LIETUVOS RESPUBLIKOS
VALSTYBĖS IR TARNYBOS PASLAPČIŲ ĮSTATYMO PAKEITIMO
Į S T A T Y M A S

2003 m. gruodžio 16 d. Nr. IX-1908
Vilnius

(Žin., 1999, Nr. 105-3019)

1 straipsnis. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo nauja redakcija

Pakeisti Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymą ir jį išdėstyti taip:

„**LIETUVOS RESPUBLIKOS**
VALSTYBĖS IR TARNYBOS PASLAPČIŲ
Į S T A T Y M A S

PIRMASIS SKIRSNIS
BENDROSIOS NUOSTATOS

1 straipsnis. Įstatymo paskirtis

1. Šis Įstatymas reglamentuoja pagrindinius valstybės ar tarnybos paslaptį sudarančios informacijos įslaptinimo, saugojimo, naudojimo, išslaptinimo, apsaugos veiksmų koordinavimo bei kontrolės pagrindus ir tvarką, nustato minimalius atskirų įslaptintos informacijos apsaugos sričių (personalo patikimumas, įslaptintos informacijos administravimas, fizinė apsauga, įslaptintų sandorių saugumas, automatizuoto duomenų apdorojimo sistemų ir tinklų apsauga) reikalavimus.

2. 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 informacijos 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.

2 straipsnis. Pagrindinės šio Įstatymo sąvokos

1. **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.

2. **Valstybės paslaptis** – šio Įstatymo nustatyta tvarka įslaptinta politinė, karinė, žvalgybos, kontržvalgybos, teisėsaugos, mokslo ir technikos 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 paslapčių kategorijų sąrašą nustato šis Įstatymas.

3. **Tarnybos paslaptis** – šio Įstatymo nustatyta tvarka įslaptinta politinė, karinė, ekonominė, teisėsaugos, mokslo ir technikos 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. Tarnybos paslapčių kategorijų sąrašą nustato šis Įstatymas.

4. **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.

5. **Įslaptinti gaminiai** – valstybės ar tarnybos paslaptimi pripažinti įvairūs įrenginiai, sistemos, ginkluotė, karinės, kompiuterinės bei kitos technikos įranga, kompleksai, agregatai, prietaisai, programinė įranga ir chemijos produkcija.

6. **Įslaptinti darbai** – valstybės ar tarnybos paslaptimi pripažinti mokslo, tyrimo, bandymų, projektavimo, techninio aptarnavimo darbai bei technologiniai procesai.

7. **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.

8. **Paslapčių subjektai** – Respublikos Prezidento, Seimo, Vyriausybės steigiamos institucijos, valstybės ir savivaldybių institucijos, jų steigiamos įmonės ir įstaigos, kurių veikla yra susijusi su informacijos įslaptinimu ir išslaptinimu, įslaptintos informacijos naudojimu ar jos apsauga.

9. **Įslaptintos informacijos rengėjas** – paslapčių subjektas, parengęs ir šio Įstatymo nustatyta tvarka įslaptinęs informaciją, arba jo teisių perėmėjas.

10. **Įslaptintos informacijos gavėjas** – paslapčių subjektas ar jo struktūrinis padalinys, asmuo, rangovas (subrangovas), teisės aktų nustatyta tvarka gavęs kito paslapčių subjekto parengtą įslaptintą informaciją.

11. **Informacijos įslaptinimas** – duomenų priskyrimas valstybės ar tarnybos paslapčiai, atitinkamos slaptumo žymos suteikimas, įslaptinimo termino nustatymas ir reikiamos apsaugos suteikimas.

12. **Įslaptintos informacijos išslaptinimas** – duomenims suteiktos slaptumo žymos ir nustatytos apsaugos panaikinimas.

13. **Įslaptintos informacijos apsauga** – apsaugos priemonių ir procedūrų taikymas siekiant išvengti įslaptintos informacijos praradimo ar neteisėto atskleidimo.

14. **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.

15. **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.

16. **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.

17. **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.

18. **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.

19. **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.

20. **Saugumo zona** – nustatyta saugoma teritorija ar patalpa, skirta dirbti su įslaptinta informacija ir šiai informacijai saugoti.

21. **Įslaptintos informacijos administravimas** – skirtingas slaptumo žymas turinčios įslaptintos informacijos rengimo, įforminimo, registracijos, siuntimo, gabenimo, gavimo, dauginimo, saugojimo, sunaikinimo bei apskaitos procedūros.

22. „**Būtinas informacijos rengėjo sutikimas**“ – nuoroda, žyminti, kad įslaptintas dokumentas negali būti dauginamas ar platinamas be įslaptintos informacijos rengėjo sutikimo.

23. **Automatizuoto duomenų apdorojimo sistemų ir tinklų** (toliau – **ADA sistemos ir tinklai**) **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 vartotojams bei tokios informacijos vientisumą ir autentiškumą.

24. **Įslaptintas sandoris** – paslapčių subjekto ir juridinio ar fizinio asmens sudaryta sutartis dėl tam tikrų darbų, gaminių ar kitų objektų, kurie patys arba informacija apie kuriuos yra žymima slaptumo žymomis „Visiškai slaptai“, „Slaptai“ arba „Konfidencialiai“, atlikimo, sukūrimo, pirkimo, pardavimo, tiekimo, fizinės apsaugos, gabenimo bei techninės priežiūros.

25. **Įslaptintų sandorių saugumas** – įslaptintos informacijos apsaugos priemonių ir procedūrų taikymas įslaptintų sandorių sudarymo bei vykdymo metu.

26. **Rangovas** – juridinis ar fizinis asmuo, su kuriuo paslapčių subjektas numato sudaryti ar yra sudaręs įslaptintą sandorį.

27. **Subrangovas** – įslaptinto sandorio daliai vykdyti rangovo pasitelktas kitas asmuo.

28. **Įmonės patikimumą patvirtinantis pažymėjimas** – šio Įstatymo nustatyta tvarka išduotas dokumentas, patvirtinantis, kad rangovas (subrangovas) yra įvykdęs visus įslaptintos informacijos apsaugos reikalavimus, būtinus konkrečiam įslaptintam sandoriui vykdyti. Reikalavimas gauti įmonės patikimumą patvirtinantį pažymėjimą yra taikomas tuo atveju, kai rangovas (subrangovas) yra juridinis asmuo.

29. **Įslaptintų sandorių saugumą užtikrinančios institucijos** – institucijos, įgyvendinančios įslaptintų sandorių saugumo reikalavimus ir vykdančios kontrolę iki pasirašant įslaptintą sandorį ir tokio sandorio vykdymo metu.

30. **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).

31. **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.

32. **Darbuotojas** – valstybės tarnautojas ar asmuo, dirbantis pagal darbo sutartį, arba karys.

33. **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.

3 straipsnis. Pagrindiniai įslaptintos informacijos apsaugos organizavimo principai

1. Informacija turi būti įslaptinama ir išslaptinama vadovaujantis teisėtumo, pagrįstumo ir savalaikiškumo principais.

2. Informacija turi būti įslaptinama, jeigu ji atitinka bent vieną iš šio Įstatymo 7 straipsnyje nurodytų informacijos kategorijų ir jeigu jos atskleidimas ar praradimas sukeltų grėsmę valstybės ar jos institucijų interesams, žmogaus gyvybei ar teisėtiems visuomenės interesams.

3. Nustatoma informacijos slaptumo žyma ir tokiai informacijai suteikiamas apsaugos lygis turi būti proporcingas įslaptinamos informacijos svarbai bei žalos, kuri atsirastų tokią informaciją neteisėtai atskleidus ar praradus, dydžiui.

4. Paslapčių subjektas, įslaptinęs informaciją, privalo užtikrinti, kad įslaptinta informacija, pasibaigus įslaptinimo būtinybei arba tuo atveju, jei informacijai pagal jos svarbą nereikia anksčiau nustatyto apsaugos lygio, būtų nedelsiant išslaptinama arba tokiai informacijai būtų suteikta žemesnė slaptumo žyma ir apie tai būtų pranešta paslapčių subjektams, kuriems tokia informacija buvo perduota.

5. Įslaptintai informacijai visuose tokios informacijos administravimo etapuose turi būti užtikrinta reikiama apsauga visą jos įslaptinimo terminą.

6. Įslaptinta informacija turi būti patikima griežtai laikantis principo „Būtina žinoti“. Principas „Būtina žinoti“ reiškia, kad įslaptinta informacija gali būti patikėta tik atitinkamus leidimus dirbti ar susipažinti su įslaptinta informacija turintiems asmenims, kuriems vykdant tarnybines pareigas reikalinga susipažinti su įslaptinta informacija. Asmeniui gali būti patikėta tokios apimties įslaptinta informacija, kokios reikia jo pareigoms atlikti.

7. Įslaptintos informacijos apsaugai užtikrinti turi būti kompleksiškai taikomi visų įslaptintos informacijos apsaugos sričių (personalo patikimumo, įslaptintos informacijos administravimo, fizinės apsaugos, įslaptintų sandorių saugumo, ADA sistemų ir tinklų apsaugos) reikalavimai.

8. Apie visus įslaptintos informacijos apsaugos reikalavimų pažeidimus, kurie gali lemti ar lėmė įslaptintos informacijos praradimą ar neteisėtą atskleidimą, nedelsiant turi būti pranešta paslapčių subjekto vadovui, o šis privalo imtis reikiamų priemonių tolesniam įslaptintos informacijos atskleidimui ar praradimui sustabdyti ir neigiamoms pasekmėms sumažinti, taip pat privalo nedelsdamas pranešti įgaliotoms institucijoms, o šios nustatyta tvarka turi atlikti tyrimą dėl informacijos apsaugos reikalavimų pažeidimų faktų nustatymo ir kaltų asmenų patraukimo atsakomybėn.

4 straipsnis. Įslaptintos informacijos nuosavybės teisė, įslaptintos informacijos perdavimas užsienio valstybėms ar tarptautinėms organizacijoms

1. Įslaptinta informacija, išskyrus užsienio valstybių ar tarptautinių organizacijų paslaptį sudarančią informaciją, yra Lietuvos Respublikos nuosavybė.

2. Įsigyjant valstybės nuosavybėn informaciją, kuri pagal savo pobūdį ir svarbą turėtų būti įslaptinta, tačiau nuosavybės teise priklauso fiziniam ar juridiniam asmeniui, kuris nėra paslapčių subjektas, turi būti teisingai atlyginama. Sprendimą dėl informacijos įsigijimo valstybės nuosavybėn priima Vyriausybė. Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija (toliau – Paslapčių apsaugos koordinavimo komisija) paslapčių subjektų teikimu įvertina tokios informacijos įsigijimo pagrįstumą ir nustato galimą atlygį informacijos savininkui. Informacijos savininkui sutikus su siūlomu atlygiu, paslapčių subjektas kreipiasi į Vyriausybę, kad būtų priimtas atitinkamas sprendimas. Informacijos savininkui nesutikus su siūlomu atlygiu, informacija Vyriausybės sprendimu paimama valstybės nuosavybėn tokios informacijos savininkui atlyginant Paslapčių apsaugos koordinavimo komisijos nustatyta kaina. Informacijos savininkas tokį Vyriausybės sprendimą įstatymų nustatyta tvarka gali apskųsti teismui.

3. Valstybės paslaptį sudaranti informacija gali būti perduodama tik toms valstybėms ar tarptautinėms organizacijoms, su kuriomis Lietuvos Respublika yra pasirašiusi sutartis dėl įslaptintos informacijos abipusės apsaugos. Valstybėms ar tarptautinėms organizacijoms, su kuriomis Lietuvos Respublika nėra sudariusi sutarties dėl įslaptintos informacijos abipusės apsaugos, tokia informacija gali būti perduodama Paslapčių apsaugos koordinavimo komisijos sprendimu.

4. Tarnybos paslaptį sudaranti informacija užsienio valstybėms ar tarptautinėms organizacijoms gali būti perduodama paslapčių subjekto vadovo ar jo įgalioto asmens sprendimu, kai tai būtina paslapčių subjekto funkcijoms atlikti.

ANTRASIS SKIRSNIS
ĮSLAPTINTOS INFORMACIJOS ŽYMĖJIMAS, ĮSLAPTINIMAS, IŠSLAPTINIMAS

5 straipsnis. Informacijos klasifikavimas ir žymėjimas

1. Įslaptinta informacija pagal svarbą, galimos žalos, kurią patirtų valstybė, jos institucijos ar asmenys, jeigu ši informacija būtų prarasta arba atskleista neturintiems teisės ją sužinoti asmenims, dydį ir pagal apsaugos, būtinos tokiai informacijai apsaugoti, lygį yra skirstoma į visiškai slaptą, slaptą, konfidencialią bei riboto naudojimo informaciją.

2. Žyma „Visiškai slaptai“ suteikiama valstybės paslaptį sudarančiai informacijai, kurios praradimas arba neteisėtas atskleidimas gali sukelti grėsmę Lietuvos Respublikos suverenitetui ar teritorijos vientisumui arba turėti ypač sunkių pasekmių valstybės interesams, arba sukelti pavojų žmogaus gyvybei.

3. Žyma „Slaptai“ suteikiama valstybės paslaptį sudarančiai informacijai, kurios praradimas arba neteisėtas atskleidimas gali pažeisti valstybės gynybinę galią ar padaryti žalos valstybės interesams.

4. Žyma „Konfidencialiai“ suteikiama tarnybos paslaptį sudarančiai informacijai, kurios praradimas arba neteisėtas atskleidimas gali pakenkti valstybės interesams arba padaryti žalos valstybės institucijų veiklai ar sudaryti prielaidas neteisėtam valstybės paslaptį sudarančios informacijos atskleidimui.

5. Žyma „Riboto naudojimo“ suteikiama tarnybos paslaptį sudarančiai informacijai, kurios praradimas arba neteisėtas atskleidimas gali pakenkti valstybės institucijų interesams.

6. Slaptumo žymos nuo aukščiausios iki žemiausios yra šios:

1) „Visiškai slaptai“;

2) „Slaptai“;

3) „Konfidencialiai“;

4) „Riboto naudojimo“.

7. Draudžiama šiame straipsnyje nustatytas informacijos slaptumo žymas suteikti šio Įstatymo nereglamentuojamai informacijai.

6 straipsnis. Informacijos įslaptinimas

1. Informacijos įslaptinimo pagrindas – šio Įstatymo 7 straipsnyje išdėstytas įslaptinamos informacijos kategorijų sąrašas, remiantis šiuo sąrašu paslapčių subjektų parengti ir nustatyta tvarka patvirtinti detalūs įslaptinamos informacijos sąrašai bei konkrečios įslaptinamos informacijos turinys.

