijos, pareigūnai) gali disponuoti ir kitoms valstybėms ar tarptautinėms organizacijoms priklausančiomis paslaptimis. Neabejotina, kad konstitucinė priedermė saugoti valstybės paslaptis (kitą įslaptintą informaciją) apima ir priedermę saugoti kitoms valstybėms ar tarptautinėms organizacijoms priklausančias paslaptis, kuriomis disponuoja Lietuvos Respublika (jos institucijos, pareigūnai). Šiame kontekste paminėtina, kad, vadovaujantis Seimo 2004 m. kovo 10 d. ratifikuotos Šiaurės Atlanto Sutarties 3 straipsniu ir siekiant įgyvendinti jame nustatytus NATO narių įsipareigojimus bendradarbiauti plėtojant kolektyvinį pajėgumą atremti ginkluotą užpuolimą, buvo sudarytos NATO valstybių narių daugiašalės tarptautinės sutartys, nustatančios įslaptintos informacijos apsaugos standartus, būtinus NATO veiklai užtikrinti; jų nuostatos detalizuojamos, turinys aiškinamas NATO institucijų dokumentuose. Seimo 2004 m. liepos 15 d. priimto Lietuvos Respublikos įstatymo dėl Šiaurės Atlanto Sutarties šalių susitarimo dėl informacijos saugumo, NATO susitarimo dėl su gynyba susijusių išradimų, dėl kurių paduotos patento paraiškos, abipusės slaptumo apsaugos bei NATO susitarimo dėl techninės informacijos perdavimo gynybos tikslais ratifikavimo 1 straipsniu buvo ratifikuoti Šiaurės Atlanto Sutarties šalių susitarimas dėl informacijos saugumo, sudarytas 1997 m. kovo 6 d. Briuselyje, NATO susitarimas dėl su gynyba susijusių išradimų, dėl kurių paduotos patento paraiškos, abipusės slaptumo apsaugos, sudarytas 1960 m. rugsėjo 21 d. Paryžiuje, ir NATO susitarimas dėl techninės informacijos perdavimo gynybos tikslais, sudarytas 1970 m. spalio 19 d. Briuselyje, o pagal šio įstatymo 3 straipsnio 2 dalį minėtos tarptautinės sutartys Lietuvos Respublikoje turi būti įgyvendinamos laikantis Šiaurės Atlanto Tarybos sprendimais nustatomų saugumo standartų ir kitų šių susitarimų įgyvendinimo tvarkos bei taikymo reikalavimų. Šiaurės Atlanto Tarybos sprendimai, sukonkretinantys įslaptintos informacijos apsaugos standartus, Lietuvos Respublikai yra privalomi.

Visa tai *mutatis mutandis* taikytina ir kitoms valstybėms ar tarptautinėms

organizacijoms priklausančioms paslaptims, kuriomis Lietuvos Respublika (jos institucijos, pareigūnai) gali disponuoti pagal Lietuvos Respublikos tarptautines sutartis, kurių Seimas pagal Konstituciją ir įstatymus neprivalo ratifikuoti, taip pat pagal valstybės institucijų sudarytus tarptautinius susitarimus.

9. Pagal Konstitucijos 30 straipsnio 1 dalį asmuo, kurio konstitucinės teisės ar laisvės pažeidžiamos, turi teisę kreiptis į teismą. Konstitucinis Teismas savo aktuose ne kartą yra konstatavęs: iš konstitucinio teisinės valstybės principo kyla imperatyvas, kad asmuo, manantis, jog jo teisės ar laisvės yra pažeistos, turi absoliučią teisę į nepriklausomą ir nešališką teismą; ši teisė negali būti dirbtinai suvaržoma arba negali būti dirbtinai pasunkinama ją įgyvendinti; šios teisės negalima paneigti; asmeniui jo pažeistų teisių gynyba teisme garantuojama nepriklausomai nuo jo teisinio statuso; pagal Konstituciją įstatymų leidėjas turi pareigą nustatyti tokį teisinį reguliavimą, kad visus ginčus dėl asmens teisių ar laisvių pažeidimo būtų galima spręsti teisme; asmens pažeistos teisės, *inter alia* įgytosios teisės, ir teisėti interesai turi būti ginami nepriklausomai nuo to, ar jie tiesiogiai įtvirtinti Konstitucijoje; asmens teisės turi būti ne formaliai, o realiai ir veiksmingai ginamos tiek nuo privačių asmenų, tiek nuo valdžios institucijų ar pareigūnų neteisėtų veiksmų; teisinis reguliavimas, įtvirtinantis asmens teisės į savo teisių ir laisvių teisminę gynybą įgyvendinimo tvarką, turi atitikti konstitucinį teisinio aiškumo reikalavimą; įstatymų leidėjas privalo įstatymuose aiškiai nustatyti, kaip ir į kokį teismą asmuo gali kreiptis, kad iš tikrųjų galėtų įgyvendinti savo teisę kreiptis į teismą dėl savo teisių ir laisvių pažeidimo.

10. Atskleidžiant konstitucinio valstybės paslapties instituto turinį pažymėtina ir tai, kad Konstitucijoje yra įtvirtinti neskelbtinos informacijos, *inter alia* valstybės paslapties, apsaugos teismams nagrinėjant ir sprendžiant bylas pagrindai: Konstitucijos 117 straipsnio 1 dalyje nustatyta, kad „visuose teismuose bylos nagrinėjamos viešai“, kad „teismo posėdis gali būti uždaras – žmogaus asmeninio ar šeimyninio gyvenimo slaptumui apsaugoti, taip pat jeigu viešai nagrinėjama byla gali atskleisti valstybinę, profesinę ar komercinę paslaptį“. Taigi konstitucinis viešo bylų nagrinėjimo teisme principas nėra absoliutus, be išimčių, *inter alia* tuo atžvilgiu, kad teismo posėdis gali būti uždaras, jeigu viešumas keltų grėsmę, jog gali būti atskleista valstybės paslaptis.

Iš Konstitucijos 109 straipsnio 1 dalies, pagal kurią teisingumą Lietuvos Respublikoje vykdo tik teismai, teismams kyla pareiga teisingai ir objektyviai išnagrinėti bylas, priimti motyvuotus ir pagrįstus sprendimus, todėl negali būti tokios teisinės situacijos, kad teismas, nagrinėdamas bylą, negalėtų susipažinti su byloje esančia valstybės paslaptį sudarančia (ar kita įslaptinta) informacija. Konstitucinis Teismas 1996 m. gruodžio 19 d. nutarime konstatavo, kad „teisėjo, nagrinėjančio bylą, teisė susipažinti su valstybės paslaptimi pagrindžiama Konstitucijos 109 straipsniu <…> ir 117 straipsniu <…>“, taip pat kad „teisėjo teisę susipažinti su bylos nagrinėjimui reikalingomis žiniomis, sudarančiomis valstybės paslaptį“, nulemia „ne teisėjo pareigų įrašymas į tam tikrų pareigų sąrašą, bet teismo kaip valstybės institucijos funkcija vykdyti teisingumą“.

11. Teismo nagrinėjamos bylos šalių galimybės susipažinti su informacija, sudarančia valstybės paslaptį (taip pat kita įslaptinta informacija), jeigu teismas nusprendžia, kad ta informacija gali būti įrodymas atitinkamoje byloje, turi būti

apibrėžtos įstatymais; turi būti nustatytas toks teisinis reguliavimas, kad būtų galima sudaryti sąlygas teismui nagrinėjant bylą apsaugoti valstybės paslaptis (taip pat kitą įslaptintą informaciją) nuo atskleidimo, kuris galėtų pakenkti Konstitucijos saugomam viešajam interesui.

Minėta, kad individo autonominiai interesai ir viešasis interesas negali būti priešpriešinami, juos būtina derinti. Šiame kontekste paminėtina, kad, kaip 2006 m. rugsėjo 21 d. nutarime yra konstatavęs Konstitucinis Teismas, kiekvienąkart, kai teismui nagrinėjant bylą „kyla klausimas, ar tam tikras interesas laikytinas viešuoju, turi būti įmanoma pagrįsti, kad, nepatenkinus tam tikro asmens ar grupės asmenų intereso, būtų pažeistos ir tam tikros Konstitucijoje įtvirtintos, jos saugomos ir ginamos vertybės. O tais atvejais, kai sprendimą, ar tam tikras interesas turi būti laikomas viešuoju ir ginamas bei saugomas kaip viešasis interesas, turi priimti bylą sprendžiantis teismas, būtina tai motyvuoti atitinkamame teismo akte. Priešingu atveju kiltų pagrįsta abejonė, kad tai, kas teismo yra ginama ir saugoma kaip viešasis interesas, iš tikrųjų yra ne viešasis, bet privatus tam tikro asmens interesas“. Minėtame Konstitucinio Teismo nutarime taip pat konstatuota, kad „pagal Konstituciją negalima nustatyti tokio teisinio reguliavimo, kad viešojo intereso negalėtų apginti teismas, į kurį buvo kreiptasi, taip pat kad teismas, spręsdamas bylą, būtų priverstas priimti tokį sprendimą, kuriuo pačiu būtų pažeidžiamas viešasis interesas, vadinasi, ir kuri nors Konstitucijoje įtvirtinta, jos ginama ir saugoma vertybė (*inter alia* asmens teisė ar laisvė). Jeigu teismas priimtų tokį sprendimą, tas sprendimas nebūtų teisingas. Tai reikštų, kad teismas Lietuvos Respublikos vardu įvykdė ne tokį teisingumą, kokį įtvirtina Konstitucija, taigi pagal Konstituciją – ne teisingumą. Šitaip būtų paneigta ir teismo, kaip Lietuvos Respublikos vardu teisingumą vykdančios institucijos, konstitucinė samprata“.

Atsižvelgiant į tai, kad, viena vertus, būtinybė apsaugoti valstybės paslaptį sudarančią (ar kitą įslaptintą) informaciją yra viešasis interesas, ir, kita vertus, turi būti užtikrinta asmens teisė į teisminę gynybą, įstatymu turi būti nustatyta, kokiais pagrindais, tvarka bei sąlygomis su valstybės paslaptį sudarančia (ar kita įslaptinta) informacija, jeigu teismas nusprendžia, kad ta informacija gali būti įrodymas atitinkamoje byloje, gali būti susipažįstama teismui nagrinėjant bylą, taip pat nustatytas toks atitinkamų procesinių veiksmų teisinis reguliavimas, kad būtų galima užtikrinti konstitucinio proporcingumo principo laikymąsi, išlaikyti pusiausvyrą tarp minėtų dviejų konstitucinių vertybių – valstybės paslapties (ar kitos įslaptintos informacijos) apsaugos, kaip viešojo intereso, ir asmens teisių ir laisvių, kurias jis gina teisme. Turi būti nustatytas toks teisinis reguliavimas, kad teismas teisingumą galėtų įvykdyti nepaneigdamas nė vienos iš šių vertybių.

Vadinasi, įstatymu turi būti nustatytas toks teisinis reguliavimas, kad, viena vertus, bylos šalis galėtų prašyti tam tikrą informaciją, sudarančią valstybės paslaptį (ar kitą įslaptintą informaciją), pripažinti įrodymu atitinkamoje byloje (jeigu ji, tos šalies manymu, turi įrodomąją vertę), kita vertus, teismas kiekvienąkart turi spręsti, ar toks prašymas yra pagrįstas ir ar jis pagal įstatymą yra tenkintinas (visas ar iš dalies), ar jį patenkinus (visą ar iš dalies) nebus pakenkta viešajam interesui (užtikrinti valstybės paslapties (kitos įslaptintos in-

formacijos) apsaugą), Konstitucijoje įtvirtintoms, jos ginamoms ir saugomoms vertybėms, *inter alia* kitų asmenų teisėms ir laisvėms, Lietuvos Respublikos tarptautiniams įsipareigojimams. Minėta bylos šalies teisė prašyti valstybės paslaptį sudarančią (ar kitą įslaptintą) informaciją pripažinti įrodymu atitinkamoje byloje savaime nesuponuoja, kad teismas turi tokį prašymą tenkinti (visą ar iš dalies), taigi ir kad šalis turi būti supažindinta su valstybės paslaptį sudarančia (ar kita įslaptinta) informacija; tai, ar tam tikra valstybės paslaptį sudaranti (ar kita įslaptinta) informacija gali būti įrodymas atitinkamoje byloje, priklauso nuo daugelio veiksnių, į kuriuos teismas privalo atsižvelgti. Šiame kontekste paminėtina, kad, kaip yra konstatavęs Konstitucinis Teismas, viešasis interesas yra dinamiškas, kintantis (Konstitucinio Teismo 2005 m. liepos 8 d., 2006 m. rugsėjo 21 d. nutarimai); jis yra labai įvairus, todėl iš esmės neįmanoma *a priori* pasakyti, kokiose gyvenimo srityse, dėl kurių gali kilti teisinių ginčų arba kuriose gali prireikti taikyti teisę, viešajam interesui (*inter alia* apsaugoti paslaptis, kurias privalu apsaugoti pagal Lietuvos Respublikos tarptautinius įsipareigojimus) gali atsirasti grėsmių arba gali prireikti viešąjį interesą užtikrinti įsikišant viešosios valdžios institucijoms ar pareigūnams. Taigi negalima *a priori* apibrėžti (išvardyti) ir visų atvejų, kada informacija, sudaranti valstybės paslaptį (ar kita įslaptinta informacija), teismo sprendimu negali būti įrodymas, taigi ir bylos šalys su tokia informacija negali būti supažindinamos. Tačiau akivaizdu, kad jeigu sprendimui teismo nagrinėjamoje byloje priimti ir tokiam teisingumui, kokį įtvirtina Konstitucija, įvykdyti teismui pakanka tokių įrodymų (medžiagos), kurie nėra valstybės paslaptį sudaranti (ar kita įslaptinta) informacija, ši neatskleistina informacija, saugant viešąjį interesą, neturi būti įrodymas toje byloje ir bylos šalys su ja negali būti supažindinamos.

Pabrėžtina, kad bylą nagrinėjančiam teismui visada kyla ypatinga atsakomybė, kai jis sprendžia, ar tam tikra valstybės paslaptį sudaranti (ar kita įslaptinta) informacija gali būti įrodymas atitinkamoje byloje.

Nagrinėjamos konstitucinės justicijos bylos kontekste pažymėtina ir tai, kad valstybės institucijoms sprendžiant, ar asmuo turi teisę dirbti ar susipažinti su valstybės paslaptį sudarančia (ar kita įslaptinta) informacija, būtina paisyti imperatyvo, jog tam, kad asmuo turėtų tokią teisę, valstybė turi besąlygiškai pasitikėti juo, taigi ir kad asmeniui, praradusiam valstybės pasitikėjimą, minėta teisė turi būti atimama.

12. Kartu pabrėžtina, kad joks teismo sprendimas negali būti grindžiamas šalims (vienai iš jų) nežinoma vien valstybės paslaptį sudarančia (ar kita įslaptinta) informacija.

13. Pabrėžtina ir tai, kad teismų sprendimai, *inter alia* sprendimai, kad tam tikra valstybės paslaptį sudaranti (ar kita įslaptinta) informacija nėra įrodymas atitinkamoje byloje, gali būti skundžiami įstatymų nustatyta tvarka.

14. Pažymėtina, kad aptartųjų santykių teisinis reguliavimas gali turėti ypatumų, kuriuos lemia tai, ar bylos nagrinėjamos baudžiamojo proceso, ar civilinio proceso, ar administracinio proceso tvarka.

15. Nagrinėjamos konstitucinės justicijos bylos kontekste paminėtina ir tai, kad toks bylos šalies teisės susipažinti su įslaptinta informacija aiškinimas būdingas ir tarptautinių teismų jurisprudencijai.

Antai Europos Žmogaus Teisių Teismo 2004 m. spalio 27 d. sprendime byloje *Edwards ir Lewis prieš Jungtinę Karalystę* (*Cour eur. D. H., arrźt Edwards et Lewis c. Royaume-Uni du 27 octobre 2004, n^{os} 39647/98 et 40461/98*) konstatuota, kad teisė į atitinkamų įrodymų atskleidimą nėra absoliuti teisė; bet kuriame baudžiamajame teismo procese gali atsirasti konkuruojančių interesų, tokių kaip nacionalinis saugumas arba būtinumas apsaugoti liudytojus, kuriems gresia atsakomieji veiksmai, arba neatskleisti policijos taikomų slaptų nusikaltimo tyrimo metodų, kurie gali nusverti kaltinamojo teises; kai kuriais atvejais gali būti būtina neleisti gynybai susipažinti su tam tikrais įrodymais siekiant apsaugoti pagrindines kito asmens teises arba apginti svarbų viešąjį interesą; leistinos tik tokios priemonės, ribojančios gynybos teises, kurios yra neišvengiamai būtinos; kad kaltinamajam būtų užtikrintas nešališkas, teisingas teismo procesas, bet kokie sunkumai, gynybai sukelti ribojant jos teises, privalo būti pakankamai atsverti teismo proceso tvarka, kurios laikytųsi teisminė valdžia.

Europos Bendrijų Pirmosios instancijos teismo 2005 m. balandžio 26 d. sprendime sujungtose bylose T-110/03, T-150/03 ir T-405/03 *Jose Maria Sison prieš Europos Sąjungos Tarybą (arrźt du Tribunal de priemičre instance du 26 avril 2005, Jose Maria Sison/Conseil de l'Union européenne, affaires jointes T-110/03, T-150/03 et T-405/03, Rec. p. II-1429)* konstatuota, jog kovos su terorizmu veiksmingumas suponuoja, kad valdžios institucijų turima informacija apie terorizmu įtariamus asmenis ar subjektus turi būti laikoma slapta, idant ši informacija išliktų svarbi ir leistų imtis efektyvių veiksmų. Teismas toje byloje vadovavosi nuostata, kad prašomo dokumento viešas atskleidimas neabejotinai padarytų žalos visuomenės interesui, susijusiam su visuomenės saugumu, ir kad bet kokia asmeninė informacija, kurią buvo prašoma atskleisti, neabejotinai atskleistų tam tikrus strateginius kovos su terorizmu aspektus, pavyzdžiui, informacijos šaltinius, jos pobūdį arba terorizmu įtariamų asmenų priežiūros laipsnį, todėl šią informaciją ir traktavo kaip neatskleistiną to prašiusiam asmeniui. Europos Bendrijų Teisingumo Teismas 2007 m. vasario 1 d. sprendimu byloje *Jose Maria Sison prieš Europos Sąjungos Tarybą* (*arrźt de la Cour (priemičre chambre) du 1er février 2007, Jose Maria Sison/Conseil de l'Union européenne, affaire C-266/05 P*) atmetė Jose Maria Sison apeliacinį skundą.

Konstitucinis Teismas savo nutarimuose ne kartą yra konstatavęs, kad Europos Žmogaus Teisių Teismo jurisprudencija, kaip teisės aiškinimo šaltinis, yra svarbi ir Lietuvos teisės aiškinimui bei taikymui; tai *mutantis mutandis* pasakytina ir apie Europos Bendrijų Teisingumo Teismo bei Europos Bendrijų Pirmosios instancijos teismo jurisprudenciją.

<...>

VI

Dėl Administracinių bylų teisenos įstatymo 57 straipsnio 3 dalies (2000 m. rugsėjo 19 d. redakcija) atitikties Konstitucijos 29 straipsniui.

1. Minėta, kad ginčijamoje Administracinių bylų teisenos įstatymo 57 straipsnio 3 dalyje (2000 m. rugsėjo 19 d. redakcija) nustatyta: „Faktiniai duomenys, sudarantys valstybės ar tarnybos paslaptį, paprastai negali būti įrodymai administracinėje byloje, kol jie bus išslaptinti įstatymų nustatyta tvarka.“

2. Iš pareiškėjo – Vilniaus apygardos administracinio teismo prašymo argumentų matyti, kad Administracinių bylų teisenos įstatymo 57 straipsnio 3 dalies (2000 m. rugsėjo 19 d. redakcija) atitiktis Konstitucijai yra ginčijama tuo aspektu, kad, pareiškėjo nuomone, neaišku, kada valstybės ar tarnybos paslaptį sudaranti informacija gali būti pripažinta įrodymu byloje: vienais atvejais asmens naudai ar prieš jį gali būti pasiremta tokiais įrodymais, nors atitinkama informacija ir nėra išslaptinta, o kitais – ne, nors pagal Konstitucijos 29 straipsnį įstatymui, teismui ir kitoms valstybės institucijoms ar pareigūnams visi asmenys lygūs.

3. Sprendžiant, ar Administracinių bylų teisenos įstatymo 57 straipsnio 3 dalis (2000 m. rugsėjo 19 d. redakcija) neprieštarauja Konstitucijai, ypač svarbi yra šios dalies formuluotė „paprastai“. Šioje dalyje yra įtvirtinta taisyklė, kad faktiniai duomenys, sudarantys valstybės ar tarnybos paslaptį, kaip įrodymai administracinėje byloje gali būti naudojami tik juos išslaptinus įstatymo (būtent Valstybės ir tarnybos paslapčių įstatymo) nustatyta tvarka, t. y. iš esmės yra draudžiama minėta tvarka neišslaptintus duomenis naudoti kaip įrodymus. Tačiau toks draudimas nėra absoliutus. Tai, ar konkrečioje nagrinėjamoje administracinėje byloje faktiniai duomenys, sudarantys valstybės ar tarnybos paslaptį, bus įrodymai, sprendžia teismas, atsižvelgdamas į visas bylos aplinkybes. Šiame Konstitucinio Teismo nutarime konstatuota, kad tai, ar tam tikra valstybės paslaptį sudaranti (ar kita įslaptinta) informacija gali būti įrodymas atitinkamoje byloje (o jeigu taip, tai kokia apimtimi), priklauso nuo daugelio veiksnių, taip pat kad jeigu sprendimui teismo nagrinėjamoje byloje priimti ir tokiam teisingumui, kokį įtvirtina Konstitucija, įvykdyti teismui pakanka tokių įrodymų (medžiagos), kurie nėra valstybės paslaptį sudaranti (ar kita įslaptinta) informacija, ši neatskleistina informacija, saugant viešąjį interesą, neturi būti įrodymas toje byloje ir šalys su ja negali būti supažindintos.

Šiame kontekste pabrėžtina, kad, kaip konstatuota šiame Konstitucinio Teismo nutarime, valstybės institucijoms sprendžiant, ar asmuo turi teisę dirbti ar susipažinti su valstybės paslaptį sudarančia (ar kita įslaptinta) informacija, būtina paisyti imperatyvo, jog tam, kad asmuo turėtų tokią teisę, valstybė turi besąlygiškai pasitikėti juo, taigi ir kad asmeniui, praradusiam valstybės pasitikėjimą, minėta teisė turi būti atimama.

Konstatuota ir tai, kad bylą nagrinėjančiam teismui visada kyla ypatinga atsakomybė, kai jis sprendžia, ar tam tikra valstybės paslaptį sudaranti (ar kita įslaptinta) informacija gali būti įrodymas toje byloje.

4. Iš Administracinių bylų teisenos įstatymo 57 straipsnio 3 dalies (2000 m. rugsėjo 19 d. redakcija) negalima daryti išvados, kad kriterijai, kuriais vadovau-

damasis bylą nagrinėjantis teismas sprendžia, ar faktiniai duomenys, sudarantys valstybės ar tarnybos paslaptį, gali būti įrodymai toje byloje, gali priklausyti nuo kokių nors subjektyvių aplinkybių. Sprendimą, ar minėti faktiniai duomenys gali būti įtraukti į bylą kaip įrodymai, teismas gali priimti tik atsižvelgęs į atitinkamos bylos medžiagą ir įvertinęs, ar jis be tų faktinių duomenų galės įvykdyti teisingumą.

5. Taigi nėra teisinių argumentų, kurie leistų teigti, kad Administracinių bylų teisenos įstatymo 57 straipsnio 3 dalyje (2000 m. rugsėjo 19 d. redakcija) nustatytas teisinis reguliavimas sudaro prielaidas teismui pareiškėjo nurodytu aspektu traktuoti bylos šalis kaip nelygias.

6. Atsižvelgiant į išdėstytus argumentus darytina išvada, kad Administracinių bylų teisenos įstatymo 57 straipsnio 3 dalis (2000 m. rugsėjo 19 d. redakcija) neprieštarauja Konstitucijos 29 straipsniui.

Vadovaudamasis Lietuvos Respublikos Konstitucijos 102, 105 straipsniais, Lietuvos Respublikos Konstitucinio Teismo įstatymo 1, 53, 54, 55, 56 straipsniais, Lietuvos Respublikos Konstitucinis Teismas

n u t a r i a:

1. Pripažinti, kad Lietuvos Respublikos administracinių bylų teisenos įstatymo 57 straipsnio 3 dalis (Žin., 2000, Nr. 85-2566) neprieštarauja Lietuvos Respublikos Konstitucijai.

<...>

Šis Konstitucinio Teismo nutarimas yra galutinis ir neskundžiamas.

