MYKOLO ROMERIO UNIVERSITETAS

VERSLO IR MEDIJŲ MOKYKLA

(BUSINESS AND MEDIA SCHOOL (BMS))

LINAS PAUKŠTĖ

Kibernetinio saugumo valdymas

KIBERNETINIO SAUGUMO VALDYMO YPATUMAI ĮGYVENDINANT INTERNETO RINKIMUS

Magistro baigiamasis darbas

Darbo vadovas –

doc. dr. T. Limba

Vilnius, 2015

MYKOLAS ROMERIS UNIVERSITY

BUSINESS AND MEDIA SCHOOL

LINAS, PAUKŠTĖ

CYBER SECURITY MANAGEMENT PECULIARITIES DURING INTERNET VOTING

Master Thesis

Supervisor:

assoc. prof. T. Limba

Vilnius, 2015

TURINYS

SANTRUMPOS

CD – Compact disc

DdoS – Distributed Denial of Service

DNS – Domain Name System

DoS – Denial of Service

DVD – Digital Versatile Disc

e. balsadėžė – elektroninė balsadėžė

e. parašas – elektroninis parašas

e.valdžia – elektroninė valdžia

e.vyriausybė – elektroninė vyriausybė

EML – Election Markup Language

HTTPS – Hyper Text Transfer Protocol Secure

ID – Identity Document

IDS – Intrusion Detection System

IP address – An Internet Protocol address

ISO – International Organization for Standardization

JAV – Jungtinės Amerikos Valstijos

KAM – Krašto apsaugos ministerija

LR – Lietuvos Respublika

LRV – Lietuvos Respublikos Vyriausybė

MRU – Mykolo Romerio universitetas

PIN – Postal Index Number

PKI – Public Key Infrastructure

QR code – Quick Response Code

RRT – Ryšių reguliavimo tarnyba

SIM – Subscriber Identity Module

SSGG – Stiprybės, Silpnybės, Galimybės, Srėsmės

SSL – Secure Sockets Layer

SWOT – Strengths, Weaknesses, Opportunities and Threats

TSL – Transport Layer Security

USB – Universal Serial Bus

VRK – Vyriausioji rinkimų komisija

WAF – Web Application Firewall

ĮVADAS

Temos aktualumas ir naujumas. Pasaulyje elektroniniu būdu leidžiama balsuoti 48 pasaulio valstybėse (Šveicarijoje, JAV, Kanadoje, Kazachstane ir kt.). Neabejotini interneto rinkimų lyderiai yra estai. Daugumoje šalių internetu galima balsuoti tik savivaldos rinkimuose, tuo tarpu Estijoje nuo 2005 metų internetu galima balsuoti visuose šalyje vykstančiuose rinkimuose. Tačiau interneto rinkimus teigiamai vertina anaiptol ne visi. Olandijoje sėkmingai veikę elektroniniai rinkimai nuo 2007 metų uždrausti. Vokietija ir Norvegija taip pat atsisakė elektroninio balsavimo kaip nepateisinusio vilčių ir negalinčio užtikrinti tiek balsavimo slaptumo, tiek apsaugos nuo pašaliečių įsilaužimo į sistemą. Šiuo metu interneto rinkimų tema Lietuvoje ypač aktuali bei kelia daug diskusijų. Lietuvos Respublikos Seimo (toliau - LR Seimo) komitetuose svarstomas jau penktasis įstatymų projektų paketas dėl galimybės balsuoti internetu rinkimuose ir referendumuose. Naujausią įstatymų projektų paketą parengė teisingumo ministras Juozas Bernatonis ir susisiekimo ministras Evaldas Sinkevičius. Atsižvelgiant į tai, kad šie politikai priklauso dabartinei LR Seimo daugumai, o įstatymų projektų priėmimui trūksta tik politinės valios, galima tikėtis sėkmingos šių projektų ateities. Šiandien, vykstant ne tik smulkiems interneto išpuoliams prieš pavienius asmenis, bet ir koncentruotoms didelio masto atakoms prieš įmones, bankus ar valstybinius sektorius, apsisaugojimas nuo kibernetinių išpuolių tampa šalių strateginiu tikslu. Interneto rinkimai yra labai specifinė bei labai svarbi demokratijos išraiška, kuriai itin svarbu apsisaugoti tiek nuo vidaus, tiek nuo išorės pavojų. Sėkminga kibernetinė ataka prieš tokį svarbų valstybei procesą kaip rinkimai gali ne tik būti priežastimi, dėl kurios rinkimai būtų pripažinti negaliojančiais, bet taip pat gali sukompromituoti valstybę bei sugriauti žmonių pasitikėjimą ja.

Šiame darbe bus nagrinėjamas visas interneto rinkimų procesas kibernetinio saugumo kontekste. Išanalizavus sėkmingai pasaulyje veikiančias interneto rinkimų sistemas bei atlikus kokybinį tyrimą (ekspertinį interviu) bus bandoma sukurti Lietuvos interneto rinkimų kibernetinio saugumo valdymo modelį.

Mokslinė problema. Mokslo šaltiniuose nepakankamai ištirtos pasaulyje sėkmingai veikiančios interneto rinkimų sistemos, grėsmių šaltiniai, galimi atakų vektoriai, metodai bei metodikos.

Darbo objektas. Kibernetinio saugumo valdymas vykdant interneto rinkimus.

Tyrimo tikslas. Išanalizavus kibernetinio saugumo valdymo ypatumus, atlikus interneto rinkimų sistemų kibernetinio saugumo analizę, pasinaudojus pasaulinėmis gerosiomis praktikomis, sukurti kibernetinio saugumo valdymo modelį interneto rinkimams.

Tyrimo uždaviniai:

1. Išnagrinėti interneto rinkimų kibernetinio saugumo valdymą teoriniu aspektu;

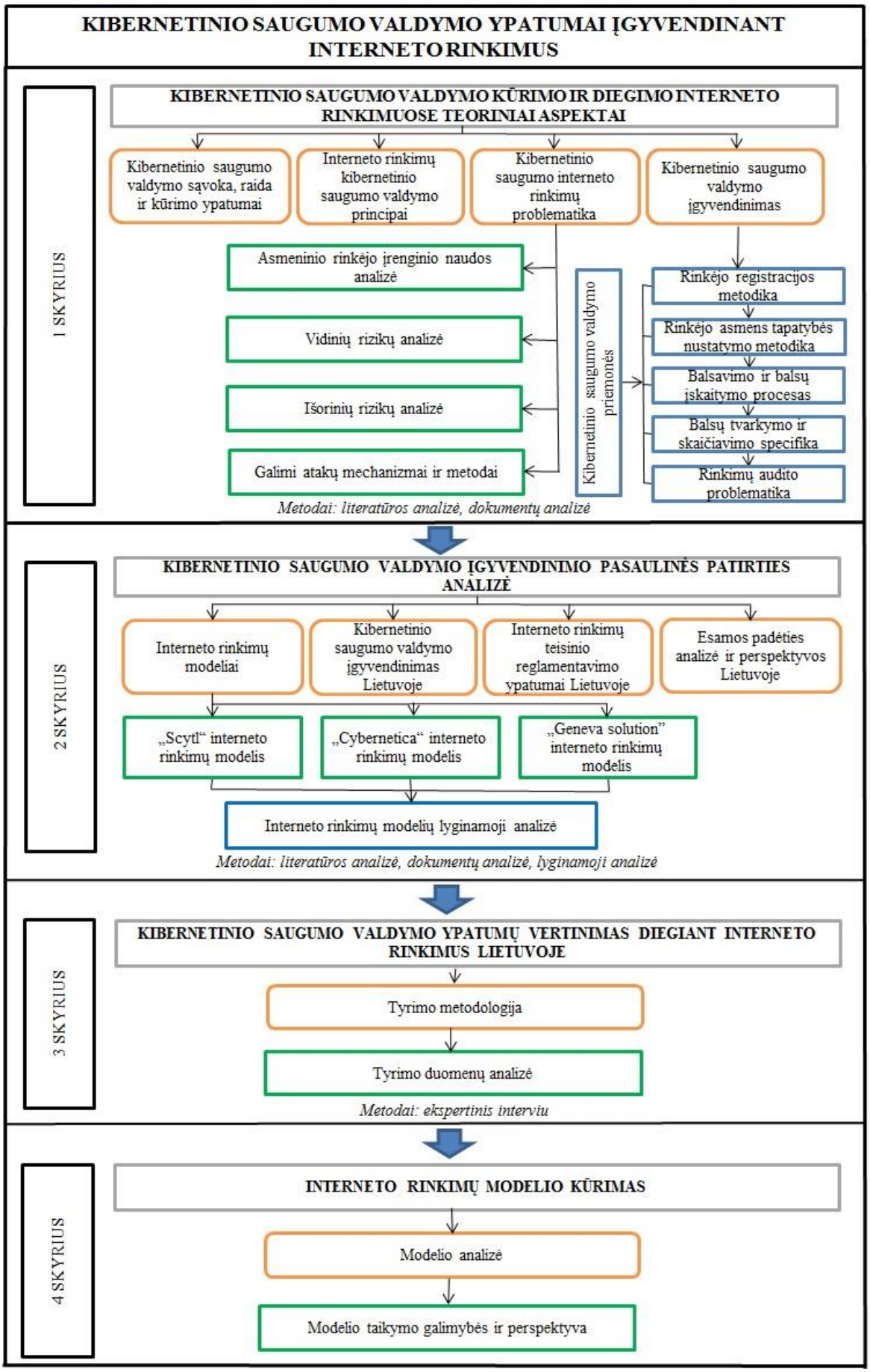
2. Atlikti kibernetinio saugumo valdymo pasaulinės patirties analizę; apžvelgti interneto kibernetinio saugumo valdymo įgyvendinimą bei interneto rinkimų teisinio reglamentavimo ypatumus Lietuvoje;

3. Atlikus interneto rinkimų ir kibernetinio saugumo ekspertų apklausą, apibrėžti probleminius interneto rinkimų bei kibernetinio saugumo valdymo aspektus ir išsiaiškinti galimas jų sprendimo metodikas bei metodus;

4. Teorinės ir praktinės pasaulio šalių gerosios praktikos pagrindu pasiūlyti kibernetinio saugumo valdymo modelį interneto rinkimams Lietuvoje.

Darbo šaltiniai ir metodai. Teoriniai tyrimo metodai: mokslinės literatūros analizė ir sintezė, kitų šalių gerajai praktikai palyginti naudojama lyginamoji analizė, renkant bei analizuojant statistinius duomenis apie kibernetinius incidentus panaudota antrinių duomenų analizė. Šaltinių paieškai naudojamos Mykolo Romerio universiteto (toliau - MRU) prenumeruojamos elektroninės duomenų bazės (EBSCO host, Mybrary, Ebrary ir kt.), MRU mokslo publikacijos, kiti interneto puslapiai. Tiriama tema yra nauja, todėl empirinių duomenų rinkimui tyrėjas rėmėsi kokybine metodologija. Tyrimui pasirenkamas pusiau struktūrizuotas giluminio interviu metodas. Buvo apklausta 13 ekspertų. Gauti duomenys apdoroti naudojant kokybinę turinio analizę. Nagrinėjama tema šaltinių lietuvių kalba nedaug. A. Ramonaitė ir kt. parengė elektroninio balsavimo galimybių studiją, kurioje nagrinėja interneto rinkimų problematiką, kitų šalių patirtį, aptaria kai kuriuos saugumo klausimus. T. Limba ir K. Agafonov aprašo elektroninių rinkimų sistemas, jų konstravimo principus, modelius. D. Štitilis nagrinėja kibernetinio saugumo teisinį reguliavimą bei kartu su M. Kiškiu, R. Petrausku ir I. Romonskiu analizuoja nusikaltimus elektroninėje erdvėje. Darbe taip pat remiamasi LR Seimo Parlamentinių tyrimų departamento parengtomis studijomis, LR įstatymais ir kitais poįstatyminiais aktais. Interneto rinkimų modelius aprašo N. Shah, J. Puiggali, D. Springall. Interneto rinkimų saugumo problematiką nagrinėja Al-Ameen , A. Samani, D. Evans, A. Rubin, D. Wallach.

Darbo struktūra. Magistro darbą sudaro 4 dalys (žr. 1 pav.). *Pirmoje* dalyje pateikiami kibernetinio saugumo valdymo, kūrimo ir diegimo interneto rinkimuose teoriniai aspektai: apibrėžiama kibernetinio saugumo valdymo sąvoka, nagrinėjami interneto rinkimų kibernetinio saugumo valdymo principai bei problematika. Aprašomas balsavimo internetu kibernetinio saugumo valdymo įgyvendinimas. *Antroje* dalyje pateikiama kibernetinio saugumo valdymo įgyvendinimo pasaulinės patirties analizė: analizuojami „Scytl“, „Cybernetica“ ir „Geneva solution“ interneto rinkimų modeliai, atliekama šių modelių lyginamoji analizė. Nagrinėjami kibernetinio saugumo valdymo įgyvendinimo aspektai Lietuvoje, aptariami interneto rinkimų teisinio reglamentavimo ypatumai bei atliekama esamos padėties analizė (SSGG analizė). *Trečioje*



Šaltinis: sudaryta autoriaus

1 pav. **Magistro baigiamojo darbo struktūros loginė schema**

dalyje atliekamas kokybinis tyrimas panaudojant ekspertinio interviu metodą. Apklausus 7 interneto rinkimų bei 6 kibernetinio saugumo ekspertus, nustatomi probleminiai interneto rinkimų aspektai, pateikiamos galimų sprendimų rekomendacijos. *Ketvirtoje* dalyje pasiūlytas interneto rinkimų kibernetinio saugumo valdymo modelis interneto rinkimams Lietuvoje. Darbo pabaigoje pateikiamos išvados ir rekomendacijos.

Darbo praktinė reikšmė. Remiantis teorinėmis ir praktinėmis pasaulinėmis gerosiomis praktikomis, atsižvelgus į Lietuvos kibernetinio saugumo valdymo įgyvendinimo aspektus ir interneto rinkimų teisinio reglamentavimo ypatumus bei dviejų sričių ekspertų (interneto rinkimų ir kibernetinio saugumo valdymo) rekomendacijas, pasiūlytas interneto rinkimų kibernetinio saugumo valdymo modelis, kuris galėtų būti pritaikytas įgyvendinus interneto rinkimus Lietuvoje.

1. KIBERNETINIO SAUGUMO VALDYMO KŪRIMO IR DIEGIMO INTERNETO RINKIMUOSE TEORINIAI ASPEKTAI

1.1. Kibernetinio saugumo valdymo sąvoka, raida ir kūrimo ypatumai

Šiuolaikinių organizacijų vidiniai valdymo procesai tapo neįmanomi be informacinių technologijų ir informacinių sistemų bei interneto prieigos. Internetas turi vis daugiau įtakos kasdieniniam gyvenimui, taip pat ir globaliai ekonomikai (Štitilis, 2013). Šiandien kasdienis gyvenimas, pagrindinės teisės, socialinė sąveika ir ekonomika priklauso nuo sklandaus informacinės ir ryšių technologijos veikimo. Fenomenali kibernetinės erdvės plėtra atnešė beprecedentį ekonomikos vystymąsi bei naujų galimybių plėtrą. Tačiau tai sąlygojo ir naujų grėsmių atsiradimą. Šie pokyčiai verčia šalių vyriausybes imtis priemonių bei kurti infrastruktūrą, kuri užtikrintų tolesnį ekonominį vystymąsi, efektyvumą bei apsaugą (Informacinių technologijų pramonės taryba, 2011). Europos Sąjungos kibernetinio saugumo strategijoje (2013) pastebima, kad „tyčiniai ar atsitiktiniai kibernetinio saugumo incidentai dažnėja nerimą keliančiu greičiu“. Šie incidentai gali sutrikdyti pagrindinių paslaugų teikimą (vandens, elektros energijos tiekimą, sveikatos priežiūros ar judriojo ryšio paslaugų teikimą). Štitilis (2013) pastebi, kad elektroninės erdvės globalumas sukūrė beprecedentes sąlygas daryti nusikaltimus iš bet kurio pasaulio taško, kur yra internetas ir grėsmės elektroninėje erdvėje kyla ne tik atskiriems vartotojams, bet net ir pačioms valstybėms.

Visuomenėje kibernetinio saugumo samprata dažnai painiojama su tokiomis sąvokomis kaip elektroninė informacijos sauga, informacijos sauga, tinklų ir informacijos saugumu bei informacinių sistemų apsauga.

Tinklų ir informacijos saugumas – tai tinklų ar informacinės sistemos pajėgumas tam tikru patikimumo lygiu išlikti atspariai nuo atsitiktinių įvykių ar neteisėtų arba tyčinių veiksmų, kurie keltų pavojų išsaugotų ar perduotų duomenų bei susijusių siūlomų ar per tuos tinklus arba sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ir slaptumui (Tinklų ir informacijos saugumas, 2015). Tinklų ir informacijos saugumas užtikrina tam tikrą atsparumo lygį, kuriuo stengiamasi išvengti tam tikros žalos. Sąvoka neapima aptikimo, analizavimo, galimo reagavimo bei veiklos atkūrimo.

Informacijos sauga - informacijos bei sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio pobūdžio poveikio, galinčio sukelti žalą informacijos ar sistemos infrastruktūros savininkams bei vartotojams (Kiškis ir kt., 2006, p. 38). Ši sąvoka taip pat yra tik siaura kibernetinio saugumo apibrėžimo dalis, apimanti informacijos bei sistemos infrastruktūros apsaugą nuo galimos žalos.

Dar daugiau neaiškumo prideda tai, kad Lietuvos Respublikos įstatymuose ir kituose teisės aktuose pateikiamos skirtingos kibernetinio saugumo sampratos. „Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011 – 2019 metais programoje“ bei 2012 metų LR vidaus reikalų ministro įsakyme „Dėl valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėjimo sistemos nuostatų patvirtinimo“ elektroninė informacijos sauga tapatinama su kibernetiniu saugumu. Tuo tarpu 2013 m. LR Vyriausybės nutarimu patvirtintame Bendrųjų elektroninės informacijos saugos reikalavimų apraše *elektroninė informacijos sauga* apibrėžiama kaip elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

Šią problemą išsprendė 2014 gruodžio 11 d. priimtas Kibernetinio saugumo įstatymas, kuris aiškiai apibrėžia kibernetinio saugumo sąvoką kaip „visumą teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti“.

Kuriant kibernetinį saugumą būtina atsižvelgti į keletą aspektų. Kiškis ir kt. (2006) išskiria keturias pagrindines elektroninės informacijos saugos grupes, kurias galima pritaikyti ir kibernetinio saugumo valdymui:

1. Normatyvinę – įstatymai, poįstatyminiai aktai, standartai ir t. t.
2. Administracinę – organizacijos vadovybės vykdomi bendro pobūdžio veiksmai;
3. Procedūrinę – konkretūs su konkrečiais asmenimis susiję saugumo veiksmai;
4. Programinę techninę – vykdomi konkretūs techninio pobūdžio veiksmai.

Jastiuginas (2011), apibrėždamas informacijos saugumo valdymo koncepciją, išskiria tris dimensijas:

1. Strateginę – apimančią administracinius, organizacinius, valdymo, ekonominius, teisinius, gerųjų praktikų ir pan. aspektus;
2. Žmogiškojo veiksnio – apimančią saugumo kultūros, etinius, kompetencijų, mokymų, psichologinius ir pan. aspektus;
3. Technologinę – apimančią informacinių technologijų, techninių ir programinių priemonių, matematinius, kriptografinius ir pan. aspektus.

Kibernetinio saugumo įstatyme (2014) yra teigiama, kad kibernetinis saugumas priklauso nuo *teisinių, informacijos sklaidos, organizacinių ir techninių priemonių.*

Apibendrinant galima teigti, kad visuomenėje kibernetinis saugumas dažnai suprantamas labai siaurai, t.y. kaip informacijos apsauga, tinklų ir informacinių sistemų saugumas, elektroninės informacijos sauga ir t.t. Lietuvos Respublikos įstatymuose ir kituose teisės aktuose pateikiamos skirtingos kibernetinio saugumo sampratos, kuriose kibernetinis saugumas tapatinamas

su kitomis sąvokomis. Šią problemą išsprendė Kibernetinio saugumo įstatymas (2014), kuriame tiksliai apibrėžiama kibernetinio saugumo samprata. Įstatyme teigiama, kad kibernetinis saugumas priklauso nuo visumos teisinių, informacijos sklaidos, organizacinių bei techninių priemonių.

