LIETUVOS RESPUBLIKOS VALSTYBĖS KONTROLĖ

VALSTYBINIO AUDITO ATASKAITA AKCINĖS BENDROVĖS RYTŲ SKIRSTOMŲJŲ TINKLŲ INFORMACINĖS SISTEMOS BENDROSIOS KONTROLĖS VERTINIMAS

2007 m. gruodžio 20 d. Nr. IA-9000-8-5
Vilnius

Auditas atliktas, vykdant
Valstybės kontrolės Informacinių technologijų valdymo ir audito departamento
direktoriaus Dainiaus Jakimavičiaus
2007-06-28 pavedimą Nr. 9000-8

Auditą atliko valstybiniai auditoriai:
Rimgaudas Gamulis (grupės vadovas)
Viktorija Mirošničenko

Auditas pradėtas 2007-07-02
Auditas baigtas 2007-12-20

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

TURINYS

SANTRAUKA

Akcinė bendrovė Rytų skirstomieji tinklai (toliau – RST) įtraukta į nacionaliniam saugumui užtikrinti svarbių įmonių sąrašą[1]. RST eksploatuojamos informacinės sistemos ir kai kurių jos posistemių duomenų konfidencialumo, vientisumo ir (ar) prieinamumo praradimas gali turėti sunkių padarinių bendrovės darbui ir (arba) turėti neigiamą įtaką kitų valstybės institucijų ir įstaigų veiklai. Įstatyme[2] paminėtoms ir Lietuvos Respublikos ūkio ministerijos (toliau – Ūkio ministerija) valdymo sričiai priskirtoms nacionaliniam saugumui užtikrinti svarbioms įmonėms kituose teisės aktuose yra detalizuoti informacijos[3] ir fizinės saugos[4] reikalavimai.

RST privalo informacinę ir fizinę saugą organizuoti ir vykdyti vadovaudamiesi Lietuvos Respublikos teisės aktų reikalavimais, kurie įpareigoja bendrovę diegti efektyvias saugos priemones ir užtikrinti tinkamą valdomos informacijos apsaugą.

Valstybinio audito ataskaitą sudaro trys dalys. Pirmoje dalyje pateikiamas RST informacinės sistemos strateginis valdymas, jos posistemių valdymo ir organizavimo procesai, parodoma kaip jie įgyvendinami praktikoje. Valstybiniai auditoriai nustatė, kad nors Lietuvos Respublikos teisės aktai[5] nereglamentuoja akcinių bendrovių informacinių sistemų strateginių planų rengimo ir strateginių planų priemonių įgyvendinimo kontrolės, RST atnaujinta ir vadovybės patvirtinta bendrovės informacinių sistemų vystymo strategija bei sudarytas jos įgyvendinimo planas laikotarpiui iki 2009 m. Kita vertus, RST nebuvo dokumentuota bendrovės informacinių sistemų strategiją įgyvendinančių dokumentų peržiūros tvarka ir periodiškumas, nesudarytas informacinių technologijų (toliau – IT) komitetas ir nepaskirti informacinių sistemų valdytojai, kaip nurodoma pasaulyje pripažintoje gerojoje praktikoje (1.1 ir 1.2 dalys).

Vadovaujantis valstybinių auditorių atlikta analize ataskaitos pirmoje dalyje vertinami RST informacinės sistemos rizikos valdymo procesai, informacijos saugos politikos ir informacinių sistemų valdymo bei saugos organizavimo principai ir procedūros. Audituojamu laikotarpiu RST saugos valdymas apėmė visą bendrovės kompiuterizuotą informaciją, tačiau RST vadovybė nebuvo patvirtinusi saugumo politikos ir kai kurių ją įgyvendinančių dokumentų, neatliktas formalus

[1] Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas, 2002-10-10 Nr. IX-1132, 4 str. 1 d.
[2] Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas, 2002-10-10 Nr. IX-1132.
[3] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymas Nr. 4-349 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimų patvirtinimo“.
[4] Lietuvos Respublikos ūkio ministro 2004-09-15 įsakymas Nr. 4-334 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių fizinės saugos reikalavimų patvirtinimo“.
[5] Lietuvos Respublikos akcinių bendrovių įstatymas, 2000-07-13 Nr. VIII-1835.

bendrovės informacinės sistemos rizikos vertinimas. Pažymėtina, kad valstybinio audito metu (2007-11-16) RST pasirašyta sutartis[6] diegti bendrovės informacijos saugumo valdymo sistemą vadovaujantis *LT ISO/IEC 27001:2006* standartu[7]. Projekto pirmajame etape numatyta sukurti RST saugos procesų taikymo sritis ir ribų aprašą, saugos politiką, rizikos vertinimo metodiką ir atlikti rizikos analizę, parengti rizikų priežiūros ir antrojo etapo darbų planus. Taip RST siekia pagerinti informacijos saugumo valdymą, įdiegdama informacijos saugumo valdymo sistemą vadovaujantis *LT ISO/IEC 27001:2006* standartu (1.3, 1.4 dalys).

Ataskaitos pirmoje dalyje taip pat nagrinėjamos RST galiojančios IT dokumentacijos normos, bendrovės informacinio turto kontrolės sistema ir aprašomi nustatyti jos trūkumai. Valstybiniai auditoriai pastebi, kad audituojamu laikotarpiu ne visi RST informacinės sistemos valdymo ir informacijos saugos procesai buvo reglamentuojami atskiromis tvarkomis ir tai neapėmė visų teisės aktuose numatytų būtinų sričių. Dalies RST reikalingų informacinių sistemų ir informacinės saugos kontrolės procedūrų oficialiai nebuvo patvirtinusi vadovybė, tačiau bendrovės IT skyriaus specialistai turi žinių ir neformaliai taiko pasaulyje pripažintas IT valdymo ir saugos gerąsias praktikas (1.5 dalis).

Ataskaitos pirmos dalies paskutiniame skyriuje nagrinėjami RST informacinės saugos ir fizinės saugos auditai ir su jais susijusios pažangos stebėjimo (poauditinės veiklos) valdymo procesai. RST dokumentų analizė rodo, kad bendrovėje iki valstybinio audito pradžios buvo atlikti trys specializuoti informacinių sistemų saugos auditai, kuriuos atliko įmonės, atitinkančios teisės aktų reikalavimus[8]. Šių auditų metu peržiūrėtas reikalavimų informaciniam saugumui įgyvendinimas, siekiant įsitikinti, ar RST praktika tinkamai atspindi informacinės saugos principus, ar ji yra tinkamai vykdoma, ir pateiktos rekomendacijos. Kita vertus, audituojamu laikotarpiu bendrovėje nebuvo atliekami periodiniai vidiniai informacijos saugos auditai ir nepakankamai vykdomi su informacinių sistemų auditais susijusios pažangos stebėjimo (poauditinės veiklos) valdymo procesai, rekomendacijų įgyvendinimo kontrolė (1.6 dalis).

Ataskaitos antroje dalyje valstybiniai auditoriai vertino RST informacinės sistemos atitiktį Lietuvos Respublikos teisės aktų reikalavimams ir rekomendacijoms. RST informacijos ir fizinės[9] saugos valdymas ir tvarkymas atitinka teisės aktų reikalavimus arba rekomendacijas, išskyrus valstybinio audito ataskaitos 3 priedo 1 ir 2 lentelėse nurodytus pastebėjimus (2 dalis).

[6] AB Rytų skirstomųjų tinklų ir UAB „Blue Bridge“ 2007-11-16 sutartis Nr. 10530/471286.
[7] *LT ISO/IEC 27001:2006* Lietuvos standartas. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai (tapatus *ISO/IEC 27001:2005*).
[8] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymas Nr. 4-349 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimų patvirtinimo“.
[9] Lietuvos Respublikos ūkio ministro 2004-09-15 įsakymu Nr. 4-334 patvirtinti strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių fizinės saugos reikalavimai vertinti tik tiek, kiek jie susiję su RST informacijos sauga.

Ataskaitos trečioje dalyje įvertintas RST informacinės sistemos valdymas ir nustatytas jos valdymo brandos lygis. RST informacinės sistemos vidaus kontrolės branda apibrėžiama kaip 1. Pirminis / *Ad Hoc* procesas (3 dalis).

Valstybiniai auditoriai rekomendavo tobulinti RST informacinės sistemos valdymo procesus. Valstybinio audito išvados ir valstybinių auditorių rekomendacijos pateiktos 30 puslapyje.

Tikimės, kad valstybinių auditorių pateiktos rekomendacijos RST sukurs pridėtinę vertę, t. y. pagerins jos informacijos valdymą ir saugą, padės pašalinti vidaus kontrolės trūkumus ir padidins vidaus kontrolės procedūrų efektyvumą ir veiksmingumą.

Apie pastebėtus trūkumus, susijusius su strateginę reikšmę nacionaliniam saugumui turinčių svarbių įmonių informacinės ir fizinės saugos reglamentavimu ir reikalavimų vykdymu, atskiru raštu bus informuota Lietuvos Respublikos Vyriausybė ir Ūkio ministerija.

ĮŽANGA

Informacinių sistemų bendrosios kontrolės vertinimas (ribotos apimties finansinis auditas) RST buvo numatytas Valstybės kontrolės 2007 m. valstybinio audito programoje. Minėtas auditas į šią programą įtrauktas atsižvelgiant į strateginio tyrimo rezultatus. Atlikto valstybinio audito rezultatai gali būti panaudoti ateityje vertinant Lietuvos Respublikos kritinės informacinės infrastruktūros saugos problematiką arba atliekant kitus auditus šioje bendrovėje.

Valstybinis auditas pradėtas 2007 m. liepos 2 d., baigtas 2007 m. gruodžio 20 d. Tyrimą atliko valstybinis auditorius Rimgaudas Gamulis (grupės vadovas) ir vyresnioji valstybinė auditorė Viktorija Mirošničenko. Audituojamas laikotarpis – nuo 2006 m. sausio 2 d. iki 2007 m. spalio 1 d. Ankstesni RST veiklos laikotarpiai nagrinėti tiek, kiek jie susiję su tuo metu bendrovėje vykdytų informacinių sistemų auditų rekomendacijų įgyvendinimu. Valstybinio audito ataskaitoje pateikiama audito metu RST padaryta pažanga valdant informacines sistemas.

Valstybinio audito metu nustatytus pastebėjimus suskirstėme į kategorijas pagal rizikos lygį:

Rizika

Didelė rizika – tai vienas ar keli informacinių sistemų valdymo trūkumai, dėl kurių akcinė bendrovė, valstybė ir (arba) piliečiai gali patirti reikšmingų finansinių nuostolių, todėl šie trūkumai turėtų būti nedelsiant pašalinti.

Rizika

Vidutinė rizika – tai su akcinės bendrovės vidaus kontrolės sistema susiję reikšmingi trūkumai, į kuriuos nedelsiant turėtų būti atkreiptas atitinkamo lygio institucijos vadovų dėmesys.

Rizika

Nedidelė rizika – tai trūkumai, kurie akcinei bendrovei gali turėti netiesioginę ir nedidelę įtaką priimant informacinių sistemų valdymo ir finansinius sprendimus, tačiau kuriuos reikia šalinti.

AUDITO APIMTIS IR PROCESAS

Audito objektas – Informacinių sistemų bendrosios kontrolės vertinimas.

RST naudojama ši informacinė sistema:

- Rytų skirstomųjų tinklų informacinė sistema, kurią sudaro 43 eksploatuojamos ir diegiamos posistemės. RST naudojamos ir diegiamos Rytų skirstomųjų tinklų informacinės sistemos posistemės išsamiau aprašytos 4 priede.

Valstybinio audito metu nebuvo nagrinėjama RST informacinės sistemos infrastruktūros dalis, kuriai priklauso *SCADA* (angl. *Supervisory control and data acquisition*)[10] ir su ja tiesiogiai susijusios sistemos bei kompiuteriniai tinklai, skirti elektros skirstomojo tinklo valdymui. Dėl šios priežasties valstybiniai auditoriai nevertino RST atliktų auditų rekomendacijų įgyvendinimo peržiūros, susijusios su *SCADA* sistemų ir kompiuterinių tinklų sauga.

Valstybiniai auditoriai, vertindami RST informacinių sistemų valdymo ir saugos procedūras, atsižvelgė į tai, kad bendrovėje iki valstybinio audito pradžios buvo atlikti trys specializuoti informacinių sistemų saugos auditai, kurių metu nagrinėti klausimai ir pateiktos rekomendacijos, susijusios su RST informacinių sistemų valdymo ir saugos procedūromis.

Audito subjektas – akcinė bendrovė Rytų skirstomieji tinklai.

Audito tikslas – atlikti ribotos apimties finansinį auditą – įvertinti informacinių sistemų bendrąją kontrolę ir pateikti rekomendacijas.

Valstybinio audito metu nagrinėta RST informacinės sistemos bendroji kontrolė ir jos atitiktis teisės aktams.

RST informacinės sistemos bendrosios kontrolės vertinimas buvo atliekamas, siekiant įvertinti bendrovės informacinių sistemų bendrosios kontrolės brandą. Tikimasi, kad valstybinio audito metu pateiktos rekomendacijos RST sukurs pridėtinę vertę, t. y. pagerins jos informacijos valdymą ir saugą.

Vertinimo kriterijai

RST bendroji kontrolė įvertinta taikant gebos brandos modelį (2 priedas).

[10] *SCADA* (*Supervisory control and data acquisition*) – AB Rytų skirstomųjų tinklų automatizuotos dispečerinio valdymo sistemos, kurios stebi ir valdo bendrovės elektros skirstomojo tinklo sistemas.

Audito procesas

Valstybinio audito metu vadovautasi Valstybinio audito reikalavimais[11], Informacinių sistemų audito metodinėmis rekomendacijomis[12], Tarptautinės aukščiausiųjų audito institucijų organizacijos (toliau – *INTOSAI*) audito standartų įgyvendinimo Europoje gairėmis[13], Informacinių sistemų audito ir kontrolės asociacijos (angl. *ISACA*) Tarptautiniais audito standartais, atsižvelgta į *ISACA* Audito gaires ir gerąją praktiką.

Valstybiniam auditui reikalingi duomenys buvo renkami bendraujant su RST ir Ūkio ministerijos Energetikos departamento Elektros ir šilumos skyriaus darbuotojais, stebint, tikrinant, analizuojant dokumentus ir kitų auditorių ataskaitas.

Valstybinis auditas buvo atliekamas darant prielaidą, kad visi auditoriams pateikti dokumentai yra išsamūs ir galutiniai, o dokumentų kopijos atitinka originalus.

RST nuomonė valstybinio audito ataskaitoje pateikta pasvirusiu šriftu.

[11] Lietuvos Respublikos valstybės kontrolieriaus 2006-02-01 įsakymas Nr. V-15 „Dėl valstybės kontrolieriaus 2002 m. vasario 21 d. įsakymu Nr.V-26 patvirtintų valstybinio audito reikalavimų pakeitimo“.
[12] Lietuvos Respublikos valstybės kontrolieriaus 2006-04-26 įsakymas Nr. V-65 „Dėl informacinių sistemų audito metodinių rekomendacijų patvirtinimo“.
[13] *INTOSAI* audito standartų įgyvendinimo Europoje gairės. Nr. 22 Informacinių sistemų auditas. Lietuvos Respublikos valstybės kontrolė, 1999 Vilnius.

AUDITO REZULTATAI

1. INFORMACINIŲ SISTEMŲ BENDROSIOS KONTROLĖS VERTINIMAS

1.1. Informacinių sistemų strategija

Lietuvos Respublikos teisės aktai[14] nereglamentuoja akcinių bendrovių informacinių sistemų strateginių planų rengimo ir strateginio valdymo organizavimo. Rengdamos šiuos planus akcinės bendrovės vadovaujasi savo patirtimi, bendrovės įstatais ir veiklos strategija.

RST 2006 m. patvirtintos AB Rytų skirstomųjų tinklų grupės 2006–2010 m. veiklos strateginės kryptys[15]. Dokumente nustatyti:

- AB Rytų skirstomųjų tinklų grupės vystymosi ilgalaikiai tikslai;
- veiksniai, sąlygojantys AB Rytų skirstomųjų tinklų ilgalaikių tikslų pasiekimą;
- uždaviniai, veiksmai, atsakingi asmenys bei terminai, sąlygojantys ilgalaikių AB Rytų skirstomųjų tinklų tikslų įgyvendinimą.

RST informacinių sistemų vystymo strategija suformuota 2002 m.[16] Jos pagrindu pradėta diegti RST informacinė sistema. Nuo informacinių sistemų vystymo strategijos suformavimo 2002 m. RST įvyko esminių pokyčių, todėl 2005 m. atlikta bendrovės verslo poreikių analizė ir atnaujinta bendrovės informacinių sistemų vystymo strategija[17]. RST Informacinių sistemų vystymo strateginis planas (toliau – IS vystymo strateginis planas) patvirtintas 2007 m. liepos 5 d. laikotarpiui iki 2009 m.[18]

Geroji praktika

> RST atnaujinta ir vadovybės patvirtinta bendrovės informacinių sistemų vystymo strategija ir sudarytas jos įgyvendinimo planas laikotarpiui iki 2009 m.