<...>

8.3. IŠTRAUKOS IŠ LIETUVOS RESPUBLIKOS KONSTITUCINIO TEISMO 2011 M. LIEPOS 7 D. NUTARIMO „DĖL LIETUVOS RESPUBLIKOS VALSTYBĖS IR TARNYBOS PASLAPČIŲ ĮSTATYMO (2003 M. GRUODŽIO 16 D. REDAKCIJA) 16 STRAIPSNIO 2 DALIES 13 PUNKTO, 18 STRAIPSNIO 1 DALIES 4 PUNKTO, LIETUVOS RESPUBLIKOS VIDAUS TARNYBOS STATUTO PATVIRTINIMO ĮSTATYMU PATVIRTINTO VIDAUS TARNYBOS STATUTO 28 STRAIPSNIO (2007 M. GEGUŽĖS 15 D. REDAKCIJA) ATITIKTIES LIETUVOS RESPUBLIKOS KONSTITUCIJAI“

Byla Nr. 22/2008-31/2008-9/2010-35/2010

(Žin., 2011-07-12, Nr. 84-4106)

<...>
Konstitucinis Teismas
konstatuoja:

I

1. Pareiškėjas – Vilniaus apygardos administracinis teismas prašo ištirti, ar Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas neprieštarauja *inter alia* Konstitucijos 33 straipsnio 1 daliai (prašymas Nr. 1B-9/2010).

Konstitucijos 33 straipsnio 1 dalyje nustatyta: „Piliečiai turi teisę dalyvauti valdant savo šalį tiek tiesiogiai, tiek per demokratiškai išrinktus atstovus, taip pat teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą.“

Iš pareiškėjo prašymo argumentų matyti, kad jis abejoja, ar Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas neprieštarauja Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“.

2. Pareiškėjas – Vilniaus apygardos administracinis teismas prašo ištirti, ar Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas neprieštarauja *inter alia* Konstitucijos 48 straipsnio 1 daliai (prašymas Nr. 1B-9/2010).

Pareiškėjas taip pat prašo ištirti, ar Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktas, taip pat Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) neprieštarauja *inter alia* Konstitucijos 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą bei verslą“ (prašymas Nr. 1B-34/2008).

Konstitucijos 48 straipsnio 1 dalyje nustatyta: „Kiekvienas žmogus gali laisvai pasirinkti darbą bei verslą ir turi teisę turėti tinkamas, saugias ir sveikas darbo sąlygas, gauti teisingą apmokėjimą už darbą ir socialinę apsaugą nedarbo atveju.“

Iš pareiškėjo prašymų argumentų matyti, kad jis abejoja, ar Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas, 18 straipsnio 1 dalies 4 punktas ir Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) pareiškėjo nurodytais aspektais neprieštarauja Konstitucijos 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“.

3. Pareiškėjas – Vilniaus apygardos administracinis teismas prašo ištirti, ar Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas neprieštarauja *inter alia* konstituciniams teisinės valstybės, proporcingumo principams (prašymas Nr. 1B-9/2010).

Pažymėtina, jog Konstitucinis Teismas ne kartą yra konstatavęs, kad konstitucinis proporcingumo principas yra vienas iš konstitucinio teisinės valstybės principo elementų (*inter alia* Konstitucinio Teismo 2004 m. gruodžio 29 d., 2005 m. rugsėjo 29 d., 2009 m. balandžio 10 d. nutarimai).

4. Pareiškėjas – Vilniaus apygardos administracinis teismas prašo ištirti Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkto konstitucingumą tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas asmeniui neišduodamas, jeigu asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką (prašymas Nr. 1B-9/2010).

Pareiškėjo ginčijamame Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio „Leidimo dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimo išdavimo sąlygos“ 2 dalies 13 punkte nustatyta:

„Leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas asmeniui neišduodamas, jeigu asmuo:

<...>

13) yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas.“

Taigi, be aplinkybės, kad asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką, pareiškėjo ginčijamame Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkte nurodomos dar dvi aplinkybės, kurioms esant asmeniui leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas neišduodamas: jeigu asmeniui dėl tyčinės nusikalstamos veikos yra atliekamas ikiteisminis ar operatyvinis tyrimas.

Prašymuose Nr. 1B-24/2008, 1B-34/2008, 1B-47/2010 pareiškėjas prašo ištirti Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkto atitiktį Konstitucijai tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas, jeigu asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atlieka-

mas ikiteisminis ar operatyvinis tyrimas.

Pareiškėjo ginčijamame Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio „Leidimo dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimo panaikinimas“ 1 dalies 4 punkte nustatyta:

„Leidimas dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimas panaikinamas, jeigu:

<...>

4) atsiranda ar paaiškėja kuri nors iš aplinkybių, nurodytų šio Įstatymo 16 straipsnio 2 dalyje.“

Taigi pareiškėjo ginčijamame Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimas panaikinamas, jeigu atsiranda ar paaiškėja kuri nors iš aplinkybių, nurodytų šio įstatymo 16 straipsnio 2 dalyje, *inter alia* kuri nors iš 13 punkte nurodytų aplinkybių: jeigu asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas.

Vadinasi, šioje konstitucinės justicijos byloje pareiškėjo ginčijamos Valstybės ir tarnybos paslapčių įstatymo nuostatos yra neatsiejamos. Todėl tirdamas Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkto nuostatos atitiktį Konstitucijai pareiškėjo ginčijamais aspektais Konstitucinis Teismas šioje konstitucinės justicijos byloje taip pat tirs šio įstatymo 16 straipsnio 2 dalies 13 punkte nustatytą teisinį reguliavimą visa apimtimi.

5. Pareiškėjas – Vilniaus apygardos administracinis teismas abejoja dėl Vidaus tarnybos statuto 28 straipsnio (2007 m. gegužės 15 d. redakcija) atitikties Konstitucijai tiek, kiek jame nėra numatyta galimybė vadovui, turinčiam teisę skirti pareigūną į pareigas, nušalinti jį nuo pareigų, kai yra atliekamas ikiteisminis ar operatyvinis tyrimas, jeigu pareigūno nušalinimo nuo tarnybos klausimo Baudžiamojo proceso kodekso nustatyta tvarka nesprendžia įgalioti tai padaryti asmenys (prašymai Nr. 1B-24/2008, 1B-34/2008). Iš pareiškėjo nurodytų argumentų matyti, kad pareiškėjas ginčija Vidaus tarnybos statuto 28 straipsnio (2007 m. gegužės 15 d. redakcija) atitiktį Konstitucijai tik tuo aspektu, kad jame nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai dėl jo tyčinės nusikalstamos veikos yra atliekamas ikiteisminis ar operatyvinis tyrimas ir pareigūno nušalinimo nuo tarnybos klausimo Baudžiamojo proceso kodekso nustatyta tvarka nesprendžia įgalioti tai padaryti asmenys.

Pažymėtina, kad pagal Baudžiamojo proceso kodekso 157 straipsnį „Laikinas nušalinimas nuo pareigų ar laikinas teisės užsiimti tam tikra veikla sustabdymas“ įtariamasis nuo pareigų laikinai gali būti nušalintas nusikalstamos veikos tyrimo metu ikiteisminio tyrimo teisėjo nutartimi, gavus prokuroro prašymą, o bylą perdavus į teismą dėl laikino nušalinimo nuo pareigų nusprendžia teismas, kurio žinioje yra byla. Laikinas nušalinimas nuo pareigų skiriamas, jei

tai būtina, kad būtų greičiau ir nešališkiau ištirta nusikalstama veika ar užkirsta galimybė daryti naujas nusikalstamas veikas.

Taip pat pažymėtina, kad pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 12 straipsnio 2 dalį už bendrą įslaptintos informacijos, kuria disponuoja paslapčių subjektas, apsaugos organizavimą ir būklę yra atsakingas paslapčių subjekto vadovas, o už įslaptintos informacijos apsaugos reikalavimų vykdymą paslapčių subjekto struktūriniuose padaliniuose, kuriuose saugoma arba naudojama įslaptinta informacija, yra atsakingi šių struktūrinių padalinių vadovai, jų įgalioti asmenys, taip pat asmenys, kuriems ši informacija yra patikėta. Leidimus dirbti ar susipažinti su įslaptinta informacija taip pat išduoda paslapčių subjektai (Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 15 straipsnio 7 dalis). Paslapčių subjektai yra valstybės ir savivaldybių institucijos, kurių veikla susijusi su informacijos įslaptinimu, išslaptinimu, įslaptintos informacijos naudojimu ir (ar) apsauga, tokių institucijų reguliavimo sričiai priskirtos įstaigos, įmonės, kurioms šios institucijos, suderinusios su Paslapčių apsaugos koordinavimo komisija, suteikė paslapčių subjekto statusą (Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 2 straipsnio 8 dalis (2010 m. gruodžio 14 d. redakcija).

Taigi už įslaptintos informacijos, kuria disponuoja paslapčių subjektai, apsaugą atsako atitinkamų paslapčių subjektų ir jų struktūrinių padalinių vadovai bei jų įgalioti asmenys. Atsižvelgiant į tai, šioje konstitucinės justicijos byloje turėtų būti tiriama Vidaus tarnybos statuto 28 straipsnio (2007 m. gegužės 15 d. redakcija) atitiktis Konstitucijai tiek, kiek jame nėra nustatyti paslapčių subjekto ar jo struktūrinio padalinio vadovo arba jo įgalioto asmens, turinčio teisę skirti asmenį į pareigas (t. y. šios konstitucinės justicijos bylos kontekste – vadovo, turinčio teisę skirti asmenį į pareigas), įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai dėl jo tyčinės nusikalstamos veikos yra atliekamas ikiteisminis ar operatyvinis tyrimas.

Konstitucinis Teismas, šioje konstitucinės justicijos byloje konstatavęs, kad tirs Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkte nustatytą teisinį reguliavimą visa apimtimi, taip pat tirs Vidaus tarnybos statuto 28 straipsnio (2007 m. gegužės 15 d. redakcija) atitiktį Konstitucijai tiek, kiek jame nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas.

6. Taigi, atsižvelgdamas į išdėstytus argumentus, šioje konstitucinės justicijos byloje Konstitucinis Teismas tirs, ar:

– Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas neprieštarauja Konstitucijos 31 straipsnio 1 daliai, 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam tei-

sinės valstybės principui;

– Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktas tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas atsiradus arba paaiškėjus šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytoms aplinkybėms, neprieštarauja Konstitucijos 31 straipsnio 1 daliai, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui;

– Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) tiek, kiek jame nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, neprieštarauja Konstitucijos 31 straipsnio 1 daliai, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

II

1. Minėta, kad pareiškėjas abejoja, ar šioje konstitucinės justicijos byloje jo ginčijamas teisinis reguliavimas neprieštarauja Konstitucijos 31 straipsnio 1 daliai, 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

2. Šioje konstitucinės justicijos byloje ginčijamos *inter alia* Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) nuostatos, įtvirtinančios leidimų dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimo išdavimo ir panaikinimo sąlygas bei pagrindus. Taigi šiame kontekste svarbu atskleisti *inter alia* konstitucinį valstybės paslapties institutą.

Sąvoka „valstybinė paslaptis“ *expressis verbis* vartojama Konstitucijoje (117 straipsnio 1 dalis). Konstitucinis Teismas 2007 m. gegužės 15 d. nutarime yra konstatavęs, kad valstybės paslaptis – konstitucinis institutas; valstybės paslaptis – tai tokia neskelbtina, neskleistina informacija, kurios atskleidimas galėtų padaryti žalos valstybei, kaip bendram visos visuomenės gėriui, visos visuomenės politinei organizacijai, kurios paskirtis – užtikrinti žmogaus teises ir laisves, garantuoti viešąjį interesą.

Konstitucinis Teismas 2007 m. gegužės 15 d. nutarime yra pažymėjęs, kad asmeniui, kuriam suteikiama teisė susipažinti su valstybės paslaptį sudarančia informacija, keliami tam tikri reikalavimai, susiję su jo patikimumu bei lojalumu Lietuvos valstybei, kurie yra sietini su valstybės pasitikėjimu tuo asmeniu. Valstybės nepasitikėjimą tam tikru asmeniu gali lemti paties to asmens veikla, *inter alia* padaryti teisės pažeidimai, taip pat to asmens savybės, ryšiai, kitos svarbios aplinkybės. Su valstybės paslaptimis gali būti leidžiama susipažinti tik tokiam asmeniui, kurio veikla, savybės, ryšiai ir kt. negali duoti pagrindo nuogąstauti, kad, jam sužinojus valstybės paslaptį, kils grėsmė, juo labiau bus

padaryta žalos valstybės suverenitetui, teritorijos vientisumui, konstitucinei santvarkai, gynybinei galiai, kitiems itin svarbiems valstybės interesams, visuomenės ir valstybės gyvenimo pagrindams, bus pažeisti svarbiausi Konstitucijos reguliuojami, ginami ir saugomi santykiai, kuriuos kaip tik ir turi padėti apsaugoti ir apginti tai, kad tam tikra informacija pagal įstatymus yra įslaptinama. Asmeniui, praradusiam valstybės pasitikėjimą, teisė susipažinti ar dirbti su informacija, sudarančia valstybės paslaptį, turi būti atimama.

Konstitucinis Teismas 2007 m. gegužės 15 d. nutarime taip pat yra konstatavęs, kad valstybės paslapties atskleidimas gali sukelti grėsmę ar net padaryti žalos valstybės suverenitetui, teritorijos vientisumui, konstitucinei santvarkai, gynybinei galiai, kitiems itin svarbiems valstybės interesams, visuomenės ir valstybės gyvenimo pagrindams. Jeigu valstybės paslaptį sudarančios informacijos atskleidimui (sužinojimui, paskleidimui) nebūtų užkertamas kelias, jeigu toks atskleidimas nebūtų teisiškai persekiojamas, būtų sudarytos prielaidos pažeisti net svarbiausius Konstitucijos reguliuojamus, ginamus ir saugomus santykius, taigi tam tikro asmens ar asmenų interesą žinoti ar skleisti tam tikrą informaciją iškelti aukščiau viešojo intereso.

3. Konstitucijos 48 straipsnio 1 dalyje *inter alia* yra įtvirtinta, kad kiekvienas žmogus gali laisvai pasirinkti darbą. Ši laisvė yra viena iš būtinų žmogaus gyvybinių poreikių tenkinimo, deramos padėties visuomenėje užtikrinimo sąlygų. Konstitucinė kiekvieno žmogaus laisvė pasirinkti darbą suponuoja įstatymų leidėjo pareigą sudaryti teisines prielaidas įgyvendinti šią laisvę. Sudarydamas jas įstatymų leidėjas turi įgaliojimus, atsižvelgdamas į darbo pobūdį, nustatyti teisės laisvai pasirinkti darbą įgyvendinimo sąlygas. Tai darydamas jis turi paisyti Konstitucijos (Konstitucinio Teismo 2002 m. lapkričio 25 d., 2003 m. liepos 4 d., 2004 m. gruodžio 29 d., 2007 m. rugpjūčio 13 d., 2008 m. sausio 7 d., 2008 m. vasario 20 d., 2010 m. kovo 22 d. nutarimai).

4. Pagal Konstitucijos 33 straipsnio 1 dalį piliečiai *inter alia* turi teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą.

4.1. Konstitucinė teisė lygiomis sąlygomis stoti į valstybės tarnybą sietina *inter alia* su Konstitucijos 48 straipsnyje įtvirtinta kiekvieno žmogaus teise laisvai pasirinkti darbą. Konstitucinis Teismas 2004 m. gruodžio 13 d., 2007 m. rugpjūčio 13 d. nutarimuose yra *inter alia* pažymėjęs, kad piliečio konstitucinė teisė lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą yra kiekvieno asmens konstitucinės teisės pasirinkti darbą atmaina.

4.2. Pažymėtina, kad Konstitucijos 33 straipsnio 1 dalies nuostata, įtvirtinanti piliečių teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą, neturi būti aiškinama tik lingvistiškai ir neturi būti suprantama tik kaip teisė stoti į valstybės tarnybą, t. y. tik kaip susijusi su asmens priėmimu į valstybės tarnybą. Kaip ne kartą pažymėjo Konstitucinis Teismas, valstybės tarnybos santykiai apima ne tik santykius, susijusius su piliečio teisės lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą įgyvendinimu, bet ir santykius, susiklostančius piliečiui įstojus į valstybės tarnybą ir einant pareigas valstybės tarnyboje (Konstitucinio Teismo 2004 m. gruodžio 13 d., 2007 m. rugpjūčio 13 d. nutarimai).

4.3. Konstitucinis Teismas *inter alia* 2007 m. rugpjūčio 13 d. nutarime yra

konstatavęs, kad, sudarydamas teisines prielaidas įgyvendinti teisę laisvai pasirinkti darbą bei verslą (taigi ir stoti į valstybės tarnybą), įstatymų leidėjas turi įgaliojimus, atsižvelgdamas į darbo pobūdį, nustatyti teisės laisvai pasirinkti darbą įgyvendinimo sąlygas.

Konstitucinis Teismas taip pat yra konstatavęs, kad piliečių teisė lygiomis sąlygomis stoti į Lietuvos Respublikos valstybės tarnybą nėra absoliuti: valstybė negali įsipareigoti ir neįsipareigoja kiekvieno asmens priimti dirbti valstybės tarnyboje. Valstybės tarnyba turi būti kvalifikuota, priimti dirbti joje asmenys turi sugebėti atlikti jai keliamus uždavinius. Norintieji tapti valstybės tarnautojais, pareigūnais paprastai privalo turėti atitinkamą išsilavinimą, profesinę patirtį, kai kurias asmens savybes, be to, kuo aukštesnės pareigos, kuo svarbesnė veiklos sritis, tuo didesni reikalavimai keliami šias pareigas einantiems asmenims (Konstitucinio Teismo 1999 m. kovo 4 d., 2007 m. rugpjūčio 13 d., 2008 m. sausio 22 d. nutarimai).

Pagal Konstituciją valstybės tarnyba – tai tarnyba Lietuvos valstybei ir pilietinei Tautai, todėl valstybės tarnyba turi būti lojali Lietuvos valstybei ir jos konstitucinei santvarkai; viena iš stojimo į valstybės tarnybą bendrųjų sąlygų yra lojalumas Lietuvos valstybei ir jos konstitucinei santvarkai (Konstitucinio Teismo 2004 m. gruodžio 13 d., 2007 m. rugpjūčio 13 d. nutarimai). Valstybės institucijose turi dirbti tik lojalūs tai valstybei asmenys, kurių ištikimybė jai ir patikimumas nekelia jokių abejonių (Konstitucinio Teismo 1998 m. lapkričio 11 d., 1999 m. kovo 4 d., 2007 m. rugpjūčio 13 d. nutarimai).

Įstatymų leidėjas ne tik gali, bet ir privalo nustatyti tokį teisinį reguliavimą, kuris leistų patikrinti siekiančių eiti pareigas valstybės tarnyboje asmenų patikimumą – lojalumą Lietuvos valstybei, reputaciją ir t. t. Pretendentų į pareigas valstybės tarnyboje patikimumas turi būti tikrinamas dar prieš jiems pradedant eiti pareigas. Kai valstybės tarnautojai eina pareigas, jų patikimumas taip pat gali būti tikrinamas, jeigu dėl jo kyla pagrįstų abejonių. Jeigu yra pagrįstai konstatuotas asmens, siekiančio tam tikrų pareigų valstybės tarnyboje, nepatikimumas, toks asmuo negali būti priimamas į atitinkamas pareigas (Konstitucinio Teismo 2007 m. rugpjūčio 13 d. nutarimas).

Konstitucinis Teismas 2004 m. gruodžio 13 d. nutarime yra konstatavęs, kad kaip vieni iš stojimo į valstybės tarnybą specialiųjų sąlygų paminėtini reikalavimai, susiję su stojančiojo reputacija, asmeninėmis savybėmis ir kt. Priimant į tam tikras pareigas gali būti nustatomos labai įvairios specialiosios sąlygos, pavyzdžiui, susijusios su asmens sveikata, fizinėmis galimybėmis, ryšiais su kitais asmenimis ir kt. Specialiosios stojimo į valstybės tarnybą sąlygos gali būti diferencijuotos pagal atitinkamų pareigų valstybės tarnyboje turinį. Visi nustatyti specialieji stojimo į valstybės tarnybą reikalavimai turi būti konstituciškai pateisinami.

4.4. Šios konstitucinės justicijos bylos kontekste pažymėtina, kad pagal Konstituciją asmenims, siekiantiems eiti ar einantiems pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, nustatoma specialioji sąlyga yra ypatingas ir nė kiek neabejotinas patikimumas ir lojalumas Lietuvos valstybei. Asmens, siekiančio eiti ar einančio pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, patikimumas ir lojalumas Lietuvos valstybei turi būti vertinami atsižvelgiant

į visas reikšmingas tą asmenį apibūdinančias aplinkybes, *inter alia* jo veiklą, padarytus teisės pažeidimus, dalykines ir asmenines savybes, reputaciją, ryšius su kitais asmenimis. Todėl įstatymų leidėjas turi plačią diskreciją reguliuodamas santykius, susijusius su valstybės ir tarnybos paslapčių apsauga, *inter alia* nustatydamas asmenų, siekiančių eiti ar einančių pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, patikimumo ir lojalumo Lietuvos valstybei kriterijus bei tokių asmenų patikrinimo procedūras. Įgyvendindamas šią diskreciją įstatymų leidėjas turi paisyti Konstitucijos normų ir principų, *inter alia* konstitucinio teisinės valstybės principo.

4.5. Šiame kontekste taip pat paminėtina, jog 2007 m. rugpjūčio 13 d. nutarime Konstitucinis Teismas *inter alia* pažymėjo, kad asmens (ir siekiančio eiti pareigas valstybės tarnyboje, ir jas jau einančio) patikimumo patikros santykių teisinis reglamentavimas turi būti toks, kad mažareikšmiai, atsitiktiniai ir pan. faktai ir aplinkybės netaptų pagrindu konstatuoti asmens, siekiančio eiti arba einančio pareigas valstybės ar savivaldybės įstaigoje, nepatikimumo, juo labiau kad asmens nepatikimumas nebūtų konstatuojamas remiantis vien prielaidomis.

Šios konstitucinės justicijos bylos kontekste pažymėtina, kad negali būti nustatytas toks teisinis reguliavimas, kuris leistų įstatymo įgaliotai valstybės institucijai konstatuoti asmens, siekiančio eiti ar einančio pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, nepatikimumą (ar nelojalumą Lietuvos valstybei) remiantis tik mažareikšmėmis aplinkybėmis. Tačiau tai nereiškia, kad įstatymų leidėjas negali numatyti tokių įslaptintos informacijos apsaugos priemonių, kurios leistų iš anksto užkirsti kelią grėsmėms įslaptintos informacijos saugumui ir kartu – grėsmėms valstybės interesams.

5. Kaip ne kartą konstatavo Konstitucinis Teismas, Konstitucijoje įtvirtintas teisinės valstybės principas, be kitų reikalavimų, suponuoja ir tai, kad turi būti užtikrintos žmogaus teisės ir laisvės (*inter alia* Konstitucinio Teismo 2001 m. liepos 12 d., 2004 m. gruodžio 13 d., 2004 m. gruodžio 29 d., 2006 m. sausio 16 d. nutarimai). Šiame Konstitucinio Teismo nutarime minėta, kad vienas iš konstitucinio teisinės valstybės principo elementų taip pat yra konstitucinis proporcingumo principas.

Konstitucinis Teismas savo nutarimuose taip pat ne kartą yra konstatavęs, kad pagal Konstituciją riboti žmogaus teises ir laisves galima, jeigu laikomasi šių sąlygų: tai daroma įstatymu; apribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti kitų asmenų teises ir laisves bei Konstitucijoje įtvirtintas vertybes, taip pat konstituciškai svarbius tikslus; apribojimais nėra paneigiama teisių ir laisvių prigimtis bei jų esmė; yra laikomasi konstitucinio proporcingumo principo. Konstitucinis proporcingumo principas reiškia ir tai, kad įstatyme numatytos priemonės turi atitikti teisėtus ir visuomenei svarbius tikslus, kad šios priemonės turi būti būtinos minėtiems tikslams pasiekti ir jos neturi varžyti asmens teisių ir laisvių akivaizdžiai labiau negu reikia šiems tikslams pasiekti (Konstitucinio Teismo 2009 m. gruodžio 11 d. nutarimas, 2010 m. balandžio 20 d. sprendimas, 2010 m. birželio 29 d. nutarimas).

Šios konstitucinės justicijos bylos kontekste pažymėtina, kad konstitucinio proporcingumo principo reikalavimas asmens teisių ir laisvių įstatymu neriboti

labiau negu reikia teisėtiems ir visuomenei svarbiems tikslams pasiekti *inter alia* suponuoja reikalavimą įstatymų leidėjui nustatyti tokį teisinį reguliavimą, kuris sudarytų prielaidas pakankamai individualizuoti asmens teisių ir laisvių apribojimus: ribojantis asmens teises ir laisves įstatymo nustatytas teisinis reguliavimas turi būti toks, kad sudarytų prielaidas kiek įmanoma įvertinti individualią kiekvieno asmens situaciją ir, atsižvelgiant į visas svarbias aplinkybes, atitinkamai individualizuoti konkrečias tam asmeniui taikytinas ribojančias jo teises priemones.