1.2. Interneto rinkimų kibernetinio saugumo valdymo principai

2004 m. rugsėjo 30 d. Europos Tarybos Ministrų Komitetas per 898 – ąjį deleguotųjų ministrų susitikimą patvirtino valstybių narių Ministrų Komiteto „Rekomendaciją (2004)11 dėl teisinių, organizacinių bei techninių normų, taikytinų balsavimui rinkimuose ir referendumuose elektroniniu būdu“. Komitetas, atsižvelgdamas į santykinai žemą rinkėjų aktyvumą valstybėse narėse, o taip pat pažymėdamas, kad kai kurios valstybės narės jau taiko arba planuoja pradėti naudoti elektroninį balsavimą, skatina valstybes nares atsižvelgti į naujų informacinių ir komunikacinių technologijų plėtrą jų demokratinėje praktikoje. Rekomendacijoje pabrėžiama, kad visi demokratinių rinkimų ir referendumų principai turi būti išlaikomi ir įdiegus elektroninių rinkimų sistemas:

Teisiniai principai:

Visuotinė rinkimų teisė. Šis principas teigia, kad elektroninio balsavimo sistemos grafinė balsavimo sąsaja (angl. interface) privalo būti suprantama ir lengvai naudojama, be papildomų techninių priemonių pritaikoma neįgaliesiems bei privalo būti tik kaip papildoma ir fakultatyvinė balsavimo priemonė, neapribojanti galimybės balsuoti tradiciniais būdais – rinkimų apylinkėje ar paštu (nutarimas „Dėl Balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo“, 2006).

Lygi rinkimų teisė. Šis principas užtikrina, kad nepriklausomai nuo to, kuriuo būdu balsuos rinkėjas, bus įskaitomas tik vienas to paties rinkėjo balsas. Kai vienu metu naudojamas ir elektroninis balsavimas ir įprastas balsavimas, turi būti įskaitytas tik vienas balsas (Recommendations Report to the Legislative Assembly of British Columbia, 2014, p. 4). Rinkimus vykdanti kompetentinga institucija neturėtų pamiršti ir rinkimuose dalyvaujančių tautinių mažumų. Al-Ameen (2013, p. 29) priduria, kad, atsižvelgiant į protingumo kriterijus bei šalyje galiojančius teisės aktus, elektroninė rinkimų sistema rinkėjui galėtų pasiūlyti balsuojant pasirinkti vieną iš kelių kalbų.

Laisva rinkimų teisė. Principas užtikrina laisvą ir nevaržomą balsavimo būdo pasirinkimą (LR Seimo nutarimas „Dėl Balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo“, 2006, 6.2 p.). Balsavimo sistema turi būti sukonstruota taip, kad neskatintų rinkėjo pasirinkti kažkurį konkretų variantą. Elektroninis balsavimas gali būti nutraukiamas bet kuriame žingsnyje iki tol, kol balsas dar nėra patekęs į elektroninę balsadėžę, o

balsavimui įvykus sistema turi užtikrinti, kad balsas nebus pakeistas (Recommendations Report to the Legislative Assembly of British Columbia, 2014, p. 9-15). Balsavimo sistema turėtų užtikrinti rinkėjui galimybę balsuoti „tuščiu biuleteniu“ (Limba ir Agafonov, 2012).

Slapta rinkimų teisė. Elektroninis balsavimas turi būti organizuojamas taip, kad balso konfidencialumas būtų išlaikytas bet kurioje procedūros stadijoje nuo pat rinkėjo identifikavimo momento (Recommendations Report to the Legislative Assembly of British Columbia, 2014, p. 4). Elektroninio balsavimo sistema turi garantuoti, kad į elektroninę balsadėžę padėti balsai ir balsų skaičiavimas būtų anonimiški, o taip pat, kad nebūtų įmanoma nustatyti ryšio tarp balso ir jį atidavusio asmens. Elektroninio balsavimo sistema turi būti organizuota taip, kad balsų skaičius elektroninėje balsadėžėje neleistų nustatyti ryšio tarp balso ir konkretaus rinkėjo (LR Seimo nutarimas „Dėl Balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo“, 2006, 6.4 p.).

Procedūrinės apsaugos priemonės:

- Valstybės narės privalo imtis priemonių, kurios užtikrintų, kad rinkėjai būtų supažindinti su elektroninio balsavimo sistemomis ir žinotų, kaip jomis naudotis. Elektroninės balsavimo sistemos veikimo principas turi būti prieinamas visuomenei. Rinkėjams turi būti suteikta galimybė priprasti ir išbandyti naują elektroninę balsavimo sistemą prieš įregistruojant balsą. Visiems stebėtojams turi būti suteikta galimybė įstatymo nustatytose ribose dalyvauti balsavime internetu, taip pat ir rezultatų nustatymo metu, jį stebėti ir komentuoti (LR Seimo nutarimas „Dėl Balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo“, 2006, 6.5 p.).
- Naujai įdiegtą elektroninio balsavimo sistemą privaloma testuoti. Taip pat būtina testuoti įvykdžius kokius nors pakeitimus jau veikiančioje sistemoje. Sistemą sudarantys komponentai ir jų techninė specifika turi būti žinoma kompetentingoms institucijoms, vykdančioms rinkimus. Elektroninė balsavimo sistema, kai tai yra būtina, privalo turėti galimybę perskaičiuoti balsus bei galimybę vykdyti dalinį ar visišką perbalsavimą (Recommendation Rec(2004)11 of the Committe of Ministers to member states of legal, operational and technical standards for e-voting, 2004, 24-27 p.).
- Valstybės narės privalo užtikrinti elektroninių balsavimo sistemų saugumą ir patikimumą, imtis visų reikalingų priemonių, kad rinkimų metu elektroninio balsavimo sistema veiktų nepertraukiamai bei būtų atspari neautentifikuotai pašalinei intervencijai. Jei interneto rinkimų sistema taptų neprieinama, būtina užtikrinti alternatyvius balsavimo variantus (Recommendations Report to the Legislative Assembly of British Columbia, 2014, p. 5). Rinkimus vykdanti kompetentinga institucija prieš rinkimus privalo patikrinti elektroninių rinkimų sistemos veiklą. Elektroninės rinkimų sistemos techninius darbus gali atlikti tik autentifikuotos komandos, susidedančios mažiausiai iš dviejų žmonių. Komandų sudėtis privalo būti nuolat keičiama. Visi

techniniai darbai, kiek tai yra įmanoma, turi būti atlikti iki rinkimų pradžios. Atidarant elektronines balsadėžes arba vykdant autentifikuotą prisijungimą prie elektroninės balsavimo sistemos, turi dalyvauti balsavimą vykdančios institucijos atstovai bei rinkimų stebėtojai. Elektroninė balsavimo sistema turi užtikrinti balsų patikimumą, konfidencialumą ir prieinamumą. Elektroniniai balsai, perduodami už kontroliuojamų įrenginių ribų, turi būti saugiai užšifruojami. Balsas nuasmeninamas tik pasibaigus rinkimams (Recommendation Rec(2004)11 of the Committe of Ministers to member states of legal, operational and technical standards for e-voting, 2004, 28-35 p.).

Organizaciniai standartai (Recommendation Rec(2004)11 of the Committe of Ministers to member states of legal, operational and technical standards for e-voting, 2004, 36-60 p.):

- Valstybės privalo priimti vidinius teisės aktus, kuriuose būtų aiškiai nustatytos visos elektroninių rinkimų stadijos, pateiktas rinkimų grafikas. Elektroniniai rinkimai gali prasidėti tik paskelbus rinkimų ar referendumo pradžią. Rinkėjai informuojami apie rinkimus lengvai suprantama forma, pateikiant informaciją apie tai, kokių veiksmų turėtų imtis, norint dalyvauti elektroniniuose rinkimuose.
- Turi būti sukurtas bei reguliariai atnaujinamas balsavimo teisę turinčių asmenų registras. Rinkėjas turi teisę susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi bei reikalauti ištaisyti netikslumus (LR asmens duomenų teisinės apsaugos įstatymas, 1996). Priešrinkiminiame laikotarpyje turėtų būti sukurtas elektroninis rinkėjų registras, kuris rinkimų metų būtų naudojamas norint prisijungti prie elektroninės rinkimų sistemos.
- Kandidatai visuomenei galėtų būti pristatomi elektroniniu būdu. Tačiau elektroniniu būdu sugeneruoti kandidatų sąrašai privalo būti prieinami viešai ir kitomis priemonėmis.
- Elektroninio balsavimo sistema turi būti sukurta taip, kad asmeniui nebūtų galimybės atiduoti daugiau nei vieną balsą. Balsavimas internetu gali prasidėti ir/ar baigtis anksčiau nei balsavimas rinkimų apylinkėse, tačiau negali baigtis vėliau. Informacija apie balsavimą nuotoliniu būdu turėtų būti pateikiama skirtingais komunikacijos kanalais. Pristatant rinkėjui balsavimo variantus, privaloma laikytis nešališkumo principo, neproteguojant kažkurio vieno būdo. Elektroninėje rinkimų sistemoje draudžiama rodyti pranešimus, kurie galėtų daryti įtaką rinkėjo pasirinkimui. Elektroninio balsavimo biuletenyje gali būti pateikiama tik su balsavimu susijusi informacija. Rinkėjai turi aiškiai suvokti, kad balsuojant internetu atiduotas balsas yra skaičiuojamas kaip lygiavertis balsas, turintis tokią pat vertę, kaip ir balsas, atiduotas įprastiniu balsavimu rinkimų apylinkėje. Elektroninio balsavimo sistema neturi rinkėjui suteikti galimybės turėti balsavimo turinio įrodymą.
- Tik pasibaigus rinkimams elektroniniai balsai gali būti nuasmeninami, iššifruojami ir skaičiuojami. Elektroninių balsų skaičiavimą privalo stebėti rinkimų stebėtojai, surašomas

elektroninių balsų skaičiavimo protokolas, kuriame nurodomi dalyvaujantys asmenys, balsų skaičiavimo pradžia ir pabaiga. Kilus balsų vientisumo pažeidimams, balsai laikomi negaliojančiais.

- Elektroninio balsavimo sistema turi būti audituojama. Audito išvados pritaikomos kitiems rinkimams ir referendumams.

Techniniai standartai (Recommendation Rec(2004)11 of the Committe of Ministers to member states of legal, operational and technical standards for e-voting, 2004, 61-76 p.):

- Šalys privalo užtikrinti, kad elektroninių rinkimų programinė įranga ir paslaugos būtų viešos ir lengvai prieinamos visiems rinkėjams. Rinkėjai turi būti įtraukiami į elektroninės rinkimų sistemos kūrimą (ypač siekiant išbandyti sistemos naudojimo paprastumą). Būtina skirti dėmesį interneto rinkimų sistemos suderinamumui su jau rinkėjų naudojamomis technologijomis.
- Siekiant užtikrinti įvairių interneto rinkimų techninių komponentų ir paslaugų sąveiką, reikėtų naudoti atvirus standartus. Europos Taryba šalims narėms, rengiančioms elektroninius rinkimus ir referendumus, rekomenduoja naudoti EML (angl. Election Markup Language) standartą.
- Kompetentinga institucija savo interneto svetainėje išplatina oficialų programinės įrangos, naudojamos interneto balsavime, sąrašą. Sudaromos procedūros nenumatytiems atvejams. Asmenys, atsakingi už įrangą, turi taikyti specialias procedūras, siekdami užtikrinti, kad balsavimo laikotarpiu balsavimo įranga ir jos naudojimas atitiktų reikalavimus. Palaikomoji priežiūra nuolat papildoma stebėsimo protokolais. Įvykus incidentams, kurie keltų grėsmę sistemos vientisumui, asmenys, atsakingi už įrangos veikimą, privalo kuo skubiau informuoti kompetentingas rinkimus prižiūrinčius institucijas, kurios, savo ruožtu, turi imtis visų reikalingų veiksmų incidento pasekmėms sumažinti.

Saugumo reikalavimai:

- Reikalavimai išankstinio balsavimo etapuose. Privalo būti užtikrinamas rinkėjų ir kandidatų registrų autentiškumas, prieinamumas ir vientisumas, laikomasi duomenų apsaugos nuostatų. Turi būti stebimos bei tikrinamos rinkėjų registracijos duotuoju laikotarpiu.
- Balsavimo etapo reikalavimai. Išlaikomas ikirinkiminiame etape surinktų duomenų (rinkėjų registrų, kandidatų sąrašų) vientisumas. Būtina užtikrinti, kad rinkėjai gautų tik autentišką interneto rinkimų biuletenį (informuoti apie visas galimybes, patikrinti ryšio su oficialiu interneto rinkimų serveriu bei elektroninio balsavimo biuletenio autentiškumą). Skirti pakankamai priemonių užtikrinti, kad rinkėjų naudojama sistema būtų apsaugota nuo poveikio, galinčio pakeisti (įtakoti) balsavimą. Informacija apie rinkėjo sprendimą ar pasirinkimo pateikimą turi būti sunaikinta iš karto po to, kai įvyko balsavimas. Rinkėjui, balsavusiam internetu, būtina pateikti informaciją, kaip ištrinti, kiek tai yra įmanoma, balsavimui naudotame įrenginyje balsavimo paliktus pėdsakus (žymes). Elektroninių rinkimų sistema pirmiausiai turi užtikrinti, kad balsuotų tik balsavimo teisę

turintys rinkėjai (Recommendations Report to the Legislative Assembly of British Columbia, 2014, p. 5). Užtikrinti patikimą rinkėjo autentifikavimą, leisti užskaityti tik vieną balsą. Elektroninių rinkimų sistema turi užtikrinti, kad rinkėjo pasirinkimas būtų tiksliai rodomas balsavime ir kad tik patvirtintas balsas pasiektų elektroninę balsadėžę. Pasibaigus interneto rinkimų laikotarpiui, teisė rinkėjui prisijungti prie rinkimų sistemos turi būti apribojama.

- Reikalavimai po balsavimo. Turi būti išlaikomas duomenų, perduotų iš rinkiminio etapo, vientisumas, vykdomas duomenų kilmės nustatymas. Skaičiavimo metu kruopščiai suskaičiuojami balsai. Būtina užtikrinti, kad skaičiavimo procesą, esant būtinybei, būtų galima atkurti.

1.3. Kibernetinio saugumo interneto rinkimų problematika

Ramonaitė ir kt. (2008) teigia, kad balsavimo internetu sistema yra ne vien techninis, bet ir socialinis darinys, kurį kuria, palaiko, juo naudojasi žmonės ir grupės. Šios grupės gali klysti arba bandyti išnaudoti balsavimo sistemą savo tikslams. Galimybė balsuoti nuotoliniu būdu suteikia galimybę atakuoti elektroninę rinkimų sistemą iš bet kurio pasaulio krašto, panaudojant ne administracinius, o informacinius išteklius Ramonaitė ir kt. (2008). Sėkmingas išpuolis prieš interneto rinkimus gali sukelti visuomenės nepasitikėjimą elektroninėmis balsavimo sistemomis, sužlugdyti šių sistemų diegimą bei naudojimą vykdant balsavimo internetu procesus. Todėl itin svarbu išanalizuoti visas įmanomas grėsmes, kurios galėtų kilti elektroninėms balsavimo sistemoms, nustatyti galimus šių grėsmių sukėlėjus bei atakų mechanizmus (Limba ir Agafonov, 2012, p. 383).

Prieš pradedant nagrinėti grėsmes, svarbu apžvelgti rizikos atsiradimo veiksnius. 2013 LR Vyriausybė nutarime (Nr. 716) apibrėžiami svarbiausi rizikos veiksniai galintys turėti įtakos elektroninės informacijos saugai:

- subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);
- subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);
- nenugalima jėga (*force majeure*).

1.3.1. Asmeninio rinkėjo įrenginio naudos analizė

Viena iš nesaugiausių interneto rinkimo grandžių yra rinkėjo kompiuteris, mobilusis telefonas ar kitas mobilus įrenginys. Asmeniniai kompiuteriai paprastai yra menkai prižiūrimi ir blogai apsaugoti nuo kenkėjiškų programų atakų. Kalbant apie nuotolinį balsavimą, tie kompiuteriai, kurie yra naudojami užfiksuoti ir perduoti balsus, yra už balsavimus prižiūrinčios institucijos kontrolės ribų, dėl to rinkimus prižiūrintys pareigūnai nelabai gali ką nors padaryti, kad atkreiptų (rinkėjų) dėmesį į šias problemas (Elections BC, 2011, p. 27).

Programišiai nuolat skanuoja milijonus kompiuterių, ieškodami tų, kurie yra lengviausiai pažeidžiami. Jefferson ir kt. (2004) pastebi, kad interneto kavinėse ar viešosiose bibliotekose esantys kompiuteriai yra dar labiau nesaugūs. Juose gali būti įdiegtos šnipinėjimo bei kitos programos. Balsuodami darbo vietoje rinkėjai rizikuoja tuo pačiu. Operacinės sistemos ir naršyklės yra neapsaugotos nuo kenkėjiškų programų, kurias rinkėjai ar kiti asmenys, prieinantys prie to paties įrenginio (kompiuterio), gali parsisiųsti dėl neapdairumo. Į rinkėjo kompiuterį ar mobilųjį įrenginį patekusi kenkėjiška programa be rinkėjo žinios gali pakeisti rinkėjo atiduotą balsą, įrašyti balsavimo faktą. Norėdami patikrinti, kaip rinkimų biuletenis buvo priimtas, rinkėjai neatitikimus galėtų pastebėti, jei turėtų priėjimą prie patikimo įrenginio ar kompiuterio. Ši situacija yra probleminė, nes leidimas rinkėjams patvirtinti jų balsus galėtų parodyti, kaip (už ką) jie balsavo. Jei klastojimas įvyksta prieš išsiunčiant rinkiminį biuletenį, rinkimus prižiūrintys pareigūnai gali neturėti būdų atskirti pranešto neatitikimo nuo vartotojo klaidos (Elections BC, 2011, p.27).

Taip pat negalima atmesti tikimybės, kad pasinaudodamas nuotolinio balsavimo platforma, rinkėjas gali bandyti ja manipuliuoti: įskaityti daugiau nei vieną balsą, turėdamas balsavimo turinio patvirtinimą, jį parduoti. Taip pat bandyti išplėsti savo turimas teises, siekdamas sugadinti balsavimo sistemą, pakeisti rinkimų rezultatą ar pakenkti rinkimų rezultatų patikimumui.

Apibendrinant galima daryti išvadą, kad rinkėjo įrenginio saugumas yra viena iš didžiausių interneto rinkimų problemų. Asmeniniai kompiuteriai paprastai yra menkai prižiūrimi ir blogai apsaugoti nuo kenkėjiškų programų atakų, o interneto kavinėse ar viešosiose bibliotekose esantys kompiuteriai yra dar labiau nesaugūs.

1.3.2. Vidinių rizikų analizė

Štitilis (2011) vidinius sistemos pažeidėjus apibūdina kaip „autorizuotus informacinės sistemos vartotojus (ar buvusius), kurie netikėtai padaro žalą organizacijai“. Limba ir Agafonov (2012) vidinius sistemos vartotojus suskirstė į tris grupes:

- *Elektroninių balsavimo sistemų vartotojų* vykdomi elektroniniai nusikaltimai nėra labai sudėtingi ir kompleksiniai, dažniausiai panaudojamos ne techninės pažeidžiamos vietos (organizacijos politika ir kt.). Pagrindinis tokių nusikaltėlių tikslas dažniausiai būna finansinė nauda, bet ne žalos padarymas organizacijai (Štitilis, 2012). Elektroninėms balsavimo sistemoms pavojus gali kilti ir dėl šių darbuotojų aplaidumo, nekompetencijos.
- *Elektroninių balsavimo sistemų administratoriai*, turėdami išskirtines prieigos teises, gali padaryti labai daug žalos. Jie gali bandyti pasinaudoti elektroninę balsavimo sistemą kuriančiais darbuotojais bei valstybės tarnautojais. Štitilis (2012) pastebi, kad dažniausias šių darbuotojų motyvas – kerštas, rečiau - finansinė nauda. Siekiant apsisaugoti nuo neteisėtų sistemų administratorių veiksmų, būtina vidaus saugumo politikoje numatyti, kad jie negalėtų patys sau suteikti daugiau teisių – tam būtų reikalingas kito administratoriaus leidimas (ACM: Statewide Databases of Registered Voters Report, 2006).
- *Kiti valstybės tarnautojai.* Tai valstybės tarnautojai, kurie tiesiogiai nedalyvauja interneto rinkimuose, tačiau turi priėjimą prie elektroninės balsavimo sistemos. Šie asmenys gali dalyvauti rengiant vidines elektroninių balsavimo sistemų atakas arba net vadovauti joms. Dažniausias šios asmenų grupės motyvas – finansinė nauda (Limba ir Agafonov, 2012).