[14] Lietuvos Respublikos akcinių bendrovių įstatymas, 2000-07-13 Nr. VIII-1835.
[15] AB Rytų skirstomųjų tinklų valdybos 2006-05-15 protokolu Nr. 7 patvirtintos RST grupės 2006–2010 m. veiklos strateginės kryptys.
[16] AB Rytų skirstomųjų tinklų informacinės sistemos strateginis planas, pateiktas AB „Alna“ 2002-10-23.
[17] AB Rytų skirstomųjų tinklų informacinės sistemos vystymo strateginio plano patikslinimas, pateiktas AB „Alna“ 2005-09-19.
[18] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-07-05 įsakymas Nr. 98 „Dėl bendrovės informacinių sistemų vystymo strateginio plano patvirtinimo“.

Valstybiniai auditoriai, nagrinėdami RST grupės veiklos[19] ir bendrovės informacinių sistemų vystymo strateginę dokumentaciją[20], neaptiko aiškių šių dokumentų tarpusavio sąsajų ir suderinamumo. RST grupės veiklos[21] strategija patvirtinta anksčiau negu bendrovės informacinių sistemų vystymo strateginiai dokumentai[22]. Pasaulinė praktika[23] rodo, kad organizacijos IT ir veiklos strategijos efektyvumą ir tinkamumą sąlygoja glaudi šių strategijų tarpusavio sąveika, kuria vadovaujantis būtų orientuojamas organizacijos darbas.

Rizika

RST nebuvo užtikrinta aiški RST grupės 2006–2010 m. veiklos strateginių krypčių ir bendrovės informacinių sistemų vystymo strategijos sąveika, todėl yra rizika, kad informacinių sistemų vystymo strategija gali neatitikti būsimų bendrovės veiklos poreikių.

RST IT skyriaus viršininkas bendrovėje paskirtas[24] atsakingu už IS vystymo strateginio plano įgyvendinimą ir jo reikalavimų taikymą diegiant ir plėtojant bendrovėje informacines sistemas. RST padalinių vadovams, įgyvendinant įvairias IT priemones, savo veikloje nurodyta vadovautis patvirtintu IS vystymo strateginiu planu[25].

Bendrovės vadovybė 2007 m. liepos mėn. įsakymu patvirtino[26] 2005 m. redakcijos RST informacinių sistemų vystymo strateginį planą ir nustatė atsakingus asmenis už šio plano įgyvendinimą.

RST informacinių sistemų vystymo strateginiame plane bendrovės informacinės sistemos plėtrą planuojama įgyvendinti atskirais etapais, priklausomai nuo RST finansinių galimybių, tačiau išlaikant bendrą sistemos pagrindą, užtikrinantį informacinį, programinį ir technologinį integralumą[27]. Plėtodama RST informacinę sistemą, bendrovė 2007–2009 m. numatė įgyvendinti projektus, reikalingus sėkmingai RST veiklai užtikrinti (5 priedas).

[19] AB Rytų skirstomųjų tinklų valdybos 2006-05-15 protokolu Nr. 7 patvirtintos RST grupės 2006–2010 m. veiklos strateginės kryptys.
[20] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-07-05 įsakymas Nr. 98 „Dėl bendrovės informacinių sistemų vystymo strateginio plano patvirtinimo“.
[21] AB Rytų skirstomųjų tinklų valdybos 2006-05-15 protokolu Nr. 7 patvirtintos RST grupės 2006–2010 m. veiklos strateginės kryptys.
[22] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-07-05 įsakymas Nr. 98 „Dėl bendrovės informacinių sistemų vystymo strateginio plano patvirtinimo“.
[23] *COBIT (Control Objectives for Information and related Technologies*) – viena iš populiariausių IT valdymo metodologijų, kuriama ir palaikoma tarptautinės *ISACA* organizacijos.
[24] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-07-05 įsakymo Nr. 98 „Dėl bendrovės informacinių sistemų vystymo strateginio plano patvirtinimo“ 2 p.
[25] Ten pat, 3 p.
[26] Ten pat, 1 p.
[27] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-07-05 įsakymu Nr. 98 patvirtintas Informacinių sistemų vystymo strateginis planas.

Valstybiniai auditoriai atliko RST informacinių sistemų vystymo strateginiame plane[28] numatytų priemonių įgyvendinimo rezultatų patikrą. Atlikus patikrą nustatyta, kad iš 10 iki 2007 m. spalio 1 d. planuotų įdiegti RST informacinės sistemos posistemių, 2 įdiegtos anksčiau negu planuota, 4 diegti buvo vėluojama, 4 – nukeltos į 2008 m. (1 lentelė).

1 lentelė. RST informacinės sistemos diegimo faktiniai rezultatai (2007 m. spalio mėn. duomenys)

Eil. Nr.	Posistemės	Planuota darbų pabaiga	Diegimo faktiniai rezultatai
1.	Tinklo eksploatavimo ir valdymo (TEVIS) informacinė posistemės II etapas:	2006-03-21	**2006-06-30**
2.	GIS informacinė posistemė	2007-01-16	**2008-07**
3.	Interneto svetainės (WEB SVETAINĖ) posistemė	2006-05-24	**2006-07**
4.	Elektros energijos vartotojų (aptarnavimo internetinis portalas) (EEVIS) informacinė sistema	2006-08-28	**2007-03**
5.	Saugos darbe ir nelaimingų atsitikimų prevencijos (SAUGA) informacinė posistemė	2007-01-02	**2008-02**
6.	Vidinio portalo RYTIS (RYTIS) informacinė posistemė	2007-04-04	**2007-03**
7.	Personalo ir darbo užmokesčio apskaitos (PERSONALAS DU) informacinė posistemė	2007-08-21	**2007-05**
8.	Netechnologinio turto valdymo (TURTAS) informacinė posistemė	2006-06-01	**2008**
9.	Call centro (CALL) informacinė posistemė (Integracija DW)	2006-11-07	**2007-04**
10.	Analizės ir prognozės (DW) informacinė posistemė	2007-05-14	**2008**

Įvykdyta anksčiau nei planuota.

Įvykdymas nukeltas.

Įvykdyti vėluojama.

Šaltinis – Valstybės kontrolė

Rizika

Audituojamu laikotarpiu RST vadovybė neformalizavo informacinių sistemų vystymo strateginio plano įgyvendinimo kontrolės.

Nedokumentuota bendrovės informacinių sistemų vystymo strateginio plano peržiūros tvarka ir periodiškumas, todėl yra rizika, kad bendrovės informacinių sistemų vystymo strategijos įgyvendinimas vėluos ir neatitiks nustatytų planų.

Dalis informacinių sistemų vystymo strateginio plano nuostatų jau neatitinka tikrovės.

RST rašte[29] teigiama, kad *informacinių sistemų strateginiuose planuose numatyti preliminarūs posistemių diegimo terminai buvo tikslinami kasmetiniuose bendrovės investiciniuose planuose, kurių vykdymas buvo kontroliuojamas.*

[28] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-07-05 įsakymas Nr. 98 „Dėl bendrovės informacinių sistemų vystymo strateginio plano patvirtinimo“.

[29] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-12-20 raštas Nr. 10530-1221 „Dėl pastabų valstybinio audito ataskaitos projektui“.

Valstybinių auditorių nuomone, nors minėta informacinių sistemų strateginių planų peržiūra yra pažangi priemonė, tačiau tai negali atstoti formalios ir dokumentuotos bendrovės informacinių sistemų vystymo strateginio plano peržiūros tvarkos.

1.2. Informacinių sistemų valdymas ir organizavimas

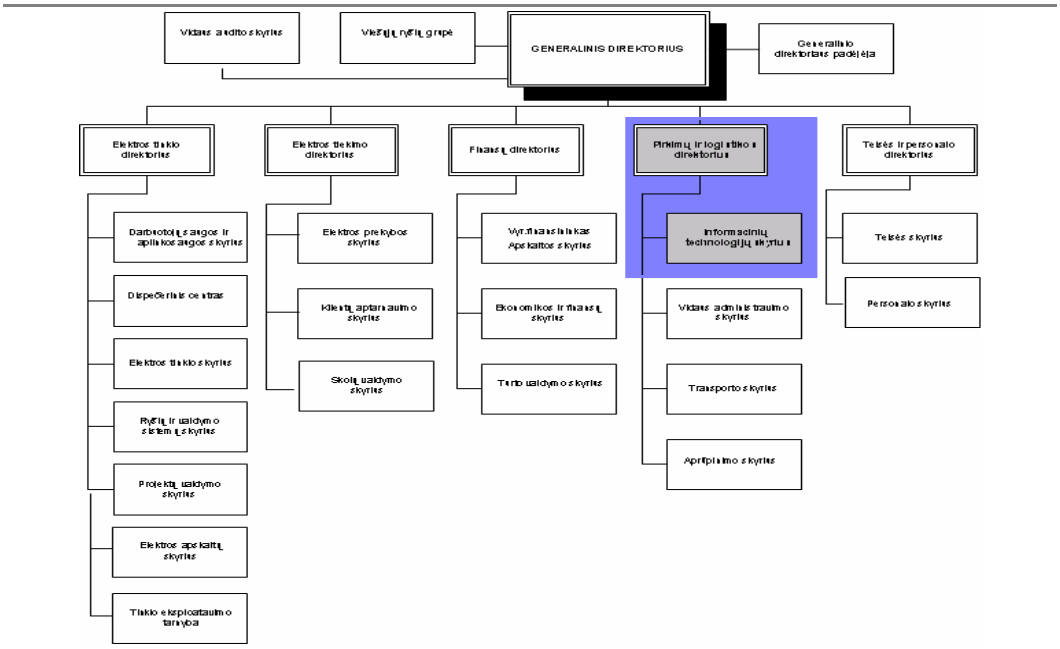
1.2.1. Informacinių sistemų strateginis valdymas

Atsakomybė už RST IT politikos formavimą, IT sprendimų integravimą į verslo procesus ir IT infrastruktūros ir informacinių (taikomųjų) sistemų kūrimo, diegimo ir priežiūros darbus nustatyta[30] bendrovės IT skyriui. Svarbiausi RST IT skyriaus uždaviniai nurodyti IT skyriaus nuostatuose[31].

> Vadovaujantis pasaulyje pripažinta gerąja praktika IT politikos formavimo uždavinys priskirtinas RST vadovybei ir IT valdymo komiteto kompetencijai[32].

RST IT skyrius tiesiogiai pavaldus[33] bendrovės pirkimų ir logistikos direktoriui. Bendrovės vadovo ir direktorių pareigų ir veiklos sričių paskirstymas pateiktas 1 paveiksle.

1 pav. RST centrinės buveinės organizacinė struktūra



Šaltinis – AB Rytų skirstomųjų tinklų generalinio direktoriaus 2004-06-14 įsakymas Nr. 94.

[30] AB Rytų skirstomųjų tinklų valdybos 2003-05-08 posėdžio protokolu Nr.7 (2003-12-17 AB Rytų skirstomųjų tinklų valdybos posėdžio protokolo Nr.15 redakcija) patvirtinti „Informacinių technologijų skyriaus nuostatai“.
[31] Ten pat.
[32] *COBIT (Control Objectives for Information and related Technologies*) – viena iš populiariausių IT valdymo metodologijų, kuriama ir palaikoma tarptautinės ISACA organizacijos.
[33] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2004-06-28 įsakymas Nr.107 „Dėl pareigų ir veiklos sričių paskirstymo pakeitimo“.

Gerojoje praktikoje teigiama[34], kad institucijoje su išplėstomis informacinėmis sistemomis turėtų būti sudarytas IT valdymo komitetas, kuris užtikrintų, kad institucijos naudojamos lėšos informacinių sistemų plėtrai sutaptų su institucijos poreikiais, būtų naudojamos efektyviai pagal aiškiai suformuluotus tikslus ir kriterijus. Vadovaujantis pasaulyje pripažinta gerąja praktika[35] RST turėtų būti sukurtas IT valdymo komitetas, kurį, valstybinių auditorių nuomone, galėtų sudaryti visų veiklos sričių direktoriai ir informacinių technologijų ir telekomunikacijų padalinių vadovai.

RST nėra IT valdymo komiteto. Dalis IT valdymo komiteto funkcijų bendrovėje patikėta spręsti pirkimų ir logistikos direktoriui[36].

Rizika

RST nesukūrus IT valdymo komiteto, atsiranda rizika, kad:

- informacines sistemas prižiūrinčių padalinių veikla ir tikslai neatitiks bendrovės vadovybės požiūrio į informacinių sistemų plėtrą;
- RST gali būti neefektyviai naudojami informacinių sistemų ištekliai;
- bendrovėje nebus koordinuojamas informacines sistemas prižiūrinčių padalinių darbas.

1.2.2. Informacinių sistemų saugos strateginis valdymas

Lietuvos Respublikos teisės aktai numato RST vadovo atsakomybę už bendrą informacijos, kurią valdo bendrovė, saugos organizavimą ir būklę[37]. RST vadovas, atsižvelgdamas į saugotinos informacijos ir informacinės sistemos apimtį, gali sudaryti informacijos apsaugą koordinuojančią komisiją arba jos funkcijas pavesti įgaliotam asmeniui[38].

Bendrovės vadovo sprendimu atsakomybė už RST informacinę saugą 2004 m. skirta IT skyriaus centro grupės vadovui[39].

Audituojamu laikotarpiu RST informacijos apsaugą koordinuojanti komisija nebuvo sudaryta. Dėl informacijos apsaugos valdymo forumo ir informacijos saugos grupės steigimo RST 2004 m.[40] ir 2007 m.[41] rašė ir UAB „Blue Bridge“ informacijos apsaugos konsultantai (2 lentelė).

[34] *COBIT (Control Objectives for Information and related Technologies*) – viena iš populiariausių IT valdymo metodologijų, kuriama ir palaikoma tarptautinės ISACA organizacijos.
[35] Ten pat.
[36] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2004-06-28 įsakymas Nr.107 „Dėl pareigų ir veiklos sričių paskirstymo pakeitimo“.
[37] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymu Nr. 4-349 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimai, 16 p.
[38] Ten pat, 18 ir 19 p.
[39] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2004-06-22 įsakymas Nr. 105 „Dėl atsakingų už saugą asmenų paskyrimo“.
[40] Informacijos apsaugos valdymo sistemos vertinimas. Informacijos apsaugos valdymo analizės ataskaita pateikta UAB „Blue Bridge“ pagal 2004-01-27 sutartį Nr. 10530/4/9.
[41] Informacijos saugos audito ataskaita pateikta UAB „Blue Bridge“ pagal 2006-12-15 sutartį Nr. 10530/461459.

2 lentelė. UAB „Blue Bridge“ informacijos apsaugos konsultantų rekomendacijos

2004 m.	2007 m.
„Įsteigti informacijos apsaugos valdymo forumą, kuriame dalyvautų skyrių vadovai. Forumas peržiūrėtų ir tvirtintų saugumo reikalavimus; užtikrintų, kad informacijos apsauga atitiktų verslo tikslus; tvirtintų iniciatyvas, peržiūrėtų saugumo incidentus.“	„Atsižvelgiant į įmonės dydį, yra tikslinga apsvarstyti informacijos saugos grupės steigimą, kuri užsiimtų informacijos apsauga, įskaitant ir atskirą darbuotoją fizinio saugumo priemonių organizavimui.“

Šaltinis – UAB „Blue Bridge“ 2004-03-05 „Informacijos apsaugos valdymo sistemos vertinimas. Informacijos apsaugos valdymo analizės ataskaita“ ir UAB „Blue Bridge“ 2007-03-07 „Informacijos saugos auditas“.

Rizika

RST nesudaryta informacijos apsaugą koordinuojanti komisija, todėl yra rizika, kad bendrovėje gali būti neužtikrinama kompleksinė apdorojamos ir perduodamos informacijos apsauga.

UAB „Blue Bridge“ informacijos apsaugos konsultantai 2007 m. kovo mėn. nustatė, kad už RST informacinę apsaugą paskirtam darbuotojui nesuteikti pakankami įgaliojimai bendrovėje užtikrinti informacijos saugą ir nesudarytos sąlygos koordinuoti saugumo valdymą, kaip reikalaujama *LT ISO/IEC 27001* standarte[42]. Siekiant tinkamai koordinuoti informacijos saugos klausimus RST vadovybei buvo rekomenduota vieną iš bendrovės direktorių paskirti atsakingą už informacijos saugumo valdymo sistemos priežiūrą (kuravimą). Iki 2007 m. spalio 1 d. RST vadovybė neįsitraukė į bendrovės IT ir informacijos saugos strateginio valdymo procesus.

Audituojamu laikotarpiu RST vadovybė nepakankamai formalizavo bendrovės informacijos saugos strateginio valdymo ir organizavimo procesus.

RST taikomi informacinės saugos reikalavimai[43] nustato būtinybę apibrėžti atsakomybę už atskirų informacijos rūšių apsaugą ir saugumo procedūrų taikymą. *COBIT 4.0* metodikoje[44] siūloma nustatyti duomenų ir sistemų valdytojus (angl. *owner* – „savininkas“). *ISACA* gerojoje praktikoje[45] nurodoma, kad informacinių išteklių valdytojais (*owner*) turėtų būti informacijos naudotojų vadovybė. *ISO 17799* standarte[46] informacinių išteklių valdytojais (*owner*) įvardijama organizacijos vadovybė, atsakinga už priskirto informacinio išteklio valdymą, naudojimą ir saugumą. Apie

[42] Informacijos saugos audito ataskaita pateikta UAB „Blue Bridge“ pagal 2006-12-15 sutartį Nr. 10530/461459.
[43] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymu Nr. 4-349 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimai, 17 p.
[44] *COBIT (Control Objectives for Information and related Technologies*) – viena iš populiariausių IT valdymo metodologijų, kuriama ir palaikoma tarptautinės *ISACA* organizacijos.
[45] *2006 Certified Information Systems Auditor Review Technical Information Manual. ISACA.*
[46] *ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management.*

būtinybę kiekvienam RST informaciniam ištekliui paskirti savininką 2004 m. kalbėjo ir UAB „Blue Bridge“ informacijos saugumo konsultantai[47].

