LIETUVOS RESPUBLIKOS SUSISIEKIMO MINISTRO

Į S A K Y M A S
DĖL LIETUVOS RESPUBLIKOS JŪRŲ LAIVŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2005 m. gruodžio 15 d. Nr. 3-568
Vilnius

Įgyvendindamas Lietuvos Respublikos Vyriausybės 2004 m. spalio 21 d. nutarimo Nr. 1318 „Dėl Lietuvos Respublikos jūrų laivų registro“ (Žin., 2004, Nr. 156-5703) 6.3 punkto reikalavimus:

1. T v i r t i n u Lietuvos Respublikos jūrų laivų registro duomenų saugos nuostatus (pridedama).

2. P a v e d u Lietuvos saugios laivybos administracijai iki š. m. gruodžio 30 d. patvirtinti Lietuvos Respublikos jūrų laivų registro informacinės sistemos nenumatytų situacijų valdymo planą ir darbo su Lietuvos Respublikos jūrų laivų registro informacinės sistemos duomenimis taisykles bei paskirti saugos įgaliotinį.

SUSISIEKIMO MINISTRAS PETRAS ČĖSNA

PATVIRTINTA
Lietuvos Respublikos susisiekimo ministro
2005 m. gruodžio 15 d. įsakymu Nr. 3-568

LIETUVOS RESPUBLIKOS JŪRŲ LAIVŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Šių nuostatų tikslas – sudaryti tinkamas sąlygas automatizuotu būdu saugoti ir tvarkyti duomenis apie jūrų transporto priemones bei jų savininkus (valdytojus).

2. Vadovaujančioji Lietuvos Respublikos jūrų laivų registro (toliau – registras) tvarkymo įstaiga – Lietuvos Respublikos susisiekimo ministerija, kuri yra ir registre tvarkomų asmens duomenų valdytoja.

3. Registro tvarkymo įstaiga – Lietuvos saugios laivybos administracija (toliau – Administracija), kuri yra ir registre tvarkomų asmens duomenų tvarkytoja. Administracija registro duomenis tvarko pagal Lietuvos Respublikos jūrų laivų registro nuostatų (toliau – registro nuostatai), patvirtintų Lietuvos Respublikos Vyriausybės 2004 m. spalio 21 d. nutarimu Nr. 1318 (Žin., 2004, Nr. 156-5703), reikalavimus. Ji taip pat vykdo registro duomenų bazės tvarkytojos funkcijas. Registro tvarkymo įstaigos būstinė – J. Janonio g. 24, Klaipėda.

4. Registro duomenų bazę sudaro kompiuterizuota registro informacinė sistema.

5. Šiuose nuostatuose vartojamos sąvokos atitinka sąvokas, vartojamas registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2004 m. spalio 21 d. nutarimu Nr. 1318 „Dėl Lietuvos Respublikos jūrų laivų registro“.

6. Valstybės įmonės Registrų centro tvarkomų registrų duomenų saugos nuostatai kartu su Nenumatytų situacijų valdymo planu ir detaliomis darbo su duomenimis taisyklėmis apibrėžia registrų informacinės sistemos saugumo politiką (toliau – saugumo politika).

II. REGISTRO DUOMENŲ BAZĖS APIBŪDINIMAS

7. Saugos nuostatai reglamentuoja duomenų tvarkymą automatizuotu būdu ir yra privalomi visiems Administracijos valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartį, kurie dirba su registru (toliau – naudotojas).

8. Registro informacinės sistemos apibūdinimas ir tvarkomų duomenų grupių aprašymas:

8.1. Registro informacinės sistemos paskirtis:

8.1.1. operatyviai ir kokybiškai rinkti, užrašyti, registruoti, kaupti, apdoroti, grupuoti, sisteminti, saugoti, naudoti ir teikti duomenis apie registro objektus, registro objektų savininkus (valdytojus), kurie tiesiogiai gaunami iš duomenų teikėjų (duomenis apie registro objektus, registro objektų savininkus (valdytojus), prieš įregistruojant, perregistruojant registro objektą, rašytine forma prašymuose užfiksuoja ir pateikia patys registro objekto savininkai (valdytojai) ar jų įgalioti asmenys);

8.1.2. įgyvendinti registro tvarkymo įstaigai pavestus uždavinius – sutikrinti automatizuotu būdu iš valstybės ir savivaldybės institucijų, valstybės registrų, kadastrų bei informacinių sistemų gautus duomenis su registro duomenimis;

8.1.3. automatizuotu būdu pagal poreikį teikti sukauptus registro duomenis:

8.1.3.1. susijusiems registrams ir informacinėms sistemoms;

8.1.3.2. valstybės ir savivaldybių institucijoms, kurios atlieka valstybės priskirtas funkcijas, susijusias su registro duomenimis, ar toms, kurioms registro duomenų reikia jų tiesioginėms funkcijoms atlikti įstatymų ir kitų teisės aktų nustatyta tvarka;

8.1.3.3. eismo įvykių tyrimo ir ekstremalių situacijų likvidavimo tarnyboms, kurioms būtina gauti registro duomenis;

8.1.3.4. mokslinių tyrimų įstaigoms, atliekančioms transporto tyrimus;

8.1.3.5. registro duomenų teikėjui, kurio duomenys įrašyti registre, – jo paties įregistruotus duomenis;

8.1.3.6. įstatymų ir kitų teisės aktų nustatyta tvarka – draudimo įmonėms, bankams, kitiems fiziniams ir juridiniams asmenims, turintiems teisę gauti registro duomenis, išskyrus tuos duomenis, kurių teikimą riboja Lietuvos Respublikos įstatymai, kiti teisės aktai ir šie Saugos nuostatai;

8.1.4. užtikrinti registro duomenų mainų saugumą pasirašant duomenų teikimo ir gavimo sutartis;

8.1.5. užtikrinti registro duomenų saugumą.

8.2. Registro informacinės sistemos tvarkomų duomenų grupės nurodytos registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2004 m. spalio 21 d. nutarimu Nr. 1318. Registro informacinėje sistemoje kaupiami šie duomenys:

8.2.1. duomenys apie registro objektų registraciją ir registro duomenų teikėjus;

8.2.2. duomenys apie registro duomenų teikėjams išduotus Lietuvos Respublikos jūrų laivų registravimo taisyklėse numatytus dokumentus;

8.2.3. bendrieji duomenys apie registro objektus:

8.2.3.1. duomenys apie jūrų laivus;

8.2.3.2. papildomi duomenys, jūrų laivą laikinai įregistruojant registre, jeigu sudaroma laivo nuomos be įgulos sutartis;

8.2.3.3. duomenys apie statomus jūrų laivus;

8.2.4. duomenys apie registro objekto savininkus (valdytojus);

8.2.5. duomenys, susiję su registruoti pateiktais dokumentais, daiktinėmis teisėmis į registro objektą ir suvaržymais.

