LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRO

Į S A K Y M A S
DĖL TECHNINIŲ VALSTYBĖS REGISTRŲ (KADASTRŲ), ŽINYBINIŲ REGISTRŲ, VALSTYBĖS INFORMACINIŲ SISTEMŲ IR KITŲ INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMŲ PATVIRTINIMO

2013 m. spalio 4 d. Nr. 1V-832
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 (Žin., 2013, Nr. 86-4310), 5 punktu:

1. T v i r t i n u Techninius valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimus (pridedama).

2. P r i p a ž į s t u netekusiu galios Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymą Nr. 1V-384 „Dėl Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techninių saugos reikalavimų patvirtinimo ir Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymo Nr. 1V-247 „Dėl Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių ir valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ pakeitimo“ (Žin., 2008, Nr. 127-4866).

TEISINGUMO MINISTRAS,
PAVADUOJANTIS VIDAUS REIKALŲ MINISTRĄ JUOZAS BERNATONIS

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų ministro
2013 m. spalio 4 d. įsakymu Nr. 1V-832

TECHNINIAI VALSTYBĖS REGISTRŲ (KADASTRŲ), ŽINYBINIŲ REGISTRŲ, VALSTYBĖS INFORMACINIŲ SISTEMŲ IR KITŲ INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMAI

I. BENDROSIOS NUOSTATOS

1. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų (toliau – reikalavimai) tikslas – nustatyti minimalius elektroninės informacijos saugos techninius reikalavimus valstybės registrams (kadastrams), žinybiniams registrams, valstybės informacinėms sistemoms ir kitoms informacinėms sistemoms (toliau – informacinė sistema).

2. Reikalavimai privalomi valstybės institucijoms, valstybės įstaigoms, valstybės įmonėms, viešosioms įstaigoms, steigiančioms, kuriančioms ir (arba) tvarkančioms informacines sistemas, finansuojamoms iš valstybės biudžeto, Valstybinio socialinio draudimo fondo biudžeto, Privalomojo sveikatos draudimo fondo biudžeto ir kitų valstybės pinigų fondų ir Lietuvos Respublikos viešojo administravimo įstatymo (Žin., 1999, Nr. 60-1945; 2006, Nr. 77-2975) nustatyta tvarka įgaliotoms atlikti viešąjį administravimą, valstybės ir savivaldybių įmonėms, savivaldybių įstaigoms ir viešosioms įstaigoms, kuriančioms kitas informacinių technologijų priemones, kuriomis apdorojama informacija, valdoma valstybės ir savivaldybių įmonių, savivaldybių įstaigų ir viešųjų įstaigų, atliekančių teisės aktų joms nustatytas funkcijas, jeigu išlaidos, patirtos kuriant tokias informacinių technologijų priemones, yra finansuojamos iš valstybės biudžeto, Valstybinio socialinio draudimo fondo biudžeto, Privalomojo sveikatos draudimo fondo biudžeto ar kitų valstybės pinigų fondų arba jeigu apdorojant informaciją informacinių technologijų priemonėmis per valstybės informacinių sistemų ar registrų sąveiką reikia gauti duomenis iš valstybės informacinių sistemų ir (arba) registrų (toliau – institucija).

3. Reikalavimai nėra taikomi įslaptintos elektroninės informacijos saugai.

4. Reikalavimuose vartojama sąvoka **vidinis informacinės sistemos naudotojas** – informacinės sistemos naudotojas, darbo santykiais susijęs su informacinės sistemos valdytoju arba informacinės sistemos tvarkytoju.

Kitos reikalavimuose vartojamos sąvokos atitinka sąvokas, nustatytas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme (Žin., 2011, Nr. 163-7739), Lietuvos Respublikos elektroninių ryšių įstatyme (Žin., 2004, Nr. 69-2382), Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 (Žin., 2013, Nr. 86-4310), kituose Lietuvos Respublikos įstatymuose ir Lietuvos standartuose LST ISO/IEC 27001:2006 ir LST ISO/IEC 27002:2009.