Siekiant apsisaugoti nuo vidinių sistemos vartotojų, sistema turi užtikrinti, kad joks asmuo, pasinaudodamas savo privilegijomis ar prieigos teisėmis negalėtų pakenkti elektroninių balsų slaptumui. Visi balsai turi būti užšifruojami taip, kad vienas asmuo neturėtų galimybės jų iššifruoti. Rinkimų privatusis raktas, atšifruojantis balsus, galėtų būti „suskaldomas“ ir padalinamas keliems asmenims (administratoriams, auditoriams ir pan.). Tik sudėjus visas rakto dalis būtų įmanoma iššifruoti balsus (Recommendations Report to the Legislative Assembly of British Columbia, 2014, p. 25).

Apibendrinant galima konstatuoti, kad vidinių sistemos vartotojų, administratorių, kitų valstybės tarnautojų neteisėtas įsikišimas į elektronines balsavimo sistemas galėtų sukelti itin didelių problemų. Tačiau šios grupės keliamą riziką galima suvaldyti nustatant saugumo politiką, organizacinius bei techninius reikalavimus.

1.3.3. Išorinių rizikų analizė

Sudarant galimybę balsuoti internetu, rinkėjai gali balsuoti iš bet kurios pasaulio vietos. Tačiau Ramonaitė ir kt. (2008) pastebi, kad tuo pačiu rinkimai tampa pažeidžiami pasaulinėje elektroninėje erdvėje esančių grėsmių, galinčių kilti taipogi iš bet kurios pasaulio vietos. Rinkimus iš išorės puolančios grupės gali sutrikdyti ar net užvaldyti elektroninio balsavimo sistemas. Elektroninius nusikaltimus vykdo įvairūs žmonės: studentai, mėgėjai, teroristai,

nusikalstamų grupuočių nariai. Šių grupių tikslai skiriasi. Dažniausiai jos veikia dėl asmeninių, finansinių ar politinių tikslų (Štitilis, 2011).

- *Programišiai* (angl. Hacker). Šiai grupei būdingas geras kompiuterių programų ir kompiuterių tinklų kūrimo procesų bei jų silpnų vietų išmanymas. Dažniausiai „programišiai“ yra kompiuterių „fanatikai“, ieškantys kompiuterinės įrangos silpnybių vien iš nuobodulio arba norėdami pademonstruoti savo sugebėjimus (Štitilis, 2011). Ramonaitė ir kt. (2008) teigia, kad interneto rinkimai „programišiams” gali tapti nauja pramoga, geras iššūkis.
- *Tipiniai nusikaltėliai.* Kriminalinės grupuotės ir pavieniai nusikaltėliai, siekdami gauti daugiau pinigų kelia savo „verslą“ į elektroninę erdvę (Štitilis, 2012). Interneto rinkimų sistema šią grupę gali sudominti dėl joje esančių privačių rinkėjų duomenų. Prie tipinių nusikaltėlių galima būtų priskirti ir „balsų“ pirkėjus, ieškančius būdų, kaip „saugiai“ nusipirkti internetu balsuojančių rinkėjų balsus.
- *Haktivistai* (angl. hacktivist) yra internetinis judėjimas, tam tikromis veiklomis kompiuteriais ir kompiuterių tinklais siekiantis įvairių tikslų. Ši veikla gali pasiekti panašius tikslus kaip protestai, aktyvizmas ar pilietinis nepaklusnumas. Šių tikslų „haktivistai” dažniausiai siekia gadindami interneto svetaines, vogdami ir viešindami konfidencialią informaciją, vykdydami DDoS (žr. 1.3.4 skyrių) atakas ir pan. (Hampson, 2012). Siekdami tam tikrų tikslų, „haktivistai“ gali bandyti kompromituoti balsavimo internetu balsavimo sistemas, trikdyti jų darbą, viešinti konfidencialią informaciją.
- *Užsienio žvalgybų tarnybos* vykdo valstybių vadovų ir jų įgaliotų pareigūnų užduotis. Be informacijos rinkimo, užsienio žvalgybos tarnybos taip pat siekia paveikti valstybinių institucijų sprendimus bei daryti įtaką viešajai nuomonei (Kas, kaip ir kodėl šnipinėja Lietuvoje, 2014). Interneto rinkimų serveriai gali būti atakuojami siekiant parodyti tam tikros šalies įtaką šiuo būdu bandant pagąsdinti visuomenę. Šiuo atveju, nebūtų bandoma nuslėpti neteisėto įsilaužimo. Kitu atveju, užsienio žvalgybos galėtų bandyti suklastoti interneto rinkimų rezultatus, siekiant išrinkti sau tinkamiausią politinę jėgą ar kandidatą. Tokiu atveju, būtų stengiamasi išlikti nepastebėtais (įtarimą galėtų kelti neįprastai didelis tam tikros politinės jėgos ar kandidato palaikymas). Trečiuoju atveju, užsienio tarnybos galėtų sukompromituoti interneto rinkimus, siekiant sumenkinti pačią valstybę, sumažinti jos žmonių pasitikėjimą (Ramonaitė ir kt., 2008).

Apibendrinant galima daryti išvada, kad didžiausią išorinę grėsmę interneto rinkimams kelia gerai organizuotos bei turinčios didelius finansinius, techninius bei žmogiškuosius pajėgumus užsienio žvalgybų tarnybos. Nemažą riziką kelia ir „haktyvistai“, kurie taip pat neblogai organizuoti, o finansinių išteklių trūkumą kompensuoja bendras tikslas. Tipiniai nusikaltėliai, siekdami naudos, galėtų bandyti pasinaudoti elektroninėmis rinkimų sistemomis, tačiau susidūrę su

gera apsauga, nerizikuotų pagaunami. Taip pat, pasinaudodami savo intelektiniais ištekliais ar siekdami įrodyti savo „vertę“, interneto rinkimus galėtų atakuoti ir programišiai.

1.3.4. Galimi atakų mechanizmai ir metodai

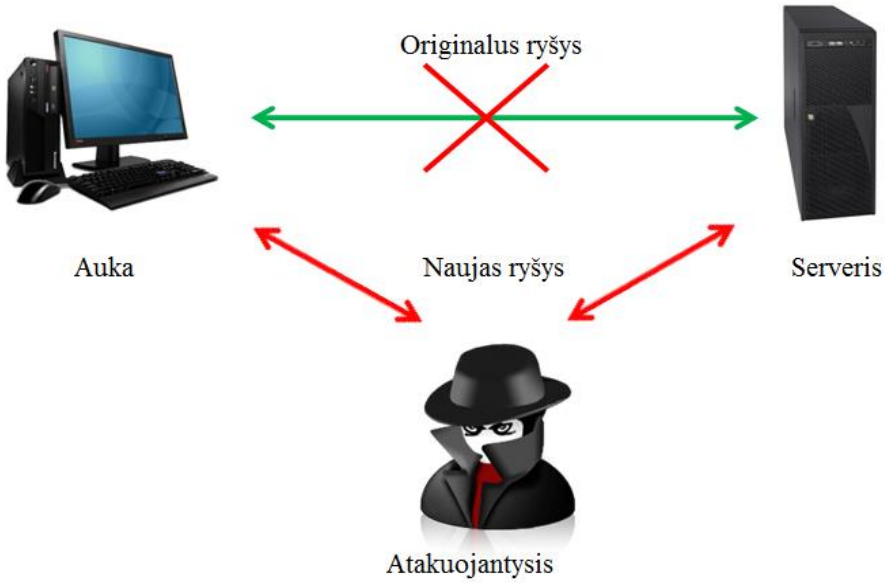
Yra daug būdų, kaip piktavaliai gali bandyti įsilaužti į elektroninio balsavimo sistemas, sutrikdyti jų darbą, stengtis pakenkti balsų vientisumui ar tiesiog sukompromituoti interneto rinkimus. Limba ir Agafonov (2012) teigia, jog *mažai tikėtina, kad individualios vartotojų sistemos (asmeniniai kompiuteriai) bus patrauklus taikinys „atakas“ vykdantiems programišiams (angl. Hacker).* Tačiau kiti autoriai (Jefferson, 2014; Alvarez, 2003; Rubin 2002), kalbėdami apie interneto rinkimų kibernetinę apsaugą, kaip vieną iš pagrindinių atakos vektorių minėjo būtent rinkėją.

Interneto rinkimų atakas galima būtų suskirstyti į tris grupes (Recommendations Report to the Legislative Assembly of British Columbia, 2014, p. 23):

1) Ataka prieš rinkėjo įrenginį galėtų būti paremta žemu asmeninio įrenginio saugumo lygiu bei pasitelkiant socialinę inžineriją. Žemiau pateikiami labiausiai tikėtini puolimo mechanizmai:

- *Žmogus viduryje* (angl. Man in the middle) yra kibernetinėje erdvėje dažnai pasitaikanti ataka, kai užpuolikas sudaro nepriklausomas jungtis su aukomis ir siuntinėja pranešimus tarp jų, priverčiant juos patikėti, kad jie bendrauja tiesiogiai vienas su kitu per privatų ryšį (žr. 2 pav.). Iš tiesų visą pokalbį kontroliuoja užpuolikas. Ši ataka gali pažeisti rinkėjo privatumą ir sužinoti, kaip balsavo rinkėjas. Šią ataką puolantysis taip pat gali panaudoti siekdamas atimti iš rinkėjo jo teisę balsuoti neleisdamas balsui patekti į elektroninį rinkimų serverį. Siekiant išvengti šios atakos, būtina užtikrinti saugų (SSL) ryšį per visą interneto rinkimų procesą. Kaip dar viena galimybė išvengti „žmogus viduryje“ atakos pasekmių yra pasitikrinti ar rinkėjo balsas buvo įskaitytas. Jei po rinkimų paaiškėtų, kad daug rinkėjų buvo prisijungę prie elektroninio rinkimų serverio, bet nebalsavo, galima būtų įtarti „žmogus viduryje“ ataką, kas galėtų priversti pripažinti rinkimus negaliojančiais. Tokia pati ataka gali būti vykdoma ir registracijos rinkimams fazėje (Jefferson, 2004, p.16).
- *Virusai.* Programišiai gali sutrukdyti interneto rinkimus, sukurdami virusą, sunaikinantį kompiuterius. Kaip pavyzdys galėtų būti „Černobylio“ virusas, kuris buvo sukurtas švelniai nusėsti į vartotojo kompiuterį iki tam tikros datos, kai jis „sprogsta“ sunaikindamas kompiuterį, kuriame jis yra. Panašus virusas gali būti sukurtas „susprogti“ prieš pat rinkimus,

sugadindamas asmeninius rinkėjų kompiuterius, kad jie negalėtų balsuoti. Žinoma, rinkėjas gali bandyti susirasti kitą kompiuterį, bet tai apsunkina interneto rinkimus (Alvarez, 2003, p. 83).



Šaltinis: sudaryta autoriaus pagal computerhope.com

2 pav. ***„Žmogus viduryje“*** **ataka**

- *Klastojimo ataka* (angl. Spoofingattack) – tai neautorizuoto priėjimo prie kompiuterio, serverio ar kitų išteklių metodas, kai įsilaužėlis siunčia žinutę su suklastotu adresu ar kitokiu identifikatoriumi. Klastojimo atakos atveju, rinkėjas gali galvoti, kad balsuoja oficialiame interneto rinkimų puslapyje, tačiau taip nėra. Šiuo atveju balsavimo internetu svetainė atrodo ir funkcionuoja kaip oficiali svetainė, tačiau neįskaito rinkėjo balso. Šios atakos dėka puolantysis taip pat gauna ir rinkėjo identifikavimo duomenis, kuriuos vėliau gali panaudoti prisijungiant prie tikrosios interneto rinkimų svetainės. Puolantysis gali pasinaudoti elektroniniu paštu atsiųsdamas rinkėjui nuorodą į netikrą interneto rinkimų puslapį. Taip pat šis metodas gali būti panaudojamas siekiant į rinkėjo kompiuterį įdiegti Trojos arklį (angl. Trojanhorse) (Alvarez, 2003, p. 84).
- *Trojos arklys* (angl. Trojanhorse) – tai destruktyvi ir nesidauginanti programa, kuri dažnai yra užmaskuota kaip atliekanti naudingas funkcijas. Įdiegus šią kenksmingą programą gali būti pažeistas duomenų konfidencialumas ir vientisumas. Net įtarus, kad elektroniniai balsai galėjo būti pažeisti, interneto rinkimai gali būti paskelbti negaliojančiais (Alvarez, 2003, p. 83).
- *Apgaulinga IP taktika* (angl. pharming). Siekiama nukreipti vienos svetainės srautą į kitą. Tai gali būti atliekama pakeitus pagrindinio kompiuterio nustatymus arba pasinaudojus sričių vardų serverių (DNS) eksploatavimo pažeidimais. Pažeisti sričių vardų serveriai vadinami užnuodytais (angl. dnscachepoisoning). Puolantysis klastoja DNS įrašus, kurie nukreipia rinkėją į iš anksto sukurtą netikrą balsavimo internetu svetainę. Rinkėjas, sekdamas nurodymus svetainėje,

atrodančioje kaip oficiali rinkimų internetu svetainė, atiduoda balsą, kuris nėra įskaitomas (Rubin, 2002, p.43).

- *Ataka prieš interneto svetainę.* Pavojinga hibridinė ataka galėtų būti įvykdyta įterpiant kenksmingą kodą į specialiai pasirinktą interneto svetainę. Pavyzdžiui, puolėjas, nusiteikęs prieš vieną iš kandidatų, jo internetinėje svetainėje paspendžia „spąstus“, kad kiekvienas ten apsilankęs rinkėjas netektų galimybės balsuoti internetu. Tokia ataka galėtų atimti iš kandidato kelis šimtus, o gal net ir tūkstančius balsų. Galbūt to pakaktų, kad laimėtų konkurentas (Jefferson, 2004, p. 63).

2) Ataka „balso“ siuntimo metu. Kai rinkėjas patvirtina balso pasirinkimą, balso turinys internetu keliauja į elektroninių rinkimų serverį. Duomenys siunčiami atvirais kanalais trečiųjų asmenų gali būti pakeisti (vientisumo pažeidimas), pavogti ar atskleisti (konfidencialumo pažeidimas). Todėl būtina užtikrinti saugų ryšį tarp rinkėjo ir rinkimų serverio, naudojant saugius protokolus (pvz. SSL/TSL). Siunčiami duomenys turėtų būti užšifruojami saugiu šifru (Recommendations Report to the Legislative Assembly of British Columbia, 2014, p. 24)

3) Ataka prieš elektroninio balsavimo sistemą. Gali pasirodyti, kad gali būti tik techninės atakos, nukreiptos prieš elektronines balsavimo sistemas, tačiau pasitikėjimą šių sistemų veikimu sužlugdyti galima pasitelkus aukščiau minėtas socialinės inžinerijos atakas. Žemiau pateikiami labiausiai tikėtini išpuoliai prieš elektroninio balsavimo sistemas:

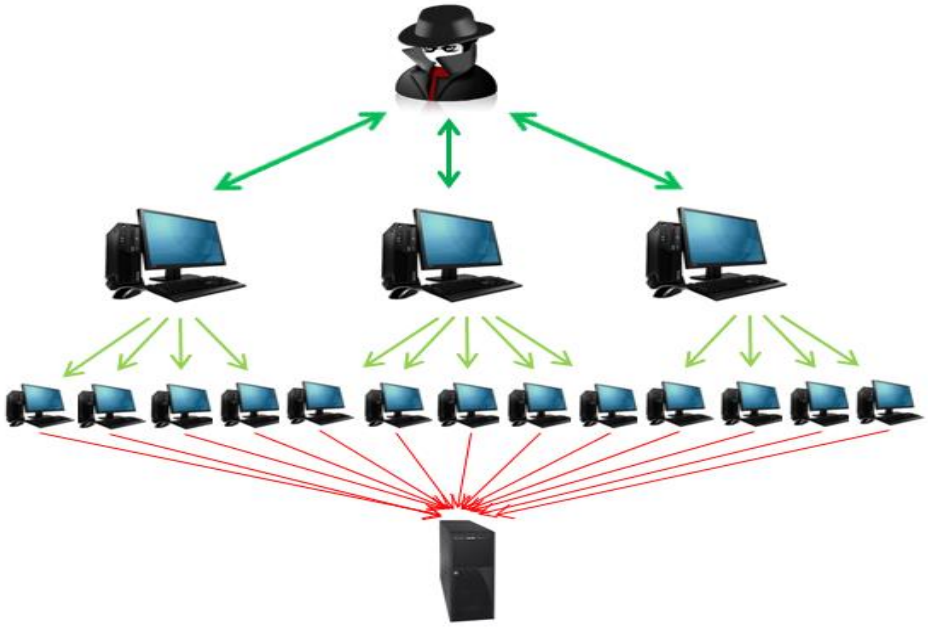
- *Paslaugų apribojimo ataka DoS* (angl. Denial of Service atack) *bei paskirstyto apribojimo ataka DdoS* (angl. Distributed Denial of Service). Šių atakų tikslas yra sukurti tokias sąlygas, kad teisėtiems sistemos naudotojams jos ištekliai taptų neprieinami ar apsunkinamas jų gavimas (žr. 3 pav.). Sugebėjus perkrauti interneto rinkimų tinklo serverį, galima sukelti laikiną arba visišką (per visą balsavimui skirtą laiką) interneto rinkimų nepasiekiamumą, tokiu būdu sukompromituojant rinkimus (Jefferson, 2004, p.19).

- *Nulinės dienos* (angl. Zerodays) ataka remiasi aplikacijų ar operacinės sistemos saugumo trūkumais, kurie dar yra niekam nežinomi, taip pat ir atakuojančiam. Dėl šios priežasties antivirusinės programos, įsibrovimų skanavimo programos, ugniasienės ir t.t. nesugeba aptikti esančios spragos. „Nulinės dienos“ ataka priskiriama prie itin pažengusių ir naudojama kaip žalingų kodų kompleksas (Verbij, 2014, p.24).

- Viena iš *socialinės inžinerijos* atakų, prisidengiant rinkimų kompanija, gali būti tam tikro balsavimo būdo propagavimas (pvz. „Nebalsuoju internetu“). Surengus eilę akcijų, kuriose būtų teigiama, kad toks balsavimo būdas yra nesaugus, galėtų kilti visuomenės nepasitikėjimas interneto rinkimais (Limba ir Agafonov, 2012).

- Kita *socialinės inžinerijos* ataka gali būti įvykdyta dar nesibaigus rinkimams paviešinant netikrus interneto rinkimų rezultatus. Taip pat paviešinti netikrą internetu balsavusių

žmonių sąrašą su jų atiduotais balsais. Panaši situacija nutiko 2015 metais Lietuvoje, kai buvo paviešintas netikras šauktinių į kariuomenę sąrašas (ELTA, 2015).



Šaltinis: sudaryta autoriaus pagal computerhope.com

3 pav. **DDOS ataka**

Apibendrinant atakų mechanizmus ir metodus galima suskirstyti į tris grupes: ataka prieš rinkėjo įrenginį, ataka balso siuntimo metu ir ataka prieš elektroninę balsavimo sistemą. Šiuo metu labiausiai paplitusios socialine inžinerija pagrįstos atakos, išnaudojant vartotojo neišmanymą. Socialinės inžinerijos pagalba, puolėjas gali perimti, pakeisti ar sunaikinti siunčiamą informaciją, nukreipti rinkėją į netikrą svetainę. Prieš elektroninę balsavimo sistemą gali būti panaudota DDoS ataka, apribojant galimybę ja naudotis. Socialinė inžinerija gali būti nukreipta ir prieš pačius interneto rinkimus, paviešinant netikrus rinkimų rezultatus, ar panaudojant socialines akcijas kaip kad „Nebalsavau internetu“.