9. Registro informacinę sistemą sudaro:

9.1. Duomenų registravimo posistemė. Ši posistemė skirta įvesti naujus ir redaguoti esamus registro informacinės sistemos duomenis. Posistemėje realizuoti šie elementai bei funkcijos:

9.1.1. unikalaus identifikacinio kodo naujai registruojamam laivui sukūrimas ir priskyrimas;

9.1.2. laivo suvaržymai;

9.1.3. kvitai rinkliavų įkainiams apmokėti;

9.1.4. pažyma Klaipėdos miesto apylinkės teismo hipotekos skyriui;

9.1.5. laivo duomenys;

9.1.6. laivo įgulos minimumo liudijimo registravimas;

9.1.7. leidimo plaukioti su Lietuvos valstybės vėliava registravimas;

9.1.8. leidimo plaukioti su Lietuvos valstybės vėliava galiojimo sustabdymas;

9.1.9. laivo registravimas;

9.1.10. laivo laikinas registravimas;

9.1.11. registracijos numerio suteikimas vykdant naują laivo registravimą;

9.1.12. laivo istorinių duomenų išsaugojimas.

9.2. Klasifikatorių duomenų tvarkymo posistemė. Ši posistemė skirta įvesti naujus ar keisti esamus klasifikatorių duomenis. Realizuoti tokie elementai:

9.2.1. bankai;

9.2.2. įkainiai;

9.2.3. šalys;

9.2.4. reikalavimai įgulai;

9.2.5. dokumento statusas;

9.2.6. pareigybės;

9.2.7. variklių tipai;

9.2.8. juridiniai asmenys;

9.2.9. plaukiojimo rajonai;

9.2.10. atsakingi asmenys;

9.2.11. uostai;

9.2.12. privatūs asmenys;

9.2.13. laivo paskirtys;

9.2.14. laivų paskirčių grupės.

9.3. Sisteminių duomenų tvarkymo posistemė. Ši posistemė skirta tvarkyti sisteminius parametrus bei kitus sisteminius duomenis. Posistemėje realizuoti šie elementai:

9.3.1. veiksmų sąrašas;

9.3.2. klaidų sąrašas;

9.3.3. objektų sąrašas;

9.3.4. kalbų sąrašas;

9.3.5. sistemos meniu;

9.3.6. objektų tipai;

9.3.7. leidimų sąrašas.

9.4. Naudotojų teisių posistemė. Visi registro informacinės sistemos naudotojai turi jiems priskirtas naudotojų teises, pagal kurias yra kontroliuojamos funkcijos, kurias jie gali atlikti. Ši posistemė skirta tvarkyti naudotojų teisių sąrašą, priskirti ar atimti naudotojų teises naujai sukurtiems ar egzistuojantiems registro naudotojams. Posistemėje realizuoti šie elementai:

9.4.1. naudotojų teisių sąrašas;

9.4.2. veiksmų sąrašas, priskirtas tam tikrai naudotojų teisei;

9.4.3. objektų sąrašas, priskirtas tam tikrai naudotojų teisei;

9.4.4. leidimai objektams, priskirtiems tam tikrai naudotojų teisei;

9.4.5. naudotojų teisių sąrašas, priskirtas tam tikram naudotojui.

9.5. Duomenų mainų posistemė. Ši posistemė vykdo:

9.5.1. duomenų gavimą iš susijusių registrų ir informacinių sistemų bei duomenų teikėjų;

9.5.2. duomenų teikimą susijusiems registrams, informacinėms sistemoms ir duomenų naudotojams.

9.6. Ataskaitų formavimo posistemė. Ši posistemė skirta suformuoti ir spausdinti įvairius liudijimus, pažymas, apskaitos žurnalus bei statistines ataskaitas. Realizuotos šios funkcijos:

9.6.1. spausdinti leidimą laikinai plaukioti su Lietuvos valstybės vėliava;

9.6.2. spausdinti laivo išregistravimo iš registro liudijimą apie laikinai įregistruoto laivo išregistravimą;

9.6.3. spausdinti laivo įgulos minimumo liudijimą;

9.6.4. spausdinti leidimą laivui plaukioti su Lietuvos valstybės vėliava;

9.6.5. spausdinti leidimo plaukioti su Lietuvos valstybės vėliava galiojimo sustabdymo liudijimą;

9.6.6. spausdinti laivo išregistravimo iš registro liudijimą;

9.6.7. spausdinti laivo įregistravimo registre liudijimą;

9.6.8. spausdinti laivo laikino įregistravimo registre *(bareboat charter)* liudijimą;

9.6.9. spausdinti statistinę ataskaitą apie atitinkamu laikotarpiu registre įregistruotus laivus;

9.6.10. spausdinti laivo išregistravimo iš registro liudijimo išdavimo registracijos žurnalą;

9.6.11. spausdinti laivo įregistravimo registre liudijimo išdavimo registracijos žurnalą;

9.6.12. spausdinti leidimo laivui plaukioti su Lietuvos valstybės vėliava išdavimo registracijos žurnalą;

9.6.13. spausdinti leidimo plaukioti su Lietuvos valstybės vėliava galiojimo sustabdymo liudijimo išdavimo registracijos žurnalą;

9.6.14. spausdinti laivo įgulos minimumo liudijimo išdavimo registracijos žurnalą;

9.6.15. spausdinti vykdomų paslaugų valstybės rinkliavų apskaitos žurnalą.

9.7. Duomenų importavimo posistemė. Ši posistemė vykdo duomenų, gautų iš susijusių registrų, informacinių sistemų ar duomenų naudotojų, pateiktų tam tikru formatu, importavimą į sistemą.

9.8. Duomenų eksportavimo posistemė. Ši posistemė vykdo duomenų eksportavimą iš sistemos nurodytu formatu susijusiems registrams, informacinėms sistemoms ar duomenų

naudotojams.

