VYRIAUSYBINIŲ RYŠIŲ CENTRO PRIE LIETUVOS RESPUBLIKOS VALSTYBĖS SAUGUMO DEPARTAMENTO DIREKTORIAUS

Į S A K Y M A S

DĖL AUTOMATIZUOTO DUOMENŲ APDOROJIMO SISTEMŲ IR TINKLŲ, KURIUOSE SAUGOMA, APDOROJAMA AR PERDUODAMA ĮSLAPTINTA INFORMACIJA, KŪRIMO METODIKOS PATVIRTINIMO

2013 m. spalio 31 d. Nr. 1-22
Vilnius

Vadovaudamasis Lietuvos Respublikos Vyriausybės 2013 m. rugpjūčio 21 d. nutarimo Nr. 759 „Dėl Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, steigimo ir įteisinimo taisyklių patvirtinimo“ (Žin., 2013, Nr. 92-4568) 4 punktu,

t v i r t i n u Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar perduodama įslaptinta informacija, kūrimo metodiką (pridedama).

DIREKTORIUS VYTAUTAS JANUŠIS

_____

PATVIRTINTA
Vyriausybinių ryšių centro prie Lietuvos Respublikos valstybės saugumo departamento direktoriaus
2013 m. spalio 31 d. įsakymu Nr. 1-22

AUTOMATIZUOTO DUOMENŲ APDOROJIMO SISTEMŲ IR TINKLŲ, KURIUOSE SAUGOMA, APDOROJAMA AR KURIAIS PERDUODAMA ĮSLAPTINTA INFORMACIJA, KŪRIMO METODIKA

I. BENDROSIOS NUOSTATOS

1. Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, kūrimo metodika (toliau – Metodika) nustato principus, kuriais vadovaujantis turi būti projektuojamos ir kuriamos automatizuoto duomenų apdorojimo (toliau – ADA) sistemos ir tinklai, kuriuose saugoma, apdorojama ar perduodama (toliau – apdorojama) Lietuvos Respublikos įslaptinta informacija, Lietuvos Respublikai perduota užsienio valstybių, Europos Sąjungos ir tarptautinių organizacijų įslaptinta informacija, žymima slaptumo žymomis „Riboto naudojimo“, „Konfidencialiai“, „Slaptai“ ir „Visiškai slaptai“ ar jų atitikmenimis (toliau – įslaptinta informacija).

2. Metodika turi vadovautis ADA sistemos ar tinklo valdytojai ir tvarkytojai.

3. Metodika paremta ADA sistemų ir tinklų gyvavimo ciklu, apibrėžiančiu ADA sistemos ar tinklo kūrimo stadijas.

4. Šioje Metodikoje vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme (Žin., 1999, Nr. 105-3019; 2004, Nr. 4-29), Lietuvos Respublikos Vyriausybės 2013 m. rugpjūčio 31 d. nutarime Nr. 759 „Dėl Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija steigimo ir įteisinimo taisyklių patvirtinimo“ (Žin., 2013, Nr. 92-4568) ir kituose teisės aktuose, reglamentuojančiuose ADA sistemų ir tinklų steigimą, įteisinimą ir valdymą.

II. ADA SISTEMŲ IR TINKLŲ GYVAVIMO CIKLAS

5. ADA sistemų ir tinklų gyvavimo ciklas susideda iš nuoseklių stadijų, kurios gali būti skaidomos į etapus, etapai – į darbus. Etapai ir darbai nustatomi taip, kad kiekvieno jų pabaigoje būtų gautas konkretus rezultatas, kuris fiksuojamas jį aprašant. Vadovaudamasis aprašymu, ADA sistemos ar tinklo valdytojas arba tvarkytojas vykdo etapo realizavimo metu atliktų darbų patikrinimą ir vertinimą. Esant teigiamam vertinimui, užsakovas ir rangovas pasirašo darbų atlikimo aktą. Kiekvienos stadijos pabaigoje priimamas sprendimas, t. y. ADA tinklo ar sistemos kūrimo darbų užsakovas sutinka, kad stadijos metu numatyti vykdyti visi veiksmai atlikti ir aprašyti tinkamai.