6. Konstitucijos 31 straipsnio 1 dalyje įtvirtinta nekaltumo prezumpcija yra viena svarbiausių teisingumo vykdymo demokratinėje teisinėje valstybėje garantijų. Tai pamatinis teisingumo vykdymo baudžiamųjų bylų procese principas, viena svarbiausių teisingumo vykdymo demokratinėje teisinėje valstybėje garantijų, kartu svarbi žmogaus teisių ir laisvių garantija (Konstitucinio Teismo 2004 m. gruodžio 29 d., 2006 m. sausio 16 d., 2007 m. sausio 16 d., 2009 m. birželio 8 d. nutarimai). Konstitucinis Teismas 1996 m. balandžio 18 d. nutarime pažymėjo, kad teismai vykdo teisingumą, t. y. sprendžia teisinius konfliktus, priimdami teisinius sprendimus. Asmuo laikomas nepadariusiu nusikaltimo, kol jo kaltumas nebus įrodytas įstatymo nustatyta tvarka ir pripažintas įsiteisėjusiu teismo nuosprendžiu (Konstitucinio Teismo 2004 m. gruodžio 29 d. nutarimas).

Konstitucinis Teismas savo aktuose ne kartą yra konstatavęs, kad nekaltumo prezumpcijos negalima aiškinti vien lingvistiškai, kaip susijusios vien su teisingumo vykdymu baudžiamųjų bylų procese. Nekaltumo prezumpcija, vertinama kitų Konstitucijos nuostatų kontekste, turi ir platesnį turinį, ji negali būti siejama vien su baudžiamaisiais teisiniais santykiais. Ypač svarbu, kad nekaltumo prezumpcijos laikytųsi valstybės institucijos ir pareigūnai, kad viešieji asmenys, kol asmens kaltumas padarius nusikaltimą nebus įstatymo nustatyta tvarka įrodytas ir pripažintas įsiteisėjusiu teismo nuosprendžiu, apskritai susilaikytų nuo asmens įvardijimo kaip nusikaltėlio (Konstitucinio Teismo 2004 m. gruodžio 29 d., 2006 m. sausio 16 d., 2007 m. sausio 16 d. nutarimai).

Taigi vykdyti teisingumą, *inter alia* pripažinti asmenį kaltu padarius nusikalstamą veiką, yra išimtinė teismų funkcija. Kad ir kokius klausimus spręstų, jokia kita valstybės institucija ar pareigūnas negali laikyti asmens kaltu padarius nusikalstamą veiką, kol jo kaltumas nėra įstatymo nustatyta tvarka įrodytas ir pripažintas įsiteisėjusiu teismo nuosprendžiu. Tačiau tai, kad asmuo nėra laikomas kaltu padarius nusikalstamą veiką, kol jo kaltumas dėl tokios veikos nėra įstatymo nustatyta tvarka įrodytas ir pripažintas įsiteisėjusiu teismo nuosprendžiu, dar nereiškia, kad asmuo, siekiantis eiti ar einantis pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, būtinai yra vertas valstybės pasitikėjimo ir kad įstatymo įgaliotai valstybės institucijai negali kilti tam tikrų abejonių dėl asmens patikimumo ar lojalumo Lietuvos valstybei, kurias sukelia ne nustatytas jo kaltumas padarius nusikalstamą veiką, o tam tikros faktinės aplinkybės, asmens veikla, savybės, reputacija, ryšiai ar kitos reikšmingos aplinkybės, *inter alia* susijusios su galbūt padaryta nusikalstama veika.

Taigi aplinkybės, sukeliančios abejonių dėl asmens, kuris siekia eiti ar eina pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar

jos apsauga, patikimumo ar lojalumo Lietuvos valstybei, gali būti susijusios ir su asmens galbūt padaryta nusikalstama veika. Vertindama šias aplinkybes įstatymo įgaliota valstybės institucija nevykdo teisingumo ir nesprendžia asmens kaltumo padarius nusikalstamą veiką klausimo.

7. Šioje konstitucinės justicijos byloje pareiškėjas ginčija, jo manymu, Vidaus tarnybos statuto 28 straipsnyje (2007 m. gegužės 15 d. redakcija) esančią legislatyvinę omisiją – tai, kas šiame teisės akte nėra nustatyta, nors, pareiškėjo manymu, pagal Konstituciją įstatymų leidėjo turėtų būti nustatyta, taigi ginčijama tokia teisinio reguliavimo spraga, kurią, pareiškėjo nuomone, Konstitucija draudžia.

Konstitucinis Teismas yra konstatavęs, jog teisės spraga, *inter alia* legislatyvinė omisija, visuomet reiškia, kad atitinkamų visuomeninių santykių teisinis reguliavimas apskritai nei eksplicitiškai, nei implicitiškai nėra nustatytas nei tam tikrame teisės akte (jo dalyje), nei kuriuose nors kituose teisės aktuose, tačiau poreikis tuos visuomeninius santykius teisiškai sureguliuoti yra, o legislatyvinės omisijos atveju tas teisinis reguliavimas turi būti nustatytas būtent tame teisės akte (būtent toje jo dalyje), nes to reikalauja kuris nors aukštesnės galios teisės aktas, *inter alia* pati Konstitucija (Konstitucinio Teismo 2006 m. rugpjūčio 8 d., 2008 m. lapkričio 5 d. sprendimai, 2009 m. kovo 2 d., 2009 m. birželio 22 d., 2009 m. gruodžio 11 d., 2010 m. rugsėjo 29 d., 2010 m. lapkričio 29 d. nutarimai).

Konstitucinio Teismo 2009 m. kovo 2 d. nutarime konstatuota, kad vidinė teisės sistemos darna, kurią suponuoja konstitucinis teisinės valstybės principas, yra *inter alia* susijusi su teisės spragomis, t. y. teisinio reguliavimo trūkumu, *inter alia* legislatyvine omisija. Konstitucinis Teismas 2006 m. rugpjūčio 8 d. sprendime, 2010 m. lapkričio 29 d. nutarime yra konstatavęs, kad teisės spragų (neišskiriant nė legislatyvinės omisijos) pašalinimas yra atitinkamo (kompetentingo) teisėkūros subjekto kompetencijos dalykas. Be to, Konstitucinis Teismas 2006 m. rugpjūčio 8 d. sprendime, 2007 m. birželio 7 d., 2010 m. lapkričio 29 d. nutarimuose yra konstatavęs: galutinai pašalinti teisės spragas galima tik teisę kuriančioms institucijoms išleidus atitinkamus teisės aktus.

8. Konstitucinis Teismas 2007 m. gegužės 15 d. nutarime pažymėjo, kad konstitucinė priedermė saugoti valstybės paslaptis (ar kitą įslaptintą informaciją) kyla ir iš Seimo ratifikuotų tarptautinių sutarčių, kurios yra sudedamoji Lietuvos Respublikos teisinės sistemos dalis (Konstitucijos 138 straipsnio 3 dalis). *Inter alia* tokios yra tarptautinės sutartys, kuriomis grindžiama Lietuvos Respublikos narystė tarptautinėse organizacijose. Konstitucinė priedermė saugoti valstybės paslaptis (kitą įslaptintą informaciją) apima ir priedermę saugoti kitoms valstybėms ar tarptautinėms organizacijoms priklausančias paslaptis, kuriomis disponuoja Lietuvos Respublika (jos institucijos, pareigūnai).

Paminėtina, kad bendriems Konstitucijoje įtvirtintiems valstybės tarptautinio bendradarbiavimo pagrindams būdinga *inter alia* tai, kad yra nustatyta Lietuvos valstybės geopolitinė orientacija – valstybės dalyvavimas Europos integracijoje būnant Europos Sąjungos (ES) nare, siekis užtikrinti šalies nepriklausomybę ir saugumą prisidedant prie teise ir teisingumu pagrįstos tarptautinės tvarkos kūrimo (Konstitucinio Teismo 2011 m. kovo 15 d. nutarimas).

Šios konstitucinės justicijos bylos kontekste pažymėtina, kad Lietuvos valstybės geopolitinė orientacija neatsiejama ir nuo kitų Lietuvos Respublikos tarptautinių įsipareigojimų, *inter alia* kylančių iš narystės transatlantinėje saugumo ir gynybos organizacijoje – Šiaurės Atlanto Sutarties Organizacijoje (NATO); tokia narystė ne tik teikia Lietuvai papildomas saugumo garantijas, bet ir suponuoja būtinumą laikytis prisiimtų tarptautinių įsipareigojimų.

Taigi Lietuvos valstybės geopolitinė orientacija reiškia Lietuvos Respublikos narystę ES ir NATO bei būtinumą vykdyti atitinkamus su šia naryste susijusius tarptautinius įsipareigojimus, *inter alia* įslaptintos informacijos apsaugos srityje. Todėl reglamentuodama valstybės paslapčių apsaugą Lietuvos Respublika negali nustatyti žemesnių šios apsaugos standartų nei ES ir NATO įslaptintos informacijos apsaugos standartai. Laikantis Konstitucijos normų ir principų gali būti nustatyti ir aukštesni Lietuvos Respublikos valstybės paslapčių apsaugos standartai.

III

1. Šioje konstitucinės justicijos byloje ginčijama *inter alia* Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkto atitiktis Konstitucijai, taip pat 18 straipsnio 1 dalies 4 punkto tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas atsiradus arba paaiškėjus šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytoms aplinkybėms, atitiktis Konstitucijai.

2. Seimas 2003 m. gruodžio 16 d. priėmė Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo pakeitimo įstatymą, kurio 1 straipsniu Valstybės ir tarnybos paslapčių įstatymą (1999 m. lapkričio 25 d. redakcija su vėlesniais pakeitimais ir papildymais) išdėstė nauja redakcija. Šis įstatymas įsigaliojo 2004 m. gegužės 1 d. Jo įgyvendinimo tvarką nustato tą pačią dieną (2003 m. gruodžio 16 d.) Seimo priimtas ir 2004 m. sausio 7 d. įsigaliojęs Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo pakeitimo įstatymo įgyvendinimo įstatymas.

3. Valstybės ir tarnybos paslapčių įstatymas (2003 m. gruodžio 16 d. redakcija) reguliuoja santykius, susijusius su valstybės ar tarnybos paslaptį sudarančios informacijos įslaptinimu, saugojimu, naudojimu, išslaptinimu, apsaugos veiksmų koordinavimu bei kontrole, nustato minimalius atskirų įslaptintos informacijos apsaugos sričių (personalo patikimumo, įslaptintos informacijos administravimo, fizinės apsaugos, įslaptintų sandorių saugumo, automatizuoto duomenų apdorojimo sistemų ir tinklų apsaugos) reikalavimus. Jame *inter alia* nustatyta, kad užsienio valstybių, Europos Sąjungos ar tarptautinių organizacijų įslaptinta informacija, perduota Lietuvos Respublikai, saugoma ir naudojama Lietuvos Respublikos tarptautinių sutarčių ir šiomis sutartimis grindžiamų bei jas įgyvendinančių tarptautinių organizacijų sprendimų, Europos Sąjungos teisės aktų ir šio įstatymo nustatyta tvarka; tais atvejais, kai Lietuvos Respublikos tarptautinėse sutartyse ir (ar) jomis grindžiamų ir (ar) jas įgyvendinančių tarptautinių organizacijų sprendimuose, Europos Sąjungos teisės aktuose yra nustatyti kitokie užsienio valstybių ar tarptautinių organizacijų įslaptintos in-

formacijos saugojimo ir naudojimo reikalavimai, negu nustato šis įstatymas, yra taikomos tarptautinių sutarčių ir (ar) jomis grindžiamų ir (ar) jas įgyvendinančių tarptautinių organizacijų sprendimų, Europos Sąjungos teisės aktų nuostatos (Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 1 straipsnis).

4. Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) ketvirtajame skirsnyje „Personalo patikimumas“ reguliuojami santykiai, susiję su leidimo dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimo išdavimu ir panaikinimu. Šiame skirsnyje yra 16 ir 18 straipsniai, kurių nuostatas šioje konstitucinės justicijos byloje ginčija pareiškėjas.

Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 2 straipsnio 15 punkte įtvirtinta, kad leidimas dirbti ar susipažinti su įslaptinta informacija – šio įstatymo nustatyta tvarka išduotas dokumentas, patvirtinantis asmens teisę dirbti ar susipažinti su Lietuvos Respublikos įslaptinta informacija, žymima slaptumo žymomis „Visiškai slaptai“, „Slaptai“, „Konfidencialiai“, arba tokią informaciją saugoti ar gabenti. Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 2 straipsnio 16 punkte nustatyta, kad asmens patikimumo pažymėjimas – šio įstatymo nustatyta tvarka išduotas dokumentas, patvirtinantis asmens teisę dirbti ar susipažinti su užsienio valstybių ar tarptautinių organizacijų perduota įslaptinta informacija, žymima slaptumo žymų „Visiškai slaptai“, „Slaptai“, „Konfidencialiai“ atitikmenimis, arba tokią informaciją saugoti ar gabenti.

Taigi leidimas dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimas patvirtina specialiąją teisę dirbti ar susipažinti su įslaptinta informacija.

5. Paminėtina, kad Seimui 2010 m. gruodžio 14 d. priėmus Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo 2, 5, 7, 8, 11, 12, 16, 18, 31, 36, 37, 40, 41, 42, 43, 44 straipsnių pakeitimo ir papildymo ir aštuntojo skirsnio pavadinimo pakeitimo įstatymą, buvo pakeisti *inter alia* Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnis (jo 2 dalies 2, 4 punktai, 7 dalis) bei 18 straipsnis (jo 5 dalis). Tačiau ginčijami Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas bei 18 straipsnio 1 dalies 4 punktas, taip pat kitos šiai konstitucinės justicijos bylai reikšmingos šio įstatymo nuostatos keičiamos nebuvo.

6. Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnyje „Leidimo dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimo išdavimo sąlygos“, kurio 2 dalies 13 punkto nuostatą ginčija pareiškėjas, nustatyta:

„1. Asmeniui, pretenduojančiam gauti leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą, toks leidimas ar pažymėjimas išduodamas, jeigu:

1) asmuo yra Lietuvos Respublikos pilietis;

2) asmuo pateikia užpildytą nustatytos formos klausimyną ir raštiškai sutinka, kad būtų tikrinama jo kandidatūra;

3) asmuo raštiškai pasižada saugoti įslaptintą informaciją;

4) tikrinimo metu surinkti faktai nekelia abejonių dėl asmens patikimumo ar lojalumo Lietuvos valstybei;

5) tikrinimo metu nenustatoma bent viena šio straipsnio 2 dalyje nurodyta aplinkybė.

2. Leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas asmeniui neišduodamas, jeigu asmuo:

1) neatitinka bent vienos šio straipsnio 1 dalyje nurodytos sąlygos;

2) nuolat gyveno Lietuvos Respublikoje mažiau kaip 5 pastaruosius metus ir šio Įstatymo 11 straipsnio 5 dalies 11 punkto nustatyta tvarka Paslapčių apsaugos koordinavimo komisija priėmė sprendimą neišduoti leidimo dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimo;

3) yra kreipęsis į atitinkamas valstybės institucijas dėl Lietuvos Respublikos pilietybės atsisakymo;

4) turi dvigubą pilietybę ir šio Įstatymo 11 straipsnio 5 dalies 11 punkto nustatyta tvarka Paslapčių apsaugos koordinavimo komisija priėmė sprendimą neišduoti leidimo dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimo;

5) buvo nuteistas už nusikaltimą Lietuvos valstybės nepriklausomybei, teritorijos vientisumui ir konstitucinei santvarkai arba bet kokį labai sunkų nusikaltimą ar nusikalstamą veiką dėl tarnybos paslapties pagrobimo, kitokio neteisėto įgijimo ar atskleidimo;

6) turi teistumą už sunkų ar apysunkį nusikaltimą;

7) įstatymų nustatyta tvarka yra pripažintas neveiksniu ar ribotai veiksniu;

8) dėl Lietuvos Respublikai priešiškų interesų yra bendradarbiavęs ar palaiko ryšius su kitos valstybės specialiąja tarnyba arba su asmenimis, bendradarbiaujančiais su kitos valstybės specialiąja tarnyba;

9) palaiko ryšius su asmenimis, priklausančiais organizuotoms nusikalstamoms grupėms arba nusikalstamiems susivienijimams;

10) dalyvauja neregistruotos religinės bendruomenės, politinės organizacijos, jų darinių veikloje;

11) sąmoningai nuslėpė arba jo kandidatūrą tikrinančioms institucijoms pateikė melagingus biografijos faktus arba kitus duomenis apie save, savo ryšius bei aplinką, galinčius turėti įtakos sprendimo dėl leidimo dirbti ar susipažinti su įslaptinta informacija, asmens patikimumo pažymėjimo išdavimo priėmimui;

12) įstatymų ar kitų teisės aktų nustatyta tvarka buvo atleistas iš pareigų dėl darbo su įslaptinta informacija tvarkos pažeidimo ar už tokius pažeidimus jam buvo panaikintas leidimas dirbti su įslaptinta informacija ar asmens patikimumo pažymėjimas;

13) yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas;

14) yra tas, kuriam taikomos prevencinio poveikio priemonės pagal Organizuoto nusikalstamumo užkardymo įstatymą;

15) gauna pajamų iš kitų valstybių karinių ar specialiųjų tarnybų, jeigu tai nėra numatyta Lietuvos Respublikos tarptautinėse sutartyse ar susitarimuose;

16) negali pagrįsti savo turto, kurį valdo, naudoja ar kuriuo disponuoja, įgijimo teisėtumo ir jo gyvenimo lygis neatitinka realių pajamų;

17) piktnaudžiauja alkoholiu, vartoja narkotines, psichotropines ar kitas psichiką veikiančias medžiagas arba nustatomos kitos asmeninės ir dalykinės savybės, dėl kurių jis netinka darbui su įslaptinta informacija;

18) turi psichinės veiklos sutrikimų ar kitų sveikatos būklės sutrikimų, galinčių riboti jo gebėjimus, neigiamai veikti jo veiksmus.

3. Asmenims, turintiems leidimus ar asmens patikimumo pažymėjimus, suteikiančius teisę dirbti ar susipažinti su informacija, žymima aukštesnio laipsnio slaptumo žyma, atskiras leidimas ar patikimumo pažymėjimas dirbti ar susipažinti su informacija, žymima žemesnio laipsnio slaptumo žyma, nereikalingas.

4. Asmeniui prireikus dirbti ar susipažinti su įslaptinta informacija, žymima aukštesne slaptumo žyma, negu asmeniui yra išduotas leidimas arba asmens patikimumo pažymėjimas, jo kandidatūra tikrinama iš naujo.

5. Asmens patikimumo pažymėjimas ir leidimas dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma „Visiškai slaptai“, išduodamas ne ilgesniam kaip 5 metų terminui, o su įslaptinta informacija, žymima slaptumo žymomis „Slaptai“, „Konfidencialiai“ – ne ilgesniam kaip 10 metų terminui. Šis terminas skaičiuojamas nuo Valstybės saugumo departamento sutikimo išduoti tokį leidimą pasirašymo dienos arba nuo kandidatūros tikrinimą atlikusios institucijos išvados pateikimo dienos, kai leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas išduodamas slaptiesiems operatyvinės veiklos dalyviams, įslaptintiems žvalgybos tarnautojams ir žvalgybos slaptiesiems bendradarbiams.

6. Likus 6 mėnesiams iki leidimo dirbti ar susipažinti su įslaptinta informacija ar asmens patikimumo pažymėjimo galiojimo termino pabaigos, asmuo tikrinamas papildomai. Asmuo gali būti pakartotinai tikrinamas ir nesibaigus šiame straipsnyje nustatytiems terminams, jeigu kyla įtarimas, kad atsirado šio straipsnio 2 dalyje numatytų aplinkybių. Pakartotinio patikrinimo metu paslapčių subjekto vadovo sprendimu asmeniui gali būti uždrausta dirbti su įslaptinta informacija.

7. Sprendimą dėl leidimo dirbti ar susipažinti su įslaptinta informacija neišdavimo, asmens patikimumo pažymėjimo neišdavimo, Valstybės saugumo departamento prieštaravimą, kad asmeniui būtų išduotas toks leidimas, taip pat kandidatūrą tikrinančių institucijų sprendimą nutraukti kandidatūros tikrinimą, nustačius šio straipsnio 2 dalyje nurodytas aplinkybes, per 30 darbo dienų nuo tokio sprendimo gavimo dienos pats asmuo arba paslapčių subjektas turi teisę apskųsti Paslapčių apsaugos koordinavimo komisijai. Prireikus ši komisija įpareigoja kandidatūros tikrinimą atlikusias institucijas surinkti ir pateikti papildomus duomenis apie tokį asmenį. Paslapčių apsaugos koordinavimo komisijos sprendimas paslapčių subjektui yra privalomas.

8. Asmenims, kurių darbas susijęs su tarnybos paslaptį sudarančios informacijos, žymimos slaptumo žyma „Riboto naudojimo“, naudojimu ar tokios informacijos apsauga, teisę dirbti ar susipažinti su tokia informacija suteikia paslapčių subjektas. Valstybės saugumo departamento sutikimo nereikia. Teisės dirbti ar susipažinti su tokia informacija suteikimo tvarką nustato paslapčių subjektai, vadovaudamiesi Paslapčių apsaugos koordinavimo komisijos patvirtintais bendraisiais principais.“

7. Taigi pagal šioje konstitucinės justicijos byloje ginčijamą Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktą leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas neišduodamas, jeigu yra bent viena iš šių aplinkybių:

– asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką;

– asmens atžvilgiu dėl tyčinės nusikalstamos veikos atliekamas ikiteisminis tyrimas;

– asmens atžvilgiu dėl tyčinės nusikalstamos veikos atliekamas operatyvinis tyrimas.

8. Šioje konstitucinės justicijos byloje ginčijamas Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas aiškintinas kartu su kitomis šio įstatymo nuostatomis.

8.1. Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 1 dalies 4 punkte nustatyta, kad asmeniui, pretenduojančiam gauti leidimą dirbti arba susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą, toks leidimas ar pažymėjimas išduodamas, jeigu tikrinimo metu surinkti faktai nekelia abejonių dėl asmens patikimumo ar lojalumo Lietuvos valstybei.

Taigi Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 1 dalies 4 punkte yra įtvirtintas bendrasis personalo patikimumo reikalavimas, kad leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą gali turėti tik toks asmuo, kurio patikimumas ir lojalumas Lietuvos valstybei nekelia abejonių. Atsižvelgiant į tai, šios konstitucinės justicijos bylos kontekste pažymėtina, kad ginčijamas Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas yra skirtas šiam bendrajam personalo patikimumo reikalavimui užtikrinti.

8.2. Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 15 straipsnio 1 dalyje nustatyta, kad eiti pareigas, susijusias su Lietuvos Respublikos įslaptintos informacijos, žymimos slaptumo žymomis „Visiškai slaptai“, „Slaptai“ arba „Konfidencialiai“ ar jų atitikmenimis, naudojimu ar tokios informacijos apsauga gali tik atitinkamus leidimus dirbti ar susipažinti su įslaptinta informacija turintys asmenys, o eiti pareigas, susijusias su užsienio valstybių ar tarptautinių organizacijų įslaptintos informacijos, žymimos slaptumo žymų „Visiškai slaptai“, „Slaptai“ arba „Konfidencialiai“ atitikmenimis, naudojimu ar tokios informacijos apsauga, gali tik atitinkamus asmens patikimumo pažymėjimus turintys asmenys.

Taigi šios konstitucinės justicijos bylos kontekste pažymėtina, kad leidimo dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimo turėjimas yra būtina specialioji sąlyga asmeniui eiti pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar apsauga.

9. Apibendrinant Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkte nustatytą teisinį reguliavimą kitų minėtų šio įstatymo nuostatų kontekste pažymėtina, jog juo siekiama užti-

krinti bendrąjį personalo patikimumo reikalavimą, kad leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą gali turėti tik toks asmuo, kurio patikimumas ir lojalumas Lietuvos valstybei nekelia abejonių: šiame punkte nurodytos aplinkybės, kurios kelia abejonių dėl asmens, siekiančio eiti pareigas valstybės tarnyboje, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, patikimumo ar lojalumo Lietuvos valstybei, – asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas. Esant kuriai nors iš šių aplinkybių, asmeniui negali būti išduotas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas. Todėl kol yra kuri nors iš Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkte nurodytų aplinkybių, asmuo, siekiantis eiti pareigas valstybės tarnyboje, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, negali būti skiriamas į tokias pareigas.

10. Minėta, kad šioje konstitucinės justicijos byloje pareiškėjas ginčija ir Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktą tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas atsiradus arba paaiškėjus šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytoms aplinkybėms.

Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnyje „Leidimo dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimo panaikinimas“ nustatyta:

„1. Leidimas dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimas panaikinamas, jeigu:

1) asmuo atsisako arba netenka Lietuvos Respublikos pilietybės;

2) asmuo daugiau negu vieną kartą pažeidė nustatytą darbo su įslaptinta informacija tvarką arba dėl šiurkštaus šios tvarkos pažeidimo kilo grėsmė, kad įslaptinta informacija gali būti prarasta ar neteisėtai atskleista;

3) su paslapčių subjektu nutraukiami darbo (tarnybos) santykiai ar pasibaigia renkamų arba skiriamų į pareigas asmenų įgaliojimų laikas;

4) atsiranda ar paaiškėja kuri nors iš aplinkybių, nurodytų šio Įstatymo 16 straipsnio 2 dalyje.

