LIETUVOS RESPUBLIKOS VALSTYBĖS KONTROLĖ

TVIRTINU:
Valstybės kontrolierė
Rasa Budbergytė

_____

IŠANKSTINIO TYRIMO ATASKAITA

STRATEGINĖS INFORMACIJOS SAUGA

2009 m. kovo 16 d. Nr. IT-P-900-1-3
Vilnius

Išankstinis tyrimas atliktas, vykdant
Valstybės kontrolės Informacinių sistemų valdymo ir audito departamento
direktoriaus Dainiaus Jakimavičiaus
2009-01-20 pavedimą Nr. P-900-1

Auditą atliko audito grupė:
Rimgaudas Gamulis (grupės vadovas)
Irina Kiškina

Išankstinis tyrimas pradėtas 2009-01-21
Išankstinis tyrimas baigtas 2009-03-16

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

TURINYS

IŠANKSTINIO TYRIMO ATLIKIMO PRIEŽASTYS

Informacijos sauga pastaruoju metu tampa vis aktualesnė problema, galinti paliesti ne tik šalies elektroninių ryšių tinklus ar informacines sistemas turinčias įtakos nacionaliniam saugumui, bet ir kiekvieną Lietuvos pilietį (pvz.: internetinės bankininkystės sutrikimai, neprieinami Lietuvos Respublikos gyventojų registro duomenys). Po 2008 metų birželio mėnesio įvykių, kuomet įsilaužus į kelių Lietuvos valstybinių institucijų interneto svetaines buvo sutrikdytas jų darbas, žiniasklaidoje nuolat diskutuojama apie tai, koks yra optimalus būdas užtikrinti Lietuvos valstybei svarbios elektroninės informacijos saugą.

Strateginio tyrimo metu pastebėta, kad nebuvo sukurta bendra kritinės informacinės infrastruktūros[1] saugos užtikrinimo sistema, todėl nėra aišku, kaip reikėtų valdyti kritines situacijas, kylančias dėl įsilaužėlių atakų ir techninių nesklandumų elektroninėje erdvėje. Nesuvaldžius kritinės situacijos, gali nukentėti ne tik valstybinės reikšmės informacija ir kiekvienas pilietis, bet ir šalies prestižas, pasitikėjimas naujomis technologijomis.

Lietuvos Respublikos valstybės kontrolė (toliau – Valstybės kontrolė), jau kelerius metus atlikdama informacinių sistemų auditus, pastebi pasikartojančių su strateginės elektroninės informacijos sauga susijusių teisinio reglamentavimo, institucinės sistemos ir kitų trūkumų.

Šios priežastys paskatino atlikti „Strateginės informacijos saugos“ vertinimą, kuris yra numatytas Lietuvos Respublikos valstybės kontrolės 2009 metų valstybinio audito programoje[2].

[1] Kritinė informacinė infrastruktūra – elektroninių ryšių tinklas, informacinė sistema ar informacinių sistemų grupė, prie kurios neteisėtas prisijungimas ir sąlygų neteisėtai prisijungti sudarymas, kurios neteisėtas sutrikimas ar pakeitimas, kurioje saugomų, tvarkomų, iš jos išrenkamų arba ja perduodamų elektroninių duomenų sunaikinimas, sugadinimas, ištrynimas ar pakeitimas, galimybės naudotis tokiais elektroniniais duomenimis panaikinimas arba apribojimas turi ar gali turėti ženklios neigiamos įtakos nacionaliniam saugumui, šalies ūkiui ar visuomenės gerovei.
[2] Lietuvos Respublikos valstybės kontrolieriaus 2009-01-19 įsakymas Nr. V-8 „Dėl 2009 metų valstybinio audito programos“.

IŠANKSTINIO TYRIMO PROCESAS IR INFORMACIJOS RINKIMO METODAI

Informacija, susijusi su elektroninės informacijos sauga, buvo gauta iš Krizių valdymo centro prie Lietuvos Respublikos krašto apsaugos ministerijos (toliau – Krizių valdymo centras). Susipažinome su Krizių valdymo centro, Lietuvos Respublikos Ministro Pirmininko sudarytos tarpžinybinės darbo grupės[3] ir Lietuvos Respublikos ryšių reguliavimo tarnybos (toliau – RRT) veiklos ataskaitomis, pateiktomis rekomendacijomis. Nagrinėjome Lietuvos Respublikos krašto apsaugos ministerijos (toliau – KAM), Lietuvos Respublikos susisiekimo ministerijos (toliau – Susisiekimo ministerija), RRT, Lietuvos Respublikos vidaus reikalų ministerijos (toliau – VRM) ir kitose interneto svetainėse pateiktą informaciją. Analizavome teisės aktus, susijusius su strateginės elektroninės informacijos saugos reglamentavimu.

Tyrimo laikotarpis – 2007–2008 metai.

Išankstinio tyrimo tikslai – išnagrinėti su strateginės elektroninės informacijos sauga susijusį teisinį reglamentavimą, sritį koordinuojančių institucijų funkcijas ir jų taikomų priemonių efektyvumą, nustatyti strateginės elektroninės informacijos saugos problemines sritis. Išnagrinėjus numatytas sritis – nustatyti audito tikslus ir subjektus, nuspręsti, ar tikslinga pradėti pagrindinį tyrimą.

Strateginės informacijos saugos išankstinį tyrimą vykdant Informacinių sistemų valdymo ir audito departamento direktoriaus D. Jakimavičiaus 2009 m. sausio 20 d. pavedimą Nr. P-900-1 atliko vyresnysis valstybinis auditorius R. Gamulis (grupės vadovas) ir vyresnioji valstybinė auditorė I. Kiškina.

Išankstinio tyrimo metu taikyti duomenų rinkimo metodai: dokumentinis (rašytinių ir elektroninių dokumentų nagrinėjimas), apklausos (pokalbiai su darbuotojais).

Surinktai informacijai analizuoti taikyti šie metodai: loginės ir palyginamosios analizių ir kitos procedūros.

Atlikdami tyrimą laikėmės prielaidos, kad auditoriams pateikti duomenys yra teisingi, dokumentai išsamūs ir galutiniai, o jų kopijos atitinka originalus.

[3] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita.

NAGRINĖTA VEIKLOS SRITIS

Šiandieninė Lietuvos Respublikos strateginės elektroninės informacijos sauga susijusi tiek su nacionaliniu, tiek su tarptautiniu šios srities reglamentavimu.

Lietuvos Respublikos Ministro Pirmininko 2008 m. birželio 17 d. potvarkiu Nr. 225 sutarytos darbo grupės veiklos ataskaitoje[4] pastebėta, kad Europos Sąjungos teisės aktai numato atitinkamus įpareigojimus keliant elektroninių ryšių tinklų ir informacijos saugumo lygį nacionaliniu ir tarptautiniu lygiu. Europos Komisija planuoja parengti 2010–2014 metų ilgalaikę programą, skirtą kovai su kibernetiniu nusikalstamumu. Europos Sąjungos Taryba yra išreiškusi pritarimą steigti Europos ir nacionalines perspėjimo platformas, kuriose būtų skelbiami pranešimai apie internete pastebėtus pažeidimus[5].

Šiame kontekste labai svarbi tvirta ir aiški Lietuvos pozicija strateginės elektroninės informacijos saugumo klausimais. Deja, Lietuvoje kol kas nėra įstatymo, nuosekliai reglamentuojančio su strateginės elektroninės informacijos saugumu susijusius visuomeninius santykius. Kai kuriuose teisės aktuose esama nuostatų, susijusių su elektroninių ryšių tinklų ir informacijos saugumu, tačiau jos neužtikrina visapusiško ir aiškaus šių santykių reglamentavimo. Minėtą reglamentavimo spragą numatyta pašalinti parengus ir priėmus Lietuvos Respublikos Vyriausybės (toliau – Vyriausybė) 2006–2008 metų programos[6] įgyvendinimo priemonėse numatytus Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymą ir įstatymą, reglamentuojantį valstybės informacinių išteklių valdymą. Įstatymų projektai parengti, tačiau iki 2009 m. vasario 27 d. nebuvo priimti ir Lietuvos Respublikos Seime neužregistruoti.

Nesant aiškaus strateginės elektroninės informacijos saugos teisinio reglamentavimo, atsiranda šios srities sąvokų neapibrėžtumas, objektų identifikavimo ir klasifikavimo neaiškumų.

Tyrimo laikotarpiu (2007–2008 metai), įstatymų projektuose buvo pateikta keletas siūlymų siekiant nustatyti pagrindines šios srities sąvokas, tačiau jos nebaigtos teisiškai apibrėžti.

Auditorių manymu, strateginės elektroninės informacijos sąvoka galėtų apimti elektroninę informaciją, kuri svarbi visai valstybei ir yra tvarkoma ypatingos svarbos elektroninių ryšių tinkluose, žinybiniuose registruose (kadastruose) ir informacinėse sistemose ar jų grupėse, kaip tai siūloma numatyti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo ir įstatymo, reglamentuojančio valstybės informacinių išteklių valdymą, projektuose.

[4] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita.
[5] Ten pat.
[6] Lietuvos Respublikos Vyriausybės 2006-10-17 nutarimas Nr. 1020 „Dėl Lietuvos Respublikos Vyriausybės 2006-2008 metų programos įgyvendinimo priemonių patvirtinimo“.

Pažymėtina, kad teisinio reglamentavimo spragos neleidžia aiškiai identifikuoti su strateginės elektroninės informacijos sauga susijusių objektų ir informacinės infrastruktūros (detaliau apie strateginės elektroninės informacijos saugos planavimą, teisinį reglamentavimą ir šios srities saugos objektų identifikavimą 8–12 psl.).

Apibendrinant elektroninės informacijos saugą valstybės informacinėse sistemose 2006 metais pastebėta, kad nebaigta formuoti elektroninės informacijos saugos valdymo ir priežiūros struktūra valstybės ir institucijų mastu[7]. Pripažinta, kad elektroninių ryšių tinklų ir informacijos saugumui užtikrinti reikia kompleksinio reguliavimo[8].