2. Informacijai slaptumo žymas suteikia, keičia ir jos įslaptinimo terminus nustato informaciją parengę paslapčių subjektai šio Įstatymo nustatyta tvarka.

3. Už informacijos įslaptinimą ir pagrįstų slaptumo žymų suteikimą atsako paslapčių subjekto struktūrinio padalinio, parengusio ir nustatyta tvarka įslaptinusio informaciją, vadovas.

7 straipsnis. Įslaptinamos informacijos kategorijų sąrašas

1. Valstybės paslaptį gali sudaryti:

1) detalūs duomenys apie valstybės gynybinį rezervą ir suvestiniai detalizuoti duomenys apie mobilizacinį materialinių išteklių rezervą;

2) valstybės ir savivaldybių institucijų veiklos nepaprastosios padėties ir karo padėties sąlygomis planai bei mobilizacijos planai;

3) detalūs duomenys apie technologinės apsaugos elementų, naudojamų vertybiniams popieriams, dokumentams, banderolėms, žymenims, banknotams, monetoms nuo suklastojimo apsaugoti, kūrimą, gamybos technologijas, fizikines ir chemines savybes;

4) detali informacija apie technologinių procesų panaudojimą kokybiškai tobulinant ginkluotę, karinę techniką bei operatyvinėje veikloje naudojamas technines priemones;

5) detali informacija apie derybas su užsienio valstybėmis ar tarptautinėmis organizacijomis; su užsienio valstybėmis ar tarptautinėmis organizacijomis susijusi informacija, kurios praradimas arba neteisėtas atskleidimas gali pakenkti valstybių tarpusavio santykiams, valstybės interesams arba sutarčių sudarymui;

6) detali informacija apie bendradarbiavimo su užsienio valstybių ar tarptautinių organizacijų specialiosiomis tarnybomis eigą, objektus, turinį, rezultatus;

7) detalūs duomenys apie Ignalinos valstybinės atominės elektrinės apsaugos organizavimą;

8) detalūs duomenys apie įslaptintos informacijos perdavimui skirtų tinklų kabelines magistrales, įrengimų įjungimo, elektros tiekimo ir nekriptografines apsaugos sistemas bei jų detalias schemas;

9) duomenys apie šifrus, šifravimo techniką, skirtą įslaptintai informacijai šifruoti ar jai apsaugoti, ir su tuo susijusius dokumentus, šifravimo darbų organizavimą bei atlikimą;

10) duomenys apie informacinių sistemų, apdorojančių įslaptintą informaciją, įrangą, veikimą, taikomas apsaugos priemones;

11) detalūs duomenys apie radijo dažnių, šaukinių naudojimą karo ar neparastosios padėties atveju, taip pat telekomunikacijų tinklų sandarą, ryšio schemas bei jungiamųjų linijų, telekomunikacinių tinklų eksploatavimą valstybės saugumo ir gynybos tikslams;

12) valstybės gynybos, kariuomenės ir kitų ginkluotųjų pajėgų valdymo ir vadovavimo planai;

13) detalūs duomenys apie valstybės gynybai naudojamą oro erdvės stebėjimo ir kontrolės sistemą;

14) mobilizaciniai kariuomenės ir jos rūšių, kitų ginkluotųjų pajėgų išdėstymo planai, mobilizacinio pranešimo ir mobilizacinio išdėstymo valdymo schema, taip pat informacija apie kariuomenės bei kitų ginkluotųjų pajėgų veiksmus ir karinių vienetų valdymą aliarmo parengties pakopų įvedimo atveju;

15) suvestiniai detalizuoti Lietuvos Respublikos ginklų fondo prie Lietuvos Respublikos Vyriausybės (toliau – Ginklų fondas) tvarkomo registro duomenys, kai ginklo savininkas, valdytojas ar naudotojas yra krašto apsaugos sistemos institucija, vidaus reikalų sistemos ar Valstybės saugumo departamento sistemos institucija arba operatyvinės veiklos subjektai;

16) informacija, galinti atskleisti operatyvinės veiklos slaptųjų dalyvių asmens tapatybę;

17) detalūs duomenys apie operatyvinės veiklos slaptųjų dalyvių, apdraustų valstybiniu socialiniu draudimu bei privalomuoju sveikatos draudimu, įskaitos duomenis, valstybinio socialinio draudimo ir privalomojo sveikatos draudimo įmokas, pajamų mokesčių įmokas, šių asmenų ir jų šeimos narių turto ir pajamų deklaravimo duomenys;

18) detalūs duomenys apie Valstybės saugumo departamento bei Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos struktūrinių padalinių, vykdančių žvalgybą ar kontržvalgybą, vykdomos operatyvinės veiklos organizavimą, eigą ir rezultatus, priemonių ir metodų naudojimą, jų finansavimą, aprūpinimą operatyvinės veiklos techninėmis priemonėmis, kitą materialinį bei techninį aprūpinimą, operatyvinių veiksmų metu gauta informacija, taip pat analitinė informacija, kurioje naudojama žvalgybos, kontržvalgybos metu gauta informacija;

19) detalūs duomenys apie operatyvinės veiklos subjektų operatyvinės veiklos slaptųjų dalyvių vykdomos operatyvinės veiklos organizavimą, eigą ir rezultatus, priemonių ir metodų naudojimą, jų finansavimą, materialinį bei techninį aprūpinimą, operatyvinės veiklos slaptųjų dalyvių operatyvinių veiksmų metu gauta informacija bei jos pagrindu parengta analitinė informacija;

20) informacija, kurią esami ar buvę kitų valstybių specialiųjų tarnybų darbuotojai ar slaptieji bendradarbiai savanoriškai suteikė operatyvinės veiklos subjektams;

21) ikiteisminio tyrimo ar baudžiamosios bylos medžiagoje esantys įslaptinti liudytojo ar nukentėjusiojo asmens tapatybę padedantys nustatyti duomenys;

22) duomenys, galintys atskleisti tapatybę asmenų, kuriems pagal įstatymus taikoma apsauga nuo nusikalstamo poveikio, taip pat informacija apie šių asmenų pajamų mokesčio įmokas, detali informacija apie tokių asmenų apsaugos organizavimą ir apsaugos finansavimą;

23) kovos su terorizmu bei diversijomis operacijų planai;

24) informacija, susijusi su įslaptintais žvalgybos tarnautojais bei žvalgybos slaptaisiais bendradarbiais, apie jiems taikomas specialias garantijas;

25) informacija, susijusi su operatyvinę veiklą užtikrinančiais ir jai palankias sąlygas sudarančiais juridiniais asmenimis;

26) nacionalinį saugumą užtikrinančių institucijų parengta analitinė informacija, susijusi su užsienio rizikos veiksnių ir grėsmių įvertinimu;

27) duomenys apie krašto apsaugos sistemos specialiosios paskirties karinių vienetų operacijų eigą bei jų personalinę sudėtį;

28) detalūs duomenys apie naujas technologijas, mokslinius tyrimus, bandymus ir jų rezultatus, turinčius ypatingą reikšmę valstybės interesams.

2. Tarnybos paslaptį gali sudaryti:

1) detalūs duomenys apie įslaptintos informacijos apsaugos organizavimą, tokios informacijos apskaitą ir tvarkymą;

2) detalūs duomenys apie asmenų, pretenduojančių gauti leidimą dirbti ar susipažinti su įslaptinta informacija, kandidatūrų tikrinimo tvarką bei eigą, taip pat tikrinimo metu apie juos surinkti detalizuoti duomenys, jei tokie duomenys nepriskiriami valstybės paslapčiai;

3) ikiteisminio tyrimo institucijų detalūs planai dėl asmenų, padariusių, įtariamų ar kaltinamų padariusių nusikalstamas veikas, paieškos ir sulaikymo bei kompleksinių priemonių ir operacijų organizavimo;

4) detalūs duomenys apie valstybės institucijų ar jų struktūrinių padalinių saugomų asmenų ir svarbių valstybės bei karinių objektų apsaugos organizavimą, naudojamas apsaugos sistemas, tokių objektų projektavimo, statybos ir remonto darbų dokumentai;

5) informacija apie operatyvinės veiklos subjektų sąveiką operatyvinės veiklos tikslais su savivaldybės institucijomis, įmonėmis, įstaigomis ir organizacijomis;

6) suvestiniai detalizuoti duomenys apie Lietuvos kariuomenės specialiosios paskirties padalinių ir operatyvinės veiklos subjektų materialinį techninį aprūpinimą, kiekybinę ir personalinę sudėtį;

7) suvestiniai detalizuoti duomenys apie valstybės materialinių išteklių rezervą;

8) duomenys apie Lietuvos kariuomenės specialiosios paskirties padalinių, operatyvinės veiklos subjektų tvarkomą jų pareigūnų, apdraustų valstybiniu socialiniu draudimu, įskaitą ir duomenys apie išvardytų subjektų lėšas jų pareigūnų valstybinio socialinio draudimo įmokoms bei pajamų mokesčių įmokoms;

9) detalūs duomenys apie specialiųjų krovinių gabenimo organizavimą ir taktiką;

10) detalūs duomenys apie Lietuvos kariuomenės, krašto apsaugos sistemos institucijų, vidaus reikalų sistemos institucijų, operatyvinės veiklos subjektų aprūpinimą ryšio įranga, radijo dažnių ir šaukinių naudojimo tvarką;

11) bankų ir kitų kredito įstaigų, draudimo įmonių, draudimo tarpininkų, loterijas ir azartinius lošimus organizuojančių įmonių inspektavimo ir tikrinimo duomenys;

12) nacionalinės ir bazinės valiutos kurso nustatymo projektai bei duomenys apie Lietuvos banko vykdomų atpirkimo sandorių, terminuotų indėlių, Vyriausybės, Lietuvos banko vertybinių popierių aukcionų dalyvius ir jų siūlymus, likvidumo paskolas;

13) informacija, pateikta finansinių institucijų pasiūlymuose dėl valstybės skolinimosi užsienio ir vidaus kapitalo rinkose ir išvestinių finansinių priemonių taikymo;

14) suvestiniai detalizuoti duomenys apie valstybės sienos apsaugos organizavimą ir vykdymą bei su tuo susiję planai;

15) detalūs Lietuvos kariuomenės, atskirų jos rūšių, kitų krašto apsaugos sistemos institucijų ir ginkluotųjų pajėgų organizacinės bei techninės plėtros planai;

16) suvestiniai detalizuoti duomenys apie Lietuvos kariuomenės, kitų krašto apsaugos sistemos institucijų ir ginkluotųjų pajėgų, vidaus reikalų sistemos institucijų, operatyvinės veiklos subjektų, Ginklų fondo aprūpinimą ginklais, šaudmenimis, sprogmenimis, kovine technika, specialiosiomis priemonėmis, taip pat informacija apie operatyvinės veiklos subjektų aprūpinimą operatyvinės veiklos techninėmis priemonėmis;

17) detalūs duomenys apie ginklų, šaudmenų, sprogmenų, kovinės technikos, specialiųjų priemonių, operatyvinės veiklos techninių priemonių gamybos programas ir planus;

18) detalūs duomenys apie operatyvinės veiklos subjektų lėšas ir išlaidas operatyvinei veiklai vykdyti, ginklams, šaudmenims, sprogmenims, kovinei technikai, specialiosioms priemonėms ir operatyvinės veiklos techninėms priemonėms įsigyti;

19) detalūs duomenys apie krašto apsaugos sistemos institucijų, vidaus reikalų sistemos institucijų, operatyvinės veiklos subjektų, prokuratūros, Lietuvos banko, Ginklų fondo turimus ginklus, šaudmenis, sprogmenis, kovinę techniką, specialiąsias priemones, operatyvinės veiklos technines priemones, taip pat asmens saugos ir aktyviosios ginties, radiacinės ir cheminės saugos, specialiųjų degazavimo priemonių ir inžinerinės technikos saugojimo bei apskaitos normas, paskirstymą ir apsaugos organizavimą;

20) detalūs duomenys apie operatyvinės veiklos subjektų operatyvinės veiklos organizavimą ir eigą, priemonių ir metodų naudojimą, užduotis, operacijas, jų finansavimą, rezultatus, materialinį bei techninį aprūpinimą, operatyvinių veiksmų metu gauta informacija, jeigu tokia informacija nepriskiriama valstybės paslaptims, taip pat operatyvinės veiklos subjektų parengta analitinė-informacinė medžiaga, kurioje naudojama operatyvinių veiksmų metu gauta informacija;

21) Lietuvos Respublikos topografiniai žemėlapiai, kuriuose nurodytos strateginių objektų charakteristikos, karinių ir valstybės sienos apsaugos objektų charakteristikos bei paskirtis, taip pat karinės paskirties žemėlapiai;

22) tyrimo poligrafu išvada ir tyrimo metu padaryti garso ir (ar) vaizdo įrašai;

23) informacija, telekomunikacinės veiklos reguliavimo, priežiūros ir Telekomunikacijų įstatymo nuostatų įgyvendinimo tikslams gauta iš valstybės ir savivaldybės institucijų, telekomunikacijų operatorių bei paslaugų teikėjų ir radijo dažnių (kanalų) bei telefono ryšio numerių naudotojų;

24) informacija apie Strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymo 3 straipsnio 1 dalyje ir 4 straipsnio 1 dalyje nurodytų įmonių privatizavimo sandorių sudarymą, jeigu tokios informacijos atskleidimas padarytų žalą valstybės ekonominiams ir politiniams interesams;

25) valstybės institucijų parengta informacija apie kandidato į Lietuvos Respublikos diplomatinius atstovus asmenines ir dalykines savybes, turinčias įtakos sprendimo dėl jo paskyrimo priėmimui.

3. Įslaptinta informacija, išvardyta šio straipsnio 1 dalyje, informacijos rengėjo sprendimu gali būti įslaptinama kaip tarnybos paslaptis, jei pagal savo turinį bei dydį galimos žalos, kurią patirtų valstybė ją neteisėtai atskleidus ar praradus, tokia informacija nereikalauja aukštesnio apsaugos lygio.

4. Paslapčių subjektai, vadovaudamiesi įslaptinamos informacijos kategorijų sąrašu, sudaro detalius įslaptinamos informacijos, susijusios su jų veikla, sąrašus. Detaliuose įslaptinamos informacijos sąrašuose turi būti numatytos įslaptinamos informacijos slaptumo žymos, tokios informacijos įslaptinimo terminai arba išslaptinimo sąlygos. Detalius įslaptinamos informacijos sąrašus tvirtina ir keičia paslapčių subjektų vadovai, suderinę su Paslapčių apsaugos koordinavimo komisija.

