LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS

Į S A K Y M A S
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

2007 m. liepos 11 d. Nr. 1V-247
Vilnius

Įgyvendindamas Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų įgyvendinimo priemonių plano, patvirtinto Lietuvos Respublikos Vyriausybės 2006 m. birželio 19 d. nutarimu Nr. 601 (Žin., 2006, Nr. 70-2575), 2.1.2 punktą:

1. T v i r t i n u pridedamus:

1.1. Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gaires.

1.2. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimus.

2. P r i p a ž į s t u netekusiu galios Lietuvos Respublikos vidaus reikalų ministro 2003 m. sausio 27 d. įsakymą Nr. 1V-33 „Dėl Informacijos klasifikavimo pagal duomenų grupes rekomendacijų patvirtinimo“ (Žin., 2003, Nr. 77-3541).

TEISINGUMO MINISTRAS,
PAVADUOJANTIS VIDAUS REIKALŲ MINISTRĄ PETRAS BAGUŠKA

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų ministro
2007 m. liepos 11 d. įsakymu Nr. 1V-247

VALSTYBĖS INSTITUCIJŲ IR ĮSTAIGŲ INFORMACINIŲ SISTEMŲ KLASIFIKAVIMO PAGAL JOSE TVARKOMĄ ELEKTRONINĘ INFORMACIJĄ GAIRĖS

I. BENDROSIOS NUOSTATOS

1. Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės (toliau – gairės) reglamentuoja valstybės institucijų ir įstaigų informacinių sistemų (toliau – informacinė sistema) klasifikavimą pagal informacinėse sistemose tvarkomos elektroninės informacijos svarbą.

2. Gairėse vartojamos sąvokos atitinka sąvokas, nustatytas 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; 2007, Nr. 49-1891), bei Lietuvos Respublikos įstatymuose ir kituose teisės aktuose.

II. INFORMACINIŲ SISTEMŲ KATEGORIJŲ NUSTATYMAS

3. Informacinės sistemos klasifikuojamos pagal kategorijas nuo pirmos (aukščiausioji kategorija) iki ketvirtos (žemiausioji kategorija):

3.1. Pirmos kategorijos informacinė sistema – informacinė sistema, kuri atitinka bent vieną iš šių kriterijų:

3.1.1. tai yra informacinė sistema, kurioje logiškai tarpusavyje susijusių duomenų konfidencialumo, vientisumo ir (ar) prieinamumo praradimas gali sukelti ypač sunkius padarinius valstybei;

3.1.2. tai yra informacinė sistema, kurios pagrindu funkcionuoja pagrindinis valstybės registras;

3.1.3. tai yra Valstybinio socialinio draudimo fondo funkcijų vykdymą užtikrinanti informacinė sistema;

3.1.4. tai yra mokesčių administratoriaus funkcijų vykdymą užtikrinanti informacinė sistema;

3.1.5. skirta valstybės piniginiams ištekliams planuoti, kaupti, išduoti, jų apskaitai tvarkyti, naudojimo kontrolei atlikti, rengti atskaitomybę ir stebėti valstybės piniginių išteklių srautus.

3.2. Antros kategorijos informacinė sistema – informacinė sistema, kuri atitinka bent vieną iš šių kriterijų:

3.2.1. tai yra informacinė sistema, kurioje logiškai tarpusavyje susijusių duomenų konfidencialumo, vientisumo ir (ar) prieinamumo praradimas gali turėti sunkių padarinių valstybės institucijos ar įstaigos darbui bei turėti neigiamą įtaką kitų valstybės institucijų ar įstaigų veiklai;

3.2.2. joje tvarkomi duomenys yra teikiami pirmos kategorijos informacinei sistemai;

3.2.3. joje tvarkomi ypatingi asmens duomenys, išskyrus duomenis, susijusius su asmens sveikata;

3.2.4. užtikrina pirmos kategorijos informacinių sistemų sąveiką;

3.2.5. tai yra informacinė sistema, kurioje tvarkomi iš pirmos kategorijos informacinės sistemos gauti duomenys;

3.2.6. tai yra informacinė sistema, kurios pagrindu funkcionuoja valstybės registras;

3.2.7. sudaryta iš ne mažiau kaip 5 posistemių, vykdančių elektroninės informacijos, reikalingos valstybės institucijai teisės aktų nustatytoms funkcijoms, išskyrus vidaus administravimą, atlikti, apdorojimo procesus.