Tyrimo metu elektroninių ryšių tinklų ir informacijos saugos klausimais Lietuvoje dirbo šios institucijos: Susisiekimo ministerija, VRM, RRT, Krizių valdymo centras[9], Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos Vyriausybės (toliau – IVPK), Nusikaltimų elektroninėje erdvėje tyrimo valdyba, Valstybinė duomenų apsaugos inspekcija, Valstybės saugumo departamentas. Tačiau nė viena iš išvardytų institucijų neturi pakankamai įgaliojimų, kad galėtų savarankiškai užtikrinti strateginės elektroninės informacijos saugą.

Pažymėtina, kad šiuo metu galiojančiais teisės aktais neapibrėžti svarbiausi strateginės elektroninės informacijos saugos politikos formuotojai ir įgyvendintojai, jų tarpusavio ryšiai. Neįvardyti subjektai, turintys teisę sudaryti šios srities saugomų objektų sąrašą ir teikti pasiūlymus dėl tokio sąrašo sudarymo, pakeitimo ar papildymo. Ne visiškai identifikuotos institucijos, atliekančios šios srities kontrolės ir priežiūros funkcijas, nenustatyti viešojo ir privataus sektorių bendradarbiavimo principai ir nesukurti mechanizmai (detalesnė elektroninės informacijos saugos valdymo sistema pateikta 12–15 psl.).

Informacinių technologijų (toliau – IT) valdymo gerojoje praktikoje[10] ir standartuose[11] rekomenduojama elektroninės informacijos saugą valdyti atsižvelgiant į tam tikrus principus. Tarpžinybinei darbo grupei įvertinus Lietuvos kibernetinį saugumą[12], konstatuota, kad šioje srityje saugumo užtikrinimas priklauso nuo gebėjimo ir galimybių sukurti ir palaikyti keturis esminius elementus:

- kibernetinės grėsmės ir pažeidžiamumo prevenciją;
- kibernetinių incidentų ir masinių kibernetinių atakų identifikavimą ir tyrimų atlikimą;

[7] Lietuvos Respublikos Vyriausybės 2006-06-19 nutarimu Nr. 601 patvirtinta „Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 metų“.
[8] Lietuvos Respublikos Vyriausybės 2006-12-06 nutarimu Nr. 1211 patvirtinta „Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija“.
[9] Lietuvos Respublikos Vyriausybės įsteigtas Krizių valdymo centras yra pagrindinis valstybės įvairaus pobūdžio krizių valdymo strateginiu lygmeniu štabas.
[10] *CobIT (Control Objectives for Information and related Technologies*) – visame pasaulyje žinomas tarptautinės *ISACA* organizacijos standartas. *CobIT* aprašo geriausią praktiką informacinių technologijų valdymo srityje.
[11] *ISO/IEC 27001:2005*. Information technology - Security techniques - Information security management systems - Requirements (tapatus *LT ISO/IEC 27001:2006*).
[12] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita.

- reagavimą į kibernetinius incidentus ir masines kibernetinės atakas;
- kibernetinių incidentų ir masinių kibernetinių atakų pasekmių valdymą ir likvidavimą.

Auditoriai pastebi, kad Lietuvoje iki šiol nėra sukurta nacionalinė elektroninės informacijos saugos stebėsenos sistema, taip pat elektroninės informacijos pažeidžiamumo vertinimo metodika. Strateginės elektroninės informacijos saugos srities patikimumo tyrimai vykdomi nereguliariai.

Nepakankamai aiškūs teisiniai pagrindai ir nevieninga viešojo ir privataus sektoriaus institucinė sistema neleidžia efektyviai koordinuoti su strateginės elektroninės informacijos sauga susijusių incidentų pasekmių valdymo ir likvidavimo procesų, o tai neigiamai atsiliepia bendrajai elektroninių ryšių tinklų ir informacijos saugumo situacijai Lietuvoje (detaliau apie strateginės elektroninės informacijos saugos stebėseną, grėsmių ir pažeidžiamumų nustatymą, prevenciją ir likvidavimą 15–16 psl.).

Atkreiptinas dėmesys, kad Lietuvos Respublikos Seimas 2008 m. gruodžio 9 d. pritarė Ministro Pirmininko pateiktai Vyriausybės veiklos programai[13]. Minėtos programos 2008-2012 metų veiklos strategijos pagrindinių nuostatų dalyje „Informacinės ir žinių visuomenės plėtra“ numatyta įstatymiškai reglamentuoti elektroninės informacijos saugumo užtikrinimo politiką, strategiją ir koordinavimą. Ketinama apsispręsti dėl elektroninės skaitmeninės terpės saugumo didinimo teisinės ir institucijų sandaros, taip pat neatidėliotinų įgyvendinimo priemonių. Numatytas siekis inventorizuoti valstybės valdomus informacijos ir ryšių technologijų (toliau – IRT) tinklus ir jais teikiamas paslaugas, įvertinti valstybinių įmonių, veikiančių IRT rinkoje, efektyvumą ir optimizuoti jų veiklą.

Iki tyrimo pabaigos (2009 m. vasario 27 d.) šios Vyriausybės veiklos programos įgyvendinimo priemonių planas nebuvo patvirtintas, todėl nėra konkretizuotos minėtos veiklos priemonės, jų atsakingi vykdytojai ir įvykdymo terminai.

[13] Lietuvos Respublikos Seimo 2008-12-09 nutarimu Nr. XI-52 pritarta „Penkioliktosios Lietuvos Respublikos Vyriausybės veiklos programai“.

LĖŠOS, JŲ FINANSAVIMO ŠALTINIAI

Informacija apie strateginės elektroninės informacijos saugai skiriamas Valstybės biudžeto lėšas buvo renkama nagrinėjant 2007-2008 metų biudžeto asignavimų paskirstymą pagal programas ir asignavimų valdytojus[14] ir šio laikotarpio Valstybės kapitalo investicijų pasiskirstymą[15]. Europos Sąjungos lėšų skyrimas šiam tikslui buvo nagrinėjamas analizuojant struktūrinių fondų lėšomis finansuojamų informacinės visuomenės plėtros 2004-2006 metų projektus ir 2007-2013 metų paramos prioriteto „Informacinė visuomenė visiems“ paskirstymo pagal priemones planavimą.

Išanalizavus valstybės biudžeto lėšų paskirstymą institucijoms, kurios vykdo su informacijos sauga susijusias funkcijas, nustatyta, kad 2007-2008 metais joms buvo skirta 460 517 tūkst. Lt. Pažymėtina, kad negalima tiksliai nustatyti, kokia jų dalis buvo tiesiogiai skirta strateginės elektroninės informacijos saugos užtikrinimui, nes esamos teisinio reglamentavimo spragos neleido aiškiai identifikuoti su strateginės elektroninės informacijos sauga susijusių objektų, informacinės infrastruktūros ir institucinės sistemos.

Tyrimo metu auditoriai atliko finansavimo, skirto septynioms įstaigoms ir institucijoms[16], kurias Vyriausybės sudaryta tarpžinybinė darbo grupė nurodė kaip šiuo metu Lietuvoje dirbančias elektroninių ryšių tinklų ir informacijos saugumo klausimais, analizę. Nustatyta, kad 2007-2008 metais lėšos informacijos saugai buvo skiriamos įstaigoms ir institucijoms, tiesiogiai nedirbančioms elektroninių ryšių tinklų ir informacijos saugumo klausimais, todėl neatsakingoms už šių priemonių įgyvendinimą (1 pavyzdys).

1 pavyzdys

Per 2007–2008 metus Valstybinei mokesčių inspekcijai prie Lietuvos Respublikos finansų ministerijos, Valstybinių ryšių centrui prie Valstybės saugumo departamento ir Muitinės departamentui prie Lietuvos Respublikos finansų ministerijos valstybės kapitalo investiciniams projektams, susijusiems su informacinių sistemų saugumo užtikrinimu, buvo skirta atitinkamai 21 116, 3 900 ir 24 838 tūkst. Lt.

Nesant aiškaus su strateginės elektroninės informacijos sauga susijusio teisinio reglamentavimo, trūksta nuoseklaus ir kompleksinio požiūrio į šios srities finansavimą. Todėl kyla rizika, kad dalis elektroninės informacijos saugai skiriamų lėšų gali būti naudojama neefektyviai, siauros srities (ar institucijos) problemoms spręsti.

[14] Lietuvos Respublikos Vyriausybės 2007-01-29 nutarimas Nr. 91 „Dėl 2007 metų Lietuvos Respublikos valstybės biudžeto patvirtintų asignavimų paskirstymo pagal programas“ ir 2008-01-30 nutarimas Nr. 79 „Dėl 2008 metų Lietuvos Respublikos valstybės biudžeto patvirtintų asignavimų paskirstymo pagal programas“.
[15] Lietuvos Respublikos Vyriausybės 2007-01-24 nutarimas Nr. 146 „Dėl Valstybės investicijų 2007–2009 metų programoje numatytų 2007 metams kapitalo investicijų paskirstymo pagal asignavimų valdytojus ir investicijų projektus“ ir 2008-01-30 nutarimas Nr. 105 „Dėl Valstybės investicijų 2008–2010 metų programoje numatytų 2008 metams kapitalo investicijų paskirstymo“.
[16] Susisiekimo ministerija, VRM, RRT, IVPK, Nacionalinė vartotojų teisių apsaugos tarnyba, Valstybinė duomenų apsaugos inspekcija (Lietuvos Respublikos Ministro pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita).