8 straipsnis. Įslaptinimo terminai

1. Informacija įslaptinama šiems terminams:

1) informacija, žymima slaptumo žyma „Visiškai slaptai“ – 30 metų, o informacija, padedanti nustatyti įslaptintų žvalgybos tarnautojų bei žvalgybos slaptųjų bendradarbių, taip pat

slaptųjų operatyvinės veiklos dalyvių asmens tapatybę, taip pat baudžiamojo proceso metu įslaptinti liudytojų ar nukentėjusiųjų anketiniai duomenys – 75 metams;

2) informacija, žymima slaptumo žyma „Slaptai“ – 15 metų;

3) informacija, žymima slaptumo žyma „Konfidencialiai“ – 10 metų;

4) informacija, žymima slaptumo žyma „Riboto naudojimo“ – 5 metams.

2. Informacijos įslaptinimo terminas skaičiuojamas nuo slaptumo žymos suteikimo dienos.

3. Tais atvejais, kai informaciją tikslinga įslaptinti trumpesniam įslaptinimo terminui, negu nustatyta šio straipsnio 1 dalyje, įslaptinimo terminas nurodomas šalia slaptumo žymos.

4. Tais atvejais, kai informacijos įslaptinimas yra tikslingas tik iki tam tikro įvykio, kuriam įvykus informacijos įslaptinimas nebetenka prasmės, šalia slaptumo žymos nurodomas konkretus įvykis ar kitos informacijos išslaptinimo sąlygos.

5. Tais atvejais, kai neįmanoma nustatyti konkretaus įslaptinimo termino, tačiau žinoma, kad netikslinga informaciją laikyti įslaptintą visą įstatymo nustatytą įslaptinimo terminą arba ją automatiškai išslaptinti pasibaigus įstatymo nustatytam įslaptinimo terminui, arba yra žinoma, kad bus keičiama įslaptintos informacijos slaptumo žyma, informacijos rengėjo sprendimu šalia slaptumo žymos rašoma nuoroda „ISS“ (išslaptinama subjekto sprendimu).

6. Tais atvejais, kai valstybės paslaptį sudarančios informacijos įslaptinimo terminas turi būti ilgesnis, negu nustatyta šio straipsnio 1 dalies 1 ir 2 punktuose, šį klausimą paslapčių subjekto teikimu sprendžia bei įslaptinimo terminą pratęsia Paslapčių apsaugos koordinavimo komisija. Įslaptinimo terminas gali būti pratęsiamas iki 10 metų. Pratęsimų skaičius neribojamas.

7. Tais atvejais, kai tarnybos paslaptį sudarančios informacijos įslaptinimo terminas turi būti ilgesnis, negu nustatyta šio straipsnio 1 dalies 3 ir 4 punktuose, šį klausimą sprendžia ir įslaptinimo terminą pratęsia įslaptintos informacijos rengėjas. Įslaptinimo terminas gali būti pratęsiamas iki 5 metų. Pratęsimų skaičius neribojamas.

8. Informacijos įslaptinimo pratęsimo terminas skaičiuojamas nuo sprendimo pratęsti informacijos įslaptinimo terminą priėmimo datos.

9 straipsnis. Įslaptintos informacijos slaptumo žymų ir įslaptinimo terminų keitimas

1. Įslaptintos informacijos rengėjas turi teisę šio Įstatymo nustatyta tvarka keisti nustatytą slaptumo žymą ir informacijos įslaptinimo terminą. Apie tokius pakeitimus raštu informuojami visi paslapčių subjektai, kuriems buvo perduota įslaptinta informacija.

2. Jeigu įslaptintos informacijos gavėjui atliekant savo funkcijas prireikia pakeisti nustatytą slaptumo žymą ar įslaptinimo terminą, jis motyvuotu prašymu privalo kreiptis į įslaptintos informacijos rengėją. Įslaptintos informacijos gavėjas gali keisti nustatytą slaptumo žymą ir įslaptinimo terminą tik gavęs informacijos rengėjo raštišką sutikimą.

10 straipsnis. Įslaptintos informacijos išslaptinimas

1. Įslaptinta informacija išslaptinama, kai:

1) pasibaigia šio Įstatymo 8 straipsnyje nustatytas įslaptinimo terminas;

2) išnyksta įslaptinimo tikslingumas, nors nustatytas įslaptinimo terminas dar nepasibaigęs.

2. Įslaptinta informacija, kai nustatytas įslaptinimo terminas dar nepasibaigęs, gali būti išslaptinama tik įslaptintos informacijos rengėjo sprendimu.

3. Pasibaigus nustatytam įslaptinimo terminui, informacija, žymima slaptumo žymomis „Visiškai slaptai“, „Slaptai“ ir „Konfidencialiai“, išslaptinama tik įslaptintos informacijos rengėjo sprendimu. Pasibaigus nustatytam įslaptinimo terminui, informacija, žymima slaptumo žyma „Riboto naudojimo“, laikoma išslaptinta nepriimant atskiro sprendimo, jeigu informacija neturi papildomos nuorodos ir informacijos rengėjas nepranešė apie informacijos įslaptinimo termino pratęsimą.

TREČIASIS SKIRSNIS

VALSTYBĖS INSTITUCIJŲ KOMPETENCIJA IR ĮGALIOJIMAI ĮSLAPTINTOS INFORMACIJOS APSAUGOS SRITYJE, INSTITUCIJŲ IR ASMENŲ ATSAKOMYBĖ UŽ ĮSLAPTINTOS INFORMACIJOS APSAUGOS VEIKSMŲ ĮGYVENDINIMĄ

11 straipsnis. Įslaptintos informacijos apsaugos koordinavimas

1. Lietuvos Respublikos įslaptintos informacijos, žymimos slaptumo žymomis „Visiškai slaptai“, „Slaptai“, „Konfidencialiai“, apsaugos veiksmus ir kitų valstybių ar tarptautinių organizacijų paslaptį sudarančios informacijos, perduotos Lietuvos Respublikai, apsaugos veiksmų įgyvendinimą Lietuvos Respublikos institucijose koordinuoja kolegiali institucija – Paslapčių apsaugos koordinavimo komisija. Paslapčių apsaugos koordinavimo komisijos nuostatus tvirtina Vyriausybė. Paslapčių apsaugos koordinavimo komisija turi savo blanką ir antspaudą.

2. Paslapčių apsaugos koordinavimo komisija susideda iš septynių narių – po du narius deleguoja Respublikos Prezidentas, Seimo Pirmininkas, Ministras Pirmininkas. Šios komisijos pirmininkas yra Valstybės saugumo departamento generalinis direktorius.

3. Valstybės saugumo departamento struktūrinis padalinys, įgyvendinantis ir kontroliuojantis įslaptintos informacijos apsaugos veiksmus, atlieka Paslapčių apsaugos koordinavimo komisijos sekretoriato funkcijas, šio padalinio vadovas skiriamas Paslapčių apsaugos koordinavimo komisijos sekretoriumi. Paslapčių apsaugos koordinavimo komisijos sekretoriatas rengia Paslapčių apsaugos koordinavimo komisijos posėdžių medžiagą, įgyvendina Paslapčių apsaugos koordinavimo komisijos priimtus sprendimus, kontroliuoja tokių sprendimų įgyvendinimą paslapčių subjektuose.

4. Paslapčių apsaugos koordinavimo komisijos nariais, sekretoriumi ir sekretoriato darbuotojais gali būti tik asmenys, kurie šio Įstatymo nustatyta tvarka yra gavę leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma „Visiškai slaptai“, bei asmens patikimumo pažymėjimą, suteikiantį teisę susipažinti su kitų valstybių ar tarptautinių organizacijų perduota įslaptinta informacija, žymima slaptumo žymos „Visiškai slaptai“ atitikmeniu.

5. Paslapčių apsaugos koordinavimo komisija atlieka šias pagrindines funkcijas:

1) koordinuoja Lietuvos Respublikos tarptautinių sutarčių dėl įslaptintos informacijos abipusės apsaugos reikalavimų įgyvendinimą, prireikus inicijuoja tokių sutarčių sudarymo ar sudarytų sutarčių denonsavimo procesą;

2) užtikrina užsienio valstybių, Europos Sąjungos ar tarptautinių organizacijų Lietuvos Respublikai perduotos įslaptintos informacijos, žymimos slaptumo žymų „Visiškai slaptai“, „Slaptai“ ir „Konfidencialiai“ atitikmenimis, reikiamų apsaugos veiksmų įgyvendinimo kontrolę, atlieka kitas funkcijas užtikrindama Lietuvos Respublikai perduotos įslaptintos informacijos saugumą pagal Europos Sąjungos teisės aktus ar Lietuvos Respublikos tarptautines sutartis su užsienio valstybėmis arba tarptautinėmis organizacijomis;

3) užtikrina Lietuvos Respublikos tarptautinėse sutartyse, susijusiose su įslaptintos informacijos apsaugos užtikrinimu, numatytų informacijos apsaugos veiksmų kontrolės organizavimą bei įgyvendinimą laiku visuose paslapčių subjektuose bei jų struktūriniuose padaliniuose, kuriuose saugoma užsienio valstybių ar tarptautinių organizacijų Lietuvos Respublikai perduota įslaptinta informacija;

4) kandidatūrų tikrinimą atlikusių institucijų teikimu išduoda asmens patikimumo pažymėjimus asmenims, kuriems atliekant tarnybines pareigas reikia dirbti ar susipažinti su įslaptinta užsienio valstybių ar tarptautinių organizacijų Lietuvos Respublikai perduota įslaptinta informacija, taip pat, esant šio Įstatymo nustatytiems pagrindams, panaikina asmens patikimumo pažymėjimus;

5) siūlo Valstybės saugumo departamentui steigti nacionalinę Centrinę registratūrą, vykdančią užsienio valstybių, Europos Sąjungos ar tarptautinių organizacijų Lietuvos Respublikai perduotų įslaptintų dokumentų su slaptumo žymų „Visiškai slaptai“, „Slaptai“ atitikmenimis registraciją, apskaitą ir paskirstymą;

6) paslapčių subjektų teikimu priima sprendimus dėl naujų Lietuvos Respublikai perduotos įslaptintos informacijos registratūrų steigimo tikslingumo, įsteigtas registratūras pripažįsta

tinkamomis saugoti perduotą įslaptintą informaciją, priima sprendimus dėl įsteigtų registratūrų panaikinimo tikslingumo. Prireikus siūlo paslapčių subjektams steigti kitas savarankiškas įslaptintos informacijos registratūrų sistemas arba jas panaikinti, jei to reikalauja Lietuvos Respublikos tarptautinės sutartys ar susitarimai;

7) įgalioja paslapčių subjektus ar jų struktūrinius padalinius atlikti institucijų, atsakingų už tarptautinių sutarčių dėl įslaptintos informacijos apsaugos įgyvendinimą, funkcijas;

8) teikia siūlymus dėl šio Įstatymo ir kitų teisės aktų, susijusių su įslaptintos informacijos apsauga, tobulinimo ar pripažinimo netekusiais galios, galiojančios įslaptintos informacijos apsaugos teisinio reglamentavimo sistemos tobulinimo;

9) nustato bendruosius atskirų įslaptintos informacijos apsaugos sričių (personalo patikimumo, fizinės apsaugos, įslaptintų sandorių saugumo, užsienio valstybių ar tarptautinių organizacijų Lietuvai perduotų įslaptintų dokumentų administravimo) reikalavimus, teikia paslapčių subjektams išaiškinimus įslaptintos informacijos apsaugos klausimais;

10) nagrinėja paslapčių subjektų parengtus detalius įslaptinamos informacijos, susijusios su jų vykdoma veikla, sąrašus bei tokių sąrašų pakeitimus ir teikia dėl jų paslapčių subjektams pasiūlymus bei pastabas;

11) paslapčių subjektams tarpininkaujant, sprendžia klausimus dėl galimybės išduoti asmens patikimumo pažymėjimus arba leidimus dirbti ar susipažinti su įslaptinta informacija asmenims, turintiems dvigubą pilietybę, arba asmenims, neturintiems šio Įstatymo 16 straipsnio 2 dalies 2 punkte nustatyto nuolatinio gyvenimo Lietuvos Respublikoje cenzo;

12) pasibaigus šio Įstatymo 8 straipsnio 1 dalies 1 ir 2 punktuose nustatytam informacijos įslaptinimo terminui, paslapčių subjektų teikimu sprendžia klausimus dėl įslaptinimo termino pratęsimo tikslingumo;

13) sprendžia ginčus tarp paslapčių subjektų, taip pat ginčus tarp paslapčių subjektų ir kitų asmenų, kylančius dėl informacijos įslaptinimo, įslaptintos informacijos saugojimo, naudojimo, išslaptinimo, apsaugos kontrolės ir dėl leidimų dirbti ar susipažinti su įslaptinta informacija bei asmens patikimumo pažymėjimų, įmonės patikimumo pažymėjimų neišdavimo ar panaikinimo pagrįstumo;

14) teikia paslapčių subjektams siūlymus dėl informacijos, kuri pagal savo pobūdį ir svarbą turėtų būti įslaptinta, tačiau nuosavybės teise priklauso paslapčių subjektu nesančiam fiziniam ar juridiniam asmeniui, įsigijimo pagrįstumo ir galimo atlygio informacijos savininkui dydžio;

15) paslapčių subjektų teikimu sprendžia klausimus dėl galimybės valstybės paslaptį sudarančią informaciją perduoti kitoms valstybėms ar tarptautinėms organizacijoms, su kuriomis nėra sudaryta tarptautinių sutarčių dėl įslaptintos informacijos abipusės apsaugos;

16) nustato asmens, rangovo (subrangovo) sutikimo būti tikrinamam, leidimo dirbti ar susipažinti su įslaptinta informacija, asmens patikimumo pažymėjimo ir šio pažymėjimo išdavimą patvirtinančios pažymos, klausimyno, skirto leidimui dirbti ar susipažinti su įslaptinta informacija gauti, asmens pasižadėjimo saugoti įslaptintą informaciją, įslaptintų sandorių saugumo klausimyno, įmonės patikimumą patvirtinančio pažymėjimo formas.

6. Paslapčių apsaugos koordinavimo komisija siekia užtikrinti, kad tokios pat svarbos informacijai skirtinguose paslapčių subjektuose būtų suteikiama vienoda slaptumo žyma ir nustatomas vienodas apsaugos lygis.

7. Paslapčių apsaugos koordinavimo komisijos priimti sprendimai atliekant šio straipsnio 5 dalies 1–3, 10–13, 15–16 punktuose nustatytas funkcijas, paslapčių subjektams yra privalomi.

12 straipsnis. Įslaptintos informacijos apsaugos įgyvendinimas

1. Įslaptintos informacijos apsaugos politiką formuoja Vyriausybė ir Paslapčių apsaugos koordinavimo komisija. Įslaptintos informacijos apsaugą organizuoja ir vykdo paslapčių subjektai šio Įstatymo, Vyriausybės, Paslapčių apsaugos koordinavimo komisijos, institucijų, atliekančių Saugumo priežiūros tarnybos, Nacionalinės komunikacijų apsaugos tarnybos, Nacionalinės šifrų paskirstymo tarnybos funkcijas, bei įslaptintų sandorių saugumą užtikrinančių institucijų nustatyta tvarka.

