KAUNO TECHNOLOGIJOS UNIVERSITETAS
SOCIALINIŲ, HUMANITARINIŲ MOKSLŲ IR MENŲ FAKULTETAS
VIEŠOSIOS POLITIKOS IR ADMINISTRAVIMO INSTITUTAS

Alvydas Murauskas

KIBERNETINIO SAUGUMO UŽTIKRINIMO PRIELAIDOS VIEŠAJAME VALDYME

Magistro darbas

Darbo vadovas
doc. dr. Rasa Šnapštienė

KAUNAS 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS
SOCIALINIŲ, HUMANITARINIŲ MOKSLŲ IR MENŲ FAKULTETAS
VIEŠOSIOS POLITIKOS IR ADMINISTRAVIMO INSTITUTAS

KIBERNETINIO SAUGUMO UŽTIKRINIMO PRIELAIDOS VIEŠAJAME VALDYME

Viešojo administravimo magistro darbas
Studijų programa 621N70001

Darbo vadovas

(parašas)
doc. dr. Rasa Šnapštienė
2015 - 05 - 26

Recenzentas

(parašas)
Prof. Algis Junevičius
2015 - -

Atliko

(parašas)
SMV-3/2 gr. stud.
A.Murauskas
el. paštas:
alvydas1975@gmail.com
2015 - 05 - 26

KAUNAS 2015

PATVIRTINIMAS APIE MAGISTRO BAIGIAMOJO DARBO SAVARANKIŠKUMĄ

Patvirtinu, kad parengtas **magistro darbas**

KIBERNETINIO SAUGUMO UŽTIKRINIMO PRIELAIDOS VIEŠAJAME VALDYME

- atliktas savarankiškai ir jo dalys arba visas darbas nėra nukopijuotas nuo kitų autorių darbų;
- nebuvo pateiktas atsiskaitymui šiame ar kitame KTU fakultete arba kitoje aukštojoje mokykloje;
- pateiktos nuorodos į visus kitų autorių darbus, kurių medžiaga pasinaudota.

_____ _____

Vardas pavardė Parašas

_____

Data

Murauskas, A. *Kibernetinio saugumo užtikrinimo prielaidos viešajame valdyme.* Viešojo administravimo magistro darbas. Studijų programa 621N70001. Vadovas doc. dr. R. Šnapštienė. Kaunas: Kauno technologijos universitetas, Socialinių, humanitarinių mokslų ir menu fakultetas, 2015, 57 p.

SANTRAUKA

Darbe keliamas probleminis klausimas: kokios prielaidos reikalingos užtikrinti kibernetinį saugumą Lietuvos viešajame valdyme? Tikslas – išanalizuoti kibernetinio saugumo užtikrinimo prielaidas viešajame valdyme. Uždaviniai: 1.Teoriniame lygmenyje pagrįsti e-paslaugų plėtrą kaip vieną iš viešojo valdymo modernizavimo prielaidų. 2. Atskleisti kibernetinio saugumo problematiką viešajame valdyme. 3. Įvertinti kibernetinio saugumo užtikrinimą viešajame valdyme. Tyrimo objektas – kibernetinis saugumas viešajame valdyme. Taikyti metodai: mokslinės literatūros bei dokumentų turinio analizė; kokybinių ir kiekybinių duomenų rinkimo metodai. Analizuojami Lietuvos respublikos teisės aktai, reglamentuojantys kibernetinį saugumą; Valstybinio audito ataskaita Valstybės informacinių išteklių valdymas (2013); Valstybinio audito ataskaita Žemės ūkio ministerijos informacinių išteklių valdymas (2013); Valstybinio audito ataskaita Teisingumo ministerijos informacinių išteklių valdymas (2013).

Išvados:

1. Šiuolaikinių viešojo valdymo įstaigų veiklos modernizavimas skatina informacinių technologijų plėtrą, informacijos perkėlimą į elektroninę erdvę. Tai didina viešojo valdymo veiklos kokybę, užtikrina geresnį konkurencingumą bei efektyvumą. Viešajame valdyme elektroninė valdžia yra priemonė įgyvendinti valstybės valdymo reformą. Ji sudaro optimalias prielaidas valdžios struktūrų našumo gerinimui, efektyvaus ir operatyvaus viešosios informacijos teikimui gyventojams bei sprendimų priėmimui.
2. Požiūris į informacijos saugumą iš esmės evoliucionavo – nuo siauro informacijos saugumo supratimo kaip tik grynai technologinės problemos iki plačios informacijos saugumo valdymo suvokties. Išskiriami informacijos saugumo valdymo aspektai: strateginis, žmogiškojo veiksnio ir technologinis.
3. Įvertinus kibernetinio saugumo užtikrinimą viešajame valdyme išryškėjo: Lietuvoje priimtas Kibernetinio saugumo įstatymas yra teigiamas žingsnis reglamentuojant kibernetinį saugumą. Tačiau įstatyme neaptarti institucinės kontrolės bei politikos formavimo kibernetinio saugumo srityje klausimai; pasigendama kibernetinių incidentų valdymo „vieno langelio principu“, nes atskiros institucijos priklauso įvairioms ministerijoms; Valstybės informacinių išteklių valdyme nesuderintos informacinių išteklių strateginės plėtros kryptys, o nustatyti vertinimo kriterijai atskleidžia ne visus informacinių išteklių strateginės plėtros rezultatus.

Murauskas, A. *Assumptions of Cyber Security in Public Management.* Master's Final Thesis in Public administration. Study Programme 621N70001. Supervisor doc. Dr. R. Šnapštienė. Kaunas: Kaunas University of Technology, The Faculty of Social Sciences, Arts and Humanities, 2015, 57 p.

SUMMARY

The problem of the research: What kind of assumptions is necessary for cyber security in public management of Lithuania? The aim of the research is to analyse assumptions of cyber security in public management. The objectives of the research: 1. To substantiate e-services development as one of the preconditions for the modernization of public management in theoretical level. 2. To reveal cyber security issues in public management. 3. To assess cyber security in public management. Research object is cyber security in public management. Research methods: literature and content analysis of documents; qualitative and quantitative data collection methods. There are analysed the legislation of Lithuanian republic on cyber security; Public Audit Report, Management of State Information Resources (2013); Public Audit Report, Management of Information recourses of the Ministry of Agriculture (2013); Public Audit Report, Management of Information recourses of the Ministry of Justice (2013).

Conclusions:

1. The modernization of activity of modern public administration institutions encourages the development of information technologies, information transfer in the electronic environment. This increases the quality of public management activities, ensure better competitiveness and efficiency. E-government in Public management is a tool for the implementation of public administration reform. It creates the optimal conditions to improve the productivity of government structures, efficiency of supply of public information for citizens, and decision-making.
2. The approach to information security basically evolved – from a narrow understanding of information security as a purely technological problem to wide information security management perception. There is distinguished the aspects of information security management: strategic, human factor and technological.
3. After assessment of cyber security in public management, it is clarified: The adopted law of Cyber Security of Lithuania is a positive step in the regulation of cyber security. However, the law doesn't cover the issues of institution control and policy making in the area of cyber-security; there is a lack of cyber incident management by "one-stop shop" principle, because individual institutions belong to different ministries; The directions of strategic development in the State information management don't match, and the established criteria reveal not all results of strategic development of information resources.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

SUTRUMPINIMAI

IT – informacinės technologijos

IS – informacinė sistema

ĮVADAS

Viešasis administravimas yra socialinio valdymo rūšis, siejama su valstybės vykdoma valdžia, kurios pagrindinė užduotis yra įgyvendinti įstatymus bei jų pagrindu priimtus kitus teisės aktus, t.y. įgyvendinti viešąją politiką. Viešasis administravimas yra veikla, kurią atlieka specialus subjektų ratas – viešojo administravimo subjektai, kuriems įgaliojimus suteikia įstatymai ar jų pagrindu priimti kiti teisės aktai. Viešojo administravimo subjektai, vykdydami savo funkcijas atskiras gyvenimo sritis reglamentuojančių normų kontekste, turi diskrecijos teisę, kurią įgyvendindami privalo vadovautis viešaisiais interesais.

Informacinės atviros, išsilavinusios ir besimokančios – visuomenės idėja tapo vienu iš pagrindiniu tiek didelės dalies atskirų pasaulio valstybių, tiek įvairių tarptautinių organizacijų siekių. Ne išimtis ir Europos Sąjunga bei jai priklausanti Lietuva. Viešojo administravimo tobulinimas aktualus Europos Sąjungos ir nacionaliniu lygmeniu. ES lygmeniu EŠ 2020 strategijos įgyvendinimas apima ir viešojo administravimo tobulinimo klausimus, kurių formulavimas ir įgyvendinimas nagrinėjamas konvergencijos bei nacionalinių reformų programose ir jų ataskaitose.

Lietuva, modernizuodama viešąjį sektorių adekvačiai Europos integracijos ir Europos Sąjungos plėtros nuostatomis siekia valstybės valdymo sistemą pertvarkyti remiantis sisteminiu požiūriu ir vadybos pagrindais; unifikuoti centrinės viešojo administravimo sistemos institucinę sąrangą, aiškiai nustatyti kiekvienos viešojo administravimo institucijos kompetencijos sritis, optimizuoti viešojo administravimo institucijų funkcijas ir jų skaičių ir pan.

Viešojo administravimo tobulinimo tikslai, uždaviniai ir priemonės numatyti Lietuvos Respublikos Vyriausybės 2012–2016 metų programoje ir programos įgyvendinimo prioritetinėse priemonėse, Valstybės pažangos strategijoje „Lietuvos pažangos strategija „Lietuva 2030“, 2014–2020 metų Nacionalinės pažangos programoje, Viešojo valdymo tobulinimo 2012–2020 metų programoje, rengiamoje 2014–2020 metų ES struktūrinės paramos veiksmų programoje, kituose strateginiuose dokumentuose.

Vienas iš galimų būdų plėtojant viešojo administravimo paslaugas yra elektroninė valdžia (e-valdžia). Informacini technologijų naudojimas gali tiesiog sumažinti žmogiškųjų išteklių poreikį, taip pat galima lengviau paskatinti piliečius savo žiniomis ir pastangomis prisidėti prie viešųjų sprendimų įgyvendinimo. nes tai yra nauja, įdomu ir modernu. Panaudojant informacinių technologijų priemones visuomenei tampa prieinama informacija apie teisės aktus, mokesčių prievoles, laisvas darbo vietas, nekilnojamojo turto registre esančius duomenis ir t.t. Elektroniniu būdu galima gauti pažymas apie deklaruotą gyvenamąją vietą ar šeimyninę padėtį, deklaruoti ir sumokėti mokesčius. Taigi galima teigti, kad e-valdžia – tai informacinių technologijų taikymas komunikacijai ir vidinei bei išorinei sąveikai su piliečiais, verslu ir kitomis vyriausybės organizacijomis.

E-valdžios taikymas yra neatsiejamas nuo informacijos saugumo, asmens duomenų išsaugojimo užtikrinimo. Šiame darbe informacijos saugumas suprantama kaip informacijos bei sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio pobūdžio poveikio, galinčio sukelti žalą informacijos ar sistemos infrastruktūros savininkams bei vartotojams (Kiškis et al., 2006). Kitas terminas, apibrėžiantis elektroninį saugumą – kibernetinis saugumas. Šie du terminai darbe bus traktuojami kaip sinonimai.

Kibernetinių atakų mastas, dinamika, žala organizacijoms per pastaruosius metus intensyviai auga. Pasikeitė atakos pobūdis: jei anksčiau vyravo atsitiktinės atakos, tai dabar dominuoja tikslinės, nukreiptos į konkrečius asmenis ar grupes, organizacijas. Šiais metais įvykdytos tarptautinės tikslinės kibernetinės atakos: RedOctober, MiniDuke, APT1 ir kt. Kibernetinis nusikalstamumas vis labiau industrializuojamas, didėja finansiniai nuostoliai, patiriami dėl kibernetinių atakų. Ypač padažnėjo informacijos nutekėjimo atvejų. Tai ypač aktualu viešajame sektoriuje.

Tarptautinė bendruomenė vienijasi ir siekia bendradarbiavimo stabdant kibernetinį nusikalstamumą: ATO kibernetiniam saugumui daugiau dėmesio ėmė skirti po plataus masto išpuolių prieš Estijos informacinę struktūrą. 2008 m. Taline buvo įkurtas NATO kibernetinio saugumo centras, kuriam priklauso daugiau kaip dešimt valstybių. Aljanso viduje steigiamos ir kitos struktūros. NATO generalinis sekretorius Japas de Hopas Scheperis kibernetinį saugumą pavadino XXI a. iššūkiu.

Lietuvoje „Nacionalinę informacinės visuomenės plėtros koncepciją“ ir jos pagrindu parengtą „Lietuvos informacinės visuomenės plėtros strateginį planą“ Vyriausybė patvirtino dar 2001 m., o 2005-aisiais atsirado ir bendras šalies informacinės visuomenės plėtros strateginio planavimo dokumentas – „Lietuvos informacinės visuomenės plėtros strategija“. Šiuose dokumentuose sakoma, kad viena iš kertinių priemonių išsikeltam tikslui pasiekti – informacinės technologijos ir vis didėjantis piliečių naudojimasis jomis. Tačiau negalima pamiršti, kad daug kasdienio gyvenimo dalykų perkeliant į virtualią erdvę, vis aktualesnis tampa jos saugumas (kibernetinis saugumas), nes didėja galima žala jo neužtikrinus. 2012 metais birželio 29 d. Vyriausybė priėmė pirmąją nacionalinę elektroninės informacijos saugos, kaip kibernetinio saugumo, plėtros 2011-2019 m. programą.

Elektroninės informacijos sauga yra analizuojama ir moksliniame lygmenyje. Kaip pažymi Schjolberg ir Ghernaouti-Hele (2011), kibernetinis saugumas įvardinamas kaip kertinis akmuo informacinėje visuomenėje. Petrauskas et al. (2006) analizavo tris elektroninės informacijos saugos aspektus: prieinamumą, vientisumą, slaptumą. Štitilis ir Klišauskas (2012) atliko elektroninės informacijos saugos reglamentavimo Lietuvoje ir Rusijoje lyginamąją analizę. Taip pat buvo analizuotas kibernetinio saugumo teisinis reguliavimas ES bei šio teisinio reguliavimo kontekste įvertinta Lietuvos kibernetinio saugumo programa (Štitilis, 2013).

Pastebėta, kad ši aktuali problema reikalauja gilesnės analizės, todėl kyla probleminis klausimas: **kokios prielaidos reikalingos užtikrinti kibernetinį saugumą Lietuvos viešajame valdyme?**

Tikslas – išanalizuoti kibernetinio saugumo užtikrinimo prielaidas viešajame valdyme.

Uždaviniai:

1. Teoriniame lygmenyje pagrįsti e-paslaugų plėtrą kaip vieną iš viešojo valdymo modernizavimo prielaidų.
2. Atskleisti kibernetinio saugumo problematiką viešajame valdyme.
3. Įvertinti kibernetinio saugumo užtikrinimą viešajame valdyme.

Tyrimo objektas – kibernetinis saugumas viešajame valdyme.

Darbe bus taikomi šie **metodai**:

- **mokslinės literatūros bei dokumentų turinio analizė,** kurios tikslas – atskleisti kibernetinio saugumo teisinį reguliavimą ES;
- **kokybinių ir kiekybinių duomenų rinkimo metodai,** kurių tikslas **–** atlikti kibernetinio saugumo viešajame valdyme vertinimą. Bus analizuojami Lietuvos respublikos teisės aktai, reglamentuojantys kibernetinį saugumą; Valstybinio audito ataskaita *Valstybės informacinių išteklių valdymas* (2013); Valstybinio audito ataskaita *Žemės ūkio ministerijos informacinių išteklių valdymas* (2013); Valstybinio audito ataskaita *Teisingumo ministerijos informacinių išteklių valdymas* (2013).

1. E-PASLAUGŲ PLĖTRA KAIP VIENA IŠ VIEŠOJO VALDYMO MODERNIZAVIMO PRIELAIDŲ

Šiame skyriuje bus aptarta e-paslaugų ir viešojo valdymo modernizavimas viešojo valdymo kontekste. Analizuojamas viešojo skaitmenio valdymo modelis, jo elementai. E-valdžia ir e-paslaugos traktuojamos kaip viešojo administravimo tobulinimo prielaidos, kurios yra esminės šiuolaikinės visuomenės ir valstybės modernizavimo grandys. Jos turi įtakos daugeliui politinės, socialinės, ekonominės technologinės raidos ir pažangos procesų rezultatyvumui ir efektyvumui, visuomenės įtraukimui į viešojo valdymo procesus, demokratiniam sprendimui priėmimui.

Tačiau viešojo administravimo sektoriaus skaitmenizavimas yra neatsiejamas nuo duomenų apsaugos, informacijos saugumo valdymo problemų.

1.1. E-paslaugos viešajame valdyme

Sprendžiant visuomenėje ir ekonomikoje kylančias sudėtingas problemas ir siekiant užtikrinti tvarų socialinį ir ekonominį valstybės vystymąsi, tradiciniais laikyti viešojo valdymo modeliai ir metodai tapo mažiau veiksmingi. Kaip pažymi E.Gaulė (2014) viešojo valdymo sistemai svarbu surasti atitinkamus valdymo ir viešojo sektoriaus veiklos organizavimo būdus, kuriuos naudojant būtų sprendžiamos aktualios viešojo valdymo problemos: užtikrintas tvarus vystymasis, viešojo sektoriaus integralumas ir didinimas žmonių pasitikėjimas valdžia.

Naujosios viešosios vadybos teoriniai postulatai susiformavo XX a. paskutiniame dešimtmetyje kaip viešojo valdymo praktikos modernizavimas. Kaip teigia A. Raipa (2011, psl. 168)) „žymiausi Europos ir pasaulio viešojo valdymo teoretikai (Pollitt, Bouckaert, Lane, Osborne, Hood ir kt.) savo darbuose vienaip ar kitaip sutinka, kad daugiausia dėmesio XX a. paskutinio dešimtmečio mokslinėje naujosios viešosios vadybos analizėje buvo skirta naujosios viešosios vadybos teoriniams-intelektualiniams svarstymams siekiant išgryninti naujosios viešosios vadybos logiką, definicijas ir kategorijas konstruojamiems modeliams vertinti, apskritai bendriausios naujosios viešosios vadybos ideologijos realizavimo įvairiose nacionalinėse erdvėse skirtumams pabrėžti“.

Viešojo administravimo literatūroje išskiriami du „idealūs“ viešojo valdymo modeliai: a) tradicinis, racionalios biurokratijos (dar vadinamas Weberio), ir b) naujojo viešojo valdymo (NVV) (Raipa, 2011). Kadangi šie modeliai yra „idealūs“, nė vienoje valstybėje nefunkcionuoja gryna forma, tačiau yra naudingi kaip tyrimo įrankis viešajam valdymui analizuoti ir palyginti. Visose šalyse skirtingomis proporcijomis galima rasti ir vieno, ir kito „idealaus“ modelių bruožų. Viešojo valdymo literatūroje gausu šių modelių pristatymų, palyginimų, kritikos, todėl šiame darbe jie yra aptariami tiek, kiek tai būtina siekiant juos palyginti su IT pagrįsta viešojo valdymo logika.