3.3. Trečios kategorijos informacinė sistema – informacinė sistema, kuri atitinka bent vieną

iš šių kriterijų:

3.3.1. tai yra informacinė sistema, kurioje logiškai tarpusavyje susijusių duomenų konfidencialumo, vientisumo ir (ar) prieinamumo praradimas gali turėti neigiamą įtaką valstybės institucijos ar įstaigos veiklai;

3.3.2. joje tvarkomi asmens duomenys;

3.3.3. tai yra informacinė sistema, kurioje tvarkomi iš pirmos kategorijos informacinės sistemos gauti apibendrinti arba nuasmeninti duomenys;

3.3.4. tai yra informacinė sistema, kurios pagrindu funkcionuoja žinybinis registras;

3.3.5. sudaryta iš ne mažiau kaip 3 posistemių, vykdančių elektroninės informacijos, reikalingos valstybės institucijai teisės aktų nustatytoms funkcijoms, išskyrus vidaus administravimą, atlikti, apdorojimo procesus.

3.4. Ketvirtos kategorijos informacinės sistemos – visos kitos informacinės sistemos.

III. BAIGIAMOSIOS NUOSTATOS

4. Informacinės sistemos kategorija nustatoma informacinės sistemos duomenų saugos nuostatuose.

_____

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų ministro
2007 m. liepos 11 d. įsakymu Nr. 1V-247

VALSTYBĖS INSTITUCIJŲ IR ĮSTAIGŲ INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMAI

I. BENDROSIOS NUOSTATOS

1. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimų (toliau – reikalavimai) tikslas – nustatyti minimalius elektroninės informacijos saugos reikalavimus valstybės institucijų ir įstaigų (toliau – institucija) trečios ir ketvirtos kategorijų informacinėms sistemoms (toliau – informacinės sistemos).

2. Reikalavimuose vartojamos sąvokos:

Konfidencialumas – elektroninės informacijos savybė, kad su informacinėje sistemoje tvarkoma elektronine informacija gali susipažinti tik tam įgalioti asmenys.

Vientisumas – elektroninės informacijos savybė, kad elektroninė informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

Prieinamumas – elektroninės informacijos savybė, kad elektroninė informacija gali būti tvarkoma reikiamu metu.

Sauga – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

Kitos reikalavimuose vartojamos sąvokos atitinka sąvokas, nustatytas 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; 2007, Nr. 49-1891), Lietuvos Respublikos įstatymuose ir kituose teisės aktuose.

II. INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMAI

3. Informacinių sistemų elektroninės informacijos saugos reikalavimai:

3.1. elektroninės informacijos saugos užtikrinimo reikalavimai:

3.1.1. informacinės sistemos valdytojo teisės aktų nustatyta tvarka turi būti patvirtinti informacinės sistemos duomenų saugos nuostatai;

3.1.2. informacinės sistemos valdytojo turi būti užtikrintas informacinės sistemos funkcijų pokyčių (toliau – pokyčiai) valdymo planavimas;

3.2. elektroninės informacijos saugos užtikrinimo organizavimo reikalavimai:

3.2.1. informacinės sistemos valdytojo turi būti paskirtas asmuo, atsakingas už informacijos saugą;

3.2.2. informacinė sistema turi registruoti bent vieną paskutinį duomenų pakeitimą atlikusį informacinės sistemos naudotoją ir pakeitimo laiką;