2. Už bendrą įslaptintos informacijos, kuria disponuoja paslapčių subjektas, apsaugos organizavimą ir būklę atsakingas paslapčių subjekto vadovas. 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. Už patikėtos įslaptintos informacijos praradimą ar neteisėtą atskleidimą yra tiesiogiai atsakingas asmuo, kuriam tokia informacija patikėta.

3. Paslapčių subjektai sudaro ir tvirtina struktūrinių padalinių, kuriuose dirbama su įslaptinta informacija ar saugoma įslaptinta informacija, žymima slaptumo žymomis „Visiškai slaptai“, „Slaptai“ ar „Konfidencialiai“, sąrašus ir užtikrina, kad tik į šiuos sąrašus įrašyti struktūriniai padaliniai naudotų įslaptintą informaciją ir ją saugotų.

4. Paslapčių subjektai sudaro pareigų, kurias einantiems asmenims reikia leidimų dirbti ar susipažinti su įslaptinta informacija, sąrašus.

5. Paslapčių subjektai sudaro pareigų, kurias einantiems asmenims reikia asmens patikimumo pažymėjimų, sąrašus.

6. Šio straipsnio 4 ir 5 dalyse nurodytuose pareigų sąrašuose turi būti nurodoma aukščiausia kategorija įslaptintos informacijos, su kuria asmenys, einantys sąraše nurodytas pareigas, gali dirbti ar susipažinti.

7. Asmenys, vykdantys įslaptintos informacijos, žymimos slaptumo žymomis „Visiškai slaptai“, „Slaptai“ arba „Konfidencialiai“, fizinę apsaugą ar įgalioti tokią informaciją gabenti, privalo turėti leidimus dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma „Slaptai“.

8. Paslapčių subjektuose ar jų struktūriniuose padaliniuose, disponuojančiuose Lietuvos Respublikos, užsienio valstybių ar tarptautinių organizacijų įslaptinta informacija, turi būti sudaryti sąrašai asmenų, kuriems yra išduoti leidimai dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimai.

13 straipsnis. Specialioji ekspertų komisija

1. Paslapčių subjektuose įslaptintos informacijos apsaugą koordinuoja paslapčių subjekto vadovo sprendimu sudaromos nuolatinės specialiosios ekspertų komisijos. Jos:

1) rengia paslapčių subjekto teisės aktus, susijusius su įslaptintos informacijos apsauga, prižiūri, kaip šie teisės aktai vykdomi;

2) teikia siūlymus paslapčių subjekto vadovui dėl leidimų dirbti ar susipažinti su įslaptinta informacija išdavimo asmenims arba išduotų leidimų panaikinimo;

3) teikia siūlymus bei išvadas dėl informacijos įslaptinimo pagrįstumo, slaptumo žymų keitimo, įslaptintos informacijos išslaptinimo ar sunaikinimo;

4) organizuoja įslaptintos informacijos, kuria disponuoja paslapčių subjektas, apsaugos būklės tikrinimus ir teikia pasiūlymus dėl įslaptintos informacijos apsaugos reikalavimų pažeidimų prevencijos, sprendžia kitus klausimus, susijusius su įslaptintos informacijos apsauga.

2. Atsižvelgdamas į įslaptintos informacijos apimtį, paslapčių subjekto vadovas gali nesudaryti specialiosios ekspertų komisijos ir jos funkcijas pavesti įgaliotam asmeniui.

3. Specialiosios ekspertų komisijos nariais gali būti tik asmenys, kurie šio Įstatymo nustatyta tvarka yra gavę leidimą dirbti ar susipažinti su įslaptinta informacija arba, jei paslapčių subjektas naudoja užsienio valstybių ar tarptautinių organizacijų parengtą įslaptintą informaciją, asmens patikimumo pažymėjimą. Specialiosios ekspertų komisijos narių leidimai dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimai turi atitikti įslaptintos informacijos, kuria disponuoja paslapčių subjektas, aukščiausią slaptumo žymą.

14 straipsnis. Pareiga paskirti atsakingą asmenį

Paslapčių subjekto vadovo ar jo įgalioto asmens arba rangovo (subrangovo) vadovo sprendimu turi būti paskirtas atsakingas asmuo, organizuojantis ir įgyvendinantis įslaptintos

informacijos, kuria disponuoja paslapčių subjektas, rangovas (subrangovas), administravimą, apsaugą ir kontrolę.

KETVIRTASIS SKIRSNIS
PERSONALO PATIKIMUMAS

15 straipsnis. Leidimas dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimas

1. Eiti pareigas, susijusias su Lietuvos Respublikos įslaptintos informacijos, žymimos slaptumo žymomis „Visiškai slaptai“, „Slaptai“ arba „Konfidencialiai“, naudojimu ar tokios informacijos apsauga, gali tik atitinkamus leidimus dirbti ar susipažinti su įslaptinta informacija turintys asmenys. 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. Pretendentai, atrinkti pareigoms, susijusioms su įslaptintos informacijos naudojimu ar jos apsauga, į šias pareigas gali būti skiriami prieš tai patikrinus jų kandidatūras ir gavus išvadą, kad asmuo atitinka šio Įstatymo 16 straipsnio 1 dalyje nurodytas sąlygas.

2. Pagal pareigas susipažinti su įslaptinta informacija ir ja naudotis gali Respublikos Prezidentas, Seimo Pirmininkas ir Ministras Pirmininkas.

3. Atliekant ikiteisminį tyrimą ir nagrinėjant baudžiamąją bylą, kurių medžiagoje yra įslaptintos informacijos, įtariamasis (kaltinamasis) ir įtariamojo (kaltinamojo) gynėjai Baudžiamojo proceso kodekso nustatyta tvarka turi teisę susipažinti su bylos medžiagoje esančia įslaptinta informacija, išskyrus nukentėjusiojo ar liudytojo, kuriam taikomas anonimiškumas, asmens tapatybę padedančius nustatyti duomenis.

4. Šio straipsnio 3 dalyje išvardyti asmenys, prieš jiems suteikiant teisę susipažinti su įslaptinta informacija, yra įspėjami dėl baudžiamosios atsakomybės už įslaptintos informacijos atskleidimą. Šio straipsnio 5 ir 6 dalyse išvardyti asmenys prieš išduodant laikiną leidimą dirbti ar susipažinti su Lietuvos Respublikos, užsienio valstybių ar tarptautinių organizacijų įslaptinta informacija turi duoti nustatyto pavyzdžio rašytinį pasižadėjimą saugoti patikėtą įslaptintą informaciją.

5. Lietuvos Respublikoje paskelbus karo ar nepaprastąją padėtį arba karinių operacijų metu paslapčių subjekto vadovo ar jo įgalioto asmens sprendimu asmeniui, kuris neturi leidimo dirbti su įslaptinta informacija, gali būti suteikta teisė su ja susipažinti, jeigu tokia informacija yra būtina atliekant jam pavestas funkcijas ar užduotis.

6. Išimtiniais atvejais, nustatytais NATO norminiuose dokumentuose, reglamentuojančiuose įslaptintos informacijos apsaugą, asmeniui, neturinčiam asmens patikimumo pažymėjimo, paslapčių subjekto vadovas gali išduoti rašytinį laikiną leidimą susipažinti su Lietuvai perduota NATO įslaptinta informacija, jei tokio asmens lojalumas Lietuvos valstybei ir patikimumas nekelia abejonių. Paslapčių subjekto vadovo išduotame leidime privalo būti nurodyta, su kokia įslaptinta informacija asmeniui suteikiama teisė susipažinti.

7. Paslapčių subjektai gali išduoti asmenims leidimus dirbti ar susipažinti su įslaptinta informacija tik gavę Valstybės saugumo departamento išvadą, kad asmuo atitinka šio Įstatymo 16 straipsnio 1 dalyje nurodytas sąlygas. Ši nuostata netaikoma išduodant leidimus šio Įstatymo 17 straipsnio 3 dalies 4 punkte nurodytiems asmenims.

8. Sprendimą dėl asmens patikimumo pažymėjimo išdavimo šio Įstatymo nustatyta tvarka priima Paslapčių apsaugos koordinavimo komisija.

16 straipsnis. Leidimo dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimo išdavimo sąlygos

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.

17 straipsnis. Asmens kandidatūros tikrinimas

1. Pagrindinis asmens kandidatūros tikrinimo tikslas – nustatyti, ar asmeniui, kuris pretenduoja gauti leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą, gali būti patikėta įslaptinta informacija, ar tikrinamas asmuo yra patikimas ir lojalus Lietuvos valstybei. Kandidatūros tikrinamos paslapčių subjekto vadovo ar jo įgalioto asmens teikimu.

2. Asmuo, pretenduojantis gauti leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą, atsakingam asmeniui pateikia užpildytą nustatyto pavyzdžio klausimyną, rašytinį sutikimą būti tikrinamam. Šis asmuo taip pat pateikia išsamią autobiografiją, jei pretenduoja gauti leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žymomis „Visiškai slaptai“ arba „Slaptai“. Kandidatūros patikrinimo metu siekiama nustatyti, ar nėra šio Įstatymo 16 straipsnio 2 dalyje nustatytų sąlygų. Patikrinimo metu negali būti naudojami operatyvinės veiklos metodai ir priemonės, išskyrus operatyvinę apklausą ir duomenų, esančių operatyvinėje įskaitoje, peržiūrą. Prieš priimdamos sprendimą, kandidatūrą tikrinančios institucijos asmenį gali iškviesti pokalbio, pareikalauti raštiškų asmens paaiškinimų ir prireikus, jei šis asmuo sutinka, patikrinti poligrafu.

3. Asmenų, kurie pretenduoja gauti leidimą dirbti ar susipažinti su įslaptinta informacija, kandidatūras tikrina:

1) dirbančių arba pretenduojančių dirbti krašto apsaugos sistemoje – Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos ir Valstybės saugumo departamentas;

2) dirbančių arba pretenduojančių dirbti vidaus reikalų sistemoje – vidaus reikalų ministro įgaliotos institucijos ir Valstybės saugumo departamentas;

3) dirbančių arba pretenduojančių dirbti Specialiųjų tyrimų tarnyboje – Specialiųjų tyrimų tarnyba ir Valstybės saugumo departamentas;

4) slaptųjų operatyvinės veiklos dalyvių, įslaptintų žvalgybos tarnautojų ir žvalgybos slaptųjų bendradarbių – patys paslapčių subjektai;

5) Valstybės saugumo departamentas, jei leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą pretenduoja gauti asmuo, nenurodytas šios dalies 1–4 punktuose.

4. Jeigu kandidatūrą patikrino Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, vidaus reikalų ministro įgaliotos institucijos ar Specialiųjų tyrimų tarnyba ir patikrinimo metu nebuvo nustatytos aplinkybės, nurodytos šio Įstatymo 16 straipsnio 2 dalyje, asmens užpildytas klausimynas, autobiografija ir atlikto tikrinimo išvados pateikiamos Valstybės saugumo departamentui. Valstybės saugumo departamentas įvertina atlikto tikrinimo rezultatus pagal informaciją, kuria jis disponuoja, prireikus surenka papildomą informaciją arba rekomenduoja tai padaryti kandidatūrą tikrinusioms institucijoms ir teikia paslapčių subjektui sutikimą arba motyvuotą prieštaravimą dėl galimybės asmeniui išduoti atitinkamos kategorijos leidimą dirbti ar susipažinti su įslaptinta informacija.

5. Tais atvejais, kai kandidatūrą patikrino Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, vidaus reikalų ministro įgaliotos institucijos ar Specialiųjų tyrimų tarnyba, ir tikrinimo metu buvo nustatytos aplinkybės, nurodytos šio Įstatymo 16 straipsnio 2 dalyje, tikrinimas krašto apsaugos arba vidaus reikalų ministrų ar jų įgaliotų asmenų arba Specialiųjų tyrimų tarnybos direktoriaus sprendimu nutraukiamas. Apie šį sprendimą informuojamas paslapčių subjektas ir asmuo, kurio kandidatūra buvo tikrinama. Valstybės saugumo departamentas tokios kandidatūros netikrina.

6. Asmens, kuris pretenduoja gauti asmens patikimumo pažymėjimą, kandidatūrą tikrina Valstybės saugumo departamentas. Jeigu asmuo turi leidimą dirbti ar susipažinti su įslaptinta informacija, išduotą ne anksčiau kaip prieš 18 mėnesių, Valstybės saugumo departamentas pateikia Paslapčių apsaugos koordinavimo komisijai medžiagą, kurios pagrindu asmeniui buvo suteiktas šis leidimas. Tokia kandidatūra iš naujo gali būti netikrinama.

7. Tikrinimą atliekančios institucijos privalo patikrinti asmens, pretenduojančio gauti leidimą dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimą, kandidatūrą:

1) per 60 darbo dienų, jeigu asmuo pretenduoja gauti leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma „Konfidencialiai“, arba atitinkamą asmens patikimumo pažymėjimą;

2) per 90 darbo dienų, jeigu asmuo pretenduoja gauti leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma „Slaptai“, arba atitinkamą asmens patikimumo pažymėjimą;

3) per 120 darbo dienų, jeigu asmuo pretenduoja gauti leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma „Visiškai slaptai“, arba atitinkamą asmens patikimumo pažymėjimą.

8. Jeigu Valstybės saugumo departamentas sutinka, kad asmeniui būtų išduotas leidimas dirbti ar susipažinti su įslaptinta informacija, paslapčių subjektas išduoda nustatyto pavyzdžio leidimą dirbti ar susipažinti su įslaptinta informacija.

9. Sprendimą dėl leidimo dirbti ar susipažinti su atitinkama slaptumo žyma žymima įslaptinta informacija išdavimo paslapčių subjektas privalo priimti per 20 darbo dienų nuo Valstybės saugumo departamento sutikimo išduoti tokį leidimą pasirašymo dienos. Apie išduotus

leidimus dirbti ar susipažinti su įslaptinta informacija paslapčių subjektas per 10 darbo dienų privalo pranešti Valstybės saugumo departamentui.

10. Paslapčių subjekto asmeniui išduotas leidimas dirbti ar susipažinti su įslaptinta informacija kartu su asmens rašytiniu pasižadėjimu saugoti įslaptintą informaciją laikomi asmens byloje arba paslapčių subjekto vadovo nustatyta tvarka.