2. Paslapčių subjektas savo iniciatyva arba Valstybės saugumo departamento motyvuotu teikimu panaikina leidimą dirbti ar susipažinti su įslaptinta informacija. Apie priimtą sprendimą panaikinti asmeniui išduotą leidimą dirbti ar susipažinti su įslaptinta informacija paslapčių subjektas per 10 darbo dienų raštu praneša Valstybės saugumo departamentui.

3. Asmens, kuriam panaikintas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, prašymu paslapčių subjektas turi raštu nurodyti leidimo dirbti ar susipažinti su įslaptinta informacija panaikinimo motyvus.

4. Asmens patikimumo pažymėjimą savo iniciatyva ar Valstybės saugumo departamento arba paslapčių subjekto motyvuotu teikimu panaikina Paslapčių apsaugos koordinavimo komisija.

5. Sprendimą dėl leidimo dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimo panaikinimo per 30 darbo dienų nuo tokio sprendimo gavimo dienos asmuo arba paslapčių subjektas, gavęs Valstybės saugumo departamento motyvuotą teikimą dėl leidimo panaikinimo, turi teisę apskųsti Paslapčių apsaugos koordinavimo komisijai. Prireikus ši komisija įpareigoja kandidatūros tikrinimą atlikusias institucijas surinkti ir pateikti papildomų duomenų apie tokį asmenį. Paslapčių apsaugos koordinavimo komisijos sprendimas paslapčių subjektui yra privalomas.

6. Leidimo dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimo panaikinimas neatleidžia asmens nuo įsipareigojimo neatskleisti tarnybos metu sužinotos įslaptintos informacijos, taip pat nuo atsakomybės už tokios informacijos atskleidimą.“

11. Taigi pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktą asmeniui išduotas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas, jeigu atsiranda arba paaiškėja *inter alia* bent viena iš šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytų aplinkybių:

– asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką;

– asmens atžvilgiu dėl tyčinės nusikalstamos veikos atliekamas ikiteisminis tyrimas;

– asmens atžvilgiu dėl tyčinės nusikalstamos veikos atliekamas operatyvinis tyrimas.

12. Minėta, kad šioje konstitucinės justicijos byloje Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktas pareiškėjo ginčijamais aspektais neatsiejamas nuo šio įstatymo 16 straipsnio 2 dalies 13 punkto. Todėl, kaip ir Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas, ginčijamos šio įstatymo 18 straipsnio 1 dalies 4 punkto nuostatos aiškintinos kartu su šio įstatymo 16 straipsnio 1 dalies 4 punktu ir 15 straipsnio 1 dalimi.

12.1. Minėta, kad Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 1 dalies 4 punktas įtvirtina bendrąjį personalo patikimumo reikalavimą, kad leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą gali turėti tik toks asmuo, kurio patikimumas ir lojalumas Lietuvos valstybei nekelia abejonių. Taip pat minėta, kad Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas yra skirtas bendrajam personalo patikimumo reikalavimui užtikrinti.

Vadinasi, Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatyto teisinio reguliavimo tikslas taip pat yra užtikrinti bendrąjį personalo patikimumo reikalavimą, kad leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą gali turėti tik toks asmuo, kurio patikimumas ir lojalumas Lietuvos valstybei nekelia abejonių. Tačiau, kitaip nei Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas, šio įstatymo 18 straipsnio 1 dalies 4 punktas yra susijęs ne su asmenimis, siekiančiais eiti

pareigas valstybės tarnyboje, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, o su asmenimis, kurie jau eina tokias pareigas, t. y. jau turi leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą. Kitaip tariant, Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktas reguliuoja tokio leidimo ar pažymėjimo panaikinimą ir nustato, kad jis turi būti panaikintas *inter alia* atsiradus arba paaiškėjus kuriai nors iš šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytų aplinkybių.

12.2. Minėta, kad pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 15 straipsnio 1 dalį leidimo dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimo turėjimas yra būtina sąlyga eiti pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar apsauga.

Atsižvelgiant į tai pažymėtina, kad pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktą panaikinus leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą, *inter alia* kai paaiškėja arba atsiranda kuri nors iš šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytų aplinkybių, turėjęs tokį leidimą ar pažymėjimą asmuo nebeatitinka būtinos specialiosios sąlygos pareigoms valstybės tarnyboje eiti, susijusioms su įslaptintos informacijos naudojimu ar apsauga.

13. Ginčijamas Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytas teisinis reguliavimas aiškintinas ir šio įstatymo 16 straipsnio 6 dalies kontekste. Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 6 dalyje *inter alia* nustatyta, kad asmuo gali būti pakartotinai tikrinamas, jeigu kyla įtarimas, kad atsirado šio straipsnio 2 dalyje numatytų aplinkybių.

Kiek tai susiję su ginčijamu Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytu teisiniu reguliavimu, toks asmens pakartotinis tikrinimas pagal šio įstatymo 16 straipsnio 6 dalį būtų galimas tik norint nustatyti, ar nėra 16 straipsnio 2 dalies 13 punkte nurodytų aplinkybių, t. y. ar asmuo nėra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos nėra atliekamas ikiteisminis ar operatyvinis tyrimas. Tačiau tokio patikrinimo metu nustačius, kad yra kuri nors iš šių aplinkybių, pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktą visais atvejais leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas turi būti panaikintas be papildomo asmens, kuriam toks leidimas ar pažymėjimas buvo išduotas, tikrinimo.

14. Šios konstitucinės justicijos bylos kontekste ginčijama Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkto nuostata taip pat aiškintina kartu su Vidaus tarnybos statute nustatytu teisiniu reguliavimu.

Vidaus tarnybos statuto 53 straipsnio 1 dalies 17 punkte nustatyta:

„Pareigūnas atleidžiamas iš vidaus tarnybos:

<…>

17) kai jam įstatymų nustatyta tvarka atimamos specialiosios teisės, susijusios su jo tiesioginių pareigų atlikimu.“

Taigi Vidaus tarnybos statuto 53 straipsnio 1 dalies 17 punkte numatytas pareigūno atleidimo iš vidaus tarnybos pagrindas – kai jam įstatymų nustatyta tvarka atimama specialioji teisė, būtina jo tiesioginėms pareigoms atlikti. Vidaus tarnybos pareigūnams, kurių pareigos susijusios su įslaptintos informacijos naudojimu ar jos apsauga, tokia specialioji teisė yra teisė dirbti ar susipažinti su įslaptinta informacija, nes, kaip minėta, Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 15 straipsnio 1 dalyje nustatyta, kad eiti pareigas, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, gali tik leidimus dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimus turintys asmenys. Toks leidimas ar pažymėjimas patvirtina šią tokioms pareigoms eiti būtiną specialiąją teisę (Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 2 straipsnio 15 ir 16 dalys).

Vadinasi, vidaus tarnybos pareigūnui, kurio pareigos susijusios su įslaptintos informacijos naudojimu ar jos apsauga, panaikinus leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktą, *inter alia* kai atsiranda arba paaiškėja kuri nors iš šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytų aplinkybių (asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas), pareigūnas turi būti atleistas iš vidaus tarnybos pagal Vidaus tarnybos statuto 53 straipsnio 1 dalies 17 punktą.

15. Pažymėtina, kad Vidaus tarnybos statuto 56 straipsnio 1 dalyje nustatyta:

„Esant šio Statuto 53 straipsnio 1 dalies 2–10, 13, 14 ir 17 punktuose išvardytiems atleidimo pagrindams, pareigūnas atleidžiamas iš vidaus tarnybos kitą dieną po to, kai atsiranda ar nustatomas faktas (aplinkybė), dėl kurio pareigūnas nebegali tęsti tarnybos. Esant šiems pagrindams, pareigūną galima atleisti iš vidaus tarnybos ir jo laikinojo nedarbingumo bei atostogų metu.“

Taigi pagal Vidaus tarnybos statuto 56 straipsnio 1 dalį vidaus tarnybos pareigūnas, kurio pareigos susijusios su įslaptintos informacijos naudojimu ar jos apsauga, turi būti atleistas iš tarnybos kitą dieną po to, kai jam Valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka panaikinamas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas. Vidaus tarnybos statute, *inter alia* jo 56 straipsnio 6 dalyje, nėra nustatyta, kad asmuo, netekęs jo tiesioginėms pareigoms atlikti būtinos specialiosios teisės (šios konstitucinės justicijos bylos kontekste – teisės dirbti ar susipažinti su įslaptinta informacija), jeigu yra galimybė, turi būti perkeltas į lygiavertes pareigas arba jo sutikimu – į žemesnes pareigas, kurioms atlikti specialioji teisė nėra būtina.

16. Apibendrinant ginčijamą Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytą teisinį reguliavimą kitų minėtų šio įstatymo ir Vidaus tarnybos statuto nuostatų kontekste pažymėtina, kad:

– Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktu siekiama užtikrinti bendrąjį personalo pati-

kimumo reikalavimą, kad leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą gali turėti tik toks asmuo, kurio patikimumas ir lojalumas Lietuvos valstybei nekelia abejonių: jame nurodytos aplinkybės, kurios kelia abejonių dėl asmens, einančio pareigas valstybės tarnyboje, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija ar asmens patikimumo pažymėjimas, patikimumo ar lojalumo Lietuvos valstybei, *inter alia* tai yra aplinkybės, nurodytos šio įstatymo 16 straipsnio 2 dalies 13 punkte (asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas);

– visais atvejais, kai atsiranda arba paaiškėja kuri nors iš Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkte nurodytų aplinkybių (asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas), pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktą asmeniui turi būti panaikintas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas; asmuo, kuris yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, negali būti pakartotinai tikrinamas dėl jo patikimumo ir lojalumo Lietuvos valstybei, tokio tikrinimo metu uždraudžiant jam dirbti su įslaptinta informacija;

– pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktą asmeniui panaikinus leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą, turėjęs tokį leidimą arba pažymėjimą asmuo nebeatitinka būtinos specialiosios sąlygos pareigoms valstybės tarnyboje eiti, susijusioms su įslaptintos informacijos naudojimu ar jos apsauga; kai toks asmuo yra vidaus tarnybos pareigūnas, jis turi būti atleistas iš vidaus tarnybos pagal Vidaus tarnybos statuto 53 straipsnio 1 dalies 17 punktą (jam įstatymų nustatyta tvarka atėmus specialiąją teisę, susijusią su jo tiesioginių pareigų atlikimu).

17. Šioje konstitucinės justicijos byloje taip pat ginčijama Vidaus tarnybos statuto 28 straipsnio (2007 m. gegužės 15 d. redakcija) atitiktis Konstitucijai tiek, kiek jame nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas.

18. Seimas 2003 m. balandžio 29 d. priėmė Lietuvos Respublikos vidaus tarnybos statuto patvirtinimo įstatymą, kuris įsigaliojo 2003 m. gegužės 1 d. Šio įstatymo 1 straipsniu „Vidaus tarnybos statuto patvirtinimas“ buvo patvirtintas Vidaus tarnybos statutas.

Vidaus tarnybos statute yra nustatyti vidaus tarnybos principai, vidaus tarnybos sistemos pareigūnų statusas, priėmimas į tarnybą ir atleidimas, priėmimas į vidaus reikalų profesinio mokymo įstaigas ir mokymasis jose, pareigūnų atsa-

komybė, paskatinimai, socialinės ir kitos garantijos, profesinių sąjungų veiklos vidaus reikalų statutinėse įstaigose ypatumai, taip pat kitų valstybės tarnautojų priėmimo į tarnybą vidaus reikalų statutinėse įstaigose ypatumai (Vidaus tarnybos statuto 1 straipsnis).

19. Seimas 2007 m. gegužės 15 d. priėmė Lietuvos Respublikos vidaus tarnybos statuto 14 ir 28 straipsnių pakeitimo ir papildymo įstatymą, kuris įsigaliojo 2007 m. gegužės 29 d. Šiuo įstatymu įstatymų leidėjas pakeitė ir papildė *inter alia* Vidaus tarnybos statuto 28 straipsnį „Pareigūno nušalinimas nuo pareigų“, *inter alia* papildė šį straipsnį nauja 3 dalimi, kurioje numatyta, kad pareigūnas gali būti nušalintas nuo pareigų Baudžiamojo proceso kodekso nustatyta tvarka, jeigu pradedamas ikiteisminis tyrimas.

20. Vidaus tarnybos statuto 28 straipsnyje (2007 m. gegužės 15 d. redakcija) „Pareigūno nušalinimas nuo pareigų“ nustatyta:

„1. Tarnybos metu apsvaigusį nuo alkoholio, narkotinių, psichotropinių ar kitų svaigiųjų medžiagų pareigūną jo tiesioginis vadovas nušalina nuo pareigų tos dienos likusiam darbo laikui.

2. Tarnybinio patikrinimo metu pareigūnas gali būti nušalinamas nuo pareigų vadovo, turinčio teisę skirti į pareigas, įsakymu, tačiau ne ilgiau kaip 3 mėnesiams. Į šį terminą neįskaitomas pareigūno ligos ar atostogų laikas.

3. Jeigu pradedamas ikiteisminis tyrimas, pareigūnas gali būti nušalintas nuo pareigų Baudžiamojo proceso kodekso nustatyta tvarka.

4. Jei pareigūnas nušalinamas nuo pareigų, taip pat tais atvejais, kai nušalinamas Baudžiamojo proceso kodekso nustatyta tvarka, nušalinimo nuo pareigų laikotarpiu pareigūnui darbo užmokestis nemokamas. Šiais atvejais pareigūnui netaikomi šio Statuto 24 straipsnio 3 punkte nustatyti apribojimai.

5. Šio straipsnio 1, 2, 3 ir 4 dalyse nustatyta tvarka nušalintas nuo pareigų pareigūnas nuo nušalinimo momento grąžina pareigūno pažymėjimą, specialų ženklą, tarnybinį šaunamąjį ginklą, specialiąsias priemones ir sprogmenis vadovui, turinčiam teisę skirti į pareigas, arba jo įgaliotam pareigūnui, taip pat perduoda jam patikėtus tarnybinius dokumentus, inventorių, kitas darbo priemones.

6. Tarnybinio patikrinimo metu nustačius, kad pareigūnas nepadarė tarnybinio nusižengimo, kad nėra įstatymo nustatyta tvarka pripažintas kaltu dėl administracinio teisės pažeidimo ar nusikalstamos veikos padarymo, taip pat tais atvejais, kai nustatoma, kad pareigūnas padarė tarnybinį nusižengimą, tačiau tarnybinei nuobaudai paskirti yra pasibaigęs senaties terminas, jis toliau eina pareigas ir per 5 darbo dienas nuo tada, kai vėl pradėjo eiti pareigas, jam išmokamas darbo užmokestis už laikotarpį, kurį jis buvo nušalintas nuo pareigų, taip pat delspinigiai už šią sumą, apskaičiuoti Vyriausybės nustatyta tvarka.

7. Laikotarpis, kurį pareigūnas buvo nušalintas nuo pareigų, į vidaus tarnybos stažą neįskaitomas, išskyrus atvejus, kai tarnybinio patikrinimo metu pripažįstama, kad pareigūnas nepadarė tarnybinio nusižengimo, kad nėra įstatymo nustatyta tvarka pripažintas kaltu dėl administracinio teisės pažeidimo ar nusikalstamos veikos padarymo, taip pat tais atvejais, kai nustatoma, kad pareigūnas padarė tarnybinį nusižengimą, tačiau tarnybinei nuobaudai paskirti yra pasibaigęs senaties terminas.

8. Žymos apie sprendimus nušalinti pareigūną nuo pareigų įtraukiamos į pareigūno tarnybos bylą.“

21. Taigi Vidaus tarnybos statuto 28 straipsnyje (2007 m. gegužės 15 d. redakcija) nustatyti šie vidaus tarnybos pareigūno nušalinimo nuo pareigų atvejai:

– tarnybos metu dėl apsvaigimo nuo alkoholio, narkotinių, psichotropinių ar kitų svaigiųjų medžiagų – tiesioginio vadovo sprendimu;

– tarnybinio patikrinimo metu – vadovo, turinčio teisę skirti į pareigas, įsakymu; pagal Vidaus tarnybos statuto 26 straipsnio 6 dalį tarnybinis patikrinimas atliekamas esant duomenų apie pareigūno padarytą tarnybinį nusižengimą;

– pradėjus ikiteisminį tyrimą – Baudžiamojo proceso kodekso nustatyta tvarka.

Pažymėtina, kad kitų vidaus tarnybos pareigūno nušalinimo nuo pareigų atvejų Vidaus tarnybos statute nenumatyta.

Šiame kontekste paminėtinas Baudžiamojo proceso kodekso 157 straipsnio 4 dalyje nustatytas dar vienas laikino nušalinimo nuo pareigų atvejis: bylą perdavus į teismą, teismas, kurio žinioje byla yra, gali spręsti laikino jo nušalinimo nuo pareigų klausimą.

22. Šios konstitucinės justicijos bylos kontekste Vidaus tarnybos statuto 28 straipsnyje nustatytas teisinis reguliavimas aiškintinas kartu su Baudžiamojo proceso kodekso 157 straipsniu „Laikinas nušalinimas nuo pareigų ar laikinas teisės užsiimti tam tikra veikla sustabdymas“ (2010 m. rugsėjo 21 d. redakcija), kuriame nustatyta:

„1. Nusikalstamos veikos tyrimo metu ikiteisminio tyrimo teisėjas, gavęs prokuroro prašymą, nutartimi turi teisę laikinai nušalinti įtariamąjį nuo pareigų ar laikinai sustabdyti teisę užsiimti tam tikra veikla, jei tai būtina, kad būtų greičiau ir nešališkiau ištirta nusikalstama veika ar užkirsta įtariamajam galimybė daryti naujas nusikalstamas veikas. Nutartis laikinai nušalinti įtariamąjį nuo pareigų siunčiama įtariamojo darbdaviui vykdyti.

2. Laikinas nušalinimas nuo pareigų ar laikinas teisės užsiimti tam tikra veikla sustabdymas negali trukti ilgiau kaip šešis mėnesius. Prireikus šios priemonės taikymas gali būti pratęstas dar iki trijų mėnesių. Pratęsimų skaičius neribojamas.

3. Nutartį laikinai nušalinti įtariamąjį nuo pareigų ar laikinai sustabdyti teisę užsiimti tam tikra veikla, taip pat nutartį pratęsti šios priemonės taikymo terminą per septynias dienas nuo nutarties paskelbimo įtariamajam dienos įtariamasis ar jo gynėjas gali apskųsti aukštesniajam teismui. Šio teismo priimta nutartis yra galutinė ir neskundžiama.

4. Kai byla perduota į teismą, dėl laikino nušalinimo nuo pareigų ar laikino teisės užsiimti tam tikra veikla sustabdymo nusprendžia teismas, kurio žinioje yra byla.

5. Ikiteisminio tyrimo metu prokuroras, o perdavus bylą teismui – teismas privalo panaikinti laikiną nušalinimą nuo pareigų ar laikiną teisės užsiimti tam tikra veikla sustabdymą, kai ši priemonė pasidaro nebereikalinga.“

Taigi nors Vidaus tarnybos statuto 28 straipsnio (2007 m. gegužės 15 d. redakcija) 3 dalyje numatyta, kad pareigūnas gali būti nušalintas nuo pareigų Baudžiamojo proceso kodekso nustatyta tvarka pradėjus ikiteisminį tyrimą,

pagal Baudžiamojo proceso kodekso 157 straipsnio 1 dalį nuo pareigų laikinai gali būti nušalintas vidaus tarnybos pareigūnas, kuris yra įtariamas padaręs nusikalstamą veiką (įtariamasis). Tokiu atveju pareigūną laikinai nušalina nuo pareigų ne vadovas, turintis teisę skirti asmenį į pareigas, – jis nušalinamas nuo pareigų ikiteisminio tyrimo teisėjo nutartimi, gavus prokuroro prašymą. Tokiu nušalinimu siekiama ne užtikrinti įslaptintos informacijos apsaugą, o greičiau ir nešališkiau ištirti nusikalstamą veiką ar užkirsti galimybę daryti naujas nusikalstamas veikas.

23. Šios konstitucinės justicijos bylos kontekste apibendrinant Vidaus tarnybos statuto 28 straipsnyje (2007 m. gegužės 15 d.) nustatytą reguliavimą pažymėtina, kad šiame straipsnyje nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, taip pat nėra numatytas joks kitas vidaus tarnybos pareigūno nušalinimo nuo pareigų atvejis prireikus užtikrinti įslaptintos informacijos apsaugą.

Šiame kontekste taip pat pažymėtina, kad vidaus reikalų įstaiga, pagal Vidaus tarnybos statuto 2 straipsnio 3 dalį apibrėžiama kaip valstybės politiką visuomenės saugumo srityje įgyvendinantis Vidaus reikalų ministerijos valdymo srities viešasis juridinis asmuo, kurio pareigūnų tarnyba organizuojama statutiniais pagrindais, kartu yra ir paslapčių subjektas, kuris pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 2 straipsnio 8 dalį (2010 m. gruodžio 14 d. redakcija) *inter alia* apibrėžiamas kaip valstybės institucija, kurios veikla susijusi su informacijos įslaptinimu, išslaptinimu, įslaptintos informacijos naudojimu ir (ar) apsauga. Taigi vidaus reikalų įstaigos vadovas, turintis teisę skirti asmenį į pareigas, kartu yra ir paslapčių subjekto vadovas, kuris pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 12 straipsnio 2 dalį atsako už bendrą įslaptintos informacijos apsaugos organizavimą ir būklę.

IV

1. Pažymėtina, kad iš įstatymų leidėjo ketinimų, užfiksuotų *travaux préparatoires*, matyti, kad Valstybės ir tarnybos paslapčių įstatymas (2003 m. gruodžio 16 d. redakcija) buvo priimtas įgyvendinant NATO ir ES teisės aktus, reglamentuojančius įslaptintos informacijos apsaugą, *inter alia* personalo patikimumo standartus.

2. Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) priede yra nurodytas įgyvendinamas ES teisės aktas – ES Tarybos 2001 m. kovo 19 d. sprendimas 2001/264/EB dėl Europos Sąjungos Tarybos saugumo nuostatų (OL *2004 m. specialusis leidimas*, 1 sk., 3 t., p. 263–328).

Šiuo ES Tarybos sprendimu patvirtintuose Europos Sąjungos Tarybos saugumo nuostatuose *inter alia* buvo įtvirtinta, jog saugumo priemonės turi būti tokios, kad leistų nustatyti asmenis, kurių būklė gali kelti grėsmę įslaptintos informacijos ir svarbios įrangos, kurioje laikoma įslaptinta informacija, saugu-

mui, ir suteiktų galimybę tokius asmenis nušalinti ar atleisti.

Europos Sąjungos Tarybos saugumo nuostatuose taip pat buvo numatyta, kad išduodant leidimus naudotis informacija, pažymėta ES KONFIDENCIALIAI arba aukštesnio laipsnio slaptumo žyma, asmenys turi būti tinkamai patikrinami. Toks tikrinimas turi leisti nustatyti: ar tie asmenys yra *inter alia* neabejotinai lojalūs; ar jie yra tokio charakterio ir tokie diskretiški, kad nekyla abejonių dėl jų sąžiningumo tvarkant įslaptintą informaciją; ar jie negali pasiduoti užsienio arba kitų šaltinių spaudimui, pvz., dėl savo ankstesnės gyvenamosios vietos ar galinčių kelti grėsmę saugumui praeities ryšių. Personalo saugumo priemonės apima ir tvarką, užtikrinančią, 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 būtų pranešta atitinkamai institucijai; nustačius, kad toks asmuo kelia grėsmę saugumui, jam uždraudžiama vykdyti tokias užduotis arba jis nušalinamas nuo pareigų, kurias eidamas galėtų kelti grėsmę saugumui.

3. Pažymėtina, kad Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) priede nurodytas įgyvendinamas ES teisės aktas – 2001 m. kovo 19 d. ES sprendimas 2001/264/EB dėl Europos Sąjungos Tarybos saugumo nuostatų – buvo panaikintas ir pakeistas ES Tarybos 2011 m. kovo 31 d. sprendimu 2011/292/ES dėl Europos Sąjungos įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (OL L 141, 2011 5 27, p. 17–65), kuris įsigaliojo 2011 m. gegužės 27 d.

3.1. ES Tarybos 2011 m. kovo 31 d. sprendime 2011/292/ES dėl Europos Sąjungos įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių yra nustatyti pagrindiniai ES įslaptintos informacijos apsaugai užtikrinti skirti saugumo principai ir būtiniausi standartai, kurie taikomi ES Tarybai bei jos Generaliniam sekretoriatui ir kurių privalo laikytis valstybės narės, vadovaudamosi savo atitinkamais nacionaliniais įstatymais ir kitais teisės aktais, kad visi būtų tikri, jog yra užtikrinta lygiavertė ES įslaptintos informacijos apsauga (1 straipsnis).

Minėto sprendimo 7 straipsnyje „Personalo patikimumas“ yra nustatyti personalo patikimumo užtikrinimo priemonių pagrindai. *Inter alia* šiame straipsnyje nustatyta, kad personalo patikimumo tikrinimo procedūrų tikslas – nustatyti, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ES įslaptinta informacija; prieš leidžiant Tarybos Generaliniame sekretoriate dirbantiems asmenims, kuriems dėl jų pareigų gali reikėti susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ES įslaptinta informacija, susipažinti su tokia informacija, jų visų patikimumas turi būti atitinkamu lygiu patikrintas.