6. ADA sistemų ir tinklų gyvavimo ciklas skirstomas į šias stadijas:

6.1. ADA sistemų ir tinklų steigimas;

6.2. ADA sistemų ir tinklų kūrimas;

6.3. ADA sistemų ir tinklų naudojimas ir modernizavimas;

6.4. ADA sistemų ir tinklų likvidavimas.

III. ADA SISTEMŲ IR TINKLŲ STEIGIMAS

7. ADA sistemų ir tinklų steigimo stadijos metu įvertinami su ADA sistemų ar tinklų veikla susiję funkciniai poreikiai (įskaitant tikėtinus būsimus poreikius) bei numatoma, kas, kada, kur ir kaip ja naudosis; apibrėžiami informacijos srautai, apsisprendžiama dėl funkcinės struktūros bei atliekamas pradinis galimų grėsmių saugiam ADA sistemos ar tinklo darbui įvertinimas. Šių vertinimų ir analizės pagrindu identifikuojami saugumo reikalavimai, kuriais vadovaujantis pasirenkami saugos užtikrinimo principai ir techniniai sprendimai, leisiantys užtikrinti minėtų reikalavimų vykdymą.

8. Metodikos 7 punkte nurodytų tikslų įgyvendinimui identifikuojami ir vertinami šie aspektai:

8.1. aukščiausia įslaptintos informacijos, kuri bus apdorojama kuriamoje ADA sistemoje ar tinkle, žyma;

8.2. nustatoma ADA sistemos ar tinklo struktūra, įvertinami būsimi informaciniai srautai, apsisprendžiama dėl sujungimų su kitomis ADA sistemomis ar tinklais būtinybės;

8.3. identifikuojamos globali, lokali ir elektroninė saugumo aplinkos;

8.4. apsisprendžiama dėl ADA sistemos ar tinklo naudotojų, apibrėžiamos jų teisės, skiriamas ADA sistemą ar tinklą administruojantis personalas bei nustatomos jų teisės ir pareigos;

8.5. įvertinus ADA sistemos ar tinklo naudotojų galimybę disponuoti ADA sistemoje ar tinkle apdorojama įslaptinta informacija bei vadovaujantis Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, telekomunikacijų apsaugos reikalavimų apraše, patvirtintame Vyriausybinių ryšių centro prie Lietuvos Respublikos valstybės saugumo departamento (toliau – VRC) direktoriaus 2010 m. birželio 30 d. įsakymu Nr. 2-8RN, pateiktais ADA sistemų ir tinklų saugos režimų apibrėžimais, nustatomas kuriamos ADA sistemos ar tinklo saugos režimo tipas;

8.6. atliekamas preliminarus rizikos vertinimas, kurio metu identifikuojami rizikos saugiai ADA sistemos ar tinklo veiklai faktoriai;

8.7. identifikuojama Saugos priežiūros tarnyba (toliau – SPT), kuriai bus teikiami dokumentai, reikalingi leidimo automatizuotai apdoroti įslaptintą informaciją steigiamoje ADA sistemoje ar tinkle gavimui.

9. Atsižvelgiant į rizikos vertinimą, ADA sistemos ar tinklo saugos režimo tipą, į aukščiausią apdorojamos įslaptintos informacijos slaptumo žymą, struktūrą bei kitus faktorius, galinčius turėti įtakos saugiam apibrėžtoje aplinkoje veikiančios ADA sistemos ar tinklo

darbui, pasirenkamos priemonės, užtikrinsiančios joje apdorojamos įslaptintos informacijos konfidencialumą, vientisumą ir prieinamumą teisėtiems ADA sistemos ar tinklo naudotojams.

10. Renkantis Metodikos 9 punkte minėtas priemones, vadovaujamasi Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašu, patvirtintu Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2010 m. lapkričio 29 d. įsakymu Nr. 5V-138 (Žin., 2010, Nr. 142-7328), ir Telekomunikacijų apsaugos reikalavimų aprašu.

11. Renkantis skirtingų ADA sistemų ar tinklų sujungimo saugos užtikrinimo priemones, vadovaujamasi Telekomunikacijų apsaugos reikalavimų aprašo reikalavimais.