11. Asmens patikimumo pažymėjimai registruojami ir saugomi Paslapčių apsaugos koordinavimo komisijos nustatyta tvarka.

12. Užsienio valstybių ar tarptautinių organizacijų atitinkamų institucijų prašymu Paslapčių apsaugos koordinavimo komisija arba paslapčių subjektai pateikia Paslapčių apsaugos koordinavimo komisijos nustatyto pavyzdžio pažymas, patvirtinančias, kad asmeniui yra išduotas asmens patikimumo pažymėjimas.

13. Kandidatūros tikrinimą atliekančios institucijos turi teisę gauti informaciją apie tikrinamą asmenį iš visų valstybės, savivaldybės institucijų, bankų ir kitų juridinių asmenų.

18 straipsnis. Leidimo dirbti ar susipažinti su įslaptinta informacija ir asmens patikimumo pažymėjimo panaikinimas

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.

19 straipsnis. Asmens, kuriam yra išduotas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, pareigos

Asmuo, kuriam yra išduotas leidimas dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimas, privalo:

1) žinoti teisės aktų, reglamentuojančių įslaptintos informacijos apsaugą, reikalavimus ir juos vykdyti;

2) neatskleisti, neprarasti ir neperduoti patikėtos arba sužinotos įslaptintos informacijos pašaliniams asmenims, taip pat asmenims, kurie nors ir turi teisę dirbti su įslaptinta informacija, tačiau nėra įgalioti su ja susipažinti;

3) patikėtą ar tarnybos metu sužinotą įslaptintą informaciją saugoti visą tokios informacijos įslaptinimo terminą;

4) vadovautis principu „Būtina žinoti“;

5) užkirsti kelią neteisėtoms kitų asmenų veikoms, dėl kurių įslaptinta informacija gali būti atskleista, prarasta, pagrobta ar kitaip neteisėtai įgyta, ir apie šiuos faktus, kitas įslaptintos informacijos atskleidimo ar praradimo aplinkybes nedelsdamas pranešti atsakingam asmeniui arba paslapčių subjekto vadovui;

6) nedelsdamas pranešti atsakingam asmeniui apie patikėtos įslaptintos informacijos praradimą ar atskleidimą, taip pat įslaptintos informacijos apsaugos reikalavimų pažeidimus;

7) nutraukdamas darbo (tarnybos) santykius, pereidamas į kitas pareigas, nesusijusias su įslaptintos informacijos naudojimu, grąžinti atsakingam asmeniui visą jam patikėtą įslaptintą informaciją;

8) teikti informaciją, žodinius ir rašytinius paaiškinimus asmenims, įgaliotiems vykdyti įslaptintos informacijos apsaugos kontrolę;

9) pranešti atsakingam asmeniui apie anketos duomenų, pateiktų jo kandidatūrą tikrinusioms institucijoms, pasikeitimą;

10) likus 6 mėnesiams iki išduoto leidimo dirbti ar susipažinti su įslaptinta informacija arba asmens patikimumo pažymėjimo galiojimo termino pabaigos, taip pat įgaliotoms institucijoms atliekant papildomą patikrinimą, pateikti atsakingam asmeniui reikiamus dokumentus tikrinimui atlikti.

20 straipsnis. Atsakingo asmens funkcijos personalo patikimumo srityje

Atsakingas asmuo:

1) organizuoja leidimų dirbti ar susipažinti su įslaptinta informacija išdavimą, tvarko jų apskaitą;

2) užtikrina, kad su įslaptinta informacija susipažintų tik leidimus turintys asmenys ir būtų griežtai laikomasi principo „Būtina žinoti“;

3) užtikrina, kad įslaptintos informacijos, su kuria asmuo dirba ar susipažįsta, žyma nebūtų aukštesnė už nurodytą šiam asmeniui suteiktame leidime;

4) kontroliuoja, kad teisės aktų, reglamentuojančių įslaptintos informacijos apsaugą, reikalavimus vykdytų visi asmenys, dirbantys ar susipažįstantys su įslaptinta informacija;

5) informuoja kandidatūrą tikrinančias institucijas apie asmens anketos duomenų, galinčių turėti įtakos leidimo išdavimui ar panaikinimui, pasikeitimą;

6) likus 6 mėnesiams iki leidimo dirbti ar susipažinti su valstybės paslaptį sudarančia informacija arba asmens patikimumo pažymėjimo galiojimo termino pabaigos, organizuoja kartotinį kandidatūros tikrinimą;

7) paima iš asmenų, kuriems išduodami leidimai dirbti ar susipažinti su įslaptinta informacija, nustatyto pavyzdžio rašytinius pasižadėjimus saugoti įslaptintą informaciją;

8) pasirašytinai supažindina asmenis su detaliu įslaptintos informacijos, susijusios su paslapčių subjekto veikla, sąrašu;

9) kartą per kalendorinius metus informuoja asmenis, kuriems patikėta įslaptinta informacija, apie įstatymų nustatytą atsakomybę už neteisėtą disponavimą įslaptinta informacija, įslaptintos informacijos atskleidimą, praradimą, pagrobimą ar kitokį neteisėtą įgijimą;

10) kartą per kalendorinius metus asmenis, kurių darbas susijęs su įslaptintos informacijos naudojimu ar apsauga, pasirašytinai supažindina su įslaptintos informacijos apsaugą reglamentuojančių teisės aktų reikalavimais.

PENKTASIS SKIRSNIS
ĮSLAPTINTOS INFORMACIJOS ADMINISTRAVIMAS

21 straipsnis. Slaptumo žymos suteikimas dokumentui arba jo daliai

1. Paslapčių subjekto struktūrinio padalinio, parengusio dokumentą, vadovas įvertina dokumentą parengusio asmens siūlymą ir priima sprendimą dėl dokumento slaptumo žymos ir įslaptinimo termino suteikimo bei atsako už priimto sprendimo pagrįstumą.

2. Dokumentui nesuteikiama slaptumo žyma vien dėl jo tematikos arba dokumento, į kurį atsakoma, slaptumo žymos.

3. Dokumento slaptumo žyma nustatoma pagal aukščiausią dokumento tekste esančios informacijos slaptumo žymą.

4. Jei dokumentas susideda iš atskirų skirtingas slaptumo žymas turinčių dalių arba turi priedų, kurių slaptumo žymos skiriasi nuo jų lydimo dokumento slaptumo žymos, apie skirtingas dokumento dalių ir jo priedų slaptumo žymas turi būti aiškios nuorodos pačiame dokumente – dokumento tekste, priedų išvardijime arba dokumento dalių sąraše (turinyje), taip pat prieš tokių dokumento teksto dalių pradžią arba ant dokumento priedų.

5. Jei dokumento dalys arba dokumento priedai yra neatsiejama dokumento dalis, toks dokumentas įtraukiamas į įslaptintų dokumentų apskaitą ir saugomas pagal aukščiausią dokumento dalies arba jo priedų turimą slaptumo žymą. Dokumento dalys arba jo priedai, kurie gali būti atskirti, yra platinami, įtraukiami į apskaitą ir saugomi pagal tokių dokumento dalių arba priedų turimą slaptumo žymą.

22 straipsnis. Įslaptintų dokumentų administravimo reikalavimai

1. Įslaptinti dokumentai, žymimi slaptumo žyma „Visiškai slaptai“, administruojami taip:

1) tvarkomi ir laikomi I ar II klasės saugumo zonose;

2) perduodami įslaptintos informacijos gavėjui pasirašytinai;

3) negali būti kopijuojami;

4) vykdytojams perduodami pasirašytinai, apie perdavimo faktą pažymint įslaptintos informacijos registracijos laikmenose;

5) įslaptintos informacijos gavėjo perduodami kitam paslapčių subjektui tik esant rašytiniam informacijos rengėjo sutikimui;

6) privalo turėti prisegtus asmenų, susipažinusių su dokumento turiniu, sąrašus;

7) saugomi atskirai nuo kitas slaptumo žymas turinčių dokumentų, išskyrus kompiuterių informacijos laikmenose saugomus dokumentus;

8) negali būti naikinami – nereikalingas dokumentas grąžinamas informacijos rengėjui, išskyrus šio Įstatymo 26 straipsnyje nustatytus atvejus.

2. Įslaptinti dokumentai, žymimi slaptumo žyma „Slaptai“, administruojami taip:

1) tvarkomi ir laikomi I arba II klasės saugumo zonoje;

2) perduodami įslaptintos informacijos gavėjui pasirašytinai;

3) gali būti dauginami ar kopijuojami tik raštišku paslapčių subjekto vadovo arba jo įgalioto asmens sprendimu, gavus rašytinį informacijos rengėjo sutikimą;

4) kopijuojant registruojami ir sunumeruojami;

5) įslaptintos informacijos gavėjo gali būti perduodami kitam paslapčių subjektui tik esant rašytiniam informacijos rengėjo sutikimui;

6) vykdytojams perduodami pasirašytinai, apie perdavimo faktą pažymint įslaptintos informacijos registracijos laikmenose;

7) naikinami (įskaitant jų kopijas) surašant sunaikinimo aktus.

3. Įslaptinti dokumentai, žymimi slaptumo žyma „Konfidencialiai“, administruojami taip:

1) tvarkomi ir laikomi I arba II klasės saugumo zonoje;

2) gali būti dauginami ar kopijuojami už dokumento vykdymo kontrolę atsakingo asmens sprendimu, laikantis principo „Būtina žinoti“, jeigu dokumentas nėra pažymėtas nuoroda „Būtinas informacijos rengėjo sutikimas“. Kopijos turi būti registruojamos ir numeruojamos;

3) vykdytojams perduodami pasirašytinai, apie perdavimo faktą pažymint įslaptintos informacijos registracijos laikmenose;

4) naikinami (įskaitant jų kopijas) surašant sunaikinimo aktus.

4. Įslaptinti dokumentai, žymimi slaptumo žyma „Riboto naudojimo“, administruojami taip:

1) tvarkomi ir laikomi administracinėje saugumo zonoje;

2) vykdytojo sprendimu gali būti platinami, dauginami, kopijuojami ir vadovaujantis principu „Būtina žinoti“ pateikiami kitiems asmenims susipažindinti, jeigu dokumentas nėra pažymėtas nuoroda „Būtinas informacijos rengėjo sutikimas“.

5. Įslaptintų dokumentų, žymimų slaptumo žyma „Riboto naudojimo“, platinimo, dauginimo, naikinimo ar kitų asmenų susipažindinimo su jų turiniu tvarką gali nustatyti paslapčių subjektai.

23 straipsnis. Susipažinimas su įslaptinta informacija, kuria disponuoja kitas paslapčių subjektas

1. Asmeniui teisę susipažinti su įslaptinta informacija, žymima slaptumo žymomis „Visiškai slaptai“, „Slaptai“ ar „Konfidencialiai“, kuria disponuoja kitas paslapčių subjektas, vadovaudamasis principu „Būtina žinoti“, suteikia šia informacija disponuojančio paslapčių subjekto vadovas. Asmuo privalo pateikti institucijos, kurioje dirba, vadovo tikslinį siuntimą. Siuntime turi būti patvirtinta, kad asmuo turi leidimą dirbti ar susipažinti su atitinkama slaptumo žyma pažymėta įslaptinta informacija arba asmens patikimumo pažymėjimą, jeigu reikia susipažinti su užsienio valstybės ar tarptautinės organizacijos perduota įslaptinta informacija, taip pat tiesioginių pareigų vykdymu pagrįstas poreikis susipažinti su konkrečia įslaptinta informacija ir nurodyta, su kokios apimties įslaptinta informacija asmeniui reikia susipažinti.

2. Jei priimamas sprendimas neleisti asmeniui susipažinti su siuntime nurodyta įslaptinta informacija, šia informacija disponuojančio paslapčių subjekto vadovas savo sprendimą privalo pagrįsti ir per 10 darbo dienų su šiuo sprendimu supažindinti asmenį siuntusios institucijos vadovą. Toks sprendimas gali būti apskųstas Paslapčių apsaugos koordinavimo komisijai, kuri priima paslapčių subjektui privalomą sprendimą.

24 straipsnis. Įslaptintos informacijos gabenimas

1. Įslaptintus dokumentus, gaminius ir kitus objektus, žymimus slaptumo žymomis „Visiškai slaptai“ ir „Slaptai“, turi gabenti šaunamaisiais ginklais ginkluoti diplomatiniai, kariniai, specialius įgaliojimus turinčių kurjerių pašto tarnybų kurjeriai arba paslapčių subjekto įgalioti asmenys.

2. Įslaptintus dokumentus, gaminius ir kitus objektus, žymimus slaptumo žymomis „Konfidencialiai“ ir „Riboto naudojimo“, gali gabenti šio straipsnio 1 dalyje išvardyti asmenys arba kurjerių pašto tarnybų kurjeriai.

3. Įslaptintus dokumentus, gaminius ir kitus objektus gabenantys asmenys:

1) privalo užtikrinti gabenamų dokumentų, gaminių ir kitų objektų saugumą;

2) dokumentus, gaminius ir kitus objektus privalo gabenti taip, kad atsitiktiniai asmenys negalėtų nustatyti, jog gabenama įslaptinta informacija, ar susipažinti su tokios informacijos turiniu.

4. Įslaptintų dokumentų, gaminių ir kitų objektų, žymimų slaptumo žymomis „Visiškai slaptai“ ir „Slaptai“, pristatymo faktą parašu turi patvirtinti įslaptintos informacijos gavėjas.

5. Įslaptintus dokumentus, gaminius ir kitus objektus gabenantiems asmenims draudžiama susipažinti su įslaptinta informacija.

6. 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.

7. Įslaptinti dokumentai, gaminiai ir kiti objektai gabenami parenkant saugiausią maršrutą ir gabenimo būdą.

25 straipsnis. Įslaptintos informacijos naikinimas

1. Įslaptinta informacija naikinama Vyriausybės nustatyta tvarka.

2. Sprendimą dėl įslaptintos informacijos sunaikinimo priima paslapčių subjekto vadovas ar jo įgaliotas asmuo, išskyrus šio Įstatymo 22 straipsnio 1 dalies 8 punkte nurodytus atvejus.

3. Įslaptinta informacija turi būti sunaikinama taip, kad nebūtų įmanoma atkurti įslaptintos informacijos ar jos dalies turinio.

26 straipsnis. Įslaptintos informacijos evakuacija arba sunaikinimas karo padėties ar ekstremalių situacijų atveju

1. Paslapčių subjektas, kuriame dirbama su įslaptinta informacija arba tokia informacija yra saugoma, turi parengti ir patvirtinti įslaptintos informacijos evakuacijos arba sunaikinimo planus karo padėties ar ekstremalių situacijų atveju.

2. Planuose turi būti nustatyta įslaptintos informacijos evakuacijos arba sunaikinimo eiliškumo tvarka iškilus realiai grėsmei prarasti ar atskleisti įslaptintą informaciją. Pirmiausia evakuojama arba naikinama aukštesnę slaptumo žymą turinti įslaptinta informacija.