Tarybos 2011 m. kovo 31 d. sprendimo 2011/292/ES A priedėlyje personalo patikimumo tikrinimas apibrėžiamas kaip tikrinimo procedūros, kurias, vadovaudamasi valstybėje narėje galiojančiais įstatymais ir kitais teisės aktais, atlieka kompetentinga institucija, siekdama gauti užtikrinimą, kad nėra jokios nepalankios informacijos, kuri neleistų asmeniui išduoti nacionalinio arba ES asmens patikimumo pažymėjimo, suteikiančio galimybę susipažinti su tam tikro lygio ES įslaptinta informacija (CONFIDENTIEL UE/EU CONFIDENTIAL

arba aukštesnio laipsnio slaptumo žyma pažymėta informacija).

3.2. Tarybos 2011 m. kovo 31 d. sprendimo 2011/292/ES 7 straipsnio įgyvendinimo nuostatos išdėstytos šio sprendimo I priede. Jame *inter alia* nurodyti personalo patikimumo tikrinimo kriterijai, kuriais remiantis nustatoma, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti išduotas asmens patikimumo pažymėjimas, leidžiantis susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ES įslaptinta informacija. Atsižvelgiant į nacionalinius įstatymus ir kitus teisės aktus, tokie pagrindiniai kriterijai *inter alia* apima nagrinėjimą, ar asmuo buvo nuteistas už nusikalstamą veiką ar nusikalstamas veikas, atlieka ar atliko veiksmus, dėl kurių jį galima šantažuoti ar daryti jam spaudimą, savo elgesiu ar žodžiais pasirodė esąs nesąžiningas, nelojalus ar nepatikimas, gali patirti spaudimą (pvz., dėl vienos ar kelių ne ES pilietybių turėjimo arba dėl giminaičių ar artimų asmenų, kurie galėtų būti pažeidžiami dėl užsienio žvalgybos tarnybų, teroristų grupių ar kitų ardomojo pobūdžio organizacijų ar asmenų, kurių siekiai gali kelti grėsmę ES ir (arba) valstybių narių saugumo interesams, poveikio); vykdant patikimumo tikrinimą, atitinkamais atvejais, vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, taip pat gali būti svarbi informacija apie asmens finansinę padėtį ir sveikatą, sutuoktinio, sugyventinio ar artimo šeimos nario charakteris, elgesys ir gyvenimo aplinkybės.

Tarybos 2011 m. kovo 31 d. sprendimo 2011/292/ES I priede nustatytos taikytinos personalo patikimumo tikrinimo ir administracinės procedūros. Jame *inter alia* nustatyta, jog prireikus, vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, gali būti atliekami papildomi patikimumo patikrinimai, kad būtų surinkta visa svarbi informacija apie asmenį ir būtų pagrįsta arba paneigta nepalanki informacija. Jei sužinoma informacija apie tai, kad galiojantį ES asmens patikimumo pažymėjimą turintis asmuo kelia pavojų saugumui, laikantis atitinkamų taisyklių ir teisės aktų apie tai pranešama atitinkamai nacionalinei saugumo institucijai. Jei nepalanki informacija patvirtinama, ES asmens patikimumo pažymėjimas panaikinamas, o asmeniui neleidžiama susipažinti su ES įslaptinta informacija ir eiti pareigų, kurias eidamas jis galėtų susipažinti su ta informacija arba sukelti pavojų saugumui.

4. NATO įslaptintos informacijos apsaugos standartus *inter alia* nustato 1997 m. kovo 6 d. Šiaurės Atlanto Sutarties Šalių susitarimas dėl informacijos saugumo, sudarytas siekiant įgyvendinti Šiaurės Atlanto Sutarties 3 straipsnyje nustatytus NATO narių įsipareigojimus bendradarbiauti plėtojant kolektyvinį pajėgumą atremti ginkluotą užpuolimą. Šiaurės Atlanto Sutarties Šalių susitarimas dėl informacijos saugumo buvo ratifikuotas Seimo 2004 m. liepos 15 d. priimto Lietuvos Respublikos įstatymo „Dėl Šiaurės Atlanto Sutarties Šalių susitarimo dėl informacijos saugumo, NATO susitarimo dėl su gynyba susijusių išradimų, dėl kurių paduotos patento paraiškos, abipusės slaptumo apsaugos bei NATO susitarimo dėl techninės informacijos perdavimo gynybos tikslais ratifikavimo“ 1 straipsniu. Pagal šio įstatymo 3 straipsnio 2 dalį Šiaurės Atlanto Sutarties Šalių susitarimas dėl informacijos saugumo Lietuvos Respublikoje turi būti įgyvendinamas laikantis Šiaurės Atlanto Tarybos sprendimais nustatomų saugumo standartų ir kitų šių susitarimų įgyvendinimo tvarkos bei taikymo

reikalavimų.

4.1. Šiaurės Atlanto Sutarties Šalių susitarimo dėl informacijos saugumo 3 straipsnyje yra nustatyta pareiga Šalims užtikrinti tinkamą visų jų pilietybę turinčių asmenų, kurie, vykdydami tarnybines pareigas, turi arba gali susipažinti su informacija, žymima slaptumo žyma „Konfidencialiai“ ir aukštesnio laipsnio slaptumo žymomis, patikimumo patikrinimą prieš jiems pradedant eiti tokias pareigas; asmens patikimumo patikrinimo procedūros turi būti tokios, kad pagal jas būtų galima nustatyti, ar asmuo, atsižvelgiant į jo lojalumą ir patikimumą, gali susipažinti su įslaptinta informacija, nesukeldamas nepriimtino pavojaus saugumui.

4.2. Kituose NATO dokumentuose, priimtuose įgyvendinant Šiaurės Atlanto Sutarties Šalių susitarimą dėl informacijos saugumo (*inter alia* NATO dokumente C-M(2002)49 „Saugumas Šiaurės Atlanto Sutarties Organizacijoje (NATO)“), *inter alia* nustatyta, kad personalo saugumo procedūros turi būti tokios, kad būtų vertinama, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su įslaptinta informacija be nepriimtinos rizikos saugumui, taip pat kad visi asmenys, kurie dėl savo pareigų privalo gauti informaciją, klasifikuojamą NATO CONFIDENTIAL ir aukštesnio lygio žyma, turi būti tinkamai ištirti, kad būtų pakankamai pasitikima jų tinkamumu prieiti prie tokios informacijos. Juose taip pat *inter alia* nustatyti pagrindiniai lojalumo ir patikimumo vertinimo kriterijai, kai sprendžiamas personalo saugumo leidimo klausimas. Pagal šiuos kriterijus nustatomi asmens reputacijos aspektai ar aplinkybės, galinčios kelti potencialias saugumo problemas. Jie *inter alia* apima informaciją apie tai, ar asmuo ir, prireikus atsižvelgiant į nacionalinės teisės aktus, jo sutuoktinis, sugyventinis ar artimas šeimos narys savo veiksmais ar kalbomis nedemonstravo nesąžiningumo, nelojalumo, nepatikimumo arba nerūpestingumo, ar jis nebuvo nuteistas už nusikalstamą veiką arba už veikas, rodančias recidyvizmo tendencijas, ar jis negali pasiduoti spaudimui per giminaičius ar artimus asmenis, kurie gali būti pažeidžiami dėl užsienio žvalgybų tarnybų, teroristų grupių ar kitų ardomojo pobūdžio organizacijų arba asmenų, kurių interesai gali kelti grėsmę NATO ir (ar) NATO valstybių saugumo interesams, įtakos. Personalo saugumo priemonės apima ir tvarką, kuri užtikrintų, kad, gavus tam tikram asmeniui nepalankios informacijos, būtų nustatyta, ar jis gali toliau turėti personalo saugumo leidimą; nustačius nepriimtiną riziką saugumui, personalo saugumo leidimas turi būti panaikintas, tam asmeniui turi būti atimta galimybė naudotis NATO įslaptinta informacija ir jis turi būti pašalintas iš pareigų, kurias eidamas galėtų kelti grėsmę saugumui.

5. Taigi NATO ir ES dokumentuose nustatyti įslaptintos informacijos apsaugos standartai yra panašūs. Apibendrinant šiuos standartus šios konstitucinės justicijos bylos kontekste pažymėtina, kad jie *inter alia* skirti užtikrinti, kad prieigą prie įslaptintos informacijos turėtų tik tie asmenys, kurių lojalumas ir patikimumas yra patikrintas ir nekelia jokių abejonių. Personalo saugumo procedūros turi būti tokios, kad būtų vertinama, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su įslaptinta informacija be nepriimtinos rizikos tokios informacijos saugumui. Pagrindiniai arba minimalūs kriterijai vertinant asmens lojalumą ir patikimumą nėra siejami tik su asmens

kalte padarius nusikalstamą veiką ar kitokį teisės pažeidimą; jie apima ir informaciją apie potencialias grėsmes saugumui: asmens savybes, veiklą bei kitas aplinkybes, liudijančias jo nesąžiningumą, nelojalumą, nepatikimumą ar neapdairumą, taip pat jo pažeidžiamumą per su juo susijusius artimus asmenis. Taikytinos saugumo priemonės taip pat turi būti tokios, kad leistų nustatyti tokius jau turinčius teisę dirbti ir susipažinti su įslaptinta informacija asmenis, kurių būklė gali kelti grėsmę įslaptintos informacijos saugumui, ir suteiktų galimybę tokius asmenis nušalinti ar atleisti. Gavus tam tikram asmeniui nepalankios informacijos turėtų būti patikrinta, ar tolesnis jo darbas su įslaptinta informacija nesukelia nepriimtinos rizikos tokios informacijos saugumui, o nustačius tokią riziką, asmeniui turi būti atimta galimybė naudotis įslaptinta informacija – jam turi būti uždraudžiama vykdyti užduotis, susijusias su įslaptinta informacija, jis nušalinamas nuo pareigų, kurioms vykdyti būtina įslaptinta informacija, arba iš tų pareigų atleidžiamas. Šiame kontekste paminėtina, jog svarbu, kad asmuo, kurio tolesnis darbas su įslaptinta informacija sudarytų nepriimtiną riziką tokios informacijos saugumui, negalėtų prieiti prie įslaptintos informacijos ir nebevykdytų atitinkamų pareigų. Tai gali būti pasiekiama įvairiomis teisinėmis priemonėmis, t. y. ne tik atleidžiant asmenį iš pareigų, bet ir taikant švelnesnes pagal savo pobūdį priemones – nušalinant nuo pareigų arba uždraudžiant vykdyti su įslaptinta informacija susijusias užduotis.

Pažymėtina ir tai, kad NATO ir ES dokumentai nustato pagrindinius arba minimalius (būtiniausius) personalo saugumo standartus, t. y. nacionalinėje teisėje gali būti numatyti ir papildomi bei griežtesni kriterijai, į kuriuos atsižvelgiant būtų vertinamas asmens lojalumas ir patikimumas, taip pat papildomas ir griežtesnes personalo saugumo užtikrinimo priemones.

V

Dėl Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkto atitikties Konstitucijos 31 straipsnio 1 daliai, 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

1. Minėta, kad šioje konstitucinės justicijos byloje pareiškėjas abejoja, ar Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas neprieštarauja Konstitucijos 31 straipsnio 1 daliai, 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

2. Kaip minėta, ginčijamame Valstybės ir tarnybos paslapčių įstatymo 16 straipsnio „Leidimo dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimo išdavimo sąlygos“ 2 dalies 13 punkte nustatyta:

„Leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas asmeniui neišduodamas, jeigu asmuo:

<...>

13) yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas."

3. Minėta, kad ginčijamame Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkte nurodytos aplinkybės, kurioms esant kyla abejonių dėl asmens, siekiančio eiti pareigas valstybės tarnyboje, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, patikimumo ar lojalumo Lietuvos valstybei ir asmeniui negali būti išduotas toks leidimas ar pažymėjimas.

4. Pareiškėjo nuomone, Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas prieštarauja *inter alia* Konstitucijos 31 straipsnio 1 dalyje įtvirtintam asmens nekaltumo prezumpcijos principui, nes asmuo negali būti laikomas padariusiu nusikalstamą veiką ir dėl tokios veikos jam negali būti neleidžiama eiti pareigų, susijusių su įslaptintos informacijos naudojimu ar jos apsauga, kol jo kaltumas nėra nustatytas įsiteisėjusiu teismo nuosprendžiu.

4.1. Šiame Konstitucinio Teismo nutarime pažymėta, kad asmenims, siekiantiems eiti ar einantiems pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, keliama specialioji sąlyga yra ypatingas ir nė kiek neabejotinas patikimumas ir lojalumas Lietuvos valstybei; ši sąlyga sietina su valstybės pasitikėjimu tokiu asmeniu.

4.2. Šiame Konstitucinio Teismo nutarime aiškinant Konstitucijos 31 straipsnio 1 dalyje įtvirtintą asmens nekaltumo prezumpcijos principą minėta, jog tai, kad asmuo nėra laikomas kaltu padaręs nusikalstamą veiką, kol jo kaltumas dėl tokios veikos nėra įstatymo nustatyta tvarka įrodytas ir pripažintas įsiteisėjusiu teismo nuosprendžiu, dar nereiškia, kad asmuo, siekiantis eiti ar einantis pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, būtinai yra vertas valstybės pasitikėjimo ir kad įstatymo įgaliotai valstybės institucijai negali kilti tam tikrų abejonių dėl asmens patikimumo ar lojalumo Lietuvos valstybei, kurias sukelia ne nustatytas jo kaltumas padarius nusikalstamą veiką, o tam tikros reikšmingos aplinkybės, *inter alia* susijusios su galbūt padaryta nusikalstama veika. Minėta ir tai, kad vertindama šias aplinkybes įstatymo įgaliota valstybės institucija nevykdo teisingumo ir nesprendžia asmens kaltumo padarius nusikalstamą veiką klausimo.

4.3. Taigi, sprendžiant leidimo dirbti ar susipažinti su įslaptinta informacija išdavimo klausimą, asmuo yra tikrinamas siekiant nustatyti, ar juo galima pasitikėti, t. y. ar nėra jokių abejonių dėl asmens patikimumo ar lojalumo Lietuvos valstybei, kad nebūtų sukelta grėsmės įslaptintos informacijos saugumui. Todėl Valstybės ir tarnybos paslapčių įstatymo reguliuojamuose santykiuose, kai sprendžiama dėl asmens patikimumo ir lojalumo Lietuvos valstybei, *inter alia* dėl leidimo dirbti ar susipažinti su įslaptinta informacija ar asmens patikimumo pažymėjimo išdavimo, nesprendžiamas asmens kaltumo padarius nusikalstamą veiką klausimas.

4.4. Atsižvelgiant į išdėstytus argumentus darytina išvada, kad Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2

dalies 13 punktas neprieštarauja Konstitucijos 31 straipsnio 1 daliai.

5. Pareiškėjo nuomone, Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas prieštarauja *inter alia* Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui, nes ginčijamu teisiniu reguliavimu nustatytas konstitucinės teisės į darbą apribojimas – neleidimas asmeniui eiti valstybės tarnautojo pareigų, susijusių su įslaptintos informacijos naudojimu ar apsauga, yra neproporcingas demokratinės visuomenės tikslui apsaugoti valstybę nuo galimos nusikalstamos veikos ar kitų pavojingų pažeidimų padarinių.

5.1. Minėta, kad Konstitucijos 33 straipsnio 1 dalyje įtvirtinta teisė lygiomis sąlygomis stoti į valstybės tarnybą sietina *inter alia* su Konstitucijos 48 straipsnio 1 dalyje įtvirtinta kiekvieno žmogaus teise laisvai pasirinkti darbą. Piliečio konstitucinė teisė lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą yra kiekvieno asmens konstitucinės teisės pasirinkti darbą atmaina.

5.2. Taip pat minėta, kad, sudarydamas teisines prielaidas įgyvendinti teisę laisvai pasirinkti darbą bei verslą (taigi ir stoti į valstybės tarnybą), įstatymų leidėjas turi įgaliojimus, atsižvelgdamas į darbo pobūdį, nustatyti teisės laisvai pasirinkti darbą įgyvendinimo sąlygas. Piliečių teisė stoti į Lietuvos Respublikos valstybės tarnybą nėra absoliuti.

5.3. Šiame Konstitucinio Teismo nutarime *inter alia* konstatuota, kad:

– asmenims, siekiantiems eiti ar einantiems pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, keliama specialioji sąlyga yra ypatingas ir nė kiek neabejotinas patikimumas ir lojalumas Lietuvos valstybei;

– įstatymų leidėjas turi plačią diskreciją reguliuodamas santykius, susijusius su valstybės ir tarnybos paslapčių apsauga, *inter alia* nustatydamas asmenų, siekiančių eiti ar einančių pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, patikimumo bei lojalumo Lietuvos valstybei kriterijus ir tokių asmenų patikrinimo procedūras;

– įstatymų leidėjas gali numatyti tokias įslaptintos informacijos apsaugos priemones, kurios leistų iš anksto užkirsti kelią grėsmėms įslaptintos informacijos saugumui ir kartu – grėsmėms valstybės interesams.

5.4. Pažymėtina, jog aplinkybės, kad asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, gali suponuoti asmens pažeidžiamumą, kartu kelti abejonių dėl jo patikimumo ar lojalumo Lietuvos valstybei.

5.5. Įstatymų leidėjas, ginčijamame Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkte nustatęs, jog leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas neišduodamas dėl to, kad asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, kitaip nei teigia pareiškėjas, siekė ne apsaugoti valstybę nuo galimos nusikalstamos veikos ar kitų pavojingų pažeidimų padarinių, o sudarė prielaidas, kad prieigos prie įslaptintos informacijos netu-

rėtų asmuo, dėl kurio patikimumo ar lojalumo Lietuvos valstybei yra abejonių. Todėl toks teisinis reguliavimas vertintinas kaip užkertantis kelią galimai žalai valstybės interesams, susijusiems su įslaptintos informacijos apsauga.

Šiame Konstitucinio Teismo nutarime konstatuota ir tai, kad su valstybės paslaptimis gali būti leidžiama susipažinti tik tokiam asmeniui, kurio veikla, savybės, ryšiai ir kt. negali duoti pagrindo nuogąstauti, kad, jam sužinojus valstybės paslaptį, kils grėsmė, juo labiau bus padaryta žalos svarbiems valstybės interesams.

5.6. Taigi Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkte nustatytu teisiniu reguliavimu, pagal kurį leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas asmeniui neišduodamas, jeigu asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, Konstitucijos 33 straipsnio 1 dalyje įtvirtinta piliečio teisė lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą, kartu ir Konstitucijos 48 straipsnio 1 dalyje įtvirtinta asmens teisė pasirinkti darbą nėra paneigiama ar varžoma labiau negu reikia teisėtiems ir visuomenei svarbiems tikslams pasiekti.

Atsižvelgiant į išdėstytus argumentus konstatuotina, kad Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punktas neprieštarauja Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

VI

Dėl Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkto tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas atsiradus arba paaiškėjus Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkte nurodytoms aplinkybėms, atitikties Konstitucijos 31 straipsnio 1 daliai, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

1. Minėta, kad šioje konstitucinės justicijos byloje pareiškėjas abejoja, ar Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktas tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas atsiradus arba paaiškėjus šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytoms aplinkybėms, neprieštarauja Konstitucijos 31 straipsnio 1 daliai, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

2. Minėta, kad ginčijamame Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio „Leidimo dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimo panaikinimas“ 1

dalies 4 punkte nustatyta:

„Leidimas dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimas panaikinamas, jeigu:

<...>

4) atsiranda ar paaiškėja kuri nors iš aplinkybių, nurodytų šio Įstatymo 16 straipsnio 2 dalyje.“

Kaip minėta, pareiškėjas ginčija šią Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkto nuostatą ne visa apimtimi, o tiek, kiek joje nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas atsiradus arba paaiškėjus šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytoms aplinkybėms.

3. Taip pat minėta, kad:

– Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytu teisiniu reguliavimu tiek, kiek jis yra susijęs su šio įstatymo 16 straipsnio 2 dalies 13 punktu, siekiama užtikrinti bendrąjį personalo patikimumo reikalavimą, kad leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą gali turėti tik toks asmuo, kurio patikimumas ir lojalumas Lietuvos valstybei nekelia abejonių: šiuo teisiniu reguliavimu nustatytos aplinkybės, kurios kelia abejonių dėl asmens, einančio pareigas valstybės tarnyboje, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, patikimumo ar lojalumo Lietuvos valstybei, – asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas;

– atsiradus arba paaiškėjus kuriai nors iš Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 13 punkte nurodytų aplinkybių (asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas), pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktą visais atvejais turi būti panaikintas asmeniui išduotas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas ir nėra numatyta, kad toks asmuo galėtų būti pakartotinai tikrinamas dėl jo patikimumo ir lojalumo Lietuvos valstybei;

– pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktą panaikinus leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą, turėjęs tokį leidimą arba pažymėjimą asmuo nebeatitinka būtinos specialiosios sąlygos, kad galėtų eiti valstybės tarnyboje pareigas, susijusias su įslaptintos informacijos naudojimu ar jos apsauga. Tokiu atveju vidaus tarnybos pareigūnas turi būti atleistas iš vidaus tarnybos pagal Vidaus tarnybos statuto 53 straipsnio 1 dalies 17 punktą (jam įstatymų nustatyta tvarka atėmus specialiąją teisę, susijusią su jo tiesioginių pareigų atlikimu).

4. Pareiškėjo nuomone, Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytas teisinis regu-

liavimas jo nurodyta apimtimi prieštarauja *inter alia* Konstitucijos 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“ ir konstituciniam teisinės valstybės principui, nes šis teisinis reguliavimas vertintinas kaip neproporcingas konstitucinės asmens laisvės pasirinkti darbą suvaržymas.

5. Šiame Konstitucinio Teismo nutarime minėta, kad Konstitucijos 48 straipsnio 1 dalyje įtvirtintos kiekvieno asmens konstitucinės teisės pasirinkti darbą atmaina yra Konstitucijos 33 straipsnio 1 dalyje įtvirtinta piliečio teisė lygiomis sąlygomis stoti į valstybės tarnybą. Taip pat minėta, kad Konstitucijos 33 straipsnio 1 dalies nuostata, įtvirtinanti piliečių teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą, neturi būti aiškinama tik lingvistiškai ir neturi būti suprantama tik kaip teisė stoti į valstybės tarnybą, t. y. tik kaip susijusi su asmens priėmimu į valstybės tarnybą; valstybės tarnybos santykiai apima ne tik santykius, susijusius su piliečio teisės lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą įgyvendinimu, bet ir santykius, susiklostančius piliečiui įstojus į valstybės tarnybą ir einant pareigas valstybės tarnyboje.

Atsižvelgdamas į tai, Konstitucinis Teismas tirs ir tai, ar pareiškėjo ginčijamas Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytas teisinis reguliavimas neprieštarauja Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“.

6. Minėta, kad pagal Konstituciją riboti žmogaus teises ir laisves galima, jeigu laikomasi šių sąlygų: tai daroma įstatymu; apribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti kitų asmenų teises ir laisves bei Konstitucijoje įtvirtintas vertybes, taip pat konstituciškai svarbius tikslus; apribojimais nėra paneigiama teisių ir laisvių prigimtis bei jų esmė; yra laikomasi konstitucinio proporcingumo principo.

Šiame Konstitucinio Teismo nutarime konstatuota, kad konstitucinio proporcingumo principo reikalavimas asmens teisių ir laisvių įstatymu neriboti labiau negu reikia teisėtiems ir visuomenei svarbiems tikslams pasiekti *inter alia* suponuoja reikalavimą įstatymų leidėjui nustatyti tokį teisinį reguliavimą, kuris sudarytų prielaidas pakankamai individualizuoti asmens teisių ir laisvių apribojimus: ribojantis asmens teises ir laisves įstatymo nustatytas teisinis reguliavimas turi būti toks, kad sudarytų prielaidas kiek įmanoma įvertinti individualią kiekvieno asmens situaciją ir, atsižvelgiant į visas svarbias aplinkybes, atitinkamai individualizuoti konkrečias tam asmeniui taikytinas ribojančias jo teises priemones.

7. Vertinant ginčijamą Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytą teisinį reguliavimą pažymėtina, kad juo siekiama konstituciškai svarbių tikslų – užtikrinti, kad pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, eitų tik tokie asmenys, kurių patikimumas ir lojalumas Lietuvos valstybei nekelia jokių abejonių, kartu užkirsti kelią galimoms grėsmėms įslaptintos informacijos saugumui ir su tokia informacija susijusiems valstybės interesams.

8. Minėta, pagal ginčijamą Valstybės ir tarnybos paslapčių įstatymo (2003 m.

gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytą teisinį reguliavimą visais atvejais, atsiradus arba paaiškėjus kuriai nors iš šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytų aplinkybių, t. y. kai asmuo traukiamas baudžiamojon atsakomybėn už bet kokią tyčinę nusikalstamą veiką arba jam dėl bet kokios tyčinės veikos atliekamas ikiteisminis ar operatyvinis tyrimas, leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas turi būti panaikintas be jokio papildomo asmens, kuriam toks leidimas ar pažymėjimas buvo išduotas, tikrinimo, ir šis asmuo nebegali toliau eiti pareigų valstybės tarnyboje, kurioms eiti būtinas toks leidimas ar pažymėjimas.