Interpretuojant P. Dunleavy poziciją, (Dunleavy, Margetts, Bastow, Tinkler, 2006) normatyvine prasme „skaitmeninio valdymo“ požiūris yra pagrįstas tokiomis vertybėmis:

- viešojo sektoriaus misija: viešojo sektoriaus tikslai yra kitokie, negu privačių įmonių, todėl radikalus privačiame sektoriuje taikomų principų diegimas (konkurencija, išlaidų mažinimas ir pan.) nėra optimalus;
- viešojo sektoriaus lygiavertiškumas privačiam – radikali privatizacija ir veiklos subranga nėra naudingi viešojo intereso požiūriu;
- tarpinstitucinis bendradarbiavimas ir veiklos koordinavimas. Kaip atsvara tradicinei viešųjų organizacijų sampratai šiuolaikiniame naujojo viešojo valdymo formavimosi etape, viešosios organizacijos įvardijamos kaip pobiurokratinės, modernios, įvaldžiusios naujus viešojo valdymo principus ir metodus, paremtus tarpsektorine ir tarpšakine įvairių lygių organizacijų tinklaveika, organizacijos, kur dominuojantys tampa naujos vadybinės kultūros ir pokyčių elementai bei formuojami ir įgyvendinami nauji viešojo valdymo demokratizavimo lygmenys (Raipa, 2011).
- įvairių suinteresuotų šalių įtraukimas, sąlygų piliečiams dalyvauti priimant ir įgyvendinant jiems aktualius sprendimus sudarymas.

Vadovaujantis P. Dunleavy ir kolegų (2006) išplėtoto „skaitmeninio valdymo“ požiūriu, galima pateikti esminius viešojo valdymo modelio ypatumus (1 pav.)

1 pav. Viešojo „Skaitmeninio“ valdymo modelis
Sudaryta autoriaus pagal P. Dunleavy (2006)

Informacinės technologijos teikia galimybę peržiūrėti, automatizuoti, optimizuoti vidinius procesus, patobulinti veiklos metodus, o pačią organizacijos veiklą labiau orientuoti į rezultatus, tikslus ar kokybišką paslaugą klientams. Taip pat siekiama jungti atskiras institucijas ar jų padalinius vadovaujantis „valdymo kartu“ ir „darbo tinkle“ logika, naikinti besidubliuojančias funkcijas. Pabrėžiamas dalijimosi instituciniais ištekliais ir duomenų bazėmis elementas, t.y. informacinių sistemų sąveikumas (angl. *interoperability*). Galima sutaupyti ir geriau koordinuoti pastangas, elektroniniams ir elektroniniu parašu pasirašytiems procesams. Ištekliai gali padidėti: IT gali būti išnaudojama tobulinant darbuotojų kvalifikaciją ir didinant produktyvumą, greičiau ir pigiau teikti viešąsias paslaugas.

Informacinės technologijos gali tiesiog sumažinti žmogiškųjų išteklių poreikį, taip pat galima lengviau paskatinti piliečius savo žiniomis ir pastangomis prisidėti prie viešųjų sprendimų įgyvendinimo. „Skaitmeninio valdymo“ taikymas turėtų paskatinti susiformuoti naują administracinę kultūrą, kuri būtų labiau pagrįsta keitimuisi informacija, bendrais veiksmais ir bendra atsakomybe. Siekiama tobulinti visų lygių, rūšių ir sektorių partnerystę, dažniausiai akcentuoja sprendimų priėmimą konsensuso, dialogo, o ne hierarchinio valdymo ir įsakymų ar nurodymų forma.

Išryškėja strateginė informacijos reikšmė, poreikis išnaudoti informaciją kaip vertingą išteklių, kuriantį pridėtinę vertę visų tipų organizacijoms, taip pat siūloma sukurti specifines pareigybes, strategijas, priemones šiam ištekliui valdyti ir vertei didinti. Minėta apibrėžtis artima viešojo sektoriaus informacijos išteklių sampratai – pabrėžiama, jog valdant informaciją reikia atsižvelgti į tokias organizacijos išteklių rūšis: informacijos išteklius (duomenų, informacijos), technologinius išteklius (programinės ir techninės įrangos, programinės įrangos sistemų, technologijų infrastruktūros, telekomunikacijų), žmogiškuosius išteklius (įvairių lygių darbuotojų ir vadybininkų, kitų išorinių auditorijų) (Atkočiūnienė, Janiūnienė, 2013).

Apibendrinant galima teigti, kad vienas iš esminių „skaitmeninio valdymo“ modelio ypatumų – tai aktyvi ir vadovo atsakomybe pagrįsta lyderystė, strateginis valdymas. Nebijoma naujovių ir eksperimentų. Struktūros prasme informacinės technologijos teikia galimybę organizacijoms tapti „plokštesnėms“, taigi griežtos vidinės hierarchijos ir atsakomybės pasidalijimas tampa mažiau reikalingi. Tokios organizacijos veikla yra gerokai skaidresnė, o pati struktūra tampa daug atviresnė ir socialiai atsakingesnė tiek bendrąja, tiek specifine (pačios organizacijos lygmeniu) prasmėmis.

Viešojo administravimo tobulinimas – esminė šiuolaikinės visuomenės ir valstybės modernizavimo grandis, kuri turi įtakos daugeliui politinės, socialinės, ekonominės technologinės raidos ir pažangos procesų rezultatyvumui ir efektyvumui. Kaip pažymi I. Damirova ir R. Šnapštienė (2005), viešojo administravimo tobulinimo darbų bei įgyvendintų priemonių pagrindinis tikslas yra modernizuoti viešąjį sektorių taip, kad jis atitiktų pažangių užsienio šalių normas, standartus ir tradicijas, atitiktų Europos šalių viešojo administravimo patikimumo lygį.

XX a. antroje pusėje spartus informacinių ir telekomunikacinių technologijų (ITT) vystymasis, sudarė prielaidas modernizuoti viešojo administravimo sistemą. Jau nuo pat pirmųjų šių technologijų panaudojimo viešojo administravimo subjektų veikloje dienų, buvo pradėta kalbėti, kad ITT gali padėti užmegzti glaudesnį ryšį su gyventojais, pagerinti viešųjų paslaugų teikimą, bei kitų funkcijų atlikimą. Šios idėjos gavo naują impulsą, kai XX a. dešimtame dešimtmetyje sparčiai pradėjo augti interneto vartotojų skaičius. Šį faktorių greitai įvertino verslo pasaulis, kuriam veiklos vystymas virtualioje erdvėje žadėjo nemažą pelną. Šių tendencijų veikiamos daugelis valstybių iškėlė sau tikslą bent dalį administracijos paslaugų teikti per internetą. JAV buvo pirmoji, kada JAV viceprezidentas Al Gore pažadėjo visiems piliečiams prieigą prie vyriausybės per internetą, sujungiant visas mokyklas, ligonines, bibliotekas ir kt.

T.Limba (2007) įvardina elektroninės valdžios kūrimo motyvus:

- Valdžios struktūrų darbo našumo gerinimas pasitelkiant informacines technologijas;
- „Gero valdymo“ stiprinimas;
- Efektyvus viešosios informacijos teikimas gyventojams;
- Viešųjų paslaugų teikimo gyventojams tobulinimas;
- Visapusiškas visuomenės skaitmeninis integravimas.

Dažnai e-valdžia tapatinama su elektroninių viešųjų paslaugų teikimu. Tačiau iš e-valdžios paprastai tikimasi daugiau, negu nusistovėjusių procesų perkėlimas į elektroninę erdvę, pavyzdžiui, „e-valdžia – tai informacinės technologijos, ypač interneto, naudojimas siekiant geriau įgyvendinti viešąją valdžią. Neretai tikimasi, kad informacinės technologijos padės pakeisti tradicines biurokratines struktūras ir padaryti valdymą šiuolaikiškesnį: „e-valdžia – tai viešojo administravimo modernizavimas pasitelkiant IT“. IT turi prisidėti prie organizacinės kaitos ir paskatinti atsirasti naujiems įgūdžiams, kurie pagerintų viešąsias paslaugas, demokratinius procesus ir viešąją politiką (Europos Komisija, 2003).

Pasitelkusi informacines technologijas, e-valdžia padidins vyriausybės veiklos našumą, efektyvumą ir atskaitomybę, didins vykdomosios valdžios sprendimų priėmimo skaidrumą, užtikrins e-paslaugų prieigą; kokybiškiau ir efektyviau teiks visuomenei, verslo subjektams ir institucijoms viešąsias paslaugas ir informaciją.

Kaip teigia J. Buškevičiūtė ir A. Raipa (2011), sprendimų priėmimo kokybei labai svarbus informacijos valdymas, jos naudojimas ir tinkamas interpretavimas. Tik turint pakankamai informacijos ir mokant ją atitinkamai panaudoti galima pasiekti laukiamų rezultatų. Informacijos srautų valdymas, jų panaudojimas yra svarbiausias efektyvių sprendimų rengimo ir įgyvendinimo veiksnys. Sprendimus priimančios struktūros turi galimybes disponuoti (kartais manipuliuoti) informacijos srautais, einančiais iš įvairių valdymo lygių ir struktūrų, bei subjektų ateinančia informacija.

Apie elektroninę vadžią pradėta diskutuoti palyginti neseniai, nors informacinės technologijos viešosiose organizacijose taikomos jau keletą dešimtmečių. Informacinės technologijos turi potencialą pakeisti iki šiol objektyviomis ir nekintamomis laikytas viešojo sektoriaus organizacijų savybes: laiką, vietą, informacijos formą. Taikant informacines technologijas visos „objektyviosios“ savybės gali pasikeisti. Atsiranda galimybė nebenaudoti popieriuje išspausdintų dokumentų informacijai rinkti, kaupti ir apdoroti – techniškai įmanoma visa reikalinga informacija disponuoti skaitmeniniu būdu. Dokumento originalumu tampa ne įprastas popierinis dokumentas, bet skaitmeninis dokumentas, pasirašytas elektroniniu parašu. Tai leidžia pakeisti valdžios „vietą“, nes nyksta fizinio pastato svarba: ilgainiui „valdžios institucijos gali virsti jų interneto svetainėmis“ (Barcevičius, 2008). Valdymas tampa labiau depersonalizuotas – su valstybės tarnautojais, piliečiai ir verslininkai gali susisiekti internetu: gauti ir teikti reikalingą informaciją, gauti viešosios valdžios paslaugas, atlikti reikalingas operacijas. Vyksta ir „paslaugų suliejimas“, kai reikalingas paslaugas galima gauti vieno internetinio „langelio“ principu, nepaisant žinybinio atsakomybės pasidalijimo. Todėl informacinės technologijos turi įtakos ir „laikui“ – viešųjų organizacijų darbo ritmui: iš esmės netenka prasmės priėmimo valandos, padidėja sąveikos su piliečiais greitis. Organizacijos gali tapti virtualios ne tik piliečių požiūriu: atsiranda galimybė lanksčiau reglamentuoti darbuotojų darbo valandas, nyksta ne tik išorinės, bet ir vidinės organizacijų „sienos“, mažiau reikšmės teikiama hierarchiniams santykiams, skyriams ir departamentams. Biurokratijos terminą keičia „adhokratija“, „valdymas kartu“ (angl. *joyned-up government*), visuminis požiūris į valdymą (angl. *whole of the government*). Fizinės organizacijų „sienos“ ir vidinis tapatumas tampa mažiau svarbūs – vis didesnę reikšmę įgyja tarpinstituciniai tinklai, kuriuose organizacija arba jos padaliniai dalyvauja (Barcevičius, 2008).

Taigi modernizuojant viešąjį valdymą, sprendimų priėmimas vis dažniau suvokiamas kaip kompleksinė sąvoka, apimanti tokius reiškinius, kaip piliečių dalyvavimas, informacijos srautų valdymas, visuotinės kokybės vadybos metodų taikymas, viešųjų projektų ir programų rengimas, IT taikymas viešose organizacijose ir pan.

Mokslinėje literatūroje, europiniuose ir nacionaliniuose dokumentuose sutinkama įvairų e-valdžios apibrėžimų. Paprasčiausias e-valdžios apibrėžimas teigia, jog ši valdžia yra informacinių technologijų taikymas įgyvendinant viešosios valdžios funkcijas. Kiek platesnis požiūris: e-valdžia – tai informacinių technologijų taikymas komunikacijai ir vidinei bei išorinei sąveikai su piliečiais, verslu ir kitomis vyriausybės organizacijomis (Elektroninės valdžios Lietuvoje būklė ir perspektyvos, 2006). Elektroninė valdžia – tai informacinių ir kompiuterinių technologijų taikymas viešojo sektoriaus veikloje tam, kad pasiekti norimų organizacinių pokyčių, suteikti vartotojams naujų įgūdžių, kurie leistų pagerinti teikiamų viešųjų paslaugų kokybę, sustiprintų valstybėje vykstančius demokratinius procesus ir padidintų piliečių palaikymą valstybės vykdomai politikai (Europos Komisija, 2003). E-valdžią galima apibrėžti kaip informacinių ir komunikacinių technologijų taikymą viešojo sektoriaus institucijose,

siekiant sukurti geresnį valstybės valdymo modelį. Ji suvokiama kaip valstybinės valdžios tąsa elektroninėje erdvėje, pasireiškianti kaip valstybės funkcijų realizavimas, organizacinių pokyčių tobulinimas pasitelkiant informacines technologijas (Limba, 2007).

Apibendrinant galima teigti, kad e-valdžia sudaro optimalias prielaidas valdžios struktūrų našumo gerinimui, efektyvaus viešosios informacijos teikimui gyventojams bei jo tobulinimui, visapusiškam visuomenės skaitmeniniam integravimui. E-valdžia yra susijusi su politika, vartotojais, administravimu. E-valdžios plėtrą sąlygoja viešojo administravimo procesų atnaujinimas, reorganizacija, darbuotojai, finansavimas, skatinimas bei informaciniai sprendimai. Tai valdžios priemonė, palengvinanti viešojo sektoriaus institucijų bendradarbiavimą, sprendimų priėmimą, viešųjų paslaugų teikimą ir jų prieinamumą, panaudojant išmaniųjų technologijų teikiamas galimybes.

1.2. Viešųjų paslaugų kokybės ir skaitmeninių technologijų plėtra

Viešojo sektoriaus prieinamumas Lietuvoje pradėjo plėtotis 2000 metais, kai tuometinis Lietuvos ministras pirmininkas A. Kubilius, atsižvelgdamas į didėjančią informacinių technologijų įtaką pasaulio ūkiui, visuomenės gyvenimui ir daugelio valstybių pastangas jas taikyti valstybės valdyme, kad valdžia priartėtų prie piliečių, jos veikla būtų skaidresnė ir atskaitingesnė, potvarkiu Nr. 164 sudarė darbo grupę Elektroninės vyriausybės (e-vyriausybės) koncepcijai parengti. 2002 m. gruodžio mėn. 31 d. nutarimu Nr. 2115 Lietuvos Respublikos Vyriausybė patvirtino „Elektroninės valdžios koncepciją". Koncepcijoje buvo išdėstytas požiūris į elektroninės valdžios reiškinius Lietuvoje. Joje įtvirtintas siekis pnaudojant skaitmenines technologijas pagerinti viešųjų paslaugų teikimą valstybės ir savivaldybių institucijoms ir įstaigoms, Lietuvos Respublikos gyventojams, bei verslo subjektams.

Šioje koncepcijoje pažymima, kad jos ribose sąvoka "viešosios paslaugos" yra vartojama plačiąja prasme ir apima visą gyventojų ar verslo subjektų bendravimą (pvz. paklausimas ir atsakymas į paklausimą, įvairių dokumentų pildymas ir pateikimas, atsiskaitymas ir kt.). Šios paslaugos turi būti teikiamos nuotoliniu būtu, t.y. tokiomis priemonėmis, kurios leistų bendrauti, paklausti ir gauti viešąją paslaugą be tiesioginio ryšio tarp viešosios paslaugos teikėjo ir gavėjo. Tokiomis priemonėmis yra laikomos skaitmeninės technologijos, kaip internetas, mobilieji telefonai ir kt.

1 lentelėje pateikiami viešųjų paslaugų perkėlimo į internetą brandos lygiai.

Viešųjų paslaugų perkėlimo į internetą brandos lygiai

1 lentelė

Lygis	Viešųjų paslaugų apibūdinimas
Pirmasis lygis	Informacinio pobūdžio viešosios paslaugos. Institucija pateikia viešąją informaciją internetu.
Antrasis lygis	Dalinė transakcija . Institucija pateikia vartotojui savo tinklalapiuose iš dalies automatizuotas formas ir anketas, kurias užpildęs ir išspausdinęs vartotojas gali jomis naudotis (pvz., pateikti institucijai duomenis).
Trečiasis lygis	Dalinis interaktyvumas. Vartotojo tapatybė nustatoma sistemoje. Vartotojas gali pateikti užklausas ir institucija į elektroninę užklausą atsako. Tačiau viešoji paslauga (pvz., pažyma) pristatoma neelektronine forma.
Ketvirtasis lygis	Visiškas interaktyvumas. Baigtas e-valdžios projektas. Vartotojas elektroniniais kanalais pateikia užklausą ir gauna galiojančią elektroninę viešąją paslaugą.

Taigi pirmasis lygis numato tokį vartotojo ir valstybės institucijos ryšį: institucija internete pateikia vartotojui informaciją, o vartotojas turi galimybę ją gauti, naudodamas šiuolaikines informacines technologijas. Antrasis lygis suteikia vartotojui platesnių galimybių: vartotojas gali internetu parsisiųsti reikalingą elektroninę formą ir ją užpildyti, tačiau pateikti ją gali tik tradiciniais būdais (pvz., asmeniškai, paštu arba faksu). Trečiasis lygis suteikia galimybę ne tik atsisiųsti elektroninę dokumento formą, bet ir užpildytą formą internetu pateikti institucijai. O ketvirtasis lygis sudaro galimybę ne tik elektroniniu būdu vykdyti procedūras, bet ir gauti paslaugą (pvz., sprendimą, pažymą, apmokėjimą).

Šioje koncepcijoje buvo numatyta, kad iki 2005 m. visos viešosios paslaugos, kurias administruoja institucijos, iki trečiojo lygio turės būti perkeltos į internetą ar teikiamos kitais nuotoliniais būdais (išskyrus viešąsias paslaugas, kurios negali būti teikiamos nuotoliniu būdu, pavyzdžiui, viešosios paslaugos, kurias teikiant privalo dalyvauti pats valstybės tarnautojas). Ši sąlyga dar bėra įvykdyta.

Elektroninės valdžios koncepcijos tikslas – didinti vykdomosios valdžios sprendimų priėmimo skaidrumą, kokybiškiau ir efektyviau teikti visuomenei, verslo subjektams ir institucijoms viešąsias paslaugas ir informaciją, tam panaudojant informacinių technologijų teikiamas galimybes. Elektroninės valdžios koncepcijos įgyvendinimo priemonių plano projekte numatomos priemonės, kurios leis tobulinti viešojo administravimo sektorių, skatinti ir plėtoti organizacinių priemonių diegimą, kurti saugų valstybės institucijų tinklą, sukurti fizinių ir juridinių asmenų identifikavimo sistemą valstybės informacinėse sistemose ir panaudojant skaitmenines technologijas teikti viešąsias paslaugas.

Elektroninė viešoji paslauga — tai teisės aktais reglamentuojama viešojo administravimo subjektų veikla, skirta teisės subjektams už užmokestį arba nemokamai, padėti įgyvendinti jų teises bei įvykdyti pareigas, nuotoliniu būdu, naudojant informacines ir telekomunikacines technologijas, jiems teikiant ir iš jų priimant duomenis, informaciją bei dokumentus.

