Suvestinė redakcija nuo 2012-07-06 iki 2016-05-12

Įsakymas paskelbtas: Žin. 2011, Nr. 25-1246, i. k. 1112214ISAK0000V-73

VALSTYBINĖS GELEŽINKELIO INSPEKCIJOS
PRIE SUSISIEKIMO MINISTERIJOS VIRŠININKO
Į S A K Y M A S

DĖL GELEŽINKELIŲ TRANSPORTO VALSTYBINĖS PRIEŽIŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2011 m. vasario 19 d. Nr. V-73
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 2007 m. balandžio 25 d. nutarimu Nr. 410 (Žin., 2007, Nr. 49-1891), 6.1 ir 8 punktais:

1. T v i r t i n u Geležinkelių transporto valstybinės priežiūros informacinės sistemos duomenų saugos nuostatus (pridedama);

2. S k i r i u Geležinkelių transporto valstybinės priežiūros informacinės sistemos saugos įgaliotiniu Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos (toliau – Inspekcija) Informacinių technologijų skyriaus vedėją Joną Masiulionį;

3. P a v e d u:

3.1. Geležinkelių transporto valstybinės priežiūros informacinės sistemos saugos įgaliotiniui per 3 mėnesius nuo šio įsakymo įsigaliojimo dienos parengti ir pateikti Inspekcijos viršininkui tvirtinti Saugaus elektroninės informacijos tvarkymo taisykles, Informacinės sistemos veiklos tęstinumo valdymo planą ir Informacinės sistemos naudotojų administravimo taisykles;

3.2. Inspekcijos viršininko pavaduotojui Robertui Šerėnui kontroliuoti šio įsakymo 3.1 punkto vykdymą.

VIRŠININKAS STASYS PIESLIKAS

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2011 m. vasario 2 d. raštu Nr. 1D-893

PATVIRTINTA
Valstybinės geležinkelio inspekcijos prie
Susisiekimo ministerijos viršininko
2011 m. vasario 19 d. įsakymu Nr. V-73

GELEŽINKELIŲ TRANSPORTO VALSTYBINĖS PRIEŽIŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Geležinkelių transporto valstybinės priežiūros informacinės sistemos (toliau – VGI IS) duomenų saugos nuostatų (toliau – Saugos nuostatai) tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją VGI IS.

2. Saugos nuostatuose vartojamos sąvokos atitinka Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, patvirtintuose Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2008, Nr. 85-3393), Saugos dokumentų turinio gairėse, patvirtintose Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070) ir kituose teisės aktuose bei Lietuvos standartuose LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006 vartojamas sąvokas.

3. Saugos nuostatų reikalavimai taikomi tvarkant VGI IS duomenis ir yra privalomi Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos (toliau – Inspekcija) valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis, turintiems bet kokias VGI IS naudotojų teises.

4. Saugos nuostatai reglamentuoja VGI IS saugos politiką, kurią įgyvendina šie Inspekcijos patvirtinti teisės aktai (toliau – Saugos dokumentai):

4.1. Saugaus elektroninės informacijos tvarkymo taisyklės;

4.2. Naudotojų administravimo taisyklės;

4.3. Veiklos tęstinumo valdymo planas.

5. VGI IS duomenų saugos tikslai yra šie:

5.1. sudaryti sąlygas automatiniu būdu saugiai tvarkyti elektroninę informaciją;

5.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo ar neteisėto jos tvarkymo.

6. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

6.1. elektroninės informacijos prieinamumo užtikrinimas;

6.2. elektroninės informacijos vientisumo užtikrinimas;

6.3. elektroninės informacijos konfidencialumo užtikrinimas;

6.4. veiklos tęstinumo užtikrinimas.

7. VGI IS valdytojas ir tvarkytojas yra Inspekcija, adresas: Pamėnkalnio g. 26, LT-01114, Vilnius.

8. Už VGI IS elektroninės informacijos tvarkymo teisėtumą, patikimumą, elektroninės informacijos teikimo VGI IS elektroninės informacijos gavėjams teisėtumą, patikimumą ir elektroninės informacijos saugą atsako VGI IS valdytojas.

9. VGI IS valdytojo ir tvarkytojo funkcijos ir atsakomybė:

9.1. leidžia įsakymus, susijusius su VGI IS saugos užtikrinimu;

9.2. atsako už tinkamą šiuose nuostatuose nustatytų funkcijų vykdymą;

9.3. skiria VGI IS saugos įgaliotinį (toliau – Saugos įgaliotinis).