10. Saugų registro informacinės sistemos duomenų tvarkymą reglamentuoja:

10.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2000, Nr. 64-1924; 2003, Nr. 15-597);

10.2. Bendrieji duomenų saugos reikalavimai, patvirtinti Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“ (Žin., 1997, Nr. 83-2075; 2003, Nr. 2-45) (toliau – Bendrieji duomenų saugos reikalavimai);

10.3. Lietuvos standartas LST ISO/IEC 17799:2005, Lietuvos ir tarptautiniai grupės „Informacijos technologija. Saugumo technika“ standartai, reglamentuojantys saugų duomenų tvarkymą;

10.4. teisės aktai, reglamentuojantys duomenų tvarkymo teisėtumą, registro tvarkymo įstaigos veiklą bei duomenų saugos valdymą.

III. DUOMENŲ SAUGOS ORGANIZAVIMAS IR NENUMATYTŲ SITUACIJŲ VALDYMAS

11. Už duomenų tvarkymo teisėtumą ir duomenų saugumą atsako registro tvarkymo įstaiga.

12. Tvirtindama šiuos nuostatus ir kitus duomenų saugumo politiką reglamentuojančius teisės aktus, registro tvarkymo įstaiga skiria saugos įgaliotinį, kuris atsako už duomenų saugumo politikos įgyvendinimą ir kontrolę registro tvarkymo įstaigoje.

13. Saugos įgaliotinis teikia siūlymus dėl atskirų registro informacinės sistemos posistemių ar funkcijų administratorių (toliau – administratorius), kurie už paskirtų funkcijų vykdymą tiesiogiai atsiskaito saugos įgaliotiniui, paskyrimo.

14. Naudotojai, pastebėję saugumo politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti atitinkamos funkcijos administratoriui, kuris apie tai informuoja saugos įgaliotinį, o nesant administratoriaus – saugos įgaliotiniui.

15. Naudotojai privalo rūpintis registro informacinėje sistemoje kaupiamos informacijos saugumu bei turi būti susipažinę su šiais nuostatais, Nenumatytų situacijų valdymo planu, detaliomis darbo su duomenimis taisyklėmis ir kitais teisės aktais, nustatančiais saugumo politiką.

16. Saugos įgaliotinis prižiūri informacijos saugumo užtikrinimą registrų informacinėje sistemoje ir, siekdamas užtikrinti registrų informacinės sistemos ir joje tvarkomų duomenų saugumą, teikia pasiūlymus registrų informacinės sistemos tvarkytojo vadovui dėl saugumo politiką reglamentuojančių teisės aktų priėmimo, keitimo ar panaikinimo.

17. Administratorius privalo būti susipažinęs su saugumo politiką reglamentuojančiais dokumentais, turėti darbo su kompiuteriniais tinklais patirties, mokėti užtikrinti jų saugumą ir administruoti duomenų bazes.

18. Registro informacinės sistemos naudotojų veiksmus esant nenumatytai situacijai reglamentuoja Nenumatytų situacijų valdymo planas, kurį saugos įgaliotinis teikia tvirtinti registro tvarkymo įstaigos vadovui.

IV. DETALI DARBO TVARKA

19. Konkrečios registro informacinės sistemos duomenų tvarkymo ir saugumo procedūros išdėstytos detaliose saugaus darbo su duomenimis taisyklėse (toliau – taisyklės), kurias saugos įgaliotinis teikia tvirtinti registro informacinės sistemos tvarkymo įstaigos vadovui.

V. RIZIKOS VEIKSNIAI IR GRĖSMĖS

20. Numatomi šie vidiniai registro informacinės sistemos rizikos veiksniai:

20.1. Atsitiktinės techninės avarijos. Sugedus vienai sudedamajai daliai (energijos šaltiniui, vietiniam tinklui, duomenų teikimo įrenginiams), gali sutrikti visos registro informacinės sistemos darbas.

20.2. Purvo, dulkių bei magnetinių laukų įtaka. Kompiuterinė ir kita įranga turi būti nuolat valoma bei taisoma. Duomenų laikmenos turi būti laikomos atokiau nuo elektros ar radiacijos šaltinių, nes yra jautrios magnetiniams laukams.

20.3. Darbuotojų praradimas. Registro informacinės sistemos aptarnaujančių darbuotojų netekimas dėl ligų, nelaimingų atsitikimų, socialinių veiksnių įtakos.

21. Numatomi šie išoriniai registro informacinės sistemos rizikos veiksniai:

21.1. Gaisras. Galimos šios gaisrų priežastys: nesaugus degių medžiagų laikymas, neatsparių ugniai medžiagų naudojimas pastato konstrukciniams ir apdailos elementams, priešgaisrinių įtaisų trūkumas, nepakankama įrangos apsauga nuo ugnies, galimas pavojus žaibuojant ir kt.

21.2. Vandens poveikis. Vanduo į patalpas gali patekti dėl lietaus, gaisrų gesinimo.

21.3. Elektros energijos tiekimo sutrikimai, kurie gali atsirasti dėl gedimų tiekimo tinkle, dėl iš anksto nepaskelbtų linijų taisymo darbų, kabelių pažeidimų.

21.4. Techninės ir programinės įrangos gedimas.

22. Išorinių ir vidinių rizikos veiksnių grėsmės:

22.1. Ugnis gali išplisti po visą sistemą.

22.2. Vanduo gali sukelti didelį pavojų energijos tiekimo šaltiniams bei kompiuterinei įrangai.

22.3. Didelis duomenų pažeidimo laipsnis.

22.4. Galimas atsarginių kopijų sugadinimas, ypač jei jos saugomos viename pastate.

22.5. Visos kompiuterinės ir komunikacinės bazės sugadinimas.

22.6. Visiškas duomenų sugadinimas.

22.7. Kompiuterinės sistemos neveikimas.

23. Netyčinės subjektyvios aplinkybės ir priemonės joms išvengti yra šios:

23.1. Veiksniai, kylantys dėl darbo organizavimo nesklandumų.

23.2. Vidaus tvarkos taisyklių pažeidimai. Su Administracijos vidaus tvarkos taisyklėmis privalo susipažinti ir jų laikytis visi Administracijos darbuotojai.

23.3. Priežiūros trūkumas. Būtina nuolatinė registro informacinės sistemos priežiūra. Į saugomas patalpas Administracijos darbuotojams bei kitiems asmenims be leidimo patekti draudžiama.