Informacinės visuomenės plėtros komiteto (IVPK) prie Lietuvos Respublikos Vyriausybės užsakymu sukurtuose elektroninės valdžios vartuose (juos galima aplankyti adresais http://www.epaslaugos.lt, http://www.govonline.lt arba http://www.evaldzia.lt) yra siūlomos viešosios paslaugos, kurios čia įvardijamos, kaip teisės aktais nustatyta duomenų, informacijos bei dokumentų teikimo ar gavimo tvarka, kurios procedūros atliekamos asmens buvimo vietoje bei jo pageidavimu, skaitmeniniu pavidalu, nuotoliniu būdu per internetą ar (ir) kitomis telekomunikacijų priemonėmis ir apima visą gyventojo ar verslo subjekto bendravimą su viešojo administravimo subjektais.

Svetainėje *www.el.valdžia.lt* nurodoma, kad naudojantis šiais „elektroniniais vartais“ galima pasiekti 421 viešąją paslaugą. Kai kuriose šalyse (Estijoje, Šveicarijoje, Ispanijoje) netgi balsuoti jau galima internetu. Vyksta ir paprastam piliečiui mažiau pastebimi pokyčiai: viešojo valdymo institucijos skaitmenizuoja vidinius veiklos procesus, naudoja IT keistis duomenimis, veiksmams geriau koordinuoti ir taip toliau.

Už valstybės politikos formavimą viešojo administravimo srityje, jos įgyvendinimo organizavimą, koordinavimą ir kontroliavimą atsakinga LR vidaus reikalų ministerija, kuri vykdydama šias funkcijas bendradarbiauja su LR Vyriausybės kanceliarija.

Viešojo sektoriaus prieinamumas Lietuvoje didinamas diegiant **įvairias elektronines paslaugas.** 2007–2013 m. EŠ struktūrinės paramos laikotarpiu pagal prioritetą „Informacinė visuomenė visiems“ daugiausia lėšų skiriama būtent viešųjų elektroninių paslaugų kūrimui. 2010 m. buvo patvirtintas Viešųjų paslaugų perkėlimo į elektroninę erdvę veiksmų iki 2012 metų planas, kuris užtikrino geresnį viešųjų paslaugų prieinamumą. Pavyzdžiui, nuo 2010 m. vairuotojai elektroniniu būdu gali gauti ir keisti vairuotojo pažymėjimą, pranešti apie prarastą pažymėjimą arba gauti informaciją apie laikytus egzaminus. Tais pačiais metais buvo įgyvendintas projektas „E-policija“, kuris leidžia pateikti pranešimus policijai internetu, gauti informaciją apie nusikaltimus ir eismo įvykius ŠMŠ ir MMŠ žinutėmis. 2010 m. buvo pradėta vykdyti „E-Seimo“ iniciatyva, kuria siekiama didinant piliečių informuotumą apie Seimo vykdomą veiklą, sudaryti galimybes kreiptis į šią instituciją el. Būdu ir dalyvauti teisėkūros procesuose (Nacionalinė reformų darbotvarkė, 2013).

Vykdant įvairias iniciatyvas, pagrindinių viešųjų paslaugų perkėlimo į elektroninę terpę lygis 2012 m. Lietuvoje pasiekė 87 proc. (2011 m. – 81,5 proc.). Tačiau verslui skirtos paslaugos yra perkeliamos sparčiau nei skirtos gyventojams: verslui skirtų paslaugų perkėlimo lygis 2012 m. siekė 98 proc., o gyventojams – 79 proc. Remiantis Lietuvos statistikos departamento duomenimis, 2012 m. pradžioje 59,6 proc. įstaigų teikė galimybę parsisiųsti įvairias formas, 15,7 proc. – grąžinti jas užpildytas. 18,4

proc. įstaigų nurodė, kad teikia galimybę atlikti administracines procedūras elektroniniu būdu, t. y. be papildomų popierinių procedūrų. 10,2 proc. įstaigų automatiškai (nereikalaudamos atskiro prašymo) teikė tam tikras socialinio ar ekonominio pobūdžio paslaugas ir naudojo buvusią vartotojo registraciją ir duomenis apie vartotoją (Informacinės technologijos Lietuvoje, 2012 m. LR Statistikos departamentas).

Taip pat Lietuvoje vykdomos viešojo sektoriaus veiklos skaidrinimo iniciatyvos, kurios **didina informacijos prieinamumą**. Pavyzdžiui, pradėjus skelbti valstybės ir savivaldybių biudžeto **suvestines interneto svetainėse**, buvo sudaryta galimybė (prieš Seimui priimant sprendimą dėl kitiems metams skiriamų asignavimų) visuomenei susipažinti su įstaigų veiklos rezultatai. Ši iniciatyva didina viešojo sektoriaus atskaitomybę piliečiams. Tuo tarpu Ūkio ministerija pradėjo **atvirų duomenų iniciatyvą,** kurios dėka pradeda atsirasti informacinių rinkmenų puslapiai kaip http://www.atviriduomenys.lt/. Lietuvoje įsteigtos mobiliųjų aplikacijų laboratorijos gali būti puikia vieta „įdarbinti“ atvertus duomenis ir kurti modernias mobilias aplikacijas. 2012 m. pradžioje 82,7 proc. valstybės ir savivaldybių institucijų ir įstaigų teikė pirmojo lygio elektronines paslaugas internetu, t. y. informaciją apie įstaigų vykdomas funkcijas ir teikiamas paslaugas buvo galima buvo rasti jų interneto svetainėse. Tačiau 2012 m. patvirtintoje Viešojo valdymo tobulinimo 2012-2020 m. programoje numatyta, kad viešojo valdymo institucijų turimos informacijos apimtis išlieka neaiški, o skelbtino visuomenei informacijos turinio ir masto yra neįmanoma nustatyti.

Analizuojant teikiamas viešąsias paslaugas gyventojams galima teigti, kad šiuo metu Lietoje teikiamos šios viešosios paslaugos gyventojams:

- Pajamų deklaravimas;
- Laisvų darbo vietų (iš jų ir valstybės tarnyboje) paieška;
- Socialinės išmokos ir kompensacijos (bedarbio pašalpos, kompensacijos už vaistus, stipendijos, pašalpos daugiavaikėms šeimoms);
- Asmens dokumentai (pasai, asmens tapatybės kortelės, vairuotojų pažymėjimai, autorių teisių apsauga);
- Transporto priemonių registravimas;
- Leidimai statyti pastatus;
- Pranešimai policijai;
- Leidinių, publikacijų paieška viešosiose bibliotekose;
- Gimimo ir mirties liudijimai;
- Gyvenamosios vietos deklaracija;
- Interaktyvios gydytojų konsultacijų ir registracija poliklinikose;
- Paraiškos (mokytis aukštojoje mokykloje, kelti kvalifikaciją).

Verslo subjektams teikiamos šios viešosios paslaugos:

- Įmonių mokesčiai;
- Pridėtinės vertės mokestis (PVM);
- Naujų įmonių registravimas;
- Duomenų teikimas Statistikos departamentui prie Lietuvos Respublikos Vyriausybės;
- Viešieji pirkimai;
- Socialinės išmokos darbuotojams;
- Muitinės deklaracijos;
- Leidimai, kuriuos reikia derinti su aplinkos apsaugos tarnybomis.

Apibendrinant galima teigti, kad e-valdžios įgyvendinimas padidina paslaugų, teikiamų internetu, poreikį. Viešųjų paslaugų teikimas elektroniniu būdu sudaro sąlygas tvarkyti reikalus su viešojo administravimo institucijomis patogesnėse vietose, patogiu metu bei gauti paslaugą greičiau negu kitais būdais. Skaidresnis valstybės valdymas, valstybės tarnautojų asmeninė atsakomybė, aiški atskaitomybės sistema, skaidrūs sprendimų priėmimo mechanizmai – tai tik keletas tiesiogiai su valdymu susijusios naudos aspektų. Taigi vienas iš galimų būdų plėtojant viešojo administravimo paslaugas yra elektroninė valdžia, nes informacinių technologijų naudojimas yra nauja, modernu ir prieinama daugumai piliečių, padidina vyriausybės veiklos našumą, efektyvumą, skaidrumą ir atskaitomybę.

Informacinių technologijų plėtra, informacijos perkėlimas į elektroninę erdvę didina informacinių procesų ir veiklos kokybę, užtikrina geresnį konkurencingumą bei efektyvumą. Tik turint pakankamai informacijos ir mokant ją atitinkamai panaudoti galima pasiekti laukiamų rezultatų. Informacijos srautų valdymas, jų panaudojimas yra svarbiausias efektyvių sprendimų rengimo ir įgyvendinimo veiksnys. Tačiau tai sukelia ir neigiamas pasekmes, tokias kaip svarbios elektroninės informacijos praradimas ar net skatina elektroninį nusikalstamumą. Taigi e-valdžios taikymas gali būti pažeidžiamas, todėl jis yra neatsiejamas nuo informacijos saugumo, asmens duomenų išsaugojimo užtikrinimo.

Kasdien vis labiau ryškėja trūkumai tarp žmonių, kurie moka naudotis kompiuteriais ir interneto teikiamomis galimybėmis, bei tų, kuriems šios sritys vis dar yra nežinomos. Taip pat e-valdžios plėtra kelia potencialią grėsmę piliečių privatumui. Didėjant valdžios ir piliečių sąveikai elektroninėje erdvėje, valdžia kaupia vis daugiau asmeninės informacijos. Blogiausiu įvykių sekos atveju, tokia sistema galėtų tapti totalitarinės valstybės įrankiu. Informacijos saugumo aktualumas išryškėjo atsiradus poreikiui saugoti, perduoti ir kitaip tvarkyti informaciją. Greta e-valdžios turi būti sukurta sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio pobūdžio poveikio, galinčio sukelti žalą informacijos ar sistemos infrastruktūros savininkams bei vartotojams.

Informacijos saugumas, jos užtikrinimas viešajame valdyme – labai svarbi ir specifinė veiklos rūšis, kuri reikalauja nuoseklios ir detalios analizės. Tam bus skirta antroji darbo dalis.

2. KIBERNETINIS SAUGUMAS VIEŠAJAME VALDYME

Skyriuje aptariami kibernetinio saugumo viešajame valdyme klausimai. Analizuojami penki informacijos saugumo valdymo raidos etapai, išryškinant penktąją – kibernetinio saugumo *(Cyber Security*) bangą. Pateikiama kibernetinio saugumo samprata ir jos užtikrinimo ciklas ir pagrindiniai veiksniai: žmogiškasis, organizacijos, technologinis. Trumpai apibūdinami kibernetiniai incidentai, kurių sparčiai daugėja. Kibernetinė ataka – informacinių sistemų, jose tvarkomos elektroninės informacijos puolimas, panaudojant informacines sistemas ar kitas informacinių technologijų priemones, siekiant sutrikdyti informacinių sistemų ir šias sistemas naudojančių organizacijų veiklą. Aptariamas kibernetinio saugumo teisinis reguliavimas Europos Sąjungoje, atliekama Anglijos, Vokietijos, Prancūzijos valstybių patirtis kibernetinio saugumo užtikrinimo srityje.

2.1 Informacijos saugumo valdymo genezė

Kaip teigia Jastiuginas (2011, psl. 9), *informacijos saugumo valdymo* sąvokos apibrėžimą pirmiausia komplikuoja *informacijos saugumo* apibrėžtis, todėl svarbu nuosekliai aptarti *informacijos saugumo, informacijos saugumo valdymo,* kitas susijusias sąvokas, jų genezę bei tarpusavio ryšius, o *informacijos saugumo valdymo koncepciją* suformuluoti kaip holistinį požiūrį į informacijos saugumo valdymą.

Dauguma *informacijos saugumo* apibrėžimų remiasi D. B. Parker apibrėžtais informacijos saugumo tikslais. Anot Parker, Donn (1981), *informacijos saugumo* tikslas – užtikrinti informacijos *konfidencialumą*, *vientisumą* ir *prieinamumą*. *Konfidencialumas* suprantamas kaip informacijos slaptumą, t. y. informacija turi būti prieinama tik tiems, kam ji skirta; *vientisumas* apima pradinės informacijos tikrumą, patikimumą ir autentiškumą, t. y. informacija turi būti apsaugota nuo klaidingo ar nesankcionuoto pakeitimo; *prieinamumas* – užtikrinta galimybė pasinaudoti informacija, t. y. sankcionuoti vartotojai turi turėti galimybę pasiekti informaciją, kai jos jiems reikia (Parker, Donn, 1981).

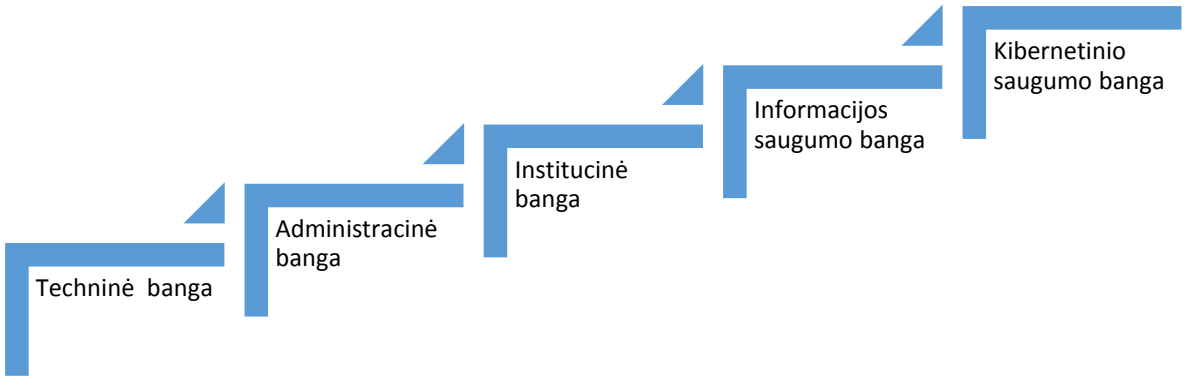
Informacijos saugumo srityje vartojami įvairūs terminai: *informacijos, duomenų, kompiuterių, ryšių tinklų, informacijos technologijų, informacinių sistemų saugumas (apsauga),* ir nors šie terminai skiriasi savo objektu ir turiniu, literatūroje dažna sinonimiška jų vartosena. *Informacinių technologijų saugumas* apima daugiau technologinius aspektus, o *informacinių sistemų saugumas* – dar ir žmogiškąjį veiksnį (Mikalauskienė, Brazaitis, 2010).

Lietuvoje nėra griežtai nusistovėjęs šiame kontekste anglų kalboje vartojamo termino *security* vertimas – *saugumas, sauga, apsauga.* Šiuo metu terminas *apsauga* dažniausiai pasitaiko asmens duomenų teisinės apsaugos, privatumo kontekste; *sauga* – valstybės registrų ir informacinių sistemų

kontekste (Valstybės registrų įstatymas, 2009), *saugumas* vartojamas plačiausiai, kaip apimantis visus išvardytus aspektus, todėl *informacijos saugumo* sąvoka labiausiai tinka siekiant atskleisti įvairialypį informacijos saugumo valdymo kontekstą.

Vertinant *informacijos saugumo* sąvokos genezę, galima teigti, kad požiūris į informacijos saugumą nuo pirmųjų kompiuterių pasirodymo iki šių dienų iš esmės evoliucionavo – nuo siauro informacijos saugumo supratimo kaip tik grynai technologinės problemos iki plačios informacijos saugumo valdymo suvokties.

Šiuos organizacijų lygmens pokyčius detaliai analizavo Basie von Solms (2006). Autorius išskyrė penkias saugumo genezės bangas (2 pav).



2 pav. Informacijos saugumo sąvokos genezė

Sudaryta autoriaus pagal Von Solms, 2006

Pirmoji banga, trukusi iki devintojo dešimtmečio, charakterizuojama kaip **technologinė banga** (*Technical Wave*) – informacijos saugumo užtikrinimas buvo suprantamas kaip technologijų problema, kuria rūpinosi vien techninis personalas. **Antroji banga** pasižymėjo organizacijų vadovybės įtraukimu į saugumo užtikrinimo procesus, buvo pradėti formalizuoti saugumo tikslai ir uždaviniai, kuriuos tvirtindavo vadovybė, kartu įpareigodama atsakingus už saugumą pareigūnus atsiskaityti apie situaciją ir pažangą užtikrinant saugumą organizacijoje. Ši banga buvo pavadinta **administracine banga** (*Management Wave*). Ji truko maždaug iki dešimtojo dešimtmečio vidurinio. **Trečiosios – institucinės bangos** *(Institutionalization Wave)* formavimąsi lėmė glaudesnis organizacijų vadovybės įsitraukimas sprendžiant saugumo problemas. Tai leido iš esmės pareginti saugumo situaciją ir nuolat įtraukti saugumo klausimus į kasdieninę organizacijos veiklą. Organizacijos pradėjo lyginti savo saugumo lygį su kitomis, taikyti gerosios praktikos pavyzdžius ir standartus, o pripažinus žmogiškojo veiksnio įtaką saugumui, pradėtas skatinti saugumo kultūros ugdymas. **Ketvirtoji – informacijos saugumo valdymo** *(Information Security Governance)* banga pradėjo formuotis po 2000 metų. Didėjantis organizacijų poreikis vertinti ir tarpusavyje lyginti informacijos saugumo situaciją padėjo formuotis praktikai plačiau taikyti informacijos saugumo valdymo standartus, pvz., ISO 27000 standartų grupė), informacinių

technologijų valdymo metodikas, pvz., Cobit, ITIL.Šie dokumentai nustato, kad organizacijos turi gebėti valdyti rizikas, susijusias su tinkamu informacijos technologijų veikimu, visą jų gyvavimo ciklą, o organizacijos vadovybė yra tiesiog atsakinga už rizikų valdymo sistemos ir atitinkamų kontrolės priemonių diegimą, nuolatinį saugos kultūros skatinimą organizacijoje. Jastiuginas (2011) pažymi, kad prie glaudaus valdymo funkcijų integravimo į informacijos saugumo valdymo sąvoką daug prisidėjo informacijos saugumo valdymo reikalavimų įteisinimas atskirų šalių teisės aktais, kurie įtvirtino privalomą saugos standartais ir metodikomis grindžiamų informacijos saugumo valdymo priemonių taikymą bei nustatė asmeninę organizacijos vadovų atsakomybę, pavyzdžiui, Didžiosios Britanijos ir Švedijos sprendimai taikyti ISO 27000 informacijos saugumo valdymo standartus viešajame sektoriuje (Cyber Security Strategy of the United Kingdom (2009), JAV patvirtintas SOX (2002), kuris įtvirtino reikalavimus privačiam sektoriui, ir FISMA (2002), kuris apibrėžė privalomus informacijos saugumo valdymo įpareigojimus visam JAV viešajam sektoriui. Saugumo valdymo reikalavimai ilgainiui buvo nustatyti ir specifinėms verslo bei veiklos šakoms: medicininę informaciją tvarkančioms organizacijoms – Health Insurance Portability and Accountability Act (HIPAA, 1996), finansinę informaciją – Payment Card Industry Data Security Standard (PSI, 2008), kurie dėl savo universalumo taikomi kaip saugumo valdymo metodikos ir kitose srityse. **Penktąją – kibernetinio saugumo** *(Cyber Security*) **bangą.** Prie šios bangos susiformavimo prisidėjo ir besikeičiantis rizikos šaltinis; autoriaus teigimu, vis didesnę grėsmę pradeda kelti ne pakankamai gerai apsaugotais organizacijos ištekliais bandantys neteisėtai pasinaudoti asmenys, o paprasti, „naivūs“ vartotojai, kurie kartu yra ir organizacijų elektroninių paslaugų klientai, ar darbuotojai, kurie dirba iš įvairiausių nutolusių kompiuterių, tačiau skiria nepakankamai dėmesio savo asmeninių kompiuterių saugumui ir taip tampa grėsme organizacijų informaciniams ištekliams. Taigi kibernetinio saugumo banga pasižymi dėmesiu ir organizacijos išorinės aplinkos poveikiui (Von Solms, 2006).