Elektroninės informacijos sauga yra viena iš prioritetinių sričių skiriant Europos Sąjungos struktūrinių fondų paramą. Naujojo laikotarpio (2007–2013 metų) priemonės „Informacinių technologijų apsauga“ įgyvendinimui planuojama skirti 77 000 tūkst. Lt Europos regioninės plėtros fondo ir Lietuvos Respublikos valstybės biudžeto lėšų[17]. Tyrimo metu šios priemonės įgyvendinimas nebuvo pradėtas, planuojama įgyvendinimo pradžia – 2009 metų III ketvirtis.

Iš Europos Sąjungos struktūrinių fondų 2004–2006 metų finansuojamo laikotarpio buvo skirtas finansavimas[18] (26 156 tūkst. Lt) dviem projektams, susijusiems su strateginės elektroninės informacijos sauga:

- VRM vykdomam projektui „Valstybinių institucijų informacinių sistemų sauga (VIISS)“;
- Valstybės įmonės „Infostruktūra“ vykdomam projektui „Saugaus valstybinio duomenų perdavimo tinklo (SVDPT) kamieninės dalies sukūrimas“.

Pažymėtina, kad 2008 metais atliekant Europos Sąjungos struktūrinių fondų lėšomis finansuojamų informacinės visuomenės plėtros projektų valdymo veiklos auditą[19], buvo nustatyti rizikos veiksniai, galintys turėti įtakos elektroninės informacijos saugą užtikrinančių projektų rezultatyvumui ir efektyviam lėšų naudojimui.

ATLIKTI TYRIMAI IR JŲ REZULTATAI

Valstybės kontrolė 2006–2008 metais atliko aštuonis valstybinius auditus, kurių metu pastebėta su strateginės elektroninės informacijos saugos užtikrinimu susijusių trūkumų. Auditoriai nustatė šios srities teisinio reglamentavimo, institucinės sistemos problemų, buvo nagrinėti finansavimo, incidentų valdymo ir veiklos tęstinumo užtikrinimo klausimai, kitos su strateginės elektroninės informacijos sauga susijusios problemos. Pagrindinė informacija apie šiuos auditus pateikta ataskaitos 3 priede.

> Tyrimo metu tebebuvo tos pačios problemos, susijusios su strateginės elektroninės informacijos sauga, ne visi nustatyti trūkumai buvo pašalinti, o kai kurios nuo 2006 metų auditorių pateiktos svarbios rekomendacijos iki šiol neįgyvendintos.

Auditoriai pastebi, kad pastaruoju metu strateginės elektroninės informacijos saugos srityje atliekami įvairūs tyrimai ir apklausos (2 pavyzdys). Visuomenės informavimo priemonėse

[17] Prieiga per internetą http://www.ivpk.lt/fondai/12.htm (žiūrėta 2009-02-23).
[18] Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2004-11-23 įsakymas Nr. T-150 „Dėl paramos skyrimo ir neskyrimo pagal Lietuvos 2004–2006 metų bendrojo programavimo dokumento 3.3 priemonės „Informacinių technologijų paslaugų ir infrastruktūros plėtra“ paskelbtą kvietimą teikti paraiškas konkursui „Elektroninė infrastruktūra“ ir 2005-07-08 įsakymas Nr. T-65 „Dėl paramos skyrimo ir neskyrimo pagal Lietuvos 2004–2006 metų bendrojo programavimo dokumento 3.3 priemonės „Informacinių technologijų paslaugų ir infrastruktūros plėtra“ paskelbtą kvietimą teikti paraiškas konkursui „Elektroninė valdžia ir elektroninės paslaugos“ ir „Elektroninė infrastruktūra“ (2007-08-21 įsakymo Nr. T-110 redakcija).
[19] Valstybės kontrolės 2008-11-19 valstybinio audito ataskaita Nr. VA-9000-2-25 „Europos Sąjungos struktūrinių fondų lėšomis finansuojamų informacinės visuomenės plėtros projektų valdymas“.

skiriamas pakankamas dėmesys šios srities kritinėms situacijoms ir incidentams. Tačiau, mūsų nuomone, viešojoje erdvėje ir atsakingų institucijų pateikiamose ataskaitose nepakankamai nagrinėjamos Lietuvos strateginės elektroninės informacijos saugos užtikrinimo silpnosios pusės ir pasiruošimas kritinėms šios srities situacijoms. Stinga konkrečių pasiūlymų ir priemonių, kaip paskatinti viešo ir privataus sektorių bendradarbiavimą tinklų ir informacijos saugumo srityje.

2 pavyzdys

Nuo 2004 metų RRT atliekami išsamūs tinklų ir informacijos saugumo padėties Lietuvoje tyrimai, rengiamos jų apžvalgos[20]. „Deloitte Touche Tohmatsu“ 2008 metais atliko detalų informacijos saugos valdymo tyrimą energetikos ir gamtinių išteklių sektoriaus įmonėse, įsikūrusiose visame pasaulyje. Šio tyrimo rezultatai palyginti su Lietuvoje atliktais RRT tyrimais[21]. UAB „Baltic Consulting Group“ 2008 metų lapkričio mėnesį atliko apklausą „Kiek saugi yra Lietuvos įmonių Informacija“. Šioje apklausoje dalyvavo 400 įvairaus masto Lietuvos įmonių iš visų Lietuvos regionų[22].

Pažymėtina, kad 2008 metų lapkričio mėnesį Lietuvos Respublikos Ministro Pirmininko potvarkiu[23] sudaryta tarpžinybinė darbo grupė pateikė Vyriausybei veiklos ataskaitą ir pasiūlymus dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių. Identifikuotos aštuonios svarbiausios veiklos kryptys ir penkiasdešimt konkrečių priemonių šios srities galimam tobulinimui (detaliau apie tarpžinybinės darbo grupės 2008 metų lapkričio mėnesį Vyriausybei pateiktas Lietuvos kibernetinio saugumo stiprinimo kryptis ir identifikuotas konkrečias priemones ataskaitos 1 priede).

> Tarpžinybinės darbo grupės pateikti pasiūlymai yra išsamūs ir pateikia galimų veiksmų alternatyvias galimybes, tačiau Vyriausybei yra tik rekomendacinio pobūdžio, todėl neaiški jų įgyvendinimo perspektyva ir terminai.

[20] Prieiga per internetą http://www.esaugumas.lt/index.php?-1927404872 (žiūrėta 2009-02-23).
[21] Prieiga per internetą http://www.esaugumas.lt/index.php?1512988419 (žiūrėta 2009-02-23).
[22] Prieiga per internetą http://www.e-bcg.com/ (žiūrėta 2009-02-23).
[23] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės Lietuvos kibernetinio saugumo klausimams išnagrinėti ir pasiūlymams dėl jo stiprinimo parengti pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti.

NUSTATYTOS VEIKLOS PROBLEMOS

Tyrimo metu nustatėme, kad egzistuoja šios su strateginės elektroninės informacijos sauga susijusios problemos:

1. STRATEGINIO PLANAVIMO IR TEISINIO REGLAMENTAVIMO TRŪKUMAI

Pirmoji IT saugos valstybinė strategija[24] patvirtinta 2001 metais. Įgyvendinimo laikotarpiu (2002–2004 metais) strategija numatė valstybės IT saugos raidos pagrindines kryptis ir priemones IT saugos tikslams pasiekti. Nuo 2006 metų birželio mėnesio iki 2008 metų pagrindinius valstybės elektroninės informacijos saugos užtikrinimo principus, tikslus, uždavinius ir jų įgyvendinimą nustatė Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija[25].

Tyrimo metu nustatyta, kad po 2008 metų Lietuvoje nebuvo parengtos naujos ar atnaujintos galiojančios strategijos ir jų įgyvendinimo priemonių planai, numatantys elektroninių ryšių tinklų ir informacinių sistemų saugumo srities raidą. Nenumatyti tolimesni strateginiai žingsniai, kaip bus tobulinamas elektroninės informacijos saugos koordinavimas ir priežiūra (pvz.: aiškiai neįvardyti teisės aktai, kuriais bus siekiama reguliuoti nacionalinės elektroninės informacijos saugą, tobulinti elektroninės informacijos perdavimo infrastruktūros saugą, kelti elektroninės informacijos saugos kultūrą). Neapsispręsta, kaip po 2008 metų bus skatinamas strateginio lygmens elektroninės informacijos saugos užtikrinimo projektų įgyvendinimas.

> Yra rizika, kad neįvardijus strateginių nacionalinių elektroninės informacijos saugos principų ir metodų, gali kilti neaiškumų, prieštaravimų ir skirtingų interpretavimų priimant strateginius sprendimus dėl konkrečių šios srities saugumo stiprinimo krypčių ir priemonių.

Atsižvelgdama į gerąją kitų valstybių praktiką ir poreikį turėti nacionalines strateginio lygmens gaires kibernetinio saugumo srityje, tarpžinybinė darbo grupė[26] 2008 metų lapkričio mėnesį pasiūlė Vyriausybei inicijuoti šių strategijų rengimą:

- Lietuvos kibernetinio saugumo;
- Lietuvos ypatingai svarbios infrastruktūros apsaugos[27].

[24] Lietuvos Respublikos Vyriausybės 2001-12-22 nutarimu Nr. 1625 patvirtinta „Informacijos technologijų saugos valstybinė strategiją“.
[25] Lietuvos Respublikos Vyriausybės 2006-06-19 nutarimu Nr. 601 patvirtinta „Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 metų“.
[26] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita.

Tarpžinybinė darbo grupė Vyriausybei pasiūlė šias strategijas parengti iki 2009 metų pabaigos. Tyrimo metu Vyriausybė konkrečių sprendimų dėl šių darbo grupės pateiktų siūlymų dar nebuvo priėmusi.

1.1. Strateginės elektroninės informacinės saugos teisinis reglamentavimas

Sėkmingas strateginės informacinės saugumo politikos įgyvendinimas neatsiejamai susijęs su aiškiu šios srities teisiniu reglamentavimu.