1.4. Kibernetinio saugumo valdymo įgyvendinimas

1.4.1. Rinkėjo registracijos metodika

Iš pirmo žvilgsnio rinkėjo registracija gali pasirodyti paprasta procedūra - rinkėjas įrašo savo vardą, gyvenamosios vietos adresą bei gimimo datą. Iš tiesų, rinkimus vykdanti kompetentinga institucija turi numatyti kompleksinį šio proceso valdymą. Rinkėjo informacija turi būti tiksliai įrašyta ir saugoma, tuo pačiu užtikrinant sistemos skaidrumą bei privačios informacijos apsaugą nuo neteisėto atskleidimo. Gerai valdoma rinkimų registravimo sistema yra gyvybiškai svarbi siekiant užtikrinti visuomenės pasitikėjimą interneto rinkimais. Kuriant rinkėjų registravimo

sistemą, kibernetinio saugumo užtikrinimas yra viena iš svarbiausių užduočių (Al-Ameen,Talab 2013).

Elektroninis rinkėjų registras turi užtikrinti, kad balsuoti būtų leidžiama tik tam teisę turintiems piliečiams, kuriems rinkimų dieną yra sukakę 18 metų. Rinkimuose nedalyvauja piliečiai, kurie teismo sprendimu yra pripažinti neveiksniais (LR Konstitucijos 34 str.).

1.4.2. Rinkėjo asmens tapatybės nustatymo metodika

Saugus ir patikimas rinkėjo asmens tapatybės nustatymas yra labai svarbi interneto rinkimų proceso dalis. Autentifikacija – tai tikrinimo metodas, kuris leidžia įsitikinti, kad subjektas yra tas, kas iš tikrųjų yra. Subjektas patvirtina savo tapatybę bent vienu iš sekančių būdų (Nathanael ir kt., 2003):

- *Tai, ką tu žinai*. Vartotojui suteiktas slaptažodis arba asmeninis identifikavimo numeris (toliau - PIN);
- *Tai, ką tu turi*. Fiziniai įrenginiai, kurie naudojami tapatybės patvirtinimui. Tai yra lustinės kortelės, kortelės su magnetinėmis juostelėmis, vienkartinio naudojimo slaptažodžių generatoriai ir t.t.
- *Tai, kas tu esi.* Tapatybei nustatyti pateikiami žmogaus fiziniai (biometriniai) požymiai, pvz. pirštų antspaudai, akies tinklainė, ranka rašytas tekstas ir t.t.

Vartotojo autentifikavimas užtikrinamas pasitelkiant trečiąjį asmenį – sertifikavimo paslaugų teikėją, kuris per išduodamą sertifikatą (liudijimą) susieja pasirašančio asmens tapatybę (ja sertifikavimo paslaugų teikėjas įsitikina (LR elektroninio parašo įstatymas, 2000) su parašo formavimo ir tikrinimo duomenimis bei suteikia galimybę bet kam susipažinti su sertifikatu.

Skaitmeninis sertifikatas - tai elektroninis paso ar tapatybės kortelės atitikmuo, kurio pagalba galima įrodyti savo asmens tapatybę arba teisę prieiti prie reikalingos informacijos internete. Skaitmeninių sertifikatų veikimas yra paremtas kodavimo viešuoju raktu technologija, kai naudojama vienas kitą papildančių raktų pora - privatus ir viešasis. Jie gali funkcionuoti tiktai tada, kai naudojami kartu. Viešasis raktas perduodamas asmenims, su kuriais palaikomi kontaktai, o privatų raktą saugo sertifikato savininkas. Bet koks pranešimas, užšifruotas privataus rakto pagalba, gali būti iššifruotas tiktai tos pačios raktų poros viešuoju raktu. Ir atvirkščiai, jeigu siunčiama informacija yra užšifruota viešuoju raktu, ją gali iššifruoti tik tos pačios raktų poros privatus raktas. Naudojant skaitmeninį sertifikatą yra galimybė patikrinti vartotojo teises į konkretų raktą - tai užkerta kelią neteisėtam privataus rakto naudojimui. Skaitmeniniai sertifikatai specialaus šifravimo dėka suteikia absoliutų saugumą ir garantuoja visų elektroninių veiksmų dalyvių tapatybę. Skaitmeninį sertifikatą sudaro ir skiria sertifikavimo paslaugas teikianti organizacija, pasirašanti

savo privačiu raktu. Ji taip pat teikia sertifikatų duomenis parašo naudotojams elektroniniams parašams tikrinti (Skaitmeninio sertifikavimo centras, 2015).

Kasdien milijonai žmonių autentifikavimo priemones naudoja elektroniniu būdu jungdamiesi prie elektroninių bankų sistemų, norėdami gauti elektroninės valdžios paslaugas ir pan. Šiuo metu populiariausi autentifikavimo elektroninėje erdvėje būdai yra elektroninis parašas (mobilusis parašas, asmens tapatybės kortelėje esantis elektroninis parašas, USB laikmenoje esantis elektroninis parašas) bei panaudojant elektroninės bankininkystės sistemą.

1) Elektroninis parašas. Pagal LR elektroninio parašo įstatymą, elektroninis parašas (toliau - e. parašas) tai - duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir (ar) pasirašančiam asmeniui identifikuoti. Saugus e. parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu, elektroniniams duomenims turi tokią pat teisinę galią kaip ir parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme. Elektroninio dokumento, pasirašyto e. parašu, specifikacija yra patvirtinta Lietuvos archyvų departamento direktoriaus įsakymu („Dėl elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos ADOC-V1.0 patvirtinimo“, 2009).

E. parašas yra sudarytas iš dviejų sertifikatų (LR ryšių reguliavimo tarnyba, 2015):

- asmens identifikavimui skirtas skaitmeninis sertifikatas yra elektroninis asmens tapatybės liudijimas. Jis susieja e. parašą su pasirašančiu asmeniu ir patvirtina arba leidžia nustatyti pasirašančio asmens tapatybę.
- pasirašymui skirtas skaitmeninis sertifikatas užtikrina e. parašu pasirašytų duomenų tikrumą ir jų apsaugą nuo klastojimo. Skaitmeninio sertifikato veikimas grindžiamas asimetrinio šifravimo technologija.

Dažniausiai naudojamas e. parašo technologinis sprendimas vadinamas viešojo rakto infrastruktūra (angl. Public Key Infrastructure). Šiuo atveju e. parašas yra sukuriamas pasirašomų duomenų santrauką (angl. Hash) užšifruojant asmens privačiuoju raktu. Kadangi elektroninio parašo kūrimui naudojami pasirašomi duomenys, e. parašas kiekvienu pasirašymo atveju yra unikalus (LR ryšių regiliavimo tarnyba, 2015).

E. parašų saugumas yra paremtas kriptografija – duomenų šifravimu. Tai yra duomenų pavertimas nesuprantamais, kol jie nebus atšifruoti atitinkamu būdu. Populiariausi yra du duomenų šifravimo metodai: simetrinis ir asimetrinis (LR Seimo Parlamentinių tyrimų departamentas, 2002).

Simetriniame šifravimo metode sugeneruojamas vienas šifravimo raktas (labai didelis skaičius). Jį gauna du asmenys - duomenų siuntėjas ir gavėjas. Duomenims užšifruoti prieš siunčiant ir gautiems užšifruotiems duomenims atšifruoti yra naudojamas tas pats raktas. Metodas naudojamas duomenų konfidencialumui užtikrinti, t. y. kai norima apsisaugoti nuo duomenų

atskleidimo tretiesiems asmenims. Simetrinio šifravimo metodo privalumas yra tas, kad duomenų užšifravimas ir atšifravimas vyksta greitai. Trūkumai: raktą žino du arba daugiau asmenų, todėl ginčo atveju sunku įrodyti, kuris asmuo neteisus; raktui perduoti asmenys turi susitikti betarpiškai arba naudoti kitokius saugius perdavimo būdus.

Asimetrinio šifravimo metode generuojami du tarpusavyje susiję raktai. Tikimybė sugeneruoti du kartus tokią pačią šifravimo raktų porą yra labai maža. Jei duomenys užšifruojami vienu raktu, tai juos atšifruoti įmanoma tik kitu tos poros raktu. Žinant tik vieną poros raktą neįmanoma atstatyti kito rakto. Palyginus su simetrinio šifravimo metodu, duomenims užšifruoti ir atšifruoti sugaištama žymiai daugiau laiko (LR Seimo Parlamentinių tyrimų departamentas, 2002).

E. parašas gali būti suteikiamas įvairiomis formomis:

USB laikmena. Norint naudoti kriptografinę USB laikmeną elektroninių dokumentų pasirašymui elektroniniu parašu, reikalinga USB jungtis kompiuteryje. Taip pat kompiuteryje reikia įdiegti USB laikmenos programinę įrangą.

Mobilus parašas. Sudarius e. parašo paslaugos sutartį su mobilias paslaugas teikiančia įmone, suteikiama speciali SIM kortelė su įdiegtu saugiu kriptografiniu moduliu bei skaitmeniniu sertifikatu, apsaugotu PIN kodu. Jis naudojamas prisijungti prie sistemų internete, pavyzdžiui, elektroninio banko ir leidžia elektroniniu būdu nustatyti pasirašančio asmens tapatybę. Šiuo metu Lietuvoje mobiliojo parašo paslaugas teikia didieji mobiliojo ryšio operatoriai („Omnitel“, „Bitė“, „Tele2) bei šalies bankai („Swedbank“, „SEB“, „Dnb“ ir kt.).

Asmens tapatybės kortelė. Nuo 2009 m. pradžios Lietuvos Respublikos piliečiams yra išduodamos lustinės asmens tapatybės kortelės, kurios be savo įprastinės paskirties gali būti naudojamos kaip e. parašo kūrimo priemonė. E. parašai, sukurti naudojant asmens tapatybės korteles, yra tvirtinami Gyventojų registro tarnybos sudarytais skaitmeniniais sertifikatais – specialaus formato elektroniniais dokumentais, patvirtinančiais pasirašančio asmens tapatybę ir leidžiančiais patikrinti pasirašančio asmens e. parašą. Gyventojų registro tarnybos sudaromų sertifikatų autentiškumas yra užtikrinamas šiuose sertifikatuose esančiu vienos iš Gyventojų registro tarnybos administruojamų sertifikavimo tarnybų elektroniniu parašu (LR vidaus reikalų ministerija, 2015).

2) Elektroninės bankininkystės sistema – paslaugos, kurias bankai teikia pasinaudodami šiuolaikinėmis elektroninio ryšio priemonėmis. Šių paslaugų dėka galima identifikuoti klientą ir atlikti kliento norimą pavedimą ar valią. Elektroninė bankininkystė yra apibrėžiama kaip banko kliento sąskaitų tvarkymo sistema, kuri leidžia gauti informaciją bei atlikti operacijas iš bet kurios pasaulio vietos neatvykstant į banką. Prisijungti galima panaudojant kompiuterį su įdiegta specialia įranga bei interneto ryšiu arba mobiliuoju telefonu (Laurinaitis, Andrulytė, 2010).

Balsavimo internetu rinkimuose ir referendumuose koncepcijoje (2006) pradinėje interneto rinkimų diegimo stadijoje rekomenduojama pasirinkti Lietuvoje gerai išvystytą elektroninės bankininkystės sistemą. Tačiau saugumo uždavinių sprendimas viename iš pačių svarbiausių valstybės politinių įvykių privačių bankų išteklių pagalba yra problemiškas. Sunku užtikrinti, kad bankams, kurie yra privatūs subjektai, nebūtų prieinama konfidenciali su rinkimais susijusi informacija. Pačioje Balsavimo internetu rinkimuose ir referendumuose koncepcijoje (2006) pripažįstama, jog problemų gali kilti dėl banko darbuotojų nesąžiningumo: „*bankas, žinodamas ar spėdamas, kad konkretus rinkėjas nebalsuoja ar yra išvykęs į užsienį, gali jungtis prie VRK serverio apsimesdamas rinkėju*“. Be to, toks svarbus valstybės procesas kaip rinkimai taptų priklausomas nuo sėkmingo privačių bankų gyvavimo. Dauguma Lietuvos gyventojų, prisijungdami prie elektroninės bankininkystės sistemos, naudoja popierines arba plastikines kodų korteles, kurios šiuo metu yra laikomos nesaugiomis. Lietuvos bankas 2015 m. spalio 30 d. nutarimu patvirtino pereinamąjį 3 mėn. laikotarpį iki 2016 m. balandžio 1 d., kuomet bankai turės papildyti slaptažodžių kodų korteles saugesnėmis elektroninės atpažinties priemonėmis arba jas pakeisti kitais, saugesniais sprendimais. Šiuo metu patys bankai ieško sprendimų, kuriais klientui būtų lengva ir saugu naudotis, jungiantis prie elektroninės bankininkystės.

1.4.3. Balsavimas ir balsų įskaitymas

Kaip ir tradiciniuose rinkimuose apylinkėje ar balsavime paštu, interneto rinkimuose turi būti užtikrinamas *balso slaptumas*. Balsuojant internetu negalima užtikrinti, kad rinkėjas balsavo tik savo valia (nebuvo prievartos), taip pat atsiranda pavojus „balsų pirkimams/pardavimams“. Siekiant išvengti pašalinių asmenų įsikišimo balsavimo procese, rinkėjui internetu leidžiama balsuoti „n“ kartų. Tokiu būdu panaikinama „balso pirkimo“ prasmė, nes rinkėjas po kiek laiko gali perbalsuoti ir pakeisti sprendimą. Tačiau techniškai išpildyti šią sąlygą nėra taip paprasta. Užkertant galimybę balsą susieti su rinkėju, tuo pačiu yra būtina užtikrinti, kad balsas nebūtų nuasmenintas. Užkoduotas balsas turi būti saugiai sujungtas su rinkėju.

Kyla grėsmė, kad tam tikros rinkėjų grupės (pvz. benamiai, nepasiturintys asmenys ir t.t.) gali suteikti savo prisijungimo informaciją tretiesiems asmenims. Šiuo atveju galima būtų riboti masinį balsavimą iš vieno fizinio adreso (angl. Mac) (Jefferson, 2004).

Itin svarbu, kad vienas rinkėjas neturėtų galimybės atiduoti daugiau kaip vieną „balsą“. Kiekvieną kartą balsuojant, sistema tikrina rinkėjo tapatumą, teisę balsuoti bei ar šis rinkėjas jau balsavo. Rinkėjui internetu balsuojant kelis kartus, įskaitomas tik paskutinis balsas. Sistema taip pat turi užtikrinti, kad rinkėjui balsavus rinkimų apylinkėje, internetu atiduotas balsas būtų automatiškai panaikinamas.

Galimybė patikrinti yra vienas iš svarbiausių saugumo garantų vykdant interneto rinkimus prieš įvairias programinės įrangos klaidas, saugumo pažeidžiamumus bei kibernetinius nusikaltėlius, kurie dėl įvairių priežasčių gali bandyti pažeisti elektronines sistemas. Ši galimybė yra numatyta LR rinkimų įstatymų pakeitimų įstatymų projektuose (Nr. XIIP-1835/1839) Vykdant interneto rinkimus būtina suteikti galimybę vartotojui pasitikrinti ar jo balsas įskaitytas teisingai. Pabrėžtina, kad balso patikrinimas negali suteikti rinkėjui balsavimo turinio įrodymo. Priklausomai nuo interneto rinkimų sistemos, patikrinus gali būti patvirtinta, kad (U.S.VOTE foundation, 2015, p. 19):

- rinkėjo balsas įtrauktas į rinkimų rezultatus;
- sistema balso turinį įrašė teisingai;
- rinkėjų, kurie balsavo už pateiktą kandidatą, skaičius yra tiksliai apskaičiuotas (turi būti įrodoma neatskleidžiant balsavimo paslapties).

1.4.4. Balsų tvarkymo ir skaičiavimo specifika

Šios interneto rinkimų fazės metu elektroninė rinkimų sistema išsaugoja rinkėjų balsus. Pasibaigus balsavimui internetu, balsas dar negali būti atskiriamas nuo rinkėjo – asmuo dar turi teisę balsuoti rinkimų apylinkėje (tuomet internetu išreikštas balsas anuliuojamas). Elektroninė rinkimų sistema privalo užtikrinti ne tik balso slaptumą, bet ir užkirsti galimybę susieti rinkėją su jo balsu. Visi balsai turi būti teisingai įskaityti. Sistema turi drausti bandymus nukopijuoti, pakeisti ar ištrinti rinkėjų balsus, pranešti apie bet kokius bandymus atlikti šiuos veiksmus (Al-Ameen,Talab 2013, p. 29).

1.4.5. Rinkimų audito problematika

Saugumo įrašų kaupimas ir analizė neleidžia piktavaliams likti nepastebėtiems. Tačiau, net ir pastebėjus saugumo pažeidimus, labai sudėtinga nustatyti, kaip įsibrovėliai pateko į sistemą, kaip veikė žalingas kodas, kas buvo padaryta konkrečiose sistemose. Be atliekamų audito tyrimų galima apskritai nepastebėti sėkmingos atakos (Center for Internet Security, 2015).

Rinkimų auditas tikrina, ar tam teisę turintys rinkėjai galėjo balsuoti, ar jų balsai buvo įskaityti į galutinį rezultatą. Auditą atliekanti komisija turi aktyviai pranešinėti visuomenei apie kylančias problemas, sprendžiamus klausimus. Pranešti balsavusių asmenų skaičių, negaliojančių biuletenių skaičių, taip pat skelbti apie bandymus sutrikdyti elektroninių rinkimų sistemas, sistemos veikimo sutrikimus. Auditas privalo įsitikinti, kad visi rinkėjų balsai buvo įskaityti ir teisėti. Iškilus abejonėms dėl balsų teisėtumo, turi būti pranešta, koks balsų skaičius yra nepatikimas. Draudžiama

atskleisti rinkėjo balso slaptumą net jei tai yra vienintelis būdas ištirti nusikalstamą veiką prieš interneto balsavimo sistemą (U.S.VOTE foundation, 2015, p.35).

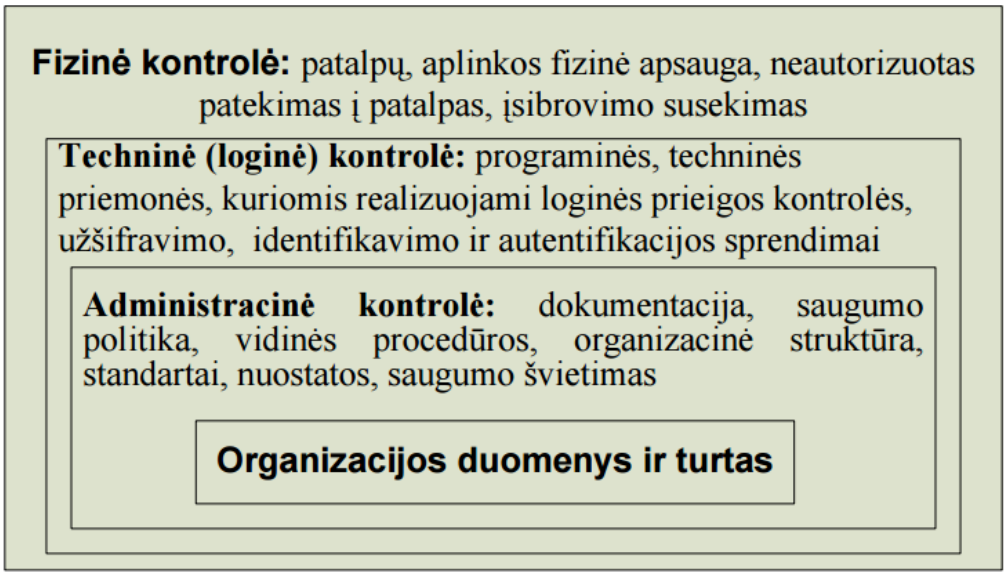
Ramonaitė ir kt. (2008) teigia, kad interneto rinkimų sistemą galima laikyti saugia tik tuo atveju, jei yra galimybė kompetentingai ją patikrinti. Elektroninio balsavimo galimybių studijoje (2008) pateikiamos su elektroninių rinkimų sistemų auditu susijusios problemos:

- Tinkamai elektroninio balsavimo programos pirminio teksto (angl. Sourcecode) analizei reikalingos specialiosios žinios;
- Saugumo sumetimais sistemos tiekėjas gali iš vis nepateikti programos pirminio teksto analizei;
- Net jei programa yra pakankamai ištyrinėta, nėra garantijų, kad rinkimuose bus naudojama ta pati. Kyla grėsmė, kad po programos klaidų pataisymų ar programos papildymo, dėl laiko ir lėšų trūkumo, gali būti neatliekami testavimo darbai;
- Rinkimų auditui lieka neprieinamas rinkėjo įrenginys. Siekiant daryti įtaką rinkėjo pasirinkimui, nebūtina įsilaužti į elektroninę balsavimo sistemą. Rinkėjo naudojama operacinė sistema ir naršyklė gali būti nepakankamai saugios balsavimo procedūrai atlikti ;
- Penkta, tiek programinė, tiek operacinė kompiuterių įranga, taip pat ir potencialių įsilaužėlių įranga, sparčiai evoliucionuoja – priešingai nei tradiciniais administraciniais ištekliais remiamai rinkimų organizacijai, elektroninės balsavimo sistemos techninės-organizacinės bazės patikimumui užtikrinti reikėtų tęstinių pastangų.