Taigi elektroninės erdvės globalumas sukūrė beprecedentes sąlygas daryti nusikaltimus iš bet kurio pasaulio taško, kuriame yra internetas. Todėl labai svarbu apsisaugoti nuo elektroninių nusikaltimų, vykdomų pasitelkiant internetą. Kibernetinis saugumas tampa vienu iš pagrindinių tikslų, turint omenyje, kad grėsmės elektroninėje erdvėje kyla ne tik atskiriems vartotojams, bet net valstybėms. Pastaruoju laikotarpiu kibernetinis saugumas yra įvardijamas kertiniu informacinės visuomenės akmeniu. Kaip teigia Vidaus reikalų ministerijos direktorius G. Čiurlionis, 2008 m. buvo įsilaužta į daugiau kaip 300 Lietuvos įmonių ir valstybinių organizacijų interneto svetainių ir pradiniuose puslapiuose įdėta Sovietų Sąjungos simbolika –kūjis ir pjautuvas. Tai buvo įvertinta kaip ataka prieš Lietuvą. Pernai, per Ukrainos krizę, Lietuvoje net 18 procentų per metus padaugėjo kibernetinių incidentų.

2.2. Kibernetinio saugumo samprata ir jos užtikrinimas

Šiuolaikinis supratimas apie informacijos saugumą pradėjo formuotis atsiradus kompiuteriams ir poreikiui valdyti informaciją ir žinias antroje XX a. pusėje. Visuomenei tampant vis labiau priklausomai nuo patikimo informaciją apdorojančių technologijų veikimo, šių jos individų, organizacijų ar net visos visuomenės gyvenimą nuolat veikia technologijų veiklos sutrikimai, pavyzdžiui, nepageidaujami laiškai, virusai, interneto svetainių sutrikimai, tapatybės pasisavinimas, slaptos informacijos nutekėjimas (pvz., Wikileaks) ar Tūkstantmečio klaidos (Y2K) sukeltas ažiotažas visame pasaulyje (Atkočiūnienė, Janiūnienė 2013).

Informacijos saugumo valdymo kaip daugiadalykio tyrimų subjekto poziciją išryškina ir Kanados bei Taivano mokslininkai, kurie savo empirinėse studijose taip pat atkreipia dėmesį į tai, kad mokslinėje literatūroje plačiai diskutuojama apie technologinius veiksnius, tačiau pabrėžia, kad būtina vertinti organizacijos kultūros ir valdymo principų sąsajas, o efektyvus informacijos saugumo valdymas turi *remtis darniu žmogiškųjų, organizacinių ir technologinių veiksnių koordinavimu* (Nott, 2011).

Jastiuginas (2011) siūlo išskirti tris informacijos saugumo valdymo aspektus:

- strateginį – apimantį administracinius, organizacinius, valdymo, ekonominius, teisinius, gerųjų praktikų ir pan. aspektus;
- žmogiškojo veiksnio – apimantį saugumo kultūros, etinius, kompetencijų, mokymų, psichologinius ir pan. aspektus;
- technologinį – apimantį informacinių technologijų, techninių ir programinių priemonių, matematinius, kriptologinius ir pan. aspektus.

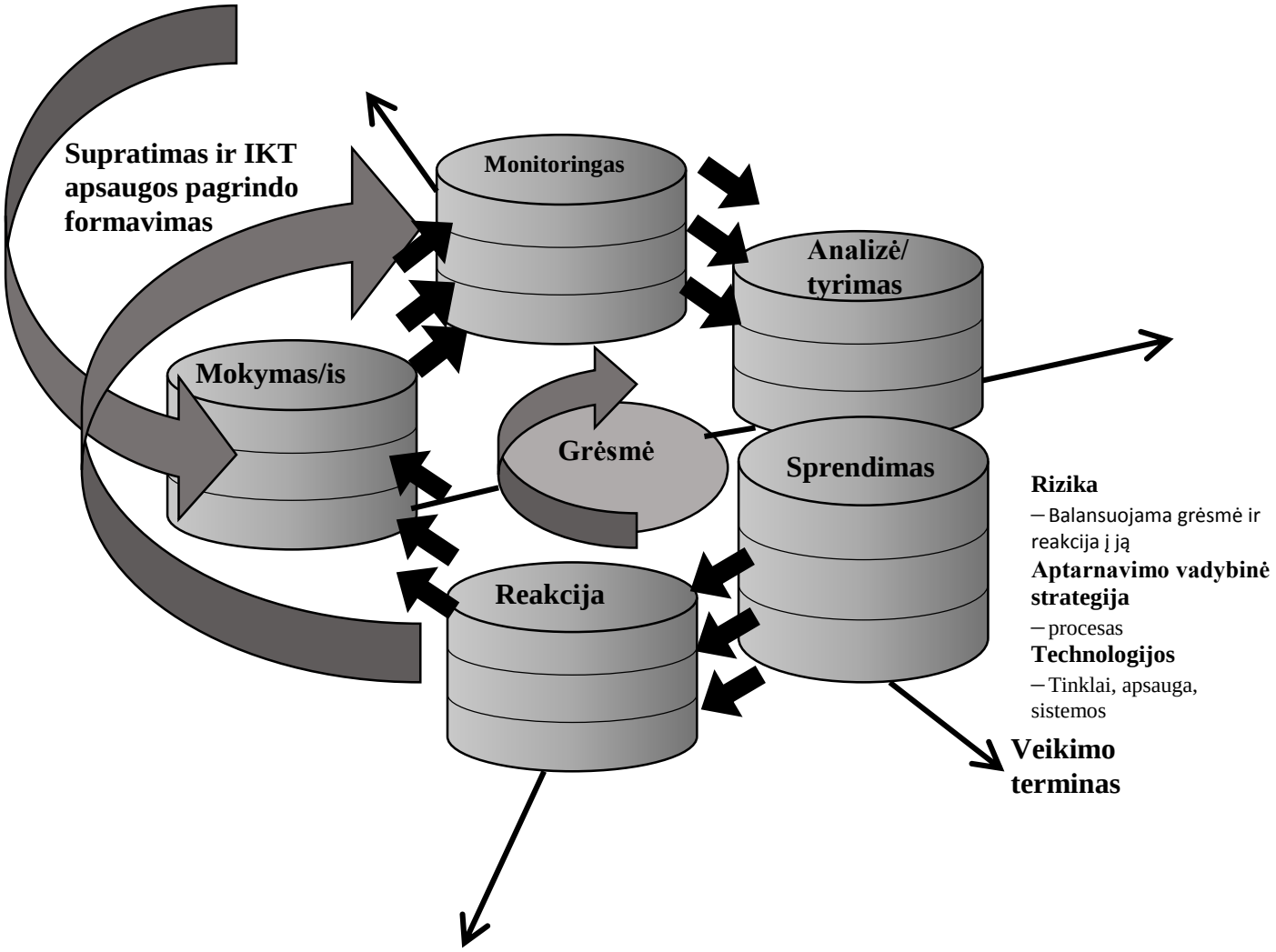
D.Štitilis ir V.Klišauskas (2012) teigia, kad elektroninės informacijos saugos aplinkos kausimus galima skirstyti į keturias pagrindines grupes:

- normatyvinę - įstatymai, įstatymų įgyvendinimų teisės aktai ir pan.;
- administracinę – organizacijos vadovybės vykdomi bendro pobūdžio veiksmai;
- procedūrinę – konkretūs su konkrečiais asmenimis susiję saugumo veiksmai;
- programinį-techninį – vykdomi konkretūs techninio pobūdžio veiksmai.

Analizuojant pasirinktą problemą, šiame darbe didžiausias dėmesys bus skiriamas pirmajai – normatyvinei grupei.

S. Jastiuginas (2011) teigia, kad kibernetinis saugumas susijęs su procesų, susijusių su kylančių kibernetinių grėsmių identifikavimu bei sąnaudomis pagrįstų kontrapriemonių taikymu, kūrimu ir palaikymu. D. Štitilis (2013) kibernetinį saugumą apibrėžia kaip apsaugą nuo netinkamo interneto infrastruktūros naudojimo ir piktnaudžiavimo (žlugdymo). Janeliūnas (2007) saugumą apibūdina kaip galios suteikta galimybė valstybei kontroliuoti tam tikrą aplinką, būti nepriklausomai nuo išorinės jėgos spaudimo.

Ch. Nott (2011) pažymi, kad būtina sukurti aiškią ir kryptingą kibernetinės apsaugos mechanizmą. Kaip vieną iš kibernetinio saugumo viešajame sektoriuje užtikrinimo būdų autorius siūlo kibernetinio užtikrinimo ciklą (3 pav.)



3 pav. Kibernetinio užtikrinimo ciklas

Sudaryta darbo autoriaus pagal Ch.Nott (2011)

Taigi kibernetinė apsauga – tai daugialypis procesas, kuris priklauso nuo darbuotojų pasirengimo, mokymo/si, IKt atnaujinimo ir palaikymo, nuolatinio situacijos monitoringo: vertinimo ir tyrinėjimo, aiškių, tikslių sprendimų priėmimo bei greitos reakcijos į ataką.

R. Werlinger ir kiti (2009) teigia, kad pagrindiniai veiksniai, išgyvendinant kibernetinio saugumo priemones yra šie:

- žmogiškasis veiksnys - tai specialistų patirtis ir nuolatinis mokymasis, organizacijos kultūra, bendradarbiavimas saugumo klausimais.

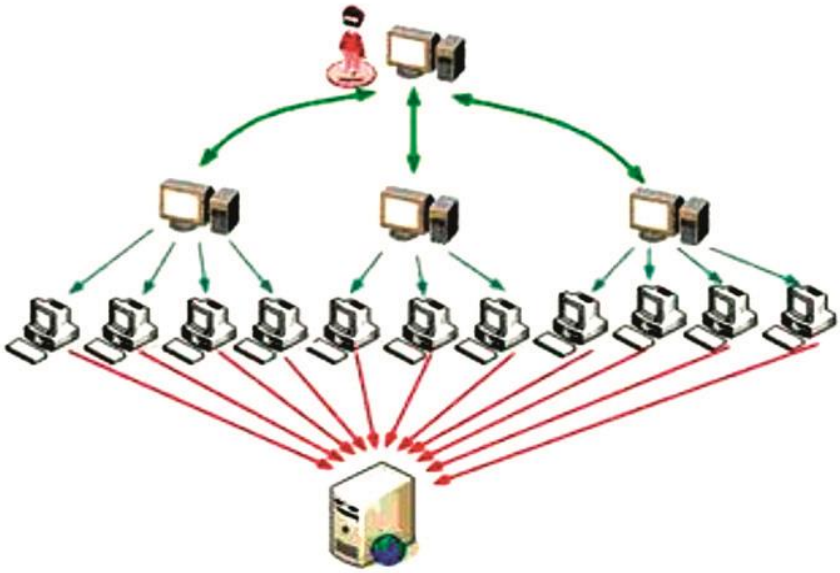
- organizacinis veiksnys - tai informacinių technologijų specialistų racionalus pareigų pasiskirstymas, kontroliuojama prieiga prie slaptų duomenų, organizacijos dydis, vadovybės parama, saugumas užtikrinimas įvardinamas kaip prioritetinė veikla, ryšiai su kitomis organizacijomis, biudžetas.
- Technologinis veiksnys – IKT sistemų ir duomenų bazių saugumas, tinklo, sistemų apsauga, biudžetas, naujausių apsaugos technologijų diegimas.

Apibendrinat galima teigti, kad. į elektroninę formą perkeliama vis daugiau informacijos apie šalies valdymo ir technologinius procesus. Dėl tos priežasties kibernetinė erdvė tapo patraukliu nusikalstamų grupuočių, politinių jėgų ir kitų subjektų taikiniu. Kibernetinis saugumas ir ypatingos svarbos informacinės infrastruktūros apsauga priklauso nuo technologinių, žmogiškųjų ir organizacinių veiksnių. Tik jų efektyvus funkcionavimas ir dermė gali sudaryti optimalias prielaidas kibernetinio saugumo užtikrinimui.

2.3. Kibernetiniai incidentai

Incidentu laikomas įvykis, kuris sutrikdo, pakeičia arba perima informacinės sistemos veikimą, gali sudarkyti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę ja naudotis, taip pat sudaryti sąlygas pasisavinti neviešą elektroninę informaciją tokios teisės neturintiems asmenims (Štitilis, Paškauskas, 2007). Incidentų kibernetinėje erdvėje sparčiai daugėja. Kibernetinė ataka – informacinių sistemų, jose tvarkomos elektroninės informacijos puolimas, panaudojant informacines sistemas ar kitas informacinių technologijų priemones, siekiant sutrikdyti informacinių sistemų ir šias sistemas naudojančių organizacijų veiklą. Žinomos 2007 m. kibernetinės atakos prieš Estijos ypatingos svarbos informacinę infrastruktūrą – šalis turėjo kuriam laikui atjungti savo internetinius tinklus nuo išorinio pasaulio. 2008 m., Rusijai įsiveržus į Gruziją, kibernetinė ataka buvo nukreipta į Gruzijos internetinę erdvę – strigo mobilusis ir internetinis ryšys, atsirado trikdžių žinių portaluose ir televizijoje. Sudėtingas virusas 2010 m. buvo panaudotas prieš Irano branduolinę programą, kurią smarkiai pažeidė. 2013 TEO padalinys Lietuvoje – HOSTEX bendrovės duomenų centras susilaukė masinės kibernetinės atakos. Daugėja masinių kibernetinių puolimų prieš kitas svarbias informacines sistemas Baltijos šalyse ir Europoje (Dzemyda, Telksnys, Žintelis, Razumas).

Pastebimi labai įvairūs kibernetinių atakų vykdymo būdai. Vienas jų – DDoS (angl. *Distributed Denial of Service* – paskirstytas atsisakymas aptarnauti) – tai atakų prieš kompiuterines sistemas būdas. Jo tikslas – sukurti tokias sąlygas, kad teisėtiems sistemos naudotojams jos ištekliai taptų neprieinami ar gaunami apsunkintai. Dažnai naudojamas kompiuterių – zombių tinklas (angl. *botnet*) – grupė tinkle esančių kompiuterių, užkrėstu specialiu kodu (botu), suteikiančiu galimybę nuotoliniu būdu juos valdyti. Paprastai naudojami DDoS atakų rengimui arba brukalams siųsti.



4 pav. DDoS - tai atakų prieš kompiuterines sistemas būdas

2013 m. gegužės mėn. vykdant kibernetines atakas prieš DELFI portalą, kartais užklausų skaičius per kelias minutes siekdavo po 50 mln., duomenų srautas siekė 6 gigabitus per sekundę. Įranga veikė kritinėse ribose, ne tiek gigabitais, bet užklausų kiekiu. Tai reiškia, kad norėta paveikti visą duomenų centro paslaugos struktūrą. Yra daug DDoS atakų tipų, tačiau jų mechanizmas yra toks pat – didelis skaičius užklausų iš daugybės kompiuterių tuo pačiu metu siunčiama į vieną ir tą patį duomenų centrą. Toks srauto išaugimas išveda iš rikiuotės serverį, į kurį nukreiptos užklausos. Visos DDoS atakos skirtos sistemos ištekliams išsekinti.

Kitas kenkimo būdas yra portalo sudarkymas (angl. *defacement*). Suradus angą portale pakeičiama jo dalis. Dar vienas puolimo veiksmas – duomenų vagystė. Daugybė institucijų svetainių yra „skylėtos“, todėl nesunku nusiųsti programinius kodus, kurie kurį laiką „miegos“. Gavę signalą iš valdytojo, nustatys ryšį, tarkime, tarp ministerijos ir valdytojo nurodyto serverio, į kurį nutekės visa reikalingą informacija. Šie puolimo būdai plačiai žinomi, bet būtina turėti omenyje, kad puolamieji kibernetiniai ginklai nuolat tobulinami.

Valstybių aktyvaus kibernetinių atakų rengimo ir vykdymo prieš kitų valstybių infrastruktūrą problemą tarptautinės bendruomenės gerokai ignoravo, nors šios atakos gresia nacionaliniam saugumui, ekonominei ir socialinei valstybių gerovei. 2010 m. birželį viešai atsiradusi kenkėjiška STUXNET tipo programinė įranga, sukurta naikinti specialiai numatytus ypatingos svarbos infrastruktūros komponentus, buvo bene pirmasis požymis, kad valstybės pajuto vieną iš piktavališkos kibernetinės veiklos sričių.

Taigi apibendrinant galima teigti, kad kibernetinių incidentų mastas auga, atsiranda vis naujų kenkėjiškų programų, kurios gali suardyti tiek asmens, tiek organizacijos ar valstybės tam tikrą veiklą.

2.4. ES kibernetinio saugumo strategija

Elektroninės informacijos sauga (kibernetinis saugumas) akcentuojama ne viename Europos Sąjungos dokumente. Jau 2001 metais ES teisės aktuose yra nurodoma, kad informacinės ir telekomunikacinės technologijos tapo šiuolaikinės visuomenės gyvenimo pagrindu ir nuo jų vis labiau yra priklausomi socialiniai ir ekonominiai visuomenės gerovės aspektai (Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 2001). 2006 metais ES atkreipė dėmesį į saugios Europos kibernetinės erdvės sukūrimą pasitelkiant visus socialinius valdžios partnerius, nes didžiuliai informacijos kiekiai yra saugomi privačių įmonių duomenų centruose, valstybės institucijų duomenų saugyklose ir informacinių sistemų duomenų bazėse. Tokios informacijos paviešinimas, nesavalaikis naudojimas ar sugadinimas gali sutelkti didžiules problemas ir ženklius nuostolius verslo organizacijoms ar viešojo administravimo subjektams (Komisijos komunikatas Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui, 2006)

Europos Sąjungos valstybės ypatingą dėmesį atkreipia į tai, kad reikalingas glaudesnis Sąjungos šalių narių bendradarbiavimas kovojant su nusikaltimais elektroninėje erdvėje, taip pat užtikrinant apsaugą nuo kibernetinių išpuolių.

Pastaraisiais metais ES kibernetinio saugumo sričiai skiriamas ypatingas dėmesys. 2012 metais Europos Komisija paskelbė konsultaciją kibernetinio saugumo teisinio reguliavimo srityje. 2013 metais vasario 7 d. Europos Komisija ir Sąjungos vyriausioji įgaliotinė užsienio reikalams ir saugumo politikai paskelbė kibernetinio saugumo strategiją kartu su Komisijos direktyvos dėl tinklų ir informacinių sistemų saugumo siūlymu (Joint Communication to the European Parliament, the Council, the European Ecomonic and Social Committee and the Committee of Regions, 2013).