8.1. Kartu pažymėtina, kad asmuo gali būti traukiamas baudžiamojon atsakomybėn arba jam gali būti pradėtas ikiteisminis tyrimas dėl labai įvairių tyčinių nusikalstamų veikų. Jis gali būti traukiamas baudžiamojon atsakomybėn *inter alia* dėl nesunkių tyčinių nusikaltimų ir tyčinių baudžiamųjų nusižengimų, dėl kurių asmens teistumas pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 16 straipsnio 2 dalies 6 punktą nebūtų kliūtis išduoti leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą.

Taip pat pažymėtina, kad pagal Operatyvinės veiklos įstatymo 9 straipsnį operatyvinis tyrimas gali būti pradėtas ne tik tada, kai reikia imtis veiksmų vykdant valstybės paslapčių apsaugą, bet ir kitais atvejais, *inter alia* kai nusikalstamos veikos požymiai nėra nustatyti, bet turima informacijos apie rengiamą, daromą ar padarytą labai sunkų ar sunkų nusikaltimą arba apie tam tikrus apysunkius nusikaltimus, kai yra informacijos apie kitų valstybių specialiųjų tarnybų veiklą, kai turima informacijos apie veikas, keliančias grėsmę valstybės konstitucinei santvarkai, jos nepriklausomybei, ekonominiam saugumui, valstybės gynybinės galios užtikrinimui ar kitiems svarbiems nacionalinio saugumo interesams, t. y. pagrindas pradėti operatyvinį tyrimą dėl asmens galimos tyčinės nusikalstamos veikos gali būti nepatikrinta operatyvinė informacija apie tokią veiką.

Todėl, įstatymų leidėjui Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nenumačius galimybės vertinti reikšmingų aplinkybių, susijusių su konkrečiu atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos yra atliekamas ikiteisminis ar operatyvinis tyrimas ir kartu patikrinti asmens patikimumo ir lojalumo Lietuvos valstybei, yra sudaromos prielaidos atsirasti ir tokioms situacijoms, kai asmeniui panaikinamas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas ir dėl to asmuo netenka pareigų valstybės tarnyboje, kurioms eiti toks leidimas ar pažymėjimas yra būtinas, net ir tais atvejais, kai su asmens traukimu baudžiamojon atsakomybėn, ikiteisminiu ar operatyviniu tyrimu susijusios aplinkybės nėra tokios, kurios keltų abejonių dėl tokio asmens patikimumo ir lojalumo Lietuvos valstybei ir dėl kurių tolesnis asmens darbas su įslaptinta informacija galėtų kelti grėsmę tokios informacijos saugumui.

Taigi pagal ginčijamame Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytą teisinį reguliavimą galimi ir tokie atvejai, kai mažareikšmės aplinkybės būtų pagrindas

abejoti asmens patikimumu ar lojalumu Lietuvos valstybei ir dėl to asmuo netektų darbo valstybės tarnyboje.

8.2. Nors įstatymų leidėjas ir turi plačią diskreciją reguliuoti santykius, susijusius su valstybės ir tarnybos paslapčių apsauga, jis negali nustatyti tokio teisinio reguliavimo, kuris sudarytų prielaidas įstatymo įgaliotai valstybės institucijai, remiantis mažareikšmėmis aplinkybėmis, konstatuoti asmens, einančio pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, nepatikimumą ar nelojalumą Lietuvos valstybei ir dėl to asmeniui netekti darbo valstybės tarnyboje.

9. Taigi ginčijamas Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytas teisinis reguliavimas nesudaro prielaidų valstybės įgaliotai institucijai vertinti su asmens traukimu baudžiamojon atsakomybėn, ikiteisminiu ar operatyviniu tyrimu susijusių aplinkybių ir atitinkamai individualizuoti konkrečių tam asmeniui taikytinų priemonių, ribojančių jo teises; vienintelė priemonė, kuri taikoma visais atvejais, kai asmuo traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, yra leidimo dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimo panaikinimas ir paskesnis asmens atleidimas iš pareigų valstybės tarnyboje, kurioms eiti toks leidimas ar pažymėjimas yra būtinas.

Todėl konstatuotina, kad ginčijamas Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punkte nustatytas teisinis reguliavimas, pagal kurį nenumatyta galimybė vertinti, ar su asmens traukimu baudžiamojon atsakomybėn, ikiteisminiu ar operatyviniu tyrimu susijusios aplinkybės kelia tokių abejonių dėl asmens patikimumo ir lojalumo Lietuvos valstybei, kad tolesnis jo darbas su įslaptinta informacija keltų grėsmę tokios informacijos saugumui, neatitinka iš konstitucinio proporcingumo principo kylančio reikalavimo pakankamai individualizuoti asmens teisių ir laisvių apribojimus ir yra vertintinas kaip neproporcingas Konstitucijos 33 straipsnio 1 dalyje įtvirtintos piliečio teisės lygiomis sąlygomis stoti į valstybės tarnybą varžymas.

10. Atsižvelgiant į išdėstytus argumentus darytina išvada, kad Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktas tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas atsiradus arba paaiškėjus 16 straipsnio 2 dalies 13 punkte nurodytoms aplinkybėms, ir nenustatyta, kad prieš sprendžiant dėl tokio leidimo arba pažymėjimo panaikinimo atsiradus arba paaiškėjus šioms aplinkybėms asmens patikimumas ir lojalumas Lietuvos valstybei turi būti papildomai tikrinami siekiant nustatyti, ar tolesnis jo darbas nekeltų grėsmės įslaptintos informacijos saugumui, prieštarauja Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, konstituciniam teisinės valstybės principui.

11. Atsižvelgiant į tai, kad, kaip minėta, Konstitucijos 33 straipsnio 1 dalyje įtvirtinta piliečio teisė lygiomis sąlygomis stoti į valstybės tarnybą yra Konstitucijos 48 straipsnio 1 dalyje įtvirtintos kiekvieno asmens konstitucinės teisės

pasirinkti darbą atmaina, dėl tų pačių argumentų konstatuotina, kad Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktas tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas atsiradus arba paaiškėjus 16 straipsnio 2 dalies 13 punkte nurodytoms aplinkybėms, ir nenustatyta, kad prieš sprendžiant dėl tokio leidimo arba pažymėjimo panaikinimo atsiradus arba paaiškėjus šioms aplinkybėms asmens patikimumas ir lojalumas Lietuvos valstybei turi būti papildomai tikrinami siekiant nustatyti, ar tolesnis jo darbas su įslaptinta informacija nekeltų grėsmės tokios informacijos saugumui, prieštarauja ir Konstitucijos 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“.

12. Konstitucinis Teismas, šiame nutarime konstatavęs, kad Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktas tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas atsiradus arba paaiškėjus 16 straipsnio 2 dalies 13 punkte nurodytoms aplinkybėms, ir nenustatyta, kad prieš sprendžiant dėl tokio leidimo arba pažymėjimo panaikinimo atsiradus arba paaiškėjus šioms aplinkybėms asmens patikimumas ir lojalumas Lietuvos valstybei turi būti papildomai tikrinami siekiant nustatyti, ar tolesnis jo darbas su įslaptinta informacija nekeltų grėsmės tokios informacijos saugumui, prieštarauja Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui, toliau netirs, ar Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktas tiek pat neprieštarauja Konstitucijos 31 straipsnio 1 daliai.

VII

Dėl Vidaus tarnybos statuto 28 straipsnio (2007 m. gegužės 15 d. redakcija) tiek, kiek jame nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, atitikties Konstitucijos 31 straipsnio 1 daliai, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

1. Minėta, kad šioje konstitucinės justicijos byloje pareiškėjas abejoja, ar Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) tiek, kiek jame nėra nustatyti vadovo, turinčio teisę asmenį skirti į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, neprieštarauja Konstitucijos 31 straipsnio 1 daliai, 48 straipsnio

1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

2. Minėta, kad Vidaus tarnybos statuto 28 straipsnyje „Pareigūno nušalinimas nuo pareigų“ (2007 m. gegužės 15 d. redakcija) nustatyti trys vidaus tarnybos pareigūno nušalinimo nuo pareigų atvejai:

– tarnybos metu dėl apsvaigimo nuo alkoholio, narkotinių, psichotropinių ar kitų svaigiųjų medžiagų – tiesioginio vadovo sprendimu;

– tarnybinio patikrinimo metu – vadovo, turinčio teisę skirti į pareigas, įsakymu;

– pradėjus ikiteisminį tyrimą – Baudžiamojo proceso kodekso nustatyta tvarka.

Pažymėtina, kad kitų vidaus tarnybos pareigūno nušalinimo nuo pareigų atvejų Vidaus tarnybos statute nenumatyta.

Minėta ir tai, kad Baudžiamojo proceso kodekso 157 straipsnyje numatyti teismo įgaliojimai laikinai nušalinti nuo pareigų, tačiau jie skirti ne įslaptintos informacijos apsaugai užtikrinti, o tam, kad būtų greičiau ir nešališkiau ištirta nusikalstama veika ar užkirsta galimybė daryti naujas nusikalstamas veikas.

Taip pat minėta, kad už įslaptintos informacijos apsaugą atsako *inter alia* vadovas, turintis teisę skirti asmenį į pareigas; vienintelė priemonė, kurią jis gali taikyti tais atvejais, kai asmuo traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, yra leidimo dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimo panaikinimas ir paskesnis asmens atleidimas iš pareigų valstybės tarnyboje, kurioms eiti toks leidimas ar pažymėjimas yra būtinas.

3. Pareiškėjo nuomone, Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija), kuriame nenustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, prieštarauja *inter alia* Konstitucijos 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui, nes dėl šios priežasties pagal Valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) 18 straipsnio 1 dalies 4 punktą panaikinus vidaus tarnybos pareigūnui išduotą leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą, vadovui, turinčiam teisę skirti asmenį į pareigas, nelieka jokio kito pasirinkimo, kaip tik tokį pareigūną atleisti iš vidaus tarnybos, nors demokratinėje visuomenėje nėra ir negali būti pagrįsto intereso taikyti tokią neproporcingą priemonę.

4. Minėta, kad Konstitucijos 48 straipsnio 1 dalyje įtvirtintos kiekvieno asmens konstitucinės teisės pasirinkti darbą atmaina yra Konstitucijos 33 straipsnio 1 dalyje įtvirtinta piliečio teisė lygiomis sąlygomis stoti į valstybės tarnybą. Taip pat minėta, kad Konstitucijos 33 straipsnio 1 dalies nuostata, įtvirtinanti piliečių teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą, neturi būti aiškinama tik lingvistiškai ir neturi būti suprantama tik kaip teisė stoti į valstybės tarnybą, t. y. tik kaip susijusi su asmens priėmimu į valstybės

tarnybą; valstybės tarnybos santykiai apima ne tik santykius, susijusius su piliečio teisės lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą įgyvendinimu, bet ir santykius, susiklostančius piliečiui įstojus į valstybės tarnybą ir einant pareigas valstybės tarnyboje.

Atsižvelgdamas į tai, Konstitucinis Teismas šioje konstitucinės justicijos byloje tirs ir tai, ar pareiškėjo ginčijamas Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) neprieštarauja Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“.

5. Minėta, kad pareiškėjas ginčija, jo manymu, Vidaus tarnybos statuto 28 straipsnyje (2007 m. gegužės 15 d. redakcija) esančią legislatyvinę omisiją – tai, kas šiame teisės akte nėra nustatyta, nors, pareiškėjo manymu, pagal Konstituciją įstatymų leidėjo turėtų būti nustatyta, taigi ginčijama tokia teisinio reguliavimo spraga, kurią, pareiškėjo nuomone, Konstitucija draudžia.

Kaip minėta, teisės spraga, *inter alia* legislatyvinė omisija, visuomet reiškia, kad atitinkamų visuomeninių santykių teisinis reguliavimas apskritai nei eksplicitiškai, nei implicitiškai nėra nustatytas nei tam tikrame teisės akte (jo dalyje), nei kuriuose nors kituose teisės aktuose, tačiau poreikis tuos visuomeninius santykius teisiškai sureguliuoti yra, o legislatyvinės omisijos atveju tas teisinis reguliavimas turi būti nustatytas būtent tame teisės akte (būtent toje jo dalyje), nes to reikalauja kuris nors aukštesnės galios teisės aktas, *inter alia* pati Konstitucija.

6. Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) skirtas vidaus tarnybos pareigūno nušalinimui nuo pareigų reguliuoti. Tačiau nei jame, nei kitose šio statuto nuostatose nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai pareigūnas yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas.

Pažymėtina, kad vidaus tarnybos pareigūno nušalinimo nuo pareigų, susijusių su įslaptintos informacijos naudojimu ar jos apsauga, atvejų, kai siekiama užtikrinti įslaptintos informacijos apsaugą, nenustato nei Valstybės ir tarnybos paslapčių įstatymas (2003 m. gruodžio 16 d. redakcija), nei Lietuvos Respublikos valstybės tarnybos įstatymas (2002 m. balandžio 23 d. redakcija su vėlesniais pakeitimais ir papildymais).

7. Šiame Konstitucinio Teismo nutarime aiškinant Konstitucijos 33 straipsnio 1 dalies nuostatą, įtvirtinančią piliečių teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą, ir iš konstitucinio teisinės valstybės principo kylančius imperatyvus minėta, kad:

– asmenims, einantiems pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos naudojimu ar jos apsauga, keliama specialioji sąlyga yra ypatingas ir nė kiek neabejotinas patikimumas ir lojalumas Lietuvos valstybei;

– įstatymų leidėjas turi plačią diskreciją reguliuodamas santykius, susijusius su valstybės ir tarnybos paslapčių apsauga, *inter alia* nustatydamas asmenų, einančių pareigas valstybės tarnyboje, susijusias su įslaptintos informacijos nau-

dojimu ar jos apsauga, patikimumo ir lojalumo Lietuvos valstybei kriterijus ir tokių asmenų patikrinimo procedūras; įgyvendindamas šią diskreciją įstatymų leidėjas turi paisyti Konstitucijos normų ir principų, *inter alia* konstitucinio teisinės valstybės principo;

– reguliuojant valstybės tarnybos santykius, *inter alia* santykius, susijusius su valstybės ir tarnybos paslapčių apsauga, turi būti paisoma *inter alia* konstitucinio proporcingumo principo, kuris reiškia, kad įstatyme numatytos priemonės turi atitikti teisėtus ir visuomenei svarbius tikslus, kad jos turi būti būtinos minėtiems tikslams pasiekti ir kad neturi varžyti asmens teisių ir laisvių akivaizdžiai labiau negu reikia šiems tikslams pasiekti;

– konstitucinio proporcingumo principo reikalavimas asmens teisių ir laisvių įstatymu neriboti labiau negu reikia teisėtiems ir visuomenei svarbiems tikslams pasiekti *inter alia* suponuoja reikalavimą įstatymų leidėjui nustatyti tokį teisinį reguliavimą, kuris sudarytų prielaidas pakankamai individualizuoti asmens teisių ir laisvių apribojimus: ribojantis asmens teises ir laisves įstatymo nustatytas teisinis reguliavimas turi būti toks, kad sudarytų prielaidas kiek įmanoma įvertinti individualią kiekvieno asmens situaciją ir, atsižvelgiant į visas svarbias aplinkybes, atitinkamai individualizuoti konkrečias tam asmeniui taikytinas ribojančias jo teises priemones.

8. Taigi iš Konstitucijos 33 straipsnio 1 dalies nuostatos „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“ ir iš minėtų konstitucinių teisinės valstybės principo imperatyvų įstatymų leidėjui kyla pareiga nustatyti tokį teisinį reguliavimą, kuriuo būtų nustatyta alternatyvi priemonė leidimui dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimui panaikinti ir asmeniui atleisti iš pareigų valstybės tarnyboje, kuri sudarytų prielaidas pakankamai individualizuoti asmens teisių ir laisvių apribojimus ir kiek įmanoma įvertinti individualią kiekvieno asmens situaciją. Tokia priemonė *inter alia* yra nušalinimas nuo pareigų, taikomas tais atvejais, kai asmuo traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, ir sudarantis prielaidas papildomai patikrinti asmens patikimumą ir lojalumą Lietuvos valstybei siekiant nustatyti, ar tolesnis jo darbas nekeltų grėsmės įslaptintos informacijos saugumui.

9. Atsižvelgiant į išdėstytus argumentus darytina išvada, kad Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) tiek, kiek jame nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, prieštarauja Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, konstituciniam teisinės valstybės principui.

10. Atsižvelgiant į tai, kad, kaip minėta, Konstitucijos 33 straipsnio 1 dalyje įtvirtinta piliečio teisė lygiomis sąlygomis stoti į valstybės tarnybą yra Konstitucijos 48 straipsnio 1 dalyje įtvirtintos kiekvieno asmens konstitucinės teisės

pasirinkti darbą atmaina, dėl tų pačių argumentų konstatuotina, kad Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) tiek, kiek jame nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, prieštarauja ir Konstitucijos 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“.

11. Konstitucinis Teismas, šiame nutarime konstatavęs, kad Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) tiek, kiek jame nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, prieštarauja Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui, toliau netirs, ar Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) tiek pat neprieštarauja Konstitucijos 31 straipsnio 1 daliai.

Vadovaudamasis Lietuvos Respublikos Konstitucijos 102, 105 straipsniais, Lietuvos Respublikos Konstitucinio Teismo įstatymo 1, 53, 54, 55, 56 straipsniais, Lietuvos Respublikos Konstitucinis Teismas

nutaria:

1. Pripažinti, kad Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) (Žin., 2004, Nr. 4-29) 16 straipsnio 2 dalies 13 punktas neprieštarauja Lietuvos Respublikos Konstitucijai.

2. Pripažinti, kad Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo (2003 m. gruodžio 16 d. redakcija) (Žin., 2004, Nr. 4-29) 18 straipsnio 1 dalies 4 punktas tiek, kiek jame nustatyta, kad leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas panaikinamas atsiradus arba paaiškėjus šio įstatymo 16 straipsnio 2 dalies 13 punkte nurodytoms aplinkybėms, ir nenustatyta, kad prieš sprendžiant dėl tokio leidimo arba pažymėjimo panaikinimo atsiradus ar paaiškėjus šioms aplinkybėms asmens patikimumas ir lojalumas Lietuvos valstybei turi būti papildomai tikrinami siekiant nustatyti, ar tolesnis jo darbas su įslaptinta informacija nekeltų grėsmės tokios informacijos saugumui, prieštarauja Lietuvos Respublikos Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

3. Pripažinti, kad Lietuvos Respublikos vidaus tarnybos statuto patvirtini-

mo įstatymu patvirtinto Vidaus tarnybos statuto 28 straipsnis (2007 m. gegužės 15 d. redakcija) (Žin., 2007, Nr. 59-2282) tiek, kiek jame nėra nustatyti vadovo, turinčio teisę skirti asmenį į pareigas, įgaliojimai nušalinti pareigūną nuo pareigų, kurioms eiti būtinas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, tuo atveju, kai asmuo yra traukiamas baudžiamojon atsakomybėn už tyčinę nusikalstamą veiką arba jam dėl tokios veikos atliekamas ikiteisminis ar operatyvinis tyrimas, prieštarauja Lietuvos Respublikos Konstitucijos 33 straipsnio 1 dalies nuostatai „piliečiai turi <...> teisę lygiomis sąlygomis stoti į Lietuvos Respublikos valstybinę tarnybą“, 48 straipsnio 1 dalies nuostatai „kiekvienas žmogus gali laisvai pasirinkti darbą“, konstituciniam teisinės valstybės principui.

Šis Konstitucinio Teismo nutarimas yra galutinis ir neskundžiamas.
<...>

SANTRUMPOS

ADA	Automatizuoto duomenų apdorojimo sistema
AOTD	Antrasis operatyvinių tarnybų departamentas prie Lietuvos Respublikos krašto apsaugos ministerijos
ATOMAL	Slaptumo žyma, kuria žymima atominė informacija
ES	Europos Sąjunga
IRD	Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos
KI	Kompetentinga institucija
NATO	Šiaurės Altanto Sutarties Organizacija
NKAT	Nacionalinė komunikacijų apsaugos tarnyba
NSI	Nacionalinė saugumo institucija
NŠPT	Nacionalinė šifrų paskirstymo tarnyba
PAKK	Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
SPT	Saugumo priežiūros tarnyba
TEMPEST	Automatizuoto duomenų apdorojimo (ADA) sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsauga nuo informatyviojo spinduliavimo
VRC	Vyriausybinių ryšių centras prie Lietuvos Respublikos krašto apsaugos ministerijos
VSD	Lietuvos Respublikos valstybės saugumo departamentas
VTPĮ	Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas
ŽSPT	Žinybinė saugumo priežiūros tarnyba

VALSTYBĖS IR TARNYBOS PASLAPČIŲ APSAUGOS TERMINŲ ŽINYNAS

A

Automatizuoto duomenų apdorojimo sistemos ir tinklai (toliau – **ADA sistemos ir tinklai**) – iš vieno ar daugiau kompiuterių, išorinių įrenginių ir programinės įrangos sudarytos ir informacinių technologijų pagrindu veikiančios infrastruktūros visuma, skirta atlikti įslaptintos informacijos automatizuoto apdorojimo ir saugojimo funkcijas, ir elektroninių ryšių tinklai, kuriais perduodama įslaptinta informacija (išskyrus viešuosius ryšių tinklus) *(Valstybės ir tarnybos paslapčių įstatymas)*.

ADA sistemų ir tinklų apsauga – mechaninių, programinių, procedūrinių ir elektroninių apsaugos priemonių visuma, užtikrinanti ADA sistemose ir tinkluose saugomos, apdorojamos bei šiais tinklais perduodamos įslaptintos informacijos slaptumą (konfidencialumą), prieinamumą teisėtiems informacijos naudotojams bei tokios informacijos vientisumą ir autentiškumą *(Valstybės ir tarnybos paslapčių įstatymas)*.

ADA sistemos ar tinklo naudotojas – valstybės institucijos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, taip pat rangovo (subrangovo) darbuotojas, teisės aktų nustatyta tvarka turintis teisę dirbti ar susipažinti su įslaptinta informacija ir pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją, naudojantis elektronines paslaugas *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, steigimo ir įteisinimo taisyklės)*.

ADA sistemos ar tinklo nuostatai – dokumentas, kuriame pateikta pagrindinė ADA sistemą ar tinklą apibūdinanti informacija, pagrindžianti ADA sistemos ar tinklo reikalingumą *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, steigimo ir įteisinimo taisyklės)*.

ADA sistemos ar tinklo slaptumo žyma – aukščiausia slaptumo žyma, kuria pažymėta įslaptinta informacija gali būti saugoma, apdorojama ADA sistemoje ar perduodama ADA tinklu *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas)*.

ADA sistemos ar tinklo specifikacija – dokumentas, kuriame pateikti techniniai reikalavimai ADA sistemai ar tinklui, ADA sistemos ar tinklo valdytojo sprendimu – ir ekonominis pagrindimas, darbų planas *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, steigimo ir įteisinimo taisyklės).*

ADA sistemos ar tinklo steigėjas – paslapčių subjektas arba rangovas (subrangovas), kuris, siekdamas automatizuotai apdoroti, saugoti ar perduoti įslaptintą informaciją, inicijuoja ADA sistemos ar tinklo steigimą, nustato ADA sistemos ar tinklo tikslus ir patvirtina ADA sistemos ar tinklo nuostatus *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, steigimo ir įteisinimo taisyklės).*

ADA sistemos ar tinklo valdytojas – ADA sistemos ar tinklo nuostatuose nurodytas paslapčių subjektas arba jo įgaliotas struktūrinis padalinys, arba rangovas (subrangovas), kuris valdo ADA sistemą ar tinklą, juos sukūręs ar užsakęs sukurti arba įsigijęs *(Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės)*.

ADA sistemos ar tinklo tvarkytojas – ADA sistemos ar tinklo valdytojas arba kitas ADA sistemos ar tinklo nuostatuose nurodytas paslapčių subjektas, arba jo įgaliotas struktūrinis padalinys, arba rangovas (subrangovas), kuris tvarko ADA sistemą ar tinklą, jų duomenis *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, steigimo ir įteisinimo taisyklės)*.

Antrinis dokumentas – tai dokumentas, kuriame yra ATOMAL informacijos, gautos iš vieno ar kelių ATOMAL dokumentų ar kitų šaltinių, ir kuris nėra atgaminys, nes jame netiesiogiai naudojama ATOMAL informacija. Šiame dokumente užrašai, daromi konferencijų, vizitų ar mokymo kursų metu, laikomi antriniais dokumentais *(Šiaurės Atlanto Sutarties Šalių susitarimas dėl bendradarbiavimo, susijusio su atomine informacija).*

Apsaugos darbuotojas – objekto, asmenų ir turto apsaugą vykdantis paslapčių subjekto arba rangovo (subrangovo) darbuotojas *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

Apsauginė įsilaužimo signalizacija – tai visuma signalizacijos priemonių, kurios automatiškai nustato ir fiksuoja neteisėtą patekimą į saugumo zoną bei informaciją apie tai perduoda į vietinį ir (arba) centralizuotą stebėjimo pultą *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

Apsauga nuo aktyvaus neteisėto įslaptintos informacijos fiksavimo ir perdavimo – įslaptintos informacijos, perteikiamos garsu ar vaizdu, apsauga nuo jos fiksavimo ar perdavimo neteisėtais informacijos rinkimo įrenginiais

(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).

