

MYKOLO ROMERIO UNIVERSITETAS

**SOCIALINIŲ TECHNOLOGIJŲ FAKULTETAS
SKAITMENINIŲ TECHNOLOGIJŲ INSTITUTAS**

KORNELIJA PRAKAPAVIČIENĖ

Naujų technologijų teisė

**TECHNOLOGIJŲ KONVERGENCIJOS ĮTAKA
ELEKTRONINĖS VALDŽIOS
TEISINEI APLINKAI**

Magistro baigiamasis darbas

Darbo vadovas -

Prof. dr. Mindaugas Kiškis

Vilnius, 2014

Turinys

IVADAS	3
I. TECHNOLOGIJŲ KONVERGENCIJOS REIŠKINYS	5
1.1. Technologijų konvergencijos reiškinio paplitimas ir jo definicijos	5
1.2. Technologijų konvergencijos skiriamieji bruožai	12
1.2.1. Elektroninių ryšių tinklai	12
1.2.2. Galinių įrenginių objektai	13
1.2.3. Elektroninis identifikavimas	14
1.2.4. Programinė įranga, mobiliosios aplikacijos.....	15
1.3. Technologijų konvergencijos reiškinys viešajame administravime.....	16
II. TECHNOLOGIJŲ KONVERGENCIJOS ĮTAKA E. VALDŽIOS PLĖTRAI: STRATEGINIŲ DOKUMENTŲ ANALIZĖ	24
2.1. Technologijų konvergencijos reiškinys strateginiuose ES e. valdžios dokumentuose ..	24
2.2. Lietuvos e. valdžios strateginiai dokumentai, skaitmeninė aplinka ir gairės	30
III. SPECIALAUS TEISINIO REGULIAVIMO PAVYZDŽIAI	37
3.1. Informacijos saugos teisiniai aspektai Valstybės informaciniuose ištekliuose	37
3.2. Kibernetinio saugumo teisinis reglamentavimas ES ir Lietuvoje	42
3.3. Asmens duomenų apsaugos teisiniai aspektai.....	47
3.4. Teisinis reguliavimas ateityje ir rekomendacijos.....	51
IV. IŠVADOS	55
LITERATŪRA	57
SANTRAUKA.....	62
SUMMARY	63
Priedai	64
1 priedas. Plačiajuostės interneto prieigos technologijų suvestinė	64
2 priedas. Galinių įrenginių pavyzdžiai.	65
3 priedas. Saugumo spragų klasifikacija konverguojančiais įrenginiais.....	66
4 priedas. Informacijos saugą reglamentuojantys teisės aktai	67

IVADAS

Informacinės visuomenės raidoje tobulėjant technologijoms vis mažiau reikšmės turi atstumas ir laikas, vienos technologijos keičia kitas, jos spartėja, mažėja apimtimi, pinga, tampa patogesnės naudoti, vienu įrenginiu galima atlikti kelias funkcijas, gauti kelias paslaugas skirtingais formatais. Šiems veiksniams apibrėžti atsirado „technologijų konvergencijos“ sąvoka. „Technologijų konvergencijos“ sąvoka aiškinama labai plačiai¹, ji naudojama apibrėžti **susiliejimo** (suartėjimo, supanašėjimo) reiškiniui tarp įrenginių, tinklų, paslaugų, mokslo sričių, rinkų ir pan. Dažniausiai „technologijų konvergencijos“ sąvoka taikoma, apibūdinant žiniasklaidos, telekomunikacijų ir informacinių technologijų sektorių susiliejimui, tačiau ji betarpiškai sąveikauja su kitomis sąvokomis kaip „galinių įrenginių konvergencija“ (kai pavyzdžiui išmaniuoju telefonu galima atlikti kitų įrenginių funkcijas ar valdymą) ir „paslaugų konvergencija“ (skaitmeninio turinio susiliejimui, kai pavyzdžiui pranešimus galima pateikti ar gauti skirtingu formatu (tekstu, vaizdu, garsu) ir pan.). Darbe šiame platesniame kontekste ir bus nagrinėjami suformuluoti **uždaviniai**:

1. Išanalizuoti technologijų konvergencijos reiškinį visuomeniniame gyvenime, moksle ir viešajame administravime bei išskirti jam būdingus bruožus.
2. Atlikti ES ir Lietuvos informacinės visuomenės plėtros teisinės bazės analizę, kuri leistų įvertinti technologijų konvergencijos reiškinio įtaką viešojo administravimo modernizavimui ir elektroninės valdžios plėtrai.
3. Identifikuoti ir išanalizuoti teisinio reglamentavimo problemas, kurios iškyla dėl technologijų konvergencijos įtakos kibernetinio saugumo bei asmens duomenų apsaugos kontekste, pateikti rekomendacijas.

Konvergencijos reiškinį lemia technologijų ir mokslo spartėjanti pažanga, apimanti vis daugiau gyvenimo sričių, kas rodo šio reiškinio aktualumą, paplitimą, naudojimą, svarbą. Nors ši pažanga daro mūsų gyvenimą patogesnį, tačiau kartu renka didžiulius kiekius asmens duomenų, taip įgalindamos nuolatinį skaitmeninį stebėjimą, dažnai vartotojui net nežinant, kad tai vyksta ir kam jo duomenys naudojami. Akivaizdu, kad tai turi įtakos ne tik pasitikėjimui naujomis technologijomis, bet ir skatina elektroninių nusikaltimų atsiradimą. Darbe bus nagrinėjamas technologijų konvergencijos reiškinys ne kaip visuma, bet tik tiek, kiek reikalinga atskleisti jo sąsajas su elektronine valdžia, kad suvokti įtaką elektroninės valdžios pasirengimui kurti efektyvų valdymą, patikimą aplinką elektroninių paslaugų teikimui.

Šio darbo **pirmoji dalis** skirta „konvergencijos“ ir „technologijų konvergencijos“ reiškinių analizei: pateikiami lietuvių ir užsienio mokslininkų darbų, susijusių su šiuo reiškiniu įžvalgos,

¹ Interneto paieškos sistema google.com pasiūlo virš 31 mln. nuorodų į šaltinius pagal žodžių junginį „technological convergence“, „Converging technologies“ - 161 tūkst., „digital convergence“ - 575 tūkst., „convergence“ - virš 17 mln.

naudojamos definicijos, išskiriami jo esminiai bruožai. Didžioji dalis skiriama analizei, kaip technologijų konvergencija veikia viešojo valdymo sritį bei elektroninių projektų įgyvendinimo rezultate įdiegtas elektroninių paslaugų integruotas platformas, saugumo sprendimus.

Antroje dalyje atliekama strateginių teisinių dokumentų, reglamentuojančių Europos Sąjungos, Lietuvos viešojo sektoriaus informacinių technologijų plėtrą, elektroninės valdžios projektų įgyvendinimą, analizė, aptariamos e. valdžios prioritetų gairės, kryptys ir tikslai, pateikiama numatomų e. valdžios priemonių analizė, tiriamos sąlygos jų įgyvendinimui. Pateikiama Lietuvos skaitmeninės aplinkos apžvalga, kuri parodo situaciją bei prielaidas technologijų konvergencijos plėtrai, apžvelgiami ateities scenarijai.

Trečioje dalyje nagrinėjami specialaus teisinio reglamentavimo pavyzdžiai, informacijos saugumo problemos, su kuriomis konverguojant technologijoms susiduria viešasis sektorius, aptariamos dvi teisinio reglamentavimo sritys: kibernetinis saugumas ir asmens duomenų apsauga.

Darbo tikslas. Išanalizuoti technologijų konvergencijos proceso ypatumus ir tendencijas, nustatyti kokią įtaką šis procesas turi viešojo administravimo modernizavimui, informacinės visuomenės ir elektroninės valdžios plėtrai, bei pateikti technologijų konvergencijos poveikio teisei aplinkai įvertinimą, analizuojant kibernetinio saugumo bei asmens duomenų teisinės apsaugos atvejus.

Hipotezė:

Technologijų konvergencija įtakoja viešojo administravimo modernizavimą per e. valdžios projektais įgyvendinamus integruotus veiklos bei elektroninių paslaugų centralizuotus sprendimus, tuo pačiu iškelia naujų teisinių grėsmių kibernetiniam saugumui bei asmens duomenų apsaugai.

Darbe atlikus išsamią teisinės bazės, reglamentuojančios Lietuvos bei Europos Sąjungos viešojo sektoriaus informacinių sistemų plėtrą, analizę, siekiama įvertinti, kokį informacinių sistemų, elektroninių paslaugų ir jų teisinio reglamentavimo brandos lygį Lietuva jau pasiekė ir ką reikėtų tobulinti, kad technologijų konvergencijos proceso plėtra būtų suderinta su esamais duomenų apsaugos teisiniais principais, būtų vartotojui patraukli ir patikima, o viešasis sektorius galėtų ir sugebėtų užtikrinti saugią elektroninės valdžios aplinką, skatinant interaktyvų bendravimą, pažangiais metodais pagrįstą sprendimų priėmimo procesą bei savalaikiai reaguotų į naujus saugumo iššūkius. Pasirinktų uždavinių sprendimui naudojami tyrimo metodai: pirminių ir antrinių duomenų šaltinių analizė, mokslinės literatūros studijavimas ir analizė, palyginamosios analizės metodai. Darbas naudingas tiek mokslinė tiek praktinė prasme visiems besidomintiems naujų informacinių technologijų integracija, kurios suteikia daug privalumų gauti elektronines paslaugas patogesniu būdu. Taip pat darbas padės didinti visuomenės supratimą apie teises problemas, kurias kelia technologijų konvergencija kibernetiniam saugumui bei asmens duomenų apsaugai.

I. TECHNOLOGIJŲ KONVERGENCIJOS REIŠKINYS

1.1. Technologijų konvergencijos reiškinio paplitimas ir jo definicijos

Informacinėje visuomenėje pastaruoju metu technologinė pažanga yra itin ženkli, kadangi informacinės ir ryšių technologijos (toliau – IRT) įžengia į visuotinio pritaikymo etapą, kuris iš esmės keičia žmonių darbo, mokslo, gyvenimo ir bendravimo būdą. Didelis informacijos kiekis tampa prieinamas naujais, įvairiais formatais ir gali būti pateiktas nepriklausomai nuo vietos ir laiko bei pritaikomas pagal atskirų asmenų poreikius naudotis naujausiomis technologijomis. Technine prasme vyksta ryšių tinklų, visuomenės informavimo priemonių, turinio, paslaugų ir įrenginių skaitmeninė konvergencija². Šioje darbo dalyje iš pradžių bus apžvelgiama kaip „konvergencija“, „technologijų konvergencija“ suprantama atskirose mokslo, darbo bei gyvenimo srityse, pateikiama jos pavyzdžių, kad labiau suvokti patį reiškinį ir jo paplitimą.

Biologijoje konvergencija suprantama kaip „negiminingų organizmų grupių išorinių požymių ir sandaros supanašėjimas per jų evoliuciją dėl panašių gyvenimo sąlygų³“. Konvergentinė evoliucija - evoliucijos procesas, kurio metu negiminingos organizmų grupės įgyja panašių bruožų. Dėl tokio proceso rūšys įgauna konvergentišką panašumą, tai yra panašumą, kuris remiasi ne jų giminingumu, o bruožais susiformavusiais nepriklausomose grupėse⁴.

Geofizikoje konvergencijos sąvoka sutinkama apibūdinant „oro masių suartėjimą⁵“.

Konvergencija **geografijoje** naudojama kai kalbama apie vandenyno srovių sąlytį, pvz., Pasaulinio vandenyno konvergencijos zonos⁶.

Geologijoje - kai kalbama apie tektoninių plokščių judėjimą, t.y. egzistuoja plokščių tarpusavio judėjimo tipai: plėtimasis (divergencija) ir susidūrimas (konvergencija).⁷

Matematikoje - tai artėjimo prie ribos savybė ar būdas⁸.

Konvergencija **meteorologijoje** apibūdina oro masės padidėjimą tam tikrame erdvės taške dėl srauto linijų suartėjimo ar oro judėjimo greičio skirtumų išilgai srauto linijos⁹.

Kalbotyroje sutinkama konvergencija, kai kalbama apie panašių struktūrinių ypatybių atsiradimą tolimos giminytės ar negiminiškose kalbose dėl gretimos teritorijos ar ilgų kontaktų¹⁰.

Kelių atskirų mokslų rūšių tokių kaip **biofizika**, **astrofizika**, **biochemija** ir pan. susilieėjimas taip pat yra nuoroda į konvergencijos reiškinį, tačiau pastebima tendencija, kai IRT vis labiau

² Lietuvos žinių visuomenės plėtros procesų apžvalga // http://archyvas.infobalt.lt/sl/index_lt.php?t=ivpk, [žiūrėta 2013 10 26].

³ <http://www.tzz.lt/k/konvergencija>, [2013 12 26].

⁴ http://lt.wikipedia.org/wiki/Konvergentin%C4%97_evoliucija, [2013 12 26].

⁵ <http://www.tzz.lt/k/konvergencija>, [2013 12 26].

⁶ <http://www.tzz.lt/k/konvergencija>, [2013 12 26].

⁷ http://lt.wikipedia.org/wiki/Plok%C5%A1%C4%8Di%C5%B3_tektonika, [2013 12 26].

⁸ <http://ru.wikipedia.org/wiki/>, [2013 12 26].

⁹ http://www.biogeonauka-a.lt/wp-content/uploads/2012/11/2011_Meteorologijos_ivadas.pdf, [2013 12 26].

¹⁰ <http://www.zodziai.lt/reiksme&word=konvergencija&wid=10556>, [2013 12 26].

spartina svarbiausių įgalinančių technologijų (angl. Key Enabling Technologies) vystymąsi skatindama ne tik jų susiliejimą bet ir naujų mokslo šakų sukūrimą. Šias tendencijas galima pastebėti tokiose srityse, kurios susijusios su **nanotechnologijomis**, **mikro** ir **nano elektronika**, **fotonika**, **biotechnologijomis**, pažangiomis (angl. advanced) medžiagomis¹¹, taip pat, **dirbtiniu intelektu**, **lingvistika**, **robotika**, **neuronų tinklais** ir pan. Technologijų konvergencijos reiškinių galima aptikti mokslinių tyrimų projektuose: "Konverguojančios technologijos natūralios kalbos apdorojimo sistemose", "Konverguojančios technologijos gydant nutukimo problemas", "Konverguojančios technologijos kuriant intelektualų būstą" ir pan.¹²

Dr. APJ Abdulkalam aprašo naujo mokslo - **bioinformatikos** atsiradimą, kuris yra biotechnologijų ir IT kombinacija (IRT, kosmoso ir nanotechnologijų konvergencijos įtaka erdvėlaivių pramonei). Ši technologinė konvergencija leis pastatyti ekonomiškai efektyvių mažo svorio, aukštos naudingosios apkrovos, ir labai patikimas kosmoso sistemas, kurios gali būti naudojamos kaip transporto priemonės tarp skirtingų planetų¹³.

Vilniaus universiteto GMF Neurobiologijos ir Biofizikos katedros prof. biomedicinos mokslų daktaras D. Kirvelis konverguojančių technologijų sąvoką naudoja **naujam visuomenės raidos modeliui** aprašyti: „Industrinei visuomenei keičiantis nauja, kaip gyvas organizmas paradigmine – pagrįsta konverguojančių NBICE (Nano-Bio-Info-Cogno-Eco) technologijų mokslinės kūrybos visuomene – turi keistis ir jos valdymo būdas“¹⁴ ir pateikia jos simbolizuotą schemą (2 pav.).



2 pav. Simbolizuota konverguojančių NBICE technologijų schema. (Nano-biomolekulinių, Bio-genetinių, Info-skaitmeninių, Cogno-psichoneuroninių ir Eco-harmoningai suderintai su gyvąja gamta)¹⁵

¹¹ <http://televizorius.files.wordpress.com/2011/12/samprata-ir-pletros-tendencijos.pdf>, [2013 11 12].

¹² Converging Technologies– Shaping the Future of European Societies http://ec.europa.eu/research/social-sciences/pdf/ntw-report-alfred-nordmann_en.pdf, [2013 10 02].

¹³ Technology in development of civil society // Dr. APJ Abdul Kalam http://www.abdulkalam.com/kalam/jsp/display_searchcontent.jsp?content=775&columnno=0&starts=0&search_for=University%20of%20Toronto&sublink_id=68, [2013 09 26].

¹⁴ D. Kirvelis. Socialmeritokratija versus socialdemokratija, <http://webcache.googleusercontent.com/search?q=cache:LUHI ioVx AJ:web.vu.lt/gf/d.kirvelis/files/2012/01/Socialmeritokratija-red.doc+&cd=2&hl=lt&ct=clnk&gl=lt>, [2013 12 16].

¹⁵ <http://www.kvalitetas.lt/lt/straipsniai/387-2014-02-19-dobilas-kirvelis-apie-nauju-technologiju-ratus-xxi-amziaus-gyvenimui>, [2013 12 16].

Kai kurie mokslininkai, analizuojantys gyvojo pasaulio ir žmonijos raidą, išvelgia tam tikrus dėsningumus, ir kelia idėjas apie „ateinančias kokybiškai kitokias – konverguojančias nano- bio- info- eko (NBICE) žmonių gyvenimo technologijas, kurios yra jau naujos – transhumanizmo arba posthumanizmo ideologijos mokslu pagrįstos technologijos¹⁶. Pavyzdžiui, transhumanistai, vadovaujami Oksfordo universiteto pro. Nick Bostromo, Žmonijos Ateities Instituto direktoriaus, 1998 m. deklaracijoje įvardina 10 pagrindinių technologijų, kurios turėtų pakeisti visuomenę iki 2050 m.: Krionika (žmogaus kūno gyvybinių procesų sustabdymas-užšaldymas), Virtualios Realybės metodai, Genų terapija, Kosminės Erdvės Kolonizavimas, Kibernetika, Autonominiai Savarankiškieji Robotai, Molekulinė Gamyba, Megaerdvinė Inžinerija, Minčių Perdavimas, Dirbtinis Protas. Transhumanistai tvirtina, kad jau kai kuriuos projektus pavyko sėkmingai sukurti, tačiau atviru klausimu išlieka aktuali vertybinė šių projektų pusė: ar naujos technologijos žmonijai tikrai atneš gerį, o ne susinaikinimą, pasitarnaus jos gerovei, o ne priešingai - ves į naujas kančias, ligas ir didesnę atskirtį; ar žmogus netaps priemone tikslams pasiekti ("bioobjektu", "statistiniu vienetu", "darbiniu ištekliumi", pažeminant jo kaip asmens garbę ir orumą), kur baigiasi mokslinių tyrinėjimų ribos ir kas prisiims atsakomybę už mokslinių tyrinėjimų rezultatus ir pasekmes.

Anksčiau taikyta tiksluosiuose moksluose, technologijų konvergencijos sąvoka šiandien įgavo universalią prasmę ir vis dažniau vartojama **informacinėse technologijose, elektroninėje komercijoje, ekonomikoje, teisėje, kultūroje, žiniasklaidoje, viešajame administravime** ir daugelyje kitų gyvenimo, darbo, bendravimo bei mokslo sričių. Konvergencija reiškia technologinių barjerų tarp atskirų sistemų eliminavimą, šių sistemų suderinamumą, kitaip – supanašėjimą, susijungimą, sujimą į vieną tašką¹⁷.

Elektroninėje komercijoje - technologijos byloja apie mobiliojo ryšio įrenginių ir interneto technologijų konvergenciją, rinkų konvergenciją, prekybos būdų konvergenciją. Netgi atsirado nauja sąvoka – mobilusis verslas arba tiesiog m. verslas. E. verslą paskatino kompiuterinio tinklo atsiradimas, o m. verslas prasidėjo, prijungus mobiliuosius telefonus prie skaitmeninių telekomunikacinių tinklų. Geoffrey Sampsono nuomone, e. verslo ateitis turėtų būti m. verslas, naudojantis bevielio ryšio technologijas¹⁸.

Informacinėse technologijose vyksta skaitmeninė konvergencija, t.y. skaitmeninės technologijos sąlygotas iki tol buvusių atskirų sistemų technologinis suderinamumas. IT srityje labiausiai iš paplitusių skaitmeninės konvergencijos pavyzdžių yra vaizdo konferencijos, interneto telefonija, teatrų, filmų perdavimas skaitmeniniu būdu iš platintojo per internetą; mobilieji telefonai

¹⁶ http://www.technologijos.lt/n/zmoniu_pasaulis/redakcijos_akiratis/S-28962/straipsnis/Ateities-visuomene-transhumanizmas-ir-posthumanizmas?l=2&p=1, [2013 11 11].

¹⁷ Karlaitė D. Radijo žurnalistikos ateitis. <http://zurnalistika.jimdo.com/referatai-1/radijo-%C5%BEurnalistikos-ateitis/>, [2013 11 06].

¹⁸ Sampson, Geoffrey. Network Computing, Mobile and Wireless. 2006. p. 177.

su įmontuotais fotoaparatais ir asmeniniai skaitmeniniai asistentai (PDA) su bevielio interneto prieiga.



1 pav. Personalinių kompiuterių raida¹⁹

Televizijos reklamos naudoja technologijų konvergenciją teikiant telefono paslaugas per kabelines bendroves TV elektroninio balsavimo metu. Naudojant technologijų konvergenciją, prietaisai ir periferiniai įrenginiai gali belaidžiu būdu suprasti kitus prietaisus, susikonfigūruoti be žmogaus įsikišimo ir bendrauti su kitais įrenginiais. Spausdintuvai gali aptikti skaitmeninių fotoaparatus ir spausdintuvų vaizdus, išsaugotus juose. PDA gali sinchronizuoti savo turinį į kompiuterį be jungiamųjų laidų. Didelės spartos plačiajuosčio ryšio tinklai leidžia greitai ir lengvai perduoti didelius duomenų kiekius, taikomoji programinė įranga buvo sukurta siekiant suspausti didelius duomenų srautus ir saugiai perduoti juos, o, kompiuterinė įranga buvo sukurta apjungti vieną ar daugiau technologijų ir sukurti naujų metodų ryšį²⁰.

Elektroninių ryšių sektoriaus raidą iššaukė tokie konvergenciją sąlygojantys veiksniai:

1. Nuolatinis nepertraukiamas ryšys, nepriklausantis nuo vietos ar laiko;
2. Įvairių įrenginių ir paslaugų sąveika ir integracija, sudaranti sąlygas integruotoms elektronikos sistemoms, tarpusavyje **besikeičiančiomis** informacija;
3. Vieninga ir visaapimanti adresavimo elektroniniuose ryšiuose sistema, kuri leidžia pasiekti paslaugų gavėją nepriklausomai nuo jo lokacijos, kas sudaro galimybę turėti informaciją apie galinių įrenginių turėtojus, paslaugų gavėjų prisijungimą prie tinklo;
4. Skirtingi paslaugų kokybės lygiai leidžia teikti įvairaus lygio ir formato paslaugas.

Tai nurodo į plataus spektro paslaugų poreikį (balso perdavimą, vaizdo ryšį, duomenų perdavimą). Šių poreikių tenkinimą iliustruoja naujų paslaugų pavyzdžiai: balso perdavimas internetu, atpažinimo galimybės pasiekti paslaugų gavėją naudojant įvairius galinius įrenginius, interneto paslaugos, sujungtos su televizijos paslaugomis ir pan. Šie poreikiai ir tendencijos turėjo įtakos tradiciškai atskirų reguliavimo objektų - transliavimo, telekomunikacijų ir informacinių

¹⁹ Gatautis R. Elektroninio verslo ir elektroninės komercijos samprata ir plėtros tendencijos <http://televizorius.files.wordpress.com/2011/12/samprata-ir-pletros-tendencijos.pdf>, [2013 11 16].

²⁰ Įvadas į skaitmeninę konvergenciją. http://www.texascollaborative.org/SmithModule02/sec1_con.php, [2013 11 26].

technologijų - susiliejimui (**technologijų konvergencijai**). Šis reiškinys sąlygoja **paslaugų konvergenciją**, lemiančią, kad tos pačios paslaugos gali būti teikiamos bet koku elektroninių ryšių tinklu bei skirtingais formatais. Su šiuo reiškiniu glaudžiai siejasi ir **galinių įrenginių konvergencija** (kai tas pats galinis įrenginys gali būti naudojamas įvairaus pobūdžio ir technologijų elektroninėms paslaugoms gauti)²¹.

Kitas ryškus technologijų konvergencijos pavyzdys – **žiniasklaida**. Joje konvergencija reiškiasi barjerų tirpsmu tarp skirtingų technologijų žiniasklaidos – radijo, televizijos, spaudos, interneto²². Dar 1983 m. Ithiel de Sola Pool savo knygoje „Laisvės technologijos“ rašė: „Istoriškai atskirų komunikacijos rūšių konvergencijos paaiškinimas slypi skaitmeninėje elektronikoje. Telekomunikacija, teatras, žinios, tekstas vis dažniau įgauna elektroninį pavidalą, kuri visas komunikacijos rūšis perkelia į vieną bendrą sistemą“²³.

Žemiau pateiktoje lentelėje pateiktos „technologijų konvergencijos“ definicijos iš mokslo darbų, oficialių Europos ir Lietuvos teisės aktų, konferencijų, publikacijų:

Eil.Nr.	TK sąvoka	Autorius, šaltinis	Paaiškinimas
1.	Konvergencija	Kiškis M., Petrauskas R. kt. ²⁴	Konvergencija – žiniasklaidos, telekomunikacijų ir informacijos technologijų sektorių susiliejimas, įskaitant fiksuotųjų, judriųjų, antžeminių ir palydovinių ryšių, ryšių ir vietos nustatymo sistemų susiliejimą. Elektroninėje erdvėje išryškėjo konvergencijos požymiai – elektroniniai ryšiai pakeičia tokius įprastus dalykus kaip telefoną, televiziją, banko biurą, laikraščius, taip pat vartotojiškų sandorių pobūdį.
2.	Konvergencija	V. Šalauskas ²⁵ , Lietuvos Respublikos susisiekimo ministerija	Konvergencijos sąvoka, aiškinama kaip žiniasklaidos, telekomunikacijų ir informacinių technologijų sektorių susiliejimas, įskaitant fiksuotųjų, judriųjų, antžeminių ir palydovinių ryšių bei ryšių ir vietos nustatymo, taip pat lokacijos sistemų susiliejimą.
3.	Technologijų konvergencija	Europos Parlamentas ²⁶	Interneto, mobiliųjų telefonų ir optinio pluošto atsiradimas ir sparti plėtra, pastaraisiais metais vykstanti skaičiavimo, telekomunikacijų ir palydovinių technologijų konvergencija keičianti žmonių bendravimo, įmonių veiklos ir visuomenės ekonominės bei žmogiškosios plėtros planavimo būdus.
4.	Konvergencija	ŽALIOJI KNYGA Pasirengimas visiškam audiovizualinės aplinkos integravimui: augimas, kūrimas ir vertybės /	Konvergenciją galima suprasti kaip laipsnišką tradicinio transliavimo paslaugų ir internetu teikiamų paslaugų jungimąsi. Tai suteikia galimybę ne tik matyti informaciją televizoriaus ekrane naudojant priedėlius, kuriais teikiamas internetinis vaizdo turinys (angl. over-the-top, OTT) bet ir naudotis

²¹ Jarukaitis I. ir kt. Elektroninių ryšių teisė, Vilnius: Eugrimas, 2005.

²² <http://www.csisponline.net/2013/03/20/a-writing-exercise-for-the-public-warren-sack-on-digital-convergence/>, [2014 01 13].

²³ Ithiel de Sola Pool „Laisvės technologijos“, [2014 02 13].

²⁴ Teisės informatika ir informatikos teisė. – Vilnius: Mykolo Romerio Universiteto Leidybos centras, 2006.

²⁵ Elektronika ir elektrotechnika <http://www.ee.ktu.lt/journal/2003/5/Salauskas.pdf>, [2014 03 13].

²⁶ http://circa.europa.eu/irc/opoce/fact_sheets/info/data/policies/industrial/article_7281_lt.htm, [2014 01 17].

		COM/2013/0231 final ²⁷	audiovizualinėmis paslaugomis naudojant asmeninius, nešiojamuosius ar planšetinius kompiuterius, taip pat kitus judriojo ryšio įrenginius.
5.	Skaitmeninių technologijų konvergencija	Žalioji knyga dėl telekomunikacijų, žiniasklaidos ir informacijos technologijų sektorių konvergencijos bei jos reikšmės reglamentavimui COM/97/0623 final ²⁸	...leidžia teikti tradicines ir naujas ryšių paslaugų - balso, duomenų, garso ar vaizdo - skirtingais tinklais. Rinka ieško kaip tradicines paslaugas išplėsti į naujas veiklas ir būdus. Telekomunikacijų, žiniasklaidos ir informacinių technologijų sektoriai ieško konverguojančių produktų ir konverguojančių platformų bei konverguojančių rinkų.
6.	Modernių technologijų susiliejimas, sluoksniavimas, bendradarbiavimas	Žygintas Pečiulis VU Komunikacijos fakulteto Žurnalistikos instituto profesorius humanitarinių mokslų daktaras ²⁹	Modernios technologijos suteikia naujų informacijos pateikimo galimybių, kuriose dažniausiai pabrėžiamos susiliejimo, sluoksniavimo, bendradarbiavimo sąvokos. Šie procesai būdingi ir žiniasklaidos grupių, turinčių įvairios raiškos priemonių (multimedija, plurimedija), ir informacijos pateikimo įvairovės (daugiaterpiškumas, konvergencija, reach media) lygmeniu.
7.	Tinklo ir technologijų sintezė	Narimantas Kazimieras Paliulis, Jolanta Sabaitytė ³⁰	TV, kompiuterių, mobiliojo ryšio įrenginių ir tinklo konvergencija lemia naujų verslo modelių, rinkų ir elektroninių kanalų atsiradimą.
8.	Kompleksinė infrastruktūra	Darius Štītis, Paulius Pakutinskas, Marius Laurinaitis, Inga Dauparaitė ³¹	"...per pastaruosius dešimt metų internetas tapo atskira kompleksine infrastruktūra, kurioje vyksta konvergencija tarp audiovizualinių visuomenės informavimo, leidybos ir telekomunikacinių paslaugų. Ši komunikacijos sistema ne tik skatina jau esančių ir naujų pramonės šakų plėtrą, bet ir suteikia galimybę visuomenei skleisti kultūrą, žinias. Šiandien internetas didina verslo subjektų komercinės galimybes, jį naudojant galima tiesiogiai teikti viešąsias paslaugas , atnaujinti asmeninę ir socialinę veiklą.
9.	Visiškai integruota sistemų ir tinklų visuma	R. Skyrius ir kt. ³²	„... vis daugiau kalbama apie ketvirtosios kartos mobilių ryšių (angl. 4th General Wireless Infrastructures – 4GW). Tai turėtų būti visiškai integruota sistemų ir tinklų (kompiuterių, telefono, radijo ir televizijos) visuma, veikianti interneto protokolo (IP) pagrindu ir teikianti kokybiškas QoS (angl. Quality of Service) bei saugias paslaugas bet kuriuo metu ir bet kurioje vietoje. 4G tinklai numato kabelinių ir bevielių tinklų, visų elektroninių prietaisų (buitinių, vaizdo kamerų, kompiuterių), interneto technologijų, įvairių komunikacijos technologijų (pavyzdžiui Wi-Fi ar WiMax) konvergenciją. 4G korinio ryšio tinklai turėtų veikti 100 Mb/s sparta, o vietiniai Wi-Fi tinklai – net 1Gb/s sparta. Taigi ketvirtosios kartos ryšys apibūdinamas

²⁷ <http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20130231.do>, [2014 02 13].