IV. ADA SISTEMŲ IR TINKLŲ KŪRIMAS

12. ADA sistemų ir tinklų kūrimo stadijos metu pasirenkama techninė ir programinė įranga, kuri leidžia užtikrinti ADA sistemos ar tinklo funkcionavimą bei realizuoti priemones, užtikrinančias saugų įslaptintos informacijos apdorojimą; suprojektuojamos ir įrengiamos apdorojamos įslaptintos informacijos saugos užtikrinimo reikalavimus atitinkančios ADA sistemos ar tinklai; rengiami ir SPT teikiami nustatytos apimties ir turinio ADA sistemą ar tinklą bei jame naudojamas saugos užtikrinimo priemones apibūdinantys dokumentai, vykdoma įdiegtų saugos užtikrinimo priemonių atitikties inspekcija ir vertinimas. Stadija baigiama leidimo automatizuotai apdoroti įslaptintą informaciją išdavimu.

13. ADA sistemų ir tinklų kūrimas skirstomas į šiuos etapus:

13.1. techninės ir programinės įrangos pasirinkimas;

13.2. ADA sistemos ar tinklo specifikacijos rengimas;

13.3. techninės ir programinės įrangos įsigijimas;

13.4. ADA sistemos ar tinklo įrengimas, dokumentų, reikalingų leidimo automatizuotai apdoroti įslaptintą informaciją kuriamoje ADA sistemoje ar tinkle gavimui (toliau – akreditavimo dokumentai), rengimas ir pateikimas SPT;

13.5. leidimo automatizuotai apdoroti įslaptintą informaciją gavimas.

14. Renkantis techninę įrangą, įvertinamos reikalingos techninės charakteristikos bei vadovaujamasi šiomis nuostatomis:

14.1. kriptografinė ir duomenų apdorojimo įranga, skirta ADA sistemoms ir tinklams, kuriuose aukščiausia apdorojamos įslaptintos informacijos žyma „Konfidencialiai“ ar aukštesnė, turi užtikrinti apsaugą nuo informatyviojo elektromagnetinio spinduliavimo (toliau – TEMPEST). Reikiamas įrangos TEMPEST apsaugos lygis nustatomas vadovaujantis ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašu, patvirtintu Lietuvos Respublikos paslapčių apsaugos koordinavimo komisijos 2010 m. birželio 28 d. posėdžio protokolu Nr. 56-3 (Žin., 2010, Nr. 82-4374). Esant neaiškumams, rekomenduojama konsultuotis su įgaliotomis institucijomis, užtikrinančiomis įslaptintos informacijos, saugomos, apdorojamos ADA sistemose ir tinkluose arba jais perduodamos, apsaugą nuo TEMPEST;

14.2. pasirinkta įsigyti kriptografinė įranga turi būti įtraukta į VRC administruojamą Leistinų naudoti Lietuvos Respublikoje kriptografinių priemonių sąrašą. Vadovaujamasi minėto sąrašo „Riboto naudojimo“ versija, skelbiama Vyriausybinio plačiajuosčio šifruoto duomenų ir balso perdavimo tinklo duomenų bazėje. Jei pasirinktos įsigyti kriptografinės priemonės minėtame sąraše nėra, nustatyta tvarka VRC teikiamas prašymas atlikti kriptografinės priemonės vertinimą. Kriptografinė priemonė pasirenkama tik teigiamo sprendimo atveju;

14.3. numatomos naudoti virtualios mašinos turi būti laikomos analogiškos fizinei duomenų apdorojimo įrangai. Joms taikomi fizinėje įrangoje apdorojamos informacijos saugos užtikrinimo reikalavimai.

