LIETUVOS RESPUBLIKOS VALSTYBĖS KONTROLĖ

VALSTYBINIO AUDITO ATASKAITA
UŽSIENIO REIKALŲ MINISTERIJOS INFORMACINIŲ SISTEMŲ BENDROJI IR KŪRIMO KONTROLĖ

2013 m. sausio 31 d. Nr. VA-P-90-2-2
Vilnius

Auditas atliktas, vykdant 2012-06-15 pavedimą Nr. P-90-2

Auditą atliko valstybinių auditorių grupė:
Viktorija Mirošničenko (grupės vadovė)
Jurgita Musteikienė
Donatas Vitkus

Auditas pradėtas 2012-06-15
Auditas baigtas 2013-01-31

Su valstybinio audito ataskaita galima susipažinti
Valstybės kontrolės interneto puslapyje
adresu www.vkontrole.lt

SANTRAUKA

Lietuvos Respublikos užsienio reikalų ministerija formuoja valstybės užsienio reikalų politiką, koordinuoja veiksmus, susijusius su naryste Europos Sąjungoje, atstovauja Lietuvos Respublikai ir jos piliečių teisėtiems interesams ir juos gina tarptautinėse organizacijose ir užsienio valstybėse, įgyvendina kitus ministerijos nuostatuose nurodytus veiklos tikslus[1].

Automatizuodama veiklos funkcijas, ministerija nuo 1999 m. naudoja įvairaus sudėtingumo informacines sistemas, kuriose kaupiami ir apdorojami duomenys, įskaitant asmens duomenis ir ypatingus asmens duomenis. Be to, ministerija naudoja tinklus ir sistemas, kuriomis automatizuotai apdorojama įslaptinta informacija su žyma ne aukštesne kaip „Riboto naudojimo“. Siekiant užtikrinti ministerijos informacinėse sistemose apdorojamų duomenų konfidencialumą, tikslumą ir sistemų darbo nenutrūkstamumą, turėtų būti vykdoma tinkama informacinių sistemų valdymo kontrolė.

Audito tikslas – įvertinti Užsienio reikalų ministerijos informacinių sistemų bendrąją ir kūrimo kontrolę.

Užsienio reikalų ministerija nuo 2009 m. pradžios pasiekė nemažą informacinių sistemų valdymo pažangą. Kryptingai informacinių sistemų plėtrai buvo parengtos vystymo gairės. Patvirtintas Informacinių sistemų funkcijų pokyčių valdymo tvarkos aprašas, kurio tikslas – valdyti ministerijos informacinių sistemų pokyčius, užtikrinant kokybišką reikalingų pokyčių įvykdymą ir diegimą minimaliai sutrukdant informacinių sistemų funkcionavimą. Informacinių sistemų saugai stiprinti parengta saugos politiką apimanti dokumentacija, įgyvendintos incidentų valdymo priemonės. Tačiau audito metu nustatyta informacinių sistemų valdymo ir saugos trūkumų: nėra aiškiai aprašyti turimi el. duomenų srautai (informacijos architektūros modelis); informacinių technologijų valdymas stokoja stipresnės veiklos procesų ir informacinių technologijų sąsajos; nepaskirti duomenų įgaliotiniai; informacinių sistemų rizikos vertinimas atliekamas ne kasmet, nerengiami rizikos mažinimo įgyvendinimo priemonių planai, neatnaujinti saugos politikos dokumentai, neišbandytas veiklos tęstinumo planas; informacinės sistemos modernizuojamos neatnaujinus arba neparengus jų nuostatų, specifikacijų; nepakankama kontrolė tvarkant asmens duomenis ir ypatingus asmens duomenis bei įslaptintą informaciją.

Audito metu nustatyta, kad Užsienio reikalų ministerijos informacinių sistemų vidaus kontrolės branda apibrėžiama kaip pirminis (*Ad Hoc*) procesas[2]. Norint pasiekti aukštesnį brandos lygį, turėtų būti stiprinamos veiklos procesų ir informacinių technologijų sąsajos, atnaujintos Užsienio reikalų ministerijos informacinės sistemos vystymo gairės, kad jos apimtų visas ministerijos informacines

[1] Lietuvos Respublikos Vyriausybės 1998-09-25 nutarimu Nr. 1155 patvirtinti Lietuvos Respublikos užsienio reikalų ministerijos nuostatai, 5 p.
[2] Pagal Gebos brandos modelį (angl. *Capability Maturity Model*, CMM).

sistemas, parengti ir patvirtinti visų ministerijos informacinių sistemų nuostatai. Ministerijos informacinių sistemų valdymą ir saugą apibrėžianti dokumentacija turi būti nuolat atnaujinama ir atitikti realią situaciją. Periodiškai turi būti vertinama rizika ir informacinių sistemų saugos atitiktis, užtikrinama vykdomų procesų stebėsena. Ministerijai rekomenduota apibrėžti informacinių sistemų architektūrą, tobulinti ministerijos informacinių sistemų saugos, veiklos tęstinumo, duomenų valdymo ir trečiųjų šalių teikiamų paslaugų užtikrinimo procesus.