²⁸ http://ec.europa.eu/avpolicy/docs/library/legal/com/greenp_97_623_en.pdf, [2014 01 22].

²⁹ Pečiulis Ž., Technologinių naujovių iššūkiai ir tradicinės televizijos kaita. Informacijos mokslai. 2006 36.

³⁰ Verslas XXI amžiuje. Elektroninio verslo plėtros kaip tvaraus konkurencinio pranašumo modelis, <http://webcache.googleusercontent.com/search?q=cache:Ak6VHSTfmK0J:www.mla.vgtu.lt/index.php/mla/article/download/mla.2012.34/pdf+&cd=1&hl=lt&ct=clnk>, [2014 01 03].

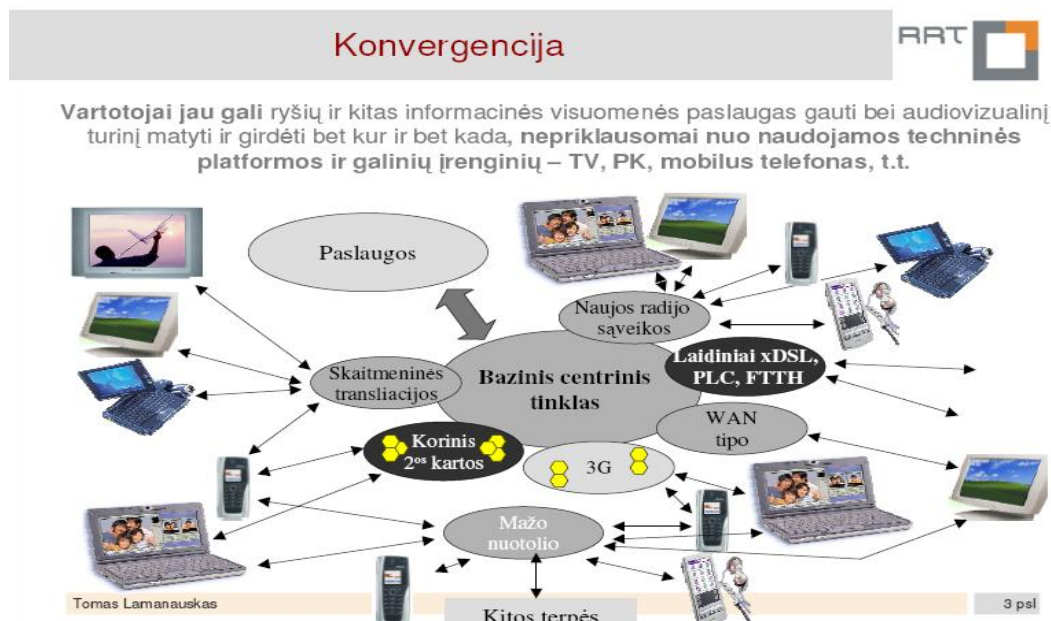
³¹ Štītis D. ir kiti. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai : kolektyvinė mokslo monografija / Mykolas Romeris universitetas. Vilnius : Mykolas Romeris universitetas, 2011

³² R. Skyrius ir kt. „Informacijos ir komunikacijos technologijos“, vadovėlis, 2008 Vilnius, psl. 144

			ne kaip atskira technologija ar standartas, o kaip technologijų ir protokolų rinkinys, skatinantis tolesnę bevielų tinklų pažangą“.
10.	Daugiplatformiškas ir daugialypisumas, technologinio suderinamumo ir sąveikos užtikrinimas.	A. Augustinavičius ir kt. ³³	...pasiekiamumas įvairiais kanalais, per asmeninius kompiuterius, mobiliuosius telefonus, skaitmeninę TV, pasinaudojant bevieliais įrenginiais, kaip antai RFID ³⁴ . Apima tekstą, grafiką, animaciją, vaizdo ir garso įrašus. Bendras informacijos sistemų, registrų ir duomenų bazių veikimas.

1 lentelė. Technologijų konvergenciją apibūdinančios definicijos

Dar kituose apibrėžimuose technologijų konvergencija įvardinama kaip: skaitmeninė konvergencija, medijų integracija, tinklo ir technologijų sintezė, simbiozė, hibridinė komunikacija, medijų mutacija, audiovizualinė komunikacija ir pan. Pastebima, kad technologijų konvergencijos reiškinyje pasižymi daugiafunkciškumu ir nuolatiniu tobulėjimu, o tai įtakoja spartesnę žinių visuomenės kūrimą, IRT infrastruktūros plėtrą, kokybiškesnę paslaugų tiekėjų ir viešųjų paslaugų perkėlimą į elektroninę erdvę, atsiradimą naujų rinkų tokių kaip e-verslas, telemedicina, nuotolinis mokymasis ir pan. Taigi konvergencijos reiškinyje ne tik išplėtė tradiciškai reguliuojamų sektorių ribas, bet ir atvėrė galimybes teikti įvairias paslaugas naudojant vartotojo prieigą, elektroninių ryšių tinklus, galinius įrenginius:



3 pav. Technologijų konvergencijos grafinis pavaizdavimas. Šaltinis: rrt.lt

Technologijų konvergencijai būdingi tokie bendri komponentai: tai įvairių galinių įrenginių, elektroninių ryšių tinklų, jais perduodamo skaitmeninio turinio susilieėjimas, integravimas vienu į kitus ar transformacija skirtingais formatais (vaizdu, garsu ir pan.):

1. Galiniai įrenginiai su daugiausia personalizuota prieiga (identifikavimu);

³³ Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas : kolektyvinė monografija / Vilnius : Mykolo Romerio universiteto Leidybos centras, 2009, p. 155 [2014 01 07].

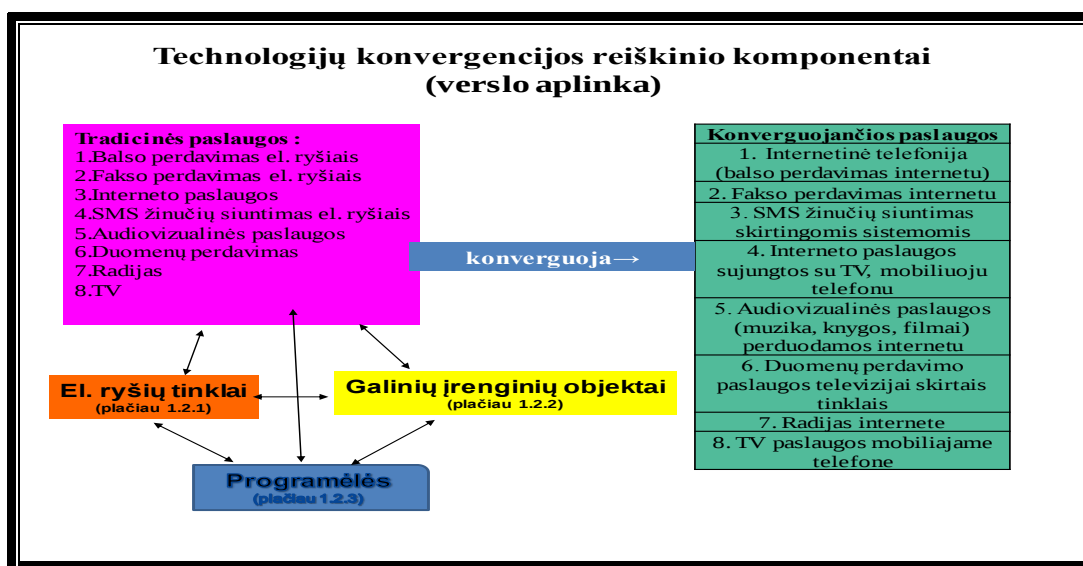
³⁴ RFID (Radio Frequency Identifying)- identifikacija radijo bangomis

2. Elektroninių ryšių tinklai (prieiga prie interneto);
3. Skaitmeninis turinys (arba elektroninės paslaugos);
4. Turiniui pateikti reikalinga programinė įranga (arba priemonės turiniui sukurti).

Technologijų konvergencijai būdingi bruožai plačiau aptariami sekančioje dalyje.

1.2. Technologijų konvergencijos skiriamieji bruožai

Kaip buvo minėta ankstesnėje darbo dalyje, technologijų konvergencijai būdingi šie komponentai: elektroninių ryšių tinklai, galiniai įrenginiai, vartotojo sąsaja (e. identifikavimas), interneto ryšys, turinys arba paslaugos, kurių pateikimui naudojamos programėlės, duomenų bazės, registrai ir pan. Grafiškai būtų galima pavaizduoti taip:



4 pav. Technologijų konvergencijos komponentai.

Toliau bus aptariamas kiekvienas komponentas atskirai.

1.2.1. Elektroninių ryšių tinklai

Pagal LR Elektroninių ryšių įstatymo 3 straipsnio 16 punktą elektroninių ryšių tinklas yra „perdavimo sistemos ir (arba) komutavimo bei maršruto parinkimo įranga, kitos priemonės, įskaitant pasyviuosius tinklo elementus, leidžiančios perduoti signalus laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuotuosius (kanalų ir paketų komutavimo, įskaitant internetą) ir judriuosius antžeminius tinklus, elektros perdavimo kabelines sistemas (kiek jos naudojamos signalams perduoti), tinklus, naudojamus radijo ir (arba) televizijos programoms transliuoti (retransliuoti), ir kabelinės televizijos bei mikrobangų daugiakanalės televizijos tinklus neatsižvelgiant į perduodamos informacijos pobūdį“³⁵. Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos (toliau - IVPK) pateikia plačiajuostės interneto prieigos technologijų suvestinę (1 priedas), kurioje aprašomos šiuo metu

³⁵ http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=460481, [2014 01 23].

veikiančios plačiajuosčių tinklų technologijos, jų privalumai, trūkumai naudojami standartai, greಿತaveika ir aprėptis bei pabrėžia, jog papildomų saugos priemonių reikalauja WiFi, PLC tinklų technologijos. Beje, Europos ekonomikos atkūrimo plane Europos Komisija iškelė tikslą spartinti investicijas į infrastruktūrą, o tarp prioritetinių infrastruktūrų išskyrė **plačiajuosčio ryšio tinklus**. Europos Komisija pabrėžė, kad investicijų į plačiajuosčio ryšio infrastruktūrą spartinimas trumpuoju laikotarpiu gali padėti stiprinti ekonomiką, o ilgalaikėje perspektyvoje – didinti Europos ilgalaikio tvaraus augimo potencialą.³⁶ „Europos skaitmeninėje darbotvarkėje“ valstybės narės įpareigosotos siekti strategijos „Europa 2020“ tikslų plačiajuosčio ryšio plėtros srityje, t. y. kad bazinis plačiajuostis ryšys (fiksuoтasis ir belaidis) būtų prieinamas visiems iki 2013 m., o interneto sparta būtų palaipsniui didinama iki 30 Mb/s ir daugiau, taip pat – kad būtų įdiegti naujos kartos prieigos tinklai, kuriuose būtų galima užtikrinti itin spartų (daugiau kaip 100 Mb/s) interneto ryšį. EK užsakymu bendrovės „Van Dijk“ atlikto tyrimo „Broadband Internet Access Cost (BIAC) 2013“ rezultatai rodo, kad 12–30 Mb/s plačiajuostis ryšys ES mastu pigiausiai siūlomas Lietuvoje³⁷.

1.2.2. Galinių įrenginių objektai

Pagal Elektroninių ryšių įstatymo 3 straipsnio 22 punktą galinis įrenginys – tai „leidžiantis priimti ir (arba) perduoti informaciją įrenginys ar jo atitinkama dalis, skirti tiesiogiai ar netiesiogiai bet kokiomis priemonėmis būti prijungti prie viešųjų ryšių tinklų“. Konverguojantiems galiniams įrenginiams būdingas daugiafunkciškumas (pvz. mobiliuoju telefonu galima skambinti, rašyti žinutes, fotografuoti, filmuoti, klausytis muzikos, žiūrėti filmus ir t.t.), jie turi vartotojo sąsajas ir prisijungimą prie interneto. 2 priede pateikta konverguojančių galinių įrenginių (personalinio, nešiojamo, planšetinio kompiuterio, delninuko, mobilaus telefono, tarnybinių stočių, skaitmeninės televizijos, skaitmeninio radijo, periferinių (daugiafunkcinių), virtualiųjų įrenginių), operacinių ir taikomųjų programų bei saugumo sprendimų pavyzdžiai, tačiau šis sąrašas nėra baigtinis.

Europos Parlamentas 2010 m. birželio 15 d. rezoliucijoje **dėl daiktų interneto**³⁸ atkreipia dėmesį į naują reiškinių "Daiktų internetą" (angl. "Internet of things") t.y. bevielį tarpusavyje susietų galinių įrenginių tinklą, kuriame integruotus daviklius – lustus ir antenas – turintys objektai radijo dažninių atpažinimo (RDA) būdu „bendrauja“ tiek tarpusavyje, tiek su žmonėmis. RDA technologijos žada revoliuciją žmonių ir daiktų sąveikos srityje, pagrindinė naujovė – daiktų „bendravimas“ tarpusavyje. Šios technologijos atneš dideles verslo plėtros, kovos su klimato kaita, efektyvaus energijos ir transporto valdymo galimybes. Deja, gali kilti problemų pamatinių teisių apsaugos srityje: mikroschemose bus užkoduota daugybė asmeninės informacijos³⁹.

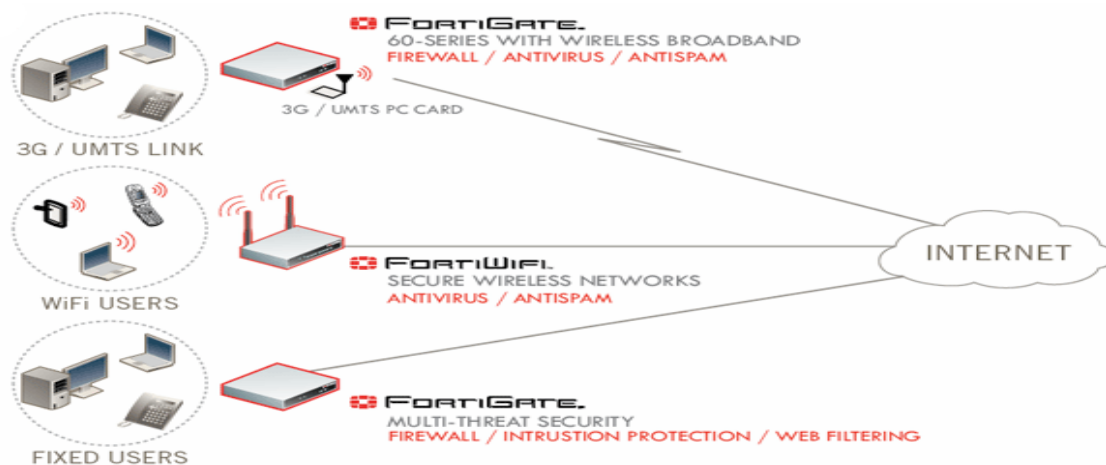
³⁶ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:087E:0098:0113:LT:PDF>, [2014 01 20].

³⁷ <http://www.ivpk.lt/news/1929/21/Lietuva-pigiausio-placiajuoscio-rysio-valstybe-Europos-Sajungoje>, [2014 01 28].

³⁸ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0207+0+DOC+XML+V0//LT>,

³⁹ ten pat, [2014 01 17].

Kitas įdomus galinio įrenginio pavyzdys galėtų būti **Tinklo saugumo sprendimai**, kai vienu įrenginiu siekiama daugelio funkcijų: tinklo apsauga nuo įsilaužimų, atakų ir duomenų vagystės, interneto virusų ir kenksmingų programų, nepageidaujamų el. laiškų ir pavojingų interneto puslapių, vartotojo kontrolė tinkle, suderinamumas su ateities Wi-Fi standartu, žalingo kodo blokavimas:



5 pav. Tinklo saugumo sprendimas, pasižymintis daugiafunkciškumu.

1.2.3. Elektroninis identifikavimas

Vartotojui, siekiančiam pasinaudoti elektroninėmis paslaugomis, iškyla būtinybė save identifiкуoti elektroninėje erdvėje. Tam įprastai naudojami identifikavimo ir autentifikavimo būdai: pin (tan) kodas; slaptažodis; elektroninis parašas; dokumentas su integruotu e. parašu, dažnių technologijomis (RFID) grįstais duomenimis: vairuotojo pažymėjimas, kreditinė kortelė, identifikavimo kortelė, socialinio draudimo pažymėjimas, ir pan.

Lietuvoje asmens identifikavimo sritį reglamentuoja LR Elektroninio parašo įstatymas. E. parašas naudojamas tam, kad vartotojas galėtų save identifiкуoti, jungdamasis prie įvairių e. paslaugų teikėjų informacinių sistemų, pasirašyti dokumentus, prašymus. E. parašai gali būti kuriami kompiuteriu arba pasinaudojant mobiliuoju telefonu. Kuriant e. parašą kompiuteryje, jame turi būti įdiegta speciali programinė įranga, prijungta techninė įranga. Kai e. dokumentų pasirašymui naudojamas mobilusis telefonas, jame turi būti e. parašo sudarymo galimybę turinti SIM kortelė, kurią išduoda mobiliojo ryšio operatoriai. Mobilioju įrenginiu sukurtas e. parašas vadinamas mobiliuoju e. parašu. Pagrindinis mobiliojo e. parašo pranašumas – patogumas, kadangi nereikia atskiro skaitytuvo ir programinės įrangos. Neretai e. dokumento sudarymo ir pasirašymo funkcija yra integruota į įvairių e. paslaugų teikimo procesą.

Vis dažniau prabylama apie kitus identifikavimo naudojimo metodus, kurie pavyzdžiui gali nustatyti objektą be tiesioginio žmogaus įsikišimo, t.y. tokie prietaisai kaip brūkšninis kodas, magnetinė juostelė, biometrinė bei radijo dažnio identifikavimas, mikroschemų implantai ir realaus laiko pozicionavimo galimybės ir kt. 2013 m. liepos mėn. 22-23 d. vykusioje konferencijoje

„Wearable Technologies“ buvo pristatyta kaip kombinuojant naujas technologijas (sensors), vartotojų informaciją, socialinius-elgsenos-sveikatos duomenis būtų galima kurti naujas „dėvimas“ technologijas, diegiant jas į žmogų, dėvimas ant kūno arba nešiojamos kaip įrenginius⁴⁰. Šios technologijos pristatomos kaip naujausios pažangos technologijos, akcentuojant grėsmės aspektus dėl asmens duomenų apsaugos.

1.2.4. Programinė įranga, mobiliosios aplikacijos

Norint konverguojančiais įrenginiais gauti elektronines paslaugas, juose turi būti įdiegta programinė įranga. Mobiliesiems įrenginiams skirtos programėlės (*apps* arba *applications*) diegiamos į išmaniuosius telefonus, planšetinius kompiuterius, namų aplinkos prietaisus, turinčius vartotojo sąsajas ir prieigą prie interneto. Šiuo metu viešajam ir privačiam sektoriui prieinama apie 6 mln. programėlių ir šis skaičius kasdien auga po daugiau nei 30 000⁴¹. Pavyzdžiui, Lietuvos nacionalinio radijo ir televizijos tarybos ataskaitoje patvirtinti planai „stiprinti ir mobiliąsias platformas. Tiesioginių transliacijų programos atsiras platformose „Symbian“, „Windows phone“, „Android“ ir „IOS“. Bus kuriamos programėlės, padėsiančios užmegzti glaudesnę ryšį su žiūrovais, jie galės interaktyviai bendrauti su televizija“⁴². Vilniaus m. savivaldybė pateikė mobiliąsias aplikacijas: "Tvarkau Vilnių" (galimybė gyventojams informuoti savivaldybės darbuotojus apie problemas esančias mieste, integruota sąsaja su "Problemų žemėlapiu"), „Vilniaus turizmas" (virtualus Vilniaus miesto gidas su lankytinų objektų informacija, nuotraukomis, žemėlapiiais, kontaktais), "Sviesoforai.lt" (paslauga vairuotojams patogiai planuoti maršrutus paga esamą eismo situaciją mieste, esamos vietos nustatymas, integracija su GPS įrenginiu⁴³):



6 pav. Vilniaus m. savivaldybės mobiliosios aplikacijos

Apie kitas mobiliąsias aplikacijas naudojamas valstybės institucijų veikloje, teikiant elektronines paslaugas plačiau bus aptariama sekančiame skyriuje.

⁴⁰ http://www.wearable-technologies.com/wp-content/uploads/2013/07/130722_Keynote_Harry-Strasser_WT.pdf, [2014 02 12].

⁴¹ Varšuvos deklaracija dėl mobiliesiems įrenginiams skirtų programėlių naudojimo // <https://privacyconference2013.org/web/pageFiles/kcfinder/files/ATT29312.pdf>, [2014 01 11].

⁴² Lietuvos nacionalinio radijo ir televizijos tarybos 2011 metų veiklos ataskaita // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=429288&p_query=program%eb1%ebs&p_tr2=2, [2013 07 22].

⁴³ <http://www.vilnius.lt/index.php?51589814>, [2014 03 10].

1.3. Technologijų konvergencijos reiškinyje viešajame administravime

Lietuvos Respublikos Vyriausybė 2014–2020 metų Nacionalinės pažangos programoje⁴⁴ numato, kad naujų technologijų diegimui bus skiriamas didžiulis dėmesys pradedant pažangių informacinių ir kitų technologijų diegimu, modernizuojant švietimo įstaigų ir aukštųjų mokyklų infrastruktūrą, diegiant ir plėtojant IRT į sveikatos priežiūros sistemą, skatinant teigiamus pokyčius versle, kai šalį pasieks naujausios pasaulio tendencijos, modernios technologijos ir nauji iššūkiai. Taigi, pažangūs technologiniai sprendimai turėtų apimti daugelį viešojo administravimo sričių. Pirmiausia šioje dalyje bus pateikiama e. valdžios technologinė samprata, po to apibrėžiama kokiame kontekste viešajame administravime daugiausia nagrinėjama technologijų konvergencija bei pateikiami šio reiškinio pavyzdžiai.

Technologijų konvergencija viešajame administravime pirmiausia siejama su pažangiomis technologijomis, integruotais sprendimais, mobilumu, naujais viešojo valdymo metodais bei valdžios transformacija į **elektroninę valdžią** (toliau – e. valdžia). E. valdžia dažniausiai suvokiama kaip valstybinės valdžios tąsa elektroninėje erdvėje, pasireiškianti kaip valstybės funkcijų realizavimas, organizacinių pokyčių tobulinimas pasitelkiant IRT⁴⁵. Taip viešasis valdymas iš specializuotos šakos transformuojasi į sudėtingą ir daugialypį skirtingų veiklų kompleksą, kuris reikalauja tarpdalykinių kompetencijų, kompleksinių gebėjimų ir vis naujų technologijų.

E. valdžia, o plačiau ir e. viešasis administravimas, šiuo metu aprėpia šias svarbiausias veiklos sritis bei aspektus⁴⁶:



7 pav. E. valdžios veiklos sritys, kuriose dalyvauja technologiniai sprendimai.

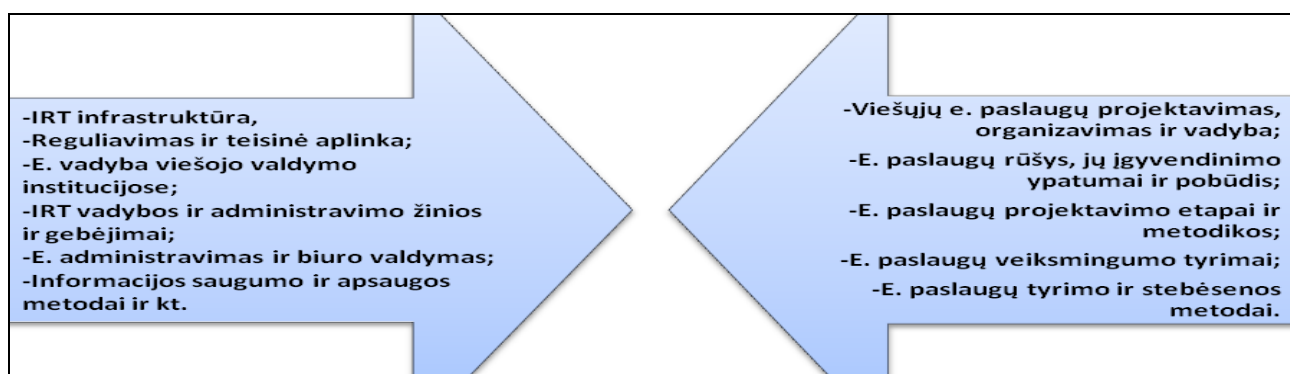
⁴⁴ patvirtinta Lietuvos Respublikos Vyriausybės 2012 m. lapkričio 28 d. nutarimu Nr. 1482 „Dėl 2014–2020 metų Nacionalinės pažangos programos patvirtinimo“

⁴⁵ Designing E-Government, 2002, p. 78: Kiškis, Petrauskas

⁴⁶ Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas : kolektyvinė monografija / Vilnius : Mykolo Romerio universiteto Leidybos centras, 2009, p.24

Pagrindinės sritys sietinos su šiuolaikinio valdymo pokyčiais žinių visuomenėje, yra valdymo metodų pasikeitimai, naujų valdžios ir piliečių sąveikos formų atsiradimas (kaip interaktyvus bendravimas), demokratijos įgyvendinimo struktūros kaita, milžiniškos ES erdvės kaip valdymo objekto formavimasis. Taip pat sparčiai plėtojamos informacinės technologijos bei įtinkinti informacijos perdavimo būdai skatina visuomenės pokyčius, viešojo administravimo kaitą bei skaitmeninį bendravimą.

Vienas iš e. valdžios tikslų yra **viešojo sektoriaus modernizavimas**. Modernizavimo kriterijai gali būti dvejopi: viena, orientuoti į strateginių visuomenės tikslų įgyvendinimą, antra, siekiantys optimizuoti pačią valdžią. E. valdžios požiūriu tai yra veiklos organizavimo ir vadybos efektyvumo skatinimas, kuris apima daugelį itin svarbių praktinių ir technologinių e. valdžios taikymo sričių, susijusių su e. paslaugų kūrimu:



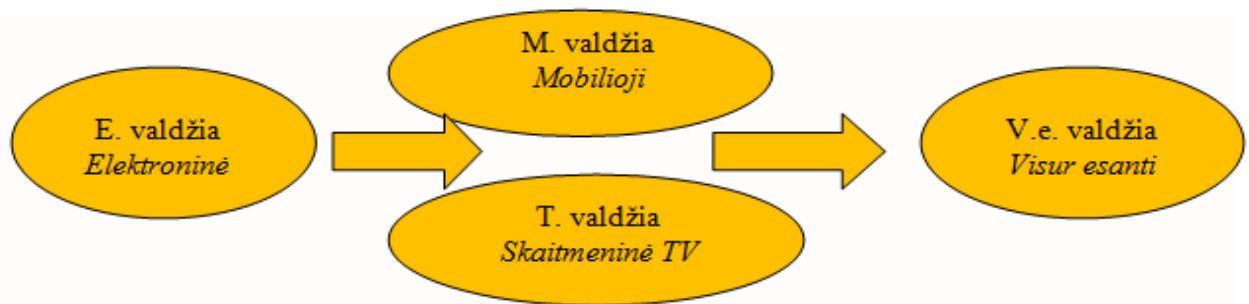
8 pav. Technologinio įgyvendinimo sąsajos su viešojo valdymo funkcinio veiksmingumu- e. paslaugų teikimu

Technologinė e. valdžios aplinka gali būti suprantama dvejopai: kaip IRT taikymas viešajame sektoriuje arba kaip integruotų priemonių (sistemų, platformų) naudojimas, kai kuriamos naujos socialinės, politinės, ekonominės ir kt. veiklos formos. IRT teikia funkcines galimybes ir išplečia sąveikų, informacijos ir žinojimo įtaką daugeliui žmogaus veiklos sričių ir kartu didina jų konkurencingumą globaliame kontekste. Abi šios tendencijos neatsiejamos nuo IRT inovacijų pritaikymo tobulinant viešąjį sektorių ir kuriant naujas elektronines paslaugas⁴⁷. Pasikeitusią e. valdžios technologinio gyvavimo aplinką lemia konkretūs technologiniai veiksniai, kai įsigali **technologijų konvergencija**, susijungiant ryšiams, duomenų perdavimui masinės komunikacijos priemonėmis ir plėtojant skirtingas medijas integruojančioms technologijoms.