Audituojamu laikotarpiu RST nebuvo nustatyti bendrovės informacinės sistemos ir jos posistemių valdytojai (*owner*).

Kita vertus siekiant tobulinti RST IT taikymo ir eksploatavimo procesus, lengvinti kompiuterinių išteklių naudotojų darbą, 2003 m. patvirtintas RST eksploatuojamų informacinių sistemų ir programų administratorių, supernaudotojų ir konsultantų sąrašas[48], 2006 m. nustatyti pagrindiniai RST eksploatuojamų informacinių sistemų ir programų valdymo ir administravimo principai[49].

Geroji praktika

RST sudarytas ir nuolat atnaujinamas bendrovės eksploatuojamų informacinių sistemų ir programų administratorių, supernaudotojų ir konsultantų sąrašas, nustatyti pagrindiniai bendrovės eksploatuojamų informacinių sistemų ir programų valdymo ir administravimo principai.

Valstybinių auditorių nuomone, supernaudotojų pareigos netapačios informacinių sistemų valdytojų pareigoms, nes valdytojų funkcijas turėtų vykdyti veiklos padalinių vadovai. Todėl valstybiniai auditoriai mano, kad bendrovėje turi būti įvardyti ir nustatyti RST informacinės sistemos ir jos posistemių valdytojai – informacijos naudotojų vadovybės atstovai. Šie asmenys turi dalyvauti priimant sprendimus dėl valdomų informacinių sistemų informacijos tvarkymo ir tiekimo apimties, saugumo užtikrinimo, modernizavimo ir plėtros. Taip pat jie turėtų būti įtraukti į rizikos vertinimo procesus.

Rizika

RST vidaus teisės aktuose nebuvo įvardyta informacinių sistemų naudotojų vadovybės atsakomybė už informacinių sistemų valdymą, todėl yra rizika, kad gali būti netinkamai reglamentuota atsakomybė ir darbų pasidalijimas tarp bendrovės veiklos padalinių darbuotojų ir informacinių sistemų specialistų.

[47] Informacijos apsaugos valdymo sistemos vertinimas. Informacijos apsaugos valdymo analizės ataskaita pateikta UAB „Blue Bridge“ pagal 2004-01-27 sutartį Nr. 10530/4/9.
[48] AB Rytų skirstomųjų tinklų pirkimų ir logistikos direktoriaus 2003-10-17 nurodymas Nr. 145 „Dėl eksploatuojamų informacinių sistemų ir programų administratorių, supernaudotojų ir konsultantų sąrašo patvirtinimo“.
[49] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2006-07-24 įsakymas Nr. 145 „Dėl informacinių sistemų ir programų eksploatavimo reglamento“.

RST rašte[50] teigiama, kad *bendrovėje naudojamas ne „valdytojo“, o „supernaudotojo“ terminas, kurio funkcijos beveik identiškos „valdytojo“ funkcijoms.*

Valstybinių auditorių nuomone, pagrindinis trūkumas yra ne pasirinkta vartoti terminologija, bet RST vidaus teisės aktuose neįvardyta informacinių sistemų naudotojų vadovybės atsakomybė už šių sistemų valdymą.

1.3. Informacinių sistemų rizikos vertinimas

RST naudojama viena informacinė sistema[51] – Rytų skirstomųjų tinklų informacinė sistema, kuri apima visas RST kompiuterizuotas informacijos valdymo ir tvarkymo sritis. Lietuvos Respublikos teisės aktai RST nurodo periodiškai peržiūrėti grėsmes bendrovei ir jos informacinei sistemai, aptarti naujas grėsmes ir pavojus bei patvirtinti, kad esami informacinės saugos priežiūros metodai vis dar veiksmingi ir tinkami[52].

Geroji praktika

Audituojamu laikotarpiu RST saugos valdymas apėmė bendrovės informacinę sistemą ir jos posistemes, t.y. visą RST kompiuterizuotą informaciją, kaip nurodoma pasaulyje pripažintoje gerojoje praktikoje.

Audituojamu laikotarpiu RST neatliktas formalus bendrovės informacinės sistemos rizikos vertinimas, nebuvo pasirinkta rizikos analizės ir valdymo metodika. Valstybinio audito metu informacinės saugos priežiūros metodai RST parinkti remiantis rangovų patirtimi, IT darbuotojų žiniomis, praktine patirtimi ir intuicija.

Rizika

Neatlikus RST informacinės sistemos rizikos analizės, negali būti užtikrinama veiksminga ir tinkama informacijos sauga, todėl keičiantis informaciniam turtui, RST gali būti parinktos netinkamos rizikos valdymo ir kontrolės priemonės. Valstybiniai auditoriai bendrovėje neaptiko formalių kriterijų, kuriais vadovaujantis būtų nustatoma RST naudojamų duomenų ir informacinio turto vertė, jų apsaugojimo ir atstatymo galimybės ir kaštai.

[50] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-12-20 raštas Nr. 10530-1221 „Dėl pastabų valstybinio audito ataskaitos projektui“.
[51] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-07-05 įsakymas Nr. 98 „Dėl bendrovės informacinių sistemų vystymo strateginio plano patvirtinimo“.

Apie būtinybę RST reguliariai atlikti rizikos analizę, kurios metu būtų aptariamos kylančios grėsmės ir būtų nustatomos kritinės RST informacinės sistemos arba informacija, 2004 m.[53] ir 2007 m.[54] rašė ir UAB „Blue Bridge“ informacijos apsaugos konsultantai.

1.4. Informacijos saugos politikos dokumentavimas

Lietuvos Respublikos teisės aktai reikalauja, kad RST būtų įdiegta ir valdoma bendrovės informacinės saugos sistema[55]. *ISACA* geroje praktikoje nurodyta, kad informacinių sistemų politiką formuoja organizacijos vadovybė[56]. RST informacijos saugos politika turėtų būti išdėstyta dokumente, kuriame bendrovės vadovybė turi nustatyti aiškią informacijos saugos strategijos kryptį, akivaizdžiai ją palaikyti ir įsipareigoti, paskelbdama ir remdama informacijos saugumo politiką visoje bendrovėje.

UAB „Blue Bridge“ 2004 m. parengė RST informacijos apsaugos politikos dokumentacijos medžiagą[57]. Atliekant informacinės saugos audito paslaugas, UAB „Blue Bridge“ 2007 m. atnaujino 2004 m. parengtą bendrovės informacijos saugos politikos dokumentaciją, ir parengė saugumo politikos projektą[58]. Audituojamu laikotarpiu (iki 2007-10-01) šis saugumo politikos projektas nebuvo patvirtintas RST vadovybės, todėl jo taikymas bendrovėje buvo rekomendacinio pobūdžio. Valstybinių auditorių nuomone, informacinės saugos politikos tvirtinimas yra svarbi kontrolės priemonė. Tvirtindama RST vadovybė įsipareigoja remti informacinės saugos principus, organizavimo pagrindus bei pagrindinius informacinės saugos reikalavimus, kurie padės užtikrinti nepertraukiamą, stabilią ir saugią bendrovės veiklą.

Rizika

RST informacinės saugos politikos formalizavimas yra nepakankamas, todėl bendrovės vadovybė neturi formalių RST informacinės sistemos saugos kriterijų.

[52] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymu Nr. 4-349 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimai, 11 p.
[53] Informacijos apsaugos valdymo sistemos vertinimas. Informacijos apsaugos valdymo analizės ataskaita pateikta UAB „Blue Bridge“ pagal 2004-01-27 sutartį Nr. 10530/4/9.
[54] Informacijos saugos audito ataskaita pateikta UAB „Blue Bridge“ pagal 2006-12-15 sutartį Nr. 10530/461459.
[55] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymu Nr. 4-349 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimai, 17 p.
[56] *2006 Certified Information Systems Auditor Review Technical Information Manual. ISACA.*
[57] Informacijos apsaugos politikos dokumentas, pateiktas UAB „Blue Bridge“ pagal 2004-01-27 sutartį Nr. 10530/4/9.
[58] Saugumo politikos projektas pateiktas UAB „Blue Bridge“ pagal 2006-12-15 sutartį Nr. 10530/461459.

Siekiant užtikrinti platesnį informacijos saugos valdymo principų taikymą, teisės aktai rekomenduoja diegti visuotinai pripažintus tarptautinius standartus[59]. Valstybinio audito metu (2007-11-16) RST pasirašyta sutartis[60] diegti bendrovės informacijos saugumo valdymo sistemą vadovaujantis *LT ISO/IEC 27001:2006* standartu[61]. Projekto pirmajame etape bus sukurtos RST saugos procesų taikymo sritys ir ribų aprašas, saugos politika, rizikos vertinimo metodika ir rizikos analizė, parengtas rizikų priežiūros ir antrojo etapo darbų planas[62].

Geroji praktika

> RST siekia pagerinti informacijos saugumo valdymą, įdiegdama informacijos saugumo valdymo sistemą vadovaujantis *LT ISO/IEC 27001:2006* standartu.

1.5. Informacinių sistemų valdymo ir saugos procedūros

Lietuvos Respublikos teisės aktai reglamentuoja reikalavimus, susijusius su RST informacine[63] ir fizine[64] sauga. Pasaulyje pripažinti informacinių sistemų valdymo ir saugos standartai bendrovei yra rekomendacinio pobūdžio[65].

Valstybinio audito metu (iki 2007-10-01) RST vidaus teisės aktais nebuvo pasirinkta informacinių sistemų valdymo metodika. Todėl valstybiniai auditoriai, vertindami teisės aktais nereglamentuotus RST informacinių sistemų valdymo procesus, vadovavosi pasaulyje pripažintais standartais (*ISO 17799*[66], *ISO 27001*[67], *ISO 20000*[68]) ir kita gerąja praktika (*COBIT*[69], *ITIL*[70]).

[59] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymu Nr. 4-349 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimai, 47 p.
[60] AB Rytų skirstomųjų tinklų ir UAB „Blue Bridge“ 2007-11-16 sutartis Nr. 10530/471286.
[61] *LT ISO/IEC 27001:2006* Lietuvos standartas. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai (tapatus *ISO/IEC 27001:2005*).
[62] AB Rytų skirstomųjų tinklų ir UAB „Blue Bridge“ 2007-11-16 sutartis Nr. 10530/471286.
[63] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymas Nr. 4-349 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimų patvirtinimo“.
[64] Lietuvos Respublikos ūkio ministro 2004-09-15 įsakymas Nr. 4-334 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių fizinės saugos reikalavimų patvirtinimo“.
[65] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymu Nr. 4-349 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimai, 47 p.
[66] *ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management.*
[67] *ISO/IEC 27001:2006 Information technology. Security techniques. Information security management systems. Requirements.*
[68] *ISO/IEC 20000-2:2005 Code of Practice.*
[69] *COBIT (Control Objectives for Information and related Technologies*) – viena iš populiariausių IT valdymo metodologijų, kuriama ir palaikoma tarptautinės *ISACA* organizacijos.
[70] ITIL (*Information Technology Infrastructure Library*) – verslo valdymo teorija, orientuota į darbo optimizavimą ir kokybės užtikrinimą IT kompanijose. ITIL yra pripažintas standartais: D. Britanijos BS-15000 bei tarptautiniu ISO-20000, ITIL suderinamas ir su visais ISO-9000 reikalavimais.

1.5.1. Informacinių sistemų ir informacijos saugos procedūrų dokumentavimas

Vadovaujantis Ūkio ministerijos informacijos saugos reikalavimais[71], RST turi būti nustatytos informacijos apdorojimo įrangų darbo ir valdymo procedūros ir jų vykdymo atsakomybė. Procedūros turi būti įformintos bendrovės vidaus teisės aktais.

Audituojamu laikotarpiu RST informacinės sistemos valdymo ir informacijos saugos procesai buvo reglamentuojami atskiromis tvarkomis, kurios neapėmė visų teisės aktuose numatytų būtinų sričių[72]. Dalies bendrovei reikalingų informacinių sistemų ir informacinės saugos kontrolės procedūrų oficialiai nebuvo patvirtinusi vadovybė.

> Detali Ūkio ministerijos informacinės ir fizinės saugos reikalavimų atitikties analizė pateikta valstybinio audito ataskaitos 3 priedo 1 ir 2 lentelėse.

Rizika

> Audituojamu laikotarpiu RST nebuvo įteisintos visos teisės aktais privalomos informacinių sistemų ir informacinės saugos valdymo procedūros ir atsakomybė už jų vykdymą, todėl yra rizika, kad bendrovės informacinės saugos valdymo sistema gali būti nevientisa ir neišbaigta.

Geroji praktika

> Nors RST nėra visiškai formalizuoti visi teisės aktais privalomi informacijos saugos procesai, bendrovės IT skyriaus specialistai turi žinių ir, siekdami užtikrinti nepertraukiamą, stabilią bei saugią bendrovės veiklą, neformaliai taiko pasaulyje pripažintas IT valdymo ir saugos gerąsias praktikas.

[71] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymu Nr. 4-349 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimai, 31 p.

[72] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymas Nr. 4-349 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimų patvirtinimo“; 2004-09-15 įsakymas Nr. 4-334 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių fizinės saugos reikalavimų patvirtinimo“.

1.5.2. Informacinio turto kontrolė

RST informacinės sistemos elementai (informacija, programinė įranga, techninė įranga) turi būti apskaitomi ir priskiriami konkretiems asmenims, numatant jų atsakomybę už tinkamą apskaitą bei priežiūrą[73]. Pasaulyje pripažintoje gerojoje praktikoje (*COBIT*[74], *ITIL*[75]) ir standartuose (*ISO 17799*[76], *ISO 27001*[77]) nurodoma konfigūracijos elementų registravimo būtinybė (3 lentelė).

3 lentelė. Konfigūracijos elementų (informacija, programinė įranga, techninė įranga) aprašymo santrauka

Informacija	Programinė įranga	Techninė įranga
Duomenų bazės, duomenų laikmenos ir rinkmenos, sutartys ir susitarimai, sistemos dokumentai, vartotojo vadovai, mokymo medžiaga, naudojimo arba palaikymo procedūros, nenutrūkstamumo planai, audito, archyvo ir kita informacija.	Taikomoji programinė įranga, sistemos programinė įranga, plėtros priemonės ir paslaugų programos.	Kompiuterinė įranga, ryšių įranga, keičiamos laikmenos, kita techninė įranga.

Šaltinis – Valstybės kontrolė

Valstybinio audito metu buvo vertintos RST konfigūracijos elementų registracijos ir apskaitos procedūros bendrovės centrinėje buveinėje.

Vadovaujantis teisės aktuose nustatytais informacijos saugos reikalavimais[78], RST konfigūracijos elemento (informacijos) dalis – duomenų laikmenos turi būti apskaitomos, kontroliuojamos ir fiziškai apsaugomos. Tam bendrovėje turi būti parengtos ir patvirtintos darbo procedūros, skirtos apsaugoti dokumentus, kompiuterines laikmenas, įvesties (išvesties) duomenis ir sistemos dokumentus nuo žalos, vagystės ir nesankcionuoto priėjimo.

RST informacinių sistemų vystymo strateginiame plane nurodyta[79], kad bendrovėje nėra vienos saugyklos, kur būtų registruota visa informacija, laikoma informacinėse sistemose, todėl neaišku, kur kokia informacija yra ir kaip prie jos prieiti. Audituojamu laikotarpiu bendrovės informacijos saugos dokumentacijoje nebuvo detalizuoti atsakingų asmenų veiksmai ir saugos

[73] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymu Nr. 4-349 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimai, 21 p.
[74] *COBIT (Control Objectives for Information and related Technologies*) – viena iš populiariausių IT valdymo metodologijų, kuriama ir palaikoma tarptautinės *ISACA* organizacijos.
[75] ITIL (*Information Technology Infrastructure Library*) – verslo valdymo teorija, orientuota į darbo optimizavimą ir kokybės užtikrinimą IT kompanijose. ITIL yra pripažintas standartais: D. Britanijos BS-15000 bei tarptautiniu ISO-20000, ITIL suderinamas ir su visais ISO-9000 reikalavimais.
[76] *ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management.*
[77] *ISO/IEC 27001:2006 Information technology. Security techniques. Information security management systems. Requirements.*
[78] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymu Nr. 4-349 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimai, 39 p.
[79] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-07-05 įsakymas Nr. 98 „Dėl bendrovės informacinių sistemų vystymo strateginio plano patvirtinimo“.

priemonės, skirtos apsaugoti RST duomenų laikmenas nuo žalos, vagystės ir nesankcionuoto priėjimo. RST 2008 m. ketinama kurti bendrovės informacinėje sistemoje esančios informacijos ir informacinių sistemų dokumentavimo tvarkymo posistemę (*DICTIONARY*)[80].

> Valstybinio audito metu RST nebuvo sistemingai valdomi dalies bendrovės informacinės sistemos konfigūracijos elemento informacijos (duomenų laikmenų) registracijos procesai, neformalizuoti atsakingų asmenų veiksmai ir saugos priemonės, skirtos apsaugoti šią informacijos dalį nuo žalos, vagystės ir nesankcionuoto priėjimo.