Auditoriai, atlikę teisės aktų, reglamentuojančių strateginės elektroninės informacijos saugos sritį analizę, pastebėjo, kad esami teisės aktai numato tik fragmentišką šios srities reglamentavimą, neužtikrina visapusiško ir nuoseklaus strateginės elektroninės informacijos saugos visuomeninių santykių reglamentavimo. Tyrimo metu nebuvo patvirtinti Elektroninių ryšių tinklų ir informacijos saugumo, Valstybės informacinių išteklių valdymo įstatymai. Neparengtas įstatymas reglamentuojantis ypatingos svarbos infrastruktūrą bendrai, tiek apimant nuostatas, susijusias su ypatingos svarbos informacine infrastruktūra[28]. Valstybės ir savivaldybių elektroninių ryšių tinklų ir informacinių sistemų saugumą reglamentuoja ne įstatymai, o Vyriausybės nutarimai, ministrų įsakymai, kuriuose nurodoma, kad Vyriausybei nepavaldžioms institucijoms ir įstaigoms jie yra tik rekomendacinio pobūdžio.

Minėtos teisinio reglamentavimo spragos neleidžia išspręsti kai kurių su strategine elektroninės informacijos sauga susijusių svarbių klausimų (pvz.: identifikuoti strateginės elektroninės informacijos saugos institucinę sistemą, aiškiai įvardinti terminus ir sąvokas, nustatyti tinklų ir elektroninės informacijos saugumo reglamentavimo, vertinimo ir incidentų tyrimo sistemas ir pan.).

> Tyrimo metu nebuvo Lietuvos Respublikos įstatymų ir poįstatyminių teisės aktų, kurie išsamiai ir sistemingai reglamentuotų procesus, susijusius su strateginės elektroninės informacijos sauga. Todėl išlieka didelė rizika, kad dėl nepakankamai apibrėžto šios srities teisinio reglamentavimo gali būti neužtikrinta strateginės elektroninės informacijos ir infrastruktūros, leidžiančios šią informaciją gauti, apdoroti, perteikti ir saugoti tinkama apsauga.

Tarpžinybinė darbo grupė 2008 metų lapkričio mėnesį taip pat pasiūlė Vyriausybei imtis konkrečių priemonių, stiprinant teisinę bazę kibernetinio saugumo politikos formavimo ir priežiūros srityje (detaliau apie tarpžinybinės darbo grupės 2008 metų lapkričio mėnesį Vyriausybei pateiktas Lietuvos kibernetinio saugumo stiprinimo kryptis ir identifikuotas konkrečias priemones – ataskaitos 1 priede).

[27] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės siūlymu šioje strategijoje turės būti apibrėžti ir ypatingos svarbos informacinės infrastruktūros nacionaliniu mastu apsaugos principai.
[28] Ten pat.

1.2. Strateginės elektroninės informacijos saugos objektų identifikavimas

Tyrimo metu nebuvo įstatymo, kuris nustatytų pagrindinius Lietuvos strateginių informacinių sistemų, tinklų ir informacijos saugumo užtikrinimo principus ir sąvokas. Auditoriai pastebėjo, kad rengiamuose šios srities teisės aktų projektuose pateikiamos netapačios su strateginės elektroninės informacijos sauga susijusios sąvokos ir jų sudėtinės dalys (3 pavyzdys).

3 pavyzdys

1. Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijoje[29] tinklų ir informacijos saugumas apibrėžiamas kaip elektroninių ryšių tinklo ar informacinės sistemos pajėgumas pakankamu patikimumo lygiu išlaikyti atsparumą nuo atsitiktinių įvykių ar veiksmų, kurie kelia ar gali sukelti pavojų išsaugotų, tvarkomų, per informacinę sistemą ar elektroninių ryšių tinklu perduodamų elektroninių duomenų ir susijusių siūlomų ar per tą informacinę sistemą arba elektroninių ryšių tinklu gaunamų paslaugų prieinamumui, tapatumui, vientisumui ar slaptumui, taip pat pajėgumas užkirsti kelią perduoti elektroninio pašto pranešimus, siunčiamus tiesioginės rinkodaros tikslu be abonento išankstinio sutikimo.

Kritinė informacinė infrastruktūra – elektroninių ryšių tinklas, informacinė sistema ar informacinių sistemų grupė, prie kurios neteisėtas prisijungimas ir sąlygų neteisėtai prisijungti sudarymas, kurios neteisėtas sutrikdymas ar pakeitimas, kurioje saugomų, tvarkomų, iš jos išrenkamų arba ja perduodamų elektroninių duomenų sunaikinimas, sugadinimas, pašalinimas ar pakeitimas, panaikinimas arba galimybės naudotis tokiais elektroniniais duomenimis apribojimas turi ar gali turėti įtakos nacionaliniam saugumui, šalies ūkiui ar visuomenės gerovei.

2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo projekte[30] ypatingos svarbos informacinius išteklius sudaro informacija, kurią valdo įstaiga, vykdydama pavestas funkcijas, svarbi visai valstybei, tvarkoma informacinėmis sistemomis ir pagrindiniais valstybės registrais. Prie ypatingos svarbos ir svarbių informacinių sistemų taip pat priskiriamos informacinės sistemos, kurioms kurti ar modernizuoti viršytas Vyriausybės ar jos įgaliotos institucijos nustatytas lėšų dydis.

Tarpžinybinė darbo grupė pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti 2008 metų lapkričio mėnesį pateikė Vyriausybei „kibernetinio saugumo“ sąvokos projektą, apimantį šiuos elementus:

- informaciją;
- tinklą, kuriuo perduodama informacija;
- informacinę sistemą, skirtą informacijai tvarkyti[31].

Auditorių manymu, tarpžinybinės darbo grupės įvardytos sąvokos, susijusios su kibernetiniu saugumu, apima ir strateginės elektroninės informacijos saugos aspektus, todėl išankstinio tyrimo ataskaitoje šie klausimai nagrinėjami kaip kibernetinio saugumo srities sudėtinė dalis (išsamiau apie sąvokas, apibrėžiančias kibernetinį saugumą ir su juo susijusius aspektus, – ataskaitos 2 priede).

Pastebėjimas

Lietuvoje kibernetinio saugumo srities sąvokų projektai ir su tuo susiję strateginės elektroninės informacijos saugos aspektai teisiškai neapibrėžti, todėl vertinti tik kaip rekomendacinio pobūdžio ir turėtų būti tobulinami priėmus galutinį sprendimą dėl šios srities elementų visumos.

[29] Lietuvos Respublikos Vyriausybės 2006-12-06 nutarimu Nr. 1211 patvirtinta „Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija“.
[30] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo projektas.
[31] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita.

Remiantis pasaulyje pripažinta IT valdymo gerąja praktika[32] ir standartais[33], Lietuvos strateginės elektroninės informacijos saugos kritinės sritys turėtų būti nustatomos atsižvelgiant į rizikos vertinimą ir reguliariai (ne rečiau kaip kartą per metus) turėtų būti peržiūrimos arba atnaujinamos.

Tyrimo metu pastebėta, kad Lietuvoje nėra atliekamas strateginės elektroninės informacijos saugos sričių rizikos vertinimas. Šios srities objektų ir informacinės infrastruktūros identifikavimo procesai nepakankamai reglamentuoti teisės aktais. Įstatymuose įtvirtintas susijusių sričių teisinis reglamentavimas yra pernelyg bendro pobūdžio, kad būtų galima aiškiai identifikuoti strateginės elektroninės informacijos saugos objektus ir informacinę infrastruktūrą (4 pavyzdys).

4 pavyzdys

Strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių (tarp jų ir steigtinų) sąrašas nustatytas įstatymu[34]. Įstatymas nereglamentuoja, kurios iš sąraše paminėtų įmonių ir įrenginių turi strateginę reikšmę informacijos saugai.

Atsižvelgiant į įmonių veiklos ypatumus, galima tik numanyti ypatingos svarbos infrastruktūros objektus ir dalį nacionalinės svarbos informacinės infrastruktūros.

> Neidentifikavus su strateginės elektroninės informacijos sauga susijusių ypatingos svarbos objektų ir informacinės infrastruktūros ir neatlikus jų rizikos vertinimo, kyla didelė rizika, kad diegiamos ir taikomos strateginės elektroninės informacijos saugos priemonės gali būti neadekvačios saugomam turtui.

Tarpžinybinė darbo grupė 2008 metų lapkričio mėnesį Vyriausybei pateikė svarstymui siūlymą identifikuoti Lietuvos ypatingos svarbos infrastruktūros objektus nacionaliniu mastu ir ypatingos nacionalinės svarbos informacinę infrastruktūrą. Be to, pasiūlyta identifikuoti viešųjų tinklų, žinybinių ir tarpžinybinių paslaugų vartotojų grupes pagal jų poreikius ir reikalavimus apsaugai nuo grėsmių viešuosiuose tinkluose kibernetinėje erdvėje.

Iki tyrimo pabaigos (2009 m. vasario 27 d.) Vyriausybė galutinio sprendimo dėl tarpžinybinės darbo grupės pateiktų siūlymų stiprinti Lietuvos kibernetinį saugumą dar nebuvo priėmusi.

[32] *CobIT (Control Objectives for Information and related Technologies*) – visame pasaulyje žinomas tarptautinės *ISACA* organizacijos standartas. *CobIT* aprašo geriausią praktiką informacinių technologijų valdymo srityje.
[33] *ISO/IEC 27001:2005*. Information technology - Security techniques - Information security management systems - Requirements (tapatus *LT ISO/IEC 27001:2006*).
[34] Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas, 2002-10-10 Nr. IX-1132.

2. NESUKURTA STRATEGINĖS ELEKTRONINĖS INFORMACIJOS SAUGOS STEBĖSENOS SISTEMA IR NEPAKANKAMAI APIBRĖŽTA ŠIĄ SRITĮ KOORDINUOJANČIŲ INSTITUCIJŲ KOMPETENCIJA

2.1. Strateginės elektroninės informacijos saugos organizacinės struktūros ir valdymo sistema

Kasdieniame Lietuvos valstybės ir visuomenės gyvenime lemiamą reikšmę įgyja informacija ir technologijos, leidžiančios šią informaciją gauti, apdoroti, perteikti ir saugoti. Todėl strateginių elektroninių ryšių tinklų ir informacijos sauga tampa ne vienos valstybinės institucijos veiklos objektu (1 lentelė).