Užsienio reikalų ministerija parengė pateiktų rekomendacijų įgyvendinimo planą (žr. ataskaitos 2 priedą).

Išvados

1. Užsienio reikalų ministerijoje nėra bendro visas informacines sistemas apimančio informacijos architektūros modelio. Ministerijai aiškiai neaprašius turimų elektroninių duomenų srautų (duomenų struktūros), gali prireikti papildomo laiko ir išteklių juos apdorojant, taip pat gali būti parenkamos nepakankamos informacijos saugą užtikrinančios priemonės (1.1 poskyris).

2. Informacinių technologijų valdymo organizacinė struktūra tobulintina, nes:

2.1. ministerijoje nėra mechanizmo, skirto kartu su vadovybe spręsti strateginius informacinių technologijų valdymo klausimus, kad pagrindinės veiklos poreikiai būtų siejami su informacinių technologijų teikiamomis galimybėmis (1.2 poskyris);

2.2. nepaskirti duomenų valdymo įgaliotiniai (1.2 poskyris);

2.3. vyksta didelė informacinių technologijų personalo kaita, tačiau audituojamu laikotarpiu nesuplanuota rezervinė darbuotojų pakaita ir jų pareigų perėmimas (1.2 poskyris).

3. Ministerijoje nustatyta informacinių sistemų saugos valdymo trūkumų:

3.1. informacinių sistemų rizikos vertinimai nebuvo atliekami kasmet, todėl neidentifikuoti ir detaliai neįvertinti šiuo laikotarpiu egzistavę informacinių sistemų rizikos veiksniai, galintys turėti įtakos informacijos saugai, nerengiamas ir netvirtinamas informacinių sistemų rizikos mažinimo (valdymo) priemonių planas (1.3 poskyris);

3.2. **vidaus dokumentuose neapibrėžta, kokios konkrečios komponentės sudaro ministerijos informacines sistemas, todėl lieka neaiškus informacinių sistemų klasifikavimas pagal kategorijas, gali būti netiksliai nustatyti ministerijos informacinėse sistemose tvarkomos elektroninės informacijos apsaugos poreikis, prioritetai ir lygis** (3.3 poskyris)**;**

3.3. **informacinių technologijų saugos atitikties vertinimas buvo atliktas tik vieną kartą (2012 m.) i**r ne visi duomenų saugą reglamentuojantys dokumentai atnaujinti, todėl juose numatytos **informacinių sistemų saugos valdymo priemonės gali būti neveiksmingos** (3.3 poskyris)**;**

3.4. automatizuotai apdorojamos įslaptintos informacijos su žyma „Riboto naudojimo“ valdymas nepakankamai saugus, nes ministerijoje šios informacijos tvarkymą (naikinimą, perkėlimą, perdavimą, saugojimą) reglamentuojančios tvarkos nebuvo peržiūrimos ir atnaujinamos (3.4 poskyris);

3.5. naudotojų paskyrų valdymo procesas užtikrinamas nepakankamai, nes, nutrūkus darbuotojo darbo ar tarnybos teisiniams santykiams su Užsienio reikalų ministerija, dar kurį laiką gali būti palikta prieiga prie tarnybinio elektroninio pašto. Taip pat nustatyta neatitikčių tarp ministerijos Personalo departamento pateiktų darbuotojų sąrašų ir informacinių sistemų naudotojų sąrašų paskyrų valdymo sistemoje. Naudotojų paskyros yra apsaugotos slaptažodžiais, tačiau jų kompleksiškumo reikalavimai ne visose ministerijos informacinėse sistemose užtikrinami technologinėmis priemonėmis (netikrinamas slaptažodžių ilgis, simbolių skaičius) (3.3 poskyris).

4. Ministerija nepakankamai pasirengė užtikrinti informacinių sistemų veiklos tęstinumą nenumatytų situacijų atveju, nes:

4.1. nenumatyti informacinių sistemų veiklos tęstinumo atkūrimo prioritetai, todėl pirmiausia gali būti atkurti mažiau svarbūs ministerijos veiklos procesai (3.2 poskyris);

4.2. nenurodyti už informacinių technologijų įrangos priežiūrą atsakingi administratoriai, neparengta aktuali informacinių sistemų sąrankos dokumentacija (informacinių technologijų įrangos sąrašai, šios įrangos parametrai, kompiuterių tinklo fizinio ir loginio sujungimo schemos ir kt.), nepildomas duomenų teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašas, duomenų mainų sutartys sudarytos tik su dalimi duomenų teikėjų ir gavėjų, dėl to gali būti susidurta su atsakomybės ir paslaugų teikimo problemomis (3.1 ir 3.2 poskyris);

