Valstybinio audito ataskaitos santrauka

POLICIJOS INFORMACINIŲ IŠTEKLIŲ VALDYMAS

2015 m. lapkričio 5 d. Nr. VA-P-90-3-15

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

SANTRUMPOS IR SĄVOKOS

ADA – automatizuoto duomenų apdorojimo informacinė sistema

ATPEĮR – Administracinių teisės pažeidimų ir eismo įvykių registras

BPC – Bendrasis pagalbos centras

BPC IS – Bendrojo pagalbos centro informacinė sistema

COBIT – ISACA[1] sukurta IT valdymo ir vadovavimo metodika

IGR – Ieškomų ginklų registras

INDR – Ieškomų numeruotų ir individualius požymius turinčių daiktų ir dokumentų registras

IRD – Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos

IS – informacinė sistema

IT – informacinės technologijos

ITKG – Informacinių technologijų koordinavimo grupė

ITPR – Ieškomų transporto priemonių registras

IVPK – Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos

NAIS – Nusikalstamumo analizės informacinė sistema

OIS – Operatyvinės veiklos informacinė sistema

PAGD – Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos

PLVIS – Policijos licencijuojamos veiklos informacinė sistema

POLIS – Policijos informacinė sistema

PPV – Policijos pajėgų vienetas

PRĮR – Policijos registruojamų įvykių registras

PVVIS – Prevencinės veiklos valdymo informacinė sistema

SPG – Strateginio planavimo grupė

VPVS – Vieninga pajėgų valdymo sistema

VRIS CDB – Vidaus reikalų ministerijos informacinės sistemos centrinis duomenų bankas

VSAT – Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos

VST – Viešojo saugumo tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos

Kitos šioje ataskaitoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.

[1] ISACA – Information Systems Audit and Control Association. Prieiga per internetą http://www.isaca.org/about-isaca/Pages/default.aspx [Žiūrėta 2015-06-10].

SANTRAUKA

Lietuvos policijos misija - efektyviai naudojant turimus išteklius ginti Lietuvos žmonių teises ir laisves, saugoti visuomenę ir valstybę, padėti žmogui, šeimai ir bendruomenei. Lietuvoje yra dvi policijos dalys: kriminalinė ir viešoji. Tai vientisa policijos organizacija, jos jungiamoji ir vadovaujamoji grandis – Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos.

Pagrindiniai policijos uždaviniai[2]: žmogaus teisių ir laisvių apsauga; viešosios tvarkos ir visuomenės saugumo užtikrinimas; neatidėliotinos pagalbos teikimas asmenims, kai ji būtina dėl jų fizinio ar psichinio bejėgiškumo, taip pat asmenims, nukentėjusiems nuo nusikalstamų veikų, kitų teisės pažeidimų, stichinių nelaimių ar panašių veiksnių; nusikalstamų veikų ir kitų teisės pažeidimų prevencija; nusikalstamų veikų ir kitų teisės pažeidimų atskleidimas ir tyrimas; saugaus eismo priežiūra.

Policijos uždaviniams įgyvendinti būtini duomenys tvarkomi žinybiniuose registruose, informacinėse sistemose, automatizuoto duomenų apdorojimo sistemose ir tinkluose, kuriuose saugoma, apdorojama ir kuriais perduodama įslaptinta informacija. Policijos departamentas yra visų šių informacinių išteklių valdytojas, todėl audito metu pagrindinis dėmesys buvo skirtas departamento veiklai ir veiksmams, užtikrinantiems šių išteklių planavimą ir organizavimą, stebėseną, vertinimą ir koordinavimą, ir kitiems IS ir registrų strateginio valdymo aspektams.

Audituojamas laikotarpis – 2012–2014 m., duomenų analizei buvo naudojami ankstesnių laikotarpių ir 2015 m. duomenys.

Audito tikslas – įvertinti Policijos departamento informacinių išteklių valdymą ir kūrimo kontrolę. Auditą atlikome Policijos departamente. Duomenis ir informaciją rinkome departamento specializuotose ir teritorinėse policijos įstaigose: Lietuvos kriminalinės policijos biure, Lietuvos policijos kriminalistinių tyrimų centre, Vilniaus, Kauno, Alytaus ir kitų apskričių vyriausiuosiuose policijos komisariatuose; VĮ „Regitra“, Greitosios medicinos pagalbos stotyje. Audito procedūras atlikome Priešgaisrinės apsaugos ir gelbėjimo departamente prie Vidaus reikalų ministerijos ir Bendrajame pagalbos centre.