Problemiška yra ir tai, kad interneto rinkimų stebėtojams, norint atlikti savo darbą, turi būti suteikta galimybė prisijungti prie interneto rinkimų serverių, operacinių sistemų ir juose esančių programų. Tačiau tai prieštarauja rinkimų stebėtojų principui nesikišti į rinkimų vykdymą.

1.4.6. Kibernetinio saugumo valdymo priemonės

Urmanavičiūtė (2010), siekiant apsaugoti informacijos duomenis ir turtą, išskyrė fizinę, techninę (loginę) bei administracinę kontrolę (žr. 4 pav.). LR kibernetinio saugumo įstatyme (2014) kibernetinis saugumas apibrėžiamas kaip „*visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių“*, kurios yra skirtos išvengti, aptikti, analizuoti bei reaguoti į kibernetinius incidentus. Žemiau pateikiamos kibernetinio saugumo valdymo priemonės:



Šaltinis: Urmanavičiūtė (2010)

4 pav. **Organizacijos duomenų ir turto administracinė, techninė ir fizinė apsauga**

Teisinės priemonės. Pagrindiniai kibernetinį saugumo užtikrinimo ir valdymo principus reglamentuojantys LR tesės aktai yra Kibernetinio saugumo įstatymas (2014), LR Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo“, Lietuvos policijos generalinio komisaro 2015 m. vasario 2. įsakymas Nr. 5-V-101„Dėl informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetinių incidentų tyrimo tvarkos aprašo patvirtinimo“. Šie teisės aktai plačiau nagrinėjami 2.3 poskyryje. Pagal LR Vyriausybės patvirtintą bendrųjų elektroninės informacijos saugos reikalavimų aprašą, saugos dokumentų turinio gairių aprašą ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašą, kiekvienas informacinės sistemos valdytojas privalo būti patvirtinęs bei su Vidaus reikalų ministerija suderinęs šiuos saugos dokumentus:

- Saugos nuostatus;
- Saugaus elektroninės informacijos tvarkymo taisykles;
- Informacinės sistemos veiklos tęstinumo planą;
- Informacinės sistemos naudotojų administravimo taisykles.

Informacijos sklaidos priemonės. Vienas iš svarbiausių organizacijos valdymo elementų yra gebėjimas taisyklingai perduoti informaciją bei suvokti gautos informacijos vertę, jos reikšmę organizacijos veiklos efektyvumui (Virbalienė, 2011).

Teisės aktai nenustato sąrašo, pagal kurį galima būtų nuspręsti, ar informacija yra įmonės ar įstaigos paslaptis. Skirtingiems ūkio subjektams gali būti svarbi skirtinga informacija. Todėl organizacijos turi savo vidiniais dokumentais nusistatyti konfidencialios informacijos sąrašus, jos saugojimo būdus bei tvarką. Pagal LR valstybės ir tarnybos paslapčių įstatymą (1999), įslaptinta informacija žymima pagal svarbą, galimos žalos, kurią patirtų valstybė, jos institucijos ar asmenys, jeigu ši informacija būtų prarasta arba atskleista neturintiems teisės ją sužinoti asmenims. Įstatyme taip pat pateikiami principai, kurių būtina laikytis dirbant bei susipažįstant su įslaptinta informacija:

- Informacija turi būti įslaptinama ir išslaptinama vadovaujantis teisėtumo, pagrįstumo ir savalaikiškumo principais;
- Nustatoma informacijos slaptumo žyma ir tokiai informacijai suteikiamas apsaugos lygis turi būti proporcingas įslaptinamos informacijos svarbai bei žalos, kuri atsirastų tokią informaciją neteisėtai atskleidus ar praradus, dydžiui;
- Įslaptinta informacija turi būti patikima griežtai laikantis principo „Būtina žinoti“. Principas „Būtina žinoti“ reiškia, kad įslaptinta informacija gali būti patikėta tik atitinkamus leidimus dirbti ar susipažinti su įslaptinta informacija turintiems asmenims, kuriems vykdant tarnybines pareigas reikalinga susipažinti su įslaptinta informacija. Asmeniui gali būti patikėta tokios apimties įslaptinta informacija, kokios reikia jo pareigoms atlikti.

Organizacinės priemonės. Apsaugos priemonės bus nieko vertos, jei prie informacijos apsaugos neprisidės visi organizacijos darbuotojai. Personalo apsauga apima platų organizacinių priemonių ratą. Informacijos apsaugos mokymai didina darbuotojų suvokimą, ką ir nuo ko reikia saugoti, kokios yra grėsmės ir pažeidžiamumai (LR vidaus reikalų ministerija, 2005). Center for Internet Security (2015) nuolat pabrėžia, kad žmogiškasis faktorius turi reikšmingos įtakos visoms sistemos dizaino, taikymo, veikimo, naudojimo ir stebėjimo funkcijoms. Association for Computing Machinery (2006) teigia, kad autorizuoti sistemos vartotojai turi išmanyti, kaip apsaugoti slaptažodžius, apsiginti nuo socialinės inžinerijos išpuolių ir pan. Todėl labai svarbu įvertinti, kokių gebėjimų ir žinių trūksta konkrečiai grupei bei sudaryti mokymų planą, kuris turi būti nuolat papildomas įtraukiant naujausias grėsmes (Center for Internet Security, 2015). Vidaus reikalų ministerijos parengtose rekomendacijose dėl informacijos apsaugos (2005) kaip personalo apsaugos priemonės minimi pareigų ir atsakomybės ribų nustatymas. Taip pat vidinių organizacijos tvarkų, kurios reglamentuoja organizacijos informacijos apsaugos politiką, procedūras ir instrukcijas, nustatymas. Procedūrose apibrėžiama, kaip saugiai naudotis sistemomis arba elgtis tam tikrose situacijose: kurti bei keisti slaptažodžius ir pan., patekti į įstaigą ne darbo valandomis. 2013 m. LR Vyriausybės nutarime (Nr. 716) taip pat atkreipiamas dėmesys į saugų elektroninės informacijos

keitimą, atnaujinimą, įvedimą, naikinimą; programinės ir techninės įrangos keitimą bei atnaujinimą; informacinės sistemos pokyčių valdymą.

Association for Computing Machinery (2006) teigia, kad įgyvendinant interneto rinkimus būtina užtikrinti, kad administratoriaus teisės būtų griežtai kontroliuojamos ir suteikiamos tik tiems darbuotojams, kuriems yra būtinos darbui atlikti. Administratoriaus teises turintys vartotojai negali patys sau suteikti daugiau teisių – tam reikalingas kito administratoriaus leidimas. Taisyklėse gali būti numatyta išimtis, kad kritiniais atvejais yra nebūtinas kito administratoriaus leidimas. Sudaryta bendra struktūra: numatytos pareigos ir paskirstytos atsakomybės. Center for Internet Security (2015) pastebi, kad piktavaliai gali aptikti ir išnaudoti anksčiau buvusias teisėtas naudotojų (buvusių darbuotojų, testuotojų, pratybų dalyvių) paskyras, kurios nebuvo deaktyvuotos ir išlaikė joms priklausiusias teises. Todėl turi būti reguliariai stebimos visos sistemos paskyros. Būtina užtikrinti, kad visos paskyros turėtų baigtumo laikotarpį, taip pat užtikrinti paskyrų blokavimą, susietą su darbo sutarties pabaiga. Reagavimas į incidentus ir jų valdymo planai privalo būti parengti iš anksto. Incidento metu yra per vėlu kurti reikiamas procedūras, duomenų surinkimą, įrašų kaupimą ir kitus procesus, kurie padėtų susigaudyti situacijoje. Chaotiškas reagavimas gali padėti puolėjui pagrobti daugiau duomenų, padaryti daugiau žalos, todėl būtina paruošti reagavimo į incidentus procedūras. Būtina nustatyti incidentų valdymo fazes, numatyti vadovus, kurie, prisiimdami atsakomybę, priiminės sprendimus.

Techninės apsaugos priemonės. Techninės apsaugos priemonės yra skirstomos į aparatūros (įeigos kontrolės sistemos yra kortelės, ugniasienės ir vaizdo kameros), programines (saugo kompiuterių sistemas nuo kenksmingų programų ir virusų, užtikrina prieigą prie svarbių duomenų tik autorizuotiems sistemos vartotojams bei pašalina programinės įrangos spragas) ir mechanines (užraktai, durys, grotos ir t.t.) (LR vidaus reikalų ministerija, 2005).

Siekiant apsaugoti tinklo resursus nuo išorės veiksnių bei užtikrinti vartotojų prieigos prie resursų kontrolę, yra sukurta įvairių sprendimų. Populiariausi iš jų:

802.1x standartas. Tinklo prieiga yra kontroliuojama nustatant vartotojų tapatumą pagal 802.1x standartą, kuris suteikia prieigos kontrolę ir galimybę tikrinti vartotojų profailus RADIUS serveryje ir suteikti jiems priėjimo teisę iš įvairių vietų tinkle (Urbanavičiūtė, 2010).

DMZ. Demilitarizuota zona (angl. demilitarized zone) yra prieigos kontrolės valdymo priemonė, kuri leidžia užtikrinti viešųjų organizacijos serverių apsaugą. DMZ zonoje montuojami serveriai su viešomis paslaugomis arba vadinamieji tarpiniai (angl. proxy) serveriai, kurie atlieka tarpininko funkciją bei nustato dviejų žingsnių sujungimus tarp nutolusių vartotojų ir įmonės serverių, prie kurių jungiasi išoriniai vartotojai, ir taip pat padeda apsaugoti serverius nuo atakų iš išorės (Urbanavičiūtė, 2010). Center for Internet Security (2015) pabrėžia, kad, siekiant padidinti

saugumą, DMZ sistemoms reikia leisti bendrauti su vidiniu tinklu tik per aplikacijų proxy serverius ar aplikacijų ugniasienes.

PKI. Viešųjų raktų infrastruktūra (ang. Public Key Infrastructure) yra techninės, programinės įrangos, žmonių ir procedūrų visuma, kuri naudojama saugoti, kurti, valdyti, suteikti, atnaujinti, panaikinti, atnaujinti sertifikatus, pasinaudojus viešojo rakto kriptografija. Viešųjų raktų infrastruktūra gali palengvinti bei pagreitinti informacijos apsikeitimą, keičiant įprastinius popieriniais dokumentais paremtus būdus (Repečka, 2012).

IDS įsibrovimo susekimo sistema (angl. intrusion detection system) yra įrenginiai, kurie stebi srautą ir aptinka atakos mechanizmą primenantį srautą. Jie gali veikti parašų, elgsenos analizės ir kitų mechanizmų pagrindu. IDS kontroliuoja bei analizuoja vartotojų bei sistemos veiklą, tikrina sistemos konfigūraciją ir pažeidžiamumus bei vertina sistemos ir duomenų vientisumą (SANS Institute InfoSec Reading Room, 2001).

WAF tinklo aplikacijų ugniasienė (angl. web application firewall) – programinė įranga, tikrinanti duomenų srautą, skirtą tinklapio pagrindu veikiančiai programinei aplikacijai. WAF sprendimas padeda blokuoti tinklo serverio pažeidžiamumus, apsaugo jautrią informaciją nuo neteisėto atskleidimo bei kontroliuoja prieigą prie jų (Center for Internet Security, 2015).

Užtikrinant saugią komunikaciją dažniausiai naudojami SSL ir TSL protokolai (Repečka, 2007):

SSL protokolas naudoja simetrinį ir asimetrinį šifravimo metodus. Seanso (angl. *session*) tarp kliento ir tarnybinės stoties pradžioje nustatomas simetrinis seanso raktas, kurį sukuria kliento naršyklė ir užšifruoja tarnybinės stoties viešuoju raktu. Kadangi šiame žingsnyje realizuotas asimetrinis šifravimas, tik tarnybinė stotis gali iššifruoti seanso raktą savo privačiu raktu. Tiek klientas, tiek tarnybinė stotis jau turi identišką simetrinį seanso raktą ir gali pradėti tarpusavyje saugiai keistis duomenimis.

TSL atliekamas tik tarnybinės stoties atpažinimas, o klientas lieka neatpažintas, tačiau šiuo atveju būtent klientui svarbu teisingai žinoti su kuo jis komunikuoja, t.y. identifikuoti tarnybinę stotį. Egzistuoja ir aukštesnio lygio schema, vadinama abipuse autentifikacija (angl. mutual authentication), tačiau ji reikalauja išvystytos viešojo rakto infrastruktūros. TSL veikimas pagrįstas trimis etapais:

- tiesioginis sujungimas algoritmo sutarimui;
- viešojo rakto persiuntimas ir sertifikato galiojimo patikrinimas;
- šifravimas simetriniu raktu.

Apibendrinant galima daryti išvadą, kad siekiant išvengti, aptikti, analizuoti bei reaguoti į kibernetinius incidentus, organizacijos apsaugai būtina taikyti visumą teisinių, informacijos sklaidos, organizacinių ir techninių priemonių. Vadovaujantis LR teisės aktais būtina

užtikrinti saugią komunikaciją ir informacijos sklaidą bei priimti dokumentus reglamentuojančius organizacijos informacijos apsaugos politiką, procedūras ir instrukcijas. Siekiant apsaugoti tinklo resursus nuo išorės veiksnių ir užtikrinti vartotojų prieigos prie resursų kontrolę bei užtikrinti saugią komunikaciją, parinkti ir saugiai sukonfigūruoti technines apsaugos priemones.

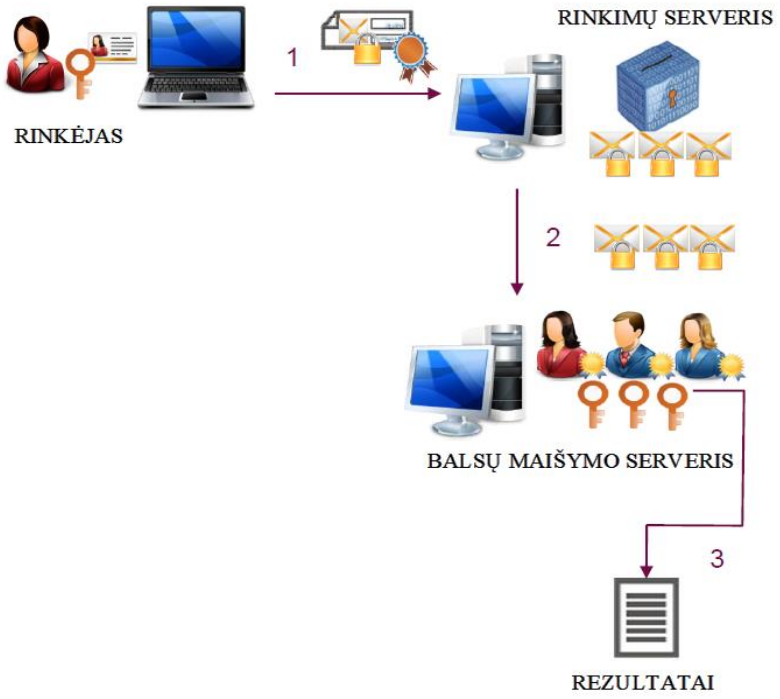
2. KIBERNETINIO SAUGUMO VALDYMO ĮGYVENDINIMO PASAULINĖS PATIRTIES ANALIZĖ

2.1. Interneto rinkimų modeliai

2.1.1. „Scytl“ interneto rinkimų modelis

„Scytl“ yra viena didžiausių pasaulio organizacijų, siūlančių įvairias rinkimų sistemas (įprastinio balsavimo, balsavimo telefonu, panaudojant elektronines balsavimo mašinas bei balsavimą internetu). Organizacija teigia, kad jos siūlomi produktai užima daugiau kaip 87 proc. viso pasaulio rinkos, o balsavimo internetu sistema yra itin patikima. „Scytl“ nuolat ieško naujų technologijų bei technikų, kurios užtikrintų dar didesnį elektroninių balsų saugumą. Tokios technologijos kaip viešojo rakto infrastruktūra, kriptografija, buvo patvirtintos dvylikos šalių ir sėkmingai naudojamos. „Scytl“ balsavimo internetu sistema buvo tirta nepriklausomų ekspertų, kurie nustatė, kad naudojama technologija yra tiksli ir patikima (Shah, 2013).

Pagal „Scytl“ balsavimo modelį (žr. 5 pav.) užšifruoti balsai pasirašomi rinkėjo elektroniniu sertifikatu ir siunčiami į elektroninį interneto rinkimų serverį. Rinkimų serveris, patikrinęs rinkėjo tinkamumą, įrašo rinkėjo balsą. Pasibaigus rinkimams, užšifruoti balsai perkeliami į maišymo serverį. Balsai yra sumaišomi ir iššifruojami. Suskaičiavus balsus gaunamas rezultatas.



Šaltinis: sudaryta autoriaus pagal Remote voting technologies, 2015

5 pav. **„Scytl“ principinė balsavimo internetu schema**

Rinkėjo registracijos metodika. „Scytl“ balsavimo internetu registracijos metodikos požymiai (Scytl, 2015):

- lengvai prieinama bei suprantama vartotojui (rinkėjui);
- leidžia rinkimus prižiūrinčioms institucijoms efektyviai tvarkyti rinkėjų registracijos procesus;
- palaiko daugiapakopę registraciją (ne tik balsavimo internetu sistemas, bet ir PKI, barkodus ar biometrinių duomenų fiksavimą);
- lengvai pritaikoma ir lanksti;
- taiko dvigubo prisijungimo metodą (sistema gali būti nustatyta taip, kad vidinių darbuotojų reikalautų dvigubo prisijungimo vietoje paprasto (specifiniams veiksmams atlikti būtų reikalaujama dviejų skirtingų žmonių).

Rinkėjų registracijos sistemai pateikiami asmeniniai ir konfidencialūs duomenys, saugumo sumetimais, paskirstomi skirtinguose serveriuose. Sistema iš kiekvieno, bandančio gauti šiuos duomenis, reikalauja autentiškumo patvirtinimo. Šios procedūros užtikrina, kad asmeninius duomenis gautų tik įgaliotas vartotojas.

Rinkėjo asmens tapatybės nustatymo metodika. „Scytl“, prisiderindama prie skirtingų šalių, gali įdiegti skirtingus rinkėjo asmenybės nustatymo mechanizmus.