ES parengtoje kibernetinio saugumo strategijoje akcentuojami penki strateginiai prioritetai:

- Pasiekti kibernetinį atsparumą;
- Radikaliai sumažinti elektroninių nusikaltimų skaičių;
- Sukurti kibernetinės gynybos politiką ir pajėgumus, kiek tai susiję su bendra saugumo ir gynybos politika;
- Plėtoti pramonės ir technologinius išteklius, skirtus kibernetiniam saugumui užtikrinti;
- Sukurti nuoseklią tarptautinę elektroninės erdvės politiką ir remti pagrindines ES vertybes.

ES patvirtinta kibernetinio saugumo strategija „Atvira, saugi ir patikima kibernetinė erdvė“ yra išsami ES vizija, kaip geriausiai užkirsti kelią kibernetinės veiklos sutrikdymui bei atakoms ir kokių atsakomųjų priemonių imtis. Taip siekiama remti laisvės ir demokratijos vertybes ir užtikrinti saugų skaitmeninės ekonomikos augimą.

Analizuojamame dokumente išskiriami pagrindiniai kibernetinio saugumo principai:

1. **Pagrindinių žmogaus teisių, nuomonės reiškimo laisvės, privatumo ir asmens duomenų apsauga,** nes kibernetinis saugumas gali būti efektyvus tik tuo atveju, jei paremtas pagrindinių teisių ir laisvių apsauga, taip pat grįstas esminėmis ES vertybėmis. Taip pat asmenų teisės negali būti u-tikrintos be saugių tinklų ir sistemų.
2. **Prieiga visiems**, nes ribota prieiga prie interneto ar tokios prieigos nebuvimas sukelia nepatogumus piliečiams. Kiekvienas turi turėti prieigą prie interneto bei informacijos. Interneto integralumas bei saugumas turi būti garantuojamas, kad būtų užtikrinta saugi prieiga visiems.
3. **Demokratinis ir efektyvus valdymas.** Skaitmeninis pasaulis nėra kontroliuojamas vienos struktūros ar bendrovės. Tai ir valstybiniai, ir komerciniai, ir nevyriausybiniai dariniai, kurie įsitraukę į kasdieninį interneto resursų valdymą, protokolų ir standartų internetui kūrimą.
4. **Bendra atsakomybė užtikrinant saugumą.** Didėjanti priklausomybė nuo informacijos ir komunikacijų technologijų suponavo pažeidžiamas vietas, kurios turi būti išanalizuotos, sumažintos ir apgintos. Tiek viešasis sektorius, tiek privačios įmonės, tiek individualūs vartotojai turi pripažinti šią bendrą atsakomybę, imtis apsaugos priemonių, koordinuoti veiksmus siekiant sustiprinti kibernetinį saugumą.

ES dokumentuose akcentuojama, kad šiuolaikinėje visuomenėje kibernetiniai incidentai neturi sienų. Visi dalyviai, tiek nacionaliniu, tiek ES lygiu, turi dirbti kartu, siekiant užtikrinti kibernetinį saugumą. Šiuo metu centralizuotos europinės priežiūros koncepcija nepalaikoma. Teigiama, kad nacionalinės vyriausybės yra geriausia, kas gali organizuoti kibernetinių atakų prevenciją bei atsaką į šias atakas, taip pat bendradarbiauti su privačiu sektoriumi.

ES kibernetinio saugumo strategijoje yra išskiriami trys lygiai, kuriais būtų veikiama, siekiant užtikrinti kibernetinį saugumą (2 lentelė).

Kibernetinio saugumo užtikrinimo ES lygiai ir funkcijos

2 lentelė

Nacionalinis lygis	ES lygis	Tarptautinis lygis
1. Atitinkamos struktūros elektroninių nusikaltimų ir gynybos srityje. Šios struktūros turėtų užtikrinti reikiamus pajėgumus kovojant su kibernetiniais incidentais. 2. Koordinavimo veiklą kibernetinio saugumo srityje vykdo ministerijos.	1. Aktyvus institucijų (pvz., ENISA, Europolas, EDA) bendradarbiavimas rizikos valdymo, mokymų, apsikeitimo geriausia praktika srityse.	1. Veiksmų koordinavimas kibernetinio saugumo srityje. 2. Viešas ir skaidrus kibernetinių technologijų naudojimas. 3. Bendradarbiavimas su pagrindiniais tarptautiniais partneriais ir organizacijomis: Europos Taryba, EBPO ir kt.

3. Nustatytos įvairių nacionalinių institucijų funkcijos. 4. Užtikrinamas reikiamas apsikeitimas informacija ne tik tarp valstybės institucijų, bet ir privačių sektoriumi. 5. Kibernetinių atakų atveju užtikrinamas atitinkamų saugumo planų veikimas, įskaitant ir atitinkamų funkcijų bei atsakomybių nustatymą.		

Apibendrinant galima teigti, kad ES kibernetinio saugumo strategija yra išsamus strateginis dokumentas, kuriame reglamentuojami esminiai principai, tikslai, kibernetinio saugumo užtikrinimo lygiai bei valstybių narių ir Komisijos bendradarbiavimo mechanizmas.

2.5. Užsienio šalių patirtis kibernetinio saugumo užtikrinimo srityje

Daugėjant informacijos saugumo pažeidimų, kyla poreikis valdyti informacijos saugumo problemas valstybių lygmeniu, tačiau kibernetinės erdvės ir interneto infrastruktūros globalus pobūdis reikalauja dar platesnio požiūrio. Pavyzdžiui, pastebimi augantys informacijos saugumo pažeidimo atvejai: Jungtinėse Amerikos Valstijose per ketverius pastaruosius metus kompiuterinių incidentų skaičius išaugo daugiau nei 400 procentų (GAO ataskaita, 2010); Didžiojoje Britanijoje 92 proc. didžiųjų bendrovių praneša apie rimtus saugumo incidentus, patirtus 2009 metais (palyginimui 2008 metais – 72 proc.) ir išaugusius vidutinius didžiausio incidento atneštus nuostolius, kurie apytiksliai nuo 90–170 tūkst. svarų sterlingų išaugo iki 280–690 tūkst. svarų sterlingų (Infosecurity Europe, 2010); Lietuvoje su incidentais susiduria 85 proc. internetu besinaudojančių įmonių, o 27,2 proc. gyventojų ir 23 proc. įmonių nurodo, kad dėl incidentų patyrė nuostolių .

2013 metais balandžio mėn. 13 ES valstybių buvo pasitvirtinusios nacionalines kibernetinio saugumo strategijas (Štitilis, 2013). Plačiau bus nagrinėjamos trijų valstybių – Jungtinės Karalystės, Vokietijos ir Prancūzijos parengtos kibernetinio saugumo strategijos.

Jungtinės Karalystės kibernetinio saugumo strategija „Jungtinės Karalystės apsauga ir palaikymas skaitmeniniame pasaulyje“ patvirtinta 2011 m. lapkričio mėn. (UK Cybersecurity Strategy, 2011). Strategijoje numatyta kibernetinio saugumo vizija 2015 metams: iš energingos, tvirtos ir saugios elektroninės erdvės gauti didžiulę ekonominę ir socialinę vertę, kur šalies veiksmai, valdomi

šalies esminių laisvės vertybių, teisingumo, skaidrumo ir įstatymų galio, didins gerovę, nacionalinį saugumą ir tvirtą visuomenę. Strategijoje įvardinti strateginiai tikslai: kovoti su elektroniniais nusikaltimais Jungtinėje Karalystėje ir tapti viena iš saugiausių šalių pasaulyje verslui elektroninėje erdvėje vystyti; būti atsparesnei kibernetiniams išpuoliams ir sugebėti geriau apsaugoti savo interesus elektroninėje erdvėje.

Vokietijos kibernetinio saugumo strategija patvirtinta 2011 m. vasario mėnesį (Cybersecurity Strategy for Germany,2011). Vokietijos strategijoje išskiriami šie pagrindiniai elektroninės erdvės saugumo strateginiai tikslai ir priemonės saugumui užtikrinti: ypatingos svarbos informacinių struktūrų apsauga; saugios informacinės technologijos bei jų apsaugos stiprinimas viešojo valdymo sektoriuje; nacionalinis reagavimo į kibernetines nelaimes centras; nacionalinės kibernetinės erdvės apsaugos taryba; efektyvūs koordinuoti veiksmai siekiant užtikrinti kibernetinį saugumą Europoje ir pasaulyje; reagavimo į kibernetinius išpuolius įrankiai.

Prancūzijos informacinių sistemų gynybos ir saugumo strategija priimta 2011 m. vasario mėnesį (France information systems defence and security strategy, 2011). Strategijoje nurodyti šie pagrindiniai tikslai: įgyti pasaulinę galią kibernetinės gynybos srityje; apsaugoti Prancūzijos gebėjimą priimti sprendimus apsaugant informaciją, susijusią su jos suverenitetu; stiprinti svarbiausių nacionalinių infrastruktūrų kibernetinį saugumą; užtikrinti elektroninės erdvės saugumą.

Apibendrinant minėtų valstybių kibernetinio saugumo strategines nuostatas, galima pastebėti, kad visos valstybės kelia panašius tikslus, kurie susiję su glaudžiu bendradarbiavimu tiek nacionaliniu, tiek tarptautiniu lygiu bei informacijos keitimuisi. Esminiai tikslai – kovoti su elektroniniais nusikaltimais bei gerinti atsparumą kibernetinėms atakoms ir saugoti nacionalinį saugumą bei vystyti kibernetinio saugumo žinias bei pajėgumus užtikrinant kibernetinį saugumą. Taip pat akcentuojami kritinės informacijos infrastruktūros apsaugos, visuomenės informavimo, informacinių technologijų stiprinimo viešajame sektoriuje uždaviniai.

Daugėjant informacijos saugumo pažeidimų, kibernetinių incidentų, kyla poreikis valdyti informacijos saugumo problemas valstybės lygmeniu. Trečiojoje darbo dalyje bus vertinamas Lietuvos pasirengimas kibernetinio saugumo rizikai valdyti.

3. KIBERNETINIO SAUGUMO UŽTIKRINIMO VIEŠAJAME VALDYME VERTINIMAS

Skyriuje atliekamas kibernetinio saugumo užtikrinimo viešajame valdyme vertinimas. Analizuojami Lietuvos respublikos teisės aktai, reglamentuojantys kibernetinį saugumą; Valstybinio audito ataskaita *Valstybės informacinių išteklių valdymas* (2013); Valstybinio audito ataskaita *Žemės ūkio ministerijos informacinių išteklių valdymas* (2013); Valstybinio audito ataskaita *Teisingumo ministerijos informacinių išteklių valdymas* (2013).

XX a. antroje pusėje spartus informacinių ir telekomunikacinių technologijų vystymasis, sudarė prielaidas modernizuoti viešojo administravimo sistemą. Asmenų ir organizacijų netinkamas pasirengimas valdyti informacijos saugumo incidentus gali lemti visos valstybės ir net pasaulines problemas, todėl gebėjimas valdyti informacijos saugumą turi tapti strateginiu tiek organizacijų, tiek valstybių tikslu.

Lietuva, modernizuodama viešąjį sektorių adekvačiai Europos integracijos ir Europos Sąjungos plėtros nuostatomis siekia valstybės valdymo sistemą pertvarkyti remiantis sisteminiu požiūriu ir vadybos pagrindais; unifikuoti centrinės viešojo administravimo sistemos institucinę sąrangą, aiškiai nustatyti kiekvienos viešojo administravimo institucijos kompetencijos sritis, optimizuoti viešojo administravimo institucijų funkcijas ir jų skaičių, sukurti kibernetinio saugumo užtikrinimo sistemą ir jos įgyvendinimo mechanizmus.

Lietuvos viešasis sektorius pasirinktas atsižvelgiant į viešosios teisės principus: viešąjį sektorių įpareigoja aiškūs teisiniai rėmai, kurių sektoriaus subjektai negali peržengti pasirinkdami, kaip reaguoti į kibernetinių atakų rizikas (Atkočiūnienė, Janiūnienė, 2013).

Vykdant kibernetinio saugumo užtikrinimo viešajame valdyme vertinimą bus **atlikta dokumentų analizė – įvertintas informacijos saugumo valdymo reikalavimų, įtvirtintų Lietuvos Respublikos teisės aktais, skirtais viešojo sektoriaus organizacijoms, turinys,** ieškant sąsajų su išskirtomis informacijos saugumo valdymo koncepcijos įgyvendinimo priemonėmis – tarptautiniais informacijos saugumo valdymo standartais.

Atliekant kibernetinio saugumo užtikrinimo viešajame valdyme vertinimą, analizuojama šie dokumentai:

- Lietuvos respublikos teisės aktai, reglamentuojantys kibernetinį saugumą;
- Valstybinio audito ataskaita *Valstybės informacinių išteklių valdymas* (2013);
- Valstybinio audito ataskaita *Žemės ūkio ministerijos informacinių išteklių valdymas* (2013);
- Valstybinio audito ataskaita *Teisingumo ministerijos informacinių išteklių valdymas* (2013);

Nurodyti dokumentai bus vertinami pagal šiuos kriterijus:

- Teisės aktų kibernetinio saugumo srityje rengimo ir jų reglamentų tikslai;
- Kibernetinio saugumo politikos įgyvendinimas;
- Funkcijos ir įgaliojimai, kurie deleguoti Viešojo administravimo įstaigoms.

3.1. Teisės aktai, reglamentuojantys kibernetinį saugumą

Kibernetinis saugumas – labai svarbi ir specifinė veiklos rūšis, kuri taip pat reikalauja nuoseklaus ir detalaus teisinio reglamentavimo. Vieni iš pagrindinių dokumentų šioje srityje – strateginiai dokumentai, kibernetinio saugumo strategijos.

Pirmuosius informacijos saugumo reikalavimus Lietuvos Respublikos Vyriausybė patvirtino 1997 metais, siekdama užtikrinti duomenų patikimumą ir apsaugą nuo neteisėto naudojimo (Bendrieji duomenų apsaugos reikalavimai, 1997) ir įpareigojo duomenų valdytojus, vadovaujantis Lietuvos standartais, atitinkančiais tarptautinės grupės „Informacijos technologija. Saugumo technika“ ISO/IEC standartus, suformuluoti specialius duomenų saugos priemonių reikalavimus ir nustatyti duomenų saugos įgyvendinimo tvarką bei priemones.

2001 m. į informacijos saugumo užtikrinimą buvo pažvelgta plačiau - strateginės valstybės IT saugos raidos kryptys ir priemonės buvo išdėstytos pirmojoje Lietuvos IT saugos valstybinėje strategijoje (Informacijos technologijų saugos valstybinės strategija ir jos įgyvendinimo planas, 2001), kurioje rekomenduojama vadovautis Informacijos technologijų saugos valstybine strategija bei Lietuvos ir tarptautiniais grupės „Informacijos technologija. Saugumo technika“ grupės standartais. Strategijoje buvo suformuluoti svarbiausieji tikslai:

- informacijos technologijų saugos teisinio reglamentavimo plėtra (bendrųjų duomenų saugos reikalavimų pagal duomenų kategorijas, atsižvelgiant į tarptautinius standartus, Ekonominio bendradarbiavimo ir plėtros organizacijos, NATO ir Europos Sąjungos rekomendacijas, Europolo ir Šengeno informacinių sistemų reikalavimus, nustatymas; elektroninio verslo saugos reikalavimų nustatymas; elektroninio susirašinėjimo saugos reikalavimų nustatymas; kompiuterių tinklų saugos reikalavimų nustatymas; asmens identifikavimo elektroninio parašo saugos reikalavimų nustatymas; atsakomybės pagal pažeidimų pobūdį nustatymas;
- svarbiausiųjų valstybės informacinių sistemų saugos stiprinimas.

Informacijos ir elektroninių ryšių technologijų priemonėmis pagrįstų valstybės informacinių išteklių ir informacijos valdymo trūkumai neleido valstybei efektyviai valdyti informacinių išteklių, todėl nuo **2006 metų** valstybės elektroninės informacijos saugumo užtikrinimo tikslus ir uždavinius bei jų įgyvendinimą nustatė antrasis strateginis informacijos saugumo valdymo dokumentas – **Elektroninės informacijos saugos valstybės institucijų informacinės sistemos valstybinė strategija.** Ši strategija

buvo skirta išimtinai valstybės institucijų sektoriui. Valstybinės strategijos pagrindiniai numatyti pasiekti tikslai:

- Tobulinti elektroninės informacijos saugos koordinavimą ir priežiūrą.
- Teisės aktais reguliuoti elektroninės informacijos saugą.
- Kelti elektroninės informacijos saugos kultūrą.
- Tobulinti elektroninės informacijos perdavimo infrastruktūros saugą.
- Skatinti elektroninės informacijos saugos užtikrinimo projektų įgyvendinimą.

Minima Valstybės strategija nustojo galioti 2008 metais ir po šios datos Lietuvoje nebuvo jokios galiojančios informacijos saugos strategijos ir programos.

Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo“ buvo **patvirtinta Kibernetinio saugumo plėtros programa 2011-2019 metams**. Reikia atkreipti dėmesį, kad minėta programa buvo patvirtinta dar 2011 metais, kai Europos Komisija dar net nebuvo paskelbusi konsultacijos dėl ES kibernetinio saugumo strategijos, todėl Lietuvos Kibernetinio saugumo plėtros programa formaliai nederinta su ES kibernetinio saugumo strategija.

Kibernetinio saugumo plėtros programos 2011-2019 metams paskirtis – nustatyti elektroninės saugos (kibernetinio saugumo) plėtros tikslus ir uždavinius, kad būtų užtikrintas elektroninėje erdvėje teikiamų paslaugų konfidencialumas, vientisumas ir prieinamumas, elektroninių ryšių tinklų, informacinių sistemų ir ypatingos svarbos informacinės infrastruktūros apsauga nuo incidentų ir kibernetinių atakų, asmens duomenų ir privatumo apsauga. Įvardintas strateginis tikslas – plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 valandos, o Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje dalis pasiektų 60 procentų.

Nustatyti šie kibernetinio saugumo plėtros programos įgyvendinimo tikslai:

- Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas.
- Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą.
- Siekti užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje.

Kibernetinio saugumo plėtros programoje pažymima, kad programos įgyvendinimą koordinuoja Lietuvos Respublikos vidaus reikalų ministerija.

Analizuojant Lietuvos kibernetinio saugumo programą ES kibernetinio saugumo strategijos, taip pat kitų nagrinėtų užsienio valstybių kibernetinio saugumo strategijų kontekste pažymėtina, kad

programa neužtikrina visapusiškos Lietuvos kibernetinio saugumo strategijos, neatitinka visų Europos Komisijos projekte nustatytų kibernetinio saugumo prioritetų. Programoje nenumatytos priemonės dėl valstybės ir privataus sektoriaus bendradarbiavimo kibernetinio saugumo srityje; per mažai dėmesio skiriama elektroniniams nusikaltimams ir jų skaičiaus mažinimui; nenumatyta išsami ir sisteminė kibernetinės gynybos politika; neaptariami instituciniai klausimai, nedetalizuojamos atitinkamų institucijų funkcijos ir atsakomybės kibernetinio saugumo srityje; nenumatyti tikslai ir uždaviniai, susiję su visuomenės informavimu ir švietimu, kas būtina šiuolaikinėje informacinėje visuomenėje, nes kibernetinio saugumo grėsmės dažnai susijusios su galutiniais interneto vartotojais; nenumatytos konkrečios lėšos šios programos įgyvendinimui.