1 lentelė. Elektroninių ryšių tinklų ir informacijos saugos klausimais Lietuvoje dirbančios institucijos.

Institucija	Priskirtos funkcijos
Susisiekimo ministerija	Nustato elektroninių ryšių sričių plėtojimo pagrindines kryptis ir koordinuoja elektroninių ryšių veiklą[35].
VRM	Dalyvauja įgyvendinant valstybės informacines visuomenes plėtros politiką ir koordinuoja IT saugą valstybes institucijoje ir įstaigose[36].
RRT	Užtikrina, kad operatoriai ir elektroninių ryšių paslaugų teikėjai vykdytų įsipareigojimus, kurie gali būti nustatyti valstybės gynybos, nacionalinio saugumo ir viešosios tvarkos palaikymo interesais, taip pat ypatingų situacijų atvejais. Rengia reikalavimus telekomunikacinių paslaugų tiekėjams dėl ryšio užtikrinimo ir tikrina, kaip tokie reikalavimai yra užtikrinami. Be to, RRT vykdo nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio (toliau – *CERT*) (angl. *Computer Emergency Response Team*) veiklą[37]
Krizių valdymo centras	Vyriausybės įsteigtas Krizių valdymo centras yra pagrindinis valstybės įvairaus pobūdžio krizių valdymo strateginiu lygmeniu štabas[38].
IVPK	Dalyvauja formuojant valstybės informacijos technologijų ir telekomunikacijų kūrimo Lietuvos Respublikoje politiką ir koordinuoja jos įgyvendinimą. Įgyvendindamas šį uždavinį, inicijuoja valstybės informacinių sistemų ir valstybės registrų kūrimo užtikrinimo privalomųjų reikalavimų rengimą[39].
Nusikaltimų elektroninėje erdvėje tyrimo valdyba	Vykdo elektroninę žvalgybą tinkluose, atlieka sukčiavimo, grasinimo, vaikų išnaudojimo pornografijai bei kitų sričių ikiteisminius tyrimus. Ruošia ir teikia įvairius pasiūlymus dėl teisinės bazės tobulinimo tiriant nusikaltimus, vykdomus elektroninėje erdvėje[40].
Valstybinė duomenų apsaugos inspekcija	Užtikrina asmens duomenų apsaugą, tikrina asmens duomenų tvarkymo teisėtumą ir priima sprendimus dėl asmens duomenų tvarkymo pažeidimų. Vykdo registruotų duomenų valdytojų veiklos, susijusios su asmens duomenų tvarkymu, priežiūrą, vertina duomenų valdytojų pateiktas asmens duomenų tvarkymo taisykles. Įstatymo nustatytais atvejais atlieka išankstinę patikrą ir teikia išvadas duomenų valdytojui apie numatomą duomenų tvarkymą[41].
Valstybės saugumo departamentas	Atsakingas už įslaptintos informacijos apsaugos kontrolę. Savarankiškai arba kartu su kitomis įgaliotomis valstybės ar savivaldybių institucijomis ar įstaigomis rengia ir įgyvendina priemones ir reikalavimus dėl valstybės ir tarnybos paslapčių, svarbiausių komunikacijų, ryšių apsaugos[42].

[35] Lietuvos Respublikos Vyriausybės 1998-09-15 nutarimu Nr. 1117 patvirtinti „Lietuvos Respublikos susisiekimo ministerijos nuostatai“.
[36] Lietuvos Respublikos Vyriausybės 2001-03-14 nutarimu Nr. 291 patvirtinti „Lietuvos Respublikos vidaus reikalų ministerijos nuostatai“.
[37] Lietuvos Respublikos Vyriausybės 2004-08-19 nutarimu Nr. 1029 patvirtinti Lietuvos Respublikos ryšių reguliavimo tarnybos nuostatai“.
[38] Lietuvos Respublikos Vyriausybės 2001-07-27 nutarimu Nr. 939 patvirtinti „Krizių valdymo centro prie Krašto apsaugos ministerijos nuostatai“.
[39] Lietuvos Respublikos Vyriausybės 2001-07-05 nutarimu Nr. 844 patvirtinti „Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės nuostatai“.
[40] Lietuvos policijos generalinio komisaro 2007-08-03 įsakymu Nr. 5-V-522 patvirtinti „Lietuvos kriminalinės policijos biuro nuostatai ir struktūros schema“.
[41] Lietuvos Respublikos Vyriausybės 2001-09-25 nutarimu Nr. 1156 patvirtinti „Valstybinės duomenų apsaugos inspekcijos nuostatai“.
[42] Lietuvos Respublikos valstybės saugumo departamento įstatymas, 1994-01-20 Nr. I-380.

Iš minėtų institucijų tyrimo metu didžiausią įtaką užtikrinant Lietuvos elektroninių ryšių tinklų ir informacijos saugumą turėjo VRM, Susisiekimo ministerija ir RRT. Šių institucijų kompetencijos nėra persidengiančios, tačiau trūksta aiškios koordinacijos strateginės elektroninės informacijos saugos politikos, jos priežiūros ir įgyvendinimo klausimais. Be to, kaip buvo minėta, teisės aktais aiškiai neapibrėžti svarbiausi šios srities saugumo politikos formuotojai ir įgyvendintojai, jų tarpusavio ryšiai. Viešų, žinybinių, tarpžinybinių elektroninių ryšių tinklų ir informacinių paslaugų tiekėjams nėra nustatyti įpareigojimai teikti atsakingoms institucijoms su tinklų ir informacijos sauga susijusią informaciją ir imtis prevencijos, stebėjimo ir reagavimo, valdymo ir likvidavimo veiksmų, siekiant sumažinti grėsmes kitiems veiklos dalyviams. Pažymėtina, kad, nors teisės aktai nereglamentuoja viešojo ir privataus sektorių bendradarbiavimo principų ir mechanizmų, privatūs Lietuvos verslo subjektai (pvz.: komerciniai bankai) tinklų ir informacijos saugos klausimams skiria ypač daug dėmesio ir yra pasirengę prisidėti prie viešojo sektoriaus pastangų, siekiant užtikrinti nacionalinį šios srities saugumą[43].

Rengiant Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepciją 2006 metais, siūlyta įstatymu pataisyti atsiradusias reglamentavimo spragas ir suteikti RRT pagrindines rinkos priežiūros funkcijas tinklų ir informacijos saugumo srityje[44]. Valstybės informacinių išteklių valdymo įstatymo projekte[45] numatoma už įstaigų valdomų valstybės informacinių išteklių saugos koordinavimą ir priežiūrą atsakomybę priskirti VRM.

> Lietuvoje nebaigta formuoti strateginės elektroninės informacijos saugos valdymo ir priežiūros įstatyminė bazė ir organizacinė struktūra. Todėl kyla rizika, kad nesuderinti skirtingų institucijų sprendimai ir veiksmai gali dubliuotis, bus neefektyviai valdoma ir prižiūrima su strateginės elektroninės informacijos sauga susijusi infrastruktūra ir gali būti netaupiai naudojamos šiam tikslui skiriamos lėšos.

Apie būtinybę Lietuvoje sukurti nacionalinę kibernetinio saugumo koordinacinę sistemą 2008 metų pabaigoje Vyriausybei patarė Ministro Pirmininko potvarkiu sudaryta tarpžinybinė darbo grupė[46], kuri įvardino tris esminius šios srities saugumo politikos formavimo ir įgyvendinimo sistemos elementus:

- įsteigti (identifikuoti) kibernetinio saugumo politiką koordinuojančią ir šios politikos įgyvendinimo priežiūrą atliekančią nacionalinę instituciją (apimant ir nacionalinės reikšmės ypatingos svarbos informacines infrastruktūras);

[43] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita.
[44] Lietuvos Respublikos Vyriausybės 2006-12-06 nutarimu Nr. 1211 patvirtinta „Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija“.
[45] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo projektas.
[46] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita.

- įsteigti tarpžinybinę nenumatytų (kritinių) situacijų valdymo grupę (analogija *Ad hoc* kibernetinių situacijų centrui), kurios nariai galėtų efektyviai priimti sprendimus dėl būtinų kibernetinės gynybos priemonių gavus informaciją iš atitinkamų institucijų (kaip pavyzdžiui nacionalinis *CERT*) apie gresiančias masines kibernetines atakas (incidentus) arba jau įvykus masinėms kibernetinėms atakoms;
- stiprinti nacionalinio *CERT* pajėgumus, aiškiai apibrėžti nacionalinio ir vietinių *CERT* veiklos procedūras ir įgaliojimus rūpintis atitinkama ypatingos svarbos informacine infrastruktūra.

Pažymėtina, kad neaiški (neidentifikuota) nacionalinė strateginės elektroninės informacijos saugos valdymo ir priežiūros struktūra gali neužtikrinti efektyvaus bendradarbiavimo su Europos Sąjunga ir Šiaurės Atlanto Sutarties Organizacija, kurios skiria daugiau dėmesio elektroninės informacijos saugai. Europos Sąjungos strateginiuose dokumentuose[47] ypač daug dėmesio skiriama atsakingų šalių narių institucijų tarpusavio bendradarbiavimo ir dialogo su privačiu sektoriumi stiprinimui, operatyvinių ir strateginių informacijos mainų tarp šalių narių skatinimui, pirmiausia siekiant palengvinti teisėsaugos institucijų darbą tiriant nusikaltimus kibernetinėje erdvėje ir užtikrinti keitimąsi gerąja praktika apie šalyse veikiančias prevencijos, perspėjimo ir reagavimo sistemas[48].