10. Saugos įgaliotinis, įgyvendindamas VGI IS Saugos politiką, atlieka šias funkcijas:

10.1. registruoja elektroninės informacijos saugos incidentus VGI IS elektroninės informacijos saugos incidentų registravimo žurnale, pateiktame Geležinkelių transporto valstybinės priežiūros informacinės sistemos veiklos tęstinumo valdymo plano priede Nr. 2;

10.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių VGI IS, tyrimą;

10.3. teikia VGI IS administratoriui ir sisteminiam administratoriui su VGI IS elektroninės informacijos saugos užtikrinimu susijusius privalomus vykdyti nurodymus ir pavedimus;

10.4. kasmet organizuoja VGI IS rizikos vertinimą, VGI IS rizikos vertinimo rezultatai aprašomi rengiant VGI IS rizikos įvertinimo ataskaitą;

10.5. prireikus organizuoja neeilinį VGI IS rizikos vertinimą;

10.6. atlieka VGI IS informacijos saugos atitikties vertinimą;

10.7. periodiškai organizuoja VGI IS naudotojų mokymus informacijos saugos klausimais;

10.8. teikia Inspekcijos viršininkui pasiūlymus dėl:

10.8.1. VGI IS administratoriaus ir sisteminio administratoriaus paskyrimo;

10.8.2. Saugos nuostatų ir Saugos dokumentų keitimo;

10.9. atlieka kitas Inspekcijos viršininko pavestas užduotis ir Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, jam priskirtas funkcijas.

11. VGI IS administratorius, vykdantis VGI IS priežiūrą, atlieka šias funkcijas:

11.1. vertina VGI IS naudotojų pasirengimą dirbti su VGI IS;

11.2. atlieka VGI IS naudotojams suteiktų teisių ir priskirtų funkcijų atitikties vertinimą;

11.3. rengia ir tikrina VGI IS sudarančių komponentų sąranką;

11.4. informuoja Saugos įgaliotinį apie Saugos politikos pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

11.5. vykdo Saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu.

12. VGI IS sisteminis administratorius, vykdantis VGI IS priežiūrą, atlieka šias funkcijas:

12.1. nustato VGI IS pažeidžiamas vietas ir informuoja apie jas Saugos įgaliotinį;

12.2. atlieka VGI IS techninės ir programinės įrangos priežiūrą;

12.3. atlieka VGI IS duomenų atsarginių kopijų darymą;

12.4. informuoja Saugos įgaliotinį apie Saugos politikos pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

12.5. vykdo Saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu.

13. Teisės aktai, kuriais vadovaujamasi tvarkant VGI IS elektroninę informaciją ir užtikrinant jos saugumą:

13.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804);

Punkto pakeitimai:

Nr. V-419, 2012-07-02, Žin., 2012, Nr. 79-4137 (2012-07-05), i. k. 1122214ISAK000V-419

13.2. Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai;

Punkto pakeitimai:

Nr. V-419, 2012-07-02, Žin., 2012, Nr. 79-4137 (2012-07-05), i. k. 1122214ISAK000V-419

13.3. Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160);

13.4. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866);

13.5. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo

priemonėms, patvirtinti Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71 (Žin., 2008, Nr. 135-5298);

13.6. Geležinkelių transporto valstybinės priežiūros informacinės sistemos nuostatai, patvirtinti Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos viršininko 2011 m. vasario 17 d. įsakymu Nr. V-57 (Žin., 2011, Nr. 25-1245);

Papildyta punktu:
Nr. V-419, 2012-07-02, Žin., 2012, Nr. 79-4137 (2012-07-05), i. k. 1122214ISAK000V-419

13.7. VGIS IS saugos politiką įgyvendinantys dokumentai:

13.7.1. Geležinkelių transporto valstybinės priežiūros informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės, patvirtintos Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos viršininko 2011 m. liepos 18 d. įsakymu Nr. V-439;

13.7.2. Geležinkelių transporto valstybinės priežiūros informacinės sistemos veiklos tęstinumo valdymo planas, patvirtintas Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos viršininko 2011 m. liepos 18 d. įsakymu Nr. V-439;

13.7.3. Geležinkelių transporto valstybinės priežiūros informacinės sistemos naudotojų administravimo taisyklės, patvirtintos Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos viršininko 2011 m. liepos 18 d. įsakymu Nr. V-439.

Papildyta punktu:
Nr. V-419, 2012-07-02, Žin., 2012, Nr. 79-4137 (2012-07-05), i. k. 1122214ISAK000V-419

13.8. Lietuvos standartai LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006, Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo technika“ grupės standartai, reguliuojantys saugų informacinės sistemos duomenų tvarkymą.

Punkto numeracijos pakeitimas:
Nr. V-419, 2012-07-02, Žin., 2012, Nr. 79-4137 (2012-07-05), i. k. 1122214ISAK000V-419

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

14. Vadovaujantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių 3.2.7 punktu, VGI IS priskiriama antrai informacinių sistemų kategorijai.