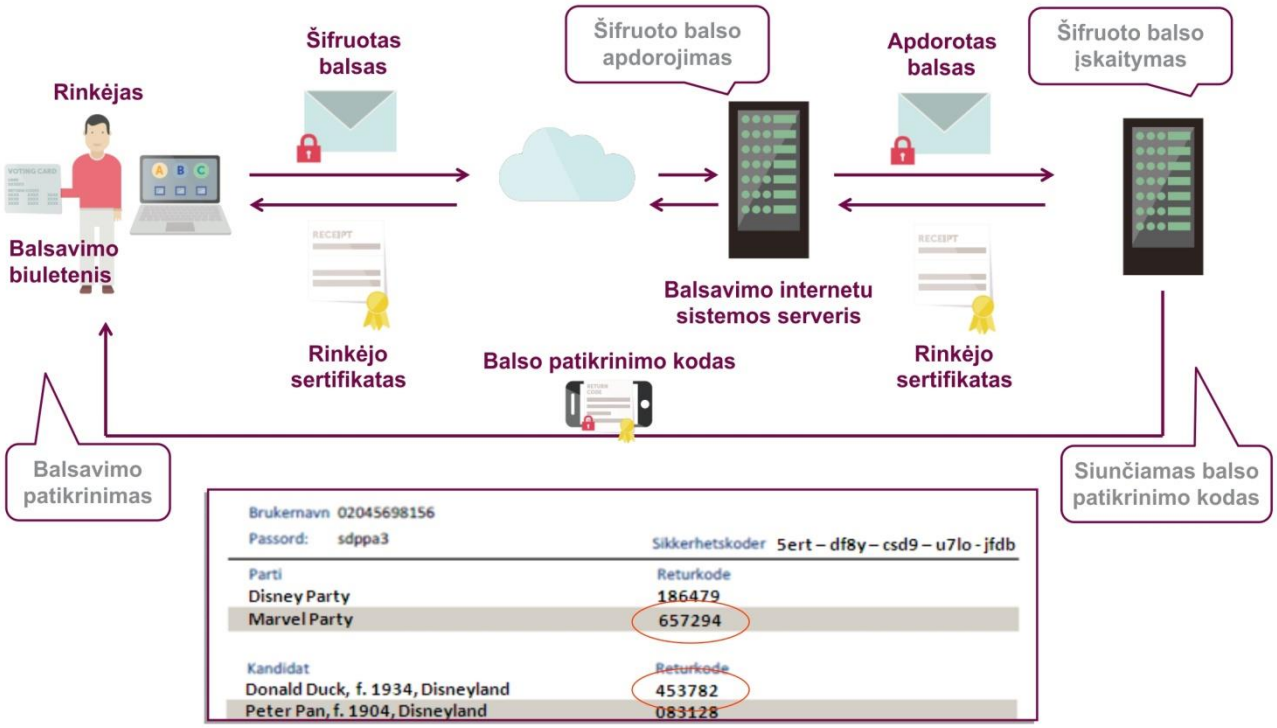
Balsavimo ir balso įskaitymo mechanizmas ir taikoma metodika. „Scytl“ naudojamas kriptografijos metodas lengvai suderinamas su Google, Android, Blackberry ir Apple IOS operacinėmis sistemomis bei užtikrina tą patį saugumo lygį, kaip ir naudojantis asmeniniu kompiuteriu. „Scytl“ biuletenį užšifruoja dar prieš tai, kai jis yra pasirašomas ir išsiunčiamas į elektronines rinkimų sistemas.

Rinkėjams, balsavusiems internetu, išduodamas balsavimo patvirtinimo kvitas su unikaliu numeriu (žr. 6 pav.), kuris įgalina rinkėją pasitikrinti, ar jo balsas sėkmingai nukeliavo iki elektroninės balsavimo sistemos ir buvo įskaitytas. Turint šį kodą, neįmanoma atkurti balso turinio, taigi užkertama galimybė parduoti balsą. Siekiant apsisaugoti nuo galimų balsų pirkimų, rinkėjams leidžiama balsuoti „n“ kartų – įskaitomas tik paskutinis pasirinkimas. Rinkėjams taip pat suteikiama galimybė sugadinti elektroninį biuletenį, kitaip tariant į elektroninę balsadėžę įmesti tuščią.

Balsų tvarkymo specifika. Naudojama šifravimo technologija užtikrina rinkėjo ir jo balso konfidencialumą ir vientisumą. Balsai užšifruojami dar prieš išsiunčiant juos į elektronines balsadėžes ir tik rinkimų valdyba gali juos iššifruoti. Pasibaigus rinkimams, prieš pradedant balsų skaičiavimą, balsai perkeliami į saugią aplinką, sumaišomi ir iššifruojami, taip garantuojant rinkėjų anonimiškumą (Puiggali, 2014).

Interneto rinkimų audito specifika. „Scytl“ balsavimo internetu sistemą galima tikrinti prieš, per ir po rinkimų. Rinkimų auditas turi galimybę patikrinti, ar elektroninėje balsadėžėje yra

tik tam turinčių teisę rinkėjų balsai (Puiggali, 2014). Rinkimų auditas yra sujungtas su saugumo informacijos ir pranešimų apie pažeidimus vadyba. Šis sprendimas užtikrina, kad visi duomenys yra tinkamai apdoroti ir išanalizuotas jų saugumas. Vykdant nuolatinį pažeidžiamumų skanavimą, sistema turi realią galimybę blokuoti saugumo pažeidimus dar prieš jiems padarant žalą (Scytl, 2015).



Šaltinis: sudaryta autoriaus pagal Remote voting technologies, 2015

6 pav. **„Scytl“ balso patikrinimas**

„Scytl“ yra patentavusi „nekintamų įrašų“ technologiją, kuri apsaugo sistemų įrašus nuo neteisėtų pakeitimų. Nekintamų įrašų šifravimas garantuoja sistemų vientisumą.

2.1.2. „Cybernetica“ interneto rinkimų modelis

„Cybernetica“ organizacija tyrinėja, vysto bei gamina įvairią programinę įrangą, tiria bei taiko teorinius ir praktinius saugumo sprendimus. Kompanija sertifikuota pagal ISO 9001:2008 ir ISO 14001:2004 standartus. „Cybernetica“ dalyvavo keliuose Estijos Vyriausybės rengtuose projektuose, tokiuose kaip Estijos nacionalinės identifikacinės kortelės (ID) testavimas bei balsavimo internetu sistemos kūrimas (cyber.ee). „Cybernetica“ balsavimo internetu sistemą naudoja tik Estija.

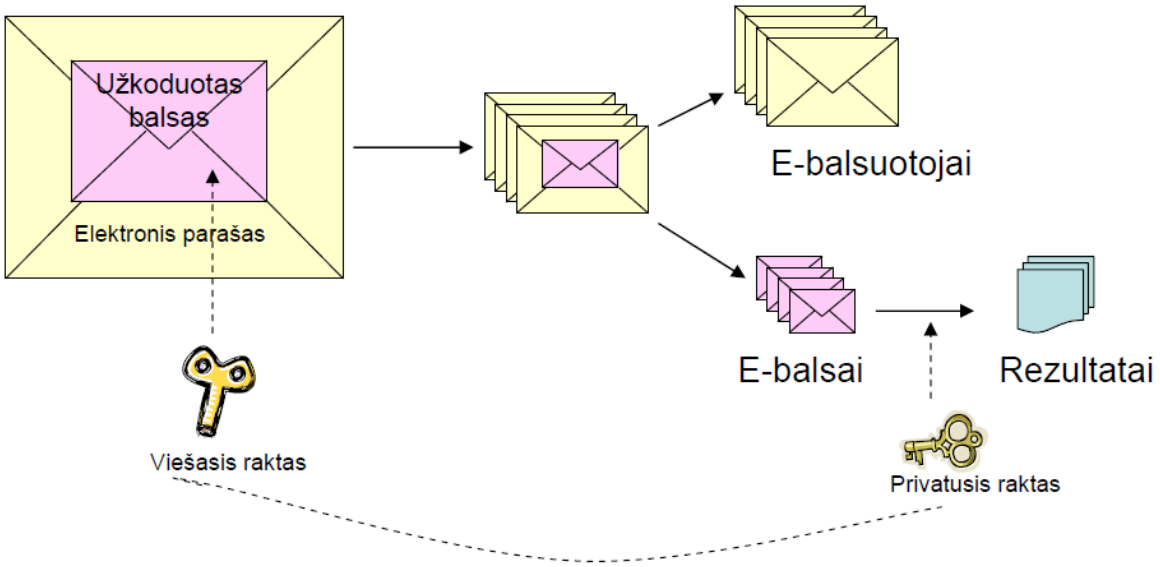
Estijoje rinkimai internetu vyksta likus 6 – 4 dienoms iki balsavimo rinkimų apylinkėse.

Rinkėjo registracijos metodika. Prieš kiekvienų rinkimų pradžią, rinkimų institucija skelbia balsavimo programų (Windows, Linux, Mac OS) rinkinius, kuriuos galima atsisiųsti iš https://valimised.ee puslapio. Rinkėjas atsisiunčia rinkimų aplikaciją, įvedamas identifikacijos raktas, kuris naudojamas, siekiant nustatyti rinkėjo tapatybę. Duomenų siuntimui naudojamas saugus ryšys (TSL) patvirtina serverio tapatybę, naudodamas užkoduotą sertifikatą. Serveris patvirtina rinkėjo tinkamumą (pagal viešąjį raktą) ir grąžina į kandidatų sąrašą. Rinkėjas pažymi savo pasirinkimą ir įveda pasirašymo raktą. Rinkėjų registracijos metu naudojamas balso ekspedijavimo serveris. Tai yra viešai prieinamas serveris, kuris priima HTTPS ryšį iš vartotojo programinės įrangos, patikrina rinkėjo tinkamumą ir veikia kaip posistemė tarpininkaujant su balsų saugojimo serveriu, kuris neprieinamas internetu (Springall ir kt., 2014).

*Rinkėjo asmens tapatybės nustatymo metodika. „*Cybernetica“ rinkimų modelyje, rinkėjo tapatybė nustatoma pasinaudojant asmens tapatybę patvirtinančia kortele (ID), kurioje yra integruotas elektroninis parašas. Kiekvienoje kortelėje yra du raktai: vartotojo identifikavimo raktas bei pasirašymo elektroninėje erdvėje raktas. Kiekvienas raktas turi po atskirą PIN kodą.

Kita galimybė rinkėjui patvirtinti savo asmens tapatybę yra panaudojant mobilųjį parašą (angl. Mobile ID). Rinkėjas savo mobiliajame įrenginyje atidaro interneto rinkimų svetainę www.valimised.ee, atsisiunčia bei įdiegia specialią interneto rinkimų programėlę. Įvedus į mobilųjį įrenginį mobiliojo parašo autentifikavimo kodą (PIN1), atsiunčiama SMS žinutė su kontroliniu kodu. Galimų kandidatų sąrašas pagal rinkėjo gyvenamąją vietą rodomas kompiuterio ekrane. Rinkėjas, kompiuterio pagalba daro pasirinkimą. Įvedęs mobiliajame įrenginyje privatųjį raktą (PIN2), sms žinute gauna kontrolinį kodą, kurį įvedęs kompiuteryje pasirašo pasirinktą balsą. Ekrane atsiranda užrašas, kad rinkėjo balsas įskaitytas (Springall ir kt., 2014). Mobilusis parašas suteikia galimybę rinkėjui identifikuoti save, tačiau išreikšti politinės valios naudojant mobiliojo telefono įrenginį šiuo metu nėra. Tam yra būtinas kompiuteris su interneto ryšiu. Dėl šių priežasčių šis būdas Estijoje nėra toks populiarus, nors valstybė ir skatina jį naudoti (Estonia.eu, 2015).

Balsavimo ir balso įskaitymo mechanizmas ir taikoma metodika. Interneto balsavimo sistema naudoja viešojo rakto infrastruktūrą, siekiant sukurti „dvigubo voko“ analogą, kuris naudojamas balsavimui paštu (žr. 7 pav.). Rinkėjo balsas, prieš išsiunčiant į elektroninę balsadėžę, yra užkoduojamas. Užkoduotą balsą galima laikyti vidiniu anoniminiu voku, kaip ir balsavime paštu. Rinkėjas, pasirašęs savo elektroniniu parašu, prie išorinio voko prideda savo identifikavimo duomenis (Ramonaitė ir kt., 2008). Išoriniame voke (skaitmeninis parašas) nustatoma rinkėjo tapatybė, o vidiniame voke (viešojo rakto šifravimas) saugoma „balso“ paslaptis. Kai nustatomas rinkėjo tinkamumas, parašas „nugarinamas“, paliekant anoniminį užšifruotą balsą. Vėliau balsas perkeliamas į fiziškai atskirtą serverį (Springall ir kt., 2014).



Šaltinis: Ramonaitė ir kt., 2008

7 pav. **Estijos balsavimo internetu techninis sprendimas**

Siekiant išvengti galimo balsų pirkimo, rinkėjui suteikiama galimybė internetu balsuoti „n“ kartų – įskaitomas tik paskutinis balsas (estonia.eu). Vartotojui rodoma, kad jis jau balsavo, bet nerodoma, kiek kartų. Jei rinkėjas balsuoja rinkimų dieną rinkimų apylinkėje, internetinis balsas panaikinamas (Springall ir kt., 2014).

Užšifruotas ir pasirašytas balsas siunčiamas į serverį bei susiejamas su neįspėjama unikalia žyma x bei grąžinamas rinkėjui QR kodo pavidalu (žr. 8 pav.). Vartotojas, naudodamas išmaniajame telefone įrašytą programėlę (angl. App), gali pasitikrinti, ar jo balsas buvo teisingai įrašytas. Programėlė nuskaito rinkėjo turimą QR kodą ir susisiekia su rinkimų serveriu, kuris grąžina šifruotą balsą (bet ne parašą) bei galimų kandidatų sąrašą. Programėlė, naudodama unikalią žymą x, užšifruoja imituojamą balsą kiekvienam galimam kandidatui. Gautą rezultatą ji palygina su užšifruotu balsu, atsiųstu iš rinkimų serverio. Jei yra sutapimų, programėlė rodo atitinkamą kandidatą.

Šaltinis: Springall ir kt., 2014

8 pav. **Balso patikrinimas Estijoje**

Estijos interneto rinkimų priešininkai teigia, kad šis balso patikrinimo būdas suteikia rinkėjui galimybę parduoti balsą, nes duodamas balsavimo turinio įrodymas. Tačiau rinkimų organizatoriai atkerta, kad ir be balso patikrinimo mechanizmo balsų pirkėjas gali sužinoti balso turinį, nes balsavimas vyksta nekontroliuojamoje aplinkoje. Šis mechanizmas tiesiog suteikia daugiau aiškumo rinkėjui, o be to, balsą patikrinti galima tik labai ribotą laiką (University of Tartu, 2015).

Balsų tvarkymo specifika. Balsų saugojimo serveryje saugomi pasirašyti, užšifruoti balsai balsavimo internetu laikotarpiu. Serveris, gavęs balsą iš balsų ekspedijavimo serverio, naudojant sertifikuotą išorinį protokolą, patikrina rinkėjo skaitmeninį parašą bei patvirtina, kad balsas suformuotas teisingai. Pasibaigus interneto rinkimams, balsų saugojimo serveris apdirba užšifruotus balsus ir iš naujo patikrina parašus bei pašalina bet kokius panaikintus ar negaliojančius balsus (Springall ir kt., 2014).

Balsų skaičiavimo metodika. Po balsų nuasmeninimo, rinkimus vykdantys pareigūnai visus galiojančius užšifruotus balsus įrašo į DVD ir perkelia į balsų skaičiavimo serverį. Skaičiavimo serveris yra prijungtas prie prietaiso, kuris turi savyje rinkimų privatų raktą, skirtą balsų dešifravimui. Pareigūnai eksportuoja suskaičiuotus balsus ir įrašo juos į DVD. Rezultatai palyginami su balsavusiųjų skaičiumi ir publikuojami. Balsų skaičiavimo serveris nėra jungiamas prie tinklo, jis naudojamas tik galutiniame rinkimų etape. Pareigūnai naudoja DVD šifruotiems balsams kopijuoti (su pašalintais jų parašais) (Springall ir kt., 2014).

Interneto rinkimų audito specifika. Siekiant stebėti interneto rinkimų procesą, naudojamas prisijungimo serveris. Šis serveris yra vidinė prisijungimo ir stebėjimo platforma, kuri stebi įvykius ir renka statistiką iš balsų ekspedijavimo serverio ir balsų saugojimo serverio. Serverio kodas ir dizainas nėra viešas. Prie šio serverio rinkimų darbuotojai gali prisijungti nuotoliniu būdu.

Pasibaigus balsavimui internetu (4 dienos iki balsavimo apylinkėse), balsavusių rinkėjų sąrašas elektroniniu būdu siunčiamas rinkimus organizuojančiai kompetentingai institucijai. Kompetentinga institucija rinkėjų sąrašuose pažymi jau balsavusius asmenis. Tradicinis balsavimas rinkimų apylinkėje visgi yra prioritetinis. Rinkėjas, jau balsavęs internetu, gali ateiti balsuoti ir rinkimų dieną į rinkimų apylinkę. Tokiu atveju, internetu atiduotas balsas ištrinamas (Estonia.eu, 2015).

2014 m. buvo viešai paskelbtos bei didelį ažiotažą sukėlusios nepriklausomų ekspertų komandos iš JAV, Jungtinės Karalystės ir Suomijos, tyrusios Estijos balsavimo internetu sistemos saugumą, išvados. Šiose išvadose teigiama, kad „*suklastoti balsavimo rezultatus galima rinkimų komisijos serveriuose, nulaužiant kompiuterius, kurie naudojami paruošti sistemos kodui prieš instaliavimą į balsų skaičiavimo serverius“*. Mokslininkai šį sistemos pažeidžiamumą pademonstravo savo laboratorijoje. Taip pat suklastoti balsavimo rezultatus galima rinkėjo

kompiuteryje, kenksmingai programai pavogus asmens tapatybės kortelės slaptažodžius ir slapta perbalsavus už rinkėją (Balsavimas internetu: užsienio valstybių patirtis ir perspektyvos Lietuvoje). Į šiuos pažeidžiamumų pastebėjimus Estijos Nacionalinio rinkimų komiteto ekspertai atsakė (University of Tartu, 2015):

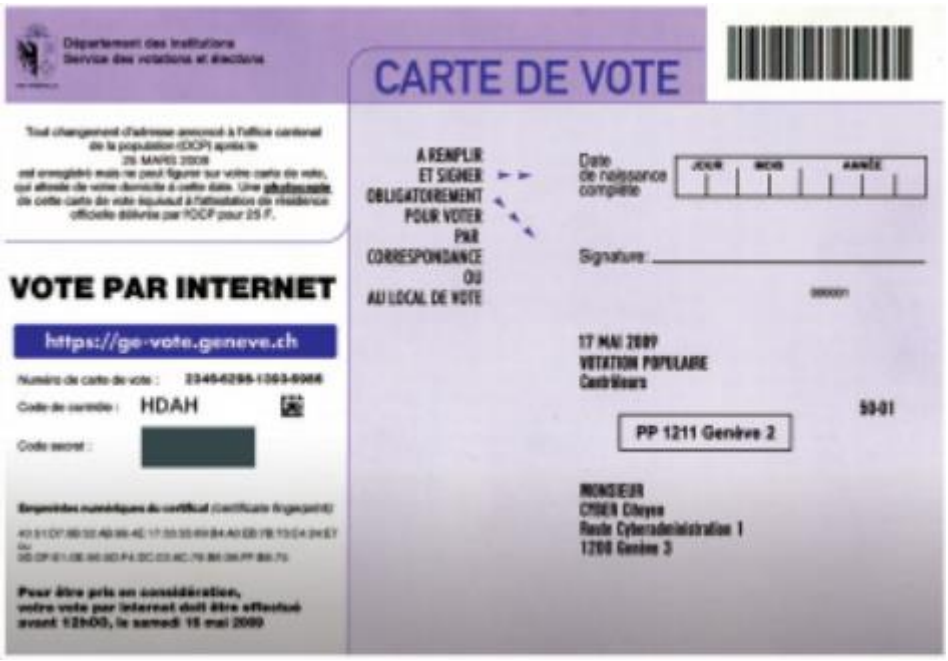
- Tyrėjai neatrado jokių naujų atakos vektorių, kurie nebūtų numatyti elektroninės sistemos projekte;
- Ekspertų pateiktų atakų metodikų neįmanoma efektyviai valdyti siekiant pakeisti rinkimų rezultatus;
- Rinkimų komitetas turi stiprią apsaugą bei automatinius mechanizmus, sugebančius aptikti atakas prieš elektroninių rinkimų sistemą ar bandymus klastoti rinkimų rezultatus;
- Interneto rinkimų svetainėje (estoniaevoting.org) esančios klaidos neatskleidžia techninių detalių apie tariamą sistemos pažeidžiamumą.

2.1.3. „Geneva solution" interneto rinkimų modelis

Šveicarijos federalinė vyriausybė interneto rinkimų projektą pradėjo įgyvendinti dar 2000 metais. Šalyje labai didelis referendumų skaičius, taigi interneto rinkimai turėjo padidinti rinkėjų prieinamumą bei aktyvumą balsuojant. Sistemos diegimą taip pat lėmė aukštas interneto skvarbos lygis. Šiuo metu Šveicarijos piliečiams internetu leidžiama balsuoti tik Europos Sąjungos valstybėse bei valstybėse, kurios yra pasirašiusios „Wassenaar" susitarimą. Balsuojant internetu, Ženevoje taikomas „Geneva solution" interneto rinkimų modelis.