Policijos departamentas investuoja į IT vadovaudamasis bendrąja departamento veiklos strategija ir tikslais, tačiau šiam dokumentui trūksta detalumo aprašant pagrindines IT plėtros kryptis, IS ir registrų steigimo prioritetus, nenurodytos Policijos departamente planuojamos, vykdomos ir įgyvendinamos IT plėtros priemonės: IS, registrų kūrimas ir modernizavimas.

Policijos departamente ir policijos įstaigose sudarytos grupės ir komisijos IT klausimams svarstyti. Joms pavesta nustatyti IT vystymo kryptis, organizuoti, koordinuoti ir kontroliuoti IT plėtrą, informacinio saugumo tikslų nustatymą ir informacinėms vertybėms kylančių grėsmių stebėjimą. Jų veikla epizodiška, nustatytos funkcijos nevykdomos visa apimtimi ir persidengia, todėl neužtikrinama tinkama IT įgyvendinimo, informacinėms vertybėms kylančių grėsmių kontrolė ir stebėsena.

Policijos departamentas ir teritorinės policijos įstaigos periodiškai atlieka darbuotojų duomenų tvarkymo (asmens duomenų peržiūros) teisėtumo ir pagrįstumo patikrinimus, bendradarbiauja su Valstybine duomenų apsaugos inspekcija. Neteisėto policijos duomenų bazių naudojimo rizika nepakankamai valdoma Lietuvos kriminalinė policijos biure.

[2] Lietuvos Respublikos policijos veiklos įstatymas, 2000-10-17 Nr. VIII-2048, 5 str.

Siekiant užtikrinti darnią Policijos departamento IT plėtrą ir indėlį įgyvendinant policijos tikslus ir uždavinius, rekomendavome parengti ir patvirtinti IT strategiją ir jos pagrindu sukurti ir nuolatos atnaujinti IT plėtros planus. Siekiant aiškios atsakomybės už strateginius sprendimus ir tinkamo požiūrio į IT valdymą, rekomendavome peržiūrėti Policijos departamente ir policijos įstaigose sudarytų grupių ir komisijų, kurioms pavesta svarstyti IT klausimus, veiklą, atskirti jų funkcijas, užtikrinti grupių veiklos tęstinumą, pavestų funkcijų vykdymą ir atskaitomybę. Taip pat Policijos departamentas turėtų skirti daugiau dėmesio sistemų saugos ir veiklos tęstinumo užtikrinimui bei sistemingam IT projektų valdymui.

Įvertinę surinktus įrodymus, teikiame valstybinio audito išvadas ir rekomendacijas.

IŠVADOS

1. Policijos departamente įgyvendinant policijos tikslus ir uždavinius trūksta nuoseklaus ir subalansuoto IT planavimo ir vystymo, nes strateginio planavimo dokumentuose nenurodytos pagrindinės IT plėtros kryptys, planuojamos kurti ar modernizuoti valstybės IS ir registrai, jų steigimo prioritetai (1.1 poskyris, 11 psl.).
2. Policijos departamentas neturi bendro informacijos architektūros modelio, apibrėžiančio departamento ir policijos įstaigų valdomą (sukuriamą) informaciją, jos klasifikavimo kriterijus, IS/registrų duomenų ir technologinę architektūrą, todėl neaiški Policijos departamento IS ir registrų tarpusavio sąveika, departamente ir policijos įstaigose valdomos informacijos svarba ir jautrumas tokios informacijos viešinimui, perdavimui ir atskleidimui (1.2 poskyris, 13 psl.).
3. Policijos departamentas neužtikrina teisės aktuose ir procedūrose nustatytų reikalavimų dėl informacinių išteklių saugos ir duomenų valdymo:
   3.1. Policijos departamente patvirtinta tvarka, nustatanti galimų grėsmių ir rizikos veiksnių policijos IS analizavimo, stebėjimo ir vertinimo procedūras, bet jos nesilaikoma, neatliekami saugos atitikties vertinimai teisės aktų nustatytu periodu, todėl netaikomos tinkamos kontrolės priemonės nustatytai rizikai valdyti, neįsitikinama, ar parinktos pakankamos saugos priemonės ir nevertinama, kaip jų laikomasi (1.3 poskyris, 14 psl.).
   3.2. Policijos departamente neatliekami duomenų atkūrimo bandymai iš atsarginių duomenų kopijų, duomenų kopijos saugomos toje pačioje patalpoje kaip ir tarnybinės stotys, o ši patalpa neturi automatinės gaisro gesinimo sistemos, todėl saugos incidento atveju gali būti negrįžtamai sugadinta techninė ir programinė tarnybinių stočių įranga, prarasti aktyviose IS duomenų bazėse esantys duomenys, o kartu ir šių duomenų kopijos (1.3. 1.4 poskyriai, 14,17 psl.).
   3.3. Policijos departamentas neįsitikino, ar yra pasiruošęs atkurti valdomų IS ir registrų veiklą per laikotarpį, kuris neturėtų neigiamos įtakos departamento ir susijusių institucijų funkcijų įgyvendinimui, nes departamento veiklos tęstinumo valdymo planas neatnaujintas ir neišbandytas (1.3 poskyris, 15 psl.).
   3.4. Policijos departamentas įgyvendina ne visas technines ir organizacines asmens duomenų saugumo priemones tvarkant duomenis automatizuotu būdu, neorganizuoja mokymų duomenų tvarkymo teisėtumo ir informacijos saugos klausimais, todėl tvarkant duomenis neužtikrinamas elektroninės informacijos konfidencialumas ir asmens duomenų apsauga nuo atsitiktinio ar neteisėto sunaikinimo, atskleidimo (1.3, 1.4 poskyriai, 15, 18 psl.).