15. Pasirenkant kuriamoje ADA sistemoje ar tinkle skirtą naudoti programinę įrangą vadovaujamasi šiomis nuostatomis:

15.1. saugos funkcijas užtikrinanti programinė įranga turi atitikti Telekomunikacijų apsaugos reikalavimų apraše nurodytus standarto LST ISO/IEC 15408 „Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai“ nustatytus saugos užtikrinimo lygius EAL. Renkantis tokią įrangą rekomenduojama naudotis NATO informacijos saugą užtikrinančių gaminių katalogu (angl. *NATO Information Assurance Product Catalogue* arba *NIAPC,* toliau – katalogas). Neįtrauktos į katalogą programinės įrangos naudojimas leidžiamas tik suderinus su Nacionalinės komunikacijų apsaugos tarnybos funkcijas vykdančia institucija (toliau – NKAT) ir vadovaujantis jos rekomendacijomis;

15.2. ADA sistemose ir tinkluose, kuriuose aukščiausia apdorojamos įslaptintos informacijos slaptumo žyma „Konfidencialiai“ ar aukštesnė, naudoti neįtrauktą į katalogą saugos funkcijas užtikrinančią programinę įrangą, sukurtą trečiose šalyse, draudžiama, o ADA sistemose ir tinkluose, kuriuose apdorojama įslaptinta informacija, žymima slaptumo žyma „Riboto naudojimo“ – nerekomenduojama;

15.3. rekomenduojama naudoti žinomų gamintojų sukurtas taikomąsias programas. Gali būti naudojamos specialiai sukurtos programos, skirtos specifinių ADA sistemų ar tinklų funkcijų vykdymui. Numačius naudoti tokias programas ADA sistemose ir tinkluose, kuriuose aukščiausia apdorojamos įslaptintos informacijos slaptumo žyma „Konfidencialiai“ ar aukštesnė, SPT gali pareikalauti, kad įgaliota institucija atliktų pirminių sukurtos programos tekstų analizę.

16. Pasirinkus Metodikos 14 ir 15 punktuose nustatytus reikalavimus atitinkančią techninę ir programinę įrangą, rengiama ADA sistemos ar tinklo specifikacija. Tai atliekama vadovaujantis VRC direktoriaus tvirtinamu Reikalavimų ADA sistemų ir tinklų specifikacijoms aprašu. Parengtas specifikacijos projektas derinamas Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, steigimo ir įteisinimo taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 2013 m. rugpjūčio 21 d. nutarimu Nr. 759 (Žin., 2013, Nr. 92-4568), nustatyta tvarka.

17. Įrengimo etapo metu ADA sistema ar tinklas rengiami eksploatacijai: įrengiamos darbo vietos, diegiama programinė įranga, montuojami tinklo komponentai. Įrengus, vykdomas ADA sistemos ar tinklo veikimo patikrinimas.

Šiame etape tikslinamos ir detalizuojamos ADA sistemos ar tinklo naudotojų teisės, administruojančio personalo teisės ir pareigos, ADA sistemos ar tinklo naudotojai mokomi naudotis tinklo įranga.

Šio etapo metu ADA sistemos ar tinklo valdytojas/tvarkytojas rengia akreditavimo dokumentus. Vadovaujantis jais, ADA sistemos ar tinklo naudotojai supažindinami su saugaus darbo ADA sistemoje ar tinkle principais, saugos užtikrinimo reikalavimais.

Šis etapas baigiamas akreditavimo dokumentų pateikimu SPT.

18. ADA sistemų ir tinklų įrengimas vykdomas vadovaujantis šiomis nuostatomis:

18.1. ADA sistemų ir tinklų techninė įranga diegiama vadovaujantis Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašu ir Telekomunikacijų apsaugos reikalavimų aprašo reikalavimais. ADA sistemoms ir tinklams, kuriuose aukščiausia apdorojamos įslaptintos informacijos slaptumo žyma „Konfidencialiai“ ar aukštesnė, papildomai vadovaujamasi ADA sistemose ir tinkluose saugomos, apdorojamos ar perduodamos įslaptintos informacijos apsaugos nuo informatyviojo elektromagnetinio spinduliavimo (TEMPEST) užtikrinimo bendrųjų reikalavimų ir procedūrų aprašu;

18.2. ADA sistemų ir tinklų įrangos ir tinklo dalies montavimą vykdantis personalas turi turėti leidimą dirbti ar susipažinti su įslaptinta informacija, žymima slaptumo žyma, atitinkančia aukščiausią ADA sistemoje ar tinkle apdorojamos įslaptintos informacijos slaptumo žymą;

18.3. diegiant programinę įrangą, ADA sistemos ar tinklo valdytojo/tvarkytojo gauta kompiuterinė laikmena, kurioje įrašyta programinė įranga, skirta naudoti ADA sistemoje ar tinkle, prieš pradedant ją naudoti turi būti patikrinta atskirame kompiuteryje, skirtame kenksmingos programinės įrangos paieškai;

18.4. visa ADA sistemoje ar tinkle naudojama programinė įranga įtraukiama į ADA sistemoje ar tinkle naudojamos kompiuterinės įrangos sąrašą, kuris, suderinus su SPT, tvirtinamas ADA sistemos ar tinklo valdytojo.