Rinkėjo registracijos metodika. Kad užsienyje gyvenantys šveicarai būtų įtraukti į rinkėjų sąrašus, būtina užregistruoti savo gyvenamąją vietą Šveicarijos konsulinėse įstaigose ir kas ketverius metus atnaujinti registraciją (Barrat, Gildsmith, Turner, 2012).

Rinkėjo asmens tapatybės nustatymo metodika. Prieš kiekvienus rinkimus, Ženevos kontono rinkėjas paštu gauna laišką su vienkartine rinkėjo kortele (žr. 9 pav.), kurioje yra tam tikrą laiką galiojantis rinkėjo identifikacinis numeris. Šioje kortelėje saugomas rinkėjo numeris ir PIN kodas (Geneva State Chancellery, 2010). Rinkėjas elektroninių rinkimų sistemoje tapatybę patvirtina pasinaudodamas šia kortele bei įvesdamas savo gimimo datą ir kilmės savivaldybę (LR Seimo Parlamentinių tyrimų departamentas, 2015).



Šaltinis: Geneva State Chancellery, 2010

9 pav. **Ženevos kantono rinkėjo kortelė**

Saugiam rinkėjo prisijungimui prie interneto rinkimų serverio naudojama HTTPS sesija, sukuriant SSL ryšį.

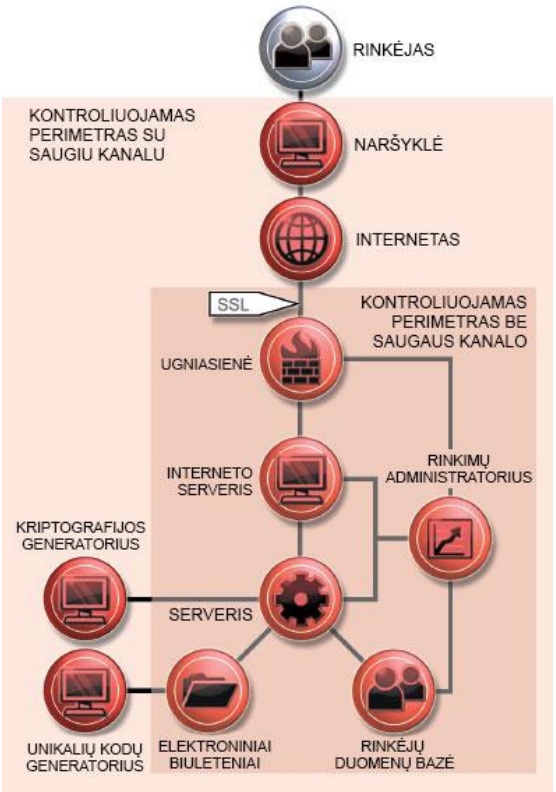
Balsavimo ir balso įskaitymo mechanizmas ir taikoma metodika. Interneto rinkimų svetainė viešai prieinama tampa po elektroninės balsadėžės antspaudavimo procedūros. Norėdamas balsuoti internetu, rinkėjas prisijungia prie https://www.evote-ch.ch/ge interneto svetainės bei įveda paštu gautą rinkėjo kortelės numerį. Paspausdamas „susipažinau“, rinkėjas patvirtina, kad susipažino su ekrane pasirodžiusia aktualia teisine informacija (gręsiančia atsakomybę už rinkimų teisės pažeidimus) (Barrat, Gildsmith, Turner, 2012). Balso įrašymas prasideda dar rinkėjo kompiuteryje, kai rinkėjas pažymi savo sprendimą. Vėliau saugiu kanalu nusiunčiamas į elektroninę balsadėžę, iššifruojamas, patikrinamas rinkėjo tinkamumas bei duomenų vientisumas. Sistema rinkėjui išsiunčia patvirtinimą dėl jo pasirinkimo su unikaliu kodu, žinomu tik elektroninei rinkimų sistemai ir pačiam rinkėjui. Tuomet rinkėjas turi patvirtinti savo asmens tapatybę įvesdamas savo gimimo datą, slaptažodį iš rinkėjo kortelės bei kilmės savivaldybę. Šių duomenų nėra viešai prieinamuose registruose. Kilmės savivaldybė taip pat yra nurodoma ir Šveicarijos piliečių asmens tapatybės kortelėse ir piliečių pasuose. Serveris patikrina rinkėjo duomenis, ar rinkėjas dar nebalsavo ir įrašo balsą. Galiausiai elektroninis rinkimų serveris nusiunčia rinkėjui patvirtinimą, kad jo balsas įskaitytas.

Balsų užšifravimui naudojamas asimetrinis šifravimo metodas, panaudojant viešąjį ir privatųjį rinkimų raktus, kurie yra sugeneruojami prieš rinkimus. Prieš išsiunčiant balsą, jis dar kartą užšifruojamas simetriniu šifru, kurio slaptas kodas paimamas iš rinkėjo kortelės. Toks

dvigubas balso šifravimas prideda daugiau saugumo. Be to, elektroninė balsavimo sistema, gavusi balsą, panaudodama maišos funkciją (angl. Hash), patikrina ar balsas nebuvo pakeistas (Canton de Geneve, 2009).

Ženevos rinkimų sistemoje yra vienas rinkėjų sąrašas, skirtas visiems trims balsavimo būdams (internetu, paštu bei rinkimų apylinkėje). Tokiu būdu yra užkertamas kelias balsuoti daugiau nei vieną kartą. Internetu leidžiama balsuoti tik vieną kartą (perbalsuoti galimybės nėra). Rinkėjas, balsavęs internetu, jau nebeturi teisės balsuoti kitais būdais (paštu ar rinkimų dieną rinkimų apylinkėje) (LR Seimo Parlamentinių tyrimų departamentas, 2015). Todėl yra pakankamai sunku užtikrinti, kad balsuojama laisva valia. Taip pat atsiranda galimybė, kad vienas šeimos narys gali prabalsuoti už kitus. Anot rinkimų organizatorių, ši problema sprendžiama balsavimo metu paklausiant privataus klausimo, kurį gali žinoti tik rinkėjas. Rinkimų administracija po rinkimų skambina 2 proc. internetu balsavusių rinkėjų, norėdami įsitikinti, kad jie balsavo savarankiškai ir niekieno neverčiami (Geneva State Chancellery, 2010).

Balsų skaičiavimo metodika. Elektroniniai balsai skaičiuojami per oficialų kompetentingos institucijos posėdį, kuriame dalyvauja ir įvairių partijų atstovai. Į rinkimų administratoriaus kompiuterį įvedant slaptažodžius (USB raktai ir CD), kuriuos turi skirtingi rinkimų darbuotojai, gaunamas privatus rinkimų raktas, kuriuo iššifruojami balsai ir suskaičiuojami rezultatai (Geneva State Chancellery, 2010).



Šaltinis: sudaryta autoriaus pagal Geneva State Chancellery, 2010

10 pav. **Ženevos balsavimo internetu procesas**

10 pav. pavaizduotas Ženevos balsavimo internetu modelis. Pagal šį modelį, rinkėjui prisijungus prie internetinės balsavimo sistemos, atsisiunčiama bei į savo įrenginį įdiegiama balsavimo internetu programėlė. Ši programėlė į interneto naršyklę automatiškai įskiepija Java skribtą (angl. Java script), kuris užtikrina saugią komunikaciją tarp rinkėjo ir elektroninės balsavimo sistemos. Tokiu būdu sukuriama kontroliuojama aplinka. Interneto ryšiu, panaudojant SSL protokolą, susijungiama su elektronine balsavimo sistema. Duomenų srautą tikrina ugniasienė. Elektroninėje balsavimo sistemoje yra interneto serveris, kuris nukreipia užklausas ir rinkėjų duomenų bazė, kuriuos prižiūri rinkimų administratorius bei elektroniniai biuleteniai. Taip pat yra unikalių kodų generatorius, kuris generuoja rinkėjo identifikavimo kortelių numerius bei kriptografijos generatorius, kuris sugeneruoja rinkimų kriptografinius raktus. Modelis neapima viso balsavimo proceso – tik pirmąją jo dalį (apima rinkėjo registraciją, asmens tapatybės nustatymą bei rinkėjo biuletenio suformavimą).

2.2. Interneto rinkimų modelių lyginamoji analizė

Atliekant lyginamąją analizę, lyginami interneto rinkimų proceso aspektai skirtinguose interneto rinkimų modeliuose. Analizei pasirinkti „Scytl“, „Cybernetica“ ir „Geneva solution“ interneto rinkimų modeliai.

Rinkėjo registracijos metodika nagrinėjamuose modeliuose skiriasi. „Scytl“ ir „Cybernetica“ modeliuose vartotojas registruojasi interneto rinkimų dieną prisijungdamas prie rinkimų svetainės. Tuo tarpu „Geneva solution“ interneto rinkimų modelyje būtina užregistruoti savo gyvenamąją vietą Šveicarijos konsulinėse įstaigose ir kas ketverius metus atnaujinti registraciją. „Scytl“ rinkimų modelis rinkėjui suteikia galimybę registruotis bei balsuoti panaudojant įrenginius su Google, Android, Blackberry ir Apple IOS operacinėmis sistemomis, tuo tarpu kiti rinkimų modeliai balsuoti leidžia tik panaudojant asmeninį kompiuterį.

Lanksčiausią *rinkėjo asmens tapatybės nustatymo metodiką* taiko „Scytl“, kuri deklaruoja galinti prisiderinti prie bet kokio saugaus rinkėjo asmens tapatybės nustatymo metodo. „Cybernetica“ rinkimų modelyje, rinkėjo tapatybė nustatoma pasinaudojant asmens tapatybę patvirtinančia kortele, taip pat valstybė skatina naudoti mobilųjį parašą. Ženevos kontono rinkėjas elektroninių rinkimų sistemoje tapatybę patvirtina pasinaudodamas specialiai rinkimams gautą kortelę bei įvesdamas tik jam žinomus slaptus duomenis (gimimo datą bei kilmės savivaldybę).

Balsavimo ir balso įskaitymo mechanizmas ir taikoma metodika. Nagrinėjami interneto modeliai užtikrinant balso slaptumą naudoja viešojo rakto infrastruktūrą, sukuriant „dvigubo voko“ analogą, kuris naudojamas balsavimui paštu. Vienintelis „Scytl“ siūlo galimybę

balsuoti panaudojant įrenginius su Google, Android, Blackberry ir Apple IOS operacinėmis sistemomis, tuo tarpu kiti rinkimų modeliai tą leidžia atlikti tik panaudojant asmeninį kompiuterį.

„Scytl“ ir „Cybernetica“ modeliai numato rinkėjui galimybę internetu balsuoti „n“ kartų užskaitant tik paskutinį balsą. Tai sumažina rinkėjo papirkimo tikimybę. „Geneva solution“ modelis rinkėjui leidžia balsuoti tik vieną kartą. Be to, Ženevos rinkėjas, prabalsavęs internetu, netenka teisės balsuoti paštu bei rinkimų apylinkėje.

„Scytl“ rinkimų modelis rinkėjui suteikia galimybę pasitikrinti, ar jo balsas įskaitytas bei įrašytas kaip numatytas. Tokiu būdu, nepateikiant balsavimo turinio, galima įsitikinti, kad balsas teisingai įrašytas ir reikia atlikti tik keletą veiksmų. „Cybernetica“, įskaičiusi rinkėjo balsą, atsiunčia unikalų QR kodą. Vartotojas, naudodamas išmaniajame telefone įrašytą programėlę, gali pasitikrinti, ar jo balsas buvo teisingai įrašytas. Ženevos interneto rinkimų modelyje galimybės patikrinti balsą nėra.

Balsų skaičiavimo metodika nagrinėjamuose interneto rinkimų modeliuose labai panaši – po rinkimų elektroniniai balsai nuasmeninami ir įrašomi į DVD diską bei perkeliami į saugią aplinką, kur, panaudojus rinkimų privatų raktą, iššifruojami bei suskaičiuojami.

*Interneto rinkimų audito specifika. „*Scytl“ balsavimo internetu sistemą galima tikrinti prieš, per ir po rinkimų. Rinkimų auditas yra sujungtas su saugumo informacijos ir pranešimų apie pažeidimus vadyba. Vykdant nuolatinį pažeidžiamumų skanavimą, sistema turi realią galimybę blokuoti saugumo pažeidimus dar prieš jiems padarant žalą. „Cybernetica“ interneto rinkimų modelis siekiant stebėti interneto rinkimų procesą naudoja prisijungimo serverį, kuris yra vidinė prisijungimo ir stebėjimo platforma, stebinti įvykius ir renkanti statistiką iš balsų ekspedijavimo serverio ir balsų saugojimo serverio. Serverio kodas ir dizainas nėra vieši. Prie šio serverio rinkimų darbuotojai gali prisijungti nuotoliniu būdu.

Apibendrinant galima konstatuoti, kad visi nagrinėti modeliai yra skirtingi. Juos visus vienija tik „dvigubo voko“ panaudojimas, siekiant užtikrinti balsų slaptumą. Autoriaus nuomone, „Geneva solution“ modelis yra nepriimtinas įgyvendinant interneto rinkimus Lietuvoje dėl nepakankamo saugumo nustatant rinkėjo asmens tapatybę. Paštu atsiųsta rinkėjo kortelė gali būti pavogta, o rinkėjo gimimo data bei gimimo vieta nėra slapti duomenys Lietuvoje. „Scytl“ ir „Cybernetica“ modeliai šiuo požiūriu yra gerokai saugesni. Sunku nuspręsti, kuris iš jų geresnis. „Scytl“ suteikia platesnes galimybes rinkėjui renkantis įrenginį balsavimui. Tačiau, autoriaus nuomone, „Cybernetica“ balso patikrinimo metodas, kritikuojamas dėl galimo balso turinio įrodymo, yra patogesnis rinkėjui.

2.3. Kibernetinio saugumo valdymo įgyvendinimas Lietuvoje

Valstybės ir visuomenės gyvenime vis didesnę reikšmę įgyja informacinėmis ir ryšių technologijomis tvarkoma ir perduodama elektroninė informacija, o atsiradusios elektroninės informacijos tvarkymo galimybės paskatino nacionalinių ir globalių informacinių visuomenių atsiradimą ir sudarė sąlygas toliau modernizuoti šalių ūkius ir efektyviau valdyti valstybę. Tuo pačiu metu į elektroninę formą perkeliama vis daugiau informacijos, sparčiai automatizuojami įvairūs šalies valdymo ir ūkio veiklos procesai, globali kibernetinė erdvė ir joje teikiamos viešosios paslaugos tapo patraukliu atskirų asmenų, nusikalstamų grupuočių, politinių jėgų ir kitų subjektų taikiniu. Taigi atsirado poreikis elektroninės informacijos saugą ir kibernetinį saugumą plačiąja prasme užtikrinti teisinėmis priemonėmis. Šiuo metu Lietuvoje kibernetinio saugumo valdymo procesas dar tik kuriamas: 2014 m. pabaigoje priimtas Kibernetinio saugumo įstatymas, rengiami atitinkami poįstatyminiai teisės aktai, dar ilgiau užtruks realios įstatymo taikymo praktikos formavimasis.

Pirmasis dokumentas, nustatantis kibernetinio saugumo plėtros tikslus, uždavinius ir konkrečias priemones – LR Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo“. Ši programa numatė, kad ją įgyvendinus turėtų būti užtikrintas valstybės informacinių išteklių saugumas, veiksmingas ypatingos svarbos informacinės infrastruktūros funkcionavimas bei Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumas kibernetinėje erdvėje. Programoje yra numatyta tobulinti kibernetinio saugumo koordinavimą ir priežiūrą, teisinį reglamentavimą, plėtoti tarptautinį bendradarbiavimą, kelti kibernetinio saugumo kultūrą, užtikrinti virtualaus Lietuvos kibernetinės erdvės perimetro apsaugą nuo išorinių kibernetinių atakų, stiprinti kibernetinėje erdvėje teikiamų paslaugų saugumą ir kt. Viena ir programos priemonių buvo parengti ir priimti esminius su elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimu susijusius reikalavimus, nustatančius specialius atitinkamą veiką ir teisinius santykius reglamentuojančius įstatymus. 2014 m. gruodžio 11 d. LR Seimas priėmė Kibernetinio saugumo įstatymą Nr. XII-1428, kuris sukūrė teisinę bazę, sudarančią prielaidas veiksmingai kovoti su incidentais viešuosiuose elektroniniuose tinkluose ir išsprendė fragmentiško ir neefektyvaus šios srities reglamentavimo žemesnės teisinės galios teisės aktais problemą.

Kibernetinio saugumo įstatymas buvo rengiamas siekiant reglamentuoti kibernetinio saugumo sritį, tikslinti teisės normas, reglamentuojančias valstybės informacinių išteklių saugą, valstybės informacinių išteklių atitiktį nustatytiems saugos reikalavimams, nustatyti teisinį pagrindą tvarkyti asmens duomenis kibernetinio saugumo užtikrinimo tikslais. Įstatymu taip pat siekiama nustatyti kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų

kompetenciją, funkcijas, teises ir pareigas, valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones. Svarbu pabrėžti, kad Kibernetinio saugumo įstatymas taikomas tiek, kiek šiame įstatyme reglamentuojamų visuomeninių santykių nereglamentuoja Asmens duomenų teisinės apsaugos įstatymas, Elektroninių ryšių įstatymas, Nacionalinio saugumo pagrindų įstatymas ir Valstybės informacinių išteklių valdymo įstatymas.

Įstatymo 3 str. nustatyta, kad kibernetinis saugumas grindžiamas bendraisiais teisės principais (pvz., teisinės valstybės, teisės į teisingą teismą), taip pat elektroninių ryšių veiklos reguliavimo principais (veiksmingo ribotų išteklių valdymo ir naudojimo, technologinio neutralumo, funkcinio lygiavertiškumo, proporcingumo, mažiausio būtino reguliavimo, teisinio tikrumo kintančioje rinkoje, ekonominės plėtros, veiksmingos konkurencijos užtikrinimo, vartotojų teisių apsaugos, reguliavimo kriterijų, sąlygų ir procedūrų objektyvumo, skaidrumo ir nediskriminavimo principais, numatytais Elektroninių ryšių įstatymo 2 str.) ir specialiaisiais kibernetinio saugumo principais: kibernetinės erdvės nediskriminavimo, kibernetinio saugumo proporcingumo ir viešojo intereso viršenybės. Visi principai turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė (Kibernetinio saugumo įstatymas, 2015).

Vienas iš pagrindinių įstatymo uždavinių – aiškiai nustatyti už kibernetinio saugumo politikos formavimą ir įgyvendinimą atsakingas institucijas, jų funkcijas, teises ir pareigas. Įstatymo 4 str. nurodyta, kad šios institucijos yra LR Vyriausybė, Krašto apsaugos ministerija, Vidaus reikalų ministerija, Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos tarnyba ir Policijos departamentas.

LR Vyriausybė yra kibernetinio saugumo politikos strateginius tikslus ir jiems pasiekti būtinas priemones nustatanti institucija. Krašto apsaugos ministerija ne tik formuoja, organizuoja, bet ir kontroliuoja bei koordinuoja kibernetinio saugumo politiką (pvz., rengia ir teikia LR Vyriausybei tvirtinti Nacionalinį kibernetinių incidentų valdymo planą, rengia ir tvirtina Kibernetinio saugumo informacinio tinklo nuostatus). Įstatymo 9 str. taip pat numato, kad prie Krašto apsaugos ministerijos veikia Kibernetinio saugumo taryba (toliau – Taryba) – nuolatinė kolegiali institucija, analizuojanti kibernetinio saugumo būklę ir teikianti siūlymus dėl šios būklės gerinimo. 2015 m. balandžio 23 d. LR Vyriausybė nutarimu Nr. 422 patvirtino Tarybos sudėtį ir reglamentą. Tarybą sudaro kibernetinio saugumo politiką formuojančių ir įgyvendinančių valstybės institucijų, informacinių technologijų srityje veiklą vykdančių verslo subjektų atstovai, mokslo ir studijų institucijų atstovai, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių

tinklų ir viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų atstovai – iš viso 24 asmenys.