4.3. nebuvo organizuojamas informacinių sistemų veiklos tęstinumo valdymo plano elementų testavimas ir veiksmingumo išbandymas praktinių mokymų metu, todėl, įvykus incidentui, veiklos tęstinumo valdymo planas gali būti neefektyvus ir realiai neįvykdomas (3.2 poskyris);

4.4. incidento metu aktualūs informacinių sistemų duomenys gali būti neatkurti, nes nenustatytos detalios rezervinio duomenų kopijavimo procedūros, apimančios duomenų kopijavimui skirtus įrenginius, duomenų kopijų tikrinimą ir duomenų atstatymą iš kopijų (3.4 poskyris).

5. Ministerija neįgyvendina organizacinių asmens duomenų tvarkymo automatiniu būdu priemonių, nes:

5.1. ne visi ministerijoje automatiniu būdu tvarkomų asmens duomenų tikslai yra registruoti Asmens duomenų valdytojų valstybės registre, todėl asmenys neturi galimybės susipažinti su išsamia informacija apie savo asmens duomenų tvarkymą (3.4 poskyris);

5.2. nenustatė tvarkomų asmens duomenų saugos lygio, neparengė ir nepatvirtino rašytinės formos dokumento, kuriame būtų išdėstytos taikomos asmens duomenų saugos priemonės, kaip numato Asmens duomenų teisinės apsaugos įstatymas (3.4 poskyris).

6. Informacinės sistemos kurtos ir modernizuotos be detaliųjų reikalavimų, priimti sprendimai nedokumentuoti:

6.1. nepatvirtinti Konsulinių procedūrų valdymo sistemos ir Supaprastinto tranzito dokumentų išdavimo informacinės sistemos nuostatai. Užsienio reikalų ministerijos informacinės sistemos nuostatai patvirtinti, tačiau nebuvo derinami su atitinkamomis institucijomis (1.1 poskyris);

6.2. neparengtos Konsulinių procedūrų valdymo sistemos ir Supaprastinto tranzito dokumentų išdavimo informacinės sistemos specifikacijos, Užsienio reikalų ministerijos informacinės sistemos specifikacija neatnaujinta nuo 1998 m. Taip pat nebuvo rengiami Konsulinių procedūrų valdymo sistemos ir Supaprastinto tranzito dokumentų išdavimo informacinės sistemos modernizavimo detalieji projektai, o Užsienio reikalų ministerijos informacinės sistemos detalusis projektas buvo parengtas tik vienos posistemės modernizavimui. Minėtos sistemos modernizuojamos vadovaujantis tik pirkimo techninė užduotimi. Neatnaujinus ar neparengus informacinės sistemos specifikacijos ir detaliojo projekto prieš informacinės sistemos modernizavimą, kyla rizika, kad modernizuotų sistemų funkcijos neatitiks veiklos poreikių (2.1 poskyris);

6.3. informacinių sistemų testavimas atliekamas specialioje aplinkoje, tačiau ne visuomet sudaromi testavimo planai ir įtraukiami galutiniai vartotojai (2.2 poskyris).

7. Galiojančios Užsienio reikalų ministerijos informacinės sistemos vystymo gairės nėra detalios, jas būtina atnaujinti ir konkretizuoti, kad būtų labiau susietos su aktualiais veiklos poreikiais ir prioritetais (4.2 poskyris).

8. Informacinių sistemų valdymo stebėsenai ir vertinimui vidaus auditoriai neskiria reikiamo dėmesio, o tai sudaro prielaidas galimiems informacinių sistemų valdymo vidaus kontrolės trūkumams atsirasti, be to, nustatyta neatitikčių išorės reikalavimams (4.1 poskyris).

Rekomendacijos

Lietuvos Respublikos užsienio reikalų ministerijai:

1. Sudaryti gerosios praktikos rekomenduojamą veiklos informacijos architektūros modelį, palengvinantį optimalų veiklos informacijos kūrimą, naudojimą ir dalijimąsi ja, išlaikant jos vientisumą (1 išvada).

2. Tobulinti ministerijos informacinių sistemų valdymo organizacinę struktūrą:

2.1. užtikrinti gerosios praktikos rekomenduojamų informacinių technologijų strategijos ir informacinių technologijų valdymo komitetų funkcijų efektyvų vykdymą, parenkant optimalius struktūrinius sprendimus (2.1 išvada);

2.2. paskirti duomenų valdymo įgaliotinius (2.2 išvada);

2.3. planuoti rezervinę darbuotojų pakaitą ir svarbių informacinių technologijų darbuotojų pareigų perėmimą (2.3 išvada).