19. ADA sistemose ir tinkluose saugoti, apdoroti ar jais perduoti įslaptintą informaciją leidžiama tik teisės aktų nustatyta tvarka gavus leidimą automatizuotai apdoroti įslaptintą informaciją (toliau – leidimas). Jo gavimui ADA sistemos ar tinklo valdytojas/tvarkytojas rengia akreditavimo dokumentus, kurių apimtį ir turinio gaires nustato Dokumentų, reikalingų leidimui automatizuotai apdoroti įslaptintą informaciją išduoti, rengimo ir leidimų automatizuotai apdoroti įslaptintą informaciją išdavimo taisyklės, patvirtintos Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2010 m. lapkričio 29 d. įsakymu Nr. 5V-138 (Žin., 2010, Nr. 142-7328) .

20. Atliekant įrengtos ADA sistemos ar tinklo veikimo patikrinimą, tikrinamas jos funkcionavimas ir įdiegtų saugos užtikrinimo priemonių veikimas. Nustačius saugos užtikrinimo trūkumus, analizuojamos priežastys, šalinami trūkumai, taikomos papildomos saugos užtikrinimo priemonės. Patikrinimo metu gauti rezultatai ir taikytos korekcinės priemonės protokoluojamos, dokumentų kopijos pridedamos prie akreditavimo dokumento – Specifinių saugumo reikalavimų aprašo.

21. Parengti akreditavimo dokumentai teikiami SPT, kurios funkcijas atliekanti institucija pateiktų dokumentų analizės ir ADA sistemos ar tinklo inspekcijų pagrindu priima sprendimą dėl leidimo išdavimo.

V. ADA SISTEMŲ IR TINKLŲ NAUDOJIMAS IR MODERNIZAVIMAS

22. ADA sistemų ir tinklų naudojimosi ir modernizavimo stadijos metu užtikrinamas reikiamo saugos lygio palaikymas: ADA sistema ar tinklu naudojamasi pagal teisės aktų nustatytus reikalavimus, siekiant išlaikyti priimtiną saugos lygį, naudojamos akreditavimo dokumentuose apibrėžtos saugos užtikrinimo priemonės ar diegiamos papildomos, vertinamos naujai iškylančios grėsmės, kurios minimizuojamos taikant papildomas saugos priemones.

23. ADA sistemos ar tinklo eksploatacijos metu turi būti užtikrinama ir vykdoma:

23.1. įslaptintos informacijos konfidencialumas, vientisumas ir pasiekiamumas užtikrinami, naudotojų identifikavimas ir autentifikavimas, naudojimosi ADA sistema ar tinklu kontrolė, auditas ir kontrolė, sąrankos valdymas, ADA sistemos ar tinklo techninis aptarnavimas, duomenų archyvavimas vykdomi vadovaujantis Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašo ir Telekomunikacijų apsaugos reikalavimų aprašo reikalavimais;

23.2. apdorojamos įslaptintos informacijos saugos užtikrinimas atliekamas vadovaujantis procedūromis, aprašytomis akreditavimo dokumente – Saugumo valdymo procedūrų apraše (toliau – SVPA);

23.3. įslaptintai informacijai kylančių grėsmių nustatymas laiku ir operatyvus reagavimas į jas; kompetentingų institucijų informavimas apie saugaus ADA sistemos ar tinklo darbo pažeidimus vykdomas vadovaujantis tvarka, apibrėžta SVPA;

23.4. periodiškai atnaujinama ADA sistemos ar tinko rizikos analizė, atliekami saugios veiklos patikrinimai;

23.5. vykdomas nuolatinis ADA sistemos ar tinklo naudotojų švietimas informacijos saugumo užtikrinimo klausimais, ADA sistemos ar tinklo naudotojai turi būti informuojami, kaip nustatyti nesankcionuotą veiklą ADA sistemoje ar tinkle, kaip atpažinti neįprastus įvykius ar nustatyti incidentus.