Buhalterinė RST konfigūracijos elementų registracija ir apskaita tvarkoma naudojant apskaitos ir verslo valdymo (*SCALA*) informacinę posistemę[81]. Bendrovė buhalterinę apskaitą tvarko vadovaudamasi Buhalterinės apskaitos[82] ir Finansinės atskaitomybės[83] įstatymais, RST apskaitos politikos vadovu[84], kitais buhalterinės apskaitos tvarką reglamentuojančiais norminiais aktais[85]. RST buhalterinę apskaitą vykdo bendrovės Apskaitos skyrius, kuriam vadovauja bendrovės vyriausiasis finansininkas. Už RST centrinės buveinės kompiuterinę ir kompiuterių tinklo įrangą, programinę įrangą ir jos licencijas, kitą su kompiuteriais susijusį ilgalaikį ir trumpalaikį turtą bei atsargas atsakingas[86] IT skyriaus centro grupės vadovas. IT skyriaus centro grupės vadovas RST centrinėje buveinėje organizuoja jam patikėtų vertybių priežiūrą ir apsaugą, dalyvauja inventorizuojant šias vertybes[87].

Audituojamu laikotarpiu valstybiniai auditoriai atliko RST centrinėje buveinėje esančio ilgalaikio materialiojo ir nematerialiojo turto sudarytų aprašų peržiūrą. Atlikus peržiūrą nustatytas vienas netikslumas – pagal 2004-05-14 sutartį Nr. 10530/4/101[88] sisteminė programinė įranga (*Windows 2003 Server Enterprise* operacinės sistemos 4 licencijos pagal atviros licencijos sutartį (OSL[89])) įtraukta į RST ilgalaikio nematerialiojo turto sąrašą. Sisteminės programinės įrangos licencijos, įsigytos pagal Microsoft atviros licencijos sutartį (OSL), nėra bendrovei priklausantis ilgalaikis nematerialusis turtas, o tik teisė naudoti produktą sutartyje Nr. 10530/4/101 nurodytą

[80] Ten pat.
[81] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2006-12-29 įsakymas Nr. 253 „Dėl bendrovės apskaitos politikos vadovo, sąskaitų plano, konsoliduotos finansinės atskaitomybės sudarymo tvarkos, atidėtojo mokesčio įvertinimo ir apskaitos tvarkos bei ilgalaikio materialiojo turto rekonstravimo ir remonto išlaidų apskaitos tvarkos patvirtinimo“.
[82] Lietuvos Respublikos buhalterinės apskaitos įstatymas, 2001-11-06 Nr. IX-574.
[83] Lietuvos Respublikos įmonių finansinės atskaitomybės įstatymas, 2001-11-06 Nr. IX-576.
[84] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2006-12-29 įsakymas Nr. 253 „Dėl bendrovės apskaitos politikos vadovo, sąskaitų plano, konsoliduotos finansinės atskaitomybės sudarymo tvarkos, atidėtojo mokesčio įvertinimo ir apskaitos tvarkos bei ilgalaikio materialiojo turto rekonstravimo ir remonto išlaidų apskaitos tvarkos patvirtinimo“.
[85] RST apskaita tvarkoma ir finansinė atskaitomybė rengiama ir pateikiama pagal galiojančius Tarptautinius finansinės atskaitomybės standartus (TFAS), kurie apima standartus ir išaiškinimus, patvirtintus Tarptautinių apskaitos standartų tarybos, bei galiojančius Tarptautinius apskaitos standartus ir Nuolatinio interpretavimo komiteto (NIK) išaiškinimus, patvirtintus Tarptautinių apskaitos standartų komiteto, priimtus taikyti Europos Sąjungoje.
[86] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2005-01-11 įsakymas Nr. 9 „Dėl materialinių vertybių perdavimo-priėmimo“.
[87] AB Rytų skirstomųjų tinklų ir J. Piliponio 2005-01-12 visiškos materialinės atsakomybės sutartis Nr. 10630/7/0014
[88] AB Rytų skirstomųjų tinklų ir AB „Alna“ 2004-05-14 sutartis Nr. 10530/4/101.
[89] Prieiga per internetą http://www.microsoft.com/lietuva/piracy/licenseguide/osl.mspx [Žiūrėta 2007-11-26]

laikotarpį[90] (nuomos paslauga, periodiškai mokamas nuomos mokestis). Dėl minėtos priežasties *Windows 2003 Server Enterprise* operacinės sistemos 4 licencijos pagal atviros licencijos sutartį (OSL) RST buhalterinėje apskaitoje turėtų būti apskaitytos kaip bendrovės sąnaudos.

Valstybiniai auditoriai, atlikę RST dokumentų analizę, nustatė, kad iki 2007 m. spalio 1 d. bendrovės finansinės apskaitos dokumentuose nebuvo užregistruotas visas su RST informacinės sistemos posistemėmis susijęs ilgalaikis nematerialusis turtas. RST finansinės apskaitos dokumentuose neregistruojama programinė įranga, kurią pagal bendrovės padalinių poreikį sukūrė IT skyriaus specialistai (4 lentelė).

4 lentelė. RST finansinės apskaitos dokumentuose neregistruota su bendrovės informacinės sistemos posistemėmis susijusi programinė įranga (ilgalaikis nematerialusis turtas) (2007 m. spalio mėn. duomenys)

Eil. Nr.	IS pavadinimas	IS funkcija, trumpas aprašymas
1.	PIRMADIENIS	Pagrindinių RST savaitės veiklos rodiklių surinkimo ir statistikos posistemė.
2.	KAD	Kintamos dalies skaičiavimo informacinė posistemė.
3.	TABELIS	Darbo laiko apskaitos informacinė posistemė.
4.	PERSONALAS	Personalo apskaitos informacinė posistemė.
5.	SPECTEISĖS	Specialiųjų teisių suteikimo informacinė posistemė.
6.	MOBILKĖS	Mobiliųjų telefonų pokalbių apskaitos informacinė posistemė.
7.	RODMENYS	ELGAMA skaitiklių parametravimo ir rodmenų nuskaitymo informacinė posistemė.
8.	TURTAS	Netechnologinio turto valdymo informacinė posistemė
9.	INVISTA (INVESTICIJOS)	Investicijų valdymo informacinė posistemė.
10.	TEMIDĖ	Teisminių bylų procesų valdymo informacinė posistemė.
11.	BLANKAS	Portalo "PORTALAS" klientų registracijos valdymo informacinė posistemė.
12.	SKAREGAS	Elektros energijos vartotojų skambučių registravimo informacinė posistemė.
13.	KCUVIS	Kontaktų centro užklausų valdymo informacinė posistemė.
14.	PIRKIMAI	Pirkimų valdymo informacinė posistemė.

Šaltinis – Valstybės kontrolė

Rizika

RST finansinės apskaitos dokumentuose neregistruojama programinė įranga, kurią pagal bendrovės padalinių poreikį sukūrė RST IT skyriaus specialistai, todėl yra rizika, kad dalis bendrovės informacinio turto galėjo būti neidentifikuota, neapskaityta ir prarasta.

[90] AB Rytų skirstomųjų tinklų ir AB „Alna“ 2004-05-14 sutartis Nr. 10530/4/101.

RST rašte[91] teigiama, kad *programinė įranga, sukurta IT skyriaus specialistų jėgomis, yra dokumentuota, įtraukta į informacinių sistemų rejestrą, paskirti administratoriai, apibrėžti naudotojai.*

Valstybinių auditorių nuomone, nors RST IT skyriaus specialistų sukurta programinė įranga yra dokumentuota, įtraukta į informacinių sistemų rejestrą ir paskirti administratoriai, ši programinė įranga turi būti įtraukta ir į ilgalaikio nematerialiojo turto sąrašus, t. y. jos apskaita turėtų būti užtikrinta teisės aktų nustatyta tvarka.

Apie RST naudojamų kompiuterių programų (ilgalaikio nematerialiojo turto) inventorizavimo ir apskaitos vidaus kontrolės trūkumus žodžiu buvo informuotas IT skyriaus centro grupės vadovas ir apskaitos skyrius.

1.6. Informacinių sistemų auditai

Vadovaujantis Ūkio ministerijos nustatytais reikalavimais[92], RST informacinės saugos ir fizinės saugos auditai turi būti atliekami ne rečiau kaip kas dvejus metus. Informacinės saugos ir fizinės saugos auditus turi atlikti vidaus audito padaliniai arba įmonės, atitinkančios teisės aktų reikalavimus.

1.6.1. Vidaus audito skyriaus atlikti informacinių sistemų auditai

RST Vidaus audito skyrius (toliau – Vidaus audito skyrius) tikrina ir vertina bendrovės informacinių sistemų saugumą, veiksmingumą ir informacinių sistemų projektus, vykdo pažangos stebėjimą (veiklą po audito)[93]. Be to, Vidaus audito skyrius tikrina ir vertina, ar bendrovėje sukurta ir įdiegta vidaus kontrolės sistema yra pakankama ir veiksminga.

Audito praktika rodo, kad vidaus kontrolės sričių įvertinimas turėtų būti atliekamas skaidant vidaus kontrolės sistemą į atskiras sritis, kurių auditas turi būti numatomas strateginiuose ir metiniuose tarnybų planuose. Vidaus audito profesinės praktikos standartai[94] tokia sritimi laiko informacijos saugumą.

[91] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-12-20 raštas Nr. 10530-1221 „Dėl pastabų valstybinio audito ataskaitos projektui“.
[92] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymas Nr. 4-349 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimų patvirtinimo“; 2004-09-15 įsakymas Nr. 4-334 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių fizinės saugos reikalavimų patvirtinimo“.
[93] AB Rytų skirstomųjų tinklų valdybos 2002-12-03 protokolu Nr. 13 (AB Rytų skirstomųjų tinklų valdybos 2004-07-01 sprendimo Nr. 6 redakcija) patvirtinti AB Rytų skirstomųjų tinklų Vidaus audito skyriaus nuostatai.
[94] Vidaus audito standartas 2110 A2 ,,Rizikos valdymas“ ir jo paaiškinimas 2100-2 ,,Informacijos saugumas“.

Audituojamu laikotarpiu Vidaus audito skyrius specializuotų informacinių sistemų auditų neatliko. Vidaus audito skyrius 2006 m.[95] atliko naujų vartotojų elektros įrenginių prijungimo prie skirstomųjų tinklų tvarkos ir sąlygų vertinimo auditą, kurio metu buvo nagrinėjami keli su IT susiję procesai.

Fizinė sauga yra informacinių sistemų bendrosios kontrolės dalis. RST fizinės saugos lygis turi atitikti identifikuotas grėsmes bei galimas pasekmes[96]. Nuo 2004 m. bendrovės projektinės grėsmės turi būti peržiūrimos ne rečiau kaip kartą per metus, o fizinės saugos auditas turi būti atliekamas ne rečiau kaip kas dvejus metus[97].

Vidaus audito skyrius fizinės saugos auditą RST ir jos dukterinėse bendrovėse atliko 2006 m.[98] Audito metu buvo nagrinėjamas RST technologinių ir netechnologinių objektų fizinės saugos organizavimas, dokumentacijos tvarkymas, tačiau nebuvo nagrinėjami visi klausimai, susiję su informacinių sistemų fizine sauga. Vadovaujantis Ūkio ministerijos nustatytais fizinės saugos reikalavimais, 2008 m. numatomas atlikti RST ir jos dukterinių bendrovių fizinės saugos auditas[99].

1.6.2. Specializuoti informacinių sistemų saugos auditai

RST specializuotus informacinės saugos auditus 2004 m.[100] ir 2006–2007 m.[101] atliko įmonės, atitinkančios teisės aktų reikalavimus[102]. Be minėtų informacinių saugos auditų, 2005–2006 m. atlikti RST informacijos saugos analizės ir sistemos atnaujinimo projekto sukūrimo, duomenų perdavimo tinklo analizės ir vystymo projekto sukūrimo darbai[103]. Taip pat UAB „PricewaterhouseCoopers“ 2006 m vykdė bendrovės finansinės atskaitomybės ir konsoliduotos finansinės atskaitomybės auditą[104], kurio metu pateikti pastebėjimai, susiję su IT veiklos atkūrimo planavimo procesais nelaimės atveju[105].

RST informacijos apsaugos valdymo sistemos vertinimas atliktas 2004 m. sausio–vasario mėn.[106] Šios patikros tikslas – įvertinti tuo metu taikytas RST informacijos apsaugos valdymo

[95] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2006-02-01 patvirtintas Vidaus audito skyriaus metinis planas 2006 m.
[96] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymu Nr. 4-349 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimai, 29 p.
[97] Lietuvos Respublikos ūkio ministro 2004-09-15 įsakymu Nr. 4-334 patvirtinti Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių fizinės saugos reikalavimai, 22 ir 23 p.
[98] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2006-10-18 įsakymas Nr. 209 „Dėl bendrovės ir jos dukterinių bendrovių fizinės saugos sistemų audito“.
[99] AB Rytų skirstomųjų tinklų 2007-02-09 raštas Nr. 10510-99 „Dėl informacijos pateikimo“.
[100] AB Rytų skirstomųjų tinklų ir UAB „Blue Bridge“ 2004-01-27 sutartis Nr. 10530/4/9.
[101] AB Rytų skirstomųjų tinklų ir UAB „Blue Bridge“ 2006-12-15 sutartis Nr. 10530/461459.
[102] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymas Nr. 4-349 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimų patvirtinimo“.
[103] AB Rytų skirstomųjų tinklų ir UAB „Blue Bridge“ 2005-09-13 sutartis Nr. 10530/4/1185.
[104] AB Rytų skirstomųjų tinklų ir UAB „PricewaterhouseCoopers“ 2006-07-17 sutartis Nr. 10410/460711.
[105] Laiškas vadovybei pateiktas UAB „PricewaterhouseCoopers“ pagal 2006-07-17 sutartį Nr. 10410/460711.
[106] AB Rytų skirstomųjų tinklų ir UAB „Blue Bridge“ 2004-01-27 sutartis Nr. 10530/4/9.

praktikas, lyginant jas su *LST ISO/IEC 17799:2000* standarto reikalavimais[107]. Įvertinimo metu buvo pateikta RST technologinės informacijos apsaugos analizės ataskaita[108], bendrovės finansų ir apskaitos valdymo sistemos (*SCALA*) atstatymo planas[109] ir bandymų protokolas[110].

RST informacijos saugumo valdymo atitikties *ISO/IEC 27001* standarto reikalavimams įvertinimas[111] ir bendrovės informacinių sistemų technologinių pažeidžiamumų įvertinimas buvo atlikti 2007 m.[112]

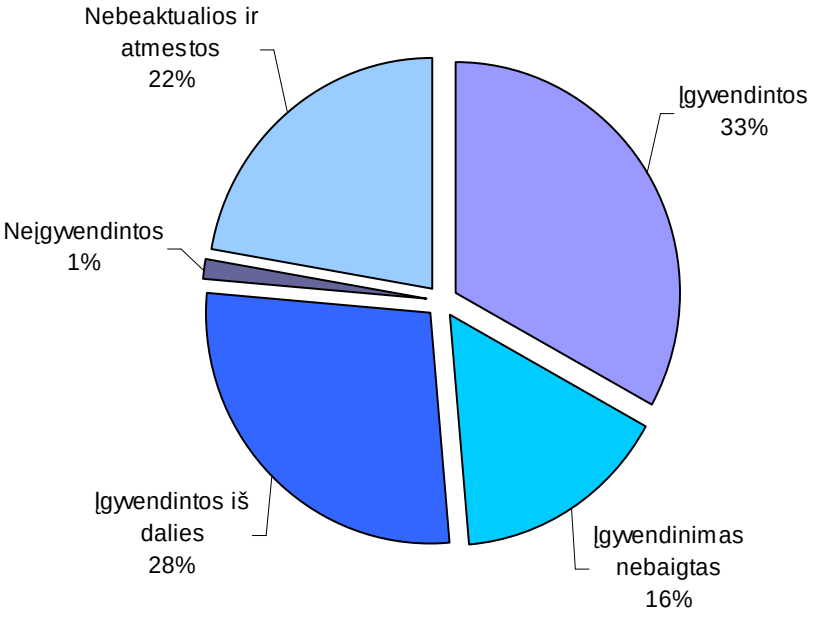
Valstybinio audito metu nustatyta, kad Vidaus audito skyrius nevykdė bendrovės IT skyriaus inicijuotų iš išorės samdomų kompanijų informacinių sistemų saugos auditų pažangos stebėjimo (poauditinės veiklos). Dėl minėtos priežasties RST nebuvo atliktos poauditinės veiklos valdymo procedūros, reglamentuojančios iš išorės samdomų kompanijų auditorių pateiktų rekomendacijų įvertinimo, registravimo, suderinamumo klausimus ir įtaką bendrovės sąnaudoms, išteklių ir laiko planavimui.

Valstybiniai auditoriai atliko 2004 m. ir 2007 m. UAB „Blue Bridge“ vertinimo ataskaitose pateiktų rekomendacijų įgyvendinimo peržiūrą. Valstybinio audito metu nustatyta, kad 2004 m. ir 2007 m. UAB „Blue Bridge“ vertinimo ataskaitose pateiktoms rekomendacijoms įgyvendinti ir trūkumams pašalinti ne visi priemonių planai buvo parengti ir formalizuoti. Kita vertus, atsižvelgiant į iki 2006 m. pateiktas informacijos apsaugos audito ataskaitas, RST sudarytas bendras informacijos saugos ir valdymo priemonių įgyvendinimo planas[113], tačiau bendrovėje nebuvo formaliai vykdoma šio dokumento įgyvendinimo kontrolė.