3. Siekiant užtikrinti ministerijos valdomos informacijos saugą:

3.1. atlikus informacinių sistemų rizikos vertinimą, parengti ir patvirtinti informacinių sistemų rizikos mažinimo (valdymo) priemonių planą (3.1 išvada);

3.2. **Informacinių sistemų duomenų saugos nuostatuose nustatyti ministerijos informacinių sistemų kategorijas ir nurodyti, kokios komponentės jas sudaro** (3.2 išvada)**;**

3.3. peržiūrėti ir atnaujinti duomenų saugą reglamentuojančius dokumentus (Užsienio reikalų ministerijos informacinių sistemų duomenų saugos nuostatus, Naudotojų administravimo taisykles, Saugaus elektroninės informacijos tvarkymo taisykles, Informacinių sistemų veiklos tęstinumo valdymo planą, Informacinių sistemų servisų administratorių sąrašą) (3.3 išvada);

3.4. peržiūrėti ir atnaujinti ministerijoje įslaptintos informacijos tvarkymą (naikinimą, perkėlimą, perdavimą, saugojimą) reglamentuojančias vidaus tvarkas (3.4 išvada);

3.5. **n**ustatyti paskyrų valdymo proceso procedūras ir **v**isose ministerijos informacinėse sistemose įdiegti vartotojų prisijungimo kompleksiškumo reikalavimus užtikrinančias technologines priemones (3.5 išvada).

4. Užtikrinant nenutrūkstamą informacinių sistemų paslaugų teikimą*:*

4.1. nustatyti informacinių sistemų veiklos tęstinumo atkūrimo prioritetus (4.1 išvada);

4.2. testuoti informacinių sistemų veiklos tęstinumo valdymo planą ir periodiškai rengti tęstinumo plano mokymus (4.3 išvada);

4.3. užpildyti informacinių technologijų įrangos sąrašus: nurodyti įrangos parametrus ir už jos priežiūrą atsakingus administratorius, parengti minimalaus funkcionalumo informacinių technologijų įrangos specifikaciją, kiekvieno pastato aukšto patalpų brėžinius ir patalpose esančios įrangos ir komunikacijos, kompiuterių tinklo fizinio ir loginio sujungimo schemas (4.2 išvada);

4.4. nustatyti detaliąsias rezervinio duomenų kopijavimo procedūras, apimančias duomenų kopijavimui skirtus įrenginius, duomenų kopijų tikrinimą, duomenų atstatymą iš kopijų (4.4 išvada);

4.5. užpildyti duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašą, su visais duomenų teikėjais ir gavėjais sudaryti duomenų mainų sutartis (4.2 išvada).

5. Stiprinti asmens duomenų valdymą ir saugą:

5.1. pranešti Valstybinei asmens duomenų apsaugos inspekcijai visus ministerijoje automatiniu būdu tvarkomų asmens duomenų tikslus (5.1 išvada);

5.2. parengti ir patvirtinti rašytinės formos dokumentą, kuriame būtų nurodytas tvarkomų asmens duomenų saugos lygis, išdėstytos organizacinės ir techninės priemonės, skirtos apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo (5.2 išvada).

6. Siekiant, kad informacinių sistemų plėtra atitiktų ministerijos veiklos poreikius:

6.1. peržiūrėti, atnaujinti, išplėsti ir detalizuoti Užsienio reikalų ministerijos informacinės sistemos vystymo gaires (7 išvada);

6.2. nustatyta tvarka patvirtinti Užsienio reikalų ministerijos informacinės sistemos, Konsulinių procedūrų valdymo sistemos ir Supaprastinto tranzito dokumentų išdavimo informacinės sistemos nuostatus (6.1 išvada);

6.3. parengti Konsulinių procedūrų valdymo sistemos, Supaprastinto tranzito dokumentų išdavimo informacinės sistemos specifikacijas, o Užsienio reikalų ministerijos informacinės sistemos specifikaciją – atnaujinti, jas visas nustatyta tvarka suderinti ir patvirtinti. Prieš kuriant naujas ar modernizuojant esamas ministerijos informacines sistemas, atnaujinti arba parengti ir nustatyta tvarka suderinti informacinių sistemų nuostatus, specifikacijas ir detaliuosius projektus (6.2 išvada);

6.4. vidaus tvarkose nustatyti, kad, sukūrus ar modernizavus informacinę sistemą, jos testavimas turėtų būti atliekamas sudarius testavimo planą, o testavimo rezultatus vertintų ir galutiniai informacinės sistemos vartotojai (6.3 išvada).

7. Periodiškai vertinti informacinių sistemų kontrolės valdymą ir atlikti išorės reglamentavimo stebėseną (1.2 išvada).