23.4. Resursų kontrolė. Draudžiama programinės įrangos arba kitos įrangos naudojimo teises suteikti asmenims, kurie nėra naudotojai, saugos įgaliotinis ar administratorius, nes dėl to susilpnėja duomenų vientisumas, prieinamumas, konfidencialumas ir gali sutrikti informacinių sistemų darbas. Visi resursai (papildoma įranga, atsargos, priedai, dalys ir kt.) įsigyjami ir naudojami tik pagal paskirtį, suderinus su duomenų saugos įgaliotiniu. Kiekvienas resursas turi turėti visus reikiamus techninę charakteristiką apibūdinančius dokumentus.

24. Netyčinių subjektyvių aplinkybių pasekmės (duomenų pažeidimo poveikio laipsnis nedidelis, dažnai padariniai nepavojingi):

24.1. Informacija nusiųsta kitam adresatui.

24.2. Netikslūs duomenys.

24.3. Dalies informacijos dingimas.

24.4. Informacijos po paskutinio kopijavimo praradimas.

24.5. Operacinės sistemos sugadinimas.

25. Tyčinės subjektyvios aplinkybės:

25.1. Neteisėtas naudojimasis registro informacine sistema:

25.1.1. klaidingų duomenų įvedimas;

25.1.2. teisių ar operacinės sistemos programinės įrangos pakeitimai ir t. t.;

25.1.3. naudotojo teisių viršijimas, bandymas atspėti kitų naudotojų slaptažodžius;

25.1.4. piktnaudžiavimas dėl patogumo (neįslaptinama teisinga kodinės spynos kombinacija, trumpam pasitraukus iš darbo vietos įrenginiai nėra saugomi ir pan.).

25.2. Fizinis įsibrovimas į registro informacinę sistemą:

25.2.1. įsiterpimas į tinklus;

25.2.2. kenkėjiškos programinės įrangos naudojimas.

26. Tyčinių subjektyvių aplinkybių pasekmės:

26.1. Duomenų pažeidimo poveikio laipsnis labai didelis, padariniai rimti – duomenys netikslūs ar visiškai sugadinti.

26.2. Duomenų bazių įrašai suklastoti ir nekorektiški, sunku atrasti klaidas bei suklastotą informaciją.

26.3. Dėl vagystės prarasti ne tik duomenys iš duomenų bazių, bet ir visos atsarginės kopijos.

26.4. Neveikia kompiuterinės programos ir operacinė sistema.

26.5. Neveikia visa kompiuterinė sistema.

27. Rizikos veiksniai ir laipsniai nurodyti šių nuostatų priede. Pastebėjus rizikos veiksnius ar grėsmes, nedelsiant pranešama administratoriui, kuris apie tai informuoja saugos įgaliotinį, o nesant administratoriaus – saugos įgaliotiniui.

VI. PRIEMONĖS RIZIKOS VEIKSNIAMS IŠVENGTI

28. Taikomos šios priemonės rizikos veiksniams išvengti:

28.1. Infrastruktūrinės – patalpų įrengimas, oro vėsinimas ir kitos fizinės saugos priemonės.

28.2. Techninės ir programinės – kompiuterinė ir programinė įranga (duomenų laikmenų priežiūra).

28.3. Administracinės – darbo organizavimas, personalas, netikėtų situacijų valdymo planavimas.

28.4. Telekomunikacinės – techninė įranga (kabeliai).

29. Infrastruktūrinės priemonės registro informacinės sistemos apsaugai yra šios:

29.1. Patalpų įrengimas:

29.1.1. pasirenkant ir įvertinant vietą pastate atsižvelgiama į šalia esančio transporto keliamų vibracijų, eismo įvykių poveikį, arti esančius radijo siųstuvus, vandens telkinius, elektrines ar specialiąsias gamyklas, galimybę įsilaužėliams pasprukti nepastebėtiems;

29.1.2. specialiosios paskirties patalpos nežymimos lentelėmis, nurodančiomis jų paskirtį;

29.1.3. įrengiamos šarvuotos ir atsparios ugniai durys;

29.1.4. vykdoma įėjimo į patalpas kontrolė;

29.1.5. Administracijos darbuotojams išeinant iš patalpų, privaloma uždaryti langus, duris bei įjungti signalizaciją;

29.1.6. langai ir durys saugomi nuleidžiamomis žaliuzėmis, tarnybinės stoties patalpa – be langų;

29.1.7. nenaudojamų įėjimų rakinimas;

29.1.8. atsarginiai išėjimai saugomi nuo pašalinių asmenų;

29.1.9. valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartį, informuojami apie saugos priemones bei supažindinami su Vidaus tvarkos taisyklėmis;

29.1.10. įrengta patekimo į patalpas apsaugos ir kontrolės sistema;

29.1.11. tarnybinės stoties bei duomenų bazių kopijų saugyklos įrengimas patalpose su riboto priėjimo galimybe.

29.2. Priešgaisrinė apsauga:

29.2.1. priešgaisrinė signalizacija;

29.2.2. priešgaisrinės apsaugos tarnybos nustatytų normų laikymasis;

29.2.3. mažų ugnies židinių gesinimas rankiniais gesintuvais, nuolatinė gesintuvų patikra;

29.2.4. apsauginių perskyrų, specialiai apsaugančių kabelius, kokybės patikra;

29.2.5. personalo informavimas apie priemones, kurių reikia imtis kilus gaisrui.

30. Techninės ir programinės priemonės registro informacinės sistemos apsaugai:

30.1. Techninės įrangos išdėstymas:

30.1.1. draudžiama statyti techninę įrangą šalia šildytuvų, prieš tiesioginius saulės spindulius, taip pat šalia langų, durų, pašaliniams asmenims matomoje vietoje;

30.1.2. įrenginiai, saugantys duomenis (t. y. tarnybinės stoties administravimo įranga, spausdintuvai, faksas, kopijavimo įranga), laikomi riboto priėjimo patalpose.

30.2. Tarnybinės stoties apsauga:

30.2.1. slaptažodžiai, leidžiantys dirbti su tarnybine stotimi, žinomi tik administratoriui;

30.2.2. tarnybinės stoties administratorius yra atsakingas už informacijos tarnybinėje stotyje konfidencialumą, vientisumą ir prieinamumą;

30.2.3. įžeminimas;

30.2.4. nepertraukiamo elektros maitinimo šaltinio, automatiškai po tam tikro laiko išjungiančio kompiuterius, prijungimas prie tarnybinės stoties;

30.2.5. nuolatinis tarnybinės stoties administravimas;

30.2.6. nuolatinis duomenų kopijavimas ir kopijų saugojimas pagal nustatytas tarnybinės stoties informacijos kopijavimo ir kopijų saugojimo taisykles;

30.2.7. duomenų kopijos saugomos nedegiose metalinėse spintose atskirose patalpose;

30.2.8. užtikrinamas duomenų atkūrimas įvykus techniniams gedimams duomenų įvedimo metu.