Šalys renkasi valstybinių informacinių išteklių reformų, siekiant jas centralizuoti, užtikrinti techninį, organizacinį ir semantinį sąveikumą, deklaruojami siekiai pereiti prie valstybinių debesų kompiuterijos infrastruktūrų, duomenų bazių konsolidavimo mechanizmų. Europos e. valdžios strategai prognozuoja esminę e. valdžios technologinę transformaciją, kai visuomenė pati taps e. valdžios bei jos paslaugų kūrėja ir vartotoja tuo pačiu metu, o sparčiai plėtojantis bei konverguojant

⁴⁷ Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas : kolektyvinė monografija / Vilnius : Mykolo Romerio universiteto Leidybos centras, 2009, p.151

technologijoms (mobilioms, aplinkos intelekto ir pan.), e. valdžios modelį palaipsniui keis „mobiliuosios valdžios“ bei „visur esančios valdžios“ („v.e. valdžios“, angl. ubiquitous) modeliai. Svarbus didėjantis mobilumas ir visuotinis pasiekiamumas, kuris yra pagrindas keisti e. valdžią į mobiliąją (m. valdžią) ir artėti prie „visur esančių“ IRT, ateities žmogaus ir IRT sąveikos modelio, kuriame informacijos apdorojimas visiškai įdiegtas į įprastus kasdienybės objektus ir veiklas, t.y. vartotojas vienu ir tuo pat metu naudojasi daugybe kompiuterijos prietaisų ir sistemų įvairiose kasdienėse savo veiklose⁴⁸:



9 pav. E. valdžios transformacija į „visur esančią“ valdžią (Kim, 2005)

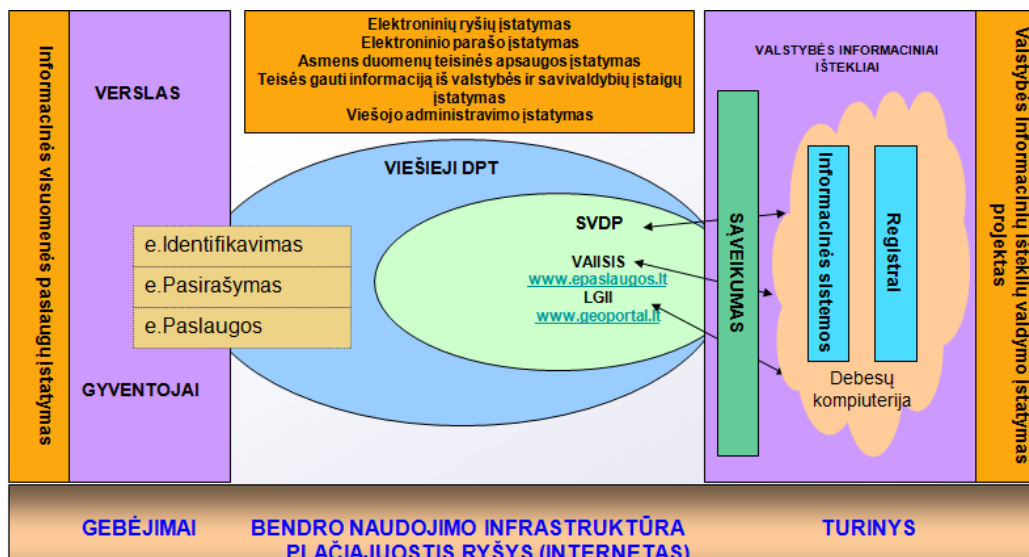
Taigi ateityje viešasis administravimas orientuosis į mobiliųjų technologijų taikymą bei jų skatinimą, kuriant „visur esančius“ miestus, „visur esantį“ verslo valdymą⁴⁹.

Viešajame administravime technologijų konvergencijos bruožų galima aptikti, kai nagrinėjami tokie klausimai:

1. Informacinių sistemų ir registrų sąveikumas (interoperabilumas), bendrų duomenų bazių kūrimas, IS centralizavimas, techninių sprendimų (serverių, duomenų bazių) konsolidavimas, duomenų bazių integracija, panaudojant web servisus, debesų kompiuterijos infrastruktūros ir pan. Pavyzdžiui, duomenų mainų platforma VIISP - informacinių sistemų tarpusavio sąveikumo užtikrinimo sistema, kurios rezultatas- vieninga valstybės institucijų informacinių sistemų ir registrų duomenų apsikeitimo sistema (vieninga infrastruktūra), leidžianti institucijoms, dalyvaujančioms duomenų mainuose, paprasčiau ir greičiau gauti duomenis iš kitų institucijų. Šioje sistemoje realizuotos tapatybės nustatymo ir autentifikavimo funkcijos. Sistemoje įdiegtos paslaugos teikimo proceso stebėsenos, mokėjimų, klientų aptarnavimo aplinkos tvarkymo, e. paslaugų konstravimo, e. formų rengimo, e. parašo panaudojimo ir informavimo paslaugų funkcinės galimybės.

⁴⁸ Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas : kolektyvinė monografija / Vilnius : Mykolo Romerio universiteto Leidybos centras, 2009, p. 154

⁴⁹ ten pat, p.67



10 pav. VIISP - elektroninių paslaugų teikimo panaudojant IRT schema⁵⁰.

2. **Elektroninių paslaugų unifikavimas, standartizavimas, racionalizavimas** (e. paslaugų konvergencija). Konverguojančios technologijos suprantamos kaip būdas tai pačiai elektroninei paslaugai suteikti papildomą vertę, geresnį prieinamumą, patogesnį, vaizdingesnį turinį, universalią e. pasirašymo galimybę, kai:

- pilietis įvairiais galiniais įrenginiais gali gauti e. paslaugą;
- pilietis įvairiais elektroninių ryšių tinklais gali gauti e. paslaugą;
- pilietis e. paslaugą gali gauti įvairiu formatu (garsu, tekstu, vaizdu) ir pan.;
- pilietis pasirašo įvairiais e. autentifikavimo būdais;
- "Vienas langelis" kuriamas kompleksinėms paslaugoms gauti (prašymų pateikimas, apmokėjimas už paslaugas, el. pasirašymas, atsakymo gavimas ir pan.).

3. Vykdomuose (ar įvykdytuose) **e. valdžios projektuose**, kurie kuria centralizuotus, nacionalinės reikšmės sprendimus: Viešųjų pirkimų portalas, Nacionalinė elektroninės tapatybės liudijimo sistema NETLIS, Lietuvos paslaugų katalogas www.lietuva.gov.lt, Paslaugų stebėsenos sistema, "Verslo vartai", "Prisijungusi Lietuva", MEPIS, Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistema ir pan. Projektų vykdytojai neretai deklaruoja rezultatų pateikimo įvairiais būdais ir kanalais privalumus. (Projektas „Elektroninės demokratijos paslaugų plėtra Lietuvos Respublikos Vyriausybėje“ - integruoti visų Vyriausybės valdymo srities įstaigų veiklos informaciją; IT projektas “Viešojo administravimo institucijų informacinių sistemų interoperabilumo – sistemų sąveikos gebos sukūrimas”; projektas "Centralizuotos viešųjų ir administracinių paslaugų sistemos kūrimas ir diegimas įgyvendinant vieno langelio principą”).

⁵⁰ http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=356833&p_tr2=2, [2013 11 22].

5. **Viešojo ir privataus sektoriaus konvergencija**, kai, pavyzdžiui, plėtojant plačiajuosčio ryšio infrastruktūrą, plačiajuosčiu internetu galima aprūpinti pagrindinius žinių centrus, elektroninių ryšių sektoriui atsiranda daugiau galimybių plėtoti nuotolinį (menamą) mobilumą, užtikrinamos naujos galimybės kurti ir tobulinti elektronines paslaugas⁵¹, naudotis debesų kompiuterijos paslaugomis.

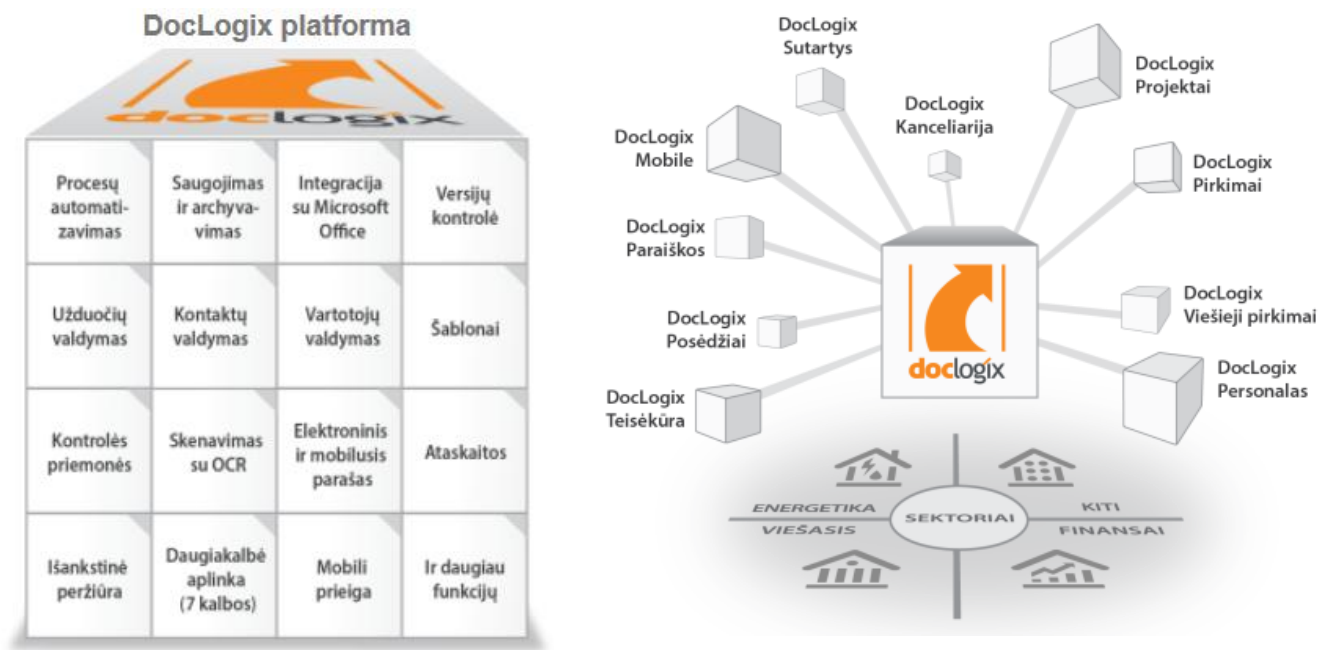
6. **Mobili (nutolusi) darbo vieta**. Technologijų konvergencija leidžia skirtingose geografinėse vietose dirbantiems darbuotojams naudotis informacija bei duomenimis ne darbo vietoje: kalbėtis telefonu, tikrinti el. paštą, naudotis internetu ir duomenų valdymo sistemomis, dokumentais, užrašais, pranešimais, o tai reiškia, jog darbuotojo darbo vieta tampa mobili.

7. Elektroninei aplinkai pritaikant technologijų įvairovę, adekvačiai auga grėsmių bei pažeidžiamumų mastas, kur technologijų įvairovė tikslams pasiekti kelia vis didesnių rūpesčių: **konverguojantys įrenginiai sukelia kibernetinio saugumo grėsmę**, gali tapti elektroninio pažeidimo įrankiu, o jų panaudojimas mobiliuose darbo vietose ne visada atitinka įstaigoje nustatytos saugumo politikos reikalavimų.

Vis daugiau valstybės institucijų stengiasi pateikti elektronines paslaugas per integruotas elektroninių paslaugų sistemas įprastose bei mobiliuose aplinkose, pasiekiamose ne tik vidiniuose tinkluose, bet ir belaidžiais tinklais. Tuo pačiu paslaugų teikėjai, kuriantys specializuotus sprendimus įstaigoms ir organizacijoms, kaip privalumą nurodo jų mobilumą, inovacijas ir efektyvumą. Pavyzdžiui, UAB „DocLogix“, pristatydamą vieną populiariausių valstybės institucijose **Elektroninių dokumentų ir procesų valdymo sistemą** nurodo produkto privalumus ir pateikia integruoto sprendimo grafinį pavaizdavimą:

1. **Inovacijos**: galimybė naudotis sistema iš mobiliųjų įrenginių; paprastas grafinis procesų modeliavimas; suderinamumas su naujausiais el. parašo standartais ir formatais; mobilusis ir elektroninis parašas; didelio našumo optinis teksto atpažinimas (OCR); savarankiškas produkto modifikavimas be programavimo; suderinamumas su el. archyvo informacine sistema (EAIS).
2. **Efektyvumas**: Daugybinis (srautinis), užduočių atlikimas; integracija su kitomis sistemomis (apskaitos ir kt.); veiksmų automatizavimas; darbas iš elektroninio pašto terpės; greitas dokumentų skenavimas ir įkėlimas;
3. **Mobilumas**: vartotojai gali naudotis nemokama mobiliąja programėle, kuri leidžia dirbti tiesiai iš išmaniojo telefono ar planšetinio kompiuterio;
4. **Suderinamumas ir skirtingų el. dokumentų standartų palaikymas**: palaiko Lietuvos, Latvijos ir Estijos elektroninių dokumentų standartus (ADOC, DigiDoc, JustaGE, eDoc, PDF);
5. **Visų dokumentų tipų palaikymas**: palaiko visus populiariausius tekstinius, vaizdo, garso ir video formatus.

⁵¹ Informacinės visuomenės plėtros 2014–2020 metų programa „Lietuvos respublikos skaitmeninė darbotvarkė“, http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=467638&p_tr2=2, [2014 03 22].



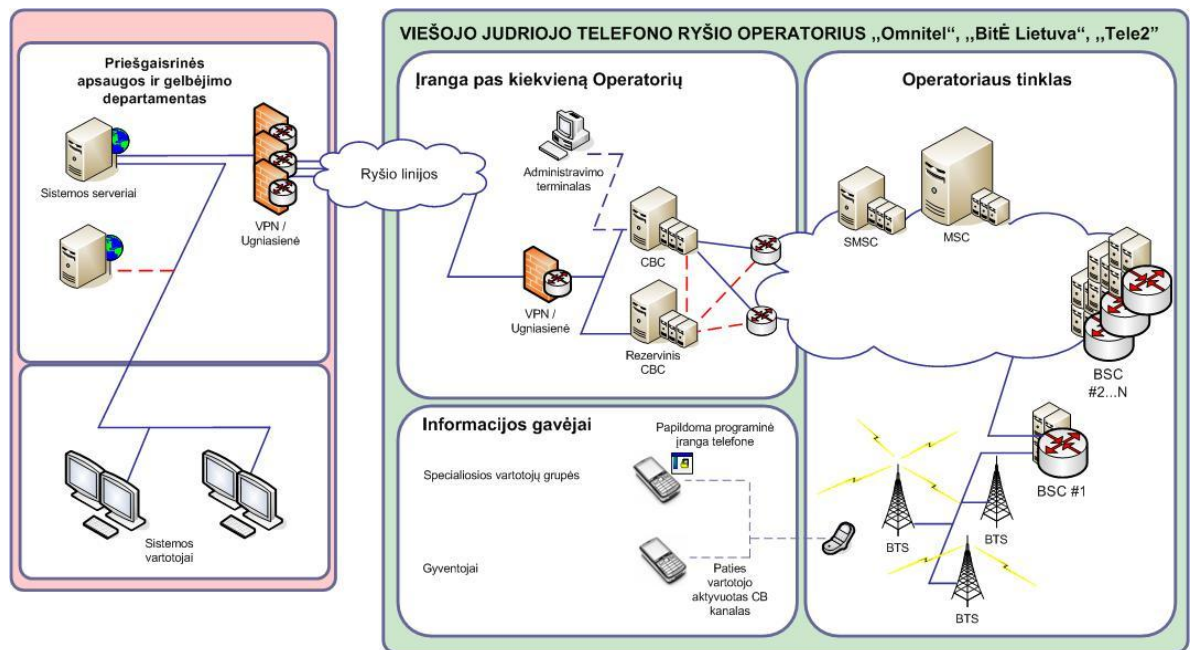
11 pav. Vienoje Doclogix platformoje integruota daugelis įstaigos sprendimų, pasiekiamų įprasta arba mobilią prieigą

E. pristatymo informacinė sistema - nacionalinės elektroninių pranešimų ir elektroninių dokumentų pristatymo fiziniams ir juridiniams asmenims, naudojant pašto tinklą, informacinė sistema – veiksmingai panaudojant informacines ir ryšių technologijas, sukuriama patogios, lengvai pasiekiamos ir naudingos elektroninių pranešimų ir elektroninių dokumentų pristatymo fiziniams ir juridiniams asmenims elektroninės paslaugos.

Infostatyba - statybos leidimų ir statybos valstybinės priežiūros informacinės sistemos mobilios aplikacijos sudaro galimybę operatyviau ir patogiau pranešti apie savavališkas statybas ir sekti pateiktų prašymų, susijusių su įvairių statybos leidimų, pritarimų, specialiųjų reikalavimų išdavimu, nagrinėjimo eigą.

Virtuali el. paveldo sistema - Lietuvos kultūros paveldo skaitmeninto turinio kūrimas ir sklaida, plėtojant virtualią elektroninio paveldo sistemą. Portale www.epaveldas.lt galima atlikti paiešką Lietuvos istorinių vietovardžių, asmenvardžių ir laikotarpių tezaure. Tezauro duomenų modelis naudoja ontologijomis grindžiamą tezaurų tvarkymo būdą ir semantinio saityno technologijas. Sukurtos integralios virtualios sistemos duomenų banke šiuo metu jau yra per 3 mln. puslapių itin vertingų senųjų knygų, laikraščių, dailės kūrinių, rankraščių, bažnytinių metrikų. Kultūros paveldo objektai skirstomi į grupes: vaizdas, garsas, tekstas.

Gyventojų perspėjimo ir informavimo sistema GPIS - sistema, užtikrinanti gyventojų perspėjimą ir informavimą apie gresiančią ar susidariusią ekstremaliąją situaciją trumpaisiais pranešimais tiesiogiai į gyventojų mobiliuosius telefonus (2G,3G tinklais):



12 pav. Gyventojų perspėjimo ir informavimo sistemos funkcinė schema

Tokiu būdu kuriama vis daugiau elektroninių paslaugų, kurios jungiamos į platformas, integruojamos į sąveikumo sistemas. Taip atsiranda „išmanieji miestai“, „išmaniosios vyriausybės“, „išmanioji planeta“. Pvz. kompanija "Hitachi" pristato „išmaniųjų miestų“ viziją, kai naudojant IT bus užtikrinamas sąveikumas tarp atskirų miesto valdymo infrastruktūros sferų, o vartotojams saugiai ir patogiai bus galimybė gauti paslaugas jiems patogiu laiku nepriklausomai nuo vietos:



13 pav. „Išmanaus miesto“, paremto IT pagrindu, modelis

"Išmanus miestas" užtikins sąveiką ir koordinavimą tarp namų administravimo, biurų, viešbučių, gamyklų, vyriausybės, mokyklų, pramonės, prekybos, logistikos, mokslinių tyrimų, aukštojo mokslo, žemės ūkio ir žuvininkystės sričių⁵².

Apžvelgus technologijų konvergencijos reiškinį, jo definicijas ir plėtrą įvairiose visuomeninio gyvenimo, mokslo bei viešojo administravimo srityse, galima teigti, kad šis reiškinys apima daugelį minėtų sričių, jis labai progresuoja ir tobulėja, galima išskirti jam būdingus bruožus. Vystantis naujoms technologijoms, kuriasi naujos mokslo šakos, kurios prognozuojama gali pakeisti ne tik žmogaus buitį, bet ir visuomeninę raidą.

Viešasis administravimas technologijų konvergencijos kontekste tobulėja kurdamas elektronines paslaugas, jungdamas jas į centralizuotas platformas, kitus integruotus sprendimus, tuo atsiliepdamas į klientų poreikį nepriklausomai nuo laiko ir vietos gauti elektronines paslaugas patogiu būdu kokybišku ir patraukliu formatu. Iš kitos pusės IRT suteikia viešajam administravimui naujų galimybių tobulinti valdymo metodus, siekiant tapti patrauklia, pažangia nuolat kintančia ir atsinaujinančia e. valdžia, o tinkamai suregulmentavus, ateityje - m.. valdžia

Kyla klausimas, kokios tendencijos vyrauja Europos Sąjungos ir Lietuvos strateginiuose teisiniuose dokumentuose, ar šis reiškinys tinkamai suregulmentuotas ir gali turėti įtakos efektyvių ir atsakingų valdymo modelių sukūrimui, ar naujos technologijos pasitarnaus interaktyviam valdžios bendravimui su piliečiais, naujų elektroninių paslaugų kūrimui.

⁵² <http://www.hitachi.com/products/smartcity/vision/concept/it.html>, [2014 04 08].

II. Technologijų konvergencijos įtaka e. valdžios plėtrai: strateginių dokumentų analizė

Nors XXI a. skelbiamas pažangių technologijų amžiumi, akivaizdu, kad žmonija susidūrė su kontraversiškais ir globaliomis problemomis. Iš vienos pusės didžiuojamasi žmonijos sukurtomis aukštosiomis, sumaniosiomis technologijomis, iš kitos pusės kelia nuostabą statistika: net 70 proc. pasaulio gyventojų dar neturi interneto, apie 1,1 milijardo žmonių - pakankamai švaraus geriamojo vandens, trečdalis pasaulio žmonių - maisto, kad valgytų 3 kartus per dieną (nors apie 40 proc. tinkamo naudoti maisto išmetama į sąvartynus), apie 1,5 mlrd. pasaulio gyventojų neturi elektros, pasaulyje yra apie 100 milijonų benamių, 42 mln. pabėgėlių, 2,6 milijardo žmonių iš viso neturi tualetų, beveik milijardas žmonių yra neraštingi, apie 1,6 mlrd. žmonių gyvena šalyse, kuriose uždrausta kalbėti apie tai, kaip šalis valdoma, daugiau nei 75% pasaulio žmonių gyvena ten, kur jų tikėjimo laisvė varžoma⁵³. Šalia šių žmogiškų problemų galima vardinti kitas XXI amžiui būdingas globalias problemas tokias kaip klimato kaita ir aplinkos būklės blogėjimas, gyventojų senėjimas ir gimstamumo mažėjimas, pasaulinio kuro atsargų mažėjimas, energetinis bei kibernetinis saugumas, informacinio karo grėsmė ir pan. Šių problemų akivaizdoje viešajam administravimui tenka didžiulė atsakomybė dalyvauti šių problemų sprendime, atsakyti kiek veiksmingas ir rezultatyvus yra viešasis valdymas pokyčių sąlygomis, kaip dinamiškai ir efektyviai viešojo valdymo sistema prisitaiko prie europeizacijos procesų ir demokratijos pokyčių, kaip greitai ir inovatyviai reaguojama į socialinius, politinius, ekonominius ir technologinius pokyčius, kaip giliai ir plačiai viešasis valdymas konverguoja su pilietine sritimi⁵⁴. Taip pat svarbu apžvelgti kiek sparčiai kintančios technologijos gali įtakoti viešojo administravimo modernizavimą bei teisinės bazės parengtumą savalaikiai reaguoti į kibernetinio saugumo, duomenų apsaugos grėsmes.

2.1. Technologijų konvergencijos reiškinys strateginiuose ES e. valdžios dokumentuose

Lietuvos pirmininkavimo Europos Sąjungos Tarybai metu Vilniuje vykusioje aukšto lygio e. valdžios konferencijoje „Kur mes esame, kur mes einame?“ (2013 m. lapkričio 14 - 15 d.), kurioje dalyvavo atstovai iš ES valstybių, šalių kandidačių, Rytų partnerystės programos šalių ir JAV, buvo akcentuota, kad siekiant spręsti naujai susiformavusias globalias problemas reikalingas naujas daugiakompleksinis valdžios požiūris, apimantis mokslo, visuomenės ir politikos

⁵³ „Globalios krikščionybės studijų centras“ skelbia, kad nuo 2000 iki 2010 metų kankinio mirtimi mirė milijonas krikščionių // <http://www.bernardinai.lt/straipsnis/2014-01-31-robert-j-morgan-pasaulio-karas-pries-krikscionyste/113063>, [2013 10 22].

⁵⁴ Lietuvos e. valdžios gairės: ateities išvalgų tyrimas : kolektyvinė monografija / Vilnius : Mykolo Romerio universiteto Leidybos centras, 2009, p.18

bendradarbiavimą. Politika turi būti pagrįsta aukštos kvalifikacijos moksliniais tyrimais, o visuomenei reikia veiksmingesnės ir aukštos kokybės valdymo sistemos⁵⁵.

2013 m. metinėje augimo apžvalgoje Komisija pabrėžė, kad viešojo administravimo institucijų modernizavimas yra vienas iš penkių valstybių narių prioritetų ir, atsižvelgdama į tai, paragino imtis plataus masto sąveikaus viešojo administravimo institucijų skaitmeninimo⁵⁶. Informacinės visuomenės kūrimas yra vienas iš Europos Sąjungos prioritetų. Europos Komisijos pristatytose 2010-2020 m. ES ekonominės plėtros strateginėse gairėse „Europa 2020“ viena iš išskirtų iniciatyvų, padėsiančių užtikrinti „protingą, darnų ir įtraukiantį“ Bendrijos augimą, yra „Skaitmeninė Europos darbotvarkė“⁵⁷. Peržiūrint šį sąrašą siekiama atsižvelgti į svarbiausius rinkos ir technologijų pokyčius, kaip antai internetines programas ir paslaugas, įvairių rūšių tinklų ir paslaugų konvergenciją bei labai sparčių interneto tinklų ir paslaugų plėtrą⁵⁸. Kaip tą pasiekti detaliau aptariama šiuose strateginiuose ES dokumentuose:

1. Europos Komisijos 2010 m. rugpjūčio 26 d. komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui **„Europos skaitmeninė darbotvarkė“** (KOM (2010) 245 galutinis/2) (toliau – Europos skaitmeninė darbotvarkė). Europos valstybių vyriausybės įsipareigojo, kad iki 2015 m. į vartotoją orientuotos, individualizuotos, daugiaplatformės e.valdžios paslaugos būtų teikiamos labai plačiai⁵⁹. Tuo tikslu valdžios institucijos turėtų imtis priemonių, kad išvengtų nereikalingų techninių reikalavimų, pavyzdžiui, reikalavimo naudoti tik konkrečiose operacinėse sistemose ar tik tam tikruose įrenginiuose veikiančias taikomas programas. Komisija rodys pavyzdį ir diegs pažangias e. valdžios paslaugas. Užtikrinus šias paslaugas, bus galima racionalizuoti administracines procedūras, palengvinti keitimąsi informacija, suprastinti ryšių su Komisija palaikymą ir taip suteikti daugiau galių vartotojams ir padidinti Komisijos veiklos našumą, veiksmingumą ir skaidrumą

Pavyzdinės iniciatyvos „Europos skaitmeninė darbotvarkė“ tikslas – išjudinti skaitmeninę ekonomiką ir pasitelkus informacines ir ryšių technologijas spręsti socialinius uždavinius. Tai apima galimybės naudotis plačiajuosčiu ryšiu visuose Europos regionuose suteikimą, spartesnio interneto (30 Mbps ar daugiau) užtikrinimą iki 2020 m. ir daugiau kaip 50 proc. Europos namų ūkių prijungimą prie spartesnio nei 100 Mbps interneto. Vietos ir regionų lygmeniu būtinas dėmesys IRT įgūdžių tobulinimui ir infrastruktūros gerinimui.

⁵⁵ E-government conference "Where we are, where we are going", 14-15th November, 2013 Vilnius, <http://www.vrm.lt/index.php?4137282738>[2014 02 22].

⁵⁶ http://ec.europa.eu/consumers/archive/strategy/docs/consumer_agenda_2012_lt.pdf[2014 03 11].

⁵⁷ Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: Europos skaitmeninė darbotvarkė, 2010-05-19, [2014 03 15].

⁵⁸ http://europa.eu/rapid/press-release_IP-12-1105_lt.htm, [2014 03 01].

⁵⁹ Bendradarbiaudama su valstybėmis narėmis, Komisija parengė veiksmų planą, kad būtų įvykdyti 2009 m. priimti įsipareigojimai. E. valdžios deklaracija, Malmė. [2014 03 05].

Pagrindinės darbotvarkės sritys:

- vieningoji skaitmeninė rinka (pvz. per vieningą turinio licencijavimą, vieningą e-mokėjimų ir e-sąskaitų sistemą, e-komercijos „be sienų“ skatinimą, standartų suderinamumą);
- kova su kiber-nusikaltimais bei nelegaliu turiniu, vartotojų duomenų ir privatumo apsauga, pasitikėjimo skatinimas;
- spartaus (>30 Mbps) ir itin spartaus (>100 Mbps) interneto skatinimas;
- tyrimų ir inovacijų IKT srityje skatinimas;
- e-raštingumo ir e-įtraukties skatinimas;
- e-sveikatos bei e-valdžios skatinimas (įskaitant e-Komisijos iniciatyvą).

2. Europos Komisijos 2010 m. kovo 3 d. **komunikatas „2020 m. Europa. Pažangaus, tvaraus ir integracinio augimo strategija“** (KOM (2010) 2020 galutinis). Jame pabrėžiama, kad būtina ES ir nacionalinius teisės aktus priderinti prie skaitmeninės eros, kad būtų skatinamas turinio platinimas, kartu užtikrinant didelį vartotojų ir įmonių pasitikėjimą. Tam būtina skatinti teikti šiuolaikiškas ir patogias interneto paslaugas ir jomis naudotis (pvz., e. valdžia, internetinės sveikatos paslaugos, pažangus namas, skaitmeniniai įgūdžiai, saugumas)⁶⁰.

3. Europos skaitmeninėje darbotvarkėje nustatomas e. valdžiai skirtas išsamus priemonių rinkinys- **E. valdžios veiksmų planas 2011-2015 m.**⁶¹, kuriuo siekiama visoje Europoje išnaudoti IRT privalumus. Kai viešieji ištekliai labai riboti, IRT gali padėti viešajam sektoriui plėtoti novatoriškus paslaugų teikimo piliečiams būdus ir kartu padidinti veiksmingumą ir sumažinti sąnaudas.⁶² Dėl atsiradusių tokių novatoriškų technologijų, kaip į paslaugas orientuota architektūra arba paslaugų „debesys“, taip pat dėl atviresnių specifikacijų, kuriomis sudaromos sąlygos intensyvesniems mainams, pakartotiniam naudojimui ir sąveikumui, IRT gali turėti dar didesnės reikšmės siekiant padidinti viešojo sektoriaus veiksmingumą. Pagrindinis Europos Komisijos įsipareigojimas – sudaryti palankesnes sąlygas plėtoti tarpvalstybines e. valdžios paslaugas, piliečiams ir įmonėms teikiamas nepaisant jų kilmės šalies. Pagrindinės veiklos kryptys:

1. Personalizuotos ir įvairiomis platformomis prieinamos e. Valdžios paslaugos;
2. Valdžios ir piliečių bendradarbiavimo e. Įrankiai;
3. Viešojo sektoriaus informacijos prieinamumas bei didesnis skaidrumas;
4. Piliečių ir verslo įtraukimas į viešosios politikos formavimo procesą;
5. Paslaugų teikimo vieningoje rinkoje procedūrų supaprastinimas ir perkėlimas į e. Erdvę;
6. Paneuropiniai viešieji pirkimai internete;
7. Priemonės piliečių mobilumui užtikrinti (e-dokumentai, jų prieinamumas ir sąveika, taip pat tarpvalstybinės e. Paslaugos);
8. Valstybių skatinimas dalintis gerąja patirtimi;
9. Biurokratų tarpvalstybinio mobilumo programa;
10. Neigiamo poveikio aplinkai mažinimas (tinkamiausių priemonių, tokių kaip video konferencijos, paieška, monitoringo rodiklių ir procedūrų numatymas);
11. Atvirų standartų ir tarpusavio sąveikos skatinimas;

⁶⁰ http://ec.europa.eu/eu2020/pdf/1_LT_ACT_part1_v1.pdf, [2014 03 01].