3.2.3. informacinės sistemos valdymo funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus identifikatorių, kuriuo galima būtų uždrausti atlikti informacinės sistemos naudotojo funkcijas;

3.2.4. informacinės sistemos naudotojai turi būti išmokyti dirbti su programine ir technine įranga bei supažindinti su informacijos saugą institucijoje reglamentuojančiais teisės aktais; trečios kategorijos informacinės sistemos naudotojai, be to, turi būti baigę informacijos saugos mokymus;

3.2.5. teisė dirbti su konkrečia informacija turi būti suteikiama konkrečiam informacinės sistemos naudotojui arba informacinės sistemos naudotojų grupei, vadovaujantis principais „būtina darbui“ ir „būtina žinoti“;

3.2.6. kiekvienas informacinės sistemos naudotojas turi būti informacinėje sistemoje

unikaliai identifikuojamas – informacinės sistemos naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kita autentiškumo patvirtinimo priemone;

3.2.7. informacinės sistemos naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai informacinės sistemos naudotojas atostogauja, vykdomas informacinės sistemos naudotojo veiklos tyrimas ir pan.; pasibaigus tarnybos (darbo) santykiams, informacinės sistemos naudotojo teisė naudotis informacine sistema turi būti panaikinta;

3.2.8. baigus darbą turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą ir pan.;

3.2.9. informacinės sistemos naudotojui neatliekant jokių veiksmų, informacinė sistema turi užsirakinti, kad toliau naudotis informacine sistema galima būtų tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

3.2.10. institucija turi išsiaiškinti, kiek ji ilgiausiai gali tęsti savo funkcijų įgyvendinimą neveikiant informacinei sistemai ar jos daliai; institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi užtikrinti informacinės sistemos veiklos atkūrimą per šį laikotarpį; turi būti parengtas veiksmų planas, užtikrinantis informacinės sistemos veiklos atnaujinimą per 8 val., trečios kategorijos informacinėms sistemoms – per 16 val.;

3.3. reikalavimai informacinės sistemos įrangai ir patalpoms:

3.3.1. pagrindinė informacinės sistemos kompiuterinė įranga turi turėti įtampos filtrą arba (ir) rezervinį maitinimo šaltinį; trečios kategorijos informacinėms sistemoms – rezervinis maitinimo šaltinis turi užtikrinti informacinės sistemos pagrindinės kompiuterinės įrangos veikimą ne mažiau nei 10 min.;

3.3.2. turi būti naudojamos kenksmingosios informacinės sistemos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos;

3.3.3. turi būti operatyviai įdiegiami informacinės sistemos operacinės sistemos ir naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

3.3.4. informacinėje sistemoje turi būti naudojama tik legali programinė įranga;

3.3.5. turi būti apribota fizinė prieiga prie informacinės sistemos tarnybinių stočių (atskiros rakinamos patalpos arba rakinama spinta);

3.3.6. patalpose, kuriose yra informacinės sistemos tarnybinės stotys, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

3.3.7. turi būti užtikrintas informacinės sistemos prieinamumas ne mažiau kaip 70 proc. laiko darbo metu darbo dienomis; trečios kategorijos informacinėms sistemoms – ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis;

3.3.8. turi būti daromos atsarginės elektroninės informacijos kopijos (toliau – kopijos), kurios turi būti laikomos atskiroje patalpoje; trečios kategorijos informacinėms sistemoms – kopijos turi būti laikomos atskiroje patalpoje ir saugomos užrakintoje nedegioje spintoje;

3.3.9. informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacinių tinklų naudojant užkardą ar kitas priemones.