Apsauga nuo pasyvaus neteisėto įslaptintos informacijos fiksavimo ir perdavimo – garsą ir elektromagnetines bangas slopinančių medžiagų arba įrangos, slopinančios įslaptintos informacijos, perteikiamos garsu, vaizdu arba elektromagnetinėmis bangomis, sklidimą už patalpos ribų, panaudojimas *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

Apsaugos postas – patalpa ar pastatas, kuriame įrengtos specializuotos darbo vietos ir telekomunikacijų infrastruktūra, ir kuriame yra fiksuojami ir įvertinami apsauginės užpuolimo, įsilaužimo ir priešgaisrinės signalizacijos suveikimo signalai, palaikomas abipusis ryšys su apsaugos darbuotojais ir reagavimo grupe *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

Apsauginė užpuolimo signalizacija – tai visuma signalizacijos priemonių, kurias įjungus nustatomas ir fiksuojamas užpuolimas bei informacija apie tai perduodama į vietinį ir (arba) centralizuotą stebėjimo pultą *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

Asmens patikimumo pažymėjimas – Valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka išduotas dokumentas, patvirtinantis asmens teisę dirbti ar susipažinti su užsienio valstybių ar tarptautinių organizacijų perduota įslaptinta informacija, žymima slaptumo žymų „Visiškai slaptai“, „Slaptai“, „Konfidencialiai“ atitikmenimis, arba tokią informaciją saugoti ar gabenti *(Valstybės ir tarnybos paslapčių įstatymas)*.

Atgaminys – tai ATOMAL dokumento kopija arba vertimas, arba ištrauka, kurią sudaro viena ar kelios ištisinės pastraipos, diagramos ar lentelės, kuriose yra ATOMAL informacijos *(Šiaurės Atlanto Sutarties Šalių susitarimas dėl bendradarbiavimo, susijusio su atomine informacija).*

ATOMAL centrinė registratūra – centrinė kontroliuojanti įstaiga, kiekvienoje NATO struktūroje paskirta prašyti, gauti, registruoti, tvarkyti ir platinti ATOMAL dokumentus *(Šiaurės Atlanto Sutarties Šalių susitarimas dėl bendradarbiavimo, susijusio su atomine informacija)*.

ATOMAL antrinė registratūra – kontroliuojanti įstaiga, atsakinga už ATOMAL dokumentų gavimą, registravimą, tvarkymą ir platinimą tam tikroje NATO struktūros dalyje *(Šiaurės Atlanto Sutarties Šalių susitarimas dėl bendradarbiavimo, susijusio su atomine informacija)*.

ATOMAL kontrolės punktas – žemesnio už antrinę registratūrą lygio kontroliuojanti įstaiga, atsakinga už ATOMAL dokumentų gavimą, registravimą, tvarkymą ir platinimą įstaigos, kurią ji aptarnauja, personalui *(Šiaurės Atlanto Sutarties Šalių susitarimas dėl bendradarbiavimo, susijusio su atomine informacija)*.

ATOMAL kontrolės pareigūnas (angl. *ATOMAL Control Officer*) – ATOMAL informacijos administravimą, apsaugą ir kontrolę vykdantis asmuo *(Asmenų, atsakingų už įslaptintos informacijos apsaugą, tipinis funkcijų sąrašas)*.

ATOMAL kontrolės pareigūną pavaduojantis asmuo (angl. *Alternate ATOMAL Control Officer*) – nesant ATOMAL kontrolės pareigūno, jo funkcijas vykdantis asmuo *(Asmenų, atsakingų už įslaptintos informacijos apsaugą, tipinis funkcijų sąrašas)*.

Atominė informacija (ATOMAL), Jungtinių Amerikos Valstijų Vyriausybės teikiama pagal Šiaurės Atlanto Sutarties Šalių susitarimą dėl bendradarbiavimo, susijusio su atomine informacija – tai informacija, Jungtinių Amerikos Valstijų Vyriausybės pažymėta kaip „Riboto naudojimo duomenys“ (*Restricted Data*) arba „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*). *(Asmenų, atsakingų už įslaptintos informacijos apsaugą, tipinis funkcijų sąrašas)*

ATOMAL informacija – tai informacija, pažymėta žyma „Riboto naudojimo duomenys“ (*Restricted Data*) arba žyma „Buvę riboto naudojimo duomenys“ (*Formerly Restricted Data*), kurią Jungtinių Amerikos Valstijų Vyriausybė pagal Susitarimą arba pagal 1955 metų susitarimą, kurį jis pakeitė, teikia kitoms NATO struktūroms; arba kaip „JK atominė informacija“ (*UK ATOMIC Information*), kurią Jungtinės Karalystės Vyriausybė pagal galiojančius susitarimus teikia kitoms NATO struktūroms *(Šiaurės Atlanto Sutarties Šalių susitarimas dėl bendradarbiavimo, susijusio su atomine informacija)*.

Atominis ginklas – tai bet koks įtaisas, naudojantis atominę energiją, išskyrus jo transportavimo ar varomąsias priemones (kai tokios priemonės yra atskiriamosios šio įtaiso dalys), kurio pagrindinė paskirtis – naudoti arba tobulinti jį kaip ginklą, ginklo eksperimentinį pavyzdį ar ginklo bandymo įtaisą *(Šiaurės Atlanto Sutarties Šalių susitarimas dėl bendradarbiavimo, susijusio su atomine informacija)*.

Atsakingas asmuo – paslapčių subjekto vadovo ar jo įgalioto asmens sprendimu paskirtas atskiras struktūrinis paslapčių subjekto padalinys (padaliniai), darbuotojas arba rangovo (subrangovo) vadovo sprendimu paskirtas darbuotojas, organizuojantis ir įgyvendinantis įslaptintos informacijos, kuria disponuoja paslapčių subjektas ar rangovas (subrangovas), administravimą, apsaugą ir kontrolę *(Valstybės ir tarnybos paslapčių įstatymas)*.

B

Barjeras – laisvai judėti kliudantis užtvaras, statinys ar kitas įrenginys *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

„**Būtinas informacijos rengėjo sutikimas**“ – nuoroda, žyminti, kad įslaptintas dokumentas negali būti dauginamas ar platinamas be įslaptintos informacijos rengėjo sutikimo *(Valstybės ir tarnybos paslapčių įstatymas)*.

C

Centralizuotas stebėjimo pultas – prietaisas, priimantis saugomų objektų apsaugos pultų pranešimus laidinėmis, belaidėmis ryšio linijomis, formuojantis šviesos ir garso signalus savo indikatoriuose arba periferiniuose įrenginiuose *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

D

Darbuotojas – valstybės tarnautojas ar asmuo, dirbantis pagal darbo sutartį, arba karys *(Valstybės ir tarnybos paslapčių įstatymas)*.

Darbuotojo kortelė – asmeniui išduodama registruota kortelė su registracijos numeriu, jį identifikuojanti kaip paslapčių subjekto ar rangovo (subrangovo) darbuotoją ir suteikianti galimybę teisėtai patekti į saugumo zoną ir (arba) teritoriją *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Darbuotojo vykdoma įeigos kontrolė – įeigos kontrolė, kurią atlieka apsaugos darbuotojas arba paslapčių subjekto ar rangovo (subrangovo) vadovo įgaliotas asmuo, nustatantis norinčių patekti asmenų tapatybę pagal asmens tapatybę patvirtinančius dokumentus *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Daugkartinio įrašymo laikmena – laikmena, į kurią duomenys dėl laikmenos konstrukcinių savybių gali būti įrašomi (perrašomi) daugiau negu vieną kartą *(Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas)*.

Diplomatinis krovinys – kiti daiktai, nenurodyti Lietuvos Respublikos diplomatinio pašto ir diplomatinio krovinio gabenimo taisyklių 5 punkto antrojoje pastraipoje, gabenami iš Užsienio reikalų ministerijos į atstovybes ir atgal arba iš atstovybės į atstovybę, arba persikeliančio atstovybės darbuotojo ar jo šeimos narių asmeniniai ir įsikūrimui skirti daiktai, turintys diplomatinio krovinio sertifikatą, kurio formą tvirtina užsienio reikalų ministras. Diplomatinis krovinys pažymimas etiketėmis užsienio reikalų ministro nustatyta tvarka *(Lietuvos Respublikos diplomatinio pašto ir diplomatinio krovinio gabenimo taisyklės)*.

Diplomatinis paštas – dokumentai ir kiti tik oficialiai veiklai skirti daiktai, gabenami iš Užsienio reikalų ministerijos į Lietuvos Respublikos diplomatines atstovybes, konsulines įstaigas, atstovybes prie tarptautinių tarpvyriausybinių organizacijų ir specialiąsias misijas (toliau vadinama – atstovybės) ir atgal arba iš atstovybės į atstovybę plombuojamuose diplomatinio pašto maišuose, daugkartinio naudojimo paketuose arba kitoje plombuojamoje taroje, pažymėtoje aiškiais išoriniais atpažinimo ženklais, turintys diplomatinio pašto sertifikatą. Diplomatinio pašto maišų, daugkartinio naudojimo paketų ar kitos plombuojamos taros išorinių atpažinimo ženklų pavyzdžius ir diplomatinio pašto sertifikato formą tvirtina užsienio reikalų ministras *(Lietuvos Respublikos diplomatinio pašto ir diplomatinio krovinio gabenimo taisyklės)*.

Diplomatinio pašto ir diplomatinio krovinio siuntėjas ir gavėjas – Užsienio reikalų ministerija ir atstovybės *(Lietuvos Respublikos diplomatinio pašto ir diplomatinio krovinio gabenimo taisyklės)*.

E

Ekstremali situacija – padėtis, kuri atsiranda paskelbus karo ar nepaprastąją padėtį ar dėl kitų įvykių, kurių metu kyla įslaptintos informacijos pagrobimo, neteiseto atskleidimo, praradimo grėsmė *(Įslaptintos informacijos evakuacijos arba sunaikinimo planų karo, nepaprastosios padėties ar ekstremalių situacijų atveju rengimo rekomendacijos)*.

Elektroninių apsaugos priemonių centrinio valdymo įranga – techninė įranga, kuria gali būti keičiama apsauginės įsilaužimo, užpuolimo ir priešgaisrinės signalizacijų, elektroninės įeigos kontrolės sistemos bei uždarosios vaizdo stebėjimo sistemos konfigūracija ir veikimo parametrai *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Elektroninė įeigos kontrolės sistema – tai įrenginys (ar jų grupė), kuris identifikuoja asmenį surenkant skaičių ar simbolių kombinaciją, nuskaito laikmenoje esančią šifruotą informaciją arba identifikuoja asmenį pagal jo individualius biometrinius duomenis (akies rainelę, papiliarinius raštus ir pan.) *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Elektroninė saugumo aplinka – saugumo aplinka, kurioje elektroniniu būdu tvarkoma įslaptinta informacija, kuri yra saugoma techninėmis ir programinėmis ADA sistemų ir tinklų apsaugos priemonėmis *(Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės)*.

Elektromagnetiniai spinduliavimo šaltiniai – bet kokie įrenginiai, skleidžiantys elektromagnetinį spinduliavimą (mobiliojo ryšio telefonai, radijo stotelės ir kt.) *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

ES VS kontrolės pareigūnas (angl. *EU TOP SECRET Control Officer*) – Europos Sąjungos (toliau – ES) Lietuvai perduotos įslaptintos informacijos, žymimos slaptumo žyma VISIŠKAI SLAPTAI (angl. *TRES SECRET UE/EU TOP SECRET*), administravimą, apsaugą ir kontrolę vykdantis asmuo *(Asmenų, atsakingų už įslaptintos informacijos apsaugą, tipinis funkcijų sąrašas).*

ES VS kontrolės pareigūną pavaduojantis asmuo (angl. *Alternate EU TOP SECRET Control Office*) – nesant ES VS kontrolės pareigūno, jo funkcijas vykdantis asmuo *(Asmenų, atsakingų už įslaptintos informacijos apsaugą, tipinis funkcijų sąrašas).*

Evakuacija – organizuotas įslaptintos informacijos išgabenimas iš jos nuolatinės saugojimo vietos į parinktą evakuacijos vietą *(Įslaptintos informacijos evakuacijos arba sunaikinimo planų karo, nepaprastosios padėties ar ekstremalių situacijų atveju rengimo rekomendacijos).*

Evakuacijos vieta – iš anksto paslapčių subjekto, rangovo (subrangovo) vadovo nustatyta vieta, į kurią evakuacijos metu išgabenama įslaptinta informacija ir saugoma iki ekstremalios situacijos pabaigos *(Įslaptintos informacijos evakuacijos arba sunaikinimo planų karo, nepaprastosios padėties ar ekstremalių situacijų atveju rengimo rekomendacijos).*

F

Fizinė apsauga – visuma fizinių, mechaninių, elektroninių ir procedūrinių apsaugos priemonių bei metodų, užtikrinančių teritorijų, patalpų, kuriose dirbama su įslaptinta informacija ar kuriose tokia informacija yra saugoma, apsaugą nuo neteisėto patekimo į jas bei jose saugomos įslaptintos informacijos apsaugą nuo pagrobimo, kitokio neteisėto įgijimo, atskleidimo, praradimo. Ji taikoma atsižvelgiant į saugomos informacijos slaptumo žymas, svarbą, tokios informacijos apimtį bei tokių teritorijų, patalpų ar darbo vietų priskyrimą atitinkamai saugumo zonai *(Valstybės ir tarnybos paslapčių įstatymas)*.

Fizinės apsaugos priemonės – mechaninės ir elektroninės priemonės, skirtos įslaptintai informacijai apsaugoti nuo pagrobimo, neteisėto atskleidimo, sunaikinimo bei užkirsti kelią neteisėtam patekimui į saugomas patalpas ar teritorijas, neteisėtam susipažinimui su šiose vietose saugoma įslaptinta informacija, taip pat padėti nustatyti neteisėtą asmenų patekimą į saugomas patalpas, užkirsti kelią neteisėtiems šių asmenų veiksmams *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

G

Globali saugumo aplinka – perimetro fizinės apsaugos priemonėmis apsaugota saugumo aplinka, kurioje įdiegti ADA sistema ir tinklai ar jų sudėtinės dalys *(Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės).*

Grėsmė – vienos ar daugiau įslaptintos informacijos savybių – konfidencialumo, vientisumo ar prieinamumo – praradimo galimybė *(Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės).*

Griežtos apskaitos ATOMAL dokumentas – tai dokumentas, pažymėtas slaptumo žyma „Visuotinės reikšmės visiškai slaptai ATOMAL“ (*COSMIC TOP SECRET ATOMAL*), „NATO Slaptai ATOMAL“ (*NATO SECRET ATOMAL*) arba „NATO Konfidencialiai ATOMAL“ (*NATO CONFIDENTIAL ATOMAL*), kuriam taikomi specialūs apribojimai pagal Susitarimo VI straipsnį ir kuris dėl to tampa griežtos apskaitos dokumentu pagal Saugumo priedo IV skyriaus D dalies nuostatas (šių dokumentų atgaminiai ir jais naudojantis parengti antriniai dokumentai taip pat yra griežtos apskaitos dokumentai) *(Šiaurės Atlanto Sutarties Šalių susitarimas dėl bendradarbiavimo, susijusio su atomine informacija).*

I

Informacijos įslaptinimas – duomenų priskyrimas valstybės ar tarnybos paslapčiai, atitinkamos slaptumo žymos suteikimas, įslaptinimo termino nustatymas ir reikiamos apsaugos suteikimas *(Valstybės ir tarnybos paslapčių įstatymas)*.

Informatyviojo elektromagnetinio spinduliavimo (TEMPEST) matavimas – informatyviojo elektromagnetinio spinduliavimo rezultatų fizikinės vertės nustatymas, siekiant užtikrinti įslaptintos informacijos, žymimos slaptumo zyma „Konfidencialiai“ ir aukštesne, skirtos perduoti, saugoti ir apdoroti ADA sistemose ir tinkluose, konfidencialumą *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas).*

Į

Įgaliotoji institucija – institucija, kuriai teisės aktais pavesta atlikti Nacionalinės komunikacijų apsaugos tarnybos arba Nacionalinės šifrų paskirstymo tarnybos, arba Saugumo priežiūros tarnybos, arba apsaugos nuo informatyviojo

elektromagnetinio spinduliavimo (TEMPEST) funkcijas *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas)*.

Įeigos kontrolės sistema – fizinių, informacinių arba biometrinių asmens identifikavimo priemonių visuma, leidžianti nustatyti asmens tapatybę bei suteikianti arba nesuteikianti galimybę asmeniui patekti į saugumo zonas *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Įmonės patikimumą patvirtinantis pažymėjimas – Valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka išduotas dokumentas, kuriuo patvirtinama, kad rangovas (subrangovas) atitinka įslaptintos informacijos apsaugos reikalavimus *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įrangos informatyviojo elektromagnetinio spinduliavimo (TEMPEST) matavimų planas – dokumentas, kuriame aprašytas matuojamos TEMPEST įrangos tipas, veikimo režimai, informaciniai signalai ir atliekamos matavimo procedūros *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Įrangos sertifikatas – įrangos atitikties TEMPEST zonai liudijimas *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Įslaptinti darbai – valstybės ar tarnybos paslaptimi pripažinti mokslo, tyrimo, bandymų, projektavimo, techninio aptarnavimo darbai bei technologiniai procesai *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptinti darbai – su įslaptinta informacija susiję darbai, atliekami nekarinio saugumo tikslais, arba darbai, kurių pirkimo procedūrų ar sutarties vykdymo metu neišvengiamai tektų atskleisti įslaptintą informaciją *(Viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymas)*.

Įslaptintas dokumentas – valstybės ar tarnybos paslaptimi pripažinta fiksuota informacija, nesvarbu, koks jos fiksavimo būdas ir informacijos laikmenos (grafiniai darbai, atlikti įvairiais būdais: parašyti ranka, išleisti spaustuvėje, išspausdinti rašomąja mašinėle, surinkti kompiuteriu, nupiešti ar nubraižyti; vaizdo ar garso įrašai, kompiuterių informacijos rinkmenos, kino ir fotografijos negatyvai, pozityvai ar kiti informacijos masyvai), taip pat bet kokiu būdu ar priemonėmis padarytos tokios informacijos laikmenų kopijos *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptinti gaminiai – valstybės ar tarnybos paslaptimi pripažinti įvairūs įrenginiai, sistemos, ginkluotė, karinės, kompiuterinės bei kitos technikos įran-

ga, kompleksai, agregatai, prietaisai, programinė įranga ir chemijos produkcija *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptinta informacija – paslapčių subjekto pripažinta valstybės ar tarnybos paslaptimi informacija apie dokumentų, darbų, gaminių ar kitų objektų buvimą, esmę ar turinį, taip pat tokia paslaptimi pripažinti patys dokumentai, darbai, gaminiai ar kiti objektai *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptintos informacijos administravimas – skirtingas slaptumo žymas turinčios įslaptintos informacijos rengimo, įforminimo, registracijos, siuntimo, gabenimo, gavimo, dauginimo, saugojimo, sunaikinimo bei apskaitos procedūros *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptintos informacijos apsauga – apsaugos priemonių ir procedūrų taikymas siekiant išvengti įslaptintos informacijos praradimo ar neteisėto atskleidimo *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptintos informacijos apsaugos pažeidimas – teisės aktų reikalavimams prieštaraujantis veikimas arba neveikimas, sukėlęs ar galintis sukelti pavojų įslaptintos informacijos saugumui arba sąlygojęs įslaptintos informacijos ar jos dalies patekimą asmenims, neturintiems teisės susipažinti su tokia informacija *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Įslaptintos informacijos gavėjas – paslapčių subjektas ar jo struktūrinis padalinys, asmuo, rangovas (subrangovas), teisės aktų nustatyta tvarka gavęs kito paslapčių subjekto parengtą įslaptintą informaciją *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptintos informacijos naudotojas – paslapčių subjekto, rangovo (subrangovo) darbuotojas, turintis teisę teisės aktų nustatyta tvarka dirbti ar susipažinti su įslaptinta informacija *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptintos informacijos rengėjas – paslapčių subjektas, parengęs ir šio Įstatymo nustatyta tvarka įslaptinęs informaciją, arba jo teisių perėmėjas. Įslaptintos informacijos rengėju nelaikomas paslapčių subjektas, išskyrus paslapčių subjekto, parengusio ir įslaptinusio informaciją, teisių perėmėją, disponuojantis ar savo veikloje naudojantis bet kokiu būdu gautą bet kokio pobūdžio ir kilmės kito paslapčių subjekto parengtą, įslaptintą ir jam perduotą informaciją *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptintos informacijos išslaptinimas – duomenims suteiktos slaptumo žymos ir nustatytos apsaugos panaikinimas *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptintos informacijos tvarkymas – visos su informacija atliekamos operacijos: rinkimas, užrašymas, klasifikavimas, grupavimas, kaupimas, sau-

gojimas, keitimas, kopijavimas, perdavimas, naudojimas, naikinimas *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Įslaptinta įranga – su įslaptinta informacija susijusi įranga, naudojama nekarinio saugumo tikslais, arba įranga, kurios pirkimo procedūrų ar sutarties vykdymo metu neišvengiamai tektų atskleisti įslaptintą informaciją *(Viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymas)*.

Įslaptintos paslaugos – su įslaptinta informacija susijusios paslaugos, teikiamos nekarinio saugumo tikslais, arba paslaugos, kurių pirkimo procedūrų ar sutarties vykdymo metu neišvengiamai tektų atskleisti įslaptintą informaciją *(Viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymas)*.

Įslaptintas sandoris – paslapčių subjekto ir rangovo sutartis dėl prekių, paslaugų ar darbų įsigijimo, kurią sudarant ar vykdant bus susipažįstama su įslaptinta informacija, tokia informacija bus patikėta, naudojama ar sukuriama *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptintų sandorių saugumas – įslaptintos informacijos apsaugos priemonių ir procedūrų taikymas įslaptintų sandorių sudarymo bei vykdymo metu *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptintų sandorių saugumą užtikrinančios institucijos – institucijos, įgyvendinančios įslaptintų sandorių saugumo reikalavimus ir vykdančios kontrolę iki pasirašant įslaptintą sandorį ir tokio sandorio vykdymo metu *(Valstybės ir tarnybos paslapčių įstatymas)*.

Įslaptinimo žinynas – konkretiems įslaptintiems sandoriams vykdyti parengtas dokumentas, kuriame nurodoma naudojama arba numatoma sukurti įslaptintina informacija, nustatomos šios informacijos slaptumo žymos, įslaptinimo terminai ir slaptumo žymų pakeitimo arba informacijos išslaptinimo sąlygos *(Valstybės ir tarnybos paslapčių įstatymas)*.

J

Juoda – laidinės linijos, optiniai kabeliai, komponentai, įranga ir sistemos, kuriose apdorojama ar kuriomis perduodama tik neslapta arba įslaptinta užšifruota informacija, taip pat zonos, kuriose nebūna įslaptintos informacijos *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

K

Kalibravimas – veiksmų visuma, kuri nurodytomis sąlygomis nustato matavimo įrangos ar matavimo sistemos rodomą dydžių verčių ryšį su etalonų sukurtomis atitinkamomis vertemis *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas).*

Karinė įranga – įranga, specialiai sukurta ar pritaikyta kariniams tikslams ir skirta naudoti kaip ginklai, įskaitant amuniciją ir karines medžiagas *(Viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymas)*.

Kenkėjiška programinė įranga – programinė įranga ar jos dalis, skirta neteisėtai prisijungti ar sudaryti sąlygas neteisėtai prisijungti prie informacinių sistemų ar elektroninių ryšių tinklo, sutrikdyti ar pakeisti (įskaitant valdymo perėmimą) informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, sudaryti sąlygas neviešus elektroninius duomenis pasisavinti, paskelbti, platinti ar kitaip panaudoti tokios teisės neturintiems asmenims *(Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas).*

Kiti įslaptinti objektai – valstybės ar tarnybos paslaptimi pripažintos medžiagos, skysčiai, dujos, mineralai, biologinės ir kitos materijos formos, kurių pagal savybes ar prigimtį negalima priskirti dokumento, gaminių ar darbų sąvokai *(Valstybės ir tarnybos paslapčių įstatymas)*.

Konfidencialumas – įslaptintos informacijos (ADA sistemos ar tinklo paslaugos ar ištekliaus) savybė – su įslaptinta informacija gali susipažinti (ADA sistemos ar tinklo paslauga ar ištekliumi gali naudotis) tik tam įgalioti asmenys *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija).*

Kontrolės postas – vieta, kurioje paslapčių subjekto ar rangovo (subrangovo) vadovo ar jo įgalioto asmens nustatyta tvarka tikrinami į saugumo zonas ar į jose esančias atskiras patalpas patenkantys asmenys ir (arba) įvažiuojančios ir išvažiuojančios transporto priemonės, nustatoma asmenų tapatybė *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

Kontroliuojama zona – teritorija ar jos dalis, kurioje žmonių, transporto priemonių atvykimas/išvykimas/judėjimas viduje yra kontroliuojamas, kai yra galimybė pastebėti ir pašalinti grėsmes. Kontroliuojama zona paprastai sutampa su subjekto administracinės saugumo zonos riba *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo*

bendrųjų reikalavimų ir procedūrų aprašas).