Auditoriai pritaria tarpžinybinės darbo grupės siūlymui nustatyti aiškias Lietuvos institucijų atsakomybės ribas, kad būtų galima efektyviai dalyvauti, formuoti ir įgyvendinti Europos Sąjungos ir nacionalinę politiką elektroninės informacijos saugos srityje.

2.2. Strateginės elektroninės informacijos saugos stebėsena, grėsmių ir pažeidžiamumų nustatymas, prevencija ir likvidavimas

Pasaulinė praktika rodo, kad informacinių technologijų saugumo incidentų tyrimo grupės *CERT* tampa svarbiausiu įrankiu vykdant IT saugumo incidentų valdymą elektroninių ryšių tinkluose.

Lietuvoje pirmasis *CERT* pradėjo veiklą 1998 metais[49]. 2006 m. spalio 2 d. RRT įsteigtasis *CERT* 2008 m. liepos 9 d. pradėjo vykdyti nacionalinio *CERT* veiklą[50].

[47] Europos Komisijos 2001-01-26 komunikatas Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Saugesnės informacinės visuomenės sukūrimas gerinant informacijos infrastruktūrų saugumą ir kovojant su kompiuteriniais nusikaltimais“; 2006-05-31 komunikatas Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Saugios informacinės visuomenės strategija – dialogas, partnerystė ir teisių suteikimas“; 2007-05-22 komunikatas Tarybai, Europos Parlamentui, Europos Regionų komitetui „Bendrosios politikos, skirtos kovai su elektroniniais nusikaltimais, linkme“.

[48] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita.

[49] Prieiga per internetą http://cert.litnet.lt/apie.html (žiūrėta 2009-02-11).

Tyrimo metu nustatyta, kad Lietuvoje *CERT* veikla nėra aiškiai apibrėžta: nereglamentuoti nacionalinio ir kitų *CERT* veiklos tikslai, uždaviniai, funkcijos, teisės ir atsakomybė, jų tarpusavio bendradarbiavimas. Neapibrėžtos teikėjų teisės ir pareigos užtikrinant elektroninių ryšių tinklų ir informacijos saugumą. Stokojama koordinuoto bendradarbiavimo tarp šios srities privataus ir viešojo sektoriaus institucijų strateginės elektroninės informacijos saugos klausimais.

Minėtos problemos aiškiai parodo, kad nacionalinis *CERT* kartu su vietiniais *CERT*, kol kas nėra pajėgūs rūpintis atitinkama ypatingos svarbos informacine infrastruktūra.

Atkreiptinas dėmesys, kad nuo 2006 metų RRT veikiančio *CERT* nuostatai nėra patvirtinti, tačiau jo veiklai 2007–2008 metais skirta valstybės biudžeto lėšų (362 tūkst. Lt) iš specialios Ryšių valdymo ir kontrolės programos[51].

> Kyla didelė rizika, kad taip Lietuvoje veikianti *CERT* sistema gali būti tarpusavyje nesuderinta, nepakankamai funkcionali, lėšos skirtos nacionalinio *CERT* veiklai gali būti panaudojamos nerezultatyviai.

Be minėtos veiklos, susijusios su reagavimu į IT saugumo incidentus, nuo 1998 metų Lietuvoje veikiantys *CERT* atlieka statistinę tinklų ir informacijos saugumo incidentų duomenų analizę, skelbia ketvirtinę ir metinę incidentų statistiką. Pažymėtina, kad nuo 2004 metų RRT atliekami išsamūs tinklų ir informacijos saugumo padėties Lietuvoje tyrimai[52]. Tačiau, kaip jau buvo minėta ankstesnėse ataskaitos dalyse, įstatymu nėra nustatyta tinklų ir informacijos saugumo incidento sąvoka, privataus ir viešojo sektorių institucijų prievolė pranešti apie tinklų ir informacijos saugumo incidentus.

> Kyla rizika, kad nesant aiškių teisinių nuostatų dėl elektroninės informacijos saugos incidentų sąvokos ir prievolės apie juos pranešti, nacionalinio ir kitų *CERT* skelbiama Lietuvos incidentų statistika gali būti netiksli, nežinomas tikrasis šios srities incidentų mastas.

Šios ir kitos elektroninės informacijos saugos silpnosios vietos jau buvo užfiksuotos 2006 metais elektroninės informacijos saugos valstybinėje strategijoje[53]. Apie pastebėtus trūkumus, susijusius su strateginę reikšmę nacionaliniam saugumui turinčių svarbių įmonių informacinės ir fizinės saugos reglamentavimu ir reikalavimų vykdymu, 2007 metais Valstybės kontrolė atskiru

[50] Lietuvos Respublikos Vyriausybės 2004-08-19 nutarimu Nr. 1029 patvirtinti „Lietuvos Respublikos ryšių reguliavimo tarnybos nuostatai“, 8.43. p. (Lietuvos Respublikos Vyriausybės 2008-07-09 nutarimo Nr. 678 redakcija).
[51] Specialioji ryšių valdymo ir kontrolės programa (Prieiga per internetą http://www.rrt.lt/index.php?564581933 ir http://www.rrt.lt/index.php?2132577681 (žiūrėta 2009-02-11)).
[52] Prieiga per internetą http://www.esaugumas.lt/index.php?-1927404872 (žiūrėta 2009-02-23).
[53] Lietuvos Respublikos Vyriausybės 2006-06-19 nutarimu Nr. 601 patvirtinta „Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 metų“.

raštu informavo Vyriausybę ir Lietuvos Respublikos ūkio ministeriją[54]. Iki tyrimo pabaigos (2009 m. vasario 27 d.) Lietuvoje dar nebuvo sukurta išankstinio perspėjimo apie galimą grėsmę ir reagavimo į elektroninės informacijos saugos incidentus sistema. Neaiškūs teisiniai įpareigojimai, reglamentuojantys viešojo ir privataus sektorių veiklą strateginės elektroninės informacijos saugos grėsmių, pažeidžiamumų stebėsenos ir prevencijos srityse.

Pažymėtina, kad su strateginės elektroninės informacijos sauga susijusių grėsmių ir pažeidžiamumų nustatymo, prevencijos, incidentų pasekmių valdymo ir likvidavimo procesai yra tarpusavyje susiję. Tyrimo metu išryškėjo visoms šios srities vykdomoms veikloms pasikartojančios problemos (pvz.: nepakankamas teisinis reglamentavimas, institucinės sistemos trūkumai ir pan.), turinčios įtakos Lietuvos pasirengimui valdyti ir likviduoti su strateginės elektroninės informacijos sauga susijusius pažeidimus. Be to, 2008 metais atlikus Lietuvos kibernetinio saugumo vertinimą[55] išsiaiškinta, kad trūksta elektroninių ryšių ir ypatingos svarbos informacinės infrastruktūros informacinių sistemų veiklos atkūrimo planų. Nesukurti rezerviniai ištekliai ir pajėgumai Lietuvos kibernetinė erdvės veiklos nenutrūkstamumui užtikrinti.

> Dauguma Lietuvos elektroninės informacijos saugos grėsmių ir pažeidžiamumų nustatymo, prevencijos, incidentų pasekmių valdymo ir likvidavimo silpnųjų vietų jau buvo žinomos nuo 2006 metų, tačiau reikiamų teisinio reglamentavimo ir organizacinių priemonių parengta nebuvo. Todėl kyla rizika, kad taikomos strateginės svarbos elektroninių ryšių tinklų ir informacijos funkcionavimo atstatymo ir apsaugos nuo netikėtų sutrikimų priemonės gali būti neefektyvios.

[54] Lietuvos Respublikos valstybės kontrolės raštai: 2007-12-22 Nr. S-(901-1.9.1)-2002 „Dėl valstybinio audito rezultatų“; 2007-12-21 Nr. S-(901-1.10.1)-1997 „Dėl valstybinio audito rezultatų“.
[55] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita.

PASIRINKTOS VEIKLOS PROBLEMOS

Išankstinio tyrimo metu nustatėme dvi pagrindines su strateginės elektroninės informacijos sauga susijusias problemas:

- Strateginio planavimo ir teisinio reglamentavimo trūkumai (neapibrėžti planavimo procesai, nepakankamas teisinis reglamentavimas, neidentifikuoti strateginės elektroninės informacijos saugos objektai).
- Nesukurta strateginės elektroninės informacijos stebėsenos sistema ir nepakankamai apibrėžta šią sritį koordinuojančių institucijų kompetencija (nebaigta formuoti organizacinė struktūra ir valdymas, nenustatyta grėsmių ir pažeidžiamumų, prevencijos, incidentų pasekmių valdymo ir likvidavimo sistema).

Manome, kad aktualios visos išankstinio tyrimo metu nustatytos problemos. Tačiau išnagrinėję su strateginės elektroninės informacijos sauga susijusias sritis nustatėme, kad auditorių įvardytoms pagrindinėms veiklos problemoms spręsti 2008 metų lapkričio mėnesį Vyriausybei buvo pateikti tarpžinybinės darbo grupės pasiūlymai ir numatytos priemonės (1 priedas).

Įvertinę Vyriausybei pateiktų pasiūlymų ir numatytų konkrečių priemonių apimtis manome, kad laiku vykdomas ir kokybiškas jų įgyvendinimas galėtų padėti išspręsti išankstinio tyrimo metu nustatytas su strateginės elektroninės informacijos sauga susijusias problemas. Dauguma tarpžinybinės darbo grupės įvardytų Lietuvos kibernetinio saugumo stiprinimo priemonių (pvz.: dėl šios srities teisinės bazės ir nacionalinės koordinacinės sistemos sukūrimo, grėsmių ir pažeidžiamumų, prevencijos, incidentų pasekmių valdymo ir likvidavimo sistemos tobulinimo) yra realiai įgyvendinamos ir sudaro galimybes taisyti ne tik kibernetinio saugumo, bet ir strateginės informacijos saugos srityje nustatytas teisinio reglamentavimo, institucinės sistemos ir kitas spragas, vykdyti jų pertvarką. Paminėti trūkumai šiose srityse yra tarpusavyje glaudžiai susiję, todėl, kompleksiškai įgyvendinant Vyriausybei siūlomas priemones, kartu būtų galima tinkamai išspręsti ir išankstinio tyrimo metu nustatytas pagrindines strateginės elektroninės informacijos saugos problemas.