27 straipsnis. Įslaptintos informacijos patikrinimas

1. Kartą per metus paslapčių subjekto vadovo įgalioti asmenys turi atlikti valstybės paslaptį sudarančios informacijos patikrinimą. Patikrinimo išvados įforminamos aktu. Jį tvirtina paslapčių subjekto vadovas.

2. Kartą per trejus metus paslapčių subjekto vadovo įgalioti asmenys turi atlikti įslaptintos informacijos, pažymėtos slaptumo žyma „Konfidencialiai“, patikrinimą. Patikrinimo išvados įforminamos aktu. Jį tvirtina paslapčių subjekto vadovas.

3. Įslaptintos informacijos, pažymėtos slaptumo žyma „Riboto naudojimo“, patikrinimo periodiškumą nustato paslapčių subjektas.

4. Patikrinimo tikslas – nustatyti, ar įslaptinta informacija nėra prarasta arba sugadinta.

5. Laikoma, kad už įslaptintą informaciją atsiskaityta, jeigu:

1) įslaptintą dokumentą, gaminį ar kitą objektą galima pamatyti;

2) yra atitinkamo paslapčių subjekto ar struktūrinio padalinio, kuriam įslaptinta informacija buvo perduota, raštiškas patvirtinimas, kad informacija gauta;

3) teisės aktų nustatyta tvarka yra užfiksuotas jos sunaikinimo faktas;

4) yra atitinkamas pranešimas ar sprendimas dėl informacijos išslaptinimo.

28 straipsnis. Atsakingo asmens funkcijos įslaptintos informacijos administravimo srityje

Atsakingas asmuo:

1) organizuoja įslaptintos informacijos apskaitą ir kontroliuoja jos apyvartą, tvarko jos registraciją;

2) atrenka informaciją naikinti, išslaptinti arba pratęsti tokios informacijos įslaptinimo terminą;

3) atsako už įslaptintos informacijos registracijos laikmenų tvarkymą;

4) atsako už įslaptintos informacijos perdavimą vykdytojams ir kitiems paslapčių subjektams;

5) atsako už tai, kad paslapčių subjektai būtų laiku informuojami apie įslaptintos informacijos slaptumo žymų keitimą, išslaptinimo ar įslaptinimo termino pratęsimą;

6) paslapčių subjekto vadovo ar jo įgalioto asmens sprendimu supažindina kitų paslapčių subjektų įgaliotus asmenis su įslaptinta informacija, žymima slaptumo žyma „Visiškai slaptai“, „Slaptai“ ar „Konfidencialiai“;

7) šio Įstatymo 27 straipsnyje nustatytais terminais organizuoja įslaptintos informacijos patikrinimą;

8) organizuoja įslaptintų dokumentų naikinimo procesą.

29 straipsnis. Įslaptintos informacijos administravimo reglamentavimas

Smulkesnę įslaptintos informacijos rengimo, įforminimo, siuntimo, gabenimo, gavimo, dauginimo, naikinimo bei apskaitos tvarką, vadovaudamasi šio Įstatymo penktojo skirsnio nuostatomis, nustato Vyriausybė.

ŠEŠTASIS SKIRSNIS
ĮSLAPTINTOS INFORMACIJOS FIZINĖ APSAUGA

30 straipsnis. Fizinės apsaugos įgyvendinimas

1. Paslapčių subjektai privalo užtikrinti, kad visos teritorijos, patalpos ir darbo vietos, kuriose dirbama su įslaptinta informacija ar tokia informacija yra saugoma, būtų reikiamai apsaugotos atitinkamomis fizinėmis, mechaninėmis, procedūrinėmis, elektroninėmis apsaugos priemonėmis ir būtų paskirti apsaugos darbuotojai.

2. Įslaptintos informacijos fizinės apsaugos priemonės turi užtikrinti, kad:

1) pašaliniai asmenys negalėtų patekti į teritorijas ir patalpas, kuriose dirbama su įslaptinta informacija ar tokia informacija yra saugoma;

2) būtų užkirstas kelias neteisėtiems darbuotojų veiksmams ir tokie veiksmai būtų fiksuojami;

3) neturintys leidimo dirbti ar susipažinti su įslaptinta informacija darbuotojai negalėtų susipažinti su įslaptintos informacijos turiniu;

4) būtų fiksuojami fizinės apsaugos pažeidimai.

3. Priimdamas sprendimą dėl konkrečių apsaugos priemonių pasirinkimo ir įdiegimo bei naudojimo, paslapčių subjektas atsižvelgia į šiuos veiksnius:

1) saugomos įslaptintos informacijos slaptumo žyma;

2) saugomos informacijos pobūdis ir apimtis;

3) rizikos veiksniai – paslapčių subjekte dirbančių asmenų patikimumas, aplinkos charakteristika, kriminogeninė padėtis, pastato dislokavimo vieta, patalpų išplanavimas, teritorijos dydis, patekimo nepastebėtam į saugomą zoną tikimybė ir kita.

4. Fizinės apsaugos užtikrinimo sudėtinės dalys:

1) saugumo zonų nustatymas;

2) mechaninių apsaugos priemonių, apsunkinančių įsibrovimą ar įsilaužimą į teritoriją, patalpas, įdiegimas ir naudojimas;

3) apsaugos signalizacijos įdiegimas ir naudojimas;

4) elektroninio stebėjimo ir elektroninių apsaugos priemonių, nustatančių asmens tapatybę ir ribojančių patekimą bei fiksuojančių asmens įėjimą į patalpas, buvimą jose ir išėjimą iš jų, įdiegimas ir naudojimas;

5) apsaugos darbuotojų apmokymas, paskyrimas bei paskirstymas;

6) fizinės apsaugos procedūrų reglamentavimas – vidaus taisyklės, numatančios, kaip turi būti atrakinamos ir užrakinamos patalpos, išjungiama ir įjungiama signalizacija, vykdomas patalpų stebėjimas ir kitos fizinės apsaugos procedūros.

5. Atsižvelgiant į šio straipsnio 3 dalyje išvardytus veiksnius ir saugomos informacijos apsaugos užtikrinimo galimybes, šio straipsnio 4 dalies 2–5 punktuose išvardytos fizinės apsaugos užtikrinimo sudėtinės dalys gali būti taikomos kompleksiškai arba pirmenybė atiduodama keletui ar vienai iš jų.

31 straipsnis. Saugumo zonos

1. Teritorijos ir patalpos, kuriose dirbama arba kuriose saugoma įslaptinta informacija, pagal informacijos slaptumo žymas, saugojimo pobūdį ir nesankcionuoto susipažinimo su įslaptinta informacija tikimybę skirstomos į atskiras saugumo zonas.

2. Administracinė saugumo zona – apibrėžta teritorija ir (ar) patalpos, kuriose kontroliuojamas asmenų ir transporto priemonių judėjimas. Patekti į I ar II klasės saugumo zoną galima tik per administracinę zoną. Administracinėje zonoje gali būti saugoma tik informacija,

žymima slaptumo žyma „Riboto naudojimo“, arba su tokia informacija dirbama. Administracinėje saugumo zonoje saugoma įslaptinta informacija turi būti laikoma metalinėse spintose arba seifuose.

3. II klasės saugumo zona – teritorijos ir patalpos, kuriose saugoma informacija, žymima slaptumo žyma „Konfidencialiai“ ir aukštesnėmis slaptumo žymomis, arba su tokia informacija dirbama, taip pat patalpos, į kurias patekus galima tiesiogiai prieiti prie šios saugumo zonos elektroninių apsaugos priemonių centrinio valdymo. II klasės saugumo zonoje saugoma įslaptinta informacija, žymima slaptumo žyma „Slaptai“ arba „Visiškai slaptai“, turi būti laikoma seifuose, turinčiuose individualius vartotojų kodinius bei mechaninius užraktus, ar specialiai tokiai informacijai saugoti skirtose saugyklose. II klasės saugumo zonoje saugoma įslaptinta informacija, žymima slaptumo žyma „Konfidencialiai“, turi būti laikoma metalinėse spintose arba seifuose.

4. II klasės saugumo zonai keliami šie reikalavimai:

1) turi būti nustatyti, saugomi bei kontroliuojami visi įėjimai į zoną ir išėjimai iš jos;

2) į zoną gali patekti tik asmenys, turintys leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma „Konfidencialiai“. Visus kitus asmenis turi lydėti apsaugos darbuotojas arba paslapčių subjekto vadovo įgaliotas asmuo;

3) jei zonoje saugoma informacija, žymima slaptumo žymomis „Slaptai“ arba „Visiškai slaptai“, asmens tapatybei nustatyti prie įėjimų į zoną arba atskiras jos patalpas turi būti įkurtas kontrolės postas arba turi būti įdiegta asmens tapatybę padedanti nustatyti sistema;

4) prieigos iki pastatų visą tamsų paros metą turi būti apšviestos;

5) zonai priskirtos patalpos turi turėti apsaugos, pavojaus ir priešgaisrinę signalizacijas;

6) elektroninės apsaugos priemonės turi perduoti dubliuojantį signalą apie bandymą įsibrauti į zoną arba neteisėtą buvimą joje ne vienai reagavimo sistemai;

7) jei zonoje saugoma informacija, žymima slaptumo žyma „Visiškai slaptai“, įėjimas į zoną arba įėjimai į zonoje esančias patalpas turi būti stebimi vaizdo kameromis, turi būti kaupiamas 30 kalendorinių dienų vaizdo archyvas.

5. I klasės saugumo zona – patalpos, kuriose dirbama ar saugoma informacija, žymima slaptumo žyma „Konfidencialiai“ ir aukštesnėmis slaptumo žymomis. Į jas patekus galima tiesiogiai prieiti prie jose saugomos informacijos, taip pat prie šios saugumo zonos elektroninių apsaugos priemonių centrinio valdymo.

6. I klasės saugumo zonai keliami šie reikalavimai:

1) šio straipsnio 4 dalyje nustatyti reikalavimai;

2) prieigos iki šios saugumo zonos turi būti kontroliuojamos elektroninėmis apsaugos priemonėmis;

3) gali būti tikrinami asmenų įnešami ir išnešami daiktai;

4) į šią saugumo zoną paslapčių subjekto vadovo ar jo įgalioto asmens sprendimu įleidžiami tik asmenys, turintys leidimus dirbti ar susipažinti su įslaptinta informacija, žymima aukščiausia toje saugumo zonoje saugomos informacijos slaptumo žyma;

5) į zoną negali būti įnešami jokie pašaliniai elektromagnetiniai spinduliavimo šaltiniai;

6) turi būti naudojama apsauginė įsilaužimo signalizacija, perimetro signalizacija, apsauginė gaisro signalizacija;

7) taikomos mechaninės apsaugos priemonės turi užkirsti kelią nesankcionuotam patekimui į saugomas patalpas.

7. Iškilus būtinybei, kai nėra asmens, kuriam patikėta įslaptinta informacija, atidaryti dokumentų saugyklas, asmeninius seifus, metalines spintas gali tik paslapčių subjekto vadovo tam įgalioti asmenys. Paslapčių subjektai turi nustatyti tokių veiksmų atlikimo ir užfiksavimo tvarką.

8. Kilus įtarimui, kad į dokumentų saugyklas galėjo patekti arba asmeninius seifus, metalines spintas atidaryti pašaliniai asmenys, apie tai nedelsiant pranešama atsakingam asmeniui, paslapčių subjekto vadovui ir Valstybės saugumo departamentui. Kol atvyks Valstybės saugumo departamento pareigūnai, atsakingas asmuo ir paslapčių subjekto vadovas imasi reikiamų priemonių įvykio vietos neliečiamumui išsaugoti.

32 straipsnis. Atsakingo asmens funkcijos įgyvendinant įslaptintos informacijos fizinę apsaugą

Atsakingas asmuo:

1) užtikrina, kad teritorijose ir patalpose, kuriose dirbama su įslaptinta informacija ar kuriose ji saugoma, būtų įdiegtos ir tinkamai veiktų reikiamos fizinės apsaugos priemonės;

2) rengia fizinės apsaugos procedūras reglamentuojančius dokumentus, kontroliuoja, kaip laikomasi nustatytų procedūrų, periodiškai atlieka taikomų fizinės apsaugos priemonių patikrinimus;

3) organizuoja darbuotojų apmokymus;

4) teikia paslapčių subjekto vadovui ar jo įgaliotam asmeniui siūlymus dėl patalpų suskirstymo į saugumo zonas;

5) praneša paslapčių subjekto vadovui apie pastebėtus saugyklų, patalpų, seifų, metalinių spintų apsaugos priemonių bei instaliacijų pažeidimus ir imasi priemonių jiems pašalinti.

SEPTINTASIS SKIRSNIS
ĮSLAPTINTŲ SANDORIŲ SAUGUMAS

33 straipsnis. Įslaptinti sandoriai

1. Paslapčių subjektai, atlikdami jiems pavestas funkcijas, turi teisę sudaryti įslaptintus sandorius. Įslaptintų sandorių sudarymo tvarką nustato Vyriausybė.

2. Rangovas iki sandorio pasirašymo dienos šio Įstatymo 35 straipsnio nustatyta tvarka turi gauti įmonės patikimumą patvirtinantį pažymėjimą. Rangovas (subrangovas), jo darbuotojai, kuriems vykdant įslaptintą sandorį reikės susipažinti su įslaptinta informacija, iki sandorio pasirašymo dienos turi gauti leidimą dirbti ar susipažinti su įslaptinta informacija. Leidimą išduoda paslapčių subjektas, sudarantis įslaptintą sandorį. Rangovas, gavęs paslapčių subjekto sutikimą, turi teisę įslaptinto sandorio daliai vykdyti pasitelkti subrangovą, kuris šio Įstatymo 35 straipsnio nustatyta tvarka turi gauti įmonės patikimumą patvirtinantį pažymėjimą.

3. Juridiniams asmenims, dalyvaujantiems užsienio valstybių ar tarptautinių organizacijų paskelbtuose konkursuose dėl įslaptinto sandorio sudarymo, jei užsienio valstybė arba tarptautinė organizacija reikalauja jų patikimumą patvirtinančių pažymėjimų, taikomi šio Įstatymo 35 straipsnio reikalavimai.

4. Užsienio valstybėse veikiančios ir ten registruotos įmonės, įstaigos ar organizacijos gali dalyvauti Lietuvos Respublikos paslapčių subjektų paskelbtuose konkursuose sudaryti įslaptintą sandorį, kurį vykdant bus perduodama Lietuvos Respublikos įslaptinta informacija, žymima slaptumo žymomis „Visiškai slaptai“, „Slaptai“ arba „Konfidencialiai“, jeigu jos atitinka tose valstybėse keliamus įslaptintų sandorių saugumo reikalavimus ir atsakinga užsienio valstybės institucija pateikia atitinkamą išvadą.