Atlikę UAB „Blue Bridge“ pateiktų rekomendacijų įgyvendinimo peržiūrą, valstybiniai auditoriai nustatė, kad 2004 m. RST informacijos apsaugos valdymo sistemos vertinimo dokumentuose[114] pateikta 251 rekomendacija. 2007 m. spalio mėnesį įgyvendintos 83 rekomendacijos, įgyvendinamos ir nebaigtos įgyvendinti – 39, įgyvendintos iš dalies – 70, neįgyvendintos – 3, nebeaktualios ir atmestos – 56 (2 pav.).

[107] *LT ISO/IEC 17799:2000* Lietuvos standartas. Informacijos technologija. Informacijos saugumo valdymo praktikos kodeksas (tapatus *ISO/IEC 17799:2000*).
[108] Technologinės informacijos apsaugos analizės ataskaita pateikta UAB „Blue Bridge“ pagal 2004-01-27 sutartį Nr. 10530/4/9.
[109] *SCALA* sistemos atstatymo planas pateiktas UAB „Blue Bridge“ pagal 2004-01-27 sutartį Nr. 10530/4/9.
[110] *SCALA* sistemos atstatymo bandymų protokolas pateiktas UAB „Blue Bridge“ pagal 2004-01-27 sutartį Nr. 10530/4/9.
[111] Informacijos saugos audito ataskaita pateikta UAB „Blue Bridge“ pagal 2006-12-15 sutartį Nr. 10530/461459.
[112] Informacinių technologijų pažeidžiamumų analizė pateikta UAB „Blue Bridge“ pagal 2006-12-15 sutartį Nr. 10530/461459.
[113] AB Rytų skirstomųjų tinklų pirkimų ir logistikos direktoriaus 2006-03-02 patvirtintas Informacijos saugos bei valdymo priemonių įgyvendinimo planas.
[114] Informacijos apsaugos valdymo sistemos vertinimas. Informacijos apsaugos valdymo analizės ataskaita. Technologinės informacijos apsaugos analizės ataskaita pateikta UAB „Blue Bridge“ pagal 2004-01-27 sutartį Nr. 10530/4/9.

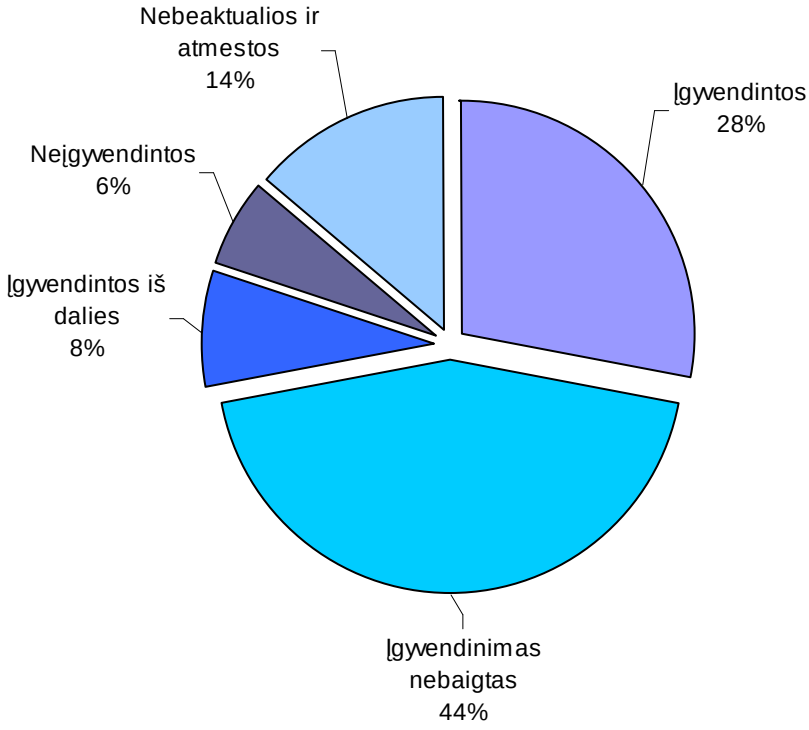
2 pav. UAB „Blue Bridge" informacijos saugumo konsultantų 2004 m. pateiktų rekomendacijų įgyvendinimas RST (2007 m. spalio mėn. duomenys)



Šaltinis – Valstybės kontrolė

Atlikę 2006 m. UAB „PricewaterhouseCoopers“ ir 2007 m. UAB „Blue Bridge“ informacijos saugumo konsultantų pateiktų rekomendacijų įgyvendinimo peržiūrą, valstybiniai auditoriai nustatė, kad 2007 m. spalio mėnesį įgyvendinta 14 rekomendacijų, 22 įgyvendinamos ir nebaigtos įgyvendinti, 4 įgyvendintos iš dalies, 3 neįgyvendintos, 7 nebeaktualios ir atmestos (3 pav.).

3 pav. UAB „PricewaterhouseCoopers“ 2006 m. ir UAB „Blue Bridge“ informacijos saugumo konsultantų 2007 m. pateiktų rekomendacijų įgyvendinimas RST (2007 m. spalio mėn. duomenys)



Šaltinis – Valstybės kontrolė

Analizuodami 2004–2007 m. RST atliktų specializuotų informacinės saugos auditų medžiagą, valstybiniai auditoriai nustatė, kad nuo 2004 m. pateiktos 74 informacinės saugos rekomendacijos iki 2007 spalio 1 d. bendrovėje įgyvendintos iš dalies, 60 jų įgyvendinti nebaigta, o 6 liko neįgyvendintos.

Rizika

RST neužtikrinama pakankama iš išorės samdomų kompanijų atliktų specializuotų informacinių sistemų saugos auditų rekomendacijų įgyvendinimo kontrolė, todėl yra rizika, kad nebus naudojamasi atliktų auditų pridėtine verte ir (arba) jų įgyvendinimas gali būti nerezultatyvus.

2. AB RYTŲ SKIRSTOMŲJŲ TINKLŲ INFORMACINĖS SISTEMOS ATITIKTIS LIETUVOS RESPUBLIKOS TEISĖS AKTAMS

Valstybinio audito metu įvertinta RST informacinės sistemos atitiktis Lietuvos Respublikos teisės aktų reikalavimams ir rekomendacijoms.

Audituojamu laikotarpiu atliktas RST saugos principų, organizavimo pagrindų atitikties vertinimas Ūkio ministerijos nustatytiems informacinės[115] ir fizinės[116] saugos reikalavimams. Fizinės saugos reikalavimai vertinti tik tiek, kiek jie susiję su RST informacine sauga. Dalis RST fizinės saugos ir bendrovės IT saugos organizavimo procedūrų įvertinta vadovaujantis Bendrosiomis priešgaisrinės saugos taisyklėmis[117] ir Darbo su videoterminalais saugos ir sveikatos reikalavimais[118].

RST informacinėje sistemoje tvarkomų asmens duomenų valdymo ir apsaugos priemonių atitiktis vertinta vadovaujantis Asmens duomenų teisinės apsaugos įstatymo[119] ir Valstybinės duomenų apsaugos inspekcijos reikalavimais[120].

> RST informacijos ir fizinės saugos valdymas ir tvarkymas atitinka teisės aktų reikalavimus arba rekomendacijas, išskyrus valstybinio audito ataskaitos 3 priedo 1 ir 2 lentelėse nurodytus pastebėjimus.

[115] Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymas Nr. 4-349 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimų patvirtinimo“.
[116] Lietuvos Respublikos ūkio ministro 2004-09-15 įsakymas Nr. 4-334 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių fizinės saugos reikalavimų patvirtinimo“.
[117] Priešgaisrinės apsaugos ir gelbėjimo departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2005-02-18 įsakymas Nr. 64 „Dėl Bendrųjų priešgaisrinės saugos taisyklių patvirtinimo ir kai kurių Priešgaisrinės apsaugos departamento prie Vidaus reikalų ministerijos ir Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus įsakymų pripažinimo netekusiais galios“.
[118] Lietuvos Respublikos sveikatos apsaugos ministro 2005-12-16 įsakymas Nr. V-984 „Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2004 m. vasario 12 d. įsakymo Nr. V-65 „Dėl Lietuvos higienos normos HN 32:2004 „Darbas su videoterminalais. Saugos ir sveikatos reikalavimai“ patvirtinimo“ pakeitimo“.
[119] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 1996-06-11 Nr. I-1374.
[120] Valstybinės duomenų apsaugos inspekcijos direktoriaus 2006-02-06 įsakymas Nr. 1T-9 „Dėl Valstybinės duomenų apsaugos inspekcijos direktoriaus 2004 m. sausio 13 d. įsakymo Nr. 1T-7 „Dėl reikalavimų duomenų apsaugos priemonių aprašui ir duomenų apsaugos priemonių aprašo“ pakeitimo“.

3. AB RYTŲ SKIRSTOMŲJŲ TINKLŲ INFORMACINĖS SISTEMOS BRANDA

Informacinių sistemų audito metodinėse rekomendacijose[121] rekomenduojama pagal Gebos brandos modelį (angl. *Capability Maturity Model* – CMM) įvertinti informacinių sistemų vidaus kontrolę. Informacinių sistemų brandos vertinimo kriterijai pateikti valstybinio audito ataskaitos 2 priede. RST informacinės sistemos brandos vertinimas atliekamas tam, kad būtų galima nustatyti tolesnio bendrovės informacijos valdymo procesų tobulinimo kriterijus.

Atsižvelgiant į šioje ataskaitoje pateiktus faktus, RST informacinės sistemos vidaus kontrolės branda apibrėžiama kaip **1. Pirminis / *Ad Hoc* procesas** (2 priedas). RST informacinės sistemos vidaus kontrolės branda grafiškai pavaizduota 4 paveiksle.

4 pav. RST informacinės sistemos vidaus kontrolės brandos lygis

GEBOS BRANDOS MODELIS (angl. - *CMM*)

	(a)	(b)	(c)	(d)	CMM
Optimalus procesas (5)	✗	✗	✗	✗	◆
Lengvai valdomas ir vertinamas procesas (4)	✗	✗	✗	✗	◆
Apibrėžtas procesas (3)	✗	✗	✗	✗	◆
Pasikartojantis, bet intuityvus procesas (2)	✓	!	✗	✓	△
Pirminis / Ad Hoc procesas (1)	✓	✓	✓	✓	●
Neegzistuojantis procesas (0)	✓	✓	✓	✓	●

✗	- neatitinka kriterijų
!	- nevisiškai atitinka kriterijų
✓	- atitinka kriterijų
◆	- nepasiektas tam tikras Gebos brandos lygis
△	- nevisiškai pasiektas tam tikras Gebos brandos lygis
●	- pasiektas tam tikras Gebos brandos lygis

(a) - problemos pripažinimas ir informavimas apie ją;
(b) - politika;
(c) - susiję procesai ir mokymas, skirti politikai įgyvendinti;
(d) - politikos efektyvumo ir susijusių procesų vertinimas ir tobulinimas, remiantis šiuo pagrindu.

Šaltinis – Valstybės kontrolė

Norint pasiekti aukštesnį brandos lygį, RST turėtų būti išsami informacinės saugos politika, pakankamai dokumentuotos procedūros. Bendrovėje reikėtų atlikti RST informacinės sistemos rizikos vertinimą, patobulinti informacinių sistemų saugos auditų rekomendacijų įgyvendinimo peržiūras. Apie problemas prireikus informuojama visa bendrovė, tačiau turėtų būti pakankamai formalizuoti procesai, susiję su jų stebėsena.

[121] Lietuvos Respublikos valstybės kontrolieriaus 2006-04-27 įsakymas Nr. V-65 „Dėl Informacinių sistemų metodinių rekomendacijų patvirtinimo“.

IŠVADOS IR REKOMENDACIJOS

Išvados

Dėl informacinių sistemų brandos:

- Akcinės bendrovės Rytų skirstomųjų tinklų informacinės sistemos vidaus kontrolės branda apibrėžiama kaip 1. Pirminis / *Ad Hoc* procesas (3 dalis).

Rekomendacijos

- Sukurti ir patvirtinti informacinių sistemų vystymo strateginio plano peržiūros ir kokybės užtikrinimo procedūras (1.1 dalis).
- Apsvarstyti galimybę sudaryti IT valdymo komitetą ir komisiją, koordinuojančią bendrovės informacijos saugos procesus, apimančius visas informacines sistemas (1.2 dalis).
- Patvirtinti informacinės sistemos ir jos posistemių valdytojus *(owner)* (1.2 dalis).
- Atlikti informacinės sistemos rizikos vertinimą. Numatyti šių informacinių išteklių rizikos vertinimo periodiškumą arba pakartotinį rizikos vertinimą, atsižvelgiant į reikšmingus valdymo, saugos ir informacinio turto pokyčius (1.3 dalis).
- Patvirtinti saugumo politiką ir jos įgyvendinimą reglamentuojančius dokumentus. Sukurti ir (arba) atnaujinti trūkstamus informacijos saugos politikos dokumentus. Su patvirtinta informacijos saugumo politika ir jos įgyvendinimą reglamentuojančias dokumentais pasirašytinai supažindinti informacinių sistemų naudotojus (1.4, 1.5 dalys).
- Atlikti kompiuterių programų ir intelekto produktų (ilgalaikio nematerialiojo turto) inventorizaciją ir užtikrinti jų apskaitą teisės aktų nustatyta tvarka (1.5.2 dalis).
- Tobulinti informacinių sistemų auditų rekomendacijų pažangos stebėjimo (poauditinės veiklos) valdymo procesus (1.6 dalis).
- Išanalizuoti kitus valstybinio audito ataskaitoje ir jos prieduose nurodytus pastebėjimus ir numatyti priemones ir prioritetus pastebėtiems trūkumams pašalinti (visos dalys).

Informacinių sistemų valdymo ir
audito departamento direktorius — Dainius Jakimavičius

Valstybinis auditorius — Rimgaudas Gamulis

Valstybinio audito ataskaitos kopijos (2 egz.) pateiktos Lietuvos Respublikos Vyriausybei ir Lietuvos Respublikos ūkio ministerijai.

PRIEDAI

Valstybinio audito ataskaitos
„Akcinės bendrovės Rytų skirstomųjų tinklų informacinės sistemos bendrosios kontrolės vertinimas“
1 priedas

Vartojamų santrumpų ir sąvokų paaiškinimas

- **CMM** – Gebos brandos modelis *(Capability Maturity Model).*
- **COBIT** – viena iš populiariausių IT valdymo metodologijų, kuriama ir palaikoma tarptautinės *ISACA* organizacijos *(Control Objectives Management Guidelines Maturity Models).*
- **INTOSAI –** Tarptautinė aukščiausiųjų audito institucijų organizacija.
- **ISACA** – Informacinių sistemų audito ir kontrolės asociacija.
- **ISO/IEC 17799** – Informacijos technologija. Informacijos saugumo valdymo praktikos kodeksas *(Information technology. Security techniques. Code of practice for information security management).*
- **ISO/IEC 20000-2** – Praktikos kodeksas *(Code of Practice).*
- **ISO/IEC 27001** – Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai *(Information technology. Security techniques. Information security management systems. Requirements).*
- **IT –** Informacinės technologijos.
- **ITIL** – pripažintas standartais: D. Britanijos BS-15000 bei tarptautiniu ISO-20000, ITIL suderinamas ir su visais ISO-9000 reikalavimais *(Information Technology Infrastructure Library).*
- **LT ISO/IEC 17799** – Lietuvos standartas. Informacijos technologija. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 17799).
- **LT ISO/IEC 27001** – Lietuvos standartas. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai (tapatus ISO/IEC 27001).
- **OSL** – visą įmonę apimanti programinės įrangos licencijų abonentinė sutartis *(Microsoft Open Subscription Licence (OSL)).*
- **RST –** AB Rytų skirstomieji tinklai.
- **SCADA** – AB Rytų skirstomųjų tinklų automatizuotos dispečerinio valdymo sistemos, kurios stebi ir valdo bendrovės elektros skirstomojo tinklo sistemas *(Supervisory control and data acquisition).*
- **Ūkio ministerija** – Lietuvos Respublikos ūkio ministerija.

Valstybinio audito ataskaitos
„Akcinės bendrovės Rytų skirstomųjų tinklų informacinės sistemos bendrosios kontrolės vertinimas“
2 priedas

Gebos brandos modelis

Šiame priede apibūdinamas Gebos brandos modelis, taikomas informacinės sistemos kontrolės tikslų brandos lygiui įvertinti.

Pateiktas kiekvieno tikslo įvertinimas yra žemiausias atitinkamo tikslo įvertinimas pagal bet kurį iš toliau išvardytų keturių punktų (a-d). Vertinimo vidurkis neišvedinėjamas, nes sudėtinių vertinimų vidurkiai neatspindi realios situacijos.

Kiekvienoje kategorijoje analizuojami šie aspektai:

a) Problemos pripažinimas ir informavimas apie ją

b) Politika

c) Susiję procesai ir mokymas, skirti politikai įgyvendinti

d) Politikos efektyvumo ir susijusių procesų vertinimas ir tobulinimas, remiantis šiuo pagrindu.

0. Neegzistuojantis procesas

a) Organizacija nepripažįsta spręstinos problemos egzistavimo ir dėl to apie tai nepateikia jokios informacijos.

b) Šiuo klausimu nėra jokios politikos.

c) Nėra jokio atpažįstamo proceso, susijusio su šia problema.

d) Neatliekamas joks vertinimas, susijęs su šia problema.