II. MINIMALIEJI ELEKTRONINĖS INFORMACIJOS SAUGOS TECHNINIAI REIKALAVIMAI

5. Bendrieji informacinių sistemų elektroninės informacijos saugos techniniai reikalavimai, taikytini visų kategorijų informacinėms sistemoms:

5.1. informacinės sistemos informacinių technologijų saugos atitikties vertinimas (toliau – atitikties vertinimas) turi būti atliekamas ne rečiau kaip kartą per du metus, jei kituose teisės aktuose nenustatyta kitaip;

5.2. informacinėje sistemoje turi būti įrašomi ir informacinės sistemos valdytojo tvirtinamose Saugaus elektroninės informacijos tvarkymo taisyklėse nustatytą laiką saugomi

duomenys apie informacinės sistemos tarnybinių stočių, informacinės sistemos taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinės sistemos tarnybinėse stotyse, informacinės sistemos taikomojoje programinėje įrangoje, visus informacinės sistemos naudotojų vykdomus veiksmus, kitus elektroninės informacijos saugai svarbius įvykius, nurodant informacinės sistemos naudotojo identifikatorių ir elektroninės informacijos saugai svarbaus įvykio ar vykdyto veiksmo laiką; šie duomenys turi būti saugomi ne toje pačioje informacinėje sistemoje, kurioje jie įrašomi, taip pat jie turi būti analizuojami ne rečiau kaip kartą per savaitę;

5.3. informacinės sistemos priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą informacinės sistemos administratoriaus paskyrą, kuria naudojantis negalima atlikti informacinės sistemos naudotojo funkcijos;

5.4. informacinių sistemų naudotojams negali būti suteikiamos informacinės sistemos administratoriaus teisės;

5.5. kiekvienas informacinės sistemos naudotojas turi būti informacinėje sistemoje unikaliai identifikuojamas (asmens kodas negali būti naudojamas kaip informacinės sistemos naudotojo identifikatorius);

5.6. nuotolinis prisijungimas prie informacinės sistemos turi būti vykdomas protokolu, skirtu duomenų šifravimui;

5.7. informacinės sistemos naudotojas ar informacinės sistemos administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita autentiškumo patvirtinimo priemone;

5.8. vidiniam informacinės sistemos naudotojui teisė dirbti su konkrečia elektronine informacija turi būti sustabdoma, kai vidinis informacinės sistemos naudotojas nesinaudoja informacine sistema ilgiau kaip 3 mėnesius, kai įstatymų nustatytais atvejais vidinis informacinės sistemos naudotojas nušalinamas nuo darbo (pareigų); pasibaigus tarnybos (darbo) santykiams, vidinio informacinės sistemos naudotojo teisė naudotis informacine sistema turi būti panaikinta nedelsiant;

5.9. baigus darbą ar pasitraukiant iš darbo vietos informacinėje sistemoje turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos, įjungiama ekrano užsklanda su slaptažodžiu; taip pat dokumentai ar jų kopijos darbo vietoje turi būti padedami į pašaliniams asmenims neprieinamą vietą;

5.10. informacinės sistemos naudotojui neatliekant jokių veiksmų informacinėje sistemoje, informacinės sistemos taikomoji programinė įranga turi užsirakinti, kad toliau naudotis informacine sistema galima būtų tik pakartotinai patvirtinus savo tapatybę; terminas, per kurį informacinės sistemos naudotojui neatliekant jokių veiksmų informacinė sistema užsirakina, nustatomas informacinės sistemos valdytojo tvirtinamose Saugaus elektroninės informacijos tvarkymo taisyklėse; terminas, per kurį informacinės sistemos naudotojui neatliekant jokių veiksmų informacinės sistema turi užsirakinti, negali būti ilgesnis nei 15 min.;

5.11. informacinės sistemos valdytojas turi nusistatyti, kiek jis ir informacinės sistemos tvarkytojas (-ai) ilgiausiai gali tęsti savo funkcijų, kurioms atlikti buvo sukurta informacinė sistema, vykdymą neveikiant informacinei sistemai ar jos daliai; informacinės sistemos neveikimo laikotarpis negali būti ilgesnis nei:

5.11.1. ketvirtos kategorijos informacinės sistemos – 24 val.;

5.11.2. trečios kategorijos informacinės sistemos – 16 val.;

5.11.3. antros kategorijos informacinės sistemos – 12 val.;

5.11.4. pirmos kategorijos informacinės sistemos – 8 val.;

5.12. reikalavimai informacinės sistemos techninei ir programinei įrangai ir patalpoms:

5.12.1. pagrindinė informacinės sistemos kompiuterinė įranga turi turėti įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį informacinės sistemos pagrindinės kompiuterinės įrangos veikimą;

5.12.2. jei informacinės sistemos tarnybinių stočių patalpose esančios įrangos bendras

galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga;

5.12.3. informacinės sistemos tarnybinėse stotyse ir vidinių informacinės sistemos naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės; šios priemonės automatiškai turi informuoti informacinės sistemos administratorių apie tai, kuriems informacinės sistemos posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas; informacinės sistemos komponentai be kenksmingo programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu rizikos vertinimo metu yra patvirtinama, kad šių komponentų rizika yra priimtina;