30.3. Vietiniai tinklai ir jų priežiūra:

30.3.1. atsižvelgiant į tiesimo vietą, aplinkos sąlygas, galimą mechaninį poveikį, specialią dangą, apsaugančią nuo ugnies ir stiprių elektrinių laukų, numatytos jungčių į elektros tinklą vietos. Tiesiamas kabelis iš karto turi turėti papildomo pajėgumo arba ateityje šalia jo gali būti nutiestas antrasis, iš anksto tam palikus vietos;

30.3.2. elektros energijos bei telekomunikacijų vidinių tinklų jungimas tiesiogiai prie išorinių linijų;

30.3.3. išorinė apsauga nuo žaibo sukeltų perkrovų;

30.3.4. elektros energijos palaikymo šaltinis, leidžiantis sėkmingai baigti darbą ir prasidėjus ilgiems elektros tiekimo nesklandumams;

30.3.5. pagrindiniai komutaciniai mazgai išdėstyti atskirose patalpose su riboto priėjimo galimybe;

30.3.6. slaptažodžių sistemos, pagal kurią nustatomos Naudotojo teisės tinkle, naudojimas prisijungimui prie vietinio tinklo. Slaptažodžiai reguliariai keičiami. Naudotojas, laiku nepakeitęs slaptažodžio, netenka galimybės prisijungti prie vietinio tinklo;

30.3.7. duomenų naudotojai vidinio tinklo duomenis pasiekia tik per užkardą (angl. – *firewall);*

30.3.8. nuotolinės vidinio tinklo administravimo sistemos naudojimas, leidžiantis diagnozuoti gedimus tinkle ir stebėti sistemos apkrovimą, kompiuterių darbą;

30.3.9. vietinio tinklo kabeliai tiesiami atskirai nuo elektros srovės kabelių.

31. Administracinės priemonės registro informacinės sistemos apsaugai:

31.1. Darbo organizavimas:

31.1.1. duomenų ir duomenų laikmenų saugojimas;

31.1.2. duomenų bazės archyvų priežiūra;

31.1.3. saugus duomenų laikmenų transportavimas;

31.1.4. saugus duomenų teikimas duomenų naudotojams;

31.1.5. saugus apsikeitimas duomenimis tarp naudotojų;

31.1.6. slaptažodžių naudojimas. Slaptažodžius suteikia tik tarnybinių stočių ir duomenų administratoriai. Slaptažodžių keitimą užtikrina naudojamos programinės priemonės;

31.1.7. naudotojų ir administratoriaus teisių paskirstymas;

31.1.8. resursų (papildoma įranga, atsargos, priedai, dalys ir kt.) kontrolė;

31.1.9. techninės ir programinės įrangos įsigijimas bei priežiūra;

31.1.10. registro informacinės sistemos taisymo ir testavimo darbai;

31.1.11. apsauga nuo kenkėjiškų kompiuterinių programų;

31.1.12. duomenų bazės auditas ir testavimas;

31.1.13. registro informacinės sistemos naudotojų instrukcijų sukūrimas;

31.1.14. konfigūracijos aprašymo atnaujinimas, keičiantis registro informacinės sistemos elementams;

31.1.15. Administratoriaus, atsakingo už registro informacinės sistemos kasdienį darbą, paskyrimas;

31.1.16. papildomų registro informacinės sistemos administratorių, atsakingų už skirtingas funkcijas ir galinčių, esant reikalui, pakeisti administratorių, paskyrimas;

31.1.17. administratoriaus funkcijos: nuolatinis sistemos darbo tikrinimas, reikiamų pakeitimų atlikimas, Registro informacinės sistemos pakeitimų dokumentų tvarkymas.

32. Darbo vietos priežiūra:

32.1. Darbo vieta turi būti tvarkinga ir turi atitikti Priešgaisrinės saugos taisyklių keliamus reikalavimus.

32.2. Nuolatinė saugos priemonių patikra.

32.3. Draudimas rūkyti patalpose, kuriose yra kompiuterinė technika.

33. Teisių suteikimas ir priežiūra:

33.1. Apibrėžtos teisės suteikiamos konkrečiam Administracijos valstybės tarnautojui ar darbuotojui, dirbančiam pagal darbo sutartį, pagal užimamas pareigas, pasirašytinai supažindinant naudotojus su šiais nuostatais ir kitais dokumentais, sudarančiais duomenų saugos politiką.

33.2. Naudojimosi suteiktomis teisėmis patikrinimas.

33.3. Tinklo administravimo, sisteminių teisių paskirstymas, ribojant naudotojo teises.

33.4. Darbo su informacine sistema teises naudotojams suteikia administratorius. Informacinės sistemos naudotojams teisės suteikiamos atsižvelgiant į vykdomas funkcijas.

33.5. Reguliarus ir profilaktinis naudotojų veiksmų ir įsiregistravimo ataskaitų tikrinimas.

33.6. Identifikavimo sistemos, kontroliuojančios naudotojų įsiregistravimą, diegimas.

34. Slaptažodžių vartojimas:

34.1. Slaptažodžiai negali būti reikšminiai žodžiai (susieti su šeimos narių vardais, gimimo datomis ar pačiu asmeniu), turi būti sudaryti iš ne mažiau kaip šešių simbolių (slaptažodžiai sudaromi iš didžiųjų ir mažųjų raidžių, skaičių ir kitų simbolių).

34.2. Gamintojo slaptažodžiai nedelsiant keičiami individualiais.

34.3. Slaptažodžiai negali būti užprogramuoti specialiais klavišais.

34.4. Slaptažodį turi žinoti tik naudotojas. Užrašytas slaptažodis laikomas užklijuotuose vokuose ir naudotinas tik nenumatytais atvejais.

34.5. Galimybės pakeisti individualų slaptažodį kiekvienam naudotojui suteikimas.

34.6. Vienkartinio slaptažodžio suteikimas, įregistruojant naujus naudotojus.

34.7. Užkoduotų slaptažodžių siuntimas tinklu.

35. Raktų naudojimas:

35.1. Užtikrinamas saugus atsarginių raktų laikymas.

35.2. Atleidžiant Administracijos darbuotoją ar pasikeitus jo pareigoms, raktai grąžinami.

36. Duomenų laikmenų apsauga:

36.1. Duomenų laikmenos registruojamos, saugiai laikomos, o siunčiant pašalinami nereikalingi duomenys.

36.2. Numatomos priemonės, apsaugančios duomenis nuo pašalinių asmenų.

36.3. Nustatoma duomenų laikmenų saugojimo vieta.

37. Programinės įrangos apsauga:

37.1. Programinę įrangą diegia tik administratorius arba jo įgaliotas asmuo. Valstybės tarnautojui arba darbuotojui, dirbančiam pagal darbo sutartį, savavališkai draudžiama diegti bet kokią programinę įrangą.