Krizė – valstybėje narėje ar trečiojoje šalyje susidariusi padėtis, dėl kurios atsiranda žala, kuri yra pastebimai didesnė negu įprasta žala ir kelia ypač didelį pavojų žmonių gyvybei ir sveikatai arba daro ypač didelį poveikį turto vertei, arba dėl kurios reikia imtis priemonių, siekiant aprūpinti gyventojus būtiniausiais reikmenimis, arba kyla neišvengiama tokios žalos grėsmė. Krize šiame įstatyme taip pat laikomas ginkluotas konfliktas ir karas *(Viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymas)*.

KF sistema ar tinklas – ADA sistema, kurioje saugoma, apdorojama įslaptinta informacija, žymima slaptumo žyma „Konfidencialiai“, ar tinklas, kuriuo tokia informacija yra perduodama *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas).*

L

Laikmena – atmintinė įslaptintiems duomenims ir (arba) programinei įrangai įrašyti, tvarkyti, laikyti ar saugoti. Laikmenos yra optiniai diskai (CD, DVD, BLUE-RAY), lankstieji diskeliai, standieji diskai, USB atmintinės, atminties kortelės, magnetinės juostos, magnetinės kortelės, įrenginiai, kuriuose atmintinės įmontuotos stacionariai ir kurių negalima išardyti, taip pat kiti objektai, skirti įslaptintai informacijai įrašyti, tvarkyti, laikyti, saugoti *(Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas).*

Laikmenos naudotojas – paslapčių subjekto, rangovo (subrangovo) darbuotojas, kuriam vykdant tarnybines pareigas teisės aktų nustatyta tvarka yra perduota laikmena *(Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas).*

Laikmenos sunaikinimas – laikmenos, kurioje įrašyta informacija, medžiagos fizinis sunaikinimas, taikant Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašo 4 priede nurodytus būdus *(Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas).*

Lankytojas – asmuo, neinantis pareigų teisėtai lankomame paslapčių subjekto ar jo struktūrinio padalinio, rangovo (subrangovo) teritorijoje ar patalpose *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

Lankytojo kortelė – lankytojui išduodama registruota kortelė su registracijos numeriu, jį identifikuojanti kaip lankytoją *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

Leidimas dirbti ar susipažinti su įslaptinta informacija – Valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka išduotas dokumentas, patvirtinantis asmens teisę dirbti ar susipažinti su Lietuvos Respublikos įslaptinta informacija, žymima slaptumo žymomis „Visiškai slaptai“, „Slaptai“, „Konfidencialiai“, arba tokią informaciją saugoti ar gabenti *(Valstybės ir tarnybos paslapčių įstatymas)*.

Lokali saugumo aplinka – globalios saugumo aplinkos apsuptos I ir (ar) II klasių saugumo zonos, kuriose įdiegti ir arba eksploatuojami ADA sistemos ir tinklai ar jų sudėtinės dalys *(Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės)*.

M

Matavimas – fizikinių dydžių vertės nustatymas matavimo priemonėmis *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Matavimų įranga – laboratoriniai ir patalpų informatyviojo elektromagnetinio spinduliavimo (TEMPEST) matavimų prietaisai *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Matavimų rezultatai – ataskaitoje pateikti duomenys, gauti išanalizavus ir įvertinus preliminariuosius matavimų rezultatus *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Mechaninė įeigos kontrolės sistema – įeigos kontrolės sistema, kai raktai nuo durų, pro kurias galima patekti į saugumo zoną, užraktų išduodami tik paslapčių subjekto ar rangovo (subrangovo) įgaliotiems asmenims *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Mobilioji platforma – judrus objektas (lėktuvas, laivas, automobilis ir kt.), kuriame įrengta raudona įranga arba sistemos *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

N

Nacionalinė saugumo institucija (NSI) – valstybės institucija, atsakinga už apsikeistos įslaptintos informacijos apsaugą. Lietuvos Respublikoje NSI funkcijas atlieka Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija.

NATO VS kontrolės pareigūnas (angl. *COSMIC Control Officer*) – Šiaurės Atlanto Sutarties Organizacijos (toliau – NATO) Lietuvai perduotos įslaptintos informacijos, žymimos slaptumo žyma VISIŠKAI SLAPTAI (angl. *COSMIC TOP SECRET*), administravimą, apsaugą ir kontrolę vykdantis asmuo *(Asmenų, atsakingų už įslaptintos informacijos apsaugą, tipinis funkcijų sąrašas).*

NATO VS kontrolės pareigūną pavaduojantis asmuo (angl. *Alternate COSMIC Control Officer*) – nesant NATO VS kontrolės pareigūno, jo funkcijas vykdantis asmuo *(Asmenų, atsakingų už įslaptintos informacijos apsaugą, tipinis funkcijų sąrašas).*

Neatkuriamas informacijos trynimas – daugkartinio įrašymo laikmenoje įrašytos įslaptintos informacijos sunaikinimas, taikant Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašo 3 priede nurodytus būdus *(Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas).*

Neteisėtas patekimas – asmenų, neturinčių teisės būti saugumo zonoje, patekimas į ją *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

Neteisėta programinė įranga – programinė įranga, neįtraukta į paslapčių subjekto, rangovo (subrangovo) vadovo patvirtintą šio paslapčių subjekto, rangovo (subrangovo) valdomose ADA sistemose ir tinkluose leidžiamos naudoti programinės įrangos sąrašą, numatytą dokumentuose, reikalinguose gauti leidimą automatizuotai apdoroti ir perduoti įslaptintą informaciją ADA sistemomis ir tinklais *(Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas).*

Nešiojamoji laikmena – laikmena, kuri nėra stacionariai įmontuota į įrenginį, arba laikmena, stacionariai įmontuota į tokį įrenginį, kuris gali būti lengvai pernešamas iš vienos vietos į kitą *(Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas).*

O

Objektas – teritorija ir joje esantys pastatai, pastatų dalys, atskiros patalpos *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

Objekto apsaugos pultas – tai prietaisas, kuris kontroliuoja ir valdo objekto apsaugines įsilaužimo, apsaugines užpuolimo ir priešgaisrines signalizacijas bei perduoda informaciją apie jų būklę vietinio ir (arba) centralizuoto stebėjimo pultams *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai).*

P

Padauginti įslaptinti dokumentai – įslaptintų dokumentų kopijos, nuorašai, išrašai, vertimai *(Įslaptintos informacijos administravimo taisyklės)*.

Pasižadėjimas saugoti įslaptintą informaciją – asmens, kuriam suteiktas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, raštiškas įsipareigojimas saugoti jam patikėtą ar sužinotą įslaptintą informaciją *(Valstybės ir tarnybos paslapčių įstatymas)*.

Paslapčių subjektai – valstybės ir savivaldybių institucijos, kurių veikla susijusi su informacijos įslaptinimu, išslaptinimu, įslaptintos informacijos naudojimu ir (ar) apsauga, tokių institucijų reguliavimo sričiai priskirtos įstaigos, įmonės, kurioms šios institucijos, suderinusios su Paslapčių apsaugos koordinavimo komisija, suteikė paslapčių subjekto statusą *(Valstybės ir tarnybos paslapčių įstatymas)*.

Pastatas – stogu apdengtas statinys, kuriame yra vienas ar daugiau kambarių ar kitų patalpų, viena nuo kitos skiriamų sienų ir pertvarų ir naudojamų žmonėms gyventi ar žemės ūkio, prekybos, kultūros, transporto ir kitai veiklai *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Patalpa – pastato vidaus erdvė, apribota sienų ir/arba durų, ir/arba lango(ų) *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Patalpos sertifikatas – patalpos atitikties TEMPEST saugumo zonai liudijimas *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Pažeidžiamumas – ADA sistemos ir tinklo savybė, sudaranti galimybę pasireikšti grėsmei *(Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės)*.

Perimetras – saugumo zonos išorinės ribos *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Personalo patikimumas – nustatytos asmenų, kurie pretenduoja gauti leidimus dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimus, kandidatūrų tikrinimo procedūros, leidžiančios priimti sprendimą, ar asmeniui galima patikėti įslaptintą informaciją, taip pat asmens, kuriam

išduotas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, kontrolė ir periodiškas instruktavimas apie įslaptintos informacijos apsaugos reikalavimus ir įstatymų nustatytą atsakomybę už tokių reikalavimų pažeidimą *(Valstybės ir tarnybos paslapčių įstatymas)*.

Poligrafas – Lietuvos Respublikos Vyriausybės nustatytos formos sertifikatą turintis prietaisas, fiksuojantis kvėpavimo, kraujotakos, kitus fiziologinius pokyčius, atsirandančius asmens organizme tyrimo poligrafu metu, kuriais grindžiamas šiuo prietaisu tiriamo asmens teiginių teisingumo vertinimas *(Poligrafo naudojimo įstatymas)*.

Preliminarieji matavimų rezultatai – duomenys, gauti atlikus informatyviojo elektromagnetinio spinduliavimo (TEMPEST) matavimus (matavimų rezultatai tarpusavyje nesusieti ir neįvertinti pagal teisės aktus) *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Prieinamumas – įslaptintos informacijos (ADA sistemos ar tinklo paslaugos ar ištekliaus) savybė – įslaptinta informacija gali būti tvarkoma (ADA sistemos ar tinklo paslauga ar ištekliumi gali būti naudojamasi) reikiamu teisėtam naudotojui metu *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas)*.

Profesinis pažeidimas – konkurencijos, darbo, darbuotojų saugos ir sveikatos, aplinkos apsaugos, informacijos apsaugos teisės aktų pažeidimas, už kurį tiekėjui, kuris yra fizinis asmuo, yra paskirta administracinė nuobauda, o tiekėjui, kuris yra juridinis asmuo, – ekonominė sankcija, nustatyta Lietuvos Respublikos įstatymuose, kai nuo sprendimo, kuriuo buvo paskirta ši sankcija, įsiteisėjimo dienos praėjo mažiau kaip vieni metai. Jeigu pirkime dalyvaujantis tiekėjas, kuris yra juridinis asmuo, pažeidė Lietuvos Respublikos konkurencijos įstatymo 5 straipsnį, toks pažeidimas pagal šį punktą laikomas profesiniu, jeigu nuo sprendimo paskirti Lietuvos Respublikos konkurencijos įstatyme nustatytą ekonominę sankciją įsiteisėjimo dienos praėjo mažiau kaip 3 metai *(Viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymas)*.

R

Radijo dažnių siųstuvas – elektroninis (elektrinis) įtaisas, įrenginys, spinduliuojantis radijo dažnio diapazonu *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Rangovas – kiekvienas ūkio subjektas – fizinis asmuo, privatus juridinis asmuo, viešasis juridinis asmuo, kitos organizacijos ir jų padaliniai ar tokių asmenų grupė – galintis pasiūlyti ar siūlantis prekes, paslaugas ar darbus, su kuriuo paslapčių subjektas numato sudaryti ar yra sudaręs įslaptintą sandorį *(Valstybės ir tarnybos paslapčių įstatymas)*.

Rangovo (subrangovo) sutikimas būti tikrinamam – rangovo (subrangovo), kuriam reikia gauti įmonės patikimumą patvirtinantį pažymėjimą, raštiškas sutikimas, suteikiantis teisę įslaptintų sandorių saugumą užtikrinančioms institucijoms rinkti ir gauti duomenis apie rangovą (subrangovą) *(Valstybės ir tarnybos paslapčių įstatymas)*.

Rangovo (subrangovo) leidimas dirbti ar susipažinti su įslaptinta informacija – Valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka fiziniam asmeniui, savarankiškai užsiimančiam ūkine veikla, išduotas dokumentas, kuriuo patvirtinama asmens teisė dirbti ar susipažinti su įslaptinta informacija, tokią informaciją saugoti ir kuriuo suteikiama teisė sudaryti įslaptintus sandorius *(Valstybės ir tarnybos paslapčių įstatymas)*.

Raudona – laidinės linijos, optiniai kabeliai, komponentai, įranga ir sistemos, kuriose apdorojama ar kuriomis perduodama nešifruota įslaptinta informacija (pažymėta žyma „Konfidencialiai“ ar aukštesne), taip pat minėtos įrangos elektromagnetinis spinduliavimas ir zonos, kuriose tvarkoma nesifruota islaptinta informacija *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Reagavimo grupė – dviejų ar daugiau apsaugos darbuotojų, reaguojančių į apsauginės įsilaužimo, apsauginės užpuolimo ir priešgaisrinės signalizacijų suveikimo signalą, grupė, kurios tikslas yra užkirsti kelią neteisėtam patekimui į saugumo zoną, įslaptintos informacijos atskleidimui ar praradimui *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Reagavimo sistema – apsaugos darbuotojas, reagavimo grupė arba paslapčių subjekto ar rangovo (subrangovo) asmuo, atsakingas už fizinę apsaugą *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Rizika – grėsmės pasireiškimo per tam tikrą laiko tarpą tikimybė *(Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės)*.

RN sistema ar tinklas – ADA sistema, kurioje saugoma, apdorojama įslaptinta informacija, žymima slaptumo žyma „Riboto naudojimo“, ar tinklas, kuriuo tokia informacija yra perduodama *(Automatizuoto duomenų apdorojimo*

sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas).

S

Saugos dokumentai – ADA sistemos ar tinklo valdytojo įsakymu patvirtinti teisės aktai, reglamentuojantys ADA sistemos ar tinklo saugą, nurodyti Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklėse *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas)*.

Saugumo aplinka – apibrėžta teritorija, patalpa ar erdvė, kurioje išdėstyta įranga, užtikrinanti įslaptintą informaciją tvarkančios ADA sistemos ir tinklo veikimą, kurioje nustatytos atitinkamos saugumo valdymo procedūros arba kurioje tvarkoma įslaptinta informacija *(Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės)*.

Saugumo incidentas – įvykis, veiksmas ar neveikimas, kuris sudaro ar gali sudaryti sąlygas neteisėtai prisijungti prie ADA sistemos ar tinklo, sutrikdyti ar pakeisti (įskaitant valdymo perėmimą) ADA sistemos ar tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti įslaptintą informaciją, elektroninius duomenis, panaikinti ar apriboti galimybę naudotis įslaptinta informacija, elektroniniais duomenimis, taip pat sudaryti sąlygas pasisavinti, paskelbti, platinti ar kitaip neteisėtai naudoti įslaptintą informaciją, elektroniniais duomenimis *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas)*.

Saugumo institucija – valstybės narės Nacionalinė saugumo institucija; Generalinis Sekretorius, veikiantis Šiaurės Atlanto Tarybos vardu ir jos vadovaujamas, taip pat santykiuose su Šiaurės Atlanto Taryba; Karinio komiteto pirmininkas; NATO vyriausieji vadai; taip pat Kanados ir Jungtinių Amerikos Valstijų regioninės planavimo grupės pirmininkas *(Šiaurės Atlanto Sutarties Šalių susitarimas dėl bendradarbiavimo, susijusio su atomine informacija)*.

Saugumo priežiūros tarnyba (**SPT**) – Lietuvos Respublikos Vyriausybės įgaliota valstybės institucija, vykdanti leidimų automatizuotai apdoroti ir perduoti įslaptintą informaciją automatizuoto duomenų apdorojimo (toliau vadinama – ADA) sistemomis ir tinklais išdavimo, šių sistemų ir tinklų apsaugos kontrolės paslapčių subjektuose ir kitas teisės aktuose numatytas funkcijas *(Bendrosios (visiems vienodos) žinybinių priežiūros tarnybų steigimo ir veiklos taisyklės)*.

Saugumo valdymo procedūros – Saugumo valdymo procedūrų apraše aprašytos įslaptintos informacijos apsaugos reikalavimų įgyvendinimo instrukcijos *(Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės)*.

Saugumo zona – nustatyta saugoma teritorija ar patalpa, skirta dirbti su įslaptinta informacija ir šiai informacijai saugoti *(Valstybės ir tarnybos paslapčių įstatymas)*.

Saugumo zonos patikrinimas – patikrinimas, kurio metu nustatoma, ar saugumo zonos apsaugos sistemos įjungtos, jos veikia ir nėra pažeistos, bei nustatoma, ar nėra neteisėtai patekta į saugumo zoną *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Subrangovas – įslaptinto sandorio daliai vykdyti rangovo pasitelktas kitas asmuo *(Valstybės ir tarnybos paslapčių įstatymas)*.

Subrangos sutartis – laimėjusio viešojo pirkimo dalyvio ir vieno arba kelių tiekėjų raštu sudaryta sutartis už piniginį atlygį atlikti darbus, numatytus perkančiosios organizacijos su laimėjusiu dalyviu sudarytoje viešojo pirkimo-pardavimo sutartyje *(Viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymas)*.

Surinkimo taškas – iš anksto nustatyta (-tos) vieta (-tos) paslapčių subjekto, rangovo (subrangovo) pastate ar teritorijoje, kur evakavimą vykdantys darbuotojai privalo sunešti evakuoti skirtas talpas ir iš kurios jos bus išgabentos į parinktą evakuacijos vietą *(Įslaptintos informacijos evakuacijos arba sunaikinimo planų karo, nepaprastosios padėties ar ekstremalių situacijų atveju rengimo rekomendacijos)*.

Sutikimas būti tikrinamam – asmens, kuris pretenduoja gauti leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą, raštiškas sutikimas, suteikiantis teisę įgaliotoms institucijoms rinkti bei gauti duomenis apie jį ir jo ryšius bei aplinką, turinčius įtakos vertinant asmens patikimumą ir lojalumą Lietuvos valstybei *(Valstybės ir tarnybos paslapčių įstatymas)*.

S sistema ar tinklas – ADA sistema, kurioje saugoma, apdorojama įslaptinta informacija, žymima slaptumo žyma „Slaptai“, ar tinklas, kuriuo tokia informacija yra perduodama *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas)*.

T

Tarnybos paslaptis – Valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka įslaptinta politinė, karinė, žvalgybos, ekonominė, teisėsaugos, švietimo, mokslo, technikos ir kita informacija, kurios praradimas arba neteisėtas atskleidimas gali pakenkti valstybės ar jos institucijų interesams arba sudaryti prielaidas neteisėtam valstybės paslaptį sudarančios informacijos atskleidimui, sukelti pavojų žmogaus sveikatai *(Valstybės ir tarnybos paslapčių įstatymas)*.

Techniškai saugios zonos – I klasės saugumo zonos patalpos, kurios apsaugotos nuo neteisėtai naudojamų informacijos fiksavimo (vaizdo, garso ir elektromagnetinių signalų įrašymo) ir perdavimo įrenginių naudojimo *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

TEMPEST įranga – ADA sistemų ir tinklų įranga, atitinkanti NATO ar ES TEMPEST reikalavimus *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

TEMPEST laboratorija – elektromagnetinių matavimų laboratorija, vykdanti TEMPEST įrangos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) lygionustatymo matavimus ir turinti įgaliotos TEMPEST institucijos išduotą sertifikatą, patvirtinantį atitiktį TEMPEST laboratorijoms nustatytiems reikalavimams *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

TEMPEST zona – tam tikros patalpos (ploto, teritorijos) arba įrangos saugumo lygis, nustatytas vadovaujantis informatyviojo elektromagnetinio spinduliavimo standartais, kurie apibrėžia saugumo reikalavimus ADA sistemų ir tinklų infrastruktūrai apsaugoti nuo nesankcionuoto įslaptintos informacijos atskleidimo dėl informatyvaus elektromagnetinio spinduliavimo *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Teritorija – aiškiai apibrėžtas, fizinėmis ar kitomis priemonemis išskirtas žemės paviršiaus plotas, kuris turi valdytoją ar atsakingą asmenį/instituciją *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

Teritorijos apsaugos sistema – elektroninių ir mechaninių priemonių, skirtų paslapčių subjektui ar rangovui (subrangovui) priskirtos teritorijos apsaugai,

visuma *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Tyrimas poligrafu – kompleksinis psichofiziologinis tyrimas, skirtas asmens teiginių teisingumui įvertinti, naudojant poligrafą *(Poligrafo naudojimo įstatymas)*.

Tyrimo poligrafu specialistas – asmuo, turintis specialų profesinį pasirengimą bei atitinkantis kitus šio įstatymo nustatytus reikalavimus *(Poligrafo naudojimo įstatymas)*.

Tyrimo poligrafu subjektai – valstybės institucijos, pagal šį įstatymą įgaliotos atlikti tyrimą poligrafu *(Poligrafo naudojimo įstatymas)*.

U

Už laikmenų administravimą ir kontrolę atsakingas asmuo (toliau – Atsakingas asmuo) – paslapčių subjekto, rangovo (subrangovo) vadovo ar jo įgalioto asmens sprendimu paskirtas paslapčių subjekto, rangovo (subrangovo) struktūrinis padalinys arba darbuotojas, organizuojantis ir įgyvendinantis laikmenų, kuriomis disponuoja paslapčių subjektas, rangovas (subrangovas), administravimą ir kontrolę. Atsakingo asmens funkcijos gali būti pavestos keliems to paties paslapčių subjekto, rangovo (subrangovo) atskirų struktūrinių padalinių darbuotojams *(Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas)*.

Uždaroji vaizdo stebėjimo sistema – vaizdo stebėjimo sistema, skirta apsaugos darbuotojams stebėti teritoriją aplink objektą, objekto viduje esančių saugumo zonų prieigas ar saugumo zonų viduje esančias patalpas bei kaupti vaizdo įrašų archyvą *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Užsakovas – Lietuvos Respublikos paslapčių subjektai ar jiems pavaldžios valstybės įstaigos, jų struktūriniai padaliniai ir rangovai (subrangovai) *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

V

Valstybės paslaptis – Valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka įslaptinta politinė, karinė, žvalgybos, teisėsaugos, mokslo, technikos ir kita informacija, kurios praradimas arba neteisėtas atskleidimas gali sukelti grėsmę Lietuvos Respublikos suverenitetui, teritorijos vientisumui, gynybinei galiai, padaryti žalos valstybės interesams, sukelti pavojų žmogaus gyvybei.

(Valstybės ir tarnybos paslapčių įstatymas).

Vientisumas – įslaptintos informacijos (ADA sistemos ar tinklo paslaugos ar ištekliaus) savybė – įslaptinta informacija (ADA sistemos ar tinklo paslauga ar išteklius) nėra atsitiktiniu ar neteisėtu būdu pakeista (pakeistas) ar sunaikinta (sunaikintas) *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas)*.

Vietinis stebėjimo pultas – prietaisas, priimantis saugomo objekto (saugomas objektas tūri būti vienas) apsaugos pultų pranešimus laidinėmis, belaidėmis ryšio linijomis, formuojantis šviesos ir garso signalus savo indikatoriuose arba periferiniuose įrenginiuose *(Bendrieji įslaptintos informacijos fizinės apsaugos reikalavimai)*.

Vykdytojas – asmuo, parengęs įslaptintą dokumentą arba vykdantis užduotis, tiesiogiai susijusias su įslaptintu dokumentu *(Įslaptintos informacijos administravimo taisyklės)*.

Vykdytojas – įgaliotų TEMPEST institucijų funkcijas vykdantis struktūrinis padalinys (padaliniai) ar tuo tikslu sudaryta darbo grupė *(ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašas)*.

VS sistema ar tinklas – ADA sistema, kurioje saugoma, apdorojama įslaptinta informacija, žymima slaptumo žyma „Visiškai slaptai“, ar tinklas, kuriuo tokia informacija yra perduodama *(Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas)*.

Ž

Žinybinė saugumo priežiūros tarnyba – teisės aktų nustatyta tvarka paslapčių subjekto vadovo ar jo įgalioto asmens sprendimu paskirtas ar įsteigtas struktūrinis paslapčių subjekto padalinys, institucija ar įstaiga, vykdanti ADA sistemų ir tinklų apsaugos kontrolės ir leidimų automatizuotai apdoroti ir perduoti įslaptintą informaciją paslapčių subjekto, jo rangovo (subrangovo) ADA sistemomis ir tinklais išdavimo funkcijas *(Valstybės ir tarnybos paslapčių įstatymas)*.

Žymėjimo ženklas – priemonė (lipdukas ar užrašas) skirta palengvinti evakuotinos ar naikintinos informacijos atskyrimą *(Įslaptintos informacijos evakuacijos arba sunaikinimo planų karo, nepaprastosios padėties ar ekstremalių situacijų atveju rengimo rekomendacijos)*.

VALSTYBĖS IR TARNYBOS PASLAPČIŲ APSAUGA

NORMINIŲ TEISĖS AKTŲ RINKINYS

II dalis

Mokomoji knyga

Atsakingoji redaktorė Audronė Petrauskaitė
Kalbos redaktorė Jolanta Budreikienė
Viršelio dizainerė Laima Adlytė
Maketuotoja Jolanta Girnytė

2014-02-21. Tiražas 150 egz. Užsakymas GL-86.
Išleido Generolo Jono Žemaičio Lietuvos karo akademija,
Šilo g. 5A, LT-10322 Vilnius
Spausdino Lietuvos kariuomenės Karo kartografijos centras,
Muitinės g. 4, Domeikava, LT-54359 Kauno r.