2014 metų gruodžio 11 d. Lietuvos Respublikos Seimas priėmė Kibernetinio saugumo įstatymą. Šiuo aktu buvo nustatytas kibernetinio saugumo sistemos organizavimas, valdymas, kontrolė, apibrėžiamos kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos, jų kompetencija, funkcijos, teisės ir pareigos, valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos paslaugų teikėjų pareigos bei atsakomybė ir kibernetinio saugumo užtikrinimo priemonės.

Kibernetinio saugumo įstatymas jame nustatytomis sąlygomis ir tvarka taikomas valstybės institucijoms, formuojančioms ir įgyvendinančioms kibernetinio saugumo politiką, viešojo administravimo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos prieglobos paslaugų teikėjams, informacinių technologijų srityje veiklą vykdantiems verslo subjektams, mokslo ir studijų institucijoms.

Įstatyme kibernetinis saugumas grindžiamas bendraisiais teisės principais, elektroninių ryšių veiklos reguliavimo principais ir šiais kibernetinio saugumo principais:

- kibernetinės erdvės nediskriminavimo – įstatymų ir kitų teisės aktų nuostatos ir saugomi gėriai vienodai taikomi tiek fizinėje, tiek kibernetinėje erdvėje;
- kibernetinio saugumo proporcingumo – taikomos kibernetinio saugumo užtikrinimo priemonės negali būti griežtesnės, negu būtina kibernetiniam saugumui užtikrinti, o taikomi teisiniai, organizaciniai ir techniniai kibernetinio saugumo reikalavimai neturi apriboti kibernetinio saugumo dalyvių veiklos kibernetinėje erdvėje labiau, negu tai būtina;
- viešojo intereso viršenybės – naudojamos kibernetinio saugumo užtikrinimo priemonės pirmiausia turi užtikrinti visuomenės viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje.

Pabrėžiama, kad taikant kibernetinį saugumą reglamentuojančias teisės normas, turi būti tinkamai atsižvelgiama į visus nurodytus principus. Šie principai turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė.

Kibernetinio saugumo įstatyme įtvirtinta nuostata, kad Kibernetinio saugumo politikos strateginius tikslus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė, kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija (toliau – Krašto apsaugos ministerija). Lietuvos Respublikos vidaus reikalų ministerija (toliau – Vidaus reikalų ministerija), Nacionalinis kibernetinio saugumo centras, Lietuvos Respublikos ryšių reguliavimo tarnyba (toliau – Ryšių reguliavimo tarnyba), Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Policijos departamentas) formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame įstatyme nustatytoms funkcijoms atlikti reikia nustatyti viešojo administravimo subjektų, valdančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veiklos teisinį reguliavimą.

Kibernetinio saugumo politiką pagal kompetenciją įgyvendina Vidaus reikalų ministerija, Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas.

Kibernetinio saugumo politikos įgyvendinimas

3 lentelė

Kibernetinio saugumo politikos įgyvendinimo subjektai	**Įgaliojimai**
Lietuvos Respublikos vyriausybė	1. Sudaro Kibernetinio saugumo tarybą ir tvirtina jos reglamentą, tarybos narių skaičių ir paveda krašto apsaugos ministrui nustatyti tarybos personalinę sudėtį; 2. Tvirtina Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką ir informacinę infrastruktūrą; 3. Tvirtina organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus ypatingos svarbos informacinei infrastruktūrai, organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus valstybės informaciniams ištekliams; 4. Tvirtina Nacionalinį kibernetinių incidentų valdymo planą bei tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus.
Krašto apsaugos ministerija	1. Rengia ir teikia Vyriausybei tvirtinti organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus ypatingos svarbos informacinei infrastruktūrai; 2. Rengia ir teikia Vyriausybei tvirtinti Nacionalinį kibernetinių incidentų valdymo planą; 3. Teikia Vyriausybei tvirtinti tipinius kibernetinių incidentų

	valdymo ypatingos svarbos informacinėse infrastruktūrose planus; 4. Tvirtina ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus, kibernetinio saugumo informacinio tinklo nuostatus.
Vidaus reikalų ministerija	1. Rengia ir teikia Vyriausybei tvirtinti Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką ir ypatingos svarbos informacinę infrastruktūrą ir (arba) šios infrastruktūros valdytojų sąrašą.
Ryšių reguliavimo tarnyba	1. Rengia ir tvirtina informacijos apie kibernetinius incidentus ir taikytas šių incidentų valdymo priemones teikimo Ryšių reguliavimo tarnybai tvarkos ir sąlygų aprašą; 2. Rengia ir tvirtina organizacinius ir techninius reikalavimus, taikomus elektroninės informacijos prieglobos paslaugų saugumui ir vientisumui užtikrinti; 3. Rengia ir tvirtina techninės informacijos, reikalingos vertinti viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būseną, teikimo Ryšių reguliavimo tarnybai tvarkos ir sąlygų aprašą; 4. Atlieka viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų interneto prieigos tinklų infrastruktūros vientisumo, viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir (arba) elektroninės informacijos prieglobos paslaugų kibernetinio saugumo būsenos tyrimus.
Kibernetinio saugumo taryba	1. Teikia pasiūlymus kibernetinio saugumo dalyviams dėl kibernetinio saugumo prioritetų, plėtros krypčių, siektinų rezultatų ir jų įgyvendinimo būdų bei dėl platesnio viešojo sektoriaus, verslo ir mokslo bendradarbiavimo galimybių kibernetinio saugumo užtikrinimo srityje; 2. Analizuoja kibernetinio saugumo užtikrinimo tobulinimo tendencijas, teikia kibernetinio saugumo dalyviams išvadas ir pasiūlymus dėl kibernetinių incidentų valdymo; 3. Teikia kibernetinio saugumo dalyviams rekomendacijas dėl kibernetinio saugumo stiprinimo.
Nacionalinis kibernetinio saugumo centras	1. Rengia ir teikia pasiūlymus krašto apsaugos ministrui dėl organizacinių ir techninių kibernetinio saugumo reikalavimų valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai; 2. Atlieka valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną; 3. Rengia tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus; 4. Teikia konsultacijas ir rekomendacijas valstybės informacinių išteklių valdytojams ir ypatingos svarbos infrastruktūros valdytojams kibernetinio saugumo klausimais; 5. Analizuoja nacionalinę kibernetinio saugumo situaciją ir rengia nacionalinio kibernetinio saugumo būklės ataskaitas; 6. Ne rečiau kaip kartą per metus rengia ir teikia nacionalinio kibernetinio saugumo būklės ataskaitas krašto apsaugos

	ministrui; 7. Rengia ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus; 8. Valdo kibernetinio saugumo informacinį tinklą; 9. Vykdo informacijos sklaidą kibernetinio saugumo klausimais.
Valstybinė duomenų apsaugos inspekcija	1. Atlieka juridinių asmenų patikrinimus, kai yra rizikos, kad kibernetiniai incidentai gali turėti įtakos asmens duomenų apsaugai; 2. Teikia visuomenei ir suinteresuotoms institucijoms informaciją apie kibernetinio saugumo, susijusio su asmens duomenų apsauga, rizikos veiksnius, pavojus ir grėsmes kibernetinėje erdvėje; 3. Nustato viešojo administravimo subjektams, valdantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams informacijos apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones pateikimo tvarką; 4. Renka, analizuoja ir vertina informaciją apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones; 5. Tikrina asmens duomenų tvarkymo teisėtumą ir priima sprendimus dėl asmens duomenų tvarkymo pažeidimų kibernetinėje erdvėje.
Policija	1. Renka, analizuoja ir apibendrina informaciją apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių; 2. Nustato viešojo administravimo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo tvarką; 3. Turi teisę duoti motyvuotus nurodymus ne ilgiau kaip 48 valandoms be teismo sankcijos, ilgesniam laikui – su apylinkės teismo sankcija, apriboti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikimą paslaugų gavėjui, kai paslaugų gavėjas ar jo naudojama informacinė ir ryšių technologijų įranga galimai dalyvauja nusikalstamoje veikoje, ir (arba) nurodyti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui ar elektroninės informacijos prieglobos paslaugų teikėjui taikyti priemones, šalinančias nusikalstamų veikų kibernetinėje erdvėje priežastis; 4. Turi teisę duoti motyvuotus nurodymus viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikėjui išsaugoti

	informaciją, susijusią su jų teikiamomis paslaugomis, iš kurios galima nustatyti naudotos ryšio paslaugos tipą, taikytas technines priemones ir naudojimo laiką, abonento tapatybę, pašto, geografinės padėties adresą, telefono ir bet kokį kitą prieigos numerį, informaciją apie sąskaitas ir atliktus mokėjimus paslaugos sutarties arba susitarimo pagrindu ir kitą informaciją ryšių aparatūros įrengimo vietoje, turimą pagal paslaugos sutartį arba susitarimą, šią informaciją gauti, taip pat teisės aktų nustatyta tvarka, kai yra motyvuota teismo nutartis, gauti paslaugų naudotojo srauto duomenis ir kontroliuoti perduodamos informacijos turinį.

Šiame įstatyme viešojo administravimo subjektams deleguojama atsakomybė už jų **valdomų ir (arba) tvarkomų valstybės informacinių išteklių kibernetinį saugumą. Pabrėžiama, kad privalo savo lėšomis užtikrinti jų valdomų ir (arba) tvarkomų valstybės informacinių išteklių atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams.** Viešojo administravimo subjektai privalo:

- informuoti Nacionalinį kibernetinio saugumo centrą apie jų valdomuose ir (arba) tvarkomuose valstybės informaciniuose ištekliuose įvykusius kibernetinius incidentus, apibrėžtus organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose, ir taikytas kibernetinių incidentų valdymo priemones Vyriausybės ar jos įgaliotos institucijos nustatyta tvarka;
- teikti Valstybinei duomenų apsaugos inspekcijai informaciją apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones šios institucijos nustatyta tvarka ir sąlygomis;
- privalo teikti policijai informaciją, reikalingą kibernetiniams incidentams, turintiems nusikalstamos veikos požymių, užkardyti ir tirti, policijos generalinio komisaro nustatyta tvarka ir sąlygomis;
- paskirti kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir Nacionaliniam kibernetinio saugumo centrui pateikti paskirto asmens ar padalinio kontaktinę informaciją;
- sudaryti sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose.

Kibernetinio saugumo įstatyme pirmą kartą reglamentuotas tarpinstitucinis bendradarbiavimas, informacijos pasikeitimo tvarka ir atsakomybė už kibernetinio saugumo reikalavimų pažeidimus. Akcentuojama, kad Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Policijos departamentas ir kitos policijos įstaigos turi bendradarbiauti tiriant kibernetinius incidentus, keistis su kibernetinių incidentų tyrimais susijusia informacija, reikalinga institucijų pagal kompetenciją

vykdomoms funkcijoms atlikti. Prireikus apie kibernetinių incidentų tyrimą informuojami kiti kriminalinės žvalgybos subjektai ir (arba) žvalgybos institucijos. Valstybinė duomenų apsaugos inspekcija bendradarbiauja su Nacionalinio kibernetinio saugumo centru ir Ryšių reguliavimo tarnyba tiriant kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, keičiasi informacija, reikalinga teisės aktų nustatytoms funkcijoms, susijusioms su kibernetinių incidentų, pažeidžiančių asmens duomenų saugumą, tyrimu, atlikti. Tarpinstitucinio bendradarbiavimo tiriant kibernetinius incidentus tvarka ir kibernetinių incidentų klasifikavimo tvarka nustatomos Nacionaliniame kibernetinių incidentų valdymo plane. Taip pat planuojamas bendradarbiavimas su NATO kibernetinio saugumo kompetencijos centru Estijoje ir kitomis tarptautinėmis kibernetinio saugumo organizacijomis.

Taigi vertinant Lietuvos teisės aktus, kurie reglamentuoja kibernetinį saugumą galima teigti, kad iki 2011 metų kibernetinio saugumo reguliavimas ir koordinavimas vyko fragmentiškai, įvairių viešojo administravimo įstaigų veikla šioje srityje nebuvo susieta į bendrą visumą. 2011 metais parengus Kibernetinio saugumo plėtros programą 2011-2019 metams išryškėjo strateginis tikslas – plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių. Taip pat aiškiai įvardinta šios veiklos koordinatorė - Lietuvos Respublikos vidaus reikalų ministerija. Tačiau formaliai ši programa nederinta su ES kibernetinio saugumo strategija, nes ji patvirtinta dar 2011 metais, kai Europos Komisija dar net nebuvo paskelbusi konsultacijos dėl ES kibernetinio saugumo strategijos.

2014 metais Lietuvos Respublikos Seimo priimtas Kibernetinio saugumo įstatymas reglamentavo Kibernetinės saugos užtikrinimą. Įstatyme atsakyta į daug konkrečių ir Lietuvos kibernetiniam saugumui svarbių klausimų: kaip procesas turėtų būti valdomas, kas turi prisiimti atsakomybę, kokios institucijos ir kokias funkcijas atlieka, kas formuoja politiką?

Šiuo įstatymu buvo nustatytas kibernetinio saugumo sistemos organizavimas, valdymas, kontrolė, apibrėžiamos kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos, jų kompetencija, funkcijos, teisės ir pareigos, valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos paslaugų teikėjų pareigos bei atsakomybė ir kibernetinio saugumo užtikrinimo priemonės.

Šio įstatymo pagrindu nuo 2015 metų sausio 1 d. Lietuvoje veiklą pradėjo Nacionalinis kibernetinio saugumo centras, suformuotas Krašto apsaugos ministerijos padalinio pagrindu. Naujai steigiamas centras tapo pagrindiniu kibernetinio saugumo politikos įgyvendinimo subjektu, o pagrindinis jo dėmesys yra sutelktas valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros

kibernetiniam saugumui. Centras analizuos kibernetinio saugumo aplinką, rengs reikalavimus viešojo sektoriaus informacinių išteklių ir ypatingos svarbos infrastruktūros kibernetiniam saugumui užtikrinti, kibernetinės gynybos bei grėsmių valdymo planus, koordinuos ir prižiūrės, kaip institucijų valdytojai įgyvendina kibernetinės apsaugos priemones, taip pat tirs ir reaguos į kibernetinius incidentus. Taip pat bus perimta geroji pasaulinė patirtis, kuri kibernetinio saugumo specialistams padės operatyviai keistis informacija apie kylančias grėsmes ir kibernetinius incidentus, koordinuoti veiksmus reaguojant į krizines situacijas.

Tačiau reikia pažymėti, kad šio įstatymą ateityje reikėtų koreguoti, siekiant efektyvesnio šio proceso valdymo. Kibernetinis saugumas turėtų būti valdomas iš vieno taško, vieno langelio principu, kad nutikus incidentui būtų žinoma į kur kreiptis, o jau vėliau būtų atitinkamai paskirstyti darbai ir atsakomybės. Tačiau šios dienos realijose tą pasiekti dar gana sudėtinga, nes atskiros institucijos priklauso įvairioms ministerijoms, todėl sureguliuoti tokius dalykus iš vieno karto, vienu įstatymu, yra sudėtingas.

3.2.Valstybės informacinių išteklių valdymo analizė

Valstybinio audito ataskaitoje *Valstybės informacinių išteklių valdymas (2013) m.* pabrėžiama, šalyje **parengti ne visų valstybės informacinių išteklių planavimo, eksploatavimo ir plėtros reikalavimai. Nenustatyti bendri reikalavimai, kurie apimtų vieną tikslą, reikšmę ar turinį, ir peržiūrėtų visų galiojančių teisės aktų, kurie reglamentuoja informacinių išteklių IT priemonių valdymą ir saugą. Neplanuojama suderinti valstybės informacinių išteklių steigimo, kūrimo, eksploatavimo, modernizavimo, likvidavimo, duomenų saugos ir kt. reikalavimų,** todėl skirtingų institucijų rengiami teisės aktų pakeitimai gali būti neišsamūs, tarpusavyje nesuderinti, dubliuoti vienas kitą ir nemažinti administracinės naštos Valstybės informacinių išteklių valdymo įstatymą įgyvendinančioms ir kontroliuojančioms institucijoms.

*Pavyzdžiui, **elektroninės informacijos saugos srityje,** atsižvelgiant į Valstybės informacinių išteklių valdymo įstatymo nuostatas Vidaus reikalų ministerija planuoja peržiūrėti ir prireikus patikslinti bendruosius el. informacijos saugos ir kitus šios ministerijos nustatytus reikalavimus el. informacijos saugai, tačiau su šia sritimi susijusius reikalavimus nustato ir kitos institucijos (Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija, Krašto apsaugos ministerija ir kt.), kurių nustatyti reikalavimai nebus peržiūrimi. Be to, VRM neplanuoja peržiūrėti visų galiojančių teisės aktų, kurie reglamentuoja el. informacijos valdymą ir saugą, nors yra tokių, kurie galioja ir nėra peržiūrėti nuo 2004 m.*

Valstybinio audito ataskaitoje pažymima, kad dar viena fragmentiškai reglamentuota sritis, susijusi su visų valstybės informacinių išteklių valdymu – **ypatingos svarbos informacinė infrastruktūra. Susisiekimo ir Vidaus reikalų ministerijos bei kitos institucijos nuo 2006 m. nesutarė dėl el. informacijos saugos (kibernetinio saugumo) įstatymo nuostatų ir jo rengimo tikslingumo**, todėl nenustatyti valstybės ir savivaldybių institucijų, ypatingos svarbos (kritinių) informacinių infrastruktūrų tinklų ir informacijos saugumo valdymo, kontrolės ir priežiūros reikalavimai. Taip pat nenustatytas ypatingos svarbos informacinės infrastruktūros objektų skaičius ir neparengta metodika, kaip juos identifikuoti ir valdyti.

Siekiant numatyti ypatingos svarbos informacinių išteklių ir infrastruktūros kūrimo, saugos, eksploatavimo ir kt. reikalavimus, VRM kartu su kitomis ministerijomis planuoja nustatyti valstybės ypatingos svarbos informacinės infrastruktūros objektus, parengti ir pateikti Vyriausybei nutarimo projektą dėl tokių objektų sąrašo patvirtinimo. Tam, kad būtų užtikrintas visapusis požiūris į ypatingos svarbos informacinę infrastruktūrą, tokiame procese turėtų dalyvauti ne tik viešojo sektoriaus institucijos, bet ir privatus sektorius, kuris valdo ir eksploatuoja ypatingos svarbos informacinės infrastruktūros objektų dalį (pvz.: telekomunikacijų bendrovės, komerciniai bankai ir kt.).

Įgyvendinant Valstybės strateginius dokumentus pastebima, kad **Valstybės informacinių išteklių strateginė plėtra nevientisa,** ji nėra pritaikyta horizontalios valstybės veiklos srities, tokios kaip el. informacijos saugos plėtrai, planavimui ir stebėsenai.

Valstybės informacinių išteklių, IT valdymo ir saugos planavimo dokumentuose vyrauja kiekybiniai rodikliai, apsiribojama sukuriamo rezultato kriterijais. Kai kurie minėtų sričių planavimo dokumentuose numatyti rodikliai nedera tarpusavyje arba bus sunkiai pamatuojami (nebus žinomas tikrasis situacijos pokytis), nes iki šiol nebuvo atliekamas tokių rodiklių vertinimas.