4. Išvados dėl automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ir kuriais perduodama įslaptinta informacija, valdymo ir šios informacijos apsaugos pateiktos atskiru raštu (įslaptinta) (1.5 poskyris, 18 psl.).
5. Policijos departamente nepatvirtinta IT pokyčių valdymo tvarka, netaikoma praktika, kad visi IT pokyčiai būtų vieningai ir standartizuotai užsakomi, pagrindžiant pokyčio reikalingumą ir naudą, nurodant pokyčio prioritetą, suskirstant juos į kategorijas pagal pokyčio tipus, todėl departamente eikvojami papildomi laiko ištekliai vertinant ir apibendrinant pateiktų IT pokyčių tikslingumą ir pagrįstumą (1.6 poskyris, 18,19 psl.).
6. Policijos departamento vidaus auditoriai nestebi ir nevertina informacinių išteklių valdymo, o tai sudaro prielaidas atsirasti galimiems informacinių sistemų valdymo vidaus kontrolės trūkumams, be to, nustatyta neatitikčių išorės reikalavimams (1.7 poskyris, 20 psl.).
7. IT valdymo organizacinė struktūra tobulintina: departamente ir policijos įstaigose sudarytos grupės ir komisijos, kad pagrindinės veiklos poreikiai būtų siejami su IT teikiamomis galimybėmis, tačiau ne visos grupės ir komisijos vykdo pavestas funkcijas visa apimtimi, grupių ir komisijų veikla nereguliari (epizodiška), todėl neužtikrinama tinkama IT įgyvendinimo kontrolė ir kylančių grėsmių stebėsena (1.8 poskyris, 20, 21 psl.).
8. Policijos departamente taikomi projektų valdymo principai neužtikrino VPVS projekto kokybės ir rizikų valdymo, nes:
   8.1. VPVS modernizuota nesilaikant teisės aktų reikalavimų: privaloma dokumentacija – VPVS nuostatai ir specifikacija – patvirtinti po projekto įgyvendinimo, baigus VPVS modernizacijos etapą nepatvirtintas VPVS perdavimo–priėmimo aktas (2.1, 2.2 poskyriai, 24, 28 psl.).
   8.2. Įgyvendinant VPVS modernizavimo projektą nesudarytas integruotas VPVS projekto valdymo planas, kuris apimtų laiko, finansinius, žmogiškuosius išteklius, sudėtinių projekto veiklų ir susijusių projektų sąlyčio taškus ar tarpusavio ryšius, todėl buvo netinkamai nustatyti IS projekto sudėtinių dalių atlikimo terminai ir iki kritinės ribos (20 kalendorinių dienų) sumažėjo VPVS funkcijų tobulinimo terminai (2.1 poskyris, 24 psl.).
   8.3. VPVS projekto įgyvendinimą koordinavusi Vidaus reikalų ministerija nesudarė sąlygų patikimam duomenų keitimuisi tarp Policijos departamento ir Bendrojo pagalbos centro, todėl buvo sukurta tik vienkryptė sąsaja tarp PRĮR, VPVS ir BPC IS (2.1 poskyris, 25 psl.).
   8.4. Nesilaikoma nustatyto vykdomų projektų kontrolės mechanizmo, VPVS programinės įrangos tobulinimo darbai buvo vykdomi skubotai, testavimo, mokymo organizavimo ir rezultatų priėmimo eiga buvo nenuosekli, neatlikta VPVS bandomoji eksploatacija ir projekto rezultatų peržiūra, todėl neįsitikinta sklandžiu sukurtų funkcijų veikimu esant realioms IS eksploatavimo sąlygoms, o baigus projektą – jo rezultatyvumu, ar sukurtos VPVS programinės įrangos funkcijos naudojamos (2.1, 2.2 poskyriai, 24, 26, 27 psl.).