34 straipsnis. Įslaptintos informacijos apsauga įslaptinto sandorio vykdymo metu

1. Paslapčių subjektai, sudarę įslaptintą sandorį, privalo kontroliuoti, kaip rangovas ar subrangovas vykdo perduotos ar sandorio metu sukurtos įslaptintos informacijos apsaugos reikalavimus.

2. Įslaptintas sandoris gali būti vienašališkai nutrauktas, jei rangovas ar subrangovas nevykdo nustatytų įslaptintos informacijos apsaugos reikalavimų.

3. Nesudarius sandorio, įvykdžius įslaptintą sandorį ar jį nutraukus, rangovas bei subrangovas privalo grąžinti visą jiems perduotą ir perduoti sandorio metu sukurtą įslaptintą informaciją.

35 straipsnis. Įmonės patikimumą patvirtinančio pažymėjimo išdavimas

1. Įslaptintų sandorių saugumą užtikrinanti institucija atlieka tikrinimą dėl rangovo (subrangovo) patikimumo, išduoda įmonės patikimumo pažymėjimą, išduotą pažymėjimą panaikina

ir kontroliuoja, kaip rangovai ar subrangovai atitinka įslaptintų sandorių saugumo reikalavimus iki pasirašant įslaptintą sandorį, kaip laikosi šių reikalavimų įslaptintą sandorį vykdydami ir baigdami.

2. Įmonės patikimumo tikrinimo tikslas – nustatyti, ar su rangovu gali būti sudarytas įslaptintas sandoris užtikrinant tinkamą įslaptintos informacijos apsaugą. Šio tikrinimo metu negali būti naudojami operatyvinės veiklos metodai ir priemonės, išskyrus operatyvinę apklausą ir duomenų, esančių operatyvinėje įskaitoje, peržiūrą.

3. Atlikus šio straipsnio 8–10 dalyse nustatytą tikrinimą, įmonės patikimumą patvirtinančius pažymėjimus išduoda šios įslaptintų sandorių saugumą užtikrinančios institucijos:

1) jei įslaptintą sandorį sudaro Krašto apsaugos sistemos institucijos – Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, įvertinęs kitų įslaptintų sandorių saugumą užtikrinančių institucijų pateiktą informaciją;

2) jei įslaptintą sandorį sudaro Vidaus reikalų sistemos institucijos – vidaus reikalų ministro įgaliotos institucijos, įvertinusios kitų įslaptintų sandorių saugumą užtikrinančių institucijų pateiktą informaciją;

3) jei įslaptintą sandorį sudaro Specialiųjų tyrimų tarnyba – Specialiųjų tyrimų tarnyba, įvertinusi kitų įslaptintų sandorių saugumą užtikrinančių institucijų pateiktą informaciją;

4) jei įslaptintą sandorį sudaro kiti paslapčių subjektai – Valstybės saugumo departamentas, įvertinęs kitų įslaptintų sandorių saugumą užtikrinančių institucijų pateiktą informaciją.

4. Rangovo (subrangovo) darbuotojų patikimumą tikrina Valstybės saugumo departamentas, vadovaudamasis šio Įstatymo 16 ir 17 straipsnių nuostatomis.

5. Paslapčių subjektai įslaptintų sandorių saugumą užtikrinančioms institucijoms pateikia:

1) duomenis apie rangovui ar subrangovui numatomos perduoti įslaptintos informacijos pobūdį, apimtis bei tokios informacijos slaptumo žymas, taip pat įslaptintame sandoryje numatytas teikti paslaugas;

2) rangovo ar subrangovo užpildytą įslaptintų sandorių saugumo klausimyną ir jo rašytinį sutikimą būti tikrinamam;

3) rangovo ar subrangovo darbuotojų, pretenduojančių gauti leidimus dirbti ar susipažinti su įslaptinta informacija ar asmens patikimumo pažymėjimus, užpildytus klausimynus, tokių asmenų rašytinius sutikimus būti tikrinamiems ir išsamias autobiografijas.

6. Paslapčių subjektas, ketinantis sudaryti įslaptintą sandorį, privalo:

1) paskirti asmenis, atsakingus už įslaptinto sandorio vykdymo metu perduotos įslaptintos informacijos bei įslaptinto sandorio reikalavimų vykdymo kontrolę;

2) teikti būtiną metodinę pagalbą įslaptintos informacijos apsaugos klausimais;

3) prireikus parengti ir pateikti įslaptinto sandorio vykdymui būtinus įslaptinimo žinynus, kuriuose įvardijama įslaptinto sandorio vykdymui perduodama arba numatoma sukurti įslaptinta informacija, jos slaptumo žymos, įslaptinimo terminai, šios informacijos išslaptinimo sąlygos.

7. Rangovas, su kuriuo sudarytas įslaptintas sandoris, taip pat subrangovas privalo:

1) šio Įstatymo bei kitų teisės aktų, reglamentuojančių įslaptintos informacijos apsaugą, nustatyta tvarka organizuoti ir vykdyti patikėtos ar įslaptinto sandorio metu sukurtos įslaptintos informacijos apsaugą;

2) užtikrinti, kad su įslaptinta informacija dirbs ar susipažins leidimus turintys asmenys ir tik vadovaudamiesi principu „Būtina žinoti“;

3) paskirti asmenį, atsakingą už įslaptinto sandorio vykdymą, įslaptintos informacijos apsaugos organizavimą, vykdymą ir kontrolę;

4) įslaptintą sandorį įvykdžius ar jo vykdymą nutraukus prieš terminą, paslapčių subjektui perduoti visus gautus ir įslaptinto sandorio vykdymo metu sukurtus dokumentus ar gaminius, kuriuose yra įslaptintos informacijos.

8. Išduodant įmonės patikimumą patvirtinantį pažymėjimą, tikrinama:

1) rangovo (subrangovo) kapitalo ir valdymo struktūra, kapitalo kilmė, savininkai bei teisinė registracija;

2) rangovo (subrangovo) administracija;

3) rangovo (subrangovo) finansinė būklė ir padaryti įstatymų pažeidimai, rangovo (subrangovo) darbuotojų ar savininkų padarytos korupcinės veikos;

4) rangovo (subrangovo) verslo ryšiai, ryšiai su kriminaliniais elementais ir užsienio valstybių specialiosiomis tarnybomis, kurių veikla yra priešiška Lietuvos valstybės interesams;

5) įslaptintos informacijos apsaugos užtikrinimo galimybės;

6) darbuotojų, kurie pretenduoja gauti leidimus dirbti ar susipažinti su įslaptinta informacija ar asmens patikimumo pažymėjimus, patikimumas.

9. Rangovas ar subrangovas įslaptintų sandorių saugumą užtikrinančioms institucijoms turi pateikti duomenis apie praėjusių finansinių metų finansinę veiklą, taip pat kitą įslaptintų sandorių saugumą užtikrinančių institucijų prašomą informaciją.

10. Duomenis apie rangovo ar subrangovo finansinius įsiskolinimus, padarytus finansinius pažeidimus įslaptintų sandorių saugumą užtikrinančioms institucijoms teikia mokesčių administratoriai.

11. Įslaptintų sandorių saugumą užtikrinančios institucijos turi teisę gauti iš valstybės, savivaldybės institucijų, bankų ir kitų juridinių asmenų visą reikiamą informaciją, susijusią su rangovo ar subrangovo bei jo darbuotojų tikrinimu dėl įmonės patikimumo pažymėjimo išdavimo.

12. Įmonės patikimumą patvirtinantis pažymėjimas galioja tik konkretaus įslaptinto sandorio vykdymo metu. Įmonės patikimumą patvirtinantis pažymėjimas gali būti atnaujintas neatliekant įmonės patikrinimo, jei nuo paskutinio įmonės patikrinimo praėjo ne daugiau kaip 36 mėnesiai ir nėra pagrindo abejoti rangovo (subrangovo) patikimumu.

13. Rangovo ar subrangovo darbuotojams išduoti leidimai dirbti ar susipažinti su įslaptinta informacija galioja tik konkretaus įslaptinto sandorio vykdymo metu, tačiau ne ilgiau, negu nustatyta šio Įstatymo 16 straipsnio 5 dalyje. Leidimas dirbti ar susipažinti su įslaptinta informacija gali būti atnaujinamas neatliekant papildomo asmens tikrinimo, jei nuo tokio leidimo išdavimo praėjo ne daugiau kaip 36 mėnesiai ir nėra pagrindo abejoti asmens patikimumu.

36 straipsnis. Įmonės patikimumą patvirtinančio pažymėjimo neišdavimo sąlygos

1. Įmonės patikimumą patvirtinantis pažymėjimas neišduodamas, jei patikrinimo metu nustatoma, kad:

1) rangovas (subrangovas) yra nemokus ar nevykdo savo sutartinių įsipareigojimų fiziniams ar juridiniams asmenims;

2) rangovui (subrangovui) yra taikomos sankcijos už įstatymų pažeidimus arba yra atliekamas tyrimas dėl jų, jei dėl tokių pažeidimų gali kilti įslaptintos informacijos praradimo ar neteisėto atskleidimo grėsmė;

3) rangovas (subrangovas) vykdo ar vykdė neteisėtą veiklą;

4) rangovas (subrangovas) įslaptintų sandorių saugumą užtikrinančiai institucijai pateikė suklastotus arba neteisingus duomenis;

5) rangovas (subrangovas) neturi galimybių užtikrinti numatytos perduoti ar sukurti įslaptintos informacijos apsaugos;

6) rangovui (subrangovui) dėl jo kaltės anksčiau buvo atsisakyta išduoti įmonės patikimumą patvirtinantį pažymėjimą, buvo panaikintas išduotas įmonės patikimumą patvirtinantis pažymėjimas ir nėra pašalintos tokio pažymėjimo neišdavimo arba panaikinimo priežastys;

7) rangovo (subrangovo) darbuotojams, kuriems bus patikima įslaptinta informacija, vadovaujantis šio Įstatymo 16 straipsnio 2 dalimi leidimas dirbti ar susipažinti su įslaptinta informacija negali būti išduodamas ir tokių asmenų negalima pakeisti kitais.

2. Įslaptintų sandorių saugumą užtikrinančių institucijų sprendimą neišduoti įmonės patikimumą patvirtinančio pažymėjimo per 30 darbo dienų nuo tokio sprendimo gavimo dienos rangovas (subrangovas) turi teisę apskųsti Paslapčių apsaugos koordinavimo komisijai, o ši priima įslaptinto sandorio saugumą užtikrinančiai institucijai privalomą sprendimą.

37 straipsnis. Įmonės patikimumą patvirtinančio pažymėjimo panaikinimas

1. Išduotas įmonės patikimumą patvirtinantis pažymėjimas panaikinamas ir sudarytas sandoris nutraukiamas, jei:

1) dėl rangovo ar subrangovo kaltės buvo atskleista ar prarasta jiems patikėta įslaptinta informacija;

2) rangovas ar subrangovas ne vieną kartą pažeidė nustatytus įslaptintos informacijos apsaugos reikalavimus arba juos šiurkščiai pažeidžia, sukeldamas įslaptintos informacijos praradimo ar neteisėto atskleidimo grėsmę;

3) nustatoma, kad rangovas ar subrangovas nuslėpė duomenis apie save ar savo veiklą arba pateikė klaidingus duomenis, turėjusius reikšmę sprendimui dėl įmonės patikimumą patvirtinančio pažymėjimo išdavimo;

4) atsiranda bent viena 36 straipsnio 1 dalyje nurodyta aplinkybė.

2. Įslaptintų sandorių saugumą užtikrinančių institucijų sprendimą panaikinti išduotą įmonės patikimumą patvirtinantį pažymėjimą per 30 darbo dienų nuo tokio sprendimo pasirašymo dienos rangovas turi teisę apskųsti Paslapčių apsaugos koordinavimo komisijai, o ši priima įslaptinto sandorio saugumą užtikrinančiai institucijai privalomą sprendimą.

38 straipsnis. Įmonės patikimumą patvirtinančių pažymėjimų apskaita

Įslaptintų sandorių saugumą užtikrinanti institucija per 10 darbo dienų privalo raštu pranešti Valstybės saugumo departamentui apie išduotus ar panaikintus įmonės patikimumą patvirtinančius pažymėjimus. Valstybės saugumo departamentas tvarko įmonių, kurioms išduoti įmonės patikimumo pažymėjimai, apskaitą.

39 straipsnis. Atsakingų asmenų funkcijos sudarant ir vykdant įslaptintus sandorius

1. Paslapčių subjekto atsakingas asmuo:

1) įslaptintų sandorių saugumą užtikrinančioms institucijoms pateikia šio Įstatymo 35 straipsnio 5 dalyje nurodytą informaciją;

2) organizuoja leidimų dirbti ar susipažinti su įslaptinta informacija išdavimą rangovo ar subrangovo darbuotojams, tvarko išduotų leidimų apskaitą;

3) organizuoja įslaptintos informacijos perdavimą rangovui ar subrangovui;

4) kontroliuoja, kaip rangovas ar subrangovas užtikrina įslaptintos informacijos apsaugą;

5) subjekto vadovo ar jo įgalioto asmens sprendimu rengia ir pateikia sandoriui vykdyti būtinus įslaptinimo žinynus;

6) rangovui ar subrangovui teikia metodinę pagalbą įslaptintos informacijos apsaugos klausimais.

2. Rangovo ar subrangovo atsakingas asmuo:

1) teikia paslapčių subjekto atsakingam asmeniui šio Įstatymo 35 straipsnio 5 dalies 2 ir 3 punktuose nurodytą informaciją;

2) užtikrina personalo patikimumo procedūrų įgyvendinimą;

3) užtikrina įslaptintos informacijos administravimo reikalavimų įgyvendinimą;

4) užtikrina fizinę įslaptintos informacijos apsaugą;

5) užtikrina ADA sistemų ir tinklų apsaugą.

AŠTUNTASIS SKIRSNIS
AUTOMATIZUOTŲ DUOMENŲ APDOROJIMO SISTEMŲ IR TINKLŲ, KURIUOSE YRA SAUGOMA, APDOROJAMA AR KURIAIS PERDUODAMA ĮSLAPTINTA INFORMACIJA, APSAUGA

40 straipsnis. Leidimų apdoroti įslaptintą informaciją ADA sistemomis ir tinklais išdavimas

1. ADA sistemų ir tinklų apsaugą paslapčių subjektai užtikrina vadovaudamiesi šio Įstatymo, Paslapčių apsaugos koordinavimo komisijos, institucijų, atliekančių Saugumo priežiūros tarnybos, Nacionalinės komunikacijų apsaugos tarnybos ir Nacionalinės šifrų paskirstymo tarnybos

funkcijas, nustatyta tvarka ir reikalavimais.

