INFORMATIKOS IR RYŠIŲ DEPARTAMENTO
PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS DIREKTORIUS
Į S A K Y M A S

DĖL BENDRŲJŲ (VISIEMS VIENODŲ) ŽINYBINIŲ SAUGUMO PRIEŽIŪROS TARNYBŲ STEIGIMO IR VEIKLOS TAISYKLIŲ, DOKUMENTŲ, REIKALINGŲ LEIDIMUI AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ IŠDUOTI, RENGIMO IR LEIDIMŲ AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ IŠDAVIMO TAISYKLIŲ IR AUTOMATIZUOTO DUOMENŲ APDOROJIMO SISTEMŲ IR TINKLŲ, KURIUOSE BUS SAUGOMA, APDOROJAMA AR KURIAIS BUS PERDUODAMA ĮSLAPTINTA INFORMACIJA, SAUGUMO REIKALAVIMŲ APRAŠO PATVIRTINIMO

2010 m. lapkričio 29 d. Nr. 5V-138
Vilnius

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

t v i r t i n u pridedamus:

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

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

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

DIREKTORIUS VYGANTAS IVANAUSKAS

_____

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

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

I. BENDROSIOS NUOSTATOS

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

2. Taisyklėse vartojamos sąvokos:

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

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

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

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

II. ŽINYBINIŲ SPT FUNKCIJOS

4. Žinybinė SPT atlieka šias funkcijas:

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

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

apsauga;

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

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

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

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

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

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

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

4.10. atlieka kitas Lietuvos Respublikos teisės aktuose numatytas funkcijas.

III. ŽINYBINIŲ SPT STEIGIMAS

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

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

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

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

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

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

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

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

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

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

IV. ŽINYBINIŲ SPT VEIKLOS KOORDINAVIMAS

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

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

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

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

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

ADA sistemomis ir tinklais.

V. ŽINYBINIŲ SPT PANAIKINIMAS

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

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

VI. BAIGIAMOSIOS NUOSTATOS

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

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

———————

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

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

I. BENDROSIOS NUOSTATOS

1.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

2.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

Taisyklėse vartojamos sąvokos:

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

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

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

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

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

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

Rizika – grėsmės pasireiškimo per tam tikrą laiko tarpą tikimybė.

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

ADA sistemos ar tinklo valdytojas – ADA sistemos ar tinklo nuostatuose nurodytas paslapčių

subjektas arba jo įgaliotas struktūrinis padalinys, arba rangovas (subrangovas), kuris valdo ADA sistemą ar tinklą, juos sukūręs ar užsakęs sukurti arba įsigijęs.

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

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

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

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

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

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

4.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

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

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

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

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

6.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

6.1. specifinių saugumo reikalavimų aprašas;

6.2. saugumo valdymo procedūrų aprašas;

6.3. rizikos analizė;

6.4. saugumo reikalavimų įgyvendinimo patikrinimo ataskaita.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

6^1.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

Rangovo ADA sistemas ir tinklus, kuriuose numatoma automatizuotai apdoroti įslaptintą informaciją ar kuriais numatoma tokią informaciją perduoti, vertina ir leidimus automatizuotai apdoroti ir perduoti įslaptintą

informaciją ADA sistemomis ir tinklais išduoda žinybinė SPT arba SPT įslaptintų sandorių saugumą užtikrinančios institucijos rašytiniu prašymu.

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

7.1. ADA sistemos ir tinklo apibūdinimas:

7.1.1. ADA sistemos ir tinklo paskirtis ir funkcijos;

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

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

7.1.4. ADA sistemos ir tinklo naudotojai, jų funkcijos;

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

7.1.6. sąsajos tarp atskirų ADA sistemų ir tinklų.

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

7.2.1. grėsmes, kylančias ADA sistemai ir tinklui;

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

7.2.3. ADA sistemos ir tinklo pažeidžiamumus;

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

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

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

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

7.3.3. elektroninė saugumo aplinka.