24. ADA sistemų ir tinklų modernizavimas:

24.1. prieš pradėdamas modernizavimą, ADA sistemos ar tinklo valdytojas/tvarkytojas turi įvertinti riziką ir grėsmes, atsirandančias atnaujinant ADA sistemą ar tinklą. Vertinimo išdavoje numatomos papildomos ar, atsisakius senųjų, planuojama naudoti naujas saugos užtikrinimo priemones;

24.2. rengiamas specifikacijos pakeitimo projektas, kuris derinamas Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, steigimo ir įteisinimo taisyklių nustatyta tvarka;

24.3. įsigyjamos reikiamos techninės ir programinės priemonės, jos diegiamos, tikrinamas jų veikimas, fiksuojami patikrinimo rezultatai;

24.4. atnaujinama ADA sistemos ar tinklo akreditavimo dokumentacija, kuri teikiama SPT. Jos funkcijas atliekanti institucija atlieka įdiegtų saugos užtikrinimo priemonių atitikties patikrinimą ir vertinimą bei išduoda leidimą.

VI. ADA SISTEMŲ IR TINKLŲ LIKVIDAVIMAS

25. Likviduojant ADA sistemas ir tinklus turi būti užtikrinamas juose apdorotos informacijos saugumas. Tuo tikslu:

25.1. planuojami ir skiriami likviduoti reikalingi ištekliai;

25.2. informacija ir ADA sistemos ar tinklo komponentai tvarkomi atsižvelgiant į būsimą jų naudojimą (archyvuojami, perkeliami į kitas ADA sistemas ar tinklus, sunaikinami, kt.);

25.3. dokumente fiksuojama paskutinė veikianti ADA sistemos ar tinklo konfigūracija;

25.4. parengiami pasirašyti visų šalinimo veiksmų atlikimo liudijimai.

25.3 ir 25.4 punktuose minimų dokumentų kopijos, kartu su kitais nustatytais dokumentais, teikiamos SPT, kuri gali patikrinti, ar likvidavimo veiksmai atlikti laikantis nustatytų saugos užtikrinimo reikalavimų.

26. Panaudojant likviduotose ADA sistemose ir tinkluose naudotą techninę įrangą, turi būti vadovaujamasi nuostatomis:

26.1. kriptografinė įranga, nereikalinga ar netinkama tolesniam naudojimui, likviduojama NKAT nustatyta tvarka;

26.2. kompiuteriai:

26.2.1. gali būti naudojami kitose ADA sistemose ir tinkluose, kuriuose apdorojamos įslaptintos informacijos aukščiausia slaptumo žyma atitinka likviduotoje apdorotos įslaptintos informacijos aukščiausią slaptumo žymą, prieš tai pašalinus visą jų standžiuose diskuose esančią informaciją Lietuvos Respublikos Vyriausybės nustatyta tvarka;

26.2.2. gali būti naudojami neįslaptintos informacijos/viešuose tinkluose, prieš tai pašalinus iš jų standžiuosius diskus ir atminties modulius (RAM, EPROM, kt.) ir pakeitus juos kitais, nenaudotais ADA sistemose ir tinkluose;

26.3. kompiuterinės laikmenos gali būti naudojamos kitose ADA sistemose ir tinkluose, kuriuose apdorojamos įslaptintos informacijos aukščiausia slaptumo žyma atitinka likviduotoje apdorotos įslaptintos informacijos aukščiausią slaptumo žymą, prieš tai pašalinus visą jose esančią informaciją Lietuvos Respublikos Vyriausybės nustatyta tvarka;

26.4. nereikalinga/netinkama tolesniam naudojimui kompiuterinė įranga ir kompiuterinės laikmenos naikinamos teisės aktų nustatyta tvarka.

VII. BAIGIAMOSIOS NUOSTATOS

27. Metodiką ir jos pakeitimus įsakymu tvirtina VRC direktorius.

_____