5.12.4. turi būti operatyviai ištestuojami ir įdiegiami informacinės sistemos tarnybinių stočių ir vidinių informacinės sistemos naudotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; informacinės sistemos administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie informacinės sistemos posistemiams, funkciškai savarankiškoms sudedamosioms dalims, vidinių informacinės sistemos naudotojų darbo vietų kompiuterinei įrangai neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumų svarbos lygius;

5.12.5. informacinės sistemos tarnybinėse stotyse turi būti naudojama tik legali programinė įranga;

5.12.6. vidinių informacinės sistemos naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga; informacinės sistemos saugos įgaliotinis turi parengti, su informacinės sistemos valdytojo vadovu suderinti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti leistinos programinės įrangos sąrašą;

5.12.7. informacinės sistemos techninė ir programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

5.12.8. informacinės sistemos techninės ir programinės įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai;

5.12.9. informacinės sistemos tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas;

5.12.10. informacinės sistemos tarnybinių stočių patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir (arba) apsaugos tarnybos stebėjimo pulto;

5.12.11. per metus turi būti užtikrintas informacinės sistemos prieinamumas: ketvirtos kategorijos informacinėms sistemoms – ne mažiau kaip 70 proc. laiko darbo metu darbo dienomis, trečios kategorijos informacinėms sistemoms – ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis, antros kategorijos informacinėms sistemoms – ne mažiau kaip 96 proc. laiko visą parą, pirmos kategorijos informacinėms sistemoms – ne mažiau kaip 99 proc. laiko visą parą;

5.12.12. informacinės sistemos valdytojo tvirtinamuose informacinės sistemos duomenų saugos nuostatuose nustatyta tvarka turi būti daromos atsarginės elektroninės informacijos kopijos (toliau – kopijos), kurios turi būti saugomos kitose patalpose nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate;

5.12.13. elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijas neteisėtai atkurti elektroninę informaciją;

5.12.14. atsarginės laikmenos su informacinės sistemos programinės įrangos kopijomis turi būti laikomos kitose patalpose arba kitame pastate nei yra informacinės sistemos tarnybinės stotys;

5.12.15. informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę; ugniasienės įvykių žurnalai (angl.

Logs) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

5.12.16. informacinės sistemos programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project* (OWASP) interneto svetainėje www.owasp.org;

5.13. informacinės sistemos tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

5.14. reikalavimai prisijungimo prie visų kategorijų informacinių sistemų slaptažodžiams:

5.14.1. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;

5.14.2. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija;

5.14.3. draudžiama slaptažodžius atskleisti tretiesiems asmenims;

5.14.4. informacinės sistemos dalys, atliekančios nutolusio prisijungimo autentikavimą, turi drausti automatiškai išsaugoti slaptažodžius;

5.14.5. informacinės sistemos valdytojo tvirtinamose Naudotojų administravimo taisyklėse turi būti nustatytas didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius, kuris turėtų būti ne didesnis nei 5 kartai; slaptažodį, neteisingai įvedus didžiausią leistiną skaičių, informacinė sistema turi užsirakinti ir neleisti informacinės sistemos naudotojui identifikuotis informacinės sistemos valdytojo tvirtinamose Naudotojų administravimo taisyklėse nustatytą laiko tarpą, kuris turi būti ne trumpesnis nei 15 minučių;

5.14.6. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais; saugos įgaliotinio sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jei:

5.14.6.1. informacinės sistemos naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio;

5.14.6.2. nėra techninių galimybių informacinės sistemos naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu;

5.14.7. papildomi reikalavimai informacinės sistemos naudotojo slaptažodžiams:

5.14.7.1. slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius;

5.14.7.2. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;

5.14.7.3. keičiant slaptažodį informacinė sistema neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

5.14.7.4. pirmojo prisijungimo prie informacinės sistemos metu iš informacinės sistemos naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį;

5.14.8. papildomi reikalavimai informacinės sistemos administratorių slaptažodžiams:

5.14.8.1. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

5.14.8.2. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

5.14.8.3. keičiant slaptažodį informacinės sistemos taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.

6. Papildomi trečiosios kategorijos informacinių sistemų elektroninės informacijos saugos techniniai reikalavimai:

6.1. informacinė sistema turi perspėti informacinės sistemos administratorių, kai pagrindinėje informacinės sistemos kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

6.2. viešaisiais ryšių tinklais perduodamos informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network*), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas

priemones;

6.3. informacinė sistema turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones;

6.4. patekimas į informacinės sistemos tarnybinių stočių patalpas ir patalpas, kuriose saugomos atsarginės kopijos, turi būti kontroliuojamas informacinės sistemos valdytojo tvirtinamose Saugaus elektroninės informacijos tvarkymo taisyklėse nustatyta tvarka;