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

7.5. Saugumo valdymo reikalavimų aprašymas. Šiame skyriuje aprašoma:

7.5.1. ADA sistemos ir tinklo veiklos tęstinumas;

7.5.2. ADA sistemos ir tinklo rizikos valdymas;

7.5.3. ADA sistemos ir tinklo pakeitimų valdymas;

7.5.4. ADA sistemos ir tinklo apsaugos dokumentavimas ir mokymai;

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

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

9. SVPA privalomai turi būti nurodyta:

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

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

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

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

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

KEISTA:

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)

(Žin., 2013, Nr. 4-158)

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

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

9.2. ADA sistemos ir tinklo fizinės apsaugos procedūros:

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

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

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

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

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

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

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

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

9.3. ADA sistemos ir tinklo personalo saugumo procedūros:

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

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

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

9.3.4. personalo mokymo ir švietimo saugumo klausimais aprašymas;

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

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

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

9.4.1. naudojamos dokumentų saugojimo terpės, taikomos slaptumo žymos;

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

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

9.5. ADA sistemos ir tinklo informacijos saugumo procedūros:

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

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

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

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

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

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

KEISTA:

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)

(Žin., 2013, Nr. 4-158)

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

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

KEISTA:

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)

(Žin., 2013, Nr. 4-158)

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

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

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

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

9.6.4. ADA sistemos ir tinklo veiklos atkūrimu;

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

9.6.6. reguliariu šio plano veiksmingumo išbandymu.

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

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

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

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

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

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

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

11.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

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

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

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

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

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

12.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

13.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

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

14^1.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

15.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

16.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

Laikinas leidimas išduodamas per taisyklių 15 punkte nustatytą terminą vertinimo metu nustačius ADA sistemų ir tinklų atitiktį taisyklių 5 punkte nustatytiems reikalavimams, tačiau dėl objektyvių priežasčių

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

17.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

19.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

20.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

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

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

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

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

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

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

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

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

27^1.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

IV. PAKARTOTINIS LEIDIMŲ ADA SISTEMOMS IR TINKLAMS IŠDAVIMAS

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

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

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

V. BAIGIAMOSIOS NUOSTATOS

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

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

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

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

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

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

NAUJA REDAKCIJA nuo 2013 01 13
(Žin., 2013, Nr. 4-158)

(LEIDIMO AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ FORMA)

20 m. d. Nr.
Vilnius

Šis leidimas išduotas

(paslapčių subjekto pavadinimas arba rangovo (subrangovo) pavadinimas)
ir patvirtina, kad automatizuoto duomenų apdorojimo sistema ar tinklas

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

(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo pavadinimas)

(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo adresas)
turi teisę atlikti visas teisės aktų nustatytas funkcijas ir automatizuotai apdoroti įslaptintą informaciją, žymimą slaptumo žyma (žymomis)

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

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

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

Leidimas galioja: (leidimo galiojimo terminas)

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

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

2 priedas

NAUJA REDAKCIJA nuo 2013 01 13
(Žin., 2013, Nr. 4-158)

(LAIKINO LEIDIMO AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ FORMA)

20 m. d. Nr.
Vilnius

Šis laikinas leidimas išduotas

_____
(paslapčių subjekto pavadinimas arba rangovo (subrangovo) pavadinimas)
ir patvirtina, kad automatizuoto duomenų apdorojimo sistema ar tinklas

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

_____,
(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo adresas)
turi teisę atlikti šio leidimo 1 p. nurodytoje išvadoje nustatytas funkcijas nurodyta apimtimi ir sąlygomis ir automatizuotai apdoroti įslaptintą informaciją, žymimą slaptumo žyma (žymomis) _____ ir žemesne (žemesnėmis).
(slaptumo žyma ar žymos)

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

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

Laikinas leidimas galioja: _____
(laikino leidimo galiojimo terminas)

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

_____

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

NAUJA REDAKCIJA nuo 2013 01 13
(Žin., 2013, Nr. 4-158)

(RIBOTO LEIDIMO AUTOMATIZUOTAI APDOROTI ĮSLAPTINTĄ INFORMACIJĄ FORMA)

20 m. d. Nr.
Vilnius

Šis ribotas leidimas išduotas

(paslapčių subjekto pavadinimas arba rangovo (subrangovo) pavadinimas)
ir patvirtina, kad automatizuoto duomenų apdorojimo sistema ar tinklas

,
(automatizuoto duomenų apdorojimo sistemos ar tinklo pavadinimas)
valdoma (-as)
(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo pavadinimas)
,
(automatizuoto duomenų apdorojimo sistemos ar tinklo valdytojo adresas)
turi teisę atlikti šio leidimo 1 p. nurodytoje išvadoje nustatytus vienkartinius veiksmus nurodyta apimtimi ir sąlygomis ir automatizuotai apdoroti įslaptintą informaciją, žymimą slaptumo žyma (žymomis)
(slaptumo žyma ar žymos) ir žemesne (žemesnėmis).