⁶¹ http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_lt.htm, [2014 03 08].

⁶² 2011–2015 m. Europos e. valdžios veiksmų planas IRT naudojimas siekiant pažangios, darnios ir novatoriškos valdžios // <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:LT:PDF>, [2014 03 17].

12. E. Atpažinties ir e. Tapatumo nustatymo (e-parašas, e-id) savitarpio pripažinimas;
13. Naujos kartos e. Valdžios paslaugos (ipv6, debesų kompiuterija).

4. Europos Komisijos 2012 m. gruodžio 18 d. komunikatas „**Europos skaitmeninė darbotvarkė. Skaitmeninėmis technologijomis grindžiamas Europos augimas**“ (KOM (2012) 784 galutinis). Svarbus veiksnys – sąveikių skaitmeninių technologijų, suteikiančių galimybę realiuoju laiku keistis duomenimis ir juos apdoroti, efektyvus naudojimas. Vien elektroninis viešasis pirkimas gali padėti sutaupyti 100 mlrd. EUR per metus⁶³, o e. valdžios sistema administravimo išlaidas gali padėti sumažinti 15–20 %. Pakartotinis viešojo sektoriaus duomenų naudojimas suteiktų daugiau galių žmonėms, skatintų verslo plėtrą ir užtikrintų apie 140 mlrd. EUR ekonominę naudą.

5. Vienoje iš oficialių ES e. valdžios vizijų **Malmö deklaracija**⁶⁴ siekiama skatinti šalių bendradarbiavimą e-valdžios srityje, idant ji būtų piliečius bei verslą įgalinančiu veiksmu, prisidėdų skatinant mobilumą ES, prieigą prie viešojo sektoriaus informacijos, įtraukiant trečiąsias šalis į e-valdžios paslaugų bei viešosios politikos kūrimą, didinant viešojo sektoriaus skaidrumą, kuriant e-valdžios paslaugas „be sienų“, mažinant administracinę naštą, gerinant organizacinius procesus ir valdžios institucijų bendradarbiavimą, mažinant neigiamą poveikį aplinkai, skatinant atvirojo standartus bei inovacijas. Dokumente pabrėžiama, kad naujų technologijų taikymas sukelia gilius kultūrinius pokyčius ir galios centrų pasislinkimą valdžios ir piliečių santykių skalėje. Šių permainų pagrindas yra naujos kartos IRT, kurios lemia naujos kartos tinklų (NGN)⁶⁵ atsiradimą ir naujas e. valdžios koncepcijas ir formas. Pirmiausia praktiškai neribotai išplečiami funkciniai parametrai, kuriuos paslaugų gavėjui ir vartotojui suteikia paketinio perdavimo plačiajuostė prieiga ir balso technologijos. Sparti NGN plėtra, perėjimas prie Ipv6 interneto protokolo, didėjanti bevielų technologijų užtikrinamos sparta, išmaniųjų IT informacinių sistemų atsiradimas, masinis RFID technologijų pritaikymas – tai yra prielaidos, kad **e. valdžios pagrindu taps išmaniosios sistemos**, grindžiamos žinojimu..

6. 2013 m. birželio mėn. EK pristatė „**Elektroninių paslaugų viziją**“ (toliau - Dokumentas), kurioje išanalizuota dabartinė e. valdžios situacija ir pateiktos gairės naujo požiūrio ir el. paslaugų modelio, kuriame akivaizdu, kad technologijų konvergencija vaidina vieną svarbiausių veiksmų. Dokumente pabrėžiama, kad dabartiniai socialiniai, technologiniai ir ekonominiai pokyčiai sukuria naujus iššūkius ir naujus lūkesčius viešųjų paslaugų sektoriuje. Todėl reikalingas naujas požiūris, t.y. reikalinga kurti **atviros ir bendradarbiaujančios vyriausybės** modelį, grindžiamą bendradarbiavimo, skaidrumo ir dalyvavimo principais, atsisakyti „bunkerio“ modelio, kai sprendimai priimami vienareikšmiškai – valdžios kabinetuose, stiprinti ryšį su piliečiais ir

⁶³ COM(2012) 179, http://ec.europa.eu/consumers/archive/strategy/docs/consumer_agenda_2012_lt.pdf, [2014 01 17].

⁶⁴ „Malmö Ministerial Declaration on e government“ <http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf>, [2014 02 02].

⁶⁵ NGN- New Generation Networks

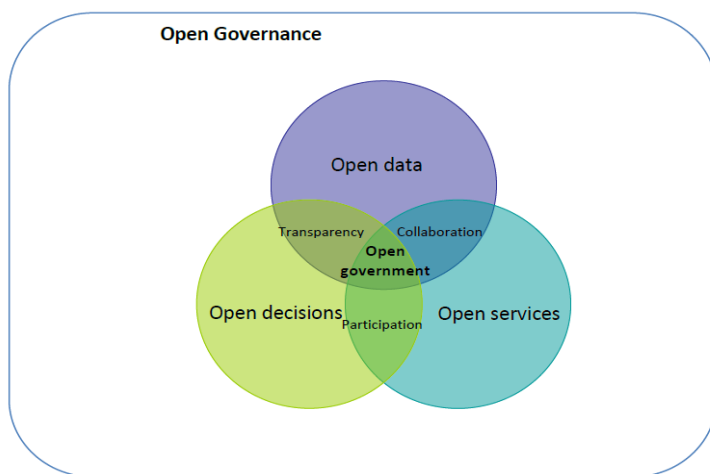
visuomeninėmis organizacijomis, pasitelkiant technologines naujoves, mažinant išlaidas, nes finansų krizės sukūrė naują impulsą modernizuoti viešąjį administravimą, paskatino ieškoti naujų ir kūrybingų būdų, kaip pagerinti elektroninių paslaugų teikimą ir kokybę.

Viešosios paslaugos turėtų tapti našesnėmis ir veiksmingesnėmis, o vyriausybės turi svarstyti naujoviškus būdus kuriant ir organizuojant viešąjį sektorių taip, kad jo vertė išaugtų. Atsižvelgiant į **mobilumo ir judumo ypatybes**, reikalinga užtikrinti galimybę žmonėms dirbti kartu, atlikti užduotis ir pasidalinti darbo krūviu nepriklausomai nuo atstumo ir sienų. Atsižvelgiant į naujų reiškinių atsiradimą: **socialinės žiniasklaidos, universalus mobiliojo ryšio ir Web 2.0**⁶⁶, pasinaudoti naujomis galimybėmis skleisti informaciją, kurti naujas paslaugas, bendradarbiauti su piliečiais. Tai apima ir dalyvavimą e. demokratijos tarp piliečių ir valdžios diskusijose ir sprendimų priėmime. Atvirų duomenų kūrimas viešajame sektoriuje, socialinių tinklų ir įvairių technologijų (medijos) naudojimas, galimybė dirbti naudojantis platformomis žymiai palengvina bendradarbiavimą su verslu ir piliečiais, skatina nekomercinių, atvirojo kodo programų kūrimą.

Šiuolaikiniai sudėtingi sprendimų priėmimai tarp skirtingų departamentų, institucijų, sektorių ir šalių reikalauja naujų technologinių sprendimų, todėl būtina vadovautis gero valdymo principais - atvirumas, dalyvavimas, atskaitomybė, veiksmingumas ir nuoseklumas, aukštos kokybės viešųjų paslaugų teikimas piliečiams, orientuojantis į dabartines ir ateities technologines tendencijas.

Dokumente aprašyti tokie vyriausybės modeliai ir pateikti jos bruožai:

– „**Atvira vyriausybė**“ - įgyvendina bendradarbiavimo, dalijimosi duomenimis ir skaidrumo principus.
– „**Skaitmeninės eros vyriausybė**“ – siūlo sutelkti dėmesį į visų paslaugų suskaitmeninimą.
– „**Naujoji viešoji vyriausybė**“ - interaktyvios formos, bendradarbiavimas, valdymo formavimas tarp organizacijų ir institucijų,
– „**Pertvarkos vyriausybė**“ - pabrėžia piliečių kaip partnerių, padedančių kurti paslaugas technologinėmis priemonėmis, pasitikėjimą.
– „**Tausi vyriausybė**“ – finansinei krizei pasirengusi vyriausybė.



14 pav. Atviros vyriausybės bruožai

Vyriausybė veikianti platformos pagrindu teikia nuoseklų informacijos ir duomenų surinkimą, paslaugų ir galimybių plėtrą, kad bendruomenės galėtų bendrauti, dalyvauti sprendimų priėmime, kurti ir išnaudoti savo galimybes, rinkas ir pažangą. Paslaugos turi būti prieinamos „Vieno langelio“ principu, **integruotos į kitas platformas**, o vartotojai galėtų jas įdėti į socialinių tinklų svetaines ar

⁶⁶ Web 2.0 – terminas, įvardijantis dabartinį tinklą kaip antrosios kartos internetą, kuris pagrįstas dalyvavimu per socialines bendruomenes (Facebook ar MySpace) ir kolektyviai kuriamą interneto turinį (pvz., per wiki ir blogus), t.y. internetas šioje koncepcijoje suvokiamas kaip įrankis sujungti ir integruoti mažus daugelio žmonių indėlius į bendrą informacijos ir žinių erdvę.

asmeninius puslapius. **Socialinės terpės platformos ir mobiliosios aplikacijos** ateityje turėtų vaidinti vis svarbesnį vaidmenį (ypač skubios pagalbos ir ekonominės plėtros srityse), todėl **suderinamumo** klausimai turėtų būti sprendžiami kartu siekiant teikti lokalizuotas paslaugas visos Europos mastu. Gali būti, kad kai kurios paslaugos bus perduotos privačiam sektoriui, kad sumažintų viešojo sektoriaus darbuotojų skaičių, todėl svarbūs išliks **teisiniai įsipareigojimai**, vertybės ir politiniai prioritetai.

Atvira vyriausybė gali paskatinti verslą diegti inovacijas, atsižvelgiant į lengvesnę prieigą prie mokslinių dokumentų ir duomenų. Tai gali paskatinti įmonių kūrimą, nes atviri duomenys ir viešojo sektoriaus informacija gali padėti sukurti naujas rinkas, produktus ir paslaugas bei gauti naujų pajamų - tai yra sukurti pridėtinę vertę, paskatinti naujų darbo vietų kūrimą. Naudojimasis realaus laiko duomenimis ir informacija gali padidinti gebėjimą greitai reaguoti į sparčiai kintančias problemas arba piliečiai galėtų pranešti apie vietos problemas, randamas žemėlapiuose. Šie pokyčiai institucijas palies technologiniu, politiniu, teisiniu, organizaciniu, darbo kultūros aspektu, kas pareikalaus tarnautojus sutelkti bendram metodo kūrimui, visų dalyvių į procesus įtraukimui.

Naujoji valdymo struktūra orientuota į koordinuotą bendradarbiavimą (valdžia – piliečiai - verslas), siekiant sutartų tikslų ir užtikrinant atsakomybės ir atskaitomybės mechanizmus per nustatytą teisinę sistemą. Modeliu siekiama **centralizuoti paslaugų teikimą viename portale**, kuriame piliečiai galėtų susipažinti su visomis vyriausybės teikiamomis paslaugomis, nepriklausomai nuo to, kuri institucija jas teikia. Taip keičiasi vyriausybės vaidmuo, nes verslas taip pat prisidės savo resursais, bus kuriamos hibridinės organizacijos (viešojo, privataus, socialinių įmonių). Vyriausybių vaidmuo bus valdyti ir koordinuoti visuomenės turtą, prisiimti tam tikras pareigas ir atsakomybę, pvz. už valstybinių duomenų kokybės standartų nustatymą, atskaitingumą, atitinkamos teisinės sistemos sukūrimą, įskaitant duomenų apsaugą ir kibernetinį saugumą.

Naujų sprendimų diegimui, sudėtingų problemų išsprendimui, bendradarbiavimui tarp partnerių reikalinga naujo tipo infrastruktūra. Nauji procesai ir metodai yra reikalingi decentralizavimo tarp valdžios ir kitų šalių architektūrai sukurti, integruojant didelių duomenų srautus ir socialines priemones. Taip pat turi būti sprendžiamos galimos problemos, susijusios su **kibernetinio saugumo, asmens privatumo ir duomenų apsaugos** klausimais. Neišvengiamai teks spręsti interoperabilumo (organizaciniu ir technologiniu lygiu), atvirųjų standartų ir debesų kompiuterijos klausimus. Web 3.0 plėtra susijusi su **duomenų, informacijos ir programų integracijos įrenginiais**, kad internetas taptų prasmingesniu ir užtikrintu bendradarbiavimo platforma. Atsižvelgiant į išorinių biuro (front-office) programų, socialinės žiniasklaidos ir veiklos mobilumo ypatumus, faktas, kad toliau tai turės didelį poveikį. Augantys tyrimai rodo, kad mobilusis ryšys gali radikaliai transformuoti vyriausybes ir suteikti prieigą prie viešosios

informacijos. „M. vyriausybė“ yra sekantis modelis, kuris bus sparčiai diegiamas naudojant IRT viešajame sektoriuje. Apskritai, viešajame sektoriuje dažnai reikalinga **kombinuoti technologijas**, pritaikant ir integruojant jas ir tai yra pats svarbiausias technologinis uždavinys. Paslaugos turi būti pritaikytos taip, kaip piliečiai galėtų bendrauti pasirinktu būdu, jos turi būti teikiamos taip, kad būtų prieinamos **įvairiais kanalais, įvairiais įrenginiais, įvairiais formatais**, personalizuotos pasirinktinu identifikavimo ir autentifikavimo būdu.

2.2. Lietuvos e. valdžios strateginiai dokumentai, skaitmeninė aplinka ir gairės

Jau 2002 m. LR Seimas patvirtino Valstybės ilgalaikės raidos strategiją, kurioje numatė, kad „šiuolaikinė valstybė turi ypatingą dėmesį skirti elektroninės vyriausybės galimybių plėtrai, diegti informacines technologijas viešojo administravimo srityje, skatinti valdžios institucijų veiklos veiksmingumą, plėtoti elektroniniu būdu teikiamas paslaugas ir elektroninę demokratiją“⁶⁷. Lietuvos informacinės visuomenės plėtros 2011–2019 metų programa toliau nustato informacinės visuomenės plėtros prioritetus, tikslus ir uždavinius, kad būtų kuo geriau naudojamosi informacinių ir ryšių technologijų teikiama socialinėmis ir ekonominėmis galimybėmis, o pirmiausia internetu – „labai svarbia ekonominės ir socialinės veiklos priemone, kuria naudojantis galima teikti ir gauti paslaugas, dirbti, pramogauti, bendrauti ir laisvai reikšti savo nuomonę“⁶⁸.

Toliau bus apžvelgta Lietuvos skaitmeninė aplinka, nagrinėjamos sąlygos, ar gyventojai ir verslas technologijų konvergencijos kontekste gali efektyviai naudotis e. paslaugomis, o valstybės institucijos - saugiai ir patikimai jas teikti bei pristatomi strateginiai teisiniai Lietuvos e. valdžios dokumentai, aptariamos e. valdžios prioritetų gairės, kryptys ir tikslai, pateikiama numatomų e. valdžios priemonių analizė, tiriamos sąlygos jų įgyvendinimui

Lietuvos statistikos departamento duomenimis, augant skaitmeniniams vartotojų poreikiams, mobiliaisiais telefonais 2013 m. naudojosi 96 % visų 16–74 metų amžiaus gyventojų, o kompiuterį namuose turėjo beveik 66 % namų ūkių:

3.1. Namų ūkiai, turintys išvardytus prietaisus, 2013 m.

3.1. Households with the devices listed, 2013

Procentais
Per cent

	Visi namų ūkiai <i>All households</i>	Mieste <i>Urban areas</i>	Iš jų – of which		Kaime <i>Rural areas</i>	
			5 didžiausiuose miestuose <i>5 largest cities</i>	kituose miestuose <i>other towns</i>		
Asmeninį kompiuterį	65,9	72,4	75,7	67,2	52,7	<i>Personal computer</i>
stalo kompiuterį	39,5	43,1	43,2	43,0	32,0	<i>desktop</i>
nešiojamąjį, planšetinį ar delninį kompiuterį	43,1	48,2	52,9	40,6	32,8	<i>portable computer (laptop, netbook, tablet)</i>
Mobilųjį telefoną	95,4	97,5	98,5	95,9	91,4	<i>Mobile phone</i>

16 pav. Galinių įrenginių panaudojimas paslaugoms gauti

⁶⁷ 2002 m. lapkričio 12 LR Seimo nutarimas. Nr. IX-1187 d. „Dėl Valstybės ilgalaikės raidos strategijos“

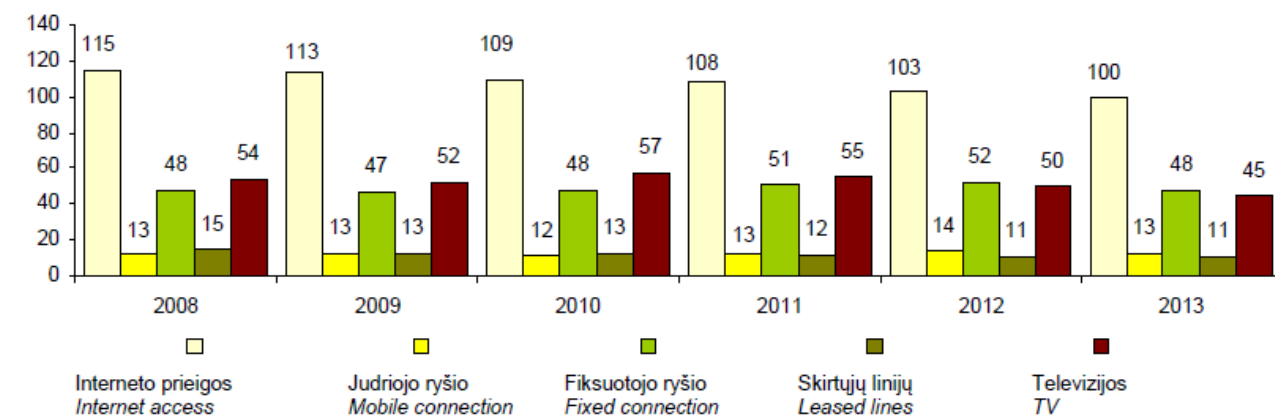
⁶⁸ 2011 m. kovo 16 d. Nr. 301 LRV nutarimas Dėl Lietuvos informacinės visuomenės plėtros 2011–2019 m. programos patvirtinimo

Kartu su plačiajuosčio ryšio plėtra bei naujomis interneto paslaugomis, kurioms paprastai reikia didelės spartos, interneto prieigos paslaugų gavėjai prioritetą teikia vis didesnei interneto spartai. 2012 m. šalyje 46,7 % visų plačiajuosčio interneto prieigos, teikiamos naudojant fiksuotojo ryšio technologijas, abonentų rinkosi 30 Mb/s ir spartesnį internetą. Tuo tarpu 53,3 % plačiajuosčio interneto naudotojų pasirinkta sparta buvo mažesnė nei 30 Mb/s.⁶⁹

Elektroninių ryšių rinkos dalyviai

Players on the electronic communications market

Lietuvos Respublikos ryšių reguliavimo tarnybos duomenys laikotarpio pradžioje
Data of the Communications Regulatory Authority, beginning of the period

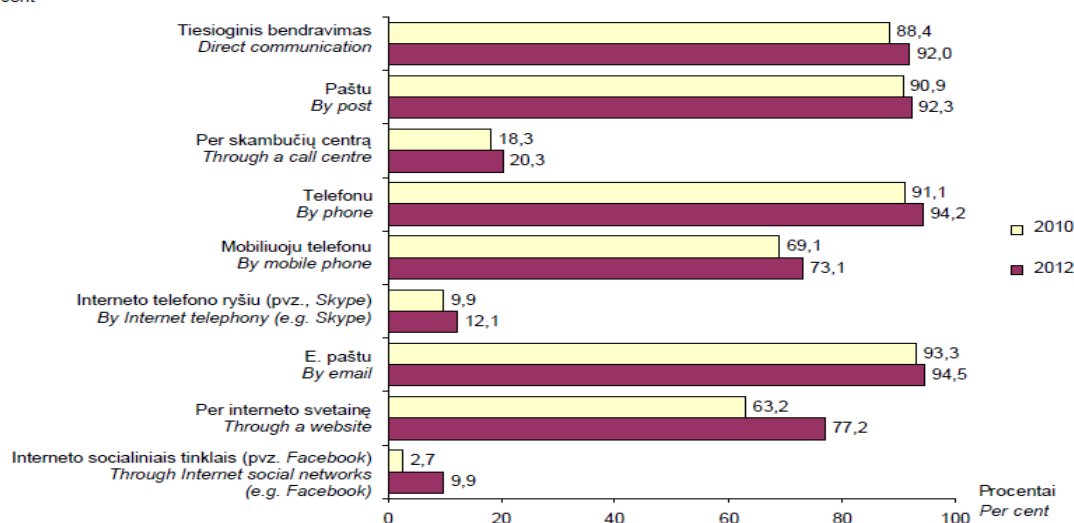


15 pav. Elektroninių ryšių rinkų dalyviai.

IVPK duomenimis, 2013 m. pradžioje pagrindinių viešųjų paslaugų perkėlimo į elektroninę terpę lygis Lietuvoje siekė 87 % (2012 m. - 82 %). Verslui skirtos paslaugos į internetą perkeliamos sparčiau negu skirtosios gyventojams - verslui skirtų paslaugų perkėlimo į internetą lygis 2013 m. pradžioje siekė 98 %, gyventojams - 79 %. 74 % teikiamų paslaugų - **visiškai interaktyvios**. Dauguma valstybės įstaigų (98,4 %) 2012 m. pradžioje naudojo plačiajuosčiu interneto ryšiu (2010 m. - 83,8 %). Daugiau kaip pusė (60,2 %) įstaigų turėjo šviesolaidinio (optinio) ryšio linijas, 43,7 % - skaitmenines abonentines linijas (DSL). Mobiliuoju interneto ryšiu naudojo 43,7 % įstaigų (mobiliuoju plačiajuosčiu ryšiu - 39,3 %). Beveik 12 % įstaigų naudojo ir lėto interneto ryšį (ISDN ar komutuojamąją liniją). 2012 m. pradžioje įstaigose kompiuterius savo darbe naudojo 82,8, internetą - 72,2 % darbuotojų (2010 m. pradžioje - atitinkamai 71,1% ir 62,6 %). Nors dauguma įstaigų viešąsias ir administracines paslaugas teikia tradiciniais būdais (paštu, telefonu ar priimdami interesus), populiarėja e. paslaugų teikimas socialiniais tinklais (pvz., Facebook, Myspace). Metų pradžioje informaciją ir konsultacijas socialiniuose tinkluose teikė 9,9 % įstaigų (2010 m. - 2,7 %). Valstybės institucijos teikdamos e. paslaugas naudojo įvairius būdus: per skambučių centrą, telefonu, mobiliuoju telefonu, interneto telefono ryšiu (pvz. Skype), e. paštu ir kt.:

⁶⁹ Informacinės technologijos Lietuvoje 2013 // <http://osp.stat.gov.lt/statistikos-leidiniu-katalogas?eventId=1135>, [2014 01 15].

Istaigos pagal viešųjų ir administracinių paslaugų teikimo būdus
Institutions by mode of provision of public and administrative services
 Procentais
 Per cent



17 pav. E. paslaugų teikimo būdai

Apibendrinant Lietuvos skaitmeninę aplinką, galima teigti, kad gerėja Lietuvos gyventojų naudojimosi internetu įgūdžiai, vis daugiau jų užsako prekes ir paslaugas internetu, įmonės vis daugiau bendrauja su viešosiomis institucijomis elektroninėmis priemonėmis, o viešajame sektoriuje vis daugiau e. paslaugų perkeliama į aukštesnį brandos lygį, populiarėja e. paslaugų teikimas socialiniais tinklais, IT žinias gilina vis daugiau institucijų darbuotojų⁷⁰. Akivaizdu, kad Lietuvos viešasis sektorius persitvarko, diegdamas naujus šiuolaikiškus metodus, technologijas bei aptarnavimo būdus, o konverguojančios technologijos ateityje turės dideles galimybes, valstybės institucijos turės adaptuoti teikiamas paslaugas mobiliems įrenginiams, bevielams tinklams.

Toliau bus analizuojami Lietuvos strateginiai e. valdžios dokumentai, kuriuose aptariama technologijų skverbties įtaka viešojo administravimo modernizavimui, numatomos e. valdžios prioritetų gairės, kryptys ir tikslai, pateikiama numatomų e. valdžios priemonių analizė.

Viešojo valdymo tobulinimo 2012–2020 metų programa⁷¹ iškelia uždavinius, kad viešasis valdymas bus modernizuojamas naudojantis naujų technologijų teikiamomis galimybėmis ir pabrėžiama, kad IRT naudojimas viešajam valdymui turėtų būti sisteminis, efektyvus ir saugus, pagrįstas asmens privatumo užtikrinimu ir patikimu asmenų identifikavimu elektroninėje erdvėje, reikalinga diegti šiuolaikiškas IRT sąveikumo sistemas, pagrįstas standartais ir sutartais principais (LST/ISO IT valdymo standartas 38500:2008). Siekiant mažinti IRT tvarkytojų funkcijų, turėtų būti taikomi veiklos ir minėtų technologijų sujungimo į bendrą įstaigų architektūrą metodai (TOGAF, COBIT, ITIL ir kiti).

⁷⁰ <http://statistika.ivpk.lt/ataskaitos>, [2014 03 03].

⁷¹ patvirtinta Lietuvos Respublikos Vyriausybės 2012 m. vasario 7 d. nutarimas Nr. 171 „Dėl Viešojo valdymo tobulinimo 2012–2020 metų programos patvirtinimo“

2014–2020 metų Nacionalinės pažangos programoje⁷² numatoma kaip skatinti prieinamų, kokybiškų ir sąveikių, IRT grindžiamų privačiųjų ir viešųjų paslaugų paklausą, skatinti piliečius, įskaitant pažeidžiamas jų grupes, verslo ir viešojo administravimo sektorius jomis naudotis, be kitų priemonių, įgyvendinant tarpvalstybines iniciatyvas. Naujų technologijų diegimui skiriamas didžiulis dėmesys pradedant pažangių informacinių ir kitų technologijų diegimu, modernizuojant švietimo įstaigų ir aukštųjų mokyklų infrastruktūrą, mokymosi ir ugdymo aplinką, diegiant ir plėtojant IRT į sveikatos priežiūros sistemą, kaip skatinti teigiamus pokyčius versle, kai šalį pasieks **naujausios pasaulio tendencijos, modernios technologijos ir nauji iššūkiai**. Siekiama užtikrinti, kad Lietuvoje sukurta, įdiegta ir naudojama IRT infrastruktūra būtų pažangi, atitinkanti aukščiausius saugumo reikalavimus ir naujausius technologijų pokyčius pasaulyje, taip pat aktuali – atitinkanti visuomenės ir verslo poreikius. Viešajam administravimui keliamas uždavinys:

5.1.4 uždavinys. Užtikrinti saugios, patikimos, sąveikos valstybės informacinių išteklių ir bendro naudojimo informacinių technologijų infrastruktūros plėtrą ir optimizuotą valdymą

Svarbus viešojo valdymo institucijų veiklos valdymo pagrindas yra sumanios, saugios ir efektyviai valdomos informacinės sistemos. Todėl įgyvendinant šį uždavinį, siekiama plėtoti racionalų viešojo sektoriaus bendro naudojimo informacinių išteklių valdymą, užtikrinti šių išteklių saugumą ir diegti „žaliuosius“, aplinką tausojančius ir energiją taupančius IRT sprendimus. Numatomos šios pagrindinės 5.1.4 uždavinio įgyvendinimo kryptys:

5.1.4.1. optimizuoti viešojo sektoriaus bendro naudojimo infrastruktūrą ir užtikrinti sąveikumą ir saugumą;

5.1.4.2. skatinti „žaliųjų“ IRT diegimą viešajame sektoriuje.

Diegiant pažangias informacines technologijas savivaldybių institucijų ir įstaigų veikla siejama su valdymo gerinimu (įskaitant teritorijų ir strateginį planavimą), administracinių paslaugų kokybės ir prieinamumo gyventojams didinimu, viešųjų ir socialinių paslaugų valdymo tobulinimu, gyventojų, nevyriausybinių organizacijų, ekspertų įtraukimu į vietos reikalų sprendimą.

Informacinės visuomenės plėtros 2014–2020 m. programa „**Lietuvos Respublikos skaitmeninė darbotvarkė**“⁷³. Joje nustatomi įgyvendinimo tikslai ir uždaviniai, aiškiai orientuoti į IRT plėtrą, daugelyje visuomenės ir valstybės veiklos sričių sparčiai kintantį procesą:

1. Mažinti Lietuvos gyventojų skaitmeninę atskirtį ir skatinti juos įgyti žinių ir įgūdžių, kad jie sėkmingai ir visapusiškai naudotųsi IRT;
2. Kurti technologiskai pažangias, gyventojų poreikius atitinkančias viešąsias ir administracines elektronines paslaugas, skatinti paslaugų gavėjus jomis naudotis;
3. Puoselėti IRT priemones Lietuvos kultūrą ir lietuvių kalbą – kurti visuomenės poreikius atitinkančią kultūrinę ir lietuvių rašytinės ir sakytinės kalbos sąsajomis pagrįstą skaitmeninį turinį, plėtoti skaitmeninius produktus ir elektronines paslaugas;
4. Skatinti naudoti IRT verslui plėtoti.