15. Saugos įgaliotinis, vadovaudamasis Lietuvos Respublikos vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“, Lietuvos standartu LST ISO/IEC 27005 „Informacijos technologija. Saugumo technika. Informacijos saugumo rizikos valdymas“, kasmet organizuoja VGI IS rizikos veiksnių vertinimą. Prireikus Saugos įgaliotinis gali organizuoti neeilinį VGI IS rizikos veiksnių vertinimą.

16. VGI IS rizikos įvertinimas pateikimas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausieji rizikos veiksniai yra šie:

16.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, fiziniai informacijos technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

16.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

16.3. nenugalima jėga *(force majeure)*.

17. Rizikos veiksniai vertinami, nustatant jų galimą pasireiškimo dažnį (žemas – gali pasireikšti ne dažniau kaip 1 kartą per metus, vidutinis – gali pasireikšti ne dažniau kaip 1 kartą per 3 mėnesius, aukštas – gali pasireikšti dažniau nei 1 kartą per 3 mėnesius) ir įtakos VGI IS elektroninės informacijos saugai laipsnius:

17.1. Ž – žemas. Duomenų pažeidimo poveikio laipsnis nėra didelis, padariniai nebus pavojingi – dingo ar yra sugadinta mažesnė nei 5 proc. dalis informacijos, tačiau ją VGI IS priemonėmis galima atstatyti iš atsarginių kopijų; atskleista iki 5 proc. neviešos informacijos; VGI IS neprieinama ne daugiau nei 20 min. per parą.;

17.2. V – vidutinis. Duomenų pažeidimo poveikio laipsnis gali būti didelis, padariniai rimti – dingo ar yra sugadinta mažesnė nei 50 proc. dalis informacijos, tačiau ją VGI IS priemonėmis galima atstatyti iš atsarginių kopijų; atskleista 5–20 proc. neviešos informacijos; VGI IS neprieinama ne daugiau nei 60 min. per parą;

17.3. A – aukštas. Duomenų pažeidimo poveikio laipsnis labai didelis, padariniai rimti – dingo ar yra sugadinta didesnė nei 50 proc. dalis informacijos ir (arba) dalis dingusios ar sugadintos informacijos VGI IS priemonėmis negali būti atstatyta iš atsarginių kopijų; atskleista daugiau kaip 20 proc. neviešos informacijos; VGI IS neprieinama daugiau nei 60 min. per parą.

18. Rizikos vertinimo metu atliekamos veiklos:

18.1. VGI IS sudarančių informacinių išteklių inventorizacija;

18.2. įtakos VGI IS veiklai vertinimas;

18.3. grėsmės ir pažeidimų analizė;

18.4. liekamosios rizikos vertinimas.

19. Atsižvelgdamas į rizikos įvertinimo ataskaitą, Inspekcijos viršininkas prireikus tvirtina rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

20. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

20.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

20.2. informacijos saugos priemonės diegimo kainos adekvatumas saugomos informacijos vertei;

20.3. esant galimybei, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

21. Siekiant užtikrinti Saugos nuostatuose ir Saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per dvejus metus organizuojamas informacinių technologijų saugos atitikties vertinimas, kurio metu:

21.1. įvertinama esamos informacijos saugos padėties atitiktis Saugos nuostatų ir Saugos dokumentų reikalavimams;

21.2. inventorizuojama VGI IS techninė ir programinė įranga;

21.3. tikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų VGI IS duomenis tvarkančių darbuotojų ir administratorių darbų vietų bei visų tarnybinių stočių programinė įranga ir jų sąranka;

21.4. įvertinama VGI IS duomenis tvarkantiems darbuotojams ir administratoriams suteiktų teisių atitiktis vykdomoms funkcijoms;

21.5. įvertinamas pasirengimas užtikrinti VGI IS veiklos tęstinumą įvykus saugos incidentui.

22. Atlikus šių nuostatų 21 punkte nurodytą vertinimą, rengiamas trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Inspekcijos viršininkas.

23. Prireikus Saugos įgaliotinis gali inicijuoti ir Inspekcijos viršininko pavedimu atlikti neeilinį VGI IS rizikos įvertinimą.

24. Neeilinis VGI IS rizikos vertinimas turi būti atliekamas:

24.1. įvykus pokyčiams VGI IS techninėje ar programinėje įrangoje, kurie galėtų įtakoti VGI IS veikimą;

24.2. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė VGI IS techninei, programinei įrangai ar VGI IS laikomiems duomenims;

24.3. po saugos incidento, kurio metu būtų sutrikdyta VGI IS veikla, sugadinti ar

prarasti VGI IS duomenys.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

25. Priemonės ir metodai, kurie taikomi užtikrinant prieigą prie VGI IS, nurodant leistiną šios prieigos laiką ir būdą, nustatomi VGI IS naudotojų administravimo taisyklėse.

26. Visos VGI IS tarnybinės stotys ir naudotojų darbo vietos turi būti apsaugotos nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.). Apsaugai naudojama programinė įranga turi būti atnaujinama automatiškai ne rečiau kaip kartą per parą.