37.2. Įsigyjant naują programinę įrangą atliekami rinkos tyrimai.

37.3. Tikrinami programinės įrangos tiekėjų registravimo pažymėjimai ir siūlomos įrangos sertifikatai.

37.4. Įrangos testavimas. Atlikus programinės įrangos testavimą, nustatoma pageidaujama konfigūracija, kuri nulemia darbo patogumą, mažą klaidų skaičių ir saugumą.

37.5. Padarius atsargines originalių duomenų kopijas, įdiegiama programinė įranga.

37.6. Bylų, susijusių su ištrinama programine įranga, pašalinimas.

38. Tinklo saugos strategija:

38.1. Išorinė linijų, išskirstymo jungčių būklės patikra.

38.2. Saugus ryšio skirstytojų dokumentų, nurodančių jų paskirtį, laikymas. Naudojamų, nebenaudojamų jungčių žymėjimas neįvardijant specifinių funkcijų. Papildomos informacijos pateikimas dokumentuose.

38.3. Duomenų gavėjo vidinio tinklo duomenų pasiekimas tik per užkardą (angl. – *firewall).* Užkardos konfigūracijos: filtrų naudojimas (informacijos filtravimas kompiuteryje ir gaunamų dokumentų atmetimas arba priėmimas pagal taisykles), nuolatinis užkardos veikimo tikrinimas, siekiant nustatyti galimas silpnąsias puses.

39. Lygiateisių mazgų tinklo saugos strategija:

39.1. Lygiateisių mazgų tinklo struktūros nustatymas.

39.2. Atsakomybės paskirstymas.

39.3. Teisių suteikimo apribojimas.

39.4. Standartinių naudotojų vardų sukūrimas, teisių į katalogus ir spausdintuvus suteikimas, slaptažodžių valdymas, naudotojų pareigų nustatymas, mokymų pravedimas.

40. Personalo funkcijos:

40.1. Bendrų instruktažų organizavimas:

40.1.1. priimant naujus valstybės tarnautojus ir darbuotojus, dirbančius pagal darbo sutartį, pradedant naudoti naujas programas ar esant dideliems registro informacinės sistemos pakitimams;

40.1.2. supažindinant naudotojus su apsauga, aptariant šiuos klausimus:

40.1.2.1. apsaugos supratimą;

40.1.2.2. priemones, susijusias su naudotojais;

40.1.2.3. priemones, siejamas su technine ir programine įranga;

40.1.2.4. veiksmus, aptikus kenkėjišką kompiuterinę programą;

40.1.2.5. naudojimąsi slaptažodžiais;

40.1.2.6. duomenų saugojimą;

40.1.2.7. asmens duomenų priežiūrą;

40.1.2.8. priemones pavojaus atveju;

40.1.2.9. priemones, neleidžiančias atskleisti viešai neskelbtinos arba slaptos informacijos;

40.1.2.10. apsaugos priemonių naudojimą.

41. Reikiamų darbo vietų užpildymas:

41.1. Pavaduojančio naudotojo numatymas, naudotojui planuotai ar neplanuotai neatvykus į darbą.

41.2. Prieš atleidžiant naudotoją, jo vietą užimsiančio asmens informavimas.

41.3. Registro tvarkymo įstaigos vidaus tvarkos taisyklių, nustatančių naudotojo veiksmus išeinant iš darbo, parengimas.

41.4. Naujų naudotojų supažindinimas su apsaugos sistema, priemonėmis ir jų naudojimu.

42. Administratorius:

42.1. Turi teisę naudotis visomis registro informacinės sistemos galimybėmis.

42.2. Savarankiškai atlieka kasdieninius registro informacinės sistemos valdymo darbus, aptinka ir panaikina smulkius gedimus, rūpinasi duomenų saugojimu.

43. Tinkamas tinklų saugos funkcijų naudojimas. Kiekvienas naudotojas rūpinasi savo tvarkomų, teikiamų ir naudojamų duomenų apsauga.

44. Kenkėjiška programinė įranga:

44.1. Kovai su kenkėjiška programine įranga numatomos šios prevencinės priemonės:

44.1.1. kenkėjiškos programinės įrangos aptikimo ir likvidavimo sistemos lokalizavimas elektroninio pašto tarnybinėje stotyje;

44.1.2. interneto kanalu plintančios kenkėjiškos programinės įrangos aptikimo ir likvidavimo sistemos diegimas;

44.1.3. centralizuotas kenkėjiškos programinės įrangos aptikimo ir likvidavimo sistemos valdymas darbo vietose, reguliarus automatinis kompiuterinių darbo vietų tikrinimas.

44.2. Kenkėjiškos programinės įrangos padarinių likvidavimo priemonės:

44.2.1. atsarginis diskelis su operacine sistema, iš kurio, kilus nesklandumams, pradedamas darbas;

44.2.2. redaktoriaus naudojimas diskelyje (atsarginių kopijų kūrimo programa);

44.2.3. panaikinus kenkėjišką programinę įrangą, pažeistos bylos atkuriamos iš atsarginių kopijų archyvo.

45. Duomenų saugumo užtikrinimas. Išsaugotų duomenų dokumentų tvarkymas:

45.1. Įrašymo data.

45.2. Struktūra.

45.3. Saugojimo įrenginiai.

45.4. Programinė įranga.

45.5. Naudoti parametrai.

45.6. Laikmenos, kuriose laikomi operaciniai ir išsaugoti duomenys.

45.7. Duomenų saugos tvarka duomenų kopijavimo, visiško, diferencinio ir duomenų perrašymo iš dalies atvejais.

46. Tarnybinės stoties operacinės sistemos „Windows Server 2003“ priežiūros vykdymas:

46.1. Mažinant tarnybinės stoties apkrovimą, įrašant duomenis į kelis kietuosius diskus.

46.2. Naudojant paleidžiamąjį diskelį.

47. Darbo stočių operacinės sistemos „Windows XP“ priežiūrą sudaro:

47.1. Paleidžiamojo diskelio naudojimas.

47.2. Saugumo užtikrinimas siekiant sumažinti tarnybinės stoties apkrovas, duomenų įrašymas į kelis kietuosius diskus, įmontuotus tarnybinėje stotyje, šiam tikslui naudojant specialią atsarginių kopijų kūrimo programą.