Pavyzdžiui, trijose programose iki 2015 m. numatoma pagerinti el. bendravimo saugumą, tačiau tai matuojama skirtingai:

- *- Lietuvos IVP 2011-2019 m. programa - 1 proc. gyventojų, susidūrusių su saugos problemomis, bendraudami su valstybės ir savivaldybės institucijomis ir įstaigomis;*
- *- Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 m. programa - Lietuvos gyventojų pasitikėjimo kibernetinėje erdvėje teikiamomis paslaugomis lygis (50 proc);*
- *- Ekonomikos augimo veiksmų programa - Interneto vartotojų, kurie pasitiki el. bendravimo su viešosiomis institucijomis saugumu, dalies padidėjimas 12 proc.*

Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 m. programa patvirtinta nenustačius tuometinės šalies kibernetinio saugumo būklės ir neįvertinus tikslaus šios srities raštingumo ir atsargumo lygio. Nesant pirminių duomenų, su kuriais bus lyginami pasiekimai, ir vertinant tokių ambicingų rodiklių kaip „saugią infrastruktūrą naudojančių informacinių išteklių dalis, procentais“ 2015 m. 70 proc, 2019 m. - 100 proc, pasiekimą, nebus žinomas tikrasis situacijos pokytis.

Gyventojų suvokimo arba saugumo jausmo gali neparodyti tokie programoje numatyti rodiklių įvertinimo rezultatai: „Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis, procentais“: 2015 m. 40 proc, 2019 m. 60 proc, ir „Lietuvos gyventojų, suvokiančių kibernetinio saugumo principus, dalis, procentais“: 2015 m. 60 proc, 2019 m. 80 proc.

Pasaulyje pripažintoje gerojoje praktikoje nėra tiksliai išskirta, kokia IT išlaidų dalis privalomai turėtų būti skirta IS saugai užtikrinti, o minėtoje programoje numatytos tikslios procentinės išraiškos (2015 m. 10 proc, 2019 m. 15 proc. nuo visų lėšų, planuojamų skirti IS plėtrai ir palaikymui) ir tai gali sudaryti sąlygas neracionaliai naudoti šiam tikslui skiriamas lėšas, nes stengiantis pasiekti numatytą rodiklį lėšos gali būti naudojamos ne pačioms svarbiausioms priemonėms, o tam, kad būtų pasiektas rodiklis.

Apibendrinant galima teigti, kad, kol nesukurti visoms valstybės valdymo sritims pritaikomi informacinių išteklių, IT valdymo ir saugos vertinimo rodikliai ir kriterijai, tol bendra įgyvendinamų ir planuojamų įgyvendinti priemonių apskaitos sistema, šių sričių plėtra valstybės mastu bus įgyvendinama fragmentiškai, nebus užtikrinama stabili plėtra, nuoseklumas ir darna, o tai sudaro prielaidas lėšas naudoti neefektyviai.

Valstybės audito ataskaitoje pabrėžiama, kad **nenustatyta atsakomybė arba trūksta valstybės informacinių išteklių politiką formuojančių ir įgyvendinančių institucijų kompetencijos atskyrimo formuojant ir įgyvendinant politiką, nė viena valstybės institucija:**

► nevertina, nekaupia ir neturi išsamios informacijos apie valstybinius el. ryšių tinklus, todėl nacionaliniu mastu jie nesaugomi nuo pavojų, nevykdoma jų priežiūra.

► neįpareigota rinkti ir analizuoti informaciją apie informacinių išteklių svarbą pagal kategorijas, nevertina, ar iš tikrųjų taikomos numatytos duomenų saugos priemonės. *Pavyzdžiui, 85 proc. (609 iš 715) valstybės valdomų IS ir registrų nepriskirta kategorija pagal svarbą.*

► neformuoja įslaptintą informaciją apdorojančių informacinių išteklių politikos, sistemiškai nekaupiama informacija apie šių išteklių kiekį ir duomenų mainų intensyvumą, planuojamas, kuriamas ADA sistemas ir tinklus, jų valdytojus, nėra institucijos, kontroliuojančios ADA sistemų steigimo poreikį.

Apibendrinant galima teigti, kad nevientisas šios srities politikos formavimas turi įtakos visai valstybės informacinių išteklių plėtrai – nesuderintos informacinių išteklių strateginės plėtros kryptys, o nustatyti vertinimo kriterijai atskleidžia ne visus informacinių išteklių strateginės plėtros rezultatus. Valstybės sukurti informacinių išteklių politikos įgyvendinimo kontrolės mechanizmai veikia su trūkumais, nėra išsamios ir patikimos informacijos apie šių išteklių kūrimo, tvarkymo, plėtros, saugos ir kt. procesus, neužtikrinamas valstybės informacinių išteklių politikos formavimo nuoseklumas.

3.3.Informacinių išteklių valdymas Žemės ūkio ir Teisingumo ministerijose

Valstybinio audito ataskaitoje „Žemės ūkio ministerijos informacinių išteklių valdymas“ (2013) akcentuojama, kad automatizuodama veiklos funkcijas, ministerija nuo 1996 m. naudoja įvairaus sudėtingumo informacines sistemas, kuriose kaupiami ir apdorojami duomenys, įskaitant ir asmens duomenis.

Ministerija yra 32 informacinių sistemų ir registrų valdytoja, 24 iš jų tvarko, kuria ir modernizuoja ministerijai pavaldi valstybės įmonė Žemės ūkio informacijos ir kaimo verslo centras. Kasmet jo išlaikymui ministerija skiria vidutiniškai po 17.5 mln. Lt. Ministerija teisės aktų numatytoms funkcijoms atlikti naudoja 25 informacinius išteklius: 6 registrus ir 19 informacinių sistemų; o 7 informaciniai ištekliai.

Ministerija yra šių (32) informacinių išteklių valdytoja, didžiosios dalies šių išteklių tvarkymo funkcijas yra perdavusi VĮ Žemės ūkio informacijos ir kaimo verslo centrui, kuris atlieka išteklių kūrimo ir palaikymo darbus. Todėl siekiant įsitikinti ministerijos valdomų registrų ir informacinių sistemų valdymo efektyvumu audito procedūros buvo atliktos ir ŽŪIKVC.

Atlikus Žemės ūkio ministerijos informacinių išteklių valdymo auditą išryškėjo, kad **ministerija neturi savo valdomų informacinių sistemų ir registrų informacijos architektūros modelio ir tikslios informacijos apie savo valdomų informacinių išteklių kiekį. Taigi galima daryti prielaidą, kad ministerija kaip valdytojas neskiria reikiamo dėmesio šiems informaciniams ištekliams.**

Konstatuota, kad ministerija neklasifikuoja valdomos el. informacijos, jai nepriskiriami svarbos kriterijai, todėl gali būti prarasti svarbūs duomenys ir/arba netinkamai paskirstytos šių išteklių valdymui skirtos lėšos.

Žemės ūkio ministerijos informacinių sistemų funkcijų pokyčiai nėra valdomi pagal teisės aktų reikalavimus, nes:

- IT pokyčiai nėra registruojami, vertinami, vykdomi negavus raštiško pritarimo, o po įgyvendinimo jie nėra peržiūrimi ir lyginami su planuotais rezultatais;
- ministerijoje nedokumentuojamas pokyčių inicijavimas, vertinimas, įgyvendinimas, nepildomas keitimų žurnalas;
- ministerija **nėra įvertinusi valdomų informacinių išteklių svarbos ir jų atkūrimo prioritetų, todėl yra rizika, kad įvykus elektroninės informacijos saugos incidentui svarbūs duomenys bus prarasti ar neveiks ypač svarbios sistemos.** LR teisės aktai nustato, kad antros kategorijos IS neveikimo laikotarpis negali būti ilgesnis nei 12 val.23 Audito metu nustatyta, kad ilgiausiai neveikimo trukmė audituojamu laikotarpių buvo 8 val.;
- nesuderinti su Vidaus reikalų ministerija ir nepatvirtinti 2 registrų ir 14 naudojamų informacinių sistemų duomenų saugos nuostatai;

- nėra nustatyta tvarka suderintų su atsakingomis institucijomis ir patvirtintų 6 registrų ir 19 informacinių sistemų saugos politiką įgyvendinančių dokumentų – Veiklos tęstinumo valdymo plano, Naudotojų administravimo taisyklių, Saugaus elektroninės informacijos tvarkymo taisyklių (audito metu buvo parengti projektai, kurie atsakingoms institucijoms pateikti derinti);
- el. informacijos saugos rizikos vertinimas buvo atliekamas ne kasmet (atliktas 2006, 2008 ir 2013 m.), ministerijoje neorganizuojami mokymai el. informacijos saugos klausimais;

Taip pat nustatyta, kad ministerijoje nėra IT saugos klausimus sprendžiančios struktūros, kurią sudarytų svarbiausių veiklos sričių atstovai: pagrindinių ministerijos veiklų, žmogiškųjų išteklių, IT saugos, teisės ir vidaus audito. Audito metu nustatytas saugos procedūrų trūkumas – **neregistruojamas patekimas į ministerijos tarnybinių stočių patalpas ir patalpas, kuriose laikomos atsarginės kopijos, todėl neužtikrinama pakankama šių patalpų apsauga.**

Žemės ūkio ministerijos IT esminiai saugos klausimai sprendžiami Informacinių technologijų priežiūros ir projektų komitete. Pažymima, kad sudarytų komisijų ir darbo grupių, kuriose svarstomi ir IT klausimai nepakanka užtikrinti reikiamą vadovybės dėmesį ir indėlį į IT valdymo ir plėtros klausimus. Siekiant tobulinti ministerijos informacinių išteklių valdymą ir plėtrą, turėtų būti įgyvendintas IT strategijos ir IT valdymo komitetų funkcijų efektyvų vykdymą užtikrinantis struktūrinis sprendimas. Įgyvendinus šiuos sprendimus, būtų sudarytos sąlygos derinti ministerijos pagrindinės veiklos ir IT veiklos poreikius bei tinkamiau derinti IT strateginį planavimą.

Vienas Teisingumo ministerijos veiklos tikslų – formuoti valstybės politiką registrų ir ministro valdymo sričiai priskirtų informacinių sistemų veiklos srityse, organizuoti, koordinuoti ir kontroliuoti šios valstybės politikos įgyvendinimą. Teisingumo ministro valdymo srityje yra visai valstybei ypač didelę svarbą turintys informaciniai ištekliai – valstybės registrai ir valstybės informacinės sistemos. **Ministerija ir teisingumo ministro valdymo sričiai priskirtos įstaigos valdo ir (ar) tvarko 28 informacines sistemas bei registrus ir 1 kadastrą**.

Teisingumo ministerija valdo ypatingos svarbos valstybės informacinius išteklius. 2010–2012 m. IT plėtros priemonės buvo nustatytos ministro valdymo sričiai priskirtų įstaigų veiklos planuose, nuo 2013 m. IT plėtra vykdyta pagal ministerijos valdomų valstybės registrų ir informacinių sistemų viešųjų paslaugų perkėlimo į elektroninę erdvę plėtros 2013–2019 metų veiksmų planą (toliau – 2013–2019 veiksmų planas). Plane numatyti viešųjų paslaugų perkėlimo į elektroninę erdvę tikslai, uždaviniai, modernizuojamų IS ir registrų plėtros prioritetai, planuojamos diegti paslaugos. **Tačiau dokumento turinys neatitinka įstatymo reikalavimų – jame nėra informacijos apie reikalingus finansinius ir žmogiškuosius išteklius, organizacines ir teisines priemones, kvalifikacinius reikalavimus darbuotojams, darbuotojų mokymų poreikį, jų veiklos organizavimą ir kontrolę. Jis apima septynių, o ne įstatymo nustatytą trejų metų laikotarpį.** Pažymėtina, kad planas nuo patvirtinimo dienos nebuvo peržiūrimas ir koreguojamas. Dalies priemonių terminai nenustatyti, tad nėra galimybės įvertinti, kada jos buvo ar bus įgyvendintos. Teisingumo

ministerijoje iki 2014 m. vidurio nebuvo teisingumo ministro valdymo srities IT plėtros plano.

Valstybės informacinių išteklių valdymo įstatyme nustatyti reikalavimai iš dalies įgyvendinti tik 2014 metais, t.y. – 2014-06-18 patvirtintas Teisingumo ministerijos valdomų registrų ir valstybės informacinių sistemų IT plėtros 2014–2016 m. planas (toliau – 2014–2016 IT plėtros planas), tačiau jis apima tik tų pačių dviejų įstaigų – Centrinės hipotekos įstaigos ir VĮ Registrų centro – veiklos sričių IT plėtrą.

Išanalizavus teisingumo ministro valdymo sričiai priskirtų įstaigų 2012–2014 m. veiklos planavimo dokumentus ir metines veiklos ataskaitas nustatyta, kad **beveik visose įstaigose buvo planuojamos, vykdomos ir įgyvendinamos IT plėtros priemonės, kurios nebuvo nurodytos ministro valdymo srities IT plėtros strateginio planavimo dokumentuose**

Pavyzdžiui, ministerijos valdomų valstybės registrų ir informacinių sistemų viešųjų paslaugų perkėlimo į elektroninę erdvę plėtros 2013–2019 metų veiksmų plane nėra informacijos apie Valstybinio patentų biuro viešųjų paslaugų perkėlimą į elektroninę erdvę (2013 m. – 213 tūkst. Lt; 2014 m. – 265 tūkst. Lt), Valstybinės duomenų apsaugos inspekcijos IS pritaikymą aptarnauti duomenų valdytojus ir duomenų subjektus elektroniniu būdu bei jos elektroninių paslaugų sistemos tobulinimą (2008–2013 m. 2 376 tūkst. Lt). Ministerijoje nėra IT strateginio planavimo dokumento, kuriame būtų numatyti ministro valdymo sričiai priskirtose įstaigose suplanuoti IT plėtros darbai: Valstybinio patentų biuro IS diegimas ir modernizavimas, dalyvavimas Europos patentų tarnybos IT plėtros projektuose; Kalėjimų departamento KADIS pertvarkymas (2010–2013 m. 2 244 tūkst. Lt); Lietuvos teismo ekspertizės centro IT ir Valstybinės teismo medicinos tarnybos IS kūrimas ir modernizavimas.

Teisingumo ministro valdymo srities veiklos tikslų perkėlimas į IT plėtros planus ir susiejimas su IT tikslais nėra sklandus, nes **planai nėra suderinti tarpusavyje ir apima ne visas vykdomas veiklas.** 2014–2016 IT plėtros plane numatytos VĮ Registrų centras veiklos, kurių nėra 2013–2019 veiksmų plane, *pavyzdžiui, kuriamos el. paslaugos vykdant Antstolių IS plėtrą, Licencijų IS kūrimą ir kt.*

Ministerija neturi nuoseklios ir išsamios visą valdymo sritį apimančios IT valdymo strategijos, kurioje ministerijos ir ministro valdymo srities veiklos prioritetai bei strateginiai tikslai būtų susieti su visų valdymo sričiai priskirtų įstaigų IT/IS plėtra ir modernizavimu.

Ministerija neturi informacijos apie ministro valdymo sričiai priskirtų institucijų IT plėtrą, nekoordinuoja ministro valdymo srities informacinių išteklių kūrimo ir tobulinimo krypčių, todėl jo valdymo sričiai priskirtos įstaigos sprendimus dėl IT plėtros prioritetų priima savarankiškai, o įstaigų IT būklė ne visada atitinka ministerijos nustatytą plėtros kryptį ir veiklos prioritetus.

Pavyzdžiui, valstybinė teismo medicinos tarnyba savo funkcijoms atlikti kuria IS, kuriose tvarkomi ypatingi asmens duomenys, tačiau nesivadovauja teisės aktais patvirtinta IS kūrimo metodika, sistema kuriama be IS specifikacijos, neparengtos IS pokyčių ir testavimo tvarkos. Vilniaus valstybės garantuojamos teisinės pagalbos tarnyboje, kaip ir kitose mažesnėse ministerijai pavaldžiose įstaigose

pastebima, kad ministerija skiria nepakankamai dėmesio efektyviam IT ūkio valdymui: neužtikrinama fizinė sauga, naudojama IS, kurios tikslai, struktūra ir procesai neaprašyti – IS neįteisinta ir neturi privalomų IS dokumentų). Valstybiniame patentų biure neatnaujinti registrų duomenų saugos nuostatai ir veiklos tęstinumo planas, topografijų registras neturi nuostatų, specifikacijos ir priėmimo akto; dizaino ir patentų registrai neturi specifikacijų ir priėmimo aktų. Nustatyta, kad biure neužtikrinamas išorės auditų rekomendacijų įgyvendinimas (rekomenduota panaikinti tarnybinių stočių patalpų įrengimo trūkumus, tačiau apžiūrėjus šias patalpas nustatyta, kad rekomendacijos nebuvo įgyvendintos).

Išnagrinėjus ministro valdymo sričiai priskirtų įstaigų veiklos planus ir dokumentus, apibūdinančius tose įstaigose esančias IS, technologijas ir kaupiamus bei saugomus duomenis, nustatyta, kad ministerija neturi parengusi ir nesivadovauja ministro valdymo sričiai sudarytu bendruoju informacinių išteklių architektūros modeliu, atitinkančiu valdymo srities sudaromiems IT plėtros planams.

Teisingumo ministerija, valdanti daug valstybės IS ir registrų ir turinti metodiškai vadovauti jų tvarkytojams bei koordinuoti šių registrų ir IS funkcionavimą, **neturi valdymo srities duomenų klasifikavimo sistemos, pagrįstos duomenų svarba ir diskretiškumu (pvz.: vieša, slapta ir pan.) ir tikslios informacijos apie ministro valdymo srityje esančių informacinių išteklių skaičių. Dėl šių priežasčių ministerijoje nėra kontrolės priemonių, padedančių užtikrinti teisės aktais nustatytą el. informacijos (duomenų) konfidencialumą, vientisumą ir prieinamumą.**

Teisingumo ministro valdymo sričiai priskirtose įstaigose planuojamos kurti, kuriamos arba jau sukurtos IS, kuriose kaupiami svarbūs duomenys. Teisingumo ministro valdymo sričiai priskirtos įstaigos kaupia ir tvarko automatizuotu būdu asmens ir kitus veiklai svarbius duomenis neįteisintose IS, kurių tvarkymo priežiūrą turėtų atlikti ir teisingumo ministro valdymo sričiai priklausanti Valstybinė duomenų apsaugos inspekcija.

Pavyzdžiui, Lietuvos teismo ekspertizės centre ir Valstybinėje teismo medicinos tarnyboje nėra el. informacijos klasifikatorių, nors šiose institucijose tvarkomi kitoms institucijoms ir gyventojams svarbūs duomenys apie nukentėjusius, mirusius asmenis, saugomi serologinių, DNR, toksikologinių ir kt. tyrimų duomenys bei atliktų ekspertizių rezultatai.

Siekiant išvengti galimų informacijos viešinimo ir perdavimo problemų, su kuriomis ministerija susidūrė 2011 m., kai Baltarusijos institucijoms buvo perduoti duomenys apie šios šalies piliečio banko sąskaitas, ministerijai reikėtų nustatyti visos valdymo srities el. informacijos klasifikavimo ir apsaugos kontrolės priemones. Ministerija galėtų pritaikyti IVPK rekomenduojamą Informacinių technologinių paslaugų valdymo metodiką ir inventorizuoti visas valdymo srities IT priemones, nustatyti jų santykį su konkrečiais veiklos tikslais. Tai užtikrintų pakankamą ministerijos dėmesį visiems valdymo srities IT poreikiams.