   Rekomendacijų įgyvendinimo planas pateiktas 2 priede.

REKOMENDACIJOS

1. Siekiant nuoseklaus ir kryptingo IS ir registrų tobulinimo ir atsižvelgiant į visos organizacijos veiklos poreikius, parengti ir patvirtinti IT strategiją ir jos pagrindu sukurti bei nuolatos atnaujinti IT plėtros planus (1 išvada).
2. Sudaryti informacijos architektūros modelį, apimantį Policijos departamento ir policijos įstaigų valdomos informacijos, IS/registrų duomenų bei technologinę architektūrą, nurodant

kiekvienos sudedamosios dalies komponentus (naudojamos technologijas, duomenis, duomenų srautus tarp išorinių ir vidinių IS) (2 išvada).

3. Siekiant užtikrinti valdomų informacinių išteklių saugą:
   3.1. Atlikti visų Policijos departamento valdomų informacinių išteklių periodišką saugos atitikties vertinimą ir užtikrinti nustatytų trūkumų šalinimo kontrolę (3.1 išvada).
   3.2. Tobulinti rizikos valdymo procesą, laikytis departamento galimų grėsmių ir rizikų policijos IS analizavimo, stebėjimo ir vertinimo procedūrų aprašo ir užtikrinti nustatytos rizikos mažinimo priemonių įgyvendinimą (3.1 išvada).
   3.3. Suderinti atsarginių duomenų kopijų saugojimo bei duomenų atkūrimo tvarką ir planus su Vidaus reikalų ministerija, atsižvelgiant į Valstybės informacinių išteklių infrastruktūros konsolidavimo darbų sąrašą (3.2 išvada).
   3.4. Atnaujinti departamento IS veiklos tęstinumo valdymo planą ir jį išbandyti (3.3 išvada).
   3.5. Periodiškai organizuoti darbuotojų mokymus duomenų tvarkymo teisėtumo ir informacijos saugos klausimais (3.4 išvada).
   3.6. Pranešti Valstybinei duomenų apsaugos inspekcijai apie departamento valdomuose informaciniuose ištekliuose automatiniu būdu tvarkomus asmens duomenis ir jų tvarkymo tikslus, kad būtų atnaujinta Asmens duomenų valdytojų registre esanti informacija (3.4 išvada).
   3.7. Peržiūrėti ir atnaujinti IS ir registrų duomenų tvarkymo taisykles: jose išdėstyti taikomos asmens duomenų saugos priemones taip, kaip nustato Asmens duomenų teisinės apsaugos įstatymas (3.4 išvada).
4. Rekomendacijos dėl automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ir kuriais perduodama įslaptinta informacija, valdymo ir šios informacijos apsaugos pateiktos atskiru raštu (įslaptinta) (4 išvada).
5. Siekiant veiksmingo ir sistemingo pokyčių valdymo, peržiūrėti taikomą pokyčių valdymo procesą ir nustatyti (patvirtinti) IT pokyčių valdymo tvarką, kurioje būtų reglamentuotas IT pokyčių valdymo planavimas ir užtikrinta šios tvarkos laikymosi (vykdymo) kontrolė (5 išvada).
6. Periodiškai stebėti ir vertinti informacinių sistemų ir registrų vidaus kontrolės būklę (6 išvada).
7. Peržiūrėti Policijos departamente ir policijos įstaigose sudarytų grupių ir komisijų, kurioms pavesta svarstyti IT klausimus, veiklą, aiškiai atskirti jų funkcijas, užtikrinti jų veiklos tęstinumą ir pavestų funkcijų vykdymą (7 išvada).
8. Siekiant užtikrinti IT projektų kokybę ir projektų rizikos valdymą:
   8.1. Peržiūrėti ir atnaujinti Policijos departamente taikomus IT projektų valdymo principus, numatant, kad būtų sudaromas integruotas projekto įgyvendinimo planas. Pagal šį planą viso projekto gyvavimo ciklo metu organizuojamas projektų įgyvendinimas ir kontrolė, o apie nuokrypius nuo plano informuojamos už įgyvendinimo kontrolę atsakingos struktūros (8.2, 8.3, 8.4 išvados).
   8.2. Parengti ir patvirtinti valdomų informacinių išteklių nuostatus bei specifikacijas ir įteisinti naudojamas sistemas ir registrus (8.1 išvada, 4 priedas).