4. Trečios kategorijos informacinių sistemų elektroninės informacijos papildomi saugos reikalavimai:

4.1. elektroninės informacijos saugos užtikrinimo ir saugos užtikrinimo organizavimo reikalavimai:

4.1.1. rekomenduojama atskirti saugos įgaliotinio ir administratoriaus funkcijas;

4.1.2. rekomenduojama, kad asmuo, planuojantis pokyčius, jų pats neįgyvendintų;

4.1.3. rekomenduojama, kad funkcijos, susijusios su informacinės sistemos plėtra, būtų atskirtos nuo informacinės sistemos administravimo (eksploatavimo) funkcijų;

4.2. reikalavimai informacinės sistemos įrangai ir patalpoms:

4.2.1. informacinės sistemos atitikties keliamiems reikalavimams vertinimas turi būti atliekamas ne rečiau kaip kartą per dvejus metus, jei teisės aktai nenustato kitaip;

4.2.2. ne rečiau kaip kartą per 2 metus turi būti atliekamas informacinės sistemos rizikos vertinimas, jei teisės aktai nenustato kitaip; neeilinis informacinės sistemos rizikos vertinimas turi

būti atliekamas:

4.2.2.1. įvykus dideliems pokyčiams informacinės sistemos techninėje ar programinėje įrangoje;

4.2.2.2. įvykus dideliems institucijos, valdančios informacinę sistemą, organizaciniams pokyčiams;

4.2.2.3. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje;

4.2.2.4. po didelio masto saugos incidentų;

4.2.3. informacinė sistema turi perspėti 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;

4.2.4. viešaisiais telekomunikaciniais tinklais perduodamos informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network),* skirtines linijas, saugų valstybinį duomenų perdavimo tinklą ar kitas priemones;

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

4.2.6. informacinėje sistemoje turi būti registruojami ir nustatytą laiką saugomi duomenys apie informacinės sistemos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinėje sistemoje, kitus saugai svarbius įvykius, nurodant informacinės sistemos naudotojo identifikatorių ir įvykio laiką; ši informacija turi būti reguliariai analizuojama;

4.2.7. patekimas į informacinės sistemos tarnybinių stočių patalpas turi būti kontroliuojamas;

4.2.8. jei informacinės sistemos tarnybinių stočių patalpose esančios informacinės sistemos įrangos bendras galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga;

4.2.9. institucija turi numatyti atsargines patalpas, į kurias galėtų laikinai perkelti informacinės sistemos įrangą, nesant galimybių tęsti veiklą pagrindinėse patalpose; institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi užtikrinti informacinės sistemos veiklos atnaujinimą atsarginėse patalpose per tokį laikotarpį, kad nebūtų nusižengta institucijos įsipareigojimams, susijusiems su informacinės sistemos veikla;

4.2.10. kopijų darymas turi būti fiksuojamas;

4.2.11. duomenys kopijose turi būti užšifruoti arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijas neteisėtam duomenų atkūrimui;

4.2.12. periodiškai turi būti atliekami duomenų atkūrimo iš kopijų bandymai;

4.2.13. atsarginės laikmenos su programine įranga turi būti laikomos nedegioje spintoje;

4.2.14. informacinės sistemos slaptažodžių valdymo sistema turi užtikrinti kokybiškų individualių slaptažodžių naudojimą:

4.2.14.1. slaptažodis turi būti keičiamas kas 6 mėnesius;

4.2.14.2. slaptažodį turi sudaryti ne mažiau kaip 6 simboliai;

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

4.2.14.4. keičiant slaptažodį informacinė sistema neturi leisti nustatyti slaptažodžio iš buvusių 3 paskutinių slaptažodžių;

4.2.14.5. slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija;

4.2.14.6. slaptažodžiai negali būti atskleidžiami tretiesiems asmenims;

4.2.14.7. pirmo prisijungimo prie informacinės sistemos metu iš informacinės sistemos naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį.

III. BAIGIAMOSIOS NUOSTATOS

5. Institucijos privalo užtikrinti saugos priemonių, skirtų ne žemesnei kategorijai, negu yra suteikta jų informacinei sistemai, taikymą. Institucijos gali taikyti saugos priemones, nustatytas

aukštesnės kategorijos informacinėms sistemoms.

_____