1. Pirminis/*Ad Hoc* procesas

a) Yra faktų, patvirtinančių, kad organizacija pripažįsta problemos egzistavimą ir būtinumą ją spręsti, tačiau apie tai per mažai informuojama.

b) Egzistuoja neišsami politika. Ji netinkamai dokumentuojama, skelbiama arba įgyvendinama.

c) Individualiu arba kiekvienu konkrečiu atveju taikomi *ad hoc* metodai. Problema nenagrinėjama valdybos lygiu.

d) Stebėsena vykdoma reaguojant į incidentą, dėl kurio organizacija patiria tam tikrą nuostolį.

2. Pasikartojantis, bet intuityvus procesas

a) Apie problemą (prireikus) atitinkamai informuojama visa organizacija.

b) Egzistuoja aiški politika.

c) Su problema susiję procesai formaliai yra nustatyti, aktyviai dalyvaujant ir prižiūrint vadovybei, tačiau taikomi ne visoje organizacijoje. Mokymas neorganizuojamas, o informavimas apie standartus ir pareigas paliktas individualių darbuotojų nuožiūrai.

d) Vadovybė yra nustačiusi pagrindinius vertinimus ir vertinimo metodus bei būdus, tačiau pastarieji parengti nepakankamai.

3. Apibrėžtas procesas

a) Visa organizacija supranta, kad reikia reaguoti į problemą, ir tam pritaria.

b) Organizacijoje vykdoma tvirta ir aiški politika, suderinta su kai kuriomis kitomis susijusiomis politikos kryptimis. Iš dalies atsižvelgiama į rizikos valdymą.

c) Procedūros standartizuotos, dokumentuotos ir dauguma jų įgyvendinamos visoje organizacijoje. Vadovybė yra informavusi apie standartizuotas procedūras ir vykdo neformalų mokymą. Nors procedūras galima įvertinti, tačiau jos nėra sudėtingos ir formaliai atspindi esamą patirtį.

d) Susijusių veiklos sričių rodiklių registravimas ir stebėsena padeda tobulinti veiklą. Beveik visų susijusių procesų stebėsena vykdoma pagal tam tikrus (pirminius) dokumentus, tačiau mažai tikėtina, kad vadovybė galėtų pastebėti bet kokį nukrypimą, kadangi tokios priemonės paprastai taikomos individualiai. Priežasčių analizė atliekama retai.

4. Lengvai valdomas ir vertinamas procesas

a) Visais atitinkamais organizacijos lygiais problema suprantama tinkamai ir reikalaujama imtis priemonių.

b) Vykdoma tvirta ir aiški politika, integruota su kitomis susijusiomis politikos kryptimis. Atsižvelgiama į rizikos valdymą.

c) Organizacija gerai pažįsta savo klientą ir turi aiškiai apibrėžtas pareigas. Procesai yra aiškiai suformuluoti, integruoti ir taikomi visoje organizacijoje. Procesai yra gerai įsisavinami ir palaikomi organizuojant atitinkamą mokymą. Visi susijusių procesų dalyviai žino apie riziką ir galimybes.

d) Susijusių procesų tobulinimas visų pirma yra pagrįstas kiekybiniu supratimu, užtikrinant galimybę stebėti ir vertinti, kaip laikomasi procedūrų bei susijusių procesų dokumentų reikalavimų. Vadovybė yra nustačiusi leistinus nukrypimus, į kuriuos būtina atsižvelgti, vykdant susijusius procesus. Paaiškėjus, kad procesai yra neveiksmingi arba neefektyvūs, dažniausiai, tačiau ne visada, imamasi priemonių. Kartais susiję procesai tobulinami, įgyvendinant geriausią vidaus praktiką. Vykdomas priežasčių analizės standartizavimas. Pradedamas nuolatinis veiklos gerinimo procesas.

5. Optimalus procesas

a) Problemos ir jos sprendimo būdų vertinimas yra pažangus bei perspektyvus.

b) Organizacija vykdo tvirtą ir aiškią politiką, integruotą su visomis kitomis susijusiomis politikos kryptimis, visapusiškai atsižvelgiant į rizikos valdymą.

c) Susiję procesai atnaujinti, atsižvelgiant į geriausią išorinę praktiką ir nuolatinio veiklos tobulinimo bei brandos modeliavimo rezultatus kitose organizacijose. Susijusių procesų rizika ir rezultatai yra apibrėžti, suderinti, ir apie juos informuojama visa organizacija. Organizuojamas modernus mokymas ir informavimas. Įgyvendinama politika užtikrino organizacijos, darbuotojų ir procesų sugebėjimą greitai prisitaikyti ir visapusiškai palaikyti rizikos struktūros pokyčius.

d) Stebėsena, savęs vertinimas ir informavimas apie problemą (prireikus) vykdomi visos organizacijos lygiu, optimaliai išnaudojant procesus ir technologijas, naudojamus vertinimo, analizės, informavimo ir mokymo tikslais. Analizuojamos visų problemų ir nukrypimų priežastys, laiku numatant ir inicijuojant veiksmingas priemones. Naudojamasi nepriklausomų ekspertų konsultavimo paslaugomis ir lyginamąja analize.

Valstybinio audito ataskaitos „Akcinės bendrovės Rytų skirstomųjų tinklų informacinės sistemos bendrosios kontrolės vertinimas“ 3 priedas

Neatitiktis privalomiems vykdyti teisės aktų reikalavimams ir rekomendacijoms

1 lentelė. Valstybinių auditorių pastebėjimai dėl informacinės saugos reikalavimų ir rekomendacijų laikymosi

Eil. Nr.	Teisės akto reikalavimai	Pastebėjimas
Lietuvos Respublikos ūkio ministro 2004-09-22 įsakymas Nr. 4-349 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių informacinės saugos reikalavimų patvirtinimo“.		
1.	*11 punktas:* Informacija, kuri laikoma komercine (gamybine) paslaptimi, taip pat kita Įmonės disponuojama informacija turi būti klasifikuojama, siekiant numatyti apsaugos poreikį, prioritetus ir laipsnį. Informacijos klasifikavimo sistema naudojama, siekiant apibrėžti tinkamą konkrečios informacijos apsaugos lygį. Informacijos apsaugos lygiai nustatomi įvertinant galimas grėsmes ir jų pasekmes Įmonei. Įmonė privalo periodiškai peržiūrėti grėsmes įmonei ir jos informacinei sistemai, siekiant atsižvelgti į komercinės veiklos reikalavimų ir prioritetų pokyčius, aptarti naujas grėsmes ir pavojus bei patvirtinti, kad esami informacinės saugos priežiūros metodai vis dar veiksmingi ir tinkami.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo atliktas rizikos (grėsmių) vertinimas, todėl valstybiniai auditoriai negalėjo įvertinti, ar esami informacinės saugos priežiūros metodai bendrovėje veiksmingi ir tinkami. RST parengtos konfidencialios ir riboto naudojimo informacijos taisyklės ir jos 2 priedas (AB Rytų skirstomųjų tinklų komercinių paslapčių sąrašas), tačiau bendrovėje šie dokumentai nėra atnaujinti nuo 2005-05-19. Su IT susijusi informacija, kuri RST laikoma komercine (gamybine) paslaptimi audituojamu laikotarpiu (iki 2007-10-01) bendrovėje nebuvo klasifikuojama atsižvelgiant į apsaugos poreikį, prioritetus ir laipsnį.
2.	*13 punktas:* Saugoma informacija, o ypač informacija, sudaranti Įmonės komercinę (gamybinę) paslaptį, turi būti pateikiama griežtai laikantis principo „Būtina žinoti“. Principas „Būtina žinoti“ reiškia, kad saugoma informacija gali būti pateikta tik atitinkamus leidimus dirbti ar susipažinti su šia informacija turintiems asmenims, kuriems vykdant pareigas reikia susipažinti su šia informacija. Asmeniui turi būti pateikta tokios apimties saugoma informacija, kokios reikia jo pareigoms atlikti.	RST pasirašoma konfidencialumo sutartis su RST darbuotojais, tačiau audituojamu laikotarpiu (iki 2007-10-01) joje nebuvo aiškiai nurodyta prie kokios konfidencialios informacijos pasirašantis pasižadėjimą asmuo turi teisę prieiti.
3.	*15 punktas:* Apie visus informacijos saugos reikalavimų pažeidimus, kurie gali lemti ar lėmė informacijos praradimą ar neteisėtą atskleidimą, nedelsiant turi būti pranešta atsakingam asmeniui, o šis privalo imtis reikiamų priemonių tolesniam informacijos atskleidimui ar praradimui sustabdyti ir neigiamoms pasekmėms sumažinti, taip pat privalo nedelsdamas pranešti Įmonės vadovui ir jo nustatyta tvarka turi atlikti tyrimą dėl informacijos saugos reikalavimų pažeidimų faktų nustatymo.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo formalizuota saugos incidentų valdymo procedūra.
4.	*17 punktas:* Siekiant įdiegti informacinės saugos sistemą ir ją valdyti, turi būti sudaroma šios sistemos valdymo struktūra, paskirti darbuotojai, atsakingi už sistemos diegimą ir priežiūrą. Atsakomybė už atskirų informacijos rūšių apsaugą ir saugumo procedūrų taikymą turi būti aiškiai apibrėžta.	RST informacinei sistemai ir kiekvienai jos eksploatuojamai posistemei audituojamu laikotarpiu (iki 2007-10-01) nebuvo paskirtas valdytojas *(owner)* t. y. vadovas atsakingas už visos RST informacinės sistemos ir kiekvienos jos posistemės valdymą, naudojimą ir saugumą. RST parengta, bet bendrovės vadovybės nepatvirtinta saugumo politika ir kai kurie jos įgyvendinimą reglamentuojantys dokumentai.
5.	*20 punktas:* Įmonės vadovo ar jo įgalioto asmens sprendimu turi būti paskirtas atsakingas asmuo arba atsakingi asmenys, organizuojantys ir įgyvendinantys saugomos informacijos ar jos atitinkamų dalių administravimą, apsaugą ir kontrolę. Atsakingas asmuo: 20.1. organizuoja informacijos apskaitą ir kontroliuoja	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo nustatyti terminai, kuriais vadovaudamasis atsakingas asmuo turi organizuoti saugomos informacijos patikrinimą, nevisiškai formalizuotos skirtingiems apsaugos lygiams priskirtos informacijos rengimo, įforminimo, registracijos, siuntimo, gabenimo, gavimo, dauginimo, saugojimo, sunaikinimo bei

Eil. Nr.	Teisės akto reikalavimai	Pastebėjimas
	jos apyvartą, tvarko jos registraciją; 20.2. atrenka naikintiną informaciją, teikia siūlymus pakeisti saugomos informacijos apsaugos lygį; 20.3. atsako už saugomos informacijos registracijos laikmenų tvarkymą; 20.4. atsako už ypatingai saugomos informacijos perdavimą sankcionuotiems vartotojams; 20.5. atsako už tai, kad informacijos vartotojai būtų laiku informuojami apie saugomos informacijos apsaugos lygio keitimą; 20.6. Įmonės vadovo nustatytais terminais organizuoja saugomos informacijos patikrinimą; 20.7. organizuoja saugomos informacijos laikmenų naikinimo procesą.	apskaitos procedūros.
6.	*21 punktas:* Informacinės sistemos elementai (informacija, programinė įranga, techninė įranga) įmonėje turi būti apskaitomi ir priskiriami konkretiems asmenims, numatant jų atsakomybę už tinkamą apskaitą bei priežiūrą.	Audituojamu laikotarpiu (iki 2007-10-01) RST finansinės apskaitos dokumentuose nebuvo registruojama programinė įranga, kurią pagal bendrovės padalinių poreikį sukūrė RST IT skyriaus specialistai, nebuvo sistemingai valdomi dalies bendrovės informacinės sistemos konfigūracijos elemento informacijos (duomenų laikmenų) registracijos procesai, neformalizuoti atsakingų asmenų veiksmai ir saugos priemonės skirtos apsaugoti šią informacijos dalį nuo žalos, vagystės ir nesankcionuoto priėjimo.
7.	*22 punktas:* Įmonėje turi būti apibrėžtos tinkamos informacijos žymėjimo ir priežiūros procedūros, atsižvelgiant į Įmonėje priimtą informacijos apsaugos lygių klasifikavimo schemą. Šios procedūros turi apimti fizinius ir elektroninius informacijos aprašų formatus.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo atliktas rizikos (grėsmių) vertinimas, todėl valstybiniai auditoriai negali įvertinti bendrovėje taikomų informacijos žymėjimo ir priežiūros metodų tinkamumo. RST apibrėžtos informacijos žymėjimo ir priežiūros procedūros, tačiau audituojamu laikotarpiu (iki 2007-10-01) jos neapėmė bendrovės elektroninių informacijos aprašų formatų t.y. klasifikuotos informacijos kompiuterinėje formoje žymėjimo, naudojimo, laikymo, siuntimo ir saugojimo procesų.
8.	*23 punktas:* Reguliariai turi būti peržiūrimas reikalavimų informaciniam saugumui įgyvendinimas, siekiant įsitikinti, ar Įmonės praktika tinkamai atspindi informacinės saugos principus, ar ji yra tinkamai vykdoma. Toks peržiūrėjimas gali būti atliktas vidinio audito metu arba kitų įmonių ar organizacijų, kurios turi reikiamą patirtį įmonių informacinės saugos srityje.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo formalizuotas iš išorės samdomų informacinės saugos auditų ir jų rezultatų poauditinės kontrolės procesų valdymas bei pateiktų rekomendacijų įgyvendinimo planavimas.
9.	*24 punktas:* Įmonės darbuotojų atsakomybę už informacinės saugos reikalavimų vykdymą būtina numatyti jų įdarbinimo stadijoje, įtraukiant į darbo sutartis atitinkamas nuostatas ir/ar supažindinant juos su Įmonės vidaus darbo taisyklėmis, kuriose yra numatyta pareiga vykdyti informacinės saugos reikalavimus, ir kontroliuoti darbuotojo veiksmus darbo metu.	RST numatyta atsakomybė už informacinės saugos reikalavimų vykdymą, tačiau šios nuostatos bendrovėje nėra atnaujintos nuo 2005-05-19.
10.	*25 punktas:* Potencialius darbuotojus, ypač priimamus darbui su aukštesnio apsaugos lygio informacija, reikia tinkamai tikrinti. Įmonėje turi būti nustatytos potencialių darbuotojų tikrinimo procedūros.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo nustatytos potencialių darbuotojų tikrinimo procedūros.
11.	*26 punktas:* Tiesioginiai vadovai turi įvertinti, kokios priežiūros reikia naujiems ir nepatyrusiems darbuotojams, kurių kreiptis į aukštesnio apsaugos lygio informaciją yra sankcionuota. Tiesioginiai vadovai turi periodiškai peržiūrėti jiems pavaldžių darbuotojų darbą informacinės saugos procedūrų laikymosi požiūriu.	RST vadovai audituojamu laikotarpiu (iki 2007-10-01) formaliai nevertino, kokios priežiūros reikia naujiems ir nepatyrusiems darbuotojams, kurių kreiptis į aukštesnio apsaugos lygio informaciją yra sankcionuota.
12.	*28 punktas:* Apie incidentus informacinės saugos srityje turi būti pranešama kiek galima skubiau. Turi būti sukurta formali pranešimo procedūra ir reagavimo į incidentą procedūra, nustatanti veiksmus, kurių reikia	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo naudojami mechanizmai kurie leistų kiekybiškai įvertinti ir kontroliuoti saugumo incidentų bei trikdžių tipus, apimtis ir kainas, neformalizuota saugos incidentų valdymo procedūra.