48. Visi saugojimo parametrų nustatymai įvedami mechaniškai, pažymint atliktus pakeitimus arba naudojant specialią programą (galvučių, sektorių ir cilindrų skaičius kietajame diske), registruojančią duomenis.

49. Nešiojamųjų kompiuterių apsaugai naudojamas įsiregistravimo slaptažodis, energijos taupymo režimas ir energijos rezervų stebėjimas, duomenų kodavimo programos. Slapti duomenys negali būti paliekami kietajame diske.

50. Programinės įrangos apsauga organizuojama:

50.1. Vykdant nuolatinę registro informacinės sistemos priežiūrą. Registro informacinės sistemos priežiūrą atlieka administratorius. Paprastiems darbams atlikti administratorius privalo turėti ir naudoti paprasto naudotojo įsiregistravimo vardą bei slaptažodį.

50.2. Atliekant saugius įsiregistravimus.

50.3. Įsiregistravimo programa naudojama ribojant nesėkmingų bandymų skaičių iki 3 (trijų) nesėkmingų bandymų. Apie įvykusį incidentą administratorius praneša saugos įgaliotiniui.

50.4. Blokuojant, ištrinant ilgą laiką nenaudojamus įsiregistravimus.

50.5. Įsiregistravimo vardą sukuriant ribotam laikui.

50.6. Įsijungus į registro informacinę sistemą arba prieš įsijungiant, tikrinant informacijos apsaugai naudojamus slaptažodžius. Slaptažodžiu turi būti apsaugotas programinės įrangos naudojimas, automatiškas darbo duomenų kopijavimas, duomenų kodavimas.

50.7. Identifikuojant administratorių ir naudotojus.

51. Duomenų laikmenų priežiūrą sudaro:

51.1. Nereikalingos informacijos ištrynimas prieš duomenų kopijavimą.

51.2. Kenkėjiškų kompiuterinių programų aptikimo, duomenų tikrinimo ir kodavimo programų prieš ir po duomenų persiuntimo naudojimas.

52. Telekomunikacijos priemonės:

52.1. Tarnybinės stoties administravimas.

52.2. Teisių naudotis tarnybinės stoties kietuoju disku ribojimas.

52.3. Įvedimo įrenginių blokavimas.

53. Kabelių tiesimas:

53.1. Pasirenkant kabelio tipą atsižvelgiama į atstumą bei duomenų persiuntimo spartą.

53.2. Techniniuose dokumentuose turi būti išsamiai aprašomi šie duomenys:

53.2.1. kabelio tipas;

53.2.2. skirstytuvų vietos;

53.2.3. tikslus kabelių išdėstymas patalpose;

53.2.4. linijų išmatavimai;

53.2.5. naudotojai;

53.2.6. jungties taškų techniniai rodikliai;

53.2.7. rizikos veiksniai.

53.3. Užtikrinamas prieinamumas tik naudotojams bei apsauga nuo tiesioginių mechaninių pažeidimų.

54. Tinklo valdymas ir plėtra vykdoma pagal sudarytą kompiuterių tinklo aparatinės ir programinės įrangos įrengimo planą, kuriame:

54.1. Įvardijama kiekvienos tarnybinės stoties ir darbo vietos kompiuterio paskirtis, juose saugomos informacijos svarba.

54.2. Nurodomi aparatinės ir programinės įrangos reikalavimai, keliami informaciją apdorojančioms, saugančioms ir perduodančioms tarnybinėms stotims ir darbo vietų kompiuteriams.

54.3. Įvardijamos ir aprašomos tinklo paslaugos. Aprašant tinklo paslaugas, nurodoma loginė tinklo paslaugų teikimo schema. Išskiriama, ar tam tikras kompiuteris atliks tarnybinės ar darbo stoties funkcijas.

54.4. Remiantis įrengimo plane nurodytais aparatinės ir programinės įrangos reikalavimais, įvardijama ir aprašoma aparatinė ir programinė įranga, kuri teiks tinklo paslaugas.

54.5. Įvardijami kompiuterių tinklo naudotojai ir jų grupės. Tinklo naudotojų suskirstymas į grupes priklauso nuo jų poreikio naudoti panašią informaciją ir atlikti panašius darbus.

54.6. Įvardijamos kiekvieno kompiuterių tinklo naudotojo ar jų grupės teisės. Kompiuterių tinklo naudotojų teisės apima informacijos skaitymą, įrašymą, pakeitimą, sukūrimą, ištrynimą, tinklo paslaugų įjungimą, išjungimą, programų įvykdymą, įdiegimą ir programinės įrangos parametrų keitimą.

55. Duomenys teikiami:

55.1. Naudojant tik naujausią elektroninio pašto programinės įrangos versiją.

55.2. Naudojant suderintas duomenų siuntimo (priėmimo) sistemas, duomenų kodavimą.

55.3. Naudotojui koduojant informaciją, nusprendžiant, ar naudotis pranešimų kodavimo ar skaitmeninio parašo apsauga.

56. Duomenų saugos priemonės turi garantuoti:

56.1. Duomenų apsaugą jos rinkimo, perdavimo ryšio kanalais, saugojimo, apdorojimo, teikimo ir naudojimo metu.

56.2. Duomenų apsaugą nuo nesankcionuoto ar neteisėto naudojimo, kaupimo, keitimo, perdavimo, skelbimo, sunaikinimo.

56.3. Duomenų apsaugą nuo:

56.3.1. pažeidimo dėl rizikos veiksnių;

56.3.2. netyčinių vidinių ir išorinių subjektyvių veiksnių (duomenų tvarkymo klaidos ir apsirikimai, bylų ištrynimas, fiziniai sutrikimai dėl elektros, duomenis gadinančių kenkėjiškų

kompiuterinių programų);

56.3.3. tyčinių subjektyvių veiksnių (neteisėtas įsibrovimas į sistemą iš išorės, piktybinis teisės aktų pažeidimas, vagystė ir kita);

56.3.4. nenugalimos jėgos (netikėti atsitiktiniai veiksniai – žaibas, gaisras, potvynis ar kitoks užliejimas, uraganas ir kt.).