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

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

Ribotas leidimas galioja: (riboto leidimo galiojimo terminas)

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

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

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

I. BENDROSIOS NUOSTATOS

1.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

2.

KEISTA:

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

Apraše vartojamos sąvokos:

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

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

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

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

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

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

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

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

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

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

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

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

3.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

Aprašas skirtas užtikrinti:

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

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

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

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

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

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

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

4.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

II. REIKALAVIMAI ADA SISTEMŲ IR TINKLŲ SAUGOS VALDYMO ORGANIZAVIMUI

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

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

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

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

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

10. ADA sistemos ar tinklo valdytojo funkcijos ir atsakomybė:

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

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

10.3. tvirtina saugos dokumentus;

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

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

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

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

12. Saugos įgaliotinio funkcijos ir atsakomybė:

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

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

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

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

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

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

12.2. rengia ADA sistemos ar tinklo saugos dokumentus;

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

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

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

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

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

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

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

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

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

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

13. Administratoriaus atsakomybė ir funkcijos:

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

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

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

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

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

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

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

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

14. Reikalavimai kriptografinių priemonių administratoriui, jo funkcijos ir atsakomybė nustatomi Bendrosiose įslaptintos informacijos kriptografinės apsaugos taisyklėse.

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

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

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

KEISTA:

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)

(Žin., 2013, Nr. 4-158)

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

KEISTA:

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)

(Žin., 2013, Nr. 4-158)

16.3. *NETEKO GALIOS:*

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)

(Žin., 2013, Nr. 4-158)

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

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

KEISTA:

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)

(Žin., 2013, Nr. 4-158)

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

KEISTA:

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)

(Žin., 2013, Nr. 4-158)

17.3. *NETEKO GALIOS:*

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)

(Žin., 2013, Nr. 4-158)

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

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

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

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

18.4. ADA sistemos ir tinklo valdytojo vadovybės pavedimu;

18.5. kitais žinybinės SPT ar SPT nustatytais atvejais.

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

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

nustatyta tvarka turi būti patvirtintas įgaliotųjų institucijų.

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

22.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

III. REIKALAVIMAI ADA SISTEMŲ IR TINKLŲ PRIEIGOS TEISIŲ VALDYMUI

23.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

25.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

26.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

27.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

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

30.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

Reikalavimus tapatybės patvirtinimo priemonėms nustato Nacionalinė komunikacijų apsaugos tarnyba.

IV. REIKALAVIMAI ADA SISTEMŲ IR TINKLŲ ĮVYKIŲ REGISTRAVIMUI

31.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

ADA sistemose ir tinkluose turi būti užtikrintas nuolatinis įvykių (ADA sistemos ar tinklo veiklos įrašų) registravimas, nurodant laiką ir susijusį naudotojo identifikatorių. Reikalaujamų registruoti įvykių sąrašą nustato Nacionalinė komunikacijų apsaugos tarnyba. ADA sistemos ar tinklo valdytojas, vadovaudamasis rizikos analize, gali savo sprendimu papildyti minėtą sąrašą. Įvykiai turi būti registruojami pagrindiniame ir rezerviniame (jei leidžia ADA sistemos ar tinklo funkcionalumas – nutolusiame) įvykių žurnaluose. Laikrodžiai, pagal kuriuos nustatomas įvykių laikas, turi būti sinchronizuoti, išskyrus ADA sistemas, kurias sudaro pavieniai, nesujungti kompiuteriai. Turi būti priemonės, leidžiančios nustatyti su įvykiais susijusius asmenis visą įvykių žurnalų saugojimo laiką.

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

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

34.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

V. KITI REIKALAVIMAI

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

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

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

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

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

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

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

KEISTA:

2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

40.2. S ir VS sistemų ir tinklų – ne rečiau kaip kartą per 6 mėnesius.
KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

42.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

43.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

45.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

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

48.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

49.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

50.

KEISTA:
2013 01 07 įsakymu Nr. 5V-1 (nuo 2013 01 13)
(Žin., 2013, Nr. 4-158)

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

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

_____