⁷² patvirtinta Lietuvos Respublikos Vyriausybės 2012 m. lapkričio 28 d. nutarimu Nr. 1482 „Dėl 2014–2020 metų Nacionalinės pažangos programos patvirtinimo“

⁷³ patvirtinta Lietuvos Respublikos Vyriausybės 2014 m. kovo 12 d. nutarimu Nr. 244 „Dėl Informacinės visuomenės plėtros 2014–2020 metų programos „Lietuvos Respublikos skaitmeninė darbotvarkė“ patvirtinimo“

5. Užtikrinti geografiškai tolygią sparčiojo plačiajuosčio ryšio infrastruktūros plėtrą ir skatinti naudotis interneto paslaugomis.
6. Užtikrinti saugios, patikimos, sąveikios IRT infrastruktūros plėtrą.

Programoje pabrėžiama, kad Valstybė yra didelės apimties informacinių išteklių kūrėja ir valdytoja. Valstybės institucijos disponuoja dideliais kiekiais duomenų ir naudojami IT tam, kad geriau atliktų joms pavestas funkcijas. Tačiau šiuo metu trūksta automatinės registrų ir valstybės informacinių sistemų sąveikos ir integralumo elektroninių priemonių, kurios užtikrintų informacijos aktualumą, patikimumą, pasiekiamumą. Jau šiandien ekonominė, socialinė ir kitokia veikla neįsivaizduojama be interneto, ir ši tendencija tik stiprės. Taigi reikėtų užtikrinti, kad valstybės mastu būtų kaupiama ir prieinama išsami informacija apie išteklius ir jų būklę, užtikrinta **automatinė valstybės informacinių sistemų ir registrų sąveika ir integralumas**.

Lietuvos informacinės visuomenės plėtros tendencijų ir prioritetų 2014-2020 metais vertinimo ataskaitoje (toliau - Ataskaita) Lietuva, pripažindama informacinės visuomenės plėtros ir IRT svarbą, svarbiausiose šalies plėtros strategijose **buvimo tarp lyderių scenarijų** įvardija kaip vieną iš horizontaliųjų prioritetų, gal net patį svarbiausią. Ataskaitoje išdėstoma vizija svarbiausiose visuomeninio gyvenimo srityse, nurodant kad:

1. Tobulinant viešąjį administravimą būtina galutinai pereiti prie keitimosi dokumentais tik elektroniniu būdu;
2. Plėtojant energetiką būtina išplėtoti pažangiuosius el. energijos tinklus (angl. smart grid);
3. Modernizuojant sveikatos paslaugas būtina pereiti prie elektroninės ligos istorijos ir el. recepto;
4. Ateities verslo plėtrai būtina mažinti administracinę naštą pasitelkiant IRT sprendimus;
5. Plėtojant transporto infrastruktūrą būtina naudoti pažangiąsias transporto sistemas;
6. Siekiant pritraukti IRT srities tiesiogines užsienio investicijas (TUI), būtina užtikrinti patikimą labai greito plačiajuosčio ryšio infrastruktūrą;
7. Įgyvendinant mokymosi visą gyvenimą viešąją politiką reikėtų siekti, kad šalies gyventojai ir darbo jėga taptų sumaniais IRT naudotojais (gebėtų naudotis el. parašu ir el. paslaugomis, pirkti internetu, užtikrinti savo asmens duomenų apsaugą ir t. t.).

Akivaizdu, kad naujųjų technologijų, jų mobiliosios savybės bei konvergencija glaudžiai susijusi su siekiama tapti pažangia, laisva, atvira ir demokratine valstybe. Lietuvai 2014–2020 m. laikotarpiu nubrėžiamos gairės - siūlomos iniciatyvos, susijusios su technologijų konvergencija:

1. Visuotinai prieinamas ir labai greitas plačiajuostis internetas;
2. Šalies gyventojai – sumanūs interneto vartotojai;
3. Interneto turinys lietuvių kalba ir Lietuvos kultūros paveldas internete;
4. Visos viešosios ir administracinės e. valdžios paslaugos prieinamos ir naudojamos internetu;
5. Viešojo sektoriaus IRT optimizavimas ir sumanus valdymas;
6. IRT gebėjimai ir IRT sprendimai ateities verslui;
7. Žaliosios IRT ir darni plėtra;
8. Asmens ir valstybės informacinių išteklių saugumas internete.

Ataskaitoje taip pat pateikiamos kryptys, kuriomis konverguojančios technologijos lems naujų paslaugų atsiradimą arba tradicinių paslaugų perkėlimą į aukštesnius brandos lygius:

1. Pranešimai apie korupciją telefonu (garso, vaizdo įrašas integruojamas į institucijos e. dokumentų valdymo sistemą), vaizdo įrašai pateikiami kaip nusikaltimo įrodomoji medžiaga skundo (pranešimo) pateikimui (teikti pranešimus policijai internetu, gauti informaciją apie nusikaltimus ir eismo įvykius SMS ir MMS žinutėmis ir pan.); galimybė pateikti prašymus / gauti leidimus (sprendimus) įvairiais kanalais, įrenginiais, formatais;
2. Robotizavimo plėtojimas lituanizavimo projektuose;
3. Išmaniųjų telefonų integravimas į paslaugų įgyvendinimą;
4. Išmaniųjų „debesų kompiuterijos“ kūrimas (valstybės informacinių išteklių perkėlimas į valstybinį „debesį“);
5. Perėjimas prie atsiskaitymo e. sąskaitomis kas leistų sutaupyti virš 1mln.Lt/metus;
6. Valstybės sprendimai dėl sumaniųjų technologijų įtraukimo į nacionalinius strateginius energetikos dokumentus (Pažangiųjų tinklų (*Smart grid*) plėtros krypties nustatymo darbo grupė koordinuoja pažangiųjų tinklų plėtros proceso eigą Lietuvoje);
7. Telemedicina;
8. El. demokratija- savivaldybių tarybų, Seimo posėdžių transliavimas ir piliečių interaktyvus dalyvavimas priimant sprendimus.

Ataskaitoje pažymima, kad Lietuvos IRT sektorius turi daug pranašumų, nes Lietuvoje yra labiausiai išvystyta pramonė Baltijos šalyse, labiausiai kvalifikuoti IT specialistai Vidurio ir Rytų Europoje, bendradarbiavimas su mokslininkais duoda ženklių vaisių, kuriant bendrus projektus, parkus, centrus, atliekant mokslinius tyrimus, sparti paslaugų technologijų plėtra bei augančios investicijos į e. ryšių infrastruktūrą, padeda privataus ir viešojo sektoriaus perėjimui nuo spartaus augimo į stabilią plėtrą.

Kaip jau buvo minėta, jog viešojo administravimo modernizavimo kriterijai gali būti dvejopi: viena, orientuoti į strateginių visuomenės tikslų įgyvendinimą, antra, siekiantys optimizuoti pačią valdžią. Pastarasis kriterijus detalai buvo nagrinėjamas tiek technologiniu požiūriu, tiek aptariant strateginius teisinius dokumentus. Akivaizdu, kad tiek Lietuvoje, tiek Europoje, tiek visame pasaulyje pastebima e. valdžios modelių transformacija į naujus, pažangius valdymo modelius, kuriems be abejo turi įtakos technologijų konvergencija. Tai leidžia kalbėti apie komponentinės e. valdžios infrastruktūros kūrimo kryptį, kai planuojama jog e. valdžios technologinės platformos veiks aukšto patikimumo „visur esančioje“ aplinkoje⁷⁴, palaikančioje sistemas ir taikomas programas, surinktas iš rinkoje jau sukurtų komponentų. Tokio tipo infrastruktūra leistų sumažinti e. valdžios sistemų kūrimo išlaidas. Mokslininkai pasisako apie intelektualias naujo tipo e. valdžios sistemas, kurių realizavimui reikalinga ne tik numatyti struktūras ir standartus, bet ir nuolat tobulinti naujausias technologijas, informaciją bei žinias. Tai būtų visuotinio žinojimo arba aplinkos intelekto koncepcijos⁷⁵, ontologijos ir informacijos bei žinių valdymo sistemos, kolektyvinių

⁷⁴ Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas : kolektyvinė monografija / Vilnius : Mykolo Romerio universiteto Leidybos centras, 2009, p. 156

⁷⁵ Aplinkos intelektas - tai vizija, kurioje žmonės gyvena supami skaičiavimus atliekančių įrenginių, sujungtų į bendrą tinklą ir įdiegtų gyvenamojoje aplinkoje

kompetencijų kūrimo ir sprendimo priėmimo sistemos, dirbtinio intelekto sistemos, susietos su įterptinių sistemų ir bevielių sensorinių tinklų technologijų plėtra, semantinio tinklo plėtra⁷⁶.

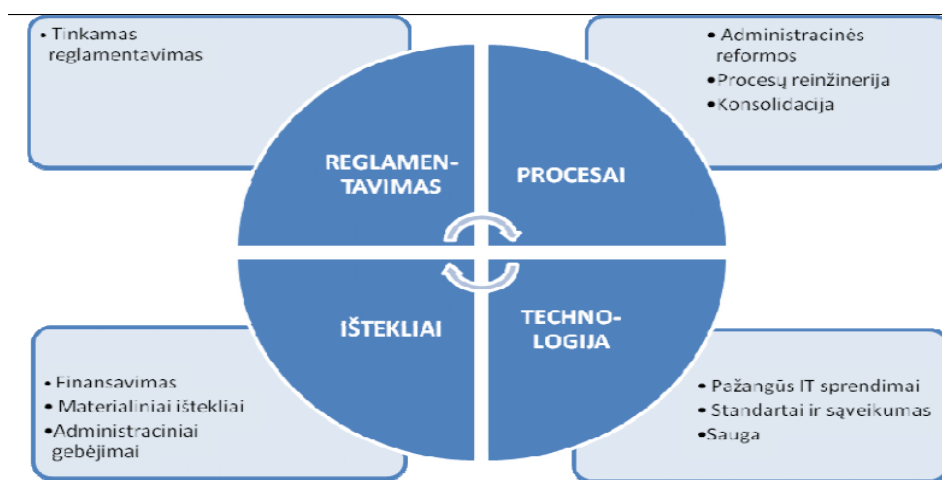
Strateginių visuomenės tikslų įgyvendinimas, globalių problemų sprendimas neapsiriboja vien technologiniais sprendimais, nes naujausių technologijų taikymas e. valdžios kontekste taip pat iškelia ir vertybinius klausimus. Suprantama, kad jokios technologijos negali įtakoti žmogiškuosius pasirinkimus, kai priimami strateginiai sprendimai, o vadovas atsiduria prieš pasirinkimą: ar visada vadovautis bendrojo gėrio supratimu, ar virš asmeninių ambicijų iškelti visuomenės gerbūvio poreikius. Jeigu pasirenkama priešingai, technologijos gali tapti griauinančiu blogiu. Pavyzdžiui, vykstant informaciniams karams nedraugiškų antidemokratinų valstybių valdžia įvairiais informaciniais kanalais siekia iškreipti tiesą, šmeižti demokratines valstybes, joms grasindama ne tik branduoliniais, bet ir nuolat tobulėjančiais kibernetiniais ginklais. Valstybės jau turėjusios skaudžios patirties, kai neretai politinio užsakomojo pobūdžio kibernetinėmis atakomis buvo atakuojamos jų valstybinės įstaigos, strateginiai objektai, patiria didelių nuostolių. Tada valdžia privalo imtis atsakomųjų saugumo priemonių, kurios ne tik brangiai kainuoja, bet ir reikalauja kvalifikuotų ekspertų parengimo, didelės atsakomybės, išmintingo vadovavimo, operatyvaus ir savalaikio reagavimo. Neretai informacinių karų akivaizdoje valstybėms iškyla problema, kaip užtikrinti valstybinių informacinių išteklių kibernetinį saugumą. Kitas svarbus aspektas - tolesnis e. valdžios ir e. demokratijos plėtros procesų tobulinimas, kaip savalaikis ir operatyvus valdžios atsakas į naujos kartos tinklų ir technologijų galimybes, pasirinkimas apsaugoti ne tik valstybinius informacinius išteklius, bet ir žmogaus privačią erdvę, asmeninę informaciją, įgalinimas saugiai ja keistis, aktyviai dalyvauti patikimoje viešojoje aplinkoje. Apie tai plačiau trečiame skyriuje.

⁷⁶ kai siekiama sukurti universalią aplinką informacijos mainams internete, suteikiant ten esančių duomenų turiniui tokią semantiką, kuri būtų lengvai suprantama kompiuteriui, t.y. kompiuteriai savarankiškai atlieka informacijos paiešką ir ją apdoroja.

III. Specialaus teisinio reguliavimo pavyzdžiai

3.1. Informacijos saugos teisiniai aspektai Valstybės informaciniuose ištekliuose

Kaip jau buvo aptarta antrame skyriuje viešojo administravimo modernizavimas, valdymo procesuose diegiant pažangias IRT, pastaraisiais metais daugelyje ES šalių tapo vienu svarbiausių uždavinių. Šalys renkasi valstybinių informacinių išteklių reformų kelią, siekiant juos centralizuoti, užtikrinti techninį, organizacinį ir semantinį sąveikumą, deklaruojami siekiai pereiti prie valstybinių debesų kompiuterijos infrastruktūrų, duomenų bazių konsolidavimo mechanizmų. Lietuvoje, kaip ir daugelyje ES šalių, siekiama tokiais centralizuotais sprendimais plėtoti elektroninę valdžią, efektyviau teikti viešąsias paslaugas, palengvinti ir pagreitinti valstybės institucijų darbą priimant sprendimus. Valstybės informaciniai ištekliai yra vienas iš esminių veiksnų, lemiančių e. valdžios plėtrą šalyje, todėl akivaizdu, kad intensyvėjant technologijų konvergencijos procesui, vis daugiau dėmesio skiriama valstybinių informacinių išteklių, informacijos saugumui, tuo siekiant sudaryti palankias sąlygas vartotojų pasitikėjimui informacinėmis bei ryšių technologijomis, saugia informacinės visuomenės plėtra, patikima e. valdžios aplinka. Viena iš esminių valstybės informacinių išteklių (tuo pačiu ir e. valdžios) plėtrai būtinų sąlygų - technologijų saugos užtikrinimas:



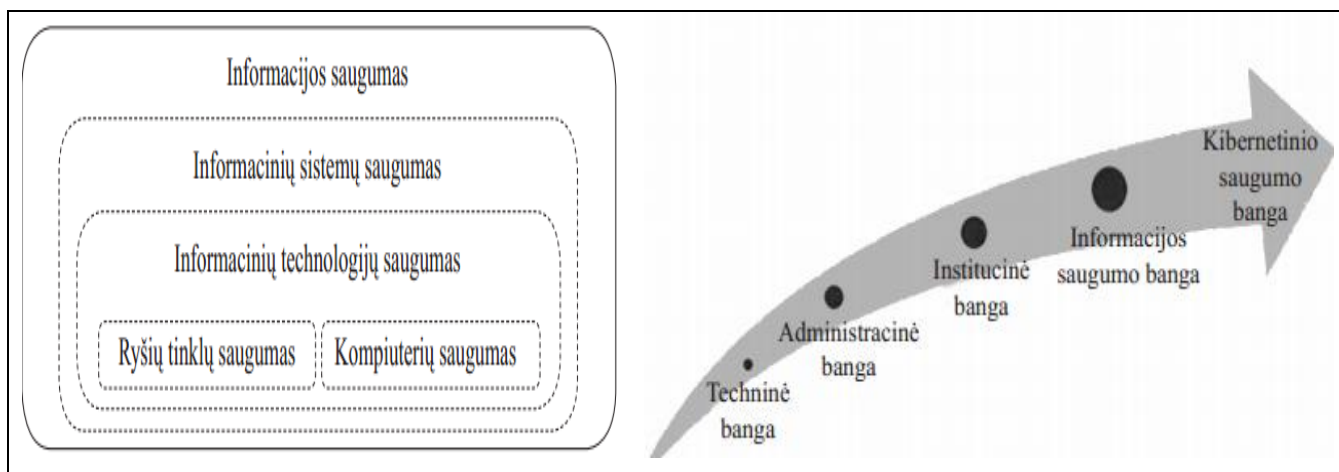
18 pav. Valstybės informacinių išteklių plėtros, teisinio reglamentavimo, IT sprendimų ir saugos sąsajos⁷⁷

Pažymėtina, kad mokslo darbuose bei teisės aktuose sutinkamos kelios saugos (saugumo) sampratos: Informacijos saugumas (sauga) suprantamas 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. Kitas terminas - elektroninės informacijos sauga suprantamas kaip elektroninės informacijos ir elektroninės informacijos infrastruktūros apsauga. Trečias terminas - kibernetinis saugumas (angl.

⁷⁷

http://www.lrv.lt/bylos/VORTprojektas/Dokumentai/2- Informaciniu%20istekliu%20valdymo%20ist%20poveikio%20vertinimo%20projektas_2011%2005%2024.pdf, [2014 03 07].

Cybersecurity) apibrėžia elektroninį saugumą⁷⁸, sutinkami ir kiti terminai: valstybės informacinių išteklių, duomenų, kompiuterių, ryšių tinklų, informacijos technologijų, informacinių sistemų saugumas (apsauga, sauga), kas neretai teisės aktuose įneša painiavos. Dr. S. Jastiuginas informacijos saugumo srities sąvokų sąsajas pavaizduoja taip⁷⁹:



19 pav. Informacijos saugumo sąvokos samprata ir raida.

Darbe kaip sinonimai bus naudojami terminai: „informacijos sauga“ ir „kibernetinis saugumas“, kadangi teisės aktuose daugiausia naudojamos šios sąvokos. Be to, darbe iškilo būtinybė labiau paaiškinti **kibernetinio saugumo** problematiką atskira dalimi, kadangi šiuo metu yra svarstomas Kibernetinio saugumo įstatymo projektas, nustatomos kompetetingos institucijos, jų funkcijų paskirstymas ir atsakomybė.

Tiek strateginiuose Lietuvos dokumentuose nustatant prioritetus, tiek tarpvalstybiniuose valdžios viršūnių susitikimuose aptariant svarbiausius klausimus, kibernetinio saugumo aspektas tampa vis aktualesniu. „Kibernetinio saugumo klausimai šiuo metu jau nebėra vien NATO kompetencija - jie tampa vis svarbesni ir Europos Sąjungai. Nagrinėjami ne tik valstybių ir jų institucijų apsaugos aspektais, tačiau vis aktualesnė tampa ir asmenų apsauga“- dalyvaudama Miuncheno saugumo konferencijoje Lietuvos Respublikos Prezidentė Dalia Grybauskaitė taip pristatė Lietuvos patirtį kibernetinio saugumo srityje.⁸⁰

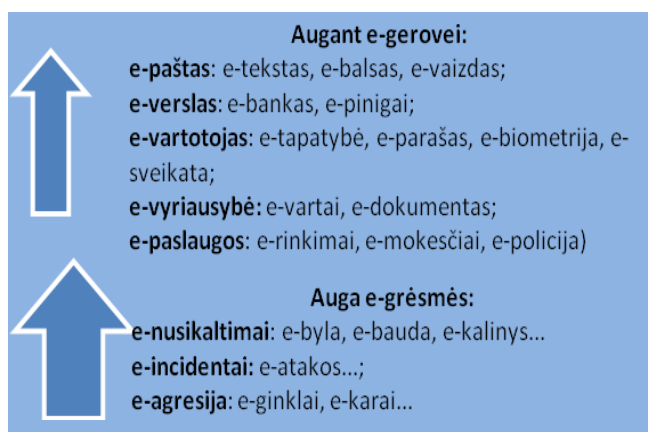
Kibernetinis saugumas tampa vis aktualesnė problema dėlto, kad šalys jau turi kibernetinių incidentų poveikio patirties, kai buvo patirta didelių nuostolių dėl dirbtinai sukeltų informacinių karų, užsakomojo (ir politinio) pobūdžio kibernetinių atakų, o tai turėjo įtakos ne tik šalies elektroniniams ryšių tinklams, informacinėms sistemoms, nacionaliniam saugumui, strateginiams objektams, bet sutrikdė valstybės institucijų, įmonių veiklą, atsiliepė piliečių gerovei.

⁷⁸ Štītis D., Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai, Socialinės technologijos, 2012, 2(2), p. 441-455

⁷⁹ Jastiuginas S. Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. Informacijos mokslai. 2011 57

⁸⁰ http://www.president.lt/lt/spaudos_centrus_392/pranesimai_spaudai/kibernetinis_ir_energetinis_saugumas_-_lietuvos_prioritetas.html

LR Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT-LT duomenimis, didžiausios 2013 m. saugumo problemos buvo valstybės institucijų informacinių sistemų nepasiekiamumas; asmens duomenų nutekėjimas; įsilaužimas į institucijų svetaines; neteisinga informacija valstybės registruose; nekorektiškai teikiamomis elektroninėmis paslaugomis⁸¹. Kenkimo programos aktyviai plito ir mobiliuosiuose įrenginiuose (išmaniuosiuose telefonuose, planšetiniuose kompiuteriuose ir pan.) Ekspertų teigimu vienos populiariausių šiandienos grėsmių – duomenų perėmimas keliant juos belaidžiu ryšiu iš vieno įrenginio į kitus, galinių įrenginių užvaldymas panaudojant kenkėjiškas programas, taip perimant jų kontrolę kenkėjiškiems tikslams⁸². Konvergencijos dėka technologijos perima viena kitos funkcijas ir gali sąveikauti tarpusavyje, dėl ko saugumas tampa aktualus ne tik kompiuteriams, bet ir mobiliems, virtualiems įrenginiams. Šiame technologijų amžiuje dideliais tempais augantis informacinių sistemų kompleksiskumas (e. bankininkystė, e. vyriausybė, e. paslaugos ir t.t.) ir jų integravimas į interneto tinklą lemia sudėtingų kompiuterių sistemų valdymo programų kūrimą, o tai savo ruožtu didina riziką, kad tokiose programose atsiranda daugiau saugumo spragų, kurias piktavaliai gali panaudoti vartotojo kompiuterių, valstybės informacinių išteklių pažeidimams. Spragų aptinkama ne tik interneto svetainėse, elektronines paslaugas teikiančiose platformose, bet ir taikomojoje programinėje įrangoje: interneto naršyklės, operacinės sistemos, dokumentų peržiūros įrankiai bei kita naudojama programinė įranga vis dažniau tampa pažeidžiama. Ekspertai prognozuoja, jog ši tendencija stiprės ir ateinančiais metais taps viena iš didžiausių saugumo grėsmių. Informatikos ir ryšių departamento prie VRM direktorius G. Čiurlionis, pristatydamas informacijos saugumo problemas Lietuvoje, akcentuoja, kad technologijų konvergencijos įtakoje augant **e-gerovei** auga ir **e-grėsmės** bei nurodo, kad kibernetiniais ginklais gali tapti ne tik kompiuteriai, bet ir kiti galiniai įrenginiai (išmanieji telefonai, planšetiniai kompiuteriai ir pan.):



20 pav. Technologinis galinių įrenginių panaudojimas kibernetinėms atakoms⁸³

⁸¹ Per šį laikotarpį CERT-LT ištyrė 11 125 kenkimo programinės įrangos panaudojimo atvejus, t.y. 43,9% visų tirtų incidentų.

⁸² <http://www.eset.com/lt/apie/spauda/straipsniai/article/kibernetiniai-sukciai-taikosi-i-ismaniuosius-irenginius/>

⁸³ http://www.slideshare.net/AB_TEO_LT/gintaras-iurlionis-kibernetins-erdvs-ikiai-lietuvoje, [2014 03 22].

Toliau bus apžvelgiama, kokios institucijos informacijos saugos srityje formuoja, organizuoja, koordinuoja informacijos saugos politiką ir kontroliuoja jos įgyvendinimą, kokios ją įgyvendina ir atlieka priežiūrą bei kokie pagrindiniai teisės aktai reglamentuoja šią sritį.

Šiuo metu už elektroninių ryšių tinklų ir informacijos saugą Lietuvoje atsakingos šios institucijos: Susisiekimo ministerija, Vidaus reikalų ministerija (toliau - VRM), Ryšių reguliavimo tarnyba (toliau - RRT), Krašto apsaugos ministerija (toliau - KAM), IVPK, Nusikaltimų elektroninėje erdvėje tyrimo valdyba, Valstybinė duomenų apsaugos inspekcija, Valstybės saugumo departamentas. Pagal kompetenciją joms priskirtos šios saugos funkcijos:

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

2 lentelė. Elektroninių ryšių tinklų ir informacijos saugos klausimais Lietuvoje dirbančių institucijų funkcijos⁸⁴

Iš minėtų institucijų didžiausią įtaką užtikrinant Lietuvos elektroninių ryšių tinklų ir informacijos saugumą turi VRM, Susisiekimo ministerija ir RRT, planuojama stiprinti KAM atsakomybę už kibernetinio saugumo politikos formavimą. Pažymėtina, kad institucinė sąranka

⁸⁴ <http://www.vkontrole.lt/failas.aspx?id=1684>, [2014 03 10].

informacijos saugumo srityje yra gana paini, nes pagal šiuo metu svarstomą Kibernetinio saugumo įstatymo projektą už kibernetinio saugumo politikos formavimą siūloma atsakomybę priskirti Krašto apsaugos ministerijai, o Vidaus reikalų ministerija būtų atsakinga tik už ypatingos svarbos informacinės infrastruktūros metodikos parengimą ir objektų sąrašo patvirtinimą bei informacijos saugos politikos formavimą, valstybės informacinių išteklių saugos užtikrinimą. Kibernetinio saugumo politiką įgyvendinančios institucijos yra: Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, Valstybinė duomenų apsaugos inspekcija, Ryšių reguliavimo tarnyba ir iš dalies Policijos departamentas prie VRM. Išanalizavus atsakomybės ir kompetencijos sritis pagal institucinę sąranką, kyla klausimas, ar priėmus Kibernetinio saugumo įstatymą nebus funkcijų dubliavimo, kaip bus paskirstyta atsakomybė.

Kalbant apie institucijų indėlį informacijos, tinklų ir technologijų saugumo srityje pažymėtinos RRT iniciatyvos:

-įkurtas Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT, kuris atlieka elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimus, veiksmų koordinavimą sprendžiant incidentus, rengia rekomendacijas apie grėsmes, organizuoja seminarus.

-sukurtas Internetinis portalas www.esaugumas.lt, skirtas visuomenės švietimui IT saugumo klausimais. Šiame tinklalapyje skelbiama aktuali informacija tinklų ir informacijos saugumo tema, skelbiami įvairūs tinklų ir informacijos saugumo srities tyrimai, pranešimai apie naujas grėsmes, siūlomos konkrečios priemonės ir būdai bei pateikiami patarimai, padedantys išvengti pavojų tykančių elektroninėje erdvėje.

-sukurta Internetinė svetainė www.draugiskasinternetas.lt kad atkreipti visuomenės dėmesį į nelegalią ir žalingą informaciją internete, skatinti saugesnį, ypač vaikų, naudojimąsi internetu ir naujomis technologijomis, supažindinti su galimais apsisaugojimo nuo tokios informacijos būdais.

- filtravimo priemonių įdiegimas ir veikimas. Prieigos prie viešųjų kompiuterių tinklų (interneto) paslaugas teikiantys asmenys privalo užtikrinti Lietuvos Respublikos ryšių reguliavimo tarnybos (RRT) aprobuotų žalingo interneto turinio, darančio neigiamą poveikį nepilnamečiams, filtravimo priemonių įdiegimą ir veikimą. RRT teikimu Vyriausybė nustato prieigos prie viešųjų kompiuterių tinklų (interneto) vietose privalomų filtravimo priemonių naudojimo tvarką.

Pažymėtina RRT parengta medžiaga internetiniame portale www.esaugumas.lt, kur pateikiamos ir aptariamasi naujausios saugumo spragos ir priemonės joms įveikti. Nors medžiaga pateikiama plačiai visuomenei, tačiau ji yra aktuali viešojo administravimo institucijoms, kurios perkelia elektronines paslaugas į mobilius, virtualius įrenginius, belaidžius tinklus, darbe naudoja įvairius galinius įrenginius. 3 priede pateikiamas aktualių grėsmių sąrašas, kai naudojamos naujausios technologijos (elektroninių paslaugų teikimas mobiliais, virtualiais įrenginiais, belaidžiais tinklais). Sąrašas yra didelis ir nebaigtinis, tačiau kyla klausimas, ar jis tinkamai įvertintas, ar sava laikais yra reglamentuojami saugumo aspektai teisės aktuose. 4 priede pateikti kai kurie svarbiausi šiuo metu informacijos saugą reglamentuojantys teisės aktai, jų priėmimo datos bei nuorodos į teisės aktų punktus, kuriuose aptariamas požiūris į kintančias technologijas. Kaip matosi iš pateiktos teisės aktų lentelės tinklų ir technologinių sprendimų saugumo nuostatų dėl įrenginių

mobilumo nėra daug, kai kurie teisės aktai yra neatnaujinti ir nebeaktualūs. Atkreiptinas dėmesys, kad Lietuvoje informacijos saugumo nuostatos fragmentiškai reglamentuotos ir kituose teisės aktuose: LR Elektroninių ryšių, LR Asmens duomenų teisinės apsaugos, LR Autorių teisių ir gretutinių teisių, LR Elektroninio parašo ir kt. įstatymuose, Vyriausybės nutarimuose, kt. teisės aktuose, kas neužtikrina visapusiško ir nuoseklaus tinklų ir elektroninės informacijos saugumo, visuomeninių santykių reglamentavimo, nesudaro sąlygų vartotojų pasitikėjimui informacine visuomene ir saugios informacinės visuomenės plėtra⁸⁵.