Eil. Nr.	Teisės akto reikalavimai	Pastebėjimas
	imtis gavus pranešimą apie incidentą. Visi darbuotojai ir rangovai turi būti informuojami apie saugumo incidentų pranešimams skirtas procedūras. Turi būti įdiegti tinkami grįžtamojo ryšio procesai, siekiant užtikrinti, kad tie, kurie pranešė apie incidentą, bus informuoti apie rezultatus, incidentui pasibaigus. Iš informacijos paslaugų vartotojų reikia reikalauti atkreipti dėmesį ir pranešti apie bet kurį pastebėtą arba įtariamą informacijos saugumo trūkumą arba sistemoms ar paslaugoms kilusią grėsmę. Turi būti numatomi mechanizmai, kurie leistų kiekybiškai įvertinti ir kontroliuoti incidentų bei trikdžių tipus, apimtis ir kainas. Šią informaciją reikia naudoti, siekiant identifikuoti pasikartojančius arba didelį poveikį darančius incidentus arba trikdžius. Tai gali nulemti informacinės saugos priežiūros metodų išplėtimą arba papildymą, siekiant apriboti būsimų įvykių dažnį, žalos vertę ir kainą.	
13.	*29 punktas:* Saugoma informacija, jos apdorojimo įranga nuo nesankcionuoto priėjimo, žalos ir trukdžių turi būti apsaugotos fiziškai. Patalpų, kuriose yra saugoma aukštesnio apsaugos lygio informacija ar jos apdorojimo įranga, fizinės saugos lygis turi atitikti identifikuotas grėsmes bei galimas pasekmes. Taikomos fizinės saugos priemonės turi užtikrinti, kad į šias patalpas galėtų patekti tik įgalioti darbuotojai.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo atliktas bendrovėje esančių netechnologinių patalpų (duomenų centrai, serverinės, ryšio komutacinės patalpos ir k.t.) fizinės saugos rizikos (grėsmių) vertinimas, neparengtos darbo patalpose, kuriose yra saugoma aukštesnio apsaugos lygio informacija ar jos apdorojimo įranga taisyklės, Į RST centrinės buveinės ir Vilniaus regiono serverinių patalpas patenka tik įgalioti darbuotojai, tačiau audituojamu laikotarpiu (iki 2007-10-01) nebuvo personalizuotas patekimas į šias patalpas naudojantis ID kortele. RST Vilniaus regiono serverinės patalpose yra įdiegta praėjimo naudojantis ID kortele ir kodu sistema, tačiau naudojamasi tik ID kortele. **Pastaba** 2007-10-23 RST generalinio direktoriaus įsakymu Nr. 153 patvirtinta AB Rytų skirstomųjų tinklų objektų fizinės saugos tvarka.
14.	*30 punktas:* Informacija ir ją apdorojanti įranga turi būti fiziškai apsaugota ne tik nuo saugumo grėsmių, bet ir aplinkos pavojų, vagysčių, sprogimų, dūmų, ugnies, vandens, dulkių, vibracijos, cheminio poveikio, mechaninio poveikio, elektros maitinimo nutrūkimo.	Audituojamu laikotarpiu (iki 2007-10-01) RST centrinės buveinės ir Vilniaus regiono serverinės patalpos nebuvo apsaugotos nuo grėsmių kylančių dėl dulkių ir cheminio poveikio. Valstybinio audito metu (2007-10-25) RST centrinės buveinės ir Vilniaus regiono serverinės patalpose buvo sandėliuojama tuo metu nenaudojama IT įranga.
15.	*31 punktas:* Įmonėje turi būti nustatytos visos informacijos apdorojimo įrangų darbo ir valdymo procedūros ir jų vykdymo atsakomybė, kuri turi būti užfiksuota darbo instrukcijose ir reagavimo į incidentus procedūrose. Darbo instrukcijos ir procedūros turi būti įformintos kaip vidiniai Įmonės teisės aktai, privalomi darbuotojams. Darbo instrukcijose ir procedūrose turi būti smulkiai apibrėžiamas kiekvieno šių darbų vykdymas: 31.1. informacijos apdorojimas ir priežiūra; 31.2. instrukcijos, kaip tvarkyti klaidas ar kitas išimtines sąlygas, kurios kiltų atliekant darbus; 31.3. instrukcijos, kilus netikėtiems darbo arba techniniams sunkumams; 31.4. sistemos kartotinio paleidimo ir atkūrimo procedūros.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo patvirtintos visos instrukcijos susijusios su eksploatuojamų sistemų kartotinio paleidimo ir atkūrimo procedūromis.
16.	*32 punktas:* Vartotojų priėjimas prie ADA sistemų ir tinklų turi būti fiksuojamas ir kontroliuojamas. Suteikiant priėjimą prie kolektyvinio naudojimo informacijos sistemos, turi būti parengta vartotojo registravimo ir išregistravimo procedūra.	Vartotojų priėjimas prie RST sistemų yra fiksuojamas ir kontroliuojamas, tačiau, audituojamu laikotarpiu (iki 2007-10-01) bendrovėje nebuvo formalizuota vartotojo registravimo ir išregistravimo procedūra, apimanti personalo skyriaus valdomus darbuotojų priėmimo, atleidimo ir

Eil. Nr.	Teisės akto reikalavimai	Pastebėjimas
		perkėlimo procesus, nebuvo apibrėžtos ir nustatytos kolektyvinio naudojimo sistemos.
17.	*33 punktas:* Įmonėje turi būti parengta slaptažodžių naudojimo tvarka. Slaptažodžiai yra vartotojų tapatybės patvirtinimo priemonė.	RST parengta slaptažodžių naudojimo tvarka, tačiau audituojamu laikotarpiu (iki 2007-10-01) joje nebuvo apibrėžtos reguliarios vartotojų ir sistemų slaptažodžių audito procedūros, pirmo ir laikino slaptažodžio suteikimo procedūra.
18.	*34 punktas:* Turi būti nustatomi naujų informacijos sistemų, jų modifikacijų ir naujų versijų priėmimo kriterijai ir prieš priimant vykdomi tinkami sistemos bandymai. Atitinkami atsakingi asmenys ir padalinių vadovai turi užtikrinti, kad naujoms sistemoms keliami reikalavimai ir priėmimo kriterijai būtų aiškiai apibrėžti, aptarti, įforminti ir išbandyti.	RST parengti, bet audituojamu laikotarpiu (iki 2007-10-01) bendrovės vadovybės nebuvo patvirtinti „Bendrieji reikalavimai Informacinių sistemų ir Programų kūrimui“, neformalizuotos konfigūracijos valdymo ir keitimų valdymo procedūros.
19.	*35 punktas:* Būtina įdiegti apsaugos priemones nuo kenkėjiškos programinės įrangos poveikio. Turi būti įgyvendintos tinkamos vartotojų informavimo procedūros ir taikomi kenkėjiškos programinės įrangos aptikimo ir išvengimo metodai.	RST parengta apsaugos nuo nepageidaujamų programų (virusų, kenkėjiškų programų) tvarka, tačiau audituojamu laikotarpiu (iki 2007-10-01) joje nebuvo nenumatytas RST informacinės sistemos ir jos posistemių pažeidžiamumo patikrų periodiškumas.
20.	*36 punktas:* Siekiant užtikrinti galimą visos pagrindinės komercinės veiklos informacijos ir programinės įrangos atitaisymą esant nelaimei arba avarijai, reikia užtikrinti tinkamą informacijos dubliavimą bei saugojimą. Įmonė turi periodiškai kopijuoti informaciją ir programinę įrangą. Atsarginės duomenų laikmenos turi būti periodiškai bandomos.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo atliktas rizikos (grėsmių) susijusios su RST veiklos tęstinumo valdymu vertinimas, todėl valstybiniai auditoriai, negalėjo įvertinti bendrovėje taikomų informacijos dubliavimo ir saugojimo valdymo priemonių tinkamumo ir jų adekvatumo. RST parengta, bet audituojamu laikotarpiu (iki 2007-10-01) bendrovės vadovybės nebuvo patvirtinta „Rytų skirstomųjų tinklų“ informacinės sistemos tęstinumo ir atstatymo strategija. Sukauptos atsarginės duomenų laikmenos audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo periodiškai bandomos.
21.	*37 punktas:* Informacijos apdorojimo klaidos, apie kurias praneša vartotojai, ir ryšių sistemų klaidos turi būti fiksuojamos. Turi būti nustatytos aiškios klaidų įrašų priežiūros taisyklės, įskaitant klaidų žurnalo peržiūrėjimą, siekiant užtikrinti, kad klaidos būtų sėkmingai pašalintos, bei koregavimo veiksmų peržiūrėjimą, siekiant užtikrinti, kad priežiūros metodams nekiltų pavojus.	RST fiksuojamos informacijos apdorojimo klaidos, tačiau audituojamu laikotarpiu (iki 2007-10-01) nebuvo formaliai ir aiškiai nustatytos konfigūracijos elemento (informacijos) apdorojimo klaidų įrašų peržiūros bei koregavimo veiksmų priežiūros taisyklės.
22.	*38 punktas:* Būtina numatyti per viešuosius tinklus perduodamos informacijos apsaugos priemones, kurias reikia derinti su šių tinklų valdytojais.	RST sutartyse su „Omnitel“ ir „Infostruktūra“ nebuvo numatytos per šiuos tinklus perduodamos informacijos apsaugos priemonės, kurios būtų suderintos su šių tinklų valdytojais.
23.	*39 punktas:* Duomenų laikmenos turi būti apskaitomos, kontroliuojamos ir fiziškai apsaugomos. Turi būti parengtos ir patvirtintos darbo procedūros, skirtos apsaugoti dokumentus, kompiuterines laikmenas, įvesties (išvesties) duomenis ir sistemos dokumentus nuo žalos, vagystės ir nesankcionuoto priėjimo. Turi būti parengtos keičiamųjų kompiuterio laikmenų valdymo procedūros.	Audituojamu laikotarpiu (iki 2007-10-01) RST informacijos saugos dokumentacijoje nebuvo formalizuotos atsakingų asmenų priemonės ir veiksmai skirti apsaugoti dokumentus, kompiuterines laikmenas, įvesties (išvesties) duomenis ir sistemos dokumentus nuo žalos, vagystės ir nesankcionuoto priėjimo, nebuvo parengtos įrangos išėmimo ir išnešimo už bendrovės ribų tvarkos.
24.	*40 punktas:* Nenaudotinos informacijos laikmenos turi būti sunaikintos patikimai ir saugiai. Įmonėje turi būti parengtos privalomos informacijos laikmenų naikinimo procedūros.	RST parengta laikmenų naudojimo ir naikinimo tvarka, tačiau audituojamu laikotarpiu (iki 2007-10-01) joje nebuvo apibrėžtos ir nustatytos privalomos informacijos laikmenų naikinimo procedūros, nenustatytos kompiuterių ir jų laikmenų pakartotinio naudojimo tvarkos.
25.	*41 punktas:* Apsikeitimas informacija ir programine įranga su kitomis įmonėmis, organizacijomis ar asmenimis turi būti kontroliuojamas. Apsikeitimas turi būti vykdomas remiantis sutartimis. Turi būti parengtos procedūros, kad būtų apsaugota perduodama informacija ir laikmenos.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo formalizuotos procedūros detalizuojančios perduodamų laikmenų su klasifikuota informacija apsaugą, nebuvo numatyta, kokia klasifikuota informacija galima keistis ir kokią ne bendradarbiaujant su išorinėmis organizacijomis.

Eil. Nr.	Teisės akto reikalavimai	Pastebėjimas
26.	*42 punktas:* Įmonėje turi būti nustatyti kontrolės metodai, leidžiantys sumažinti interneto ir elektroninio pašto sukeliamas grėsmes.	RST parengta interneto ir elektroninio pašto naudojimosi tvarka, tačiau audituojamu laikotarpiu (iki 2007-10-01) joje nebuvo formaliai dokumentuoti bendrovėje praktiškai naudojami kontrolės metodai, leidžiantys sumažinti interneto ir elektroninio pašto sukeliamas grėsmes.
27.	*43 punktas:* Priėjimas prie tinklo paslaugų per vidinį ir išorinį tinklus turi būti kontroliuojamas. Būtina užtikrinti, kad turintys priėjimą prie tinklų paslaugų vartotojai nekeltų pavojaus tinklo paslaugų saugumui.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo formalizuota kompiuterių tinklo servisų ir kompiuterinio tinklo vartotojų teisių valdymo tvarka, eksploatuojamų sistemų žurnalizavimo kompiuteriniame tinkle procedūra. RST parengtos, bet audituojamu laikotarpiu (iki 2007-10-01) nebuvo patvirtintos loginės kompiuterinių tinklų schemos.
28.	*44 punktas:* Įmonėje turi būti nustatytos darbo, naudojant nešiojamąjį kompiuterį, ir darbo su saugoma informacija namuose sąlygos bei tvarka. Įmonė gali sankcionuoti veiklą namie ar su nešiojamuoju kompiuteriu tik tuo atveju, kai įsitikinama, kad yra numatytos tinkamos informacinės saugos sąlygos.	RST parengtos naudojimosi nešiojamais įrenginiais saugumo taisyklės, tačiau audituojamu laikotarpiu (iki 2007-10-01) jose nebuvo detalizuotos nutolusių vartotojų priėjimo procedūros.
29.	*45 punktas:* Kitų įmonių ar organizacijų priėjimas prie Įmonės saugomos informacijos ir jos apdorojimo įrangos turi būti kontroliuojamas. Sankcionuotas kitų įmonių ar organizacijų priėjimas prie Įmonės informacijos ir/ar jos apdorojimo įrangos galimas tik sutarčių, kuriose turi būti numatyti informacijos saugumo reikalavimai arba pateikiama nuoroda į juos, siekiant užtikrinti Įmonės informacinės saugos reikalavimų atitiktį, konfidencialumo įsipareigojimus ir atsakomybę už jų nesilaikymą, pagrindu.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo atliktas rizikos (grėsmių) vertinimas, todėl valstybiniai auditoriai negalėjo pareikšti nuomonės dėl trečiųjų šalių prieigos prie RST saugomos informacijos taikomų kontrolės priemonių adekvatumo. Kitų įmonių ar organizacijų priėjimas prie RST saugomos informacijos ir jos apdorojimo įrangos kontroliuojamas sudarant sutartis, taikant technologines priemones, tačiau audituojamu laikotarpiu (iki 2007-10-01) trečiųjų šalių autorizavimo RST procesai (kontrolės procedūros ir auditas) nebuvo formalizuoti.

Šaltinis – Valstybės kontrolė

2 lentelė. Valstybinių auditorių pastebėjimai dėl fizinės saugos reikalavimų ir rekomendacijų laikymosi

Eil. Nr.	Teisės akto reikalavimai	Pastebėjimas
Lietuvos Respublikos ūkio ministro 2004-09-15 įsakymas Nr. 4-334 „Dėl Strateginę reikšmę nacionaliniam saugumui turinčių, Ūkio ministerijos valdymo sričiai priskirtų įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių fizinės saugos reikalavimų patvirtinimo“.		
1.	*7 punktas:* Įmonių fizinės saugos sistema projektuojama, jos veikla organizuojama ir prižiūrima vadovaujantis šiais principais: 7.1. teisiniu fizinės saugos organizavimo ir veiklos pagrįstumu. Įmonių fizinės saugos sistema organizuojama ir veikia griežtai laikantis Lietuvos Respublikos įstatymų bei kitų teisės aktų, Įmonės vidaus teisės aktų reikalavimų; 7.2. Įmonės vadovo atsakomybe. Įmonės vadovas atsako už įmonės fizinės saugos sistemos organizavimą bei priežiūrą ir kontrolę. Įmonės vadovas turi nuolatos rūpintis Įmonės patikima fizine sauga. Tuo tikslu jis privalo: 7.2.1. periodiškai kontroliuoti įmonės fizinės saugos vykdymą, analizuoti fizinės saugos sistemos Įmonėje veiklą ir aptarti su Įmonės atsakingais darbuotojais fizinės saugos sistemos veiklos problemas bei reikiamas priemones šiai sistemai tobulinti; 7.2.2. bendradarbiauti su kompetentingomis valstybės institucijomis nusikalstamų veikų bei kitų teisės pažeidimų prevencijos klausimais.	Audituojamu laikotarpiu (iki 2007-10-01) RST fizinės saugos sistema buvo formuojama ir įgyvendinama fragmentiškai, nepakankamai dėmesio skiriant elektroninės informacijos ir pačių informacinių sistemų saugos organizacinių priemonių vystymui. **Pastaba** 2007-10-02 RST generalinio direktoriaus įsakymu Nr. 141 patvirtinta įėjimo/išėjimo į AB Rytų skirstomųjų tinklų Centrinės buveinės P. Lukšio g. 5B, pastatą laikina tvarka. 2007-10-04 RST generalinio direktoriaus įsakymu Nr. 147 patvirtintas AB Rytų skirstomųjų tinklų objektų fizinės saugos reglamentas. 2007-10-23 RST generalinio direktoriaus įsakymu Nr. 153 patvirtinta AB Rytų skirstomųjų tinklų objektų fizinės saugos tvarka.