27. Draudžiama naudoti programinę įrangą, nesusijusią su VGI IS tvarkytojo ir naudotojo atliekamomis funkcijomis.

28. Prieigai prie VGI IS naudojami kompiuteriai gali būti naudojami ir kitoms VGI IS naudotojo ir administratoriaus funkcijoms atlikti.

29. VGI IS naudotojų prieiga prie kitų valstybės institucijų, žinybų kompiuterių tinklų ar interneto turi būti apsaugota ugniasienėmis. Interneto turinys turi būti kontroliuojamas, filtruojant nepageidaujamą informaciją.

30. Kompiuterius, turinčius prieigą prie VGI IS, naudojant nustatytoms funkcijoms vykdyti ne institucijos patalpose, įdiegiamos papildomos saugos priemonės (duomenų šifravimas, prisijungimo ribojimai).

31. Užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų valstybės institucijų, naudojamas Saugus valstybės duomenų perdavimo tinklas (toliau – SVDPT).

32. VGI IS naudotojų kompiuterių tinklai turi tenkinti SVDPT saugos organizavimo, valdymo ir SVDPT naudotojų prijungimo reikalavimus, nustatytus Lietuvos Respublikos vidaus reikalų ministro 2007 m. birželio 5 d. įsakyme Nr. 1V-210 „Dėl Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimų patvirtinimo“ (Žin., 2007, Nr. 66-2582).

33. Duomenys teikiami ir (ar) gaunami automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas.

34. Atsarginių kopijų darymas turi užtikrinti VGI IS veiklos tęstinumą.

35. Duomenų atkūrimo iš atsarginių kopijų testavimas atliekamas ne rečiau kaip kartą per metus.

IV. REIKALAVIMAI PERSONALUI

36. Saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus ir priemones (informacijos, konfidencialumo, vientisumo, pasiekiamumo apsaugos principus; organizacines apsaugos priemones, technines apsaugos priemones, apsaugos informacinių priemonių visumą), savo darbe vadovautis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 (Žin., 2004, Nr. 80-2855), kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais.

37. VGI IS administratoriumi ir sisteminiu administratoriumi gali būti skiriamas valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, išmanantis darbą su kompiuterių tinklais ir mokantis užtikrinti jų saugumą. Administratorius privalo būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais.

38. Visi VGI IS naudotojai privalo turėti darbo kompiuteriu įgūdžių.

39. Tvarkyti VGI IS duomenis gali tik VGI IS naudotojai, susipažinę su VGI IS nuostatais, Saugos nuostatais ir Saugos dokumentais bei raštu sutikę laikytis šių teisės aktų reikalavimų.

40. VGI IS naudotojai, pažeidę Saugos nuostatų ar Saugos dokumentų reikalavimus,

atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

V. VGI IS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS POLITIKA PRINCIPAI

41. Už VGI IS naudotojų supažindinimą su Saugos nuostatais ir Saugos dokumentais bei atsakomybe už šių reikalavimų nesilaikymą yra atsakingas Saugos įgaliotinis.

42. VGI IS naudotojai su Saugos nuostatais ir Saugos dokumentais bei atsakomybe už šių teisės aktų reikalavimų nesilaikymą supažindinami pasirašytinai.

43. Saugos įgaliotinis tvarko VGI IS naudotojų supažindinimo su saugos politika žurnalą, kuriame pildomos šios grafos: supažindinimo data, VGI IS naudotojo vardas ir pavardė, pareigos, parašas.

44. Pakartotinai su Saugos nuostatais ir Saugos dokumentais VGI IS naudotojai supažindinami tik iš esmės pasikeitus VGI IS arba informacijos saugą reglamentuojantiems teisės aktams.

45. Saugos nuostatai ir Saugos dokumentai skelbiami vidiniame Inspekcijos tinklalapyje.

VI. BAIGIAMOSIOS NUOSTATOS

46. Saugos nuostatai ir Saugos dokumentai turi būti peržiūrėti ne rečiau kaip kartą per kalendorinius metus atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą, įvykus esminiams organizaciniams, technologiniams ar kitiems VGI IS pokyčiams.

Pakeitimai:

1.
Valstybinė geležinkelio inspekcija prie Susisiekimo ministerijos, Įsakymas
Nr. V-419, 2012-07-02, Žin., 2012, Nr. 79-4137 (2012-07-05), i. k. 1122214ISAK000V-419
Dėl Valstybinės geležinkelio inspekcijos prie Susisiekimo ministerijos viršininko 2011 m. vasario 19 d. įsakymo Nr. V-73 "Dėl Geležinkelių transporto valstybinės priežiūros informacinės sistemos duomenų saugos nuostatų patvirtinimo" pakeitimo