3.2. Kibernetinio saugumo teisinis reglamentavimas ES ir Lietuvoje

Kibernetinio saugumo klausimai aktyviai buvo pradėti eskaluoti Lietuvos pirmininkavimo Europos Sąjungos Tarybai laikotarpiu bei įvykus eilei kibernetinių incidentų Lietuvoje ir pasaulyje, kai buvo atakuojamos valstybės institucijos bei strateginiai objektai (bankai, žiniasklaida, atominės elektrinės ir pan.). Nors pagal RRT statistiką kibernetinių incidentų Lietuvoje kasmet vis daugėja (2013 m. jų būta per 25 tūkst.), tačiau nusikaltimų, susijusių su kibernetine erdve, tyrimų nėra daug. Iš dalies taip yra dėl to, kad daugelis kibernetinių nusikaltėlių aukų, kuriomis tampa tiek valstybės įstaigos, tiek įmonės (bankai, kredito įstaigos, draudimo bendrovės) viešai apie tai dažniausiai neskelbia, nesikreipia į teisėsaugos institucijas, stengiasi laikyti tai paslapyje, nes vieni gal neišmano ar bijo biurokratinių tyrimų, kiti nenori, kad aplinkiniai, visų pirma - jų klientai, sužinotų apie jų apsaugos sistemose esančias spragas, silpnąsias vietas ir imtų jais nepasitikėti. Nors LR Baudžiamasis kodeksas reglamentuoja kibernetinius nusikaltimus ir numato atsakomybę už jų įvykdymą⁸⁶, teisėsaugos institucijoms nelengva ištirti ir atskleisti įvykdytą kibernetinį nusikaltimą dėl daugelio priežasčių: reikia ypač daug specialių techninių žinių, nusikaltėliai, įvykdę nusikaltimą kompiuterio pagalba, dažniausiai turi labai daug galimybių išsisukti nuo teisinės atsakomybės, nes teisėsaugos pareigūnai, atlikę tyrimą ir nustatę kompiuterį, kuriuo buvo pasinaudota vykdant nusikaltimą, dažnai patenka į aklavietę, nes neturi reikiamų įrodymų, kad tuo kompiuteriu pasinaudojo būtent jų įtariamas asmuo, o taip pat ir dėl kai kurių konkrečių nusikalstamų veikų teisinio reglamentavimo spragų. Tai yra problema, su kuria susiduria teisėsaugos institucijos ne tik Lietuvoje, bet ir kitose šalyse⁸⁷.

Prof. D. Štītis akcentuoja, kad kibernetinis saugumas yra labai svarbi ir specifinė veiklos rūšis, kuri reikalauja nuoseklaus ir detalaus teisinio reglamentavimo. Nors analizuojant ES ir Lietuvos teisinę bazę kibernetinio saugumo aspektu, sunku atskirti viešąjį ir privatų sektorių

⁸⁵ Štītis D., Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai, Socialinės technologijos, 2012 2(2), p. 441-455

⁸⁶ LR BK yra numatytas skyrius "Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui" (XXX sk.) bei straipsniai, reglamentuojantys nusikaltimus susijusius su kibernetiniais nusikaltimais (pvz. 167 str., 168 str., 182 str., 207 str., 215 str., 300 str.)

⁸⁷ <http://www.kibererdve.lt/teises-aktai-ir-statistika/teises-aktai>, [2014 02 21].

(kadangi valstybės institucijos naudoja paslaugų teikėjų paslaugomis, o pastarieji yra valstybinių išteklių naudotojai), toliau bus didesnis dėmesys skiriamas valstybinių informacinių išteklių kibernetinio saugumo teisiniam reguliavimui ES ir Lietuvoje.

Kibernetinio saugumo reglamentavimas ES. Pažymėtina 2013 m. vasario 7 d. ES priimta **Kibernetinio saugumo strategiją "Atvira, saugi ir patikima kibernetinė erdvė"**, kurioje nustatyti šie ES tarptautinės kibernetinės erdvės politikos prioritetai:

- Laisvė ir atvirumas. Strategijoje bus išdėstyta svarbiausių ES vertybių ir pagrindinių teisių taikymo elektroninėje erdvėje vizija ir principai.
- Teisės aktai, normos ir pagrindinės ES vertybės kibernetinėje erdvėje galioja lygiai taip pat, kaip ir fiziniame pasaulyje. Atsakomybė už saugesnę kibernetinę erdvę tenka visiems pasaulinės informacinės visuomenės dalyviams, pradedant piliečiais, baigiant vyriausybėmis.
- Didinti kibernetinio saugumo pajėgumus. ES bendradarbiaus su tarptautiniais partneriais ir organizacijomis, privačiuoju sektoriumi ir pilietine visuomene, kad padėtų didinti pasaulinius pajėgumus trečiosiose šalyse. Bus rūpinamasi didesne prieiga prie informacijos bei atviro interneto ir užkertamas kelias kibernetinės erdvės pavojams.
- Skatinti tarptautinį bendradarbiavimą kibernetinės erdvės klausimais. Išsaugoti atvirą, laisvą ir saugią kibernetinę erdvę yra pasaulinio masto uždavinys, kurį ES spręs kartu su atitinkamais tarptautiniais partneriais ir organizacijomis, privačiuoju sektoriumi ir pilietine visuomene⁸⁸.

Strategijoje akcentuojamas bendros atsakomybės užtikrinant kibernetinį saugumą klausimas, kadangi tiek viešasis sektorius, tiek privačios įmonės, tiek individualūs vartotojai turi **pripažinti bendrą atsakomybę**, imtis apsaugos priemonių, koordinuoti veiksmus, esant reikalui. 2013 m. pradėtas rengti ES kibernetinio saugumo strategijos įgyvendinimo priemonių planas.

ES kibernetinio saugumo srities klausimai, susiję su viešuoju sektoriumi, labiau yra aptarti Europos Parlamento ir Tarybos **direktyvos dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui** projekte, kuriame siūloma nustatyti saugumo reikalavimus ne tik rinkos dalyviams, bet ir viešojo administravimo institucijoms, nustatomi įpareigojimai visoms valstybėms narėms, susiję su tinklų ir informacinių sistemoms poveikio turinčios rizikos ir incidentų prevencija, valdymu ir atsakomaisiais veiksmais. Jame siūlomas sukurti valstybių narių bendradarbiavimo mechanizmas, skirtas užtikrinti vienodą šios direktyvos taikymą visoje Europos Sąjungoje ir, kai reikia, koordinuotą ir efektyvų tinklų ir informacinių sistemoms poveikio turinčių rizikos ir incidentų valdymą bei atsakomuosius veiksmus. Projekte siūloma, kad Nacionalinės tinklų ir informacijos saugumo (TIS) sistemai sukurti ir koordinuoti veiksmus būtų kuriamos nacionalinės TIS kompetentingos institucijos, kurios turėtų pakankamai techninių, finansinių ir žmogiškųjų išteklių, kad galėtų efektyviai ir veiksmingai vykdyti joms pavestas funkcijas. Valstybės narės turėtų užtikrinti efektyvų, veiksmingą ir saugų kompetentingų institucijų bendradarbiavimą tam sukurtame tinkle, kad kompetentingos institucijos gautų pranešimus apie incidentus iš viešojo administravimo institucijų ir rinkos dalyvių ir kad joms būtų suteikti

⁸⁸ http://eeas.europa.eu/policies/eu-cyber-security/index_lt.htm, [2014 03 29].

įgyvendinimo ir vykdymo užtikrinimo įgaliojimai. Pagal Projektą kompiuterinių incidentų tyrimo tarnybos (CERT) būtų atsakingos už incidentų ir rizikos valdymą taikant tiksliai nustatytą procesą, kuris atitiktų Direktyvoje nustatytus reikalavimus, o Valstybės narės užtikrintų, kad CERT turėtų pakankamai techninių, finansinių ir žmogiškųjų išteklių, kad galėtų efektyviai vykdyti užduotis, kad nacionaliniu lygmeniu CERT remtųsi saugia ir atsparia ryšių ir informacine infrastruktūra ir būtų su ja sąveiki. Projekte nustatyti rinkos dalyviai, kurie vaidina esminį vaidmenį kibernetinio saugumo srityje. Tai informacinės visuomenės paslaugų (e. prekyba, interneto mokėjimai, socialiniai tinklai, paieškos sistemos, „debesų“ kompiuterija, priegloba, taikomųjų programų parduotuvės) teikėjai ir ypatingos svarbos infrastruktūros (energetika, transportas, bankininkystė, finansų rinkų infrastruktūra, sveikatos sektorius) operatoriai. Valstybės narės turėtų užtikrinti, kad šie subjektai imtųsi reikiamų techninių ir organizacinių priemonių, kad galėtų valdyti riziką, kylančią tinklų ir informacinių sistemų, kurias jie kontroliuoja ir kuriomis naudojasi savo veikloje, saugumui, kad subjektai praneštų kompetentingoms institucijoms apie incidentus, kurie turi didelį poveikį pagrindinių jų teikiamų paslaugų saugumui. Kompetentingos institucijos turėtų turėti įgaliojimus atlikti saugumo auditą ir pateikti rezultatus bei teikti privalomus nurodymus šiems subjektams.

Lietuvoje pažymėtinos šios iniciatyvos kibernetinio saugumo srityje:

1. 2011 m. patvirtinta Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 m. programa;
2. 2012 - 2013 m. buvo įkurtos Elektroninės informacijos saugos (kibernetinio saugumo) koordinavimo komisija bei Elektroninės informacijos saugos (kibernetinio saugumo) konsultacinės taryba;
3. 2014 m. planuojama priimti LR Kibernetinio saugumo įstatymą, pradėti rengti naują kibernetinio saugumo ir elektroninės informacijos saugos institucinės sąrangos koncepciją, ypatingos svarbos informacinės infrastruktūros metodiką.

Daugiausia dėmesio buvo skiriama LR Kibernetinio saugumo įstatymo (toliau - Įstatymas) rengimui. Šiuo metu svarstomas Įstatymo projektas, kuriuo siekiama nustatyti kibernetinio saugumo užtikrinimo sistemą, numatant valstybės institucijas, atsakingas už kibernetinio saugumo politikos formavimą, kontroliavimą, koordinavimą ir įgyvendinimą bei minimalius organizacinius ir techninius kibernetinio saugumo reikalavimus viešojo administravimo subjektų valdomiems valstybės informaciniams ištekliams, ypatingos svarbos informacinei infrastruktūrai, elektroninių ryšių paslaugų teikėjams, ir elektroninės informacijos prieglobos paslaugų teikėjams.

Priėmus Įstatymą, bus nustatytas kibernetinio saugumo srities teisinis reglamentavimas, patikslintos teisinės normos, reglamentuojančios valstybės informacinių išteklių elektroninės informacijos saugą, valstybės informacinių išteklių atitiktį nustatytiems elektroninės informacijos

saugos reikalavimams, nustatytas teisinį pagrindą tvarkyti asmens duomenis elektroninės informacijos saugos užtikrinimo tikslais bei nustatyta administracinė atsakomybė viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams ir ypatingos svarbos informacinės infrastruktūros valdytojams už Įstatyme nustatytų pareigų kibernetiniam saugumui užtikrinti nevykdymą. Pasak įstatymo rengėjų, kibernetinio saugumo reguliavimas tenka Krašto apsaugos ministerijai, kuri siūlo įkurti **Nacionalinį kibernetinio saugumo centrą** (toliau -NKSC), kuris atliktų šias funkcijas :

- 1) vykdo valstybės informacinių išteklių ir ypatingos svarbos informacinių infrastruktūrų kibernetinių incidentų valdymo padalinio veiklą;
- 2) pagal savo kompetenciją rengia siūlymus dėl organizacinių ir techninių kibernetinio saugumo reikalavimų valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai;
- 3) vykdo valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną;
- 4) rengia tipinius kibernetinio incidento valdymo ypatingos svarbos informacinėse infrastruktūrose planus;
- 5) teikia konsultacijas ir rekomendacijas kibernetinio saugumo klausimais valstybės informacinių išteklių valdytojams ir ypatingos svarbos infrastruktūros valdytojams;
- 6) analizuoja nacionalinę kibernetinio saugumo situaciją ir rengia nacionalinio kibernetinio saugumo būklės ataskaitas;
- 7) rengia nacionalinius ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus;
- 8) valdo kibernetinio saugumo informacinį tinklą;
- 9) vykdo informacijos sklaidą kibernetinio saugumo klausimais;

Krašto apsaugos ministerija, pateikdama išvadas dėl Kibernetinio įstatymo⁸⁹ nurodo, kad NKSC veiklai vykdyti reikėtų papildomų lėšų ir 2015-2017 m. tai būtų suma - 10794,4 tūkst. Lt., tačiau iš pateiktų funkcijų aprašymų nėra aišku, ar toks centras būtų pajėgus visiškai ir pilnai suteikti operatyvią ir kvalifikuotą pagalbą, o kilus kibernetiniam incidentui prieš ypatingos svarbos informacinę infrastruktūrą, galėtų priimti sprendimus dėl Lietuvos nacionalinės kibernetinės erdvės gynybos priemonių, ar tai bus ta institucija, kuri taps kibernetinio saugumo politiką koordinuojančiu vienetu, galinčiu sukurti privatus, viešojo ir mokslo sektorių bendradarbiavimo kibernetinio saugumo srityje mechanizmą. Dėl Įstatymo projekto pasisakė septynios institucijos, kurios pateikė 63 pastabas. Kai kurios pažymėtinos pastabos:

1. Sąvokų neaiškumas. Pavyzdžiui, siūloma sąvoka "**Kibernetinis incidentas** – saugumo incidentas, vykstantis, galintis įvykti ar turėti poveikį tiek informacinei sistemai ar elektroninių ryšių tinklui, tiek pramoninių procesų valdymo sistemai" . Būtina nustatyti incidentų „gradaciją“, nes įstatymo projekto siūloma „kibernetinio incidento“ sąvoka gali apimti tiek labai mažą, bevertį poveikį turintį pažeidimą (kaip nereikšmingą virusą, nepageidaujamus pranešimus, kurie nesukelia realios grėsmės), tiek didelių nuostolių turintį pažeidimą (Ddos ataka), dėl kurio pasak įstatymo

⁸⁹ http://www.lrs.lt/pls/proj/dokpaieska.showdoc_l?p_id=230657&p_fix=n&p_gov=n, [2014 02 11].

rengėjų tiek RRT, tiek naujai kuriamas NKSC turi teisę teikti privalomus nurodymus. Akivaizdu, kad aptarti pažeidimai yra neadekvatūs, o jiems reikalingi ištyrimo kaštai - dideli. Kita sąvoka „**Pramoninių procesų valdymo sistema**“ – remiantis minėtu apibrėžimu, neaišku, kokios sistemos būtų priskirtinos pramoninių procesų valdymo sistemoms, nėra aiškūs tokio tipo sistemų valdytojai, tvarkytojai ir pan.

2. Neapibrėžti kritinės infrastruktūros kriterijai, kas paliktų spragą manipuluoti objektų svarbos nustatymu.

3. Institucinė struktūra su galimai persidengiančiomis funkcijomis apsunkina koordinavimą tarp institucijų. Be to, turėtų būti aiškesnis teisių, pareigų ir atsakomybės nustatymo mechanizmas.

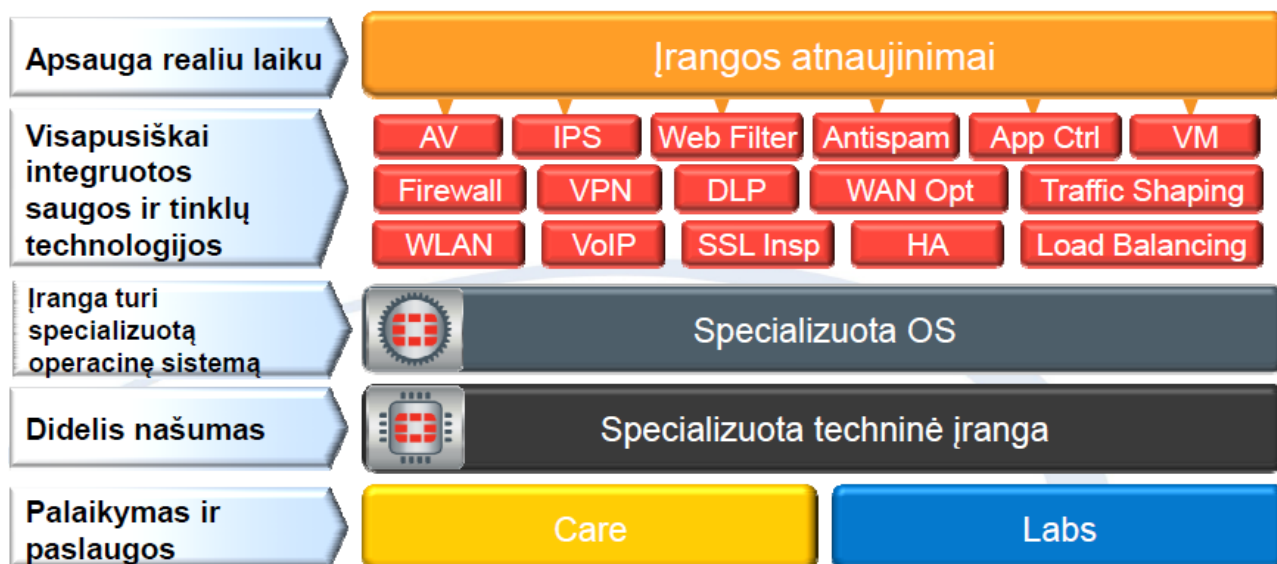
Pažymėtina, kad technologijų konvergencijos sąsajas galima išvelgti Įstatymo projekto 3 straipsnyje, kuriame apibrėžiama sąvoka "**Kibernetinė erdvė** – aplinka, kurioje elektroninė informacija perduodama per elektroninių ryšių tinklu sujungtus **kompiuterius ar kitą informacinių ir ryšių technologijų įrangą**". Įstatymas remiasi elektroninių ryšių veiklos reguliavimo principais, kurie netiesiogiai nurodo vienodų teisės normų taikymą neatsižvelgiant į technologijų, elektroninių ryšių, elektroninių paslaugų įvairovę. Tai technologinio neutralumo ir funkcinio lygiavertiškumo principai⁹⁰.

Lietuvoje akivaizdžiai pastebimos suaktyvėjusios valstybės, mokslo ir verslo sektorių bendradarbiavimo tendencijos kibernetinio saugumo srityje: vis daugėja CERT'ų, formuojasi KAM KASP savanoriai, vykdomos treniruotės (RRT, ENISA, NATO), stiprėja Cyberpolice, tyrimai, bendradarbiavimas, rengiamos konferencijos, mokymai, simuliacijos valstybės institucijų specialistams bei vadovams, RRT nacionalinio CERT-LT veiklos organizavimas 24/7 režimu, incidentų tyrimo statistika bei 2013 m. surengtos tarpinstitucinės kibernetinės pratybos „XI306", įsteigtos Galimų kibernetinių saugumo incidentų pasekmių valdymo grupės veikla, Nusikaltimų elektroninėje erdvėje tyrimo valdyboje įsteigtas naujas padalinys atlieka interneto monitoringą, pateikiami aktualūs elektroninių nusikaltimų tyrimo statistiniai duomenys.

Pažymėtinas VĮ Infostruktūros diegiamas tinklų saugumo sprendimas - SVDPT⁹¹ duomenų centrų ir tinklo infrastruktūros bei incidentų stebėjimo sistema, kuri bus pritaikyta informacinių sistemų teikiamų paslaugų (taikomųjų programų ir svarbių servisų) prieinamumo stebėjimui bei apskaitai (įskaitant GR OCSP paslaugą, naudojamą sertifikatų galiojimo tikrinimui, viešas ir vidines web svetaines) stebint iš SVDPT valdymo centro arba viešo interneto taškų:

⁹⁰ **Technologinio neutralumo principas** reiškia, kad teisės normos turi būti taikomos atsižvelgiant į tikslus, kurių siekiama atitinkamomis teisės normomis, ir stengiantis, kad, kiek tai pagrįsta, vien tik dėl jų taikymo nebūtų skatinamas arba diskriminuojamas konkrečių technologijų naudojimas, taip pat kad teisės normos būtų taikomos kiek įmanoma neatsižvelgiant į technologijas, kurios naudojamos su konkrečiu teisiniu santykiu susijusiems elektroninių ryšių tinklams ar elektroninių ryšių paslaugoms teikti. **Funkcinio lygiavertiškumo principas** reiškia, kad teisės normos turi būti kuo vienodžiau taikomos elektroninių ryšių tinklams ar paslaugoms, atliekantiems analogiškas funkcijas.

⁹¹ SVDPT - Saugus valstybinio duomenų perdavimo tinklas



21 pav. SVDPT integruotų saugos ir tinklų technologijų sprendimas.

Įdiegus tinklo įrangą, planuojamos centralizuotos paslaugos: Vartotojų duomenų srauto turinio filtravimo apsauga, kenksmingo kodo aptikimas, nepageidaujamų žinučių aptikimas, perduodamos informacijos kontrolė, aplikacijų kontrolė, naudojant Anti-virus, Anti-malware, Anti-spyware, Anti-Phishing, „švarus“ https/smtps srautas, įeinančių / išeinančių atakų blokavimas, kenksmingos PĮ blokavimas, apsauga nuo informacijos nutekėjimo, aktyvi gynyba nuo *http* grėsmių, personalo veiklos internete kontroliavimas/valdymas.

Taigi, norint užtikrinti kibernetinį atsparumą, viešasis bei privatus sektorius turėtų vystyti kibernetinio atsparumo galimybes, glaudžiai bendradarbiauti tarpusavyje, įtraukiant ir akademinę bendruomenę į mokslinius tyrinėjimus kibernetinio saugumo srityje, nes šalys yra suinteresuotos suvaldyti rizikas elektroniniuose ryšiuose, apsaugoti strateginių objektų veiklą, valstybinius informacinius išteklius, didinti pasitikėjimą informacija bei technologijomis tarp elektroninių paslaugų vartotojų, apsaugant juos ir jų tvarkomus asmens duomenis. Apie tai sekančioje dalyje.

3.3. Asmens duomenų apsaugos teisiniai aspektai

Kaip buvo minėta, dėl sparčios technologinės plėtros ir globalizacijos kasdien surenkami didžiuliai duomenų kiekiai, tame tarpe ir asmens duomenys. Nauji pasiekimai medicinoje, elektroniniuose ryšiuose, mokslinėje veikloje bei kitose srityse nuolat didina žmonių kuriamos (generuojamos) informacijos kiekį.

Teisininkas M. Civilka išskiria šias pagrindines tendencijas, kurios išryškina asmens privatumui keliamą grėsmę:

1. **Globalizacija** - kai panaikinami geografiniai suvaržymai, sienos ir pan. asmens duomenų judėjimui (geriausias pavyzdys internetas).
2. **Konvergencija** - kai eliminuojami technologiniai barjerai tarp tarpusavyje suderinamų sistemų.

3. **Multimedia** - kai sujungiamos kelios asmeninės informacijos perdavimo ir išreiškimo formos ir tokiu būdu surinkta informacija gali būti lengvai performatuota į kitą formą⁹².

Tokiu būdu vykstanti informacinių technologinių sistemų konvergencija savo ruožtu dar labiau padidina galimybes itin greitai ir efektyviai rinkti bei platinti asmens duomenis⁹³. Todėl atsiranda poreikis tiek nacionaliniu, tiek tarptautiniu lygmeniu nuolat tobulinti teisinę bazę, siekiant užtikrinti asmens privatumą bei duomenų apsaugą, atsižvelgiant į nuolat kintančių technologijų galimybes ir grėsmes. Toliau bus apžvelgiama Lietuvos asmens duomenų apsaugos teisinė aplinka technologijų konvergencijos kontekste ir pateikiama jos problematika.

Nors asmens duomenų apsauga Lietuvoje pradėta rūpintis nuo 1992 metų, kai buvo priimta Lietuvos Respublikos Konstitucija, tačiau iš esmės asmens duomenų teisinės apsaugos mechanizmas šalyje pradėjo veikti 1996 metais, įsigaliojus Asmens duomenų teisinės apsaugos įstatymui, kuris gina žmogaus teisę į privataus gyvenimo neliečiamumą tvarkant asmens duomenis. Lietuvos Respublikos Konstitucijos 22 straipsnis garantuoja, jog „Žmogaus privatus gyvenimas neliečiamas“, o „Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami“⁹⁴. Nors nuo 1992 metų technologijos ženkliai kito, vienos išnyko (kaip telegrafai), kitos atsirado (kaip mobilieji įrenginiai), stebėtinai yra Konstitucijos kūrėjų įžvalgumas, jog **technologijų įvairovė negali įtakoti prigimtinei žmogaus laisvei – privatumui**.

Šiuo metu Valstybės politiką duomenų apsaugos srityje formuoja, organizuoja, koordinuoja ir kontroliuoja jos įgyvendinimą Teisingumo ministerija, o ją įgyvendina ir atlieka priežiūrą - Valstybinė duomenų apsaugos inspekcija, priskirta teisingumo ministro valdymo sričiai.

Kadangi sparčiai tobulėjant technologijoms, automatiniu būdu tvarkoma vis daugiau asmens duomenų, asmens duomenų apsaugos politiką formuojančios ir įgyvendinančios įstaigos susiduria su problema, kaip sudaryti palankias sąlygas technologijų plėtrai ir sukurti saugią teisinę aplinką, kurioje būtų ginama žmogaus teisė į privataus gyvenimo neliečiamumą⁹⁵. Valstybės kontrolė 2013 metai iniciavusi valstybinį auditą "Automatiniu būdu tvarkomų asmens duomenų apsauga", konstatavo, kad Teisingumo ministerija ir Valstybinė duomenų apsaugos inspekcija nepakankamai užtikrina žmogaus teisės į privataus gyvenimo neliečiamumą ir pakankamą asmens duomenų saugumo lygį dėl šių priežasčių:

1. Lietuvoje asmens duomenų apsaugos teisinis reguliavimas atitinka Europos Sąjungos reikalavimus, tačiau atsilieka **nuo informacijos ir ryšių technologijų pažangos**;

⁹² Civilka M. Asmens duomenų apsauga tarptautinėje ir EB teisėje // [http://www.andriuz.skynet.lt/knygos/Teise/Asmens%20Duomenu%20Apsauga%20Tarptautineje%20ir%20ES%20Teiseje%20\(Civilka,%202001\).pdf](http://www.andriuz.skynet.lt/knygos/Teise/Asmens%20Duomenu%20Apsauga%20Tarptautineje%20ir%20ES%20Teiseje%20(Civilka,%202001).pdf)

⁹³ Spalveters K. Asmens duomenų teisinė apsauga interneto kontekste pagal Europos Sąjungos ir tarptautinę teisę. Magistro baigiamasis darbas

⁹⁴ Lietuvos Respublikos Konstitucija, Valstybės Žinios, 1992, Nr. 33-1014 (1992-11-30)

⁹⁵ Valstybinio audito ataskaita "Automatiniu būdu tvarkomų asmens duomenų apsauga", 2013 m. gruodžio 11 d. Nr. VA-P-90-3-21, <https://www.vkontrole.lt/failas.aspx?id=3088>, [2014 02 25].

2. parengtos metodinės rekomendacijos neaktualios ir apima ne visas problemines sritis susijusias **su naujų technologijų** taikymu.

Kaip savarankiška žmogaus teisių sritis, asmens duomenų apsauga pradėjo funkcionuoti, kai 1981 m. buvo priimta Strasbūro konvencija dėl asmenų apsaugos, susijusios su asmens duomenų automatizuotu tvarkymu ir 1995 m. buvo priimta ES duomenų apsaugos direktyva. Nuo to laiko automatizuota asmens duomenų tvarkymo aplinka ES keitėsi, sparčiai tobulėjo IRT, pakito duomenų rinkimo, naudojimo, perdavimo būdai, tačiau teisinis asmens duomenų apsaugos reguliavimas liko iš esmės nepakitęs. Asmens duomenų apsaugos teisinis reguliavimas užtikrina visapusišką asmens duomenų apsaugą, kai jis ne tik neatsilieka nuo IRT pažangos, bet ir yra tinkamai sureglamentuotas. „Tobulėjant informacijos ir ryšių technologijoms, kai asmens duomenys tvarkomi automatinio būdu, **technologiniai veiksniai kelia naujų grėsmių asmens duomenų tvarkymo apsaugai**“ - konstatavo Valstybės kontrolė.

Toliau bus pateikiamos šiuo metu aktualios asmens duomenų apsaugos teisinės problemos, atsiradusios technologijų konvergencijos įtakoje.

1. Teisinės bazės tobulinimas. Lietuvai įstojus į ES, duomenų apsaugos teisinis reguliavimas buvo suderintas su ES direktyva. 2008-2012 m. Asmens duomenų teisinės apsaugos įstatymas ir jį įgyvendinantys teisės aktai keisti keletą kartų, bet sparti informacijos ir ryšių technologijų plėtra nuolat iškelia asmens duomenų apsaugos praktinio taikymo klausimų, kurių esami teisės aktai nespėdžia.

Pavyzdys: Dėl sparčios technologinės plėtros ir globalizacijos kasdien surenkamas didžiulis duomenų kiekis. Teisės aktai nenumato duomenų subjektui aiškios „teisės būti pamirštam“ t y. reikalauti ištrinti asmens duomenis kai jis nebenori, kad jo duomenys būtų tvarkomi ir nėra teisėtų priežasčių juos saugoti. Technologijos leidžia perduoti asmens duomenis iš vieno paslaugų teikėjo kitam, tačiau duomenų subjekto „teisė perkelti duomenis“ nėra aiškiai reglamentuota. Pasikeitus technologijoms teisės aktuose numatyta duomenų subjekto sutikimo tvarkyti asmens duomenis procedūra tampa tariama (formali), nes naudojant naujas paslaugas (socialiniai tinklai, debesų kompiuterija) ne visi duomenų subjektai žino, kokie jų duomenys bus renkami ir tvarkomi.

Teisės aktai ir metodiniai dokumentai, reglamentuojantys asmens duomenų apsaugą, turėtų būti rengiami savalaikiai, nustatant bendruosius ir specialiuosius šios srities tvarkymo reikalavimus, operatyviai reaguojant į probleminius klausimus, technologinius pokyčius ir naujus iššūkius asmens privatumui bei duomenų apsaugai, o metodiniai dokumentai rengiami skelbiant asmens duomenų tvarkymo praktiką⁹⁶.

2. Naujų technologijų įtaka teisiniam reglamentavimui. Europos Parlamento vidaus rinkos ir vartotojų apsaugos komitetas 2012 m. išskyrė technologines sritis, kuriose kyla asmens duomenų apsaugos reglamentavimo neaiškumų: vietos nustatymo paslaugos, duomenų panaudojimas iš skirtingų šaltinių, debesų kompiuterija, išmanieji skaitikliai, biometrinės

⁹⁶ Valstybinio audito ataskaita "Automatinio būdu tvarkomų asmens duomenų apsauga", 2013 m. gruodžio 11 d. Nr. VA-P-90-3-21, <https://www.vkontrole.lt/failas.aspx?id=3088>, [2014 02 26].

technologijos, *Wi-Fi* duomenų rinkimas, *RFID* identifikavimas, socialinių tinklų paslaugos, elektroninio pašto skenavimas ir kt., taigi iškyla būtinybė savalaikiai reaguoti į naujų technologijų skverbtį, parengiant rekomendacijas "debesų kompiuterijos" paslaugų, išmaniųjų skaitiklių, biometrinių technologijų, metaduomenų, duomenų nuasmeninimo ir kt. klausimais.