Atsižvelgiant į tai, kad pateiktų Lietuvos kibernetinio saugumo stiprinimo priemonių efektyviam įgyvendinimui yra reikalingi Vyriausybės sprendimai, planuojame, pasibaigus numatytam išankstinio tyrimo terminui, kreiptis į Vyriausybę su prašymu pateikti informaciją apie priimamus sprendimus dėl tarpžinybinės darbo grupės pateiktų siūlymų ir programoje numatytų

priemonių įgyvendinimo ir stebėti jų vykdymą (iki tyrimo pabaigos Vyriausybė konkrečių sprendimų dėl šios darbo grupės pateiktų siūlymų dar nebuvo priėmusi).

Dėl nurodytų priežasčių manome, kad šiuo metu atlikti auditą būtų netikslinga. Analizuotos srities problemos bus stebimos ir toliau, atliekant strateginį tyrimą.

Informacinių sistemų valdymo ir audito departamento
direktorius Dainius Jakimavičius

Informacinių sistemų valdymo ir audito departamento
Informacinių sistemų audito skyriaus
vyresnysis valstybinis auditorius Rimgaudas Gamulis

Valstybinio audito ataskaitos kopija (1 egz.) pateikta Lietuvos Respublikos Vyriausybei.

PRIEDAI

Valstybinio audito ataskaitos
„Strateginės informacijos sauga“
1 priedas

Lietuvos kibernetinio saugumo stiprinimo kryptys ir priemonės

1 kryptis - Teisinės bazės kibernetinio saugumo srityje sukūrimas

Priemonės:

a) parengti šias strategijas:
   Lietuvos kibernetinio saugumo;
   Lietuvos ypatingai svarbios infrastruktūros apsaugos[56].
b) parengti Elektroninių ryšių tinklų ir informacijos saugumo įstatymą;
c) parengti Lietuvos Respublikos įstatymą, reglamentuojantį ypatingos svarbos infrastruktūrą bendrai, tiek apimantį nuostatas, susijusias su ypatingos svarbos informacine infrastruktūra;
d) parengti Lietuvos Respublikos Vyriausybės nutarimą, kuris reglamentuotų kibernetinių incidentų klasifikavimo ir informavimo apie juos tvarką;
e) tikslinti Lietuvos Respublikos Valstybės ir tarnybos paslapčių įstatymą (Žin., 1999, Nr. 105-3019);
f) papildyti Nacionalinio saugumo pagrindų įstatymo priedėlį (Žin., 1997, Nr. 2-16);
g) parengti kitus teisės aktus, kurie apibrėžtų kitus būtinus kibernetinio saugumo politikos formavimo ir reguliavimo aspektus[57];
h) teisiškai apibrėžti įpareigojimus veiklos kibernetinėje erdvėje dalyviams dėl minimalios būtinos informacijos teikimo koordinuojančioms institucijoms ir kitiems veiklos dalyviams;
i) teisiškai apibrėžti įpareigojimus veiklos kibernetinėje erdvėje dalyviams imtis prevencijos, stebėjimo, reagavimo, valdymo ir likvidavimo veiksmų, siekiant sumažinti grėsmes kitiems veiklos dalyviams kibernetinėje erdvėje;
j) priimti/papildyti Lietuvos Respublikos Baudžiamojo kodekso ir Lietuvos Respublikos Administracinių teisės pažeidimų kodekso straipsnius dėl nusikaltimų kibernetinėje erdvėje.

2 kryptis - Nacionalinės koordinacinės sistemos kibernetinio saugumo srityje sukūrimas

Priemonės:

a) įsteigti/identifikuoti kibernetinio saugumo politiką koordinuojančią instituciją;
b) įkurti operatyvinio lygmens tarpžinybinę darbo grupę, kuri gavusi įspėjimą iš nacionalinio CERT apie kibernetinių atakų grėsmę prieš ypatingos svarbos informacinę infrastruktūrą, turėtų teisę priimti sprendimus dėl Lietuvos nacionalinės kibernetinės erdvės gynybos priemonių;
c) sukurti privataus ir viešojo sektorių bendradarbiavimo kibernetinio saugumo srityje mechanizmą;
d) reglamentuoti nacionalinio CERT ir vietinių CERT padalinių bendradarbiavimą reaguojant į kibernetinės atakas
e) tobulinti nacionalinio CERT funkcijas;

[56] Šioje strategijoje turės būti apibrėžti ir ypatingai svarbios informacinės infrastruktūros nacionaliniu mastu apsaugos principai.
[57] Siūlome atsižvelgti į keturias teisines fazes, susijusias su kibernetinio saugumo politikos formavimu ir reguliavimu: iki kibernetinių atakų (prevencija), kibernetinių atakų metų (valdymas/reagavimas), nuostolių atsiradimas dėl kibernetinių atakų, žalos atlyginimas/kibernetinių atakų pasekmių pašalinimas.

3 kryptis - Grėsmių ir pažeidžiamumo nacionalinei kibernetinei erdvei prevencija

Priemonės:

a) identifikuoti viešųjų, žinybinių ir tarpžinybinių tinklų paslaugų vartotojų grupes pagal jų poreikius ir reikalavimus apsaugai nuo grėsmių kibernetinėje erdvėje;
b) sukurti nacionalinės kibernetinės erdvės pažeidžiamumo vertinimo metodiką ir reguliariai vykdyti kibernetinės erdvės patikimumo tyrimus;
c) sukurti ypatingos svarbos infrastruktūros objektų, kurių informacinė infrastruktūra yra identifikuota kaip ypatingai svarbi, išankstinio įspėjimo sistemą;
d) sukurti nacionalinės kibernetinės erdvės stebėjimo sistemą;
e) stiprinti privataus ir viešojo sektorių bendradarbiavimą, numatant reguliarų keitimąsi informacija apie grėsmes nacionalinėje kibernetinėje erdvėje;
f) parengti gerosios praktikos rekomendacijas identifikuotoms viešųjų, žinybinių ir tarpžinybinių tinklų paslaugų vartotojų grupėms dėl kolektyvinės gynybos nuo grėsmių kibernetinėje erdvėje;
g) sukurti naujai atsirandančios programinės įrangos, diegiamos ypatingai svarbiuose informacinės infrastruktūros objektuose, patikimumo vertinimo sistemą;
h) vertinti elektroninių ryšių infrastruktūros priklausomybės bei veiklos patikimumo ryšius;
i) stiprinti interneto srautų tarptautinių ir tarptinklinių sujungimų saugos valdymą;
j) įpareigoti privataus verslo subjektus vadovautis ISO standartais rūpinantis informacinių sistemų saugumu (atitinkamai Lietuvos standartais LST ISO/IEC 17799:2006, LST ISO/IEC 27001:2006);
k) sukurti nacionalinę platformą pranešimams apie pažeidimus nacionalinėje kibernetinėje erdvėje talpinti, atsižvelgiant į ES iniciatyvą dėl europinės platformos pranešimams internete, susijusiems daugiau nei su viena valstybe nare sukūrimo;
l) stiprinti pajėgumus identifikuojant nusikaltimus kibernetinėje erdvėje ir užtikrinti kibernetinių nusikaltėlių baudžiamąjį persekiojimą;
m) skatinti fundamentaliuosius ir projektinius tyrimus kibernetinės erdvės apsaugos srityje (pvz., remti „kibernetinių projektų“ inicijavimą ir vykdymą Vilniaus Saulėtekio technologijų slėnyje);
n) diegti saugią elektroninę erdvę kuriančias priemones: sukurti asmens tapatybės nustatymo/patvirtinimo elektroninėje erdvėje koncepciją ir jos įgyvendinimo priemonių planą

4 kryptis - Nacionalinės reagavimo į kibernetinę grėsmę sistemos sukūrimas

Priemonės:

a) įpareigoti ypatingos svarbos infrastruktūros objektus (kurių informacinė infrastruktūra yra identifikuota kaip ypatingos svarbos) sudaryti ir reguliariai testuoti reagavimo į kibernetinės atakas planus;
b) pavesti nacionaliniam CERT užmegzti ir palaikyti ryšius su NATO ir ES šalių CERT;
c) kurti kibernetinių atakų valdymo grupes (vietinius CERT) ypatingai svarbiuose informacinės infrastruktūros objektuose;
d) stiprinti viešo ir privataus sektorių bendradarbiavimą pasirengiant reaguoti ir reaguojant į kibernetinius incidentus/atakas;
e) skatinti Lietuvos privačių interneto paslaugų teikėjų tarpusavio bendradarbiavimą, identifikuojant kibernetinės atakas bei keičiantis informacija apie jas.