Eil. Nr.	Teisės akto reikalavimai	Pastebėjimas
	7.3. neteisėtų veiksmų prieš įmonę atgrasymu. Įmonės fizinės saugos sistema turi būti projektuojama, organizuojama ir veikti aplenkiant projektines grėsmes. Įmonės fizinės saugos sistema turi būti pajėgi ne tik apsunkinti neteisėto poveikio vykdymą, bet ir užkirsti kelią tokiam poveikiui įvykdyti; 7.4. Įmonių fizinės saugos sistemos adekvatumu (proporcingumu). Įmonių fizinės saugos sistemos projektuojamos atsižvelgiant į projektines grėsmes ir galimą žalą. Įmonės fizinės saugos sistemai būtini investiciniai ir eksploataciniai kaštai turi būti adekvatūs projektinėms grėsmėms; 7.5. bendradarbiavimu. Įmonės vadovas, saugos padalinys ir/ar saugos tarnyba privalo bendradarbiauti su teritorinėmis policijos įstaigomis, užtikrindamos viešąją tvarką, administracinių teisės pažeidimų ir nusikalstamų veikų prevenciją ir atskleidimą įmonės teritorijoje bei keistis kriminogenine informacija; 7.6. fizinės saugos sistemos aktyvumu. Įmonės vadovo, atsakingų darbuotojų, saugos padalinio ir/ar saugos tarnybos veikla turi užkardinti galimas neteisėtas, nukreiptas prieš įmonę, veikas; 7.7. fizinės saugos priemonių diferenciacija. Įmonės objektų skirstymas pagal svarbą, reikšmę, projektines grėsmes, galimus nuostolius (žalą įmonei, žmonėms, šalies ūkiui bei aplinkai) ir atitinkamo objekto fizinės saugos lygio priskyrimas atitinkamam objektui. Diferencijuojant atskirų Įmonės objektų saugos lygius, galima pasiekti maksimalius rezultatus su minimaliomis investicijomis, pagrindinį dėmesį skiriant svarbiausiems objektams; 7.8. saugos nepertraukiamumu. Negalima Įmonės ir/ar atskiro jos objekto palikti kurį laiką be apsaugos. Priklausomai nuo turto vertės ir svarbos Įmonės veiklai, projektinių grėsmių, pasirenkamos atitinkamos saugos jėgos ir priemonės, kurių vykdymas gali užtikrinti nuolatinę objekto saugą; 7.9. Įmonės saugos pajėgų ir priemonių kompleksiškumu. Efektyvi objektų sauga turi būti vykdoma panaudojant skirtingas priemones, maksimaliai suderinant jų poveikį. Pasirenkant saugos priemones reikėtų atsižvelgti į: 7.9.1. atitinkamos priemonės efektyvumą sprendžiant saugos klausimus; 7.9.2. saugos priemonės prieinamumą, t.y. galimybę įdiegti ją objekte; 7.9.3. pačios priemonės ir jos įdiegimo kainą; 7.9.4. galimybę derinti įvairių priemonių darbą; 7.9.5. saugos priemonių dubliavimo galimybę, užtikrinant aukščiausio lygio objektų saugą. 7.10. didėjančiu pasipriešinimu. Vykstant neteisėtam poveikiui pieš saugomą objektą turi didėti fizinės saugos sistemos pasipriešinimas.	
2.	*13 punktas:* Objekto vidaus patalpoms, kurioms reikia sustiprinto fizinės saugos dėmesio (duomenų bazės, vadovaujančio personalo kabinetai, buhalterija, archyvas ir t. t.) turi būti nustatyta ypatinga leidimų ir personalo kontrolės sistema. Objekto vidaus patalpos gali būti skirstomos į atskiras saugos zonas, į kurias asmenų patekimas bus diferencijuotas.	Audituojamu laikotarpiu (iki 2007-10-01) ne visoms RST vidaus patalpoms, kurioms reikėjo sustiprintos fizinės saugos (duomenų bazės, vadovaujančio personalo kabinetai, buhalterija, archyvas ir t. t.) buvo nustatyta ypatinga leidimų ir personalo kontrolės sistema. **Pastaba** 2007-10-02 RST generalinio direktoriaus įsakymu Nr. 141 patvirtinta įėjimo/išėjimo į AB Rytų skirstomųjų tinklų

Eil. Nr.	Teisės akto reikalavimai	Pastebėjimas
		Centrinės buveinės P. Lukšio g. 5B, pastatą laikina tvarka.
3.	*20 punktas:* Įmonės vadovas tvirtina Įmonės leidimų režimą, kuriame turi būti nustatyta patekimo į saugomą objektą ir išvykimo iš jo, taip pat buvimo saugomame objekte kontrolės tvarka, pasireiškianti darbuotojų pažymėjimų ar kitų dokumentų, patvirtinančių asmens tapatybę ar kitą reikalaujamą informaciją, ir su savimi turimų daiktų, transporto priemonėse esančių krovinių bei su jais susijusių dokumentų patikrinimu.	Audituojamu laikotarpiu (iki 2007-10-01) RST nebuvo patvirtinta patekimo į centrinės buveinės pastatą kontrolės tvarka ir leidimų išdavimo tvarka. **Pastaba** 2007-10-02 RST generalinio direktoriaus įsakymu Nr. 141 patvirtinta įėjimo/išėjimo į AB Rytų skirstomųjų tinklų Centrinės buveinės P. Lukšio g. 5B, pastatą laikina tvarka.
4.	*21 punktas:* Įmonės vadovas ar jo įgaliotas asmuo derina su teritorinėmis policijos įstaigomis sąveikos planus ypatingų situacijų atveju. Lietuvos Respublikos civilinės saugos įstatymo (Žin., 1998, Nr. 115-3230; 2000, Nr.61-1805; 2003, Nr.73-3351; 2004, Nr. 28-872) nustatyta tvarka rengia ir tvirtina civilinės saugos parengties ekstremalioms situacijoms planus, kuriuose numato ir įmonės fizinės saugos režimą esant ekstremalioms situacijoms.	Audituojamu laikotarpiu (iki 2007-10-01) RST su teritorinėmis policijos įstaigomis nederino sąveikos planų ypatingų situacijų atveju, Lietuvos Respublikos civilinės saugos įstatymo nustatyta tvarka RST nebuvo rengiami ir tvirtinami civilinės saugos parengties ekstremalioms situacijoms planai. **Pastaba** 2007-10-04 RST generalinio direktoriaus įsakymu Nr. 147 patvirtintas AB Rytų skirstomųjų tinklų objektų fizinės saugos reglamentas. RST rašte[122] teigiama, kad *bendrovės centrinės buveinės civilinės saugos parengties ekstremalioms situacijoms planas audituojamu laikotarpiu buvo derinamas su Vilniaus apskrities Civilinės saugos departamentu.*
5.	*22 punktas:* Ne rečiau kaip kartą per metus, o įvykus neteisėtai veikai prieš Įmonę, tuoj pat po jos turi būti peržiūrimos projektinės grėsmės ir, reikalui esant, koreguojama Įmonės fizinės saugos tvarka.	Audituojamu laikotarpiu (iki 2007-10-01) nebuvo parengta RST fizinės saugos tvarka. **Pastaba** 2007-10-23 RST generalinio direktoriaus įsakymu Nr. 153 patvirtinta AB Rytų skirstomųjų tinklų objektų fizinės saugos tvarka.
6.	*23 punktas:* Įmonės fizinės saugos auditas turi būti atliekamas ne rečiau kaip kas 2 metai. Įmonės fizinės saugos auditą atlieka Įmonės vidaus audito padaliniai arba įmonės, turinčios fizinės saugos licencijas.	RST Vidaus audito skyrius 2006-11-24 atlikto fizinės saugos auditą, tačiau jo metu nagrinėti ne visi klausimai susiję su bendrovės informacinių sistemų fizine sauga ir aplinkos saugumu.

Šaltinis – Valstybės kontrolė

[122] AB Rytų skirstomųjų tinklų generalinio direktoriaus 2007-12-20 raštas Nr. 10530-1221 „Dėl pastabų valstybinio audito ataskaitos projektui“.

Valstybinio audito ataskaitos „Akcinės bendrovės Rytų skirstomųjų tinklų informacinės sistemos bendrosios kontrolės vertinimas“ 4 priedas

RST naudojamų ir diegiamų informacinių sistemų trumpas aprašymas

Eil. Nr.	IS pavadinimas	IS funkcija, trumpas aprašymas
1.	ADMIN2	Informacinių sistemų administravimo informacinė posistemė.
2.	AEEAS	Automatizuota elektros energijos apskaitos informacinė posistemė.
3.	ATJUNGIMAI	35-110 kV transformatorinių ir 35 kV oro kabelių linijų neplaninių atjungimų registravimo bei 0,38-10 kV transformatorinių, oro, kabelių, oro kabelių linijų planinių ir neplaninių atjungimų registravimas.
4.	BILINGAS	Elektros energijos apskaitos informacinė posistemė. Posistemė realizuoja pardavimų klientams funkciją ir apima klientų registravimą duomenų bazėje, kliento sunaudotos elektros energijos ir kitų paslaugų apskaitą ir sąskaitų už jas formavimą, remiantis apskaitos prietaisų rodmenimis ir sunaudojimo normatyvais, mokėjimų ir įsiskolinimų apskaitą bei darbo su skolų išieškojimu eigos fiksavimą, įskaitant skolų vekselių apskaitą.
5.	BLANKAS	Portalo „PORTALAS“ klientų registracijos valdymo informacinė posistemė.
6.	CALL	Call centro informacinė posistemė, apimanti operatyvų bendravimą su klientais, sprendžiant jiems kilusias problemas, susijusias su elektros energijos tiekimu (nuo avarijų elektros energijos tiekimo sistemose iki mokėjimų neaiškumų).
7.	DICTIONARY	Informacinių sistemų dokumentavimo informacinė posistemė, apimanti visų turimų informacinių posistemių duomenų bazių struktūras su jų aprašymais ir visa pakeitimo istorija, saugojimą bei tvarkymą.
8.	DOCLOGIX	Dokumentų valdymo informacinė posistemė, apimanti visų bendrovėje cirkuliuojančių dokumentų rengimą, saugojimą ir suradimą, siunčiamos ir gaunamos korespondencijos registravimą, nukreipimą pagal paskirtį, darbų, pavedimų ar užduočių paskirstymą tarp darbuotojų ir jų vykdymo kontrolę.
9.	DW	Analizės ir prognozės informacinė posistemė, apimanti visos bendrovės veiklos siekiamų rodiklių apskaičiavimą, jų dinamikos ir priklausomybių analizę bei vertinimą.
10.	EEVIS (PORTALAS)	Elektros energijos vartotojų (aptarnavimo internetinis portalas) informacinė posistemė, realizuojanti klientų informavimo funkciją, kuri reikalinga bendraujant su klientais ir teikiant jiems papildomas paslaugas.
11.	ESIS	Energijos srautų apskaitos informacinė posistemė, apimanti energijos srautų tarp elektros perdavimo tinklo ir skirstomųjų tinklų, elektros linijų atkarpose bei pastotėse duomenų fiksavimą, surinkimą ir kaupimą.
12.	GIS	Geografinė - informacinė posistemė, atvaizduojanti techninius objektus žemėlapyje ir fiksuojanti objektų kitimą geografinėje aplinkoje.
13.	INFOLEX PRAKTIKA	Aprobuotų ir neaprobuotų teismų praktikų duomenų bazės informacinė posistemė.
14.	INVISTA (INVESTICIJOS)	Investicijų valdymo informacinė posistemė.
15.	IT SERVICE DESK (UNICENTER)	Posistemė apima visos bendrovės informacinės sistemos naudotojų problemų, susijusių su technine ir programine įranga, fiksavimą bei informavimo apie dažniausiai pasitaikančias problemas sprendimą.
16.	KAD	Kintamos dalies skaičiavimo informacinė posistemė.
17.	KCUVIS	Kontaktų centro užklausų valdymo informacinė posistemė.
18.	LITLEX	Teisės aktų peržiūros ir paieškos informacinė posistemė.
19.	MEGA KNYGA	Bibliotekos, archyvo ir straipsnių kaupimo informacinė posistemė.
20.	MOBILKĖS	Mobiliųjų telefonų pokalbių apskaitos informacinė posistemė.
21.	MOKESČIAI	Mokesčių deklaravimo formos informacinė posistemė.
22.	NVA	Naujų vartotojų elektros įrenginių prijungimo prie elektros tinklų informacinė posistemė.
23.	PASKATA	Darbo užmokesčio skaičiavimo informacinė posistemė.

Eil. Nr.	IS pavadinimas	IS funkcija, trumpas aprašymas
24.	PERSONALAS (PERSONALAS DU)	Personalo ir darbo užmokesčio apskaitos informacinė posistemė.
25.	PIRKIMAI	Pirkimų valdymo informacinė posistemė.
26.	PIRMADIENIS	Pagrindinių RST savaitės veiklos rodiklių surinkimo ir statistikos posistemė.
27.	PROGNOZAVIMAS	Valandinio elektros energijos suvartojimo prognozavimo informacinė posistemė.
28.	PROJECT	Projektų valdymo informacinė posistemė, skirta sekti ir tvarkyti visus vykdomus bendrovėje projektus, užtikrinant jų efektyvią priežiūrą bei valdymą.
29.	RYTIS	RST vidinio portalo „RYTIS“ informacinė posistemė.
30.	RODMENYS	ELGAMA skaitiklių parametravimo ir rodmenų nuskaitymo informacinė posistemė.
31.	SĄMATA	Sąmatų skaičiavimo informacinė posistemė.
32.	SAUGA	Saugos darbe ir nelaimingų atsitikimų prevencijos informacinė posistemė.
33.	SCALA	Apskaitos ir verslo valdymo posistemė, kuri sudaryta iš integruotų modulių ir gali visiškai valdyti bei kontroliuoti visas apskaitos, pirkimų ir logistikos sritis.
34.	SKAREGAS	Elektros energijos vartotojų skambučių registravimo informacinė posistemė.
35.	SPECTEISĖS	Specialiųjų teisių suteikimo informacinė posistemė.
36.	TABELIS	Darbo laiko apskaitos informacinė posistemė.
37.	TEMIDĖ	Teisminių bylų procesų valdymo informacinė posistemė.
38.	TEVIS	Tinklo eksploatavimo ir valdymo informacinė posistemė. Posistemė apima visų elektros energijos tiekimo techninių objektų (pastočių, transformatorinių ir pan.), taip pat techninės įrangos (kontrolinių ir vartotojų skaitiklių, kabelių, oro linijų ir pan.) pirminį įregistravimą, apimantį pagrindinius kontroliuojamus techninius parametrus, ir tolesnį jų būklės sekimą, fiksuojant būklės pasikeitimus pagal apžiūrų (patikrų) duomenis, einamojo remonto rezultatus.
39.	TREVIS	Kompiuterizuota transporto paslaugų filialo darbo informacinė posistemė, kaupianti duomenis apie transporto priemones, atliekanti kuro sąnaudų apskaičiavimus, vykdanti atsarginių detalių apskaitą, transporto priemonių darbo laiko, padangų ridos, akumuliatorių apskaitą, automobilių nuomos apskaitą, vairuotojų dirbto laiko apskaitą, techninių apžiūrų ir draudimų apskaitą ir kontrolę, autoįvykių apskaitą, užsakymų vykdymą ir kontrolę, mokesčių už aplinkos taršą ir kelių mokesčių apskaitą, atliktų remontų apskaitą, taip pat įvairių ataskaitų ir suvestinių formavimą, kitų statistinių duomenų kaupimą.
40.	TURTAS	Netechnologinio turto valdymo informacinė posistemė, apimti turimo netechnologinio turto tvarkymą, atsakomybės už jį apskaitą, remontų planavimą bei apskaitą, nuomos tvarkymą bei apskaitą.
41.	UŽDUOTYS	Užduočių valdymo informacinė posistemė skirta bendrovės darbuotojų darbo laiko ir užduočių apskaitai ir analizei.
42.	VIS (VIP)	Vadovybės informavimo informacinė posistemė apima informacijos, reikalingos bendrovės ar jos filialo valdymui, reguliarų atrinkimą iš sistemos duomenų bazės ir pateikimą reikiamu pjūviu ir pavidalu.
43.	WEB SVETAINĖ	Interneto svetainės informacinė posistemė.

Valstybinio audito ataskaitos „Akcinės bendrovės Rytų skirstomųjų tinklų informacinės sistemos bendrosios kontrolės vertinimas“ 5 priedas

RST informacinės sistemos vystymo kalendorinis planas

ID	Posistemės	Kūrimo / vystymo trukmė	Pradžia	Pabaiga
1	**RST IS vystymas**	**1342 d**	**2004.06.01**	**2009.08.13**
9	**Vystomos posistemės**	**1342 d**	**2004.06.01**	**2009.08.13**
10	Elektros energijos apskaitos (BILINGAS) informacinė posistemė	468 d	2004.06.01	2006.03.29
15	IT Service desk (UNICENTER) informacinė posistemė	220 d	2005.02.17	2005.12.30
12	**Tinklo eksploatavimo ir valdymo (TEVIS) informacinė posistemė**	**663 d**	**2005.05.30**	**2007.12.31**
13	II etapas	206 d	2005.05.30	2006.03.21
14	III etapas	165 d	2007.05.15	2007.12.31
11	GIS informacinė posistemė	264 d	2006.01.02	2007.01.16
20	Internetinės svetainės (WEB SVETAINĖ) posistemė	44 d	2006.03.22	2006.05.24
21	Elektros energijos vartotojų (aptarnavimo internetinis portalas) (EEVIS) informacinė posistemė	66 d	2006.05.25	2006.08.28
22	Saugos darbe ir nelamingų atsitikimų prevencijos (SAUGA) informacinė posistemė	88 d	2006.08.29	2007.01.02
23	Vidinio portalo RYTIS (RYTIS) informacinė posistemė	66 d	2007.01.03	2007.04.04
19	Personalo ir darbo užmokesčio apskaitos (PERSONALAS DU) informacinė posistemė	99 d	2007.04.05	2007.08.21
24	Pirkimų valdymo (PIRKIMAI) informacinė posistemė	99 d	2007.08.22	2008.01.07
18	Apskaitos ir verslo valdymo (SCALA) informacinė posistemė	44 d	2008.01.08	2008.03.07
28	Investicijų valdymo (INVISTA) informacinė posistemė	88 d	2008.03.10	2008.07.09
26	Informacinių sistemų administravimo (ADMIN2) informacinė sistema	22 d	2008.07.10	2008.08.08
16	Naujų vartotojų elektros įrenginių prijungimo prie elektros tinklų (NVA) informacinė posistemė	66 d	2008.08.11	2008.11.10
17	Energijos srautų apskaitos (ESIS) informacinė posistemė	88 d	2008.11.11	2009.03.12
27	Transporto priemonių eksploatacijos valdymo (TrEVIS) informacinė posistemė	110 d	2009.03.13	2009.08.13
25	Teisminių bylų procesų valdymo (TEMIDĖ) informacinė posistemė	66 d	2009.01.05	2009.04.06
2	**Naujos posistemės**	**715 d**	**2006.03.30**	**2009.01.02**
4	Netechnologinio turto valdymo (TURTAS) informacinė posistemė	44 d	2006.03.30	2006.06.01
6	Call centro (CALL) informacinė posistemė (Integracinis DW)	110 d	2006.06.02	2006.11.07
7	Analizės ir prognozės (DW) informacinė posistemė	132 d	2006.11.08	2007.05.14
3	Užduočių valdymo (UŽDUOTYS) informacinė posistemė	176 d	2008.01.01	2008.09.02
5	Projektų valdymo (PROJECT) informacinė posistemė	44 d	2008.09.03	2008.11.03
8	Informacinių sistemų dokumentavimo (DICTIONARY) informacinė posistemė	44 d	2008.11.04	2009.01.02