3. Asmens identifikavimo problema. Vis sparčiau keičiantis automatizuotomis priemonėmis, teikiant elektronines paslaugas ir užtikrinant darbuotojų asmens duomenų apsaugą darbo vietoje, esamas teisinis reglamentavimas kelia neaiškumų, nes asmens identifikavimui (autentifikavimui) yra naudojami elektroninio parašo sertifikato duomenys, biometriniai parametrai. Lietuvoje nėra vieningos asmens identifikavimo elektroninėje erdvėje sistemos, galimi keletas variantų, kuriais naudojantis susiduriama su identifikavimo problema. Populiariausios tapatybės patvirtinimo elektroninėje erdvėje formos – identifikavimasis per bankinę sistemą bei elektroninis parašas. Tačiau abiem atvejais kyla problemų – pirmuoju, dėl asmeninio prisijungimo naudojimo darbo ar tarnybos tikslais, antruoju – dėl laiko žymos. Ši žyma nėra privalomas specialusis atributas, todėl ji įdiegta ne visose elektroninio parašo technologijose, tad laiko žymos nebuvimas (ji perkama atskirai) sukelia nepatogumų⁹⁷.

Kita problema - asmens kodo naudojimas. Lietuvos vyriausiasis administracinis teismas 2013 m. gegužės 23 d. administracinėje byloje Nr. A⁸²²-1173/2013 pasisakė, jog „[...] asmenys sudarantys sutartis [...], sutartyse nurodo ne tik savo vardą ir pavardę, bet ir telefono numerį, adresą bei bendrosios atsiskaitymo knygelės numerį, remiantis šių asmens duomenų visuma, asmenį galima vienareikšmiškai identifikuoti ir tam nėra būtina naudoti asmens kodą“. Atsižvelgiant į tai, kiekvienu konkrečiu atveju reikia įvertinti būtinybę nurodyti asmens kodą. Valstybinė duomenų apsaugos inspekcija rekomenduoja tokiu atveju, kai šis duomuo nėra būtinas asmeniui identifikuoti, vietoje asmens kodo nurodyti kitą asmens duomenį, pavyzdžiui, gimimo datą.

4. Darbo vietų mobilumas kelia grėsmę asmens duomenų saugumui. Pastebima nauja tendencija darbo vietose naudoti asmeninius nešiojamus ar planšetinius kompiuterius bei išmaniuosius telefonus ir naudoti juos darbo reikmėms, kas sukelia grėsmę duomenų apsaugai, jeigu dingtų asmeninis darbuotojo kompiuteris su įstaigos duomenų baze ar kita svarbia informacija. Aktualūs saugos klausimai: ar įstaigos įgyvendina saugumo politikas šiais klausimais, ar šifruojami darbiniai duomenys ir failai, ar darbuotojai jungdamiesi prie įstaigos tinklo nenaudoja viešų interneto prieigos taškų, ar įstaigos veikloje skiriamas dėmesys bandymų įsilaužti stebėsenai.

5. E. privatumas. Vienas iš pagrindinių naršymo internete privalumų visuomet buvo anonimiškumas. Tačiau daugėjant įvairių elektroninių paslaugų, reikalaujančių identifikacijos, taip pat sparčiai populiarėjant naujoms technologijoms, susijusioms su mobilumu, elektroninis

⁹⁷ <https://www.ada.lt/go.php/lit/Asmens-identifikavimas-elektronineje-erdveje-duomenu-apsaugos-problemos/166>, [2014 03 12].

privatumas tampa vis rimtesniu iššūkiu. Kiekvieną kartą, kai internetu užsakomos e. paslaugos, jungiamasi per internetinę bankininkystę registruojantis tinklalapyje ar tiesiog naršoma viešame bevielame tinkle, rizikuojama, kad kažkas gali pasisavinti asmens duomenis ar kitaip pažeisti privatumą (asmens tapatybės vagystės, konfidencialių duomenų praradimas).

6. Programėlių (apps) gausa daro žmonių gyvenimą patogesnį, tačiau kartu renka didžiulius kiekius **asmens duomenų**, taip įgalindamos nuolatinį skaitmeninį stebėjimą, dažnai vartotojui net nežinant, kad tai vyksta ir kam jo duomenys naudojami. Neretai programėlių kūrėjai nežino savo darbo įtakos asmens privatumui. Nors pagrindinės operacinės sistemos bei programėlių platformos siūlo tam tikrus privatumo nustatymus, tačiau nesuteikia naudotojui visiškos savo duomenų apsaugos kontrolės ar galimybės patikrinti, kokia informacija ir koku tikslu renkama. Galiniuose įrenginiuose taip pat kaupiama asmeninė informacija, tačiau jiems sugedus ar pasibaigus galiojimo laikui, vartotojai ne visada pasirūpina asmens duomenų sunaikinimu⁹⁸.

Valstybinės duomenų apsaugos inspekcijos direktorius dr. Algirdas Kunčinas konferencijoje pranešime "Asmens privatumas vs šiuolaikinės technologijos" įžvelgia šias aktualios teisines problemas, išskylančios asmens duomenų teisinėje srityje ir susijusias su technologijomis: duomenų bazių integracija ir paieškos programų kūrimas (pvz. PRISM); slaptos informacijos nutekinimas (pvz. E. Snowdenas), kibernetinių incidentų pasekmės asmens duomenų saugumui, vaizdo stebėjimo plitimas, slapukų naudojimas, biometrinių duomenų naudojimas identifikavimui, išmaniųjų įrenginių naudojimas darbo vietose.

Pažymėtina, kad šiuo metu vyksta ES duomenų apsaugos reforma, kuria siekiama pašalinti esamus Direktyvos Nr. 95/46/EB taikymo skirtumus ES valstybėse narėse. Pasiūlytas ES duomenų apsaugos teisės aktas turėtų užtikrinti žmonėms galimybę patiems kontroliuoti savo asmens duomenis, padėtų **didinti jų pasitikėjimą elektroninėmis paslaugomis bei naujomis technologijomis**. Valstybinė duomenų apsaugos inspekcija 2014-2016 m. strateginiame veiklos plane numatė siekti, kad būtų įtvirtintos priemonės, užtikrinančios saugesnį asmens duomenų tvarkymą, prisitaikymą prie **nuolat augančio technologijų poveikio**.

3.4. Teisinis reguliavimas ateityje ir rekomendacijos

Atsakant į darbe iškeltus uždavinius, galima konstatuoti, kad IRT pastaruoju metu yra įžengusi į naują etapą, kai:

1. Vystosi naujosios tinklų technologijos, leidžiančios teikti tradiciškai atskiras, o taip pat ir visiškai naujas paslaugas tais pačiais naujosios kartos tinklais;
2. Tobulėja galinių įrenginių technologijos, kurios leidžia keistis duomenimis bei naudotis ryšių paslaugomis bet kurioje vietoje bet koku metu naudojant įrenginių įvairovę;
3. Užtikrinamas nuolatinis prisijungimas prie visuotinio duomenų perdavimo tinklo;

⁹⁸ <https://www.ada.lt/go.php/lit/Varsuvos-deklaracija-del-mobiliesiems-irenginiams-skirtu-programeliu-naudojimo/126>, [2014 02 14].

4. Vyksta informacijos kaitos ir elektroninių paslaugų, integruojančių tradicines telekomunikacijų, audiovizualines bei informacines paslaugas, spartus augimas ir globalėjimas;
5. Nyksta geografinės ribos informacijos kaitai ir bendravimui;
6. Nyksta ribos tarp paslaugų teikėjo (kūrėjo) ir vartotojo;
7. Stiprėja naujų grėsmių elektroninių paslaugų vartotojams, valstybės informaciniams ištekliams poveikis;
8. Kuriami nauji integruoti ir specializuoti saugumo sprendimai.

Šiame kontekste svarbu kuo greičiau rasti tinkamus teisinio reguliavimo sprendimus, kurie neužkirstų kelio naujoms galimybėms, o tuo pačiu atsakytų į kylančius saugumo iššūkius. RRT, kaip pagrindinis nacionalinio ryšių reguliuotojas, kurio vaidmuo visose Europos Sąjungos šalyse ypatingai svarbus reguliuojant ryšių rinkos dalyvių santykius, siekiant sudaryti efektyvios konkurencijos sąlygas ūkio subjektams, ginant paslaugų vartotojų interesus, skatinant naujų ir modernių technologijų atėjimą bei paslaugų vartojimą nacionaliniame lygmenyje, nurodo koks turėtų būti reguliavimas ateityje:

Koks turėtų būti reguliavimas ateityje?

RRT

- **Lankstus ir orientuotas į ateitį**
 - Nebandantis "suspėti" į įstatymą įrašyti visas įmanomas perdavimo technologijas
 - Bet vienodai taikomas visiems konkuruojantiems perdavimo būdams
- **Realistiškas**
 - Suprantantis, kad ribotų kanalų laikai baigiasi
 - Suprantantis ribotą Lietuvos institucijų jurisdikciją
- **Orientuotas į turinį**
 - Jei programa atitinka reikalavimus, ją galima skleisti visomis priemonėmis
- **Leidžiantis investuoti Lietuvoje**
 - Neturi būti skatinama investuoti užsienyje tikslu lengviau pasiekti Lietuvos vartotojus
 - Neturi būti nereikalingų administracinių barjerų
- **Pripažįstantis visuomenei vertingų programų reikšmę ir užtikrinantis, kad jos pasiektų vartotojus**
 - Turi būti užtikrinta, kad vartotojai gaus svarbiausias programas, nepriklausomai nuo technologijų pažangos

Tomas Lamanauškas

21 pav. Teisinis reguliavimas technologijų konvergencijos kontekste. Šaltinis: rrt.lt

Šiame kontekste yra svarbi ES Kibernetinio saugumo strategijoje "Atvira, saugi ir patikima kibernetinė erdvė" akcentuojama nuostata dėl bendros atsakomybės principo: tiek viešasis sektorius, tiek privačios įmonės, tiek individualūs vartotojai turi pripažinti bendrą atsakomybę, kartu diegti apsaugos priemones, o esant reikalui, koordinuoti veiksmus.

Teisinės ir institucinės saugumo aplinkos suderinimas turėtų padėti efektyviai kovoti su tinklų ir informacijos saugumu. Toliau, remiantis aukščiau pateikta medžiaga, bus pateikiami siūlymai, rekomendacijos atskiroms tikslinėms grupėms.

Saugumo politiką formuojančioms institucijoms:

1. Sukurti palankią įstatyminę bazę, užtikrinančią visų elektroninės rinkos dalyvių – paslaugų teikėjų ir vartotojų teises.
2. Priimti / papildyti saugą reglamentuojančius teisės aktus.
3. Skatinant naudotis el. paslaugomis, sukurti patikimą el. pasirašymo teisinę bazę ir infrastruktūrą.

4. Nustatyti aiškią institucinę sąranką, funkcijas ir atsakomybę informacijos saugumo srityje.
5. Visoms viešojo sektoriaus institucijoms informacijos saugumo valdymo reikalavimų taikymas turi būti nustatytas ne kaip rekomendacija, o kaip reikalavimai (įskaitant LRV nepavaldžias įstaigas).
6. Suderinti informacijos saugumo valdymo reikalavimų taikymą informaciniams ištekliams (sistemoms ir registrams), nes formaliai informacinių sistemų nevaldančios institucijos reikalavimų netaiko, o valdančios kelias sistemas turi papildomų sunkumų derindamos kelis aukščiausio lygio informacijos saugumo politikos dokumentus.

Saugumo politiką įgyvendinančioms ir priežiūrą atliekančioms institucijoms:

1. Nustatant informacijos saugumo valdymo reikalavimus įmonėms, įstaigoms ir organizacijoms, savalaikiai reaguoti į nuolat kintančius technologinius bei tinklų pažeidžiamumus.
2. Nustatyti papildomus reikalavimus paslaugų teikėjams (pvz.: dėl duomenų tvarkymo funkcijų perkėlimo tvarkos; parengiant tinkamą paslaugų sutartį; pakoreguojant turimus saugos politikos dokumentus, atsiradus papildomam duomenų tvarkytojui; jeigu tvarkomi asmens duomenys - aiškos duomenų tvarkymo sąlygos, saugių protokolų naudojimas, duomenų šifravimas, kriptografija ir pan.).
3. Skatinti naudoti pažangius metodus, gerąsias praktikas, diegti modernias ir pažangias technines saugumo priemones. Gal net teikti mokesčių lengvatų e. paslaugų vartotojams, paslaugų teikėjams.
4. Nuolat fiksuoti ir analizuoti įvykius pasaulyje, savalaikiai reaguoti į pasikeitimus, didinti informuotumą tiek tarp paslaugų teikėjų, programinės įrangos kūrėjų, tiek tarp vartotojų.
5. Organizuoti įvairius su IT technologijų naudojimu susijusius mokymus, kursus.
6. Organizuoti periodinius saugos reikalavimų atitikimo patikrinimai (atliekama rizikos analizė ar informacinės sistemos saugos atitikties vertinimas) bei viešinti jų rezultatus.
7. Skatinti bendradarbiavimą tarp ryšių operatorių CERT'ų bei nacionalinio CERT-LT.
8. Ieškoti būdų diegti šiuolaikiškas IRT sąveikumo sistemas, pagrįstas standartais ir sutartais principais (LST/ISO IT valdymo standartas 38500:2008), taikyti veiklos ir minėtų technologijų sujungimo į bendrą įstaigų architektūrą metodus (TOGAF, COBIT, ITIL ir kiti).

Valstybės įstaigoms:

1. Nepriklausomai ar yra informacinių sistemų valdytojais, kurti saugumo politikas, koordinuojant žmogiškuosius, organizacinius ir technologinius veiksmus.
2. Rūpintis kuriamos srities vidaus darbuotojų ir išorės vartotojų švietimu, kompiuterinio raštingumo didinimu, įtakoti vartotojų motyvaciją naudotis elektroninėmis paslaugomis, pabrėžiant informacijos saugumo aspektą.
3. Daugiau paslaugų perkelti į elektroninę erdvę, tokiu būdu priartinant jas prie visuomenės ir taip pratinant naudotis patogesnėmis, greitesnėmis, pigesnėmis paslaugų gavimo priemonėmis elektroniniu būdu, adekvačiai rūpinantis naudojamų tinklų, IRT ir informacijos apsauga

Duomenų centrų, debesų kompiuterijos, el. ryšių paslaugų teikėjams:

1. Diegti veiksmingas privatumo politikas, duomenų saugą iškelti į prioritetinius tikslus.
2. Aktyviai dalyvauti tarpžinybinėse grupėse, teikiant pasiūlymus saugumo klausimais.
3. Organizuoti ekspertinio lygio mokymus specialistams, visuomenei.
4. Paslaugų teikėjams diegti pažangius saugos standartus, laikytis etikos, asmens privatumo ir duomenų apsaugos principų.
5. Veikloje taikyti rizikos analizės, saugumo priemonių įvertinimo auditus, duomenų apsaugos poveikio vertinimą, kitas prevencines priemones saugumui užtikrinti.
6. Įdiegti aiškius ir suprantamus sprendimus dėl: „Teisės būti pamirštam“, "Duomenų subjekto informavimo", "Aiškaus asmens sutikimo", "Teisės į duomenų perkeliamumą".

Vartotojams:

1. Nuolat atsakingai rūpintis savo asmens duomenų saugumu.
2. Domėtis saugumo pažeidimais, naudoti naujausias saugumo priemones.
3. Laikytis kompetentingų institucijų rekomendacijų.

Programėlių kūrėjams:

1. Veikloje užtikrinti savo veiklos suderinamumą su esamomis privatumo ir duomenų apsaugos taisyklėmis.
2. Pateikti aiškią ir suprantamą informaciją apie duomenų rinkimą dar prieš pradėdant jį vykdyti.
3. Vartotojui suteikti galimybę prieiti prie jo asmeninės informacijos kiekvienu individualiu atveju.

Akademinei visuomenei:

1. Kadangi sparčiai kintančios technologijos iššaukia Lietuvoje mokslinių tyrimų trūkumą informacijos saugumo valdymo tema, plėsti mokslinių tyrimų sritį šia tema.
2. Atlikti detalią viešojo sektoriaus subjektų duomenų saugumo politikos dokumentų, galiojančių informacijos saugumo reikalavimų ir tarptautinių informacijos saugumo valdymo standartų turinio lyginamąją analizę.
3. Plačiau palyginti tyrimų rezultatus su užsienio šalių viešojo sektoriaus analogiška patirtimi ir pateikti pasiūlymus.
4. Aktyviai dalyvauti tarpžinybinėse grupėse, aptariant informacijos saugumo problemas.
5. Rengti kibernetinio saugumo specialistų ugdymo programas.

Atlikus pagrindinių ES ir Lietuvos teisės aktų, reglamentuojančių elektroninės informacijos saugą, analizę, darytina išvada, kad nors galiojantys teisės aktai neišsamiai reglamentuoja saugumo sritį arba yra neatnaujinti pagal laikmečio technologines tendencijas, šiuo metu Lietuvoje pastebimas gana aktyvus elektroninės informacijos, kibernetinio saugumo reguliavimas. Nors Lietuvoje svarstomas šiuo metu Kibernetinis saugumo įstatymo projektas turi trūkumų ir diskutuotinų klausimų, tikimasis jis bus priimtas atsakingai išdiskutavus ir radus optimaliausią sprendimą. Specialių teisės aktų, susijusių su asmens duomenų teisine apsauga, analizė parodė, jog Lietuvoje asmens duomenų apsaugos teisinis reguliavimas atitinka Europos Sąjungos reikalavimus, ir nors atsilieka nuo informacijos ir ryšių technologijų pažangos, nustatyta, kad planuojami atnaujinti Bendrieji reikalavimai apims daugelį problematiškų sričių, bus nustatyti reikalavimai tiekėjams, parengtos rekomendacijos "debesų kompiuterijos" paslaugų ir kt. klausimais bei savalaikiai reaguojanti į naujus technologinius pokyčius.

IV. Išvados

Apžvelgus ir išanalizavus pasirinktus mokslo leidinius, publikacijas, literatūros bei internetinius šaltinius, galima daryti tokias išvadas:

1. Technologijų konvergencija - paplitęs reiškinys daugelyje visuomeninio gyvenimo, mokslo ir viešojo administravimo sričių, pasižymi technologijų daugiafunkciškumu bei nuolatiniu tobulėjimu, kas įtakoja spartesnę žinių visuomenės kūrimą, IRT infrastruktūros plėtrą, kokybiškesnę paslaugų tiekėjų ir valstybės institucijų viešųjų paslaugų perkėlimą į elektroninę erdvę.

2. Technologijų konvergencija informacinėje visuomenėje yra tas skatinamasis tobulėti variklis, kuris veikia dėl pagrindinių rinkos motyvų – paklausos ir pasiūlos, o valstybė ir jos institucijos gali įtakoti šiuos motyvus, rūpinantis vartotojų švietimu, kompiuterinio raštingumo didinimu, įtakojant vartotojų motyvaciją naudotis elektroninėmis paslaugomis bei kuriant saugią ir patikimą skaitmeninę aplinką.

3. Pastebima tendencija, kad technologijų konvergencija viešajame administravime orientuojasi į mobiliųjų technologijų taikymą tiek modernizuojant darbo vietas, tiek atsiliepiant į vartotojų poreikį naudotis mobiliosiomis technologijomis, pasiūlant vis daugiau mobiliųjų paslaugų, taip siekiant kurti „visur esančius“ miestus, „visur esantį“ verslo valdymą.

4. Lietuvos e. valdžios skaitmeninė aplinka turi gerai išvystytas elektroninių ryšių sąlygas, yra išplėtotą tinklų infrastruktūrą, verslo, namų ūkio, valstybės institucijų IT ir mobilumo kriterijai, el. paslaugų plėtra (piliečiams, verslui). Lietuvos e. valdžios situacija Europos Sąjungos kontekste sparčiai vystosi ir orientuojasi į buvimo tarp lyderių scenarijų. Analizės išdavoje pastebima technologijų konvergencijos įtakota e. valdžios modelių transformacija į naujus, pažangius valdymo modelius. Šie pokyčiai suponuoja ateities komponentinės e. valdžios infrastruktūros kūrimą, kai planuojama jog e. valdžios technologinės platformos veiks aukšto patikimumo („visur esančioje“) aplinkoje.

5. Analizei pasirinkti specialaus teisinio reglamentavimo pavyzdžiai atskleidė technologijų konvergencijos įtaką kibernetiniam saugumui. Sparti technologinė plėtra sukelia grėsmių valstybiniais informaciniais ištekliais, strateginių objektų procesams, piliečių gerovei. Kibernetinis saugumas yra labai svarbi ir specifinė veiklos rūšis, kuri reikalauja nuoseklaus ir detalaus teisinio reglamentavimo. Viešasis sektorius galėtų įtakoti šią sritį koordinuojant veiksmus, savalaikiai reguliuojant teisinius ir veiklos santykius tarp institucijų ir šalių: teisinės bazės kūrimas / savalaikis keitimas, saugumo projektų plėtra, saugumo užtikrinimo reikalavimų nustatymas ir kontrolė, tyrimų duomenų savalaikis pateikimas, savalaikis vartotojų informavimas, informacinio tinklo sukūrimas, veiklos 24/7 užtikrinimas, specialistų mokymai, simuliacijos, treniruotės, prevencija, aktyvus bendradarbiavimas su tarptautinėmis organizacijomis ir pan.

6. Nauji pasiekimai medicinoje, elektroniniuose ryšiuose, mokslinėje veikloje bei kitose srityse ne tik didina žmonių generuojamos informacijos kiekį, bet ir išryškina naujas tendencijas, kurios kelia grėsmę asmens duomenų apsaugai: globalizacija, technologijų konvergencija, multimedijos gausa. Lietuvoje asmens duomenų apsaugos teisinis reguliavimas atitinka Europos Sąjungos reikalavimus, tačiau atsilieka nuo informacijos ir ryšių technologijų pažangos, parengtos metodinės rekomendacijos neaktualios ir apima ne visas problemines sritis susijusias su naujų technologijų taikymu. Viešasis sektorius galėtų įtakoti šią sritį per techninių – organizacinių reikalavimų savalaikį nustatymą ir kontrolę, teisės aktų, numatančių reguliavimą keičiantis technologijoms, atnaujinimą, savalaikių informavimo priemonių (viešosios konsultacijos, rekomendacijos, vieši renginiai, internetiniai tinklapiai, kuriuose būtų viešinama pagrindinė informacija apie naujas grėsmes, kibernetinio saugumo užtikrinimą asmens duomenų apsaugos srityje ir kt.) aktualizavimą, prevencines priemones, organizacijos saugos politikos nustatymą, rizikos vadovo, poveikio asmens duomenų apsaugai vertinimo parengimą ir pan.

Technologijų konvergencijos įtaką teisinei aplinkai sudėtinga nagrinėti tik viešojo administravimo kontekste, nes šis reiškinytis glaudžiai susijęs su kitomis tikslinėmis grupėmis (informacinės visuomenės paslaugų teikėjais, ypatingos svarbos infrastruktūros operatoriais, vartotojais, programėlių kūrėjais), veikia pasiūlos - paklausos rinkos dėsniai, visada išliks diskusijų klausimas, kiek valstybė turi reguliuoti šiuos santykius, kiek palikti savireguliacijai. Be to, sunku prognozuoti ateities technologines tendencijas, kurios nuolat keičiasi ir tobulėja. Galima pasidžiaugti, kad Lietuvoje šiuo metu svarstomas Kibernetinis saugumo įstatymo projektas, kuris tikimasi užpildys specialaus reglamentavimo spragas, o Europos Sąjungoje šiuo metu vykstanti ES duomenų apsaugos reforma turėtų užtikrinti žmonėms galimybę patiems kontroliuoti savo asmens duomenis, padėtų didinti jų pasitikėjimą elektroninėmis paslaugomis bei naujomis technologijomis. E. valdžia, savalaikiai reaguojanti į kintančias technologijas, elektroninių paslaugų plėtrą, kibernetines grėsmes ir saugumo sprendimus bei pasitelkusi mokslinių tyrinėjimų sritį, galėtų tapti koordinuojančia ašimi tarp visų bendradarbiaujančių šalių: viešo, privataus, mokslo sektorių tiek nacionaliniu, tiek tarptautiniu lygiu.

Literatūra

Norminė literatūra:

1. Lietuvos Respublikos Konstitucija.
2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 1996 m. birželio 11 d., Nr. I-1374.
3. Lietuvos Respublikos elektroninių ryšių įstatymas, 2004 m. balandžio 15 d. Nr. IX-2135.
4. Audiovizualinės žiniasklaidos paslaugų direktyva, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:341:0087:0091:LT:PDF> [žiūrėta 2014-03-22].
5. Lietuvos Respublikos Kibernetinis saugumo įstatymo projektas. http://www.lrs.lt/pls/proj/dokpaieska.showdoc_l?p_id=232334&p_org=9875&p_fix=n&p_gov=n [žiūrėta 2014-03-20].
6. Valstybės ilgalaikės raidos strategija, patvirtinta 2002 m. lapkričio 12 d. Lietuvos Respublikos Seimo nutarimu Nr. IX-1187 2011 m. kovo 16 d. Nr. 301 LRV nutarimas „Dėl Lietuvos informacinės visuomenės plėtros 2011–2019 metų programos patvirtinimo“.
7. 2011–2015 m. Europos e. valdžios veiksmų planas IRT naudojimas siekiant pažangios, darnios ir novatoriškos valdžios, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:LT:PDF> [žiūrėta 2014 01 07].
8. Europa 2020 „Pavyzdinės iniciatyvos“, http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_lt.htm [žiūrėta 2014 01 07].
9. Ataskaita „Viešosios paslaugos Web 2.0“, <http://www.rcc.gov.pt/SiteCollectionDocuments/ePractice-WorkshopReport-Public-eServ09.pdf> [žiūrėta 2013 12 22].
10. ES VN ministrų, atsakingų už elektroninę valdžią, deklaracija „Paskatinkime eSąjungos kūrimą“, <http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf> [žiūrėta 2013 12 16].
11. Lisabonos strategija, <http://www.e-library.lt/resursai/DB/IVPL/Lisabonos%20strateg/LISABONOS%20STRATEGIJA.pdf> [žiūrėta 2013 12 22].
12. Lietuvos informacinės visuomenės plėtros 2011–2019 metų programa, patvirtinta Lietuvos Respublikos Vyriausybės 2011 m. kovo 16 d. nutarimu Nr. 301.
13. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: Europos skaitmeninė darbotvarkė, 2010-05-19 http://europa.eu/rapid/press-release_IP-12-1105_lt.htm [žiūrėta 2013 12 18].

14. 2009 m. kovo 11 d. Europos Parlamento rezoliucija dėl Europos ekonomikos atkūrimo plano <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:087E:0098:0113:LT:PDF> [http://eeas.europa.eu/policies/eu-cyber-security/index_lt.htm].
15. Europos skaitmeninė darbotvarkė, http://www.europarl.europa.eu/aboutparliament/lt/displayFtu.html?ftuId=FTU_5.9.3.html [žiūrėta 2013 12 11].
16. Valstybinės duomenų apsaugos inspekcijos 2014-2016 metų strateginis veiklos planas, patvirtintas 2014-03-18 Teisingumo ministro įsakymu 1R-86.
17. 2009 m. spalio 28 d. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus įsakymas Nr. T-105 "Dėl administracinių paslaugų teikimo panaudojant informacinių ir ryšių technologijų priemones rekomendacijų patvirtinimo" .

Specialioji literatūra:

18. Kiškis M. ir kt. Teisės informatika ir informatikos teisė, Vilnius : Mykolo Romerio universiteto Leidybos centras, 2006.
19. Štītis D., Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos, Socialinės technologijos, 2013, 3(1), p. 189–207.
20. Štītis D., Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai, Socialinės technologijos, 2012 2(2), p. 441-455.
21. Štītis D., Pakutinskas P., Laurinaitis M., Dauparaitė I., Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai : kolektyvinė mokslo monografija / Mykolo Romerio universitetas. Vilnius : Mykolo Romerio universitetas, 2011.
22. Lietuvos e. valdžios gairės: ateities išvalgų tyrimas : kolektyvinė monografija / Vilnius : Mykolo Romerio universiteto Leidybos centras, 2009, p. 155
23. Juknevičius P., Bevielės technologijos elektroninio verslo paslaugų išvystymui: magistro baigiamasis darbas. Vilnius, Mykolo Romerio universitetas, 2008 http://vddb.library.lt/fedora/get/LT-eLABa-0001:E.02~2008~D_20090204_113827-99548/DS.005.0.02.ETD.
24. Kiškis M., Petrauskas R., Designing E-Government, 2002.
25. Pečiulis Ž., Technologinių naujovių iššūkiai ir tradicinės televizijos kaita. Informacijos mokslai. 2006 36.
26. Skyrius R. ir kt. „Informacijos ir komunikacijos technologijos“, vadovėlis, 2008 Vilnius.
27. Pečiulis Ž., Žiniasklaida ir žurnalistika daugiaterpės raiškos eroje. Informacijos mokslai. 2009, Nr. 51.

28. Surgailis D., Informacinių technologijų integracijos analizė ir tendencijos: magistro baigiamasis darbas. Vilnius, Vilniaus universitetas, 2008 http://vddb.library.lt/fedora/get/LT-eLABa-0001:E.02~2008~D_20101125_185246-19883/DS.005.1.01.ETD [žiūrėta 2013 12 22].
29. Šalauskas V. Telekomunikacijų ir informacinių technologijų konvergencijos įtaka visuomenės raidai. Elektronika ir elektrotechnika, 2003, Nr. 5(47), p. 74-75 <http://www.ee.ktu.lt/journal/2003/5/Salauskas.pdf> [žiūrėta 2013 12 08].
30. Sampson, Geoffrey., Network Computing, Mobile and Wireless. 2006. p. 177.
31. Jarukaitis I. ir kt. Elektroninių ryšių teisė, Vilnius: Eugrimas, 2005.