2. ADA sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, žymima slaptumo žymomis „Visiškai slaptai“, „Slaptai“, „Konfidencialiai“, projektus paslapčių subjektai turi suderinti su Saugumo priežiūros tarnyba ar jos įgaliota institucija, kuri išduoda leidimą naudoti tokius tinklus ar sistemas.

41 straipsnis. ADA sistemų ir tinklų apsaugos reikalavimai

1. ADA sistemų ir tinklų saugumui garantuoti naudojamos apsaugos priemonės turi užtikrinti:

1) saugomos, apdorojamos ar perduodamos įslaptintos informacijos slaptumą;

2) galimybę nustatyti sistemų ir tinklų vartotojų tapatybę;

3) saugomos, apdorojamos ar perduodamos informacijos bei sistemos paslaugų ir išteklių vientisumą;

4) saugomos, apdorojamos ar perduodamos informacijos bei sistemos paslaugų ir išteklių prieinamumą teisėtiems vartotojams;

5) tyčinių ar atsitiktinių ADA sistemose ir tinkluose saugomos, apdorojamos, perduodamos įslaptintos informacijos bei ADA sistemos ir tinklų paslaugų bei išteklių slaptumo, vientisumo arba prieinamumo pažeidimų fiksavimą;

6) ADA sistemų ir tinklų sujungimo kontrolę;

7) ADA sistemose ir tinkluose esančių apsaugos mechanizmų tinkamumo įvertinimą bei patikrinimą.

2. ADA sistemose ir tinkluose turi būti įdiegti apsaugos mechanizmai ir saugumo valdymo procedūros, trukdančios atsirasti saugumo pažeidimams, aptinkančios atsiradusius saugumo pažeidimus, atkuriančios saugumo pažeidimų paveiktą įslaptintos informacijos ir ADA sistemų bei tinklų paslaugų ir išteklių slaptumą, vientisumą ir prieinamumą teisėtiems vartotojams.

3. ADA sistemose ir tinkluose turi būti įdiegtos apsaugos priemonės, leidžiančios apsaugoti įslaptintą informaciją, žymimą slaptumo žyma „Konfidencialiai“ ar aukštesne slaptumo žyma, nuo atskleidimo pavojaus dėl elektromagnetinio spinduliavimo. Taikomos apsaugos priemonės turi atitikti informacijos neteisėto atskleidimo riziką ir žalą, kuri būtų patirta tokią informaciją atskleidus.

4. Visi ADA sistemų ir tinklų įrengimo ir pakeitimo darbai turi būti atliekami dalyvaujant ir darbus prižiūrint atsakingam asmeniui. Asmenys, atliekantys ryšio priemonių, kompiuterinės įrangos, kurioje saugoma ar kuria perduodama įslaptinta informacija, ADA sistemų bei tinklų techninę priežiūrą, privalo turėti leidimus dirbti ar susipažinti su įslaptinta informacija, žymima aukščiausia tokioje įrangoje ar sistemoje apdorojamos, saugomos ar perduodamos informacijos slaptumo žyma.

5. Įslaptintą informaciją apdorojančiose ADA sistemose ir tinkluose draudžiama įrengti ADA sistemų ir tinklų dokumentacijoje nenumatytą techninę ar programinę įrangą.

42 straipsnis. Įslaptintos informacijos perdavimas ADA sistemomis ir tinklais

1. Perduodant įslaptintą informaciją ADA sistemomis ir tinklais, turi būti užtikrintas perduodamos įslaptintos informacijos slaptumas, vientisumas, prieinamumas teisėtiems vartotojams.

2. ADA sistemomis ir tinklais perduodant įslaptintą informaciją, jos slaptumas turi būti užtikrintas vadovaujantis Nacionalinės šifrų paskirstymo tarnybos patvirtintais kriptografiniais metodais ir produktais bei Nacionalinės komunikacijų apsaugos tarnybos patvirtintais telekomunikacijų apsaugos reikalavimais.

3. Įslaptintą informaciją, žymimą slaptumo žymomis „Riboto naudojimo“, „Konfidencialiai“, „Slaptai“, draudžiama perduoti viešais telekomunikacijų tinklais neužšifruotą, išskyrus šio straipsnio 4 dalyje nustatytus atvejus. Įslaptintą informaciją, žymimą slaptumo žyma „Visiškai slaptai“, perduoti telekomunikacijų tinklais draudžiama.

4. Paslapčių subjekto struktūrinio padalinio, disponuojančio įslaptinta informacija, vadovo sprendimu įslaptinta informacija, žymima slaptumo žymomis „Riboto naudojimo“, „Konfidencialiai“ ir „Slaptai“, gali būti perduodama neužšifruota, jeigu paskelbta karo ar nepaprastoji padėtis ir nėra galimybių užšifruoti informaciją, o pristatymo greitis yra svarbesnis nei galimas tokios informacijos atskleidimo pavojus.

5. Kriptografiniams produktams, mechanizmams ir įslaptintai informacijai teikiama apsauga turi atitikti žalos, kurią gali sukelti įslaptintos informacijos neteisėtas atskleidimas, dydį.

43 straipsnis. Kompiuterių informacijos laikmenų apsauga

1. Visos įslaptintos kompiuterių informacijos laikmenos turi būti tinkamai identifikuotos, laikomos ir saugomos pagal jose esančios aukščiausia slaptumo žyma žymimos informacijos apsaugos reikalavimus.

2. Įslaptinta informacija, laikoma daugkartinio naudojimo kompiuterių informacijos laikmenose, gali būti ištrinama ir tokios laikmenos išslaptinamos tik vadovaujantis šio Įstatymo 40 straipsnio 1 dalyje nurodytų institucijų nustatytomis procedūromis.

44 straipsnis. Atsakingo asmens funkcijos organizuojant ADA sistemų ir tinklų apsaugą

Atsakingas asmuo privalo:

1) užtikrinti apsaugos priemonių įdiegimą, veikimą ir priežiūrą darbo vietose, turinčiose ADA elementų;

2) sudaryti telekomunikacijų planus ir schemas ir juose nurodyti laidų, kabelių lokalizacijos vietą, jų kiekį, tipus, numeraciją;

3) vadovaudamasis Saugumo priežiūros tarnybos nustatytais reikalavimais, rengti, įgyvendinti ir kontroliuoti paslapčių subjekto, rangovo (subrangovo) ADA sistemų ir tinklų saugumo valdymo procedūras ir su jomis periodiškai supažindinti ADA sistemų ir tinklų administratorius bei vartotojus;

4) parengti dokumentus apie ADA sistemas ir tinklus, reikalingus gauti leidimui saugoti, apdoroti ar perduoti įslaptintą informaciją, žymimą slaptumo žymomis „Visiškai slaptai“, „Slaptai“, „Konfidencialiai“;

5) užtikrinti, kad ADA sistemose ir tinkluose dirbtų vartotojai, kuriems suteikta teisė susipažinti su ADA sistemose ar tinkluose saugoma, apdorojama, perduodama informacija, kuri susijusi su jų pareigų vykdymu, taip pat kontroliuoti vartotojų veiksmus;

6) vykdyti vartotojams suteiktų slaptažodžių ir (ar) vartotojų tapatybės nustatymo įrenginių administravimo kontrolę;

7) organizuoti įslaptintų kompiuterinės informacijos laikmenų administravimą bei fizinę tokių laikmenų apsaugą;

8) įvertinti rangovo ar subrangovo pasirengimą įvykdyti jam numatytos perduoti įslaptintos informacijos, žymimos slaptumo žyma „Riboto naudojimo“, aparatūrinės ar programinės įrangos apsaugos reikalavimus, kontroliuoti tokių reikalavimų įgyvendinimą;

9) organizuoti ir tikrinti sisteminį rezervinį ADA sistemų ir tinklų informacijos kopijavimą ir atkūrimą;

10) tikrinti surinktą informaciją apie įvykius (procesų klaidas, neteisėtus vartotojus ir sistemos veiklą);

11) pranešti paslapčių subjekto vadovui ar jo įgaliotam asmeniui apie bet kokias paslapčių subjekto, rangovo (subrangovo) ADA sistemų ir tinklų apsaugos spragas, įvykusius pažeidimus ir imtis priemonių jiems pašalinti.

DEVINTASIS SKIRSNIS
ĮSLAPTINTOS INFORMACIJOS APSAUGOS KONTROLĖ

45 straipsnis. Įslaptintos informacijos apsaugos kontrolė

1. Lietuvos Respublikos įslaptintos informacijos apsaugos politikos įgyvendinimą ir įslaptintos informacijos apsaugos veiksmų įgyvendinimą visose institucijose šalies viduje ir užsienyje kontroliuoja Valstybės saugumo departamentas. Šis departamentas:

1) kontroliuoja, kaip laikomasi įslaptintos informacijos, žymimos slaptumo žymomis „Visiškai slaptai“, „Slaptai“, „Konfidencialiai“, įslaptinimo, naudojimo, saugojimo, naikinimo bei išslaptinimo nustatytos tvarkos. Valstybės saugumo departamento tikrinimo metu nustatytus trūkumus paslapčių subjektas privalo pašalinti per šio departamento nustatytą terminą ir apie tai raštu pranešti Valstybės saugumo departamentui;

2) teikia pasiūlymus Vyriausybei, Paslapčių apsaugos koordinavimo komisijai dėl įslaptintos informacijos apsaugos sistemos tobulinimo;

3) atlieka ikiteisminio tyrimo veiksmus dėl neteisėto disponavimo įslaptinta informacija, įslaptintos informacijos atskleidimo, praradimo, pagrobimo ar kitokio neteisėto įgijimo;

4) teikia metodinę pagalbą paslapčių subjektams dėl įslaptintos informacijos apsaugos.

2. Įslaptintos informacijos, žymimos slaptumo žyma „Riboto naudojimo“, apsaugos kontrolę vykdo šia informacija disponuojantys paslapčių subjektai.

3. Asmenys, kontroliuojantys įslaptintos informacijos apsaugą, privalo turėti leidimus dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma „Visiškai slaptai“. Asmenys, kontroliuojantys kitų valstybių ar tarptautinių organizacijų Lietuvos Respublikai perduotos įslaptintos informacijos apsaugą, privalo turėti atitinkamus asmens patikimumo pažymėjimus.

4. Įslaptintos informacijos apsaugą kontroliuojantys asmenys tikrinimų metu su įslaptintų dokumentų turiniu supažindinami tik paslapčių subjekto vadovo sutikimu.

5. Asmenys, vykdantys įslaptintos informacijos apsaugos kontrolę, turi teisę:

1) paslapčių subjekto nustatyta tvarka patekti į teritorijas ir patalpas, kuriose įslaptinta informacija yra apdorojama, saugoma arba perduodama;

2) susipažinti su paslapčių subjekto dokumentais, reglamentuojančiais įslaptintos informacijos apsaugą;

3) atlikti įslaptintų dokumentų ar jų kopijų saugojimo kontrolinius tikrinimus, kai reikia nustatyti, ar dokumentas (jo kopija) tikrai nedingęs ir saugomas apskaitos dokumentuose nurodytoje vietoje;

4) susipažinti su fizinės apsaugos priemonėmis;

5) susipažinti su ADA sistemomis ir tinklais, skirtais įslaptintai informacijai apdoroti, saugoti ar perduoti;

6) iš atsakingų asmenų bei asmenų, dirbančių su įslaptinta informacija, reikalauti žodinių bei rašytinių paaiškinimų apie įslaptintos informacijos apsaugos tvarkos laikymąsi ar šios tvarkos pažeidimus;

7) pasitelkti atitinkamų sričių specialistus, jeigu kontrolės metu būtinos specialios žinios.

6. Kilus įtarimams, kad yra prarasta ar neteisėtai atskleista įslaptinta informacija, paslapčių subjekto vadovo sprendimu atliekamas patikrinimas. Patikrinimo metu turi būti:

1) nustatyta ir patvirtinta prarastos ar atskleistos įslaptintos informacijos slaptumo žyma, turinys bei apimtis;

2) nustatyti asmenys, kurių veiksmai galėjo lemti įslaptintos informacijos praradimą ar atskleidimą;

3) įvardyti asmenys, kurie šia informacija disponavo ar kurie buvo su ja susipažinę;

4) nustatytos įslaptintos informacijos praradimo ar atskleidimo aplinkybės.

7. Jei atlikus šio straipsnio 6 dalyje ar šio Įstatymo 27 straipsnyje numatytą patikrinimą paaiškėja, kad įslaptinta informacija tikrai prarasta ar neteisėtai atskleista, paslapčių subjekto vadovas nedelsdamas apie tai praneša Valstybės saugumo departamentui, o šio įgalioti pareigūnai atlieka ikiteisminį tyrimą.

8. Jeigu atlikus patikrinimą paaiškėja, kad Lietuvos Respublikai užsienio valstybių ar tarptautinių organizacijų perduota įslaptinta informacija buvo tikrai prarasta ar neteisėtai atskleista, nedelsiant pranešama Paslapčių apsaugos koordinavimo komisijai, informaciją perdavusios

valstybės ar tarptautinės organizacijos atitinkamoms tarnyboms ir Valstybės saugumo departamentui, o šis atlieka ikiteisminį tyrimą.

DEŠIMTASIS SKIRSNIS
ATSAKOMYBĖ

46 straipsnis. Atsakomybė už neteisėtą disponavimą įslaptinta informacija, įslaptintos informacijos atskleidimą, praradimą, pagrobimą ar kitokį neteisėtą įgijimą

Asmuo už neteisėtą disponavimą įslaptinta informacija, įslaptintos informacijos atskleidimą, praradimą, pagrobimą ar kitokį neteisėtą įgijimą arba kitus įslaptintos informacijos apsaugos reikalavimų pažeidimus atsako teisės aktų nustatyta tvarka.“

2 straipsnis. Įstatymo įsigaliojimas ir įgyvendinimas

1. Šis Įstatymas įsigalioja nuo 2004 m. gegužės 1 d.

2. Šio Įstatymo įgyvendinimo tvarką nustato Valstybės ir tarnybos paslapčių įstatymo pakeitimo įstatymo įgyvendinimo įstatymas.

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

RESPUBLIKOS PREZIDENTAS ROLANDAS PAKSAS

Lietuvos Respublikos

2003 m. gruodžio 16 d.
įstatymo Nr. IX-1908
priedas

ĮGYVENDINIMAS EUROPOS SĄJUNGOS TEISĖS AKTAS

2001 m. kovo 19 d. Europos Tarybos sprendimas 2001/264/EB dėl Europos Sąjungos Tarybos saugumo nuostatų.