Taip pat ministerijoje ir ministro valdymo srityje yra trūkumų nustatant ir įgyvendinant duomenų valdymo, IT saugos ir priežiūros atsakomybes: ji neturi struktūros, kuri būtų atsakinga už IT saugą, pavaldžių institucijų IT saugos ministerijoje taip pat niekas nekuruoja; paskirti ne visų ministerijai pavaldžių institucijų duomenų valdymo ir saugos įgaliotiniai, nepaisant to, kad įstaigos tvarko ir saugo svarbius duomenis. Dėl šių priežasčių tokių informacinių išteklių plėtros, saugos politikos įgyvendinimo nekoordinuoja ir nekontroliuoja ne tik ministerija, bet šios galimybės neturi ir įstaigų vadovai.

Pavyzdžiui, *audito metu ministerija nurodė, kad IT sauga rūpinasi Strateginio valdymo departamento Projektų įgyvendinimo ir koordinavimo skyrius. Išnagrinėjus funkcijas ir vykdytas veiklas, nustatyta, kad šis skyrius neturi nieko bendra su IT saugos užtikrinimu. Kai kuriose ministerijai pavaldžiose įstaigose IT aptarnauja ne IT specialistai, o darbuotojai, kurie savanoriškai domisi IT sritimi: Lietuvos teisės institute IT prižiūri jaunesnysis mokslo darbuotojas, kurio pagrindinė funkcija – rašyti mokslinius straipsnius. Europos teisės departamente IT prižiūri darbuotojas, kurio pagrindinės funkcijos yra viešųjų pirkimų organizavimas ir departamento ūkio priežiūros organizavimas. Atliekant darbus, reikalaujančius didesnės IT srities išmanymo, kviečiami specialistai iš kitų įstaigų. Valstybinėje vartotojų teisių apsaugos tarnyboje už veiklos tęstinumą, IS atstatymą ir saugą atsakinga trečioji šalis, bet nėra darbuotojo, kuris būtų atsakingas už šios srities priežiūrą ar veiklų koordinavimą, nėra IS atliekamų veiksmų darbo vietose atsekamumo.*

Siekdama užtikrinti sistemingą valdymo srities informacinių išteklių plėtrą ir jų saugos užtikrinimą, ministerija turėtų nustatyti už duomenų ir informacijos saugos reikalavimų laikymąsi atsakingus asmenis, koordinuoti šių veiklų vykdymą ir vykdyti jų priežiūrą.

Apibendrinant galima teigti, kad įvertinus Žemės ūkio ir Teisingumo ministerijų valdomų registrų ir IS sauga yra nepakankama, nes nesuderinti su Vidaus reikalų ministerija ir nepatvirtinti vieno registro ir keturių naudojamų IS duomenų saugos nuostatai; nėra nustatyta tvarka suderintų su atsakingomis institucijomis ir patvirtintų kadastro ir šešių IS saugos politiką įgyvendinančių dokumentų – Veiklos tęstinumo valdymo plano, Naudotojų administravimo taisyklių, Saugaus elektroninės informacijos tvarkymo taisyklių; rizikos vertinimas buvo atliekamas VĮ Registrų centre, Centrinėje hipotekos įstaigoje ir Valstybiniame patentų biure, o Teisingumo ministerijoje ir kitose pavaldžiose įstaigose toks vertinimas kasmet neatliktas, ministerijoje neorganizuojami mokymai el. informacijos saugos klausimais. Ministerijose nėra IT saugos klausimus sprendžiančios struktūros, kurią sudarytų svarbiausių veiklos sričių atstovai: pagrindinių ministerijos veiklų, žmogiškųjų išteklių, IT saugos, teisės ir vidaus audito. Nustatyta ir kitų saugos procedūrų trūkumų – ministerijoje ir kai kuriose jai pavaldžiose įstaigose neužtikrinamas IS ir kompiuterizuotose darbo vietose atliktų veiksmų atsekamumas, nenustatyti svarbiausi (kritiniai) IT procesai ir ištekliai, todėl neužtikrinamas tvarkomų duomenų patikimumas ir jų apsauga.

IŠVADOS

1. Šiuolaikinių viešojo valdymo įstaigų veiklos modernizavimas skatina informacinių technologijų plėtrą, informacijos perkėlimą į elektroninę erdvę. Tai didina viešojo valdymo veiklos kokybę, užtikrina geresnį konkurencingumą bei efektyvumą. Viešajame valdyme elektroninė valdžia yra priemonė įgyvendinti valstybės valdymo reformą. E-valdžia – tai tam tikras demokratinis mechanizmas, nes ji susijusi su viešosios informacijos procesais, pilietinės informacijos sklaida. Ji sudaro optimalias prielaidas valdžios struktūrų našumo gerinimui, efektyvaus ir operatyvaus viešosios informacijos teikimui gyventojams bei sprendimų priėmimui. Elektroninė paslauga yra būdas lengviau bendradarbiauti valstybei ir žmonėms, ji teikiama nuotoliniu būdu, naudojant elektronines priemones.

2. Požiūris į informacijos saugumą iš esmės evoliucionavo – nuo siauro informacijos saugumo supratimo kaip tik grynai technologinės problemos iki plačios informacijos saugumo valdymo suvokties. Išskiriami informacijos saugumo valdymo aspektai: strateginis, žmogiškojo veiksnio ir technologinis. Kibernetinis incidentas – tai įvykis, kuris sutrikdo, pakeičia arba perima informacinės sistemos veikimą, gali sudarkyti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę ja naudotis, taip pat sudaryti sąlygas pasisavinti neviešą elektroninę informaciją tokios teisės neturintiems asmenims. Kibernetinis saugumas valstybėms tampa vienu iš pagrindinių tikslų, nes grėsmės elektroninėje erdvėje kyla ne tik atskiriems vartotojams, bet net valstybėms, todėl reikalingas glaudesnis Europos Sąjungos šalių narių bendradarbiavimas kovojant su nusikaltimais elektroninėje erdvėje, taip pat užtikrinant apsaugą nuo kibernetinių išpuolių.

3. Įvertinus kibernetinio saugumo užtikrinimą viešajame valdyme išryškėjo:

- Lietuvoje priimtas Kibernetinio saugumo įstatymas yra teigiamas žingsnis reglamentuojant kibernetinį saugumą. Tačiau įstatyme neaptarti institucinės kontrolės bei politikos formavimo kibernetinio saugumo srityje klausimai;
- Įstatyme pasigendama kibernetinių incidentų valdymo „vieno langelio principu“, nes atskiros institucijos priklauso įvairioms ministerijoms;
- Įkurtas Nacionalinis kibernetinio saugumo centras tapo pagrindiniu kibernetinio saugumo politikos įgyvendinimo subjektu, jo dėmesys yra sutelktas valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros kibernetiniam saugumui.
- Valstybės informacinių išteklių valdyme nesuderintos informacinių išteklių strateginės plėtros kryptys, o nustatyti vertinimo kriterijai atskleidžia ne visus informacinių išteklių strateginės plėtros rezultatus.
- Valstybės sukurti informacinių išteklių politikos įgyvendinimo kontrolės mechanizmai veikia su trūkumais, nėra išsamios ir patikimos informacijos apie šių išteklių kūrimo, tvarkymo,

plėtros, saugos ir kt. procesus, neužtikrinamas valstybės informacinių išteklių politikos formavimo nuoseklumas.

- Analizuotos ministerijos neturi valdymo srities duomenų klasifikavimo sistemos, pagrįstos duomenų svarba ir diskretiškumu (pvz.: vieša, slapta ir pan.), nėra kontrolės priemonių, padedančių užtikrinti teisės aktais nustatytą el. informacijos (duomenų) konfidencialumą, vientisumą ir prieinamumą.

LITERATŪRA

1. Atkočiūnienė, Z. O., Janiūnienė, E. (2013). Informacijos valdymas viešajame sektoriuje: Lietuvos ministerijų atvejis. *Informacijos mokslai*, 64, 35-36.
2. Barcevičius, E. (2008). Viešasis valdymas ir informacinės technologijos. Naujo institucinio modelio link? *Politologija*, 1 (49), 88.
3. Basie Von Solms (2006). Information Security - The Third Wave?Journal Computers & security Volume 25, http://www.sciencedirect.com/science/article/pii/S016740480600054X 165-168, [žiūrėta 2015 03 15].
4. Buškevičiūtė, J., Raipa, A. (2011). Sprendimai šiuolaikinio viešojo valdymo evoliucijoje. *Viešoji politika ir administravimas*, T.10, Nr.1, 17-26.
5. CERT-LT apibendrina III ketvirčio veiklą. https://www.cert.lt/doc/2009_3.pdf [žiūrėta 2015 03 15].
6. Cybersecurity Strategy for Germany [interaktyvus]. 2011 [žiūrėta 2015-04-20]. <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile>.
7. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for A European Policy Approach. COM/2001/298 [interaktyvus]. Briuselis, 2001 [žiūrėta 2015-04-20]. < http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf>.
8. Damirova, I., Šnapštienė, R. (2005). Viešojo administravimo stebėsenos sistemos problemos ir perspektyvos. *Viešoji politika ir administravimas*, Nr. 11.
9. Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo. Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796.
10. Dunleavy, P., Margetts, H., Bastow, S., Tinkler, J. (2006). *Digital Era Governance: IT Corporations, the State and E-government*. New York: Oxford University Press.
11. Elektroninės valdžios Lietuvoje būklė ir perspektyvos (2006). Prieiga per internetą www.lrinka.lt [žiūrėta 2014 12 05].
12. European Commission. The Role of eGovernment for Europe's Future. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Brussels, 26 9 2003 COM (2003) 567 final.
13. Federal Information Security Management Act (FISMA) (2002). http://www.dhs.gov/federal-information-security-management-act-fisma [žiūrėta 2015 03 15].
14. France information systems defence and security strategy [interaktyvus]. 2011 [žiūrėta 2013-05-20]. <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>.
15. GAO: 2010 Census Operations Successful, But Fundamental Design Needs Reform (2010) http://www.pewsocialtrends.org/2010/12/15/gao-2010-census-operations-successful-but-fundamental-design-needs-reform/ [žiūrėta 2015 03 15].

16. Gaulė, E. (2014). Sumanus viešasis valdymas: samprata ir dimensijos. *Viešoji politika ir administravimas.* T.13, Nr.3, 372-373.
17. Health Insurance Portability and Accountability Act (1996). http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/hipaalaw.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf [žiūrėta 2015 03 15].
18. Informacinės technologijos Lietuvoje, 2012 m. Lietuvos statistikos departamentas.
19. Informacinės technologijos Lietuvoje, 2012 m. LR Statistikos departamentas. <http://www.stat.gov.lt/lt/catalog/download_release/?id=3880&download=1&doc=2209&PHPSESSID=f12624f793ff17933b9028970250131e>) [žiūrėta 2015 03 15].
20. Infosecurity Europe 2010: Data integrity attacks to become more common, say experts (2010).http://www.computerweekly.com/news/1280092630/Infosecurity-Europe-2010-Data-integrity-attacks-to-become-more-common-say-experts [žiūrėta 2015 03 15].
21. Janeliūnas, T. (2007). *Komunikacinis saugumas*. Vilnius: VU leidykla.
22. Jastiuginas, S. (2011). Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. *Informacijos mokslai*, 57.
23. Joint Communication to the European Parliament, the Council, the European Ecomonic and Social Committee and the Committee of Regions „Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/1 final [interaktyvus]. Briuselis, 2013 [žiūrėta 2015-04-20]. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667>.
24. Jokantas, K. (1995). *Lotynų – lietuvių kalbos žodynas*. Vilnius, 23.
25. Kiškis, M., Petrauskas, R., Rotomskis, I., Štitilis, D. (2006). *Teisės informatika ir informatikos teisė.* Vilnius: Mykolo Romerio universitetas.
26. Komisijos komunikatas Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Saugios informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas“.COM/2006/251 [interaktyvus]. Briuselis, 2006 [žiūrėta 2015-04-20]. <http://eurlex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,lt&lng2=cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,nl,pl,pt,sk,sl,sv,&val=427504:cs>.
27. Lietuva: 2013 m. Nacionalinė reformų darbotvarkė (2013). Vilnius<http://ec.europa.eu/europe2020/pdf/nd/nrp2013_lithuania_lt.pdf>). [Žiūrėta: 2014-11-20].
28. Lietuvos nacionalinė informacinės visuomenės plėtros koncepcija. 2001 m. vasario 28 d. Nr. 229. Vilnius. Valstybės žinios, 2001-03-07, Nr. 20-652
29. Lietuvos Respublikos Vyriausybė Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose, 1997 rugsėjo 4 d. Nr. 952, Vilnius.
30. Lietuvos Respublikos Kibernetinio saugumo įstatymas. 2014 m. gruodžio 11 d. Nr. XII-1428. Vilnius.
31. Lietuvos Respublikos Seimas. Nutarimas dėl valstybės pažangos strategijos „Lietuvos pažangos strategija „Lietuva 2030“. Valstybės žinios, 2012-05-30, Nr. 61-3050

32. Lietuvos Respublikos Vyriausybė Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo. 2001 m. gruodžio 22 d. Nr. 1625, Vilnius.
33. Lietuvos Respublikos Vyriausybė nutarimas Dėl viešojo valdymo tobulinimo 2012–2020 metų programos patvirtinimo 2012 m. vasario 7 d. Nr. 171, Vilnius.
34. Lietuvos Respublikos Vyriausybė. Nutarimas dėl 2014–2020 metų nacionalinės pažangos programos patvirtinimo. 2012 m. lapkričio 28 d. Nr. 1482, Vilnius.
35. Lietuvos Respublikos Vyriausybės 2006 m. gruodžio 6 d. nutarimas Nr. 1211 „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“. Valstybės žinios. 2006, Nr.134-5081
36. Lietuvos Respublikos Vyriausybės nutarimas dėl elektroninės valdžios koncepcijos patvirtinimo. 2002 m. gruodžio 31 d. Nr. 2115, Vilnius
37. Limba, T. (2007). Elektroninės valdžios diegimas ir perspektyvos Lietuvoje: visuomenės ir valdžios institucijų sąveika. *Informacijos mokslai*, 42-43, 242 -243.
38. LR Vyriausybės nutarimas „Dėl viešojo valdymo tobulinimo 2012-2020 metų programos patvirtinimo“. Valstybės žinios, 2012-02-18, Nr. 22-1009. <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=418407&p_query=vie%F0ojo%20valdymo%20tobulinimo%20programa&p_tr2=2> [žiūrėta 2014 12 05].
39. Mankevičius V. MA Technikos mokslų skyrius surengė diskusiją „Kibernetinis saugumas“ diskutavo G. Dzemyda, L. Telksnys, G. Žintelis, V. Razumas. http://www.mokslasirtechnika.lt/mokslo-naujienos/lma-technikos-moksl-skyrius-sureng-diskusija-kibernetinis-saugumas.html [žiūrėta 2015 03 15].
40. McKinney, J. B; Howard, L. C. (1998). *Public administration, Balancing Power and Accountability.* Second Edition, 62.
41. Mikalauskienė, A., Brazaitis, Z. (2010). *Informacinių sistemų sauga*. Vilnius: VU leidykla.
42. Nacionalinė elektroninės informacijos saugos, kaip kibernetinio saugumo, plėtros 2011-2019 m. programa.2012 metais birželio 29 d.
43. Nott, Ch. (2011). *Cyber Security: Protecting the Public Sectos*. IBM Institute for Advanced Security. https://www-304.ibm.com/easyaccess/fileserve?contentid=224109 [žiūrėta 2015 03 15].
44. Parker, B. Donn (1981). *Computer Security Management*. Reston, VA: Reston Publishing Company Inc.
45. Pasaulio banko vartojamas apibrėžimas, pateikiamas šios institucijos interneto svetainės skyriuje, skirtame e. valdžios klausimams. www1.worldbank.org/ publicsector/egov [žiūrėta 2015 03 15].
46. Paulauskas, N. (2009). *Incidentų kompiuterių sistemose tyrimas ir saugumo lygio įvertinimas*. Daktaro disertacija. VGTU. Vilnius: Technika.
47. PCI SSC Data Security Standards Overview (2008). https://www.pcisecuritystandards.org/security_standards/ [žiūrėta 2015 03 15].
48. Petrauskas et al. (2006). International Legislative Regulation Provisions Concerning the Security of Information Systems and Information. Implementation of the Provisions in Lithuania. - *Databases and Information Systems: Seventh International Baltic Conference on Databases and Information Systems. Communications, Materials of Doctoral Consortium.* Vilnius, Technika.

49. Prieš Sony svetaines įvykdytos masinės DDoS atakos (2011). interaktyvus. http://webtechnologijos.blogas.lt/pries-sony-svetaines-ivykdytos-masines-ddos-atakos [žiūrėta 2015 03 15].
50. Raipa, A. (2002). Viešoji politika ir viešasis administravimas: raida, struktūra ir sąveika. *Viešoji politika ir administravimas*, Nr. 1, 14.
51. Rosenbloom, D. H. (1986). *Public administration. Understanding Management, Politics, and Law in the Public Sector*. New York: Random house.
52. Schjolberg ir Ghernaouti-Hele (2011). A Global Treaty on Cybersecurity and Cybercrime, Geneva. [Žiūrėta: 2014-11-20]. Prieina per internetą: http://www. Cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_cybercrime<_Sekond_edition_2011.pdf.
53. Štitilis D. ir Klišauskas, V. (2012). Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai. *Socialinės technologijos* Nr. 2(2), 441-455.
54. Štitilis D., Paškauskas, Ž. (2007). Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Jurisprudencija* 2 (92), 37-46.
55. Štitilis, D. (2013). Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos. *Socialinės technologijos*, 3(1), 189-207.
56. Towards Understanding Diagnostic Work During the Detection and Investigation of Security Incidents. In. www.cscan.org/openaccess/?id=26 [žiūrėta 2015 03 15].
57. U.S. Securities and Exchange Commission. (2002). The Laws That Govern the Securities Industry. http://www.sec.gov/about/laws.shtml#sox2002. [žiūrėta 2015 03 15].
58. UK cybersecurity strategy. Protecting and promoting the UK in a digital world [interaktyvus]. 2011 [žiūrėta 2015-04-20]. <http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf>.
59. Valstybinio audito ataskaita Teisingumo ministerijos informacinių išteklių valdymas (2013).
60. Valstybinio audito ataskaita Žemės ūkio ministerijos informacinių išteklių valdymas (2013).
61. Valstybinio audito ataskaita. Valstybės informacinių išteklių valdymas. 2013 m. Sausio 31 d. Nr. Va-p-90-3-3 Vilnius.
62. Viešojo valdymo tobulinimo 2012-2020 m. programa. Viešosios politikos ir vadybos institutas, LR Vidaus reikalų ministerija, 2013.
63. Viešosios politikos ir vadybos institutas. LR Vidaus reikalų ministerija. Viešojo administravimo tobulinimo tendencijos: Lietuvos ir Europos šalių vertinimas (2013). Galutinė ataskaita.
64. Werlinger, R. et al. (2009). Towards Understanding Diagnostic Work During the Detection and Investigation of Security Incidents. Proceedings of the Third International Symposium on Human Aspects of Information Security & Assurance (HAISA). http://lersse-dl.ece.ubc.ca/record/208/files/208.pdf [žiūrėta 2015 03 15].