Internetiniai šaltiniai:

32. Informacinės technologijos Lietuvoje 2013, <http://osp.stat.gov.lt/statistikos-leidiniu-katalogas?eventId=1135> [žiūrėta 2013 12 22].
33. E-government conference "Where we are, where we are going", 14-15th November, 2013 Vilnius, <http://www.vrm.lt/index.php?4137282738> [žiūrėta 2013 12 22].
34. Įvadas į skaitmeninę konvergenciją, http://www.texascollaborative.org/SmithModule02/sec1_con.php [žiūrėta 2013 11 26].
35. Valstybės informacinės sistemos ir asmens duomenys „debesyje“ – ką apie saugumą kalba teisės aktai? <http://xn--debasis-9eb.lt/valstybes-informacines-sistemos-ir-asmens-duomenys-debesyje-ka-apie-sauga-kalba-teises-aktai> [žiūrėta 2014 01 11].
36. Čiurlionis G., Kibernetinės erdvės iššūkiai Lietuvoje – teisiniai, instituciniai, administraciniai aspektai. http://www.slideshare.net/AB_TEO_LT/gintaras-iurlionis-kibernetins-erdvs-ikiai-lietuvoje [žiūrėta 2014 01 09].
37. VU mokslininkas: informacijos saugumo klausimą reikia kelti jau šiandien <http://www.technologijos.lt/n/technologijos/it/S-31575/straipsnis/VU-mokslininkas-informacijos-saugumo-klausima-reikia-kelti-jau-siandien?l=2&p=1> [žiūrėta 2014 01 07].
38. 2013 metais CERT-LT ištyrė 25 337 incidentus elektroninėje erdvėje, http://www.rtt.lt/lt/pranesimai-spaudai/2013-metais-cert-5y5d.html?utm_source=EasyWeb3&utm_medium=newsletter&utm_campaign=pranesimai-spaudai [žiūrėta 2014 01 09].
39. Gatautis R., Elektroninio verslo ir elektroninės komercijos samprata ir plėtros tendencijos, <http://televizorius.files.wordpress.com/2011/12/samprata-ir-pletros-tendencijos.pdf> [žiūrėta 2013 11 16].
40. Kibernetiniai sukčiai taikosi į išmaniuosius įrenginius, <http://www.eset.com/lt/apie/spauda/straipsniai/article/kibernetiniai-sukciai-taikosi-i-ismaniuosius-irenginius/> [žiūrėta 2014 01 07].

41. Galimybių studija, skirta įvertinti tarptautinės teisės aspektus bei tarptautinės integracijos galimybes atsižvelgiant į Lietuvos teisinę, bazę,
http://www.esparama.lt/es_parama_pletra/failai/ESFproduktai/2011_tarptautines_teises_aspektai_bei_tarptautines_integracijos_GS.pdf [žiūrėta 2014 03 07].
42. Kirvelis D., Ateities visuomenė: transhumanizmas ir posthumanizmas,
http://www.technologijos.lt/n/zmoniu_pasaulis/redakcijos_akiratis/S-28962/straipsnis/Ateities-visuomene-transhumanizmas-ir-posthumanizmas?l=2&p=1 [žiūrėta 2013 12 18]
43. Paliulis N. K., Sabaitytė J., Elektroninio verslo plėtros kaip tvaraus konkurencinio pranašumo modelis. Verslas XXI amžiuje. 2012 4(3): 205-215
<http://www.mla.vgtu.lt/index.php/mla/article/view/mla.2012.34/pdf> [žiūrėta 2014 01 07].
44. Europos Sąjungos 2007-2013 m. struktūrinės paramos, skiriamos informacinės visuomenės plėtrai, viešinimo komunikacijos strategija ir gairės 2011-2013 m.,
<http://view.officeapps.live.com/op/view.aspx?src=http%3A%2F%2Fwww.ivpk.lt%2Fuploads%2FFS%2F2011-2013%2520m%2520informacines%2520visuomenes%2520komunikacijos%2520strategija.doc> [žiūrėta 2013 12 19].
45. Lietuvos nacionalinio radijo ir televizijos tarybos 2011 metų veiklos ataskaita,
http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?P_id=429288&p_query=program%ebl%ebs&p_tr2=2 [žiūrėta 2013 12 18].
46. Varšuvos deklaracija dėl mobiliems įrenginiams skirtų programėlių naudojimo,
<https://privacyconference2013.org/web/pageFiles/kcfinder/files/ATT29312.pdf> [žiūrėta 2013 12 18]
47. Konvergencija tarp „Debesų kompiuterijos“, interneto įrankių ir nešiojamųjų technologijų
http://www.wearable-technologies.com/wp-content/uploads/2013/07/130722_Keynote_Harry-Strasser_WT.pdf [žiūrėta 2013 12 18].
48. Vaitkevičienė R., Asmens identifikavimas e. erdvėje: problemos ir geroji praktika
[http://portalas.ada.lt/images/cms/File/Renginiai/tapatybes%20valdymas%20Rita%20Vaitkeviciene%20\(2\)%20\(2\).pdf](http://portalas.ada.lt/images/cms/File/Renginiai/tapatybes%20valdymas%20Rita%20Vaitkeviciene%20(2)%20(2).pdf) [žiūrėta 2013 12 17].
49. Pirmoji tarpinė ataskaita. Projektas „plačiajuosčio ryšio infrastruktūros plėtros ir paslaugų naudojimo skatinimo modelio parengimas”,
<http://www.ivpk.lt/uploads/Leidiniai/Pirmoji%20tarpine%20ataskaita.pdf> [žiūrėta 2013 12 12]
50. Technologijų konvergencija - Europos bendrijų ateities formavimas
http://ec.europa.eu/research/social-sciences/pdf/ntw-report-alfred-nordmann_en.pdf [žiūrėta 2012 10 26].

51. Kirvelis D., Socialmeritokratija versus socialdemokratija
<http://webcache.googleusercontent.com/search?q=cache:lUHI ioVx AJ:web.vu.lt/gf/d.kirvelis/files/2012/01/Socialmeritokratija-red.doc+&cd=2&hl=lt&ct=clnk&gl=lt> [žiūrėta 2013 12 16].
52. Dr. APJ Abdul Kalam., Technology in development of civil society.
http://www.abdulkalam.com/kalam/jsp/display_searchcontent.jsp?content=775&columnno=0&start=0&search_for=University%20of%20Toronto&sublink_id=68 [žiūrėta 2013 12 14].
53. Žalioji knyga dėl telekomunikacijų, žiniasklaidos ir informacijos technologijų sektorių konvergencijos bei jos reikšmės reglamentavimui,
http://ec.europa.eu/avpolicy/docs/library/legal/com/greenp_97_623_en.pdf [žiūrėta 2013 12 12].
54. Žalioji knyga dėl pasirengimo visiškam audiovizualinės aplinkos integravimui: augimas, kūrimas ir vertybės, <http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20130231.do> [žiūrėta 2013 12 12].
55. A Writing Exercise for the Public: Warren Sack on Digital Convergence,
<http://www.csisponline.net/2013/03/20/a-writing-exercise-for-the-public-warren-sack-on-digital-convergence/> [žiūrėta 2013 12 05].
56. Skaitmeninio verslo konvergencija <http://lauramccracken.wordpress.com/2012/09/15/digital-commerce-convergence-a-new-breed-of-leadership-needed/> [žiūrėta 2013 12 05].
57. Karlonaitė D., Radijo žurnalistikos ateitis: referatas. Vilnius, Vilniaus universitetas,
<http://zurnalistika.jimdo.com/referatai-1/radijo-%C5%BEurnalistikos-ateitis/> [žiūrėta 2013 11 06].
58. Tarptautinių žodžių žodynas, <http://www.tzz.lt/k/konvergencija> [žiūrėta 2013 10 28].
59. Lietuvos žinių visuomenės plėtros procesų apžvalga,
http://archyvas.infobalt.lt/sl/index_lt.php?t=ivpk [žiūrėta 2013 10 26].
60. „i2010 – Europos informacinė visuomenė augimui ir užimtumui skatinti“ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:LT:PDF> [žiūrėta 2013 10 02].

Prakapavičienė K. Technologijų konvergencijos įtaka elektroninės valdžios teisei aplinkai / Naujų technologijų teisės magistro baigiamasis darbas. Vadovas - Prof. dr. M. Kiškis. - Vilnius: Mykolo Romerio universitetas, Socialinių technologijų fakultetas Skaitmeninių technologijų institutas, 2014

SANTRAUKA

Magistro baigiamajame darbe išanalizuotas technologijų konvergencijos reiškinys ir jo įtaka viešajam administravimui. Parodyta, kad technologijų konvergencija, kai eliminuojami technologiniai barjerai tarp atskirų technologinių bei informacinių sistemų, kai kelios informacijos perdavimo formos sujungiamos į vieną formatą arba pakeičiamos kitais, kai šiuose procesuose dalyvaujantys galiniai įrenginiai (kartu su juose surinkta informacija), kinta, tobulėja, atlieka vis daugiau funkcijų, suteikia ne tik privalumų bet ir įgalina kelti saugumo klausimus. Neišvengiamai šie procesai turi įtakos ir viešojo administravimo modernizavimui:

Pirma, e. valdžios siekis įtraukti piliečius į sprendimų priėmimus, skatinimas naudotis el. paslaugomis turi sutapti su piliečių poreikiu dalyvauti e. valdžios procesuose jiems patogiu, pažangiu būdu: naujosios kartos tinklais, naudojant nuolat tobulėjančią įrenginių įvairovę.

Antra, pažangūs konverguojantys technologiniai sprendimai skatina valstybės įstaigas pertvarkyti savo veiklą, atsižvelgiant į didėjančią mobilumą ir visuotinį pasiekiamumą, kuris yra pagrindas keisti e. valdžią į mobiliąją (m. valdžią) ir taip artėti prie „visur esančių“ IRT, ateities žmogaus ir IRT sąveikos modelio.

Trečia, integruotos paslaugos orientuojasi į esmines technines ir socialines tendencijas, kas daro joms lemiamą įtaką, kai kartu su augančiu skaitmeninių technologijų skaičiumi daugelyje gyvenimo sričių, produktų ir paslaugų, jų pritaikymu asmeniniams ar visuomeniniams poreikiams, augančia mobilizacija ir internacionalizacija auga ir pažeidžiamumų elektroninėje erdvėje mastas, kas iššaukia poreikį konverguojantiems saugumo sprendimams.

Antrame skyriuje išanalizavus ES ir Lietuvos e. valdžios skaitmeninę aplinką, strateginius teisinius dokumentus parodomas valstybių siekis technologijų konvergencijos kontekste siekti mokslo ir technologijų pažangos, aptariamoms e. valdžios prioritetų gairėms, kryptys ir tikslai, pateikiama numatomų e. valdžios priemonių analizė, tiriamos sąlygos jų įgyvendinimui.

Trečiajame skyriuje atkreipiamas dėmesys, kad didėjanti technologijų konvergencija plečiant integruotų elektroninių paslaugų, suteikiančių prieigą prie asmeninės informacijos (pvz. identifikavimo, srauto, biometrinių duomenų, vaizdo įrašų, adresų, vietos nustatymo ir pan.) galiniais įrenginiais, įvairovė gali būti panaudota ir kaip įrankis tos pačios informacijos, sistemų, įrenginių pažeidžiamumui, taip inicijuojant kibernetines atakas ir siekiant įvairių tikslų: nuo tapatybės vagystės iki politinių užsakymų, finansinių nusikaltimų. Pateikiami siūlymai atskiroms tikslinėms grupėms kaip stiprinti duomenų bei informacijos saugą.

Prakapavičienė K. The Impact of Technological Convergence on Legal environment of Electronic Governance / Master's thesis in New Technology Law. Supervisor - Ph. dr. M. Kiškis. - Vilnius: Mykolas Romeris university, Faculty of Social Technologies, Institute of Digital Technologies, 2014

SUMMARY

Master's thesis analyzed the phenomenon of technological convergence and its impact on modernization of public administration. It is shown that the convergence of technologies, when the barriers between technology and information systems are eliminated, where several forms of communication are combined into one format or replaced by others, when terminals involved in these processes (together with information gathered by them), are changing, improving, and increasing in functionality, provide not only the advantages but also enables to raise issues of security. Necessarily these processes have an impact on modernization of public administration:

At first, e. government aims at involving citizens in the decision-making, the promotion of e-services that coincides with the needs of the citizens to participate in e. government processes in a convenient, advanced method: next-generation network, using a variety of devices that are constantly improving.

Second, advanced technological solutions stimulate state institutions to transform their business, given the increasing mobility and global availability, which is the basis for changing of the e. government into the mobile (m. government) and approaching to the ubiquitous ICT, to the model of interaction of ICT and future human.

Third, integrated services focus on the essential technical and social trends that make them a decisive impact. When combined with the growing number of digital technology in many areas of life, products and services, their use for personal or social purposes, growing vulnerabilities in cyberspace extent, that evoke the need for converging security solutions.

In the second chapter after analyzing e. government's digital environment and strategic legal documents of the EU and Lithuania, State's aspiration to achieve convergence of technologies is shown. This is done in the context of scientific and technological progress of the e. government priorities, guideline, directions and goals, analysis of e. government measures is presented, the conditions for their implementation examined.

The third chapter focuses on the increasing process of convergence of technologies, advancing variety of integrated electronic services that provide the access to personal information (such as identification, flow, biometrics, video, contact, location, etc.) and terminals can also be used as tools of vulnerability to the same information, systems and facilities, and the initiation of cyber attacks of various purposes, from thefts of identity to political orders and financial crimes. There are suggestions for specific groups how to enhance data protection and information security.

Priedai

1 priedas. Plačiajuostės interneto prieigos technologijų suvestinė

Eil Nr	Technologija	Greitaveika	Privalumai	Trūkumai	Aprėptis
1.	ADSL	24/1,4 Mb/s	-Nebrangi technologinė įranga; -Išnaudojama esama varinė infrastruktūra.	Brangus naujos varinės infrastruktūros įdiegimas; Maža išsiuntimo sparta; Ribotas prieigos atstumas.	3km
2.	VDSL	26Mb/s	Išnaudojama esama varinė infrastruktūra.	Ribotas prieigos atstumas.	1km
3.	Ethernet per vytos poros kabelius	1Gb/s	Nebrangi technologinė įranga; Didelė greitaveika.	Ribotas prieigos atstumas. Brangus naujos varinės infrastruktūros įdiegimas.	100m
4.	Ethernet šviesolaidiniais kabeliais	100Gb/s	Nebrangi technologinė įranga; Didelė greitaveika..	Brangus šviesolaidinės infrastruktūros įdiegimas.	80km
5.	PON	31,25Mb/s	Viena skaidula galima pajungti iki 64 vartotojų; Didelis paslaugos atstumas.	Brangi šviesolaidinių kabelių įrengimo kaina. Brangi PON įranga.	20km
6.	3G (HSPA)	84/10,8 Mb/s	Pigesnė įrengimo kaina; Mobilumas; Įdiegta daugelyje išmaniųjų telefonų.	Sąlyginai nedidelė paslaugos greitaveika; Nepilnas padengimas; Bendrai naudojami resursai.	3km
7.	WiFi	300Mb/s	Pigi įranga; Lengvas paslaugos pateikimas; Įdiegta daugelyje išmaniųjų telefonų.	Maža aprėptis; Reikalingos apsaugos priemonės; Bendrai naudojami resursai.	300m
8.	WiMAX	70Mb/s	Mažesnė kaina nei kabelinės infrastruktūros; Mobilumas; Nemaža paslaugos greitaveika.	Veikimo kokybė priklauso nuo geografinių aplinkos sąlygų; Nepilnai padengta Lietuvos teritorija WiMAX ryšiu; Sąlyginai nedidelis galinės įrangos pasirinkimas; Bendrai naudojami resursai.	50km
9.	LTE	300/75 Mbs	Didelė paslaugos greitaveika; Mobilumas; Tinklo įrengimo kaina pigesnė lyginant su šviesol. kabelio klojimu.	Brangi įranga; Mažas galinės įrangos pasirinkimas. Brangi šviesolaidinių kabelių įrengimo į bazines stotis kaina	5km
10.	PLC	1,5Gb/s	Nebrangi įranga; Lankstumas; Naudoja esamą elektros perdavimo instaliaciją.	Yra mažiau patikima, nes veikimas priklauso trikdžių elektros perdavimo linijoje; Turi apribojimų dėl galimo atstumo ir transformatorių, esančių perdavimo grandinėje, rūšies ir kiekio; Reikalauja papildomų saugos priemonių.	1,5km

11.	Palydovinis ryšys	40/6Mb/s	Gali būtų įdiegiama vietovėse, kuriose kitų rūšių infrastruktūra neegzistuoja; Patikimas išskirtinis duomenų perdavimo kanalas be tarpininkų.	Dėl didelio vėlinimo netinka realaus laiko paslaugom; Yra mažiau patikima, nes veikimas priklauso nuo oro sąlygų; Labai brangi įranga ir paslaugos.	-
-----	-------------------	----------	--	---	---

2 priedas. Galinių įrenginių pavyzdžiai.

Galinio įrenginio pavadinimas	Operacinių sistemų pavyzdžiai / (taip /ne)	Taikomųjų programų pavyzdžiai / (taip /ne)	Saugumo sprendimų pavyzdžiai / (taip /ne)
Personalinis kompiuteris PC	MS-DOS Microsoft Windows 95 Microsoft Windows 98 Microsoft Windows 2000 Microsoft NT Unix Linux	-Bylų ir katalogų tvarkymo programos (Dos Shell, Windows Explorer); - Pagrindinės taikomosios programos (Microsoft Word; M'Access; M'Excel; M'PowerPoint; Adobe; Corel Draw; Microsoft Works); - Programavimo kalbų transliatoriai (C#, Java, JavaScript, PHP); - Enciklopedijos, žodynai (Microsoft Encarta; WinLED; Encyclopedia of Nature; Great Artist).	Antivirusinės programos; Ugniasienė; Maršrutizatoriaus ugniasienė
Nešiojamas kompiuteris	Standartinė OS	Tinka taikomoji programinė įranga kaip ir standartiniams kompiuteriams	Antivirusinės programos; Ugniasienė.
Planšetinis kompiuteris	Windows RT, iOS, Android	JustWrite ir kt.	Sophos Security & Antivirus
Delninelukas	Windows CE, Palm OS (Palm inc.), BlackBerry (Blackberry Ltd.)	Navigacija, Sandelių valdymas (EXO4 PDA)	Kaspersky Labs Security for PDA, Šifravimo programos PocketLock for Pocket PC
Mobilus telefonas	Android (Google), iOS (Apple), Symbian OS, Windows	Google Play Store, Apple Store, Samsung App Store, VMS mobiliosios aplikacijos	Antivirus Apps, Kaspersky mobile
Tarnybinės stotys	UNIX, Linux, Windows OS, Mac OS	PHP, MySQL, Apache, BIND, Exchange, IIS	2003 Server Antivirus
Skaitmeninė televizija, skaitmeninis radijas	Linux OS, Firefox OS	Samsung Smart TV, BBC iPlayer, Demand 5, BBC News. Vaizdo konferencijų app, Init, MicroVisata	Ugniasienė
Periferiniai įrenginiai (daugiafunkciniai įrenginiai)	Linux OS	Failų saugykla, el. pašto išsiuntimas, riboto naudojimo dokumentų šifravimas	Security Kit
Virtualieji įrenginiai: VMware ESXi (apima virtualią tinklo įrangą, virtualią atminties kontrolerį ir duomenų saugojimo įrangą, kitų resursų virtualizavimą)	Bet kuri standartinė OS	VmWare tools (virtualios mašinos būsenos sekimui)	Kaspersky Security for Virtualization; vShield Endpoint; VMware NSX naudojimas kartu su išmaniųjų ugniasienių sprendimais (pvz. Cisco UCS)

Saugumo spragų klasifikacija konverguojančiais įrenginiais
Kompiuterių virusai Kenkėjiška programinė įranga kuriama ne tik kompiuteriams, bet ir mobiliems telefonams. Dalis jos patenka su įrašomomis programomis, kita dalis – plinta savarankiškai. Kenkėjiška programinė įranga gali padaryti daug žalos, mes tiek kompiuteriuose, tiek mobiliuosiuose įrenginiuose saugoma daug ir svarbios informacijos, kurios praradimas gali sukelti daug problemų.
Šnipinėjimo programos Šnipinėjimo programos gali būti įdiegtos į kompiuterį ar kitą įrenginį (pvz., išmaniuosius telefonus, planšetinius kompiuterius). Jos siekia rinkti informaciją apie kompiuterio naudotoją be pastarojo žinios. Naudotojas gali tapti auka ir "savo noru" (prieš sutikdamas su programos licencija. Renka informaciją apie naudotoją – interneto naršymo įpročius, e. pašto adresus, bendravimo programų išklotines, perduoda tretiesiems asmenims kompiuteryje saugomas bylas ir pan. Jai būdingas ir galinio įrenginio konfigūracijos keitimas, naršyklės peradresavimas į kenkėjiškus puslapius, klavišų paspaudimo registravimas ir pan. Pagrindinės keliamos grėsmės: asmens duomenų rinkimas, tapatybės vagystės, konfidencialios informacijos perdavimas tretiesiems asmenims.
Nepageidaujami el. laiškai Šiuo metu pasaulyje „spam“ srautas sudaro didesniąją dalį viso el. pašto srauto ir tai yra didžiulė problema elektroninių ryšių tinklams. Interneto paslaugų tiekėjų sistemos tampa perkrautos, sumažėja bendras srauto pralaidumas, tenka pasitelkti papildomus resursus kovai su „spam“, patiriami dideli finansiniai nuostoliai. Problema tampa vis aktualesnė dėl nepageidaujamų sms žinučių, el. laiškų siuntimo, jais plintančių kompiuterių virusų bei įvairių apgaulės būdų grėsmės.
Duomenų vagystės („phishing“) Tai kompiuterio ar mobilaus telefono ekrano perėmimas ir valdymas, pvz. siekis perimti internetinės bankininkystės kodus, kurie naudojami prisijungimui prie "El. valdžios vartų" kaip asmens identifikavimo priemonė el. valdžios paslaugoms gauti (www.epaslaugos.lt). Nors E. bankininkystės paslaugoms Lietuvoje yra naudojamos moderniausios Europos standartus atitinkančios apsaugos technologijos, tačiau jos pasiekiamos mobiliu, telefoniniu, internetiniu būdu gali būti atakuojamos.
„Botnet“ tinklai. Mobilieji „botnet“ tinklai Daugelis išmaniųjų įrenginių yra prijungti prie interneto nuolatinio 3G ar panašiu ryšiu. Mobilieji įrenginiai yra pakankamai galingi ir skaičiavimo pajėgumais prilygsta galingiems kompiuteriams. Saugumo ekspertai yra aptikę mobiliųjų „botnet“ tinklų formavimo pavyzdžių: „DROIDDREAM“ ar „GEIMINI“. „DroidDream“ naudojosi dviem „Android“ spragomis, taip pat ir „Apple iOS“ pdf bylų apdorojimo spraga. Įvairių šaltinių duomenimis, 2011 metais buvo aptikta ne mažiau, nei 10 skirtingų mobiliųjų „botnet“ tinklų.
Mobilieji įrenginiai Šiuolaikiniai mobilūs įrenginiai gali patys atsisiųsti įvairias programas, jų naujinius ar jungtis prie interneto, kas padidina kenkėjiškų programų plitimą ir grėsmę.
Kitos saugumo spragos • Interneto naršyklės programoje yra aptinkama saugumo spraga, leidžianti vykdyti kodą sistemoje, kurioje įdiegta pažeidžiama programa. • Sudėtingiausia programa, veikianti kompiuteryje, yra operacinė sistema (toliau - OS), tad būtent ji ir tampa kritine vieta vartotojo kompiuterio saugumui. Dėl to OS saugumo spragos ir yra dažniausiai išnaudojamos įvairioms saugumo pažeidimo atakoms (kompiuterių virusai, „spam“ platinimas, kompiuterių zombių tinklų kūrimas ir kt.) įvykdyti. • nuo 2014 m. balandžio 8 dienos nebepalaikoma Windows XP operacinė sistema, kuri valstybiniame sektoriuje yra plačiai naudojama, o taikomoji programinė įranga išigyjama viešųjų pirkimų metu pagal pigiausią kriterijų. Tai didina saugumo grėsmę. • Vis dažniau darbo vietose naudojami planšetiniai, išmanieji įrenginiai be administratorių žinios, tokie procesai nėra sureglamentuoti vidaus tvarkos procedūromis.
Tinklo saugumo pažeidimai • Daugiafunkcinių įrenginių naudojimas įstaigose, pvz. skenavimas – atvirų prievadų paieška, naudojama aktyvioms tinklinėms paslaugoms identifikuoti, nelegalus būdas persiųsti konfidencialius duomenis. • Nesankcionuotas priejimas prie sistemos vartotojo teisėmis. • Nesankcionuotas priejimas prie sistemos administratoriaus teisėmis. • Tinklo paketų perėmimas, analizuojant jų turinį ir siekiant gauti slaptos informacijos, pavyzdžiui,

vartotojų vardus, slaptažodžius ar pan.

- DoS (*Denial of Service*⁹⁹) ataka – pažeidimas, siekiant pakenkti ar visai nutraukti sistemos darbą.
- Pasitikėjimo eksploatavimas – apsimetimas kitu vartotoju ar kompiuteriu, siekiant gauti jam paskirtus resursus.
- Kenkėjiškas kodas – tai kenkėjiškos programos, veikiančios be vartotojo žinios, pavyzdžiui, virusai, kirminai ir t.t.

Tinklo infrastruktūros atakavimas, siekiant sutrukdyti tinklo infrastruktūros darbą, pavyzdžiui, vardų serverių ir tinklo maršrutizatorių atakavimas.

Belaidžio tinklo saugumas

Paslaugų teikėjai perkeldami elektronines paslaugas, programinę įrangą, klientų duomenis į interneto svetaines, pasiekiamas išoriniais perdavimo tinklais, jų nešifruoja https protokolu, o netinkamai sukonfigūruotas belaidis tinklas gali atverti kelią įsilaužėliams ir leisti jiems perimti tinklo keliaujančius duomenis arba netgi įsilaužti į kompiuterius šiame tinkle. Mobiliaisiais įrenginiais dažnai jungiamasi prie viešųjų interneto prieigos taškų, kuriuose dažniausiai neužtikrinamas pakankamas perduodamo tinklo srauto šifravimo lygis.

4 priedas. Informacijos saugą reglamentuojantys teisės aktai

Teisės akto pavadinimas ir nuoroda	Priėmimo data	Nuorodos į teisės aktų punktus, kuriuose aptariamas požiūris į kintančias technologijas
Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas	2011 m. gruodžio 15 d. Nr. XI-1807	1,2,4,5,6,8,9,10 straipsniuose aptarti IT plėtros ir visumos klausimai
Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa	2011 m. birželio 29 d. Nr. 796	1,6 straipsniuose aptariama informacinių technologijų esami ir nuolat aptinkami nauji pažeidžiamumai, kas laiku nepašalinus, sudaro sąlygas sutrikdyti informacinių išteklių, taip pat ypatingos svarbos informacinės infrastruktūros objektų funkcionavimą.
Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, Saugos dokumentų turinio gairių aprašas ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas	2013 m. liepos 24 d. Nr. 716	3.3.4.p. leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos (jeigu kompiuterius leidžiama naudoti nustatytoms funkcijoms atlikti ne institucijos patalpose, turi būti nurodytos papildomos saugos priemonės, taikytinos tokiems kompiuteriams (šifravimas, papildomas tapatybės patvirtinimas, prisijungimo ribojimai, rakinimo įrenginių naudojimas ir panašiai).
Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai	2013 m. spalio 4 d. Nr. 1V-832	5.12.15. informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę; ugniasienės įvykių žurnalai (angl. Logs) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos; 6.2. viešaisiais ryšių tinklais perduodamos informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. <i>virtual private network</i>), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas priemones.
Informacinių technologijų saugos	2004-05-	nėra

⁹⁹ angl. "Distributed Denial of Service" - paskirstytas atsisakymas aptarnauti, yra būdas kenkti serveriui, kad jis nepajėgtų aptarnauti vartotojų užklausų. Serveriui yra pasiunčiamas didelis kiekis užklausų iš didelio kiekio kompiuterių, ko pasekoje serveris nebespėja gražinti atsakymų. Paprastai kompiuteriai būna užkrėsti virusais ir jų kiekis gali siekti dešimtis tūkstančių.

atitikties vertinimo metodika	06 d. Nr. 1V-156	
Saugaus elektroninės informacijos teikimo sutarties pavyzdinė forma	2007-06-29 d., Nr. 1V-241	nėra
Interneto tarnybinių stočių apsaugos rekomendacijos	2004-05-21 d. Nr. 1V-176	nėra
Rekomendacijos kibernetiniam saugumui užtikrinti	2013-06-19	3.1. patikrinti ugniasienių, per kurias kontroliuojamas naudotojų prisijungimas iš viešųjų elektroninių ryšių tinklų, sąrankas (konfigūracijas); 4.6. siekiant palengvinti institucijos gynybą „DDos“ atakos atveju, siūlome sukurti ir prireikus panaudoti minimalios apimties titulinio įstaigos tinklalapio versiją; pavyzdžiui, tai galėtų būti paprastas „HTML“ tinklalapis su iš anksto numatytu pranešimu: „po 5 sekundžių būsite peradresuoti į kitą įstaigos tinklalapio versiją“; 5. Rekomenduojame viešojo administravimo institucijoms ir savivaldybėms savo informacinių sistemų apsaugai naudotis Saugaus valstybinio duomenų perdavimo tinkle įrengta kolektyvine apsaugos nuo grėsmių iš viešųjų tinklų sistema.
Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimai	2007 m. birželio 5 d. Nr. 1V-210	48. SVDPT turi būti suskaidytas į SVDPT sritis, kurios fiziškai ir / arba logiškai būtų atskirtos tarpusavyje ir nuo kitų tinklų ir atitiktų bendrus tai SVDPT sričiai keliamus elektroninės informacijos saugos reikalavimus. Įslaptinta informacija ir viešam naudojimui neskirta elektroninė informacija gali būti perduodama tik šifruotu pavidalu ir negali būti prieinama kitų SVDPT sričių SVDPT naudotojams. Viešoji elektroninė informacija SVDPT gali būti perduodama nešifruota. 52p. aptartas SVDPT naudotojų saugus prijungimas prie SVDPT, įgyvendinant šiuos reikalavimus
Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms	2008 m. lapkričio 12 d. įsakymas Nr. 1T-71	10.7. užtikrinamas saugių protokolų ir (arba) slaptažodžių naudojimas, teikiant asmens duomenis išoriniais duomenų perdavimo tinklais; 10.11. Nešiojamuosiuose kompiuteriuose, jeigu jie naudojami ne duomenų valdytojo vidiniame duomenų perdavimo tinkle, esantys asmens duomenys turi būti šifruojami tokiomis priemonėmis, kurios atitiktų duomenų tvarkymo keliamą riziką.