6.5. institucija turi numatyti atsargines patalpas, į kurias galėtų laikinai perkelti informacinės sistemos įrangą, nesant galimybių tęsti veiklą pagrindinėse patalpose; informacinės sistemos veiklos tęstinumo valdymo planas turi užtikrinti informacinės sistemos veiklos atnaujinimą atsarginėse patalpose per laikotarpį, ne ilgesnį nei nustatyta reikalavimų 5.11 punkte;

6.6. atsarginės patalpos turi tenkinti pagrindinėms patalpoms keliamus reikalavimus arba informacinės sistemos veiklos tęstinumo valdymo plane turi būti nustatyta, kaip per minimalų laikotarpį pasiekti šių reikalavimų atitiktį;

6.7. atsarginės laikmenos su programinės įrangos kopijomis turi būti laikomos nedegioje spintoje, kitose patalpose arba kitame pastate nei yra informacinės sistemos tarnybinės stotys;

6.8. programinę įrangą turi diegti tik informacinės sistemos valdytojo ar tvarkytojo vadovo įgalioti asmenys;

6.9. programinė įranga turi būti testuojama naudojant atskirą testavimui skirtą aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintų Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) (Žin., 2008, Nr. 135-5298), 10.10 punkto reikalavimais.

7. Papildomi antrosios kategorijos informacinių sistemų elektroninės informacijos saugos techniniai reikalavimai:

7.1. šių reikalavimų 6 punkte nurodyti elektroninės informacijos saugos techniniai reikalavimai;

7.2. atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip;

7.3. vidinių informacinės sistemos naudotojų darbo vietose gali būti naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (pavyzdžiui, USB, CD/DVD ir kt.); šios laikmenos negali būti naudojamos veiklai, nesusijusiai su teisėtu informacinės sistemos tvarkymu;

7.4. svarbiausia kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne mažiau kaip 30 min.;

7.5. svarbiausia kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima;

7.6. svarbiausios kompiuterinės įrangos gedimai turi būti registruojami, taip pat turi būti paskirtas asmuo už gedimų registravimą;

7.7. informacija apie informacinėje sistemoje įrašomus duomenis, apie informacinės sistemos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinėje sistemoje, visus informacinės sistemos naudotojų vykdomus veiksmus, kitus saugai svarbius įvykius turi būti analizuojama ne rečiau kaip kartą per savaitę; įvykių žurnaluose duomenys turi būti saugomi ne trumpiau kaip 1 metus;

7.8. informacinės sistemos tarnybinių stočių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga;

7.9. visose patalpose, kuriose yra vidinių informacinės sistemos naudotojų ir informacinės sistemos techninė įranga, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

7.10. patekimas prie vidinių informacinės sistemos naudotojų darbo vietų turi būti kontroliuojamas;

7.11. pagrindinėse informacinės sistemos tarnybinėse stotyse turi būti naudojamos vykdomo kodo kontrolės priemonės, automatiškai apribojančios ar informuojančios apie neautorizuoto programinio kodo vykdymą;

7.12. pagrindinėse informacinės sistemos tarnybinėse stotyse turi būti įjungtos ugniasienės, sukonfigūruotos praleisti tik su informacinės sistemos funkcionalumu ir administravimu susijusį duomenų srautą; ugniasienių konfigūracijų dokumentacija turi būti saugoma kartu su informacinės sistemos dokumentacija;

7.13. informacinės sistemos tinkle turi būti įdiegtos ir veikti automatinės įsilaužimo aptikimo sistemos.

8. Papildomi pirmosios kategorijos informacinių sistemų elektroninės informacijos saugos techniniai reikalavimai:

8.1. šių reikalavimų 7 punkte nurodyti elektroninės informacijos saugos techniniai reikalavimai;

8.2. ne rečiau kaip kartą per trejus metus atitikties vertinimą turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai;

8.3. institucija turi įgyvendinti Lietuvos standarte LST ISO/IEC 27002:2009 nurodytas saugos priemones, išskyrus priemones, kurios netaikytinos dėl institucijos veiklos, informacinės sistemos ar naudojamos informacinėje sistemoje techninės įrangos pobūdžio, ir Lietuvos standarte LST ISO/IEC 27001:2006 nurodytus reikalavimus informacijos saugumo valdymo sistemai.

III. BAIGIAMOSIOS NUOSTATOS

9. Informacinių sistemų valdytojai ir tvarkytojai privalo užtikrinti saugos priemonių, skirtų ne žemesnei kategorijai negu yra nustatyta jų informacinei sistemai, taikymą. Taip pat gali būti taikomos saugos priemonės, nenurodytos reikalavimuose, tačiau rekomenduojamos pripažintose metodikose ar Lietuvos ir tarptautiniuose standartuose.

_____