5 kryptis - Nacionalinės kibernetinės erdvės pažeidimų likvidavimas

Priemonės:

a) sudaryti elektroninių ryšių ir ypatingos svarbos informacinės infrastruktūros informacinių sistemų veiklos atkūrimo po nacionalinės kibernetinės erdvės pažeidimų planus;
b) rengti nacionalines kibernetinės gynybos pratybas, kuriose reguliariai dalyvautų nacionalinis CERT ir vietiniai CERT;
c) reguliariai dalyvauti NATO kibernetinės gynybos pratybose;
d) sukurti rezervinius resursus kibernetinės erdvės „atkūrimo" pajėgumams;

6 kryptis - Informacinių technologijų (IT) saugumo standartų diegimas

Priemonės:

a) sertifikuoti IT bei IT saugos paslaugų teikėjus (arba - nustatyti kvalifikacinius reikalavimus IT bei IT saugos paslaugų teikėjams), galinčius teikti IT bei IT saugos paslaugas ypatingos svarbos informacinių infrastruktūros ir ypatingos svarbos infrastruktūros objektams;
b) įpareigoti ypatingos svarbos infrastruktūros objektus atlikti informacinių technologijų ir informacinių sistemų saugos atitikties vertinimą[58]. Identifikuoti atitinkamą instituciją, kuri tikrintų šių saugos atitikties vertinimų išsamumą ir objektyvumą;
c) įpareigoti privataus verslo subjektus vadovautis ISO standartais rūpinantis informacinių sistemų saugumu (atitinkamai Lietuvos standartais LST ISO/IEC 17799:2006, LST ISO/IEC 27001:2006)

7 kryptis - Bendradarbiavimas kibernetinio saugumo srityje su tarptautiniais partneriais

Priemonės:

a) stiprinti bendradarbiavimą žvalgybos tarnybų lygmenyje kibernetinių grėsmių vertinimo/prognozavimo klausimais;
b) stiprinti bendradarbiavimą su NATO, ES, JTO, ESBO, EBPO[59] kibernetinio saugumo klausimais;
c) aktyviai dalyvauti Kibernetinės gynybos tobulinimo centre Estijoje;
d) įsitraukti į tarptautinių CERT asociacijų FIRST ir TERENA[60] ir kitų veiklą, bei aktyviai bendradarbiauti su kitų šalių nacionaliniais CERT reguliariai keičiantis informacija ir rengiant pratybas.

8 kryptis - Nacionalinės kibernetinio saugumo kultūros formavimas

Priemonės

a) rengti ir pateikti vartotojams priemones, mažinančias neigiamą incidentų nacionalinėje kibernetinėje erdvėje įtaką;
b) skatinti apsaugos nuo incidentų ir atakų kibernetinėje erdvėje priemonių naudojimą;
c) stiprinti informacijos dėl saugaus elektroninių ryšių naudojimo sklaidą;
d) kelti valstybės institucijų vadovų ir kitų aukšto lygio tarnautojų, valstybės institucijų, valstybės įmonių ir privačių kompanijų informacinių sistemų administratorių, technologijos kūrėjų, įsigijimų politikos formuotojų, auditorių, privačių įmonių vadovų ir žinių apie informacinių technologijų saugumo standartus lygį:
    1. į mokymus įtraukti aukšto lygio valstybės tarnautojų (18-20 kategorijos) informacijos saugos mokymus, papildant LIVADIS vadovų mokymų programas;
    2. informacijos saugos klausimus įtraukti į valstybės tarnautojų įvadinio mokymo programą;
e) parengti galimybių studiją, kuri įvertintų galimybes parengti specialias mokymo programas Lietuvos universitetuose parengti IT saugumo specialistus.

[58] Saugos atitikties vertinimas turėtų buti atitikties standarto ISO/IEC 27001 reikalavimams vertinimas, reguliariai vykdomas kas 2-3 metai. Šis vertinimas turi būti pagrįstas atitinkama vertinimo metodika.
[59] Šiaurės Atlanto Sutarties Organizacija, Europos Sąjunga, Juntinių Tautų Organizacija, Europos Saugumo ir Bendradarbiavimo Organizacija, Ekonominio Bendradarbiavimo ir Plėtros Organizacija.
[60] FIRST *(angl.* Forum for Incident Response and Security Teams), TERENA – (*angl.* Trans-European Research and Education Networking Association).

Valstybinio audito ataskaitos
„Strateginės informacijos sauga“
2 priedas

Tarpžinybinės darbo grupės įvardintos sąvokos susijusios su kibernetiniu saugumu

Elektroninių ryšių tinklų ir informacinių sistemų saugumas - elektroninių ryšių tinkluose ir informacinėse sistemose įdiegtų priemonių visuma, leidžianti pakankamu patikimumo lygiu apsisaugoti nuo išorinio ir vidinio, įskaitant informacinį, žalingo poveikio, išlaikant funkcionalumą, kai elektroninių ryšių tinklų ir informacinių sistemų apkrova viršija maksimaliai suprojektuotą arba neužtikrina projektinių pajėgumų.

Kibernetinis saugumas - elektroninės informacijos tvarkymo/valdymo savybė, apimanti jos vientisumą, konfidencialumą, pasiekiamumą ir esant reikalui autentiškumą.

Konfidencialumas - informacijos savybė, kad elektroninė informacija yra tvarkoma tik asmenų turinčių tam teisę.

Vientisumas - informacijos savybė, kad informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

Prieinamumas - informacijos savybė, kad informacija gali būti tvarkoma asmenų, turinčių tam teisę, bet kuriuo jiems reikalingu metu.

Autentiškumas (tapatumas) - informacijos savybė, garantuojanti jos neiškraipymą (tikrumą) informacijos saugojimo, kaupimo, apdorojimo ir perdavimo metu.

Ypatingos svarbos informacinė infrastruktūra - elektroninių ryšių tinklas, informacinė sistema ar jų grupė, kurie patys yra priskirti *ypatingos svarbos infrastruktūrai* arba kurių tinkamas veikimas yra būtina *ypatingos svarbos infrastruktūros* funkcionavimo prielaida.

Ypatingos svarbos infrastruktūra - fiziniai ištekliai, paslaugos, informacinių technologijų infrastruktūra, elektroninių ryšių tinklai ir kitas turtas, kurio sugadinimas ar sunaikinimas sukelia ar gali sukelti didelę žalą asmenų sveikatai, saugumui, visuomenės gerovei ar šalies ūkiui ir veiksmingam (efektyviam) valstybės funkcionavimui (nacionaliniam saugumui).

Valstybinio audito ataskaitos
„Strateginės informacijos sauga“
3 priedas

Valstybiniai auditai, kuriuose nustatytos problemos susijusios su strateginės informacijos sauga

Eil. Nr.	Data	Pavadinimas	Objektas	Tikslai	Subjektai
1.	2006 m.	KAM valdomų kompiuterizuotų finansinių ir kitų informacinių sistemų bendrosios kontrolės vertinimas	KAM valdomos kompiuterizuotos finansinės ir kitos IS	Įvertinti KAM valdomų kompiuterizuotų finansinių ir kitų IS bendrąją kontrolę ir pateikti rekomendacijas	KAM
2.	2006 m.	Valstybinių informacinių sistemų bendroji kontrolė	Valstybinių institucijų informacinių sistemų bendroji kontrolė	1. Siekta įvertinti valstybinių institucijų informacinių sistemų valstybinio lygmens bendrąją kontrolę. 2. Siekta apibendrinti informacinių sistemų bendrosios kontrolės būklę valstybinėse institucijose.	VRM, IVPK ir kitos valstybinės institucijos, kuriose iki 2006 metų rugpjūčio buvo atlikti informacinių sistemų bendrosios kontrolės vertinimai.
3.	2007 m.	Lietuvos Respublikos vidaus reikalų ministerijos informacinių sistemų bendrosios kontrolės vertinimas	Vidaus reikalų ministerijos informacinių sistemų bendroji kontrolė	Įvertinti Vidaus reikalų ministerijos informacinių sistemų bendrąją ir kūrimo kontrolę ir pateikti rekomendacijas.	VRM, Informatikos ir ryšių departamentas prie VRM
4.	2007 m.	Akcinės bendrovės Rytų skirstomųjų tinklų informacinės sistemos bendrosios kontrolės vertinimas	Informacinių sistemų bendrosios kontrolės vertinimas	Įvertinti informacinių sistemų bendrąją kontrolę ir pateikti rekomendacijas	Akcinė bendrovė Rytų skirstomieji tinklai
5.	2007 m.	Valstybinių institucijų informacinių sistemų valdymas elektroninės valdžios kontekste	Valstybės informacinių sistemų bendrosios kontrolės organizavimas	Apibendrinti valstybės informacinių sistemų bendrosios kontrolės būklę atsižvelgiant į el. valdžios kontekstą; Įvertinti valstybės informacinių sistemų kūrimo, steigimo, saugos teisinį reglamentavimą; Įvertinti el. valdžios projektų įgyvendinimo prielaidas ir eigą; Įvertinti 2006 metų valstybės informacinių sistemų bendrosios kontrolės vertinimo valstybinio audito rekomendacijų įgyvendinimą; Pateikti valstybinių auditorių pastebėjimus, išvadas ir rekomendacijas nustatytiems veiklos trūkumams šalinti.	VRM IVPK Valstybinė duomenų apsaugos inspekcija
6.	2008 m.	Europos Sąjungos struktūrinių fondų lėšomis finansuojamų informacinės visuomenės plėtros projektų valdymas	ES struktūrinių fondų lėšomis finansuojamų IVP projektų valdymas	Surinkti, papildyti ir atnaujinti informaciją apie 2004–2006 m. ES struktūrinių fondų lėšomis finansuojamus IVP projektus ir jų valdymą; Įvertinti IVP projektų atrankos ir derinimo procedūrų vykdymą; Įvertinti, kaip vykdoma IVP projektų įgyvendinimo stebėsena; Įvertinti, kaip vykdomas IVP projektų rezultatų vertinimas; Nustatyti problemas, susijusias su ES struktūrinių fondų lėšomis finansuojamų IVP projektų valdymu, ir pateikti rekomendacijas.	IVPK VšĮ Centrinė projektų valdymo agentūra
7.	2008 m.	Saugaus valstybinio duomenų perdavimo tinklo operatoriaus veikla	Saugaus valstybinio duomenų perdavimo tinklo operatoriaus veikla	Įvertinti Saugaus valstybinio duomenų perdavimo tinklo operatoriaus veiklą	VĮ „Infostruktūra“ VRM
8.	2008 m.	Ekstremalių situacijų valdymo organizavimas	Ekstremalių situacijų valdymas	Įvertinti ekstremalių situacijų valdymo organizavimą	VRM Priešgaisrinės apsaugos ir gelbėjimo departamentas prie VRM