VII. REGISTRO INFORMACINĖS SISTEMOS NAUDOTOJŲ ATSAKOMYBĖ

57. Registro informacinės sistemos naudotojai privalo rūpintis registro informacine sistema bei joje tvarkomų duomenų saugumu.

58. Tvarkyti registro informacinės sistemos duomenis gali tik registro informacinės sistemos naudotojai, susipažinę su saugos nuostatais ir kitais duomenų saugumo politiką reglamentuojančiais teisės aktais bei raštiškai sutikę laikytis šių teisės aktų reikalavimų.

59. Registro informacinės sistemos naudotojus su šiais nuostatais ir kitais saugumo politiką reglamentuojančiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą pasirašytinai supažindina saugos įgaliotinis.

60. Registro informacinės sistemos naudotojams turi būti nuolat rengiami mokymai duomenų saugos klausimais, įvairiais būdais primenama apie saugumo problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės naujai priimtiems darbuotojams ir pan.).

61. Registro informacinės sistemos naudotojai, pažeidę šių nuostatų ar kitų duomenų saugumo politiką reglamentuojančių teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka.

VIII. NUOSTATŲ ATNAUJINIMO TVARKA

62. Saugos įgaliotinis, siekdamas užtikrinti registro informacinės sistemos ir joje tvarkomų duomenų saugumą, teikia siūlymus registro informacinės sistemos tvarkytojo vadovui dėl saugos nuostatų keitimo ar kitų saugumo politiką reglamentuojančių teisės aktų priėmimo, keitimo ar panaikinimo.

IX. BAIGIAMOSIOS NUOSTATOS

63. Siekiant užtikrinti šiuose nuostatuose ir kituose registro duomenų saugumo politiką reglamentuojančiuose teisės aktuose nustatytų reikalavimų įgyvendinimo kontrolę, saugos įgaliotinis kasmet organizuoja auditą, kurio metu:

63.1. Įvertinama, ar nuostatai ir kiti saugumo politiką reglamentuojantys teisės aktai atitinka realią duomenų saugos situaciją.

63.2. Inventorizuojama registro informacinės sistemos tvarkytojo techninė ir programinė įranga.

63.3. Tikrinama ne mažiau kaip 10% registro informacinės sistemos naudotojų kompiuterinių darbo vietų ir visuose paslaugų kompiuteriuose įdiegtos programos bei jų konfigūracija.

63.4. Peržiūrima, ar registro informacinės sistemos naudotojams suteiktos teisės atitinka vykdomas funkcijas.

63.5. Įvertinamas pasiruošimas atstatyti registro informacinės sistemos veiklą esant nenumatytoms situacijoms.

64. Atlikus auditą rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato registro informacinės sistemos tvarkytojo vadovas.

SUDERINTA

Lietuvos Respublikos vidaus reikalų ministerijos
2005 m. gruodžio 2 d. raštu Nr. 1D-7984-(13)

Lietuvos Respublikos jūrų laivų registro
duomenų saugos nuostatų
priedas

RIZIKOS VEIKSNIAI IR LAIPSNIAI

Nr.	Rizikos veiksniai	Rizikos laipsniai
1.	Atsitiktiniai objektyvūs veiksniai:	
1.1.	Vidiniai rizikos veiksniai:	
1.1.1.	valstybės tarnautojų ir darbuotojų praradimas	Reikšmingas
1.1.2.	atsitiktinės techninės avarijos	Reikšmingas ar kritinis
1.1.3.	purvo, dulkių, magnetinių laukų poveikis	Reikšmingas
1.2.	Išoriniai rizikos veiksmai:	
1.2.1.	audros, gaisrai	Kritinis
1.2.2.	vandens poveikis	Reikšmingas
1.2.3.	elektros instaliacijos degimas	Reikšmingas ar kritinis
1.2.4.	elektros energijos tiekimo sutrikimas	Reikšmingas
2.	Netyčiniai subjektyvūs veiksmai:	
2.1.	Kylantys dėl darbo organizavimo nesklandumų:	
2.1.1.	vidaus tvarkos taisyklių pažeidimai	Reikšmingas
2.1.2.	priežiūros trūkumas	Reikšmingas
2.1.3.	resursų kontrolė	Reikšmingas
2.1.4.	netinkamai paskirstytos naudotojų teisės	Reikšmingas
2.1.5.	programinės įrangos testai	Kritinis
2.1.6.	netinkama duomenų laikmenų priežiūra	Kritinis
2.1.7.	nepakankamas linijų pajėgumas ir apsauga	Reikšmingas
2.1.8.	kompiuterių integravimas į tinklą	Kritinis
2.1.9.	„Windows“ apsaugos trūkumai	Reikšmingas
2.2.	Susiję su techninės ir programinės įrangos gedimu:	
2.2.1.	elektros energijos tiekimo gedimas	Kritinis
2.2.2.	kitų registro informacinės sistemos grandžių veiklos nesklandumai	Reikšmingas
2.2.3.	prisijungimas prie registro informacinės sistemos	Reikšmingas ar kritinis
2.2.4.	programinės įrangos klaidos	Reikšmingas
2.2.5.	duomenų netekimas	Kritinis
2.3.	Kylantys dėl valstybės tarnautojų ir darbuotojų klaidų:	
2.3.1.	netinkamas registro informacinės sistemos naudojimas	Reikšmingas
2.3.2.	įsijungimas į tinklą	Reikšmingas
2.3.3.	duomenų laikmenos	Reikšmingas ar kritinis
2.3.4.	klaidos transportuojant informaciją	Reikšmingas
2.3.5.	duomenų pažeidimas dėl naudotojo klaidos	Reikšmingas ar kritinis
2.3.6.	teisių suteikimas	Reikšmingas
2.3.7.	operacijos su slaptažodžiais	Reikšmingas
3.	Tyčiniai subjektyvūs veiksmai:	
3.1.	Neteisėtas naudojimasis registro informacine sistema	Kritinis
3.2.	Fizinis įsibrovimas į registro informacinę sistemą	Kritinis
3.3.	Įsiterpimas į tinklus	Kritinis
3.4.	Naudotojo teisių pažeidimas	Reikšmingas ar kritinis
3.5.	Duomenų atskleidimas	Reikšmingas ar kritinis
3.6.	Pranešimų tėkmės analizė	Reikšmingas
3.7.	Siuntimo aprašymo protokolai	Reikšmingas
3.8.	Kenkėjiškos kompiuterinės programos	Reikšmingas ar kritinis

_____