Kitos Kibernetinio saugumo įstatyme įvardintos institucijos yra politiką įgyvendinančios institucijos. Ryšių reguliavimo tarnyba (toliau – RRT), įgyvendindama kibernetinio saugumo politiką, reguliuoja viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veiklą kibernetinio saugumo užtikrinimo srityje. Svarbu pabrėžti, kad RRT, siekdama užtikrinti viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų saugumą ir vientisumą, užkirsti kelią kibernetiniams incidentams plisti, mažinti dėl kibernetinių incidentų patiriamos žalos atsiradimo riziką, turi teisę duoti *privalomus* nurodymus ir nustatyti nurodymų įvykdymo terminą savo reguliuojamiems subjektams. Tokie nurodymai turi būti motyvuoti ir proporcingi tikslui pasiekti. Valstybinė duomenų apsaugos inspekcija įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje, tuo tarpu policija, tiksliau Lietuvos kriminalinės policijos biuras, teisės aktų nustatyta tvarka vykdo kibernetinių incidentų, galimai turinčių nusikalstamos veiklos požymių, užkardymą ir tyrimą. Lietuvos kriminalinės policijos biuras, įgyvendindamas šią įstatymo nuostatą, renka, analizuoja ir apibendrina informaciją apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių, rengia analitines pažymas, situacijos apžvalgas, teikia visuomenei ir suinteresuotoms institucijoms rekomendacijas dėl rizikos veiksnių, pavojų ir grėsmių kibernetinėje erdvėje bei techninius ar teisinius sprendimus siekiant išvengti kibernetinių incidentų (Lietuvos policijos generalinio komisaro 2015 m. vasario 2. įsakymas Nr. 5-V-101, 3 d.). Kibernetinio saugumo įstatymo 12 str. suteikia teisę policijai duoti motyvuotus nurodymus ne ilgiau kaip 48 valandoms be teismo sankcijos, ilgesniam laikui – su apylinkės teismo sankcija, apriboti viešųjų ryšių tinklų ar viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikimą paslaugų gavėjui, kai paslaugų gavėjas ar jo naudojama informacinė ir ryšių technologijų įranga galimai dalyvauja nusikalstamoje veikoje, ar nurodyti minėtiems subjektams taikyti priemones, šalinančias nusikalstamų veikų kibernetinėje erdvėje priežastis. Policijos nurodymus privaloma įvykdyti ne vėliau kaip per 8 val. nuo jų gavimo.

Kibernetinio saugumo įstatymas įsteigė naują instituciją – Nacionalinį kibernetinio saugumo centrą. Jo funkcijas vykdo įstaiga prie Krašto apsaugos ministerijos – šiuo metu tai yra Kibernetinio saugumo ir telekomunikacijų tarnyba. Centras, įgyvendindamas kibernetinio saugumo politiką ir vykdydamas valstybės informacinių išteklių ir ypatingos svarbos informacinių infrastruktūrų kibernetinių incidentų valdymo padalinio veiklą, rengia ir teikia pasiūlymus Krašto apsaugos ministerijai, atlieka stebėseną, teikia konsultacijas ir rekomendacijas kibernetinio saugumo klausimais, analizuoja kibernetinio saugumo situaciją ir rengia būklės ataskaitas, valdo kibernetinio saugumo informacinį tinklą ir kt. Centras gali priimti ir imperatyvaus pobūdžio

sprendimus, nes įstatymo 10 str. 3 d. 4 p. nurodyta, kad kibernetinio incidento metu jis turi teisę duoti motyvuotus privalomus nurodymus, susijusius su kibernetinio saugumo užtikrinimu, viešojo administravimo subjektams, valdantiems ar tvarkantiems valstybės informacinius išteklius, ir ypatingos svarbos informacinės infrastruktūros valdytojams. Siekiant stabdyti kibernetinio incidento poveikį valstybės informacinių išteklių ar ypatingos svarbos informacinių infrastruktūrų kibernetiniam saugumui, Centrui taip pat suteikiama teisė *be teismo sankcijos* duoti motyvuotą nurodymą viešųjų ryšių tinklų ar viešųjų elektroninių ryšių paslaugų teikėjams laikinai, bet ne ilgiau negu 48 valandoms, apriboti viešųjų elektroninių ryšių paslaugų teikimą šių paslaugų gavėjui.

Kibernetinio saugumo įstatymas įsigaliojo 2015 metų sausio 1 d., taigi galioja tik metus. Iki šiol nėra priimti visi poįstatyminiai teisės aktai, Nacionalinis kibernetinio saugumo centras kol kas dirba ne visu pajėgumu. Šio įstatymo taikymo teismų praktika taip pat nėra susiformavusi, todėl kol kas sunku kalbėti apie įstatymo spragas ar jį taikančių institucijų bendradarbiavimo problemas. Įsigaliojus Kibernetinio saugumo įstatymui valstybės institucijoms buvo aiškiai numatyta kompetencija ir funkcijos sparčiai besikeičiančioje aplinkoje, todėl šiuo metu svarbiausia – tinkamai taikyti šias teisės normas ir laiku reaguoti į besikeičiančias aplinkybes.

Kibernetinio saugumo valdymui Lietuvoje svarbus ir Valstybės informacinių išteklių valdymo įstatymas, įsigaliojęs nuo 2012 m. sausio 1 d. Šio teisės akto tikslas - užtikrinti tinkamą valstybės informacinių išteklių kūrimą, tvarkymą, valdymą, naudojimą, priežiūrą, sąveiką, planavimą, finansavimą ir saugą. Valstybės informaciniai ištekliai, pagal Įstatymo 2 str. 17 d., tai informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma. Įstatyme numatyta, kad LR Vyriausybė nustato valstybės informacinių išteklių veiklos prioritetus, plėtros kryptis, siektinus rezultatus, tvirtina informacijos saugos reikalavimų aprašą, saugos dokumentų turinio gaires, nustato informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo tvarką ir pan. (Įstatymo 4 str.). Valstybės informacinių išteklių politiką pagal kompetenciją formuoja kelios institucijos: Susisiekimo ministerija, Teisingumo ministerija ir Vidaus reikalų ministerija. Susisiekimo ministerija formuoja valstybės informacinių išteklių plėtros politiką, Teisingumo ministerija atsako už registrų politikos formavimą, o Vidaus reikalų ministerija – formuoja politiką valstybės informacinių išteklių saugos srityje tiek, kiek tai neapima kibernetinio saugumo, ir informacinių technologijų taikymo viešojo administravimo (elektroninės valdžios) srityje. Pagal institucijų kompetenciją galima teigti, kad svarbiausia šiuo atveju yra Susisiekimo ministerija. Jos įgaliota institucija, t.y. Informacinės visuomenės plėtros komitetas, atsako už valstybės informacinių išteklių funkcinį suderinamumą, kūrimą, tvarkymą ir plėtrą. Valstybinė duomenų apsaugos inspekcija atsako už asmens duomenų apsaugos reikalavimų įgyvendinimą ir jų laikymosi priežiūrą. Svarbu atkreipti dėmesį, kad prie Susisiekimo ministerijos

taip pat veikia tam tikra patariamoji institucija – Valstybės informacinių išteklių valdymo taryba. Ją sudaro valstybės informacinių išteklių politiką formuojančių institucijų, Vyriausybės kanceliarijos, Seimo kanceliarijos, Respublikos Prezidento kanceliarijos, Nacionalinės teismų administracijos, Lietuvos savivaldybių asociacijos ir kiti atstovai, kompetentingi informacinių ir ryšių technologijų srityje. Valstybės informacinių išteklių valdymo tarybos narių skaičių, personalinę sudėtį ir jos veiklos reglamentą tvirtina Vyriausybė (Įstatymo 7 str. 1 d.). Šios tarybos užduotis – teikti pasiūlymus ir rekomendacijas Vyriausybei įvairiais valstybės informacinių išteklių valdymo klausimais. Jos, kaip ir Kibernetinio saugumo tarybos, pagrindinis uždavinys – bendradarbiavimo tarp įvairių institucijų ir ekspertų skatinimas, konsultavimasis ir veiksmų koordinavimas bei informacijos sklaida.

Apibendrinant kibernetinio saugumo valdymo įgyvendinimą Lietuvoje galima pastebėti, kad kibernetinio saugumo valdymo procese dalyvauja nemažai valstybės vykdomosios valdžios institucijų. Svarbiausios iš jų – Krašto apsaugos ministerija, Susisiekimo ministerija ir Vidaus reikalų ministerija. Itin svarbus yra šių institucijų bendradarbiavimas, konsultavimasis, nuolatinis informacijos keitimasis ir savitarpio pagalba. Tuo pačiu svarbūs ir ryšiai su mokslo bendruomene bei asocijuotomis verslo struktūromis.

2.4. Interneto rinkimų teisinio reglamentavimo ypatumai Lietuvoje

Lietuvos valdžios institucijos ir politikai, įgyvendindami Europos Sąjungos skatinamus e.valdžios ir e.vyriausybės principus, ir skatindami rinkėjus aktyviau dalyvauti rinkimuose bei referendumuose, ieško būdų, kaip, remiantis sėkmingu Estijos Respublikos pavyzdžiu, įgyvendinti interneto rinkimus Lietuvoje. 2006 m. lapkričio 16 d. LR Seimo nutarimu Nr. X-912 buvo patvirtinta Vyriausiosios rinkimų komisijos (toliau – VRK) parengta „Balsavimo internetu rinkimuose ir referendumuose koncepcija“. Remiantis šia koncepcija, 2007 m. liepos 11 d. LR Vyriausybė priėmė nutarimą „Dėl balsavimo internetu diegimo programos patvirtinimo“ Nr. 759. (toliau – Programa). Šiuo metu tai yra vieninteliai teisės aktai, reglamentuojantys balsavimą internetu rinkimuose ir referendumuose, tiksliau, jo galimybę, Lietuvoje. Šie teisės aktai yra tik rekomendacinio pobūdžio, nubrėžiantys tam tikras gaires, kryptis, kuriomis reikėtų vadovautis, rengiant ir įgyvendinat atitinkamų įstatymų (Seimo rinkimų įstatymo, Prezidento rinkimų įstatymo, Savivaldybių tarybų rinkimų įstatymo, Rinkimų į Europos Parlamentą įstatymo ir Referendumo įstatymo), įteisinančių balsavimą internetu kaip alternatyvų balsavimo būdą, pakeitimus. Koncepcijoje pabrėžiama, kad taip pat būtina padaryti atitinkamas Baudžiamojo kodekso ir Administracinių teisės pažeidimų kodekso pataisas, įtvirtinant bankų, kitų juridinių bei fizinių

asmenų atsakomybę už interneto rinkimų kompromitavimą: balsų pirkimą, slaptumo ir saugumo pažeidimą, balsavimą už kitus rinkėjus ir pan.

Lietuvoje šiuo metu interneto rinkimai nėra įteisinti, t.y. nėra įstatymų, reglamentuojančių balsavimą internetu LR Seimo, Prezidento, Europos Parlamento, savivaldybių rinkimuose ir referendumuose. LR Seimas ne kartą bandė svarstyti atitinkamas įstatymų pataisas, tačiau, dėl politinės valios trūkumo ir visuomenės nuogąstavimo, nei vienas bandymas nebuvo sėkmingas. LR Seime nuo 2007 m. iki 2014 m. buvo užregistruoti penki paketai atitinkamų įstatymų pakeitimų įstatymų projektų. Kai kurie iš jų buvo pateikti LR Seimo plenariniame posėdyje, juos svarstė specializuoti LR Seimo komitetai, tačiau tolesnis svarstymas buvo nesėkmingas. Paskutinį įstatymų pakeitimų įstatymų projektų paketą 2014 m. gegužės 21 d. užregistravo teisingumo ministras Juozas Bernatonis ir susisiekimo ministras Evaldas Sinkevičius. Iki šiol šie projektai nėra pradėti svarstyti, t.y. nebuvo pateikti Seimo plenariniame posėdyje.

Balsavimo internetu rinkimuose ir referendumuose koncepcija. 2006 m. LR Seimo patvirtintos „Balsavimo internetu rinkimuose ir referendumuose koncepcijos“ tikslas - apibrėžti interneto rinkimus, numatyti balsavimo internetu galimybę Lietuvos Respublikoje vykdomuose rinkimuose bei referendumuose, nurodyti balsavimo internetu privalumus ir problemas, galinčias atsirasti vykdant tokį balsavimą. Dokumente taip pat numatomi rinkėjų identifikavimo būdai, principinė tokio balsavimo sistema, jos įdiegimo kaina ir teisinio reguliavimo reikalavimai. Koncepcijoje pabrėžiama, kad balsavimo internetu tikslai ir uždaviniai yra palengvinti dalyvavimą rinkimuose suteikiant platesnes galimybes atiduoti balsą kitoje nei balsavimo apylinkė vietoje, siūlant naujas balsavimo formas skatinti rinkėjus dalyvauti rinkimuose, pritaikyti rinkimus prie naujų telekomunikacijos technologijų bei palengvinti ir padaryti veiksmingesnį balsų skaičiavimą ir rinkimų ar referendumo rezultatų nustatymą. Įgyvendinant interneto rinkimus būtina laikytis LR Konstitucijoje nustatytų rinkimų principų: visuotinė, lygi, tiesioginė rinkimų teisė ir slaptas balsavimas. Vienas iš sudėtingiausių balsavimo internetu įgyvendinimo klausimų yra rinkėjų identifikavimas ir principinė balsavimo schema. Koncepcijos III dalyje teigiama, kad pradinėje balsavimo internetu diegimo stadijoje rinkėjų tapatybei nustatyti tikslingiausia pasirinkti Lietuvoje veikiančią gerai išvystytą, pakankamai saugią ir patikimą elektroninės bankininkystės sistemą. Asmuo, sudarydamas su banku banko sąskaitos sutartį, patvirtina banko darbuotojui savo tapatybę, pateikdamas asmens dokumentą ir savo parašo pavyzdį. Tikimybė, kad sąskaita bus atidaryta kito asmens vardu, nedidelė. Be to, asmuo nebūtų suinteresuotas kam nors atskleisti savo pinigų sąskaitos prieigos kodus. Tuo pačiu koncepcijoje pabrėžiama, kad problemų užtikrinant patikimą rinkėjo tapatybės nustatymą gali kelti banko darbuotojų nesąžiningumas. Bankas, žinodamas ar spėdamas, kad konkretus rinkėjas nebalsuoja apskritai ar yra išvykęs į užsienį, gali jungtis prie VRK serverio apsimesdamas rinkėju. Dėl to, sudarant atitinkamas sutartis su bankais, būtina

nustatyti aiškius reikalavimus, kuriuos turi atitikti tiek banko techninė įranga, tiek banko personalas. Siūloma, kad personalo, tvarkančio balsavimą internetu, patikimumas turėtų būti ne mažesnis nei tų asmenų, kuriems Valstybės saugumo departamentas suteikia teisę dirbti su slapta informacija.

Koncepcijoje taip pat yra pateikiama balsavimo internetu principinė schema, kuria remiantis turėtų būti organizuojami rinkimai ir referendumai Lietuvoje. Tiesiogiai arba per banko elektroninio aptarnavimo sistemą rinkėjas prisijungia prie VRK balsavimo tinklalapio. VRK serveris patikrina, ar toks rinkėjas yra rinkimų sąrašuose, ir priskiria rinkėją atitinkamai rinkimų apygardai. Tuomet rinkėjui ekrane pateikiamas biuletenis, jame rinkėjas pažymi savo pasirinkimą (pasirinkimus) ir jį patvirtina. Rinkėjo balsas saugiu ryšio kanalu perduodamas į VRK serverį, čia nedelsiant užkoduojamas ir patenka į elektroninę balsadėžę. Rinkėjų sąraše pažymima, kad rinkėjas balsavo, o užkoduotas balsas su rinkėjo tapatybės nustatymo duomenimis patenka į e. balsadėžę ir ten saugomas iki tradicinio balsavimo pabaigos. Pasibaigus balsavimo internetu laikui, e. balsadėžė „uždaroma“, t. y. atjungiama nuo išorinio ryšio kanalų, o pagal internetu balsavusių asmenų sąrašą pažymimi rinkėjai rinkėjų sąrašuose, numatytuose skirstyti apygardoms ir apylinkėms. Nepaisant to, kad rinkėjas jau pasinaudojo savo balsavimo teise internetu, jam suteikiama galimybė balsuoti ir tradiciniu būdu. Rinkėjui atvykus į rinkimų apylinkę rinkimų dieną ir balsavus tradiciniu būdu, rinkėjų sąrašuose (kuriuose apylinkės komisijos narys mato, kad rinkėjas balsavo internetu) pažymima, kad rinkėjas atvyko į apylinkę, ir apie tai pranešama rinkimų apygardai. Rinkimų apygarda savo ruožtu informuoja VRK serverį, o šis anuliuoja rinkėjo e-balsą. Tokiu būdu užtikrinama, kad rinkėjas turėtų tik vieną balsą. Pasibaigus rinkimų dienai, biuleteniai ir paštu gauti vokai skaičiuojami įprasta tvarka, o VRK serveryje (e. balsadėžėje) esantys balsai atskiriami nuo rinkėjo tapatybės duomenų (išardomi bet kokie ryšiai), išrūšiuojami pagal apygardas ir iššifruojami. Šioje koncepcijoje, vadovaujantis teisinės valstybės principu, pabrėžiama, kad balsavimas internetu gali būti teismo pripažintas negaliojančiu, jei butų sukompromituotas bent vienas iš tokio balsavimo principų: slaptumas, skaidrumas, lygi rinkimų teisė ir kt.

Taigi LR Seimo nutarimu patvirtintoje „Balsavimo internetu rinkimuose ir referendumuose koncepcijoje“ glaustai, bet aiškiai išvardinti šio alternatyvaus balsavimo būdo principai ir apibrėžta principinė tokio balsavimo schema, kuri turėtų būti detalizuota rinkimus ir referendumus reglamentuojančiuose įstatymuose.

Balsavimo internetu diegimo programa. 2007 m. liepos 11 d. LR Vyriausybės nutarimu Nr. 759 patvirtinta Balsavimo internetu diegimo programa buvo skirta sukurti ir įdiegti balsavimo internetu sistemą. Programos įgyvendinimo koordinavimas pavestas Informacinės visuomenės plėtros komitetui prie LRV. Šios Programos tikslas – skatinti rinkėjus aktyviau dalyvauti Lietuvos Respublikoje vykstančiuose rinkimuose ir referendumuose, pasiūlius naujas balsavimo formas, pagrįstas naujomis informacijos ir ryšių technologijomis. Tuo pačiu iškelti pagrindiniai Programos

uždaviniai: sukurti ir įdiegti balsavimo internetu informacinę sistemą ir surengti balsavimo internetu informacinę kampaniją. 2007-2008 m. Programos įgyvendinimui planuota skirti 2 mln. lt. 2009 m. Valstybės kontrolė, atlikusi Vyriausiosios rinkimų komisijos informacinių sistemų valdymo auditą, konstatavo, kad iki 2010 m. buvo išleista 650 tūkst. Lt. balsavimo internetu informacinės sistemos įsteigimo ir bandomosios sistemos versijos įsigijimo dokumentacijai parengti. 2010 m. visai sistemai įdiegti prognozuota išleisti iki 12 mln. Lt. Audito metu nustatyta, kad nei Vyriausioji rinkimų komisija, nei Informacinės visuomenės plėtros komitetas, įgyvendindami Balsavimo internetu diegimo programą, neįvertino būsimos informacinės sistemos kainos ir naudos santykio. Todėl buvo nustatyta rizika, kad išleistos lėšos nesumažins rinkimams organizuoti skirtų išlaidų, o galbūt jas net padidins. Balsavimo internetu sistema iki šiol nėra sukurta ir įdiegta, todėl ši Programa taip ir liko neįgyvendinta.

Rinkimų įstatymų pakeitimų projektai. 2007 m. liberalioms politinėms partijoms atstovaujantys LR Seimo nariai užregistravo Seimo rinkimų įstatymo, Prezidento rinkimų įstatymo, Rinkimų į Europos Parlamentą įstatymo ir Referendumo įstatymo pataisas (Nr. XP-2193/2196). Įstatymų projektuose balsavimo būdo ir balso įskaitymo prioritetai didėjimo tvarka dėstomi taip: balsavimas paštu – balsavimas internetu – balsavimas apylinkėse. Toks prioritetų nustatymas pirmiausiai buvo nulemtas dažnai pasitaikančios balsų papirkinėjimo balsuojant paštu praktikos. Autorių nuomone, suteikus balsavimui internetu aukštesnį prioritetą, bandymai neteisėtai paveikti paštu balsuojančius rinkėjus netektų prasmės, kadangi jų balsavimas galės būti pakeistas jiems balsuojant internetu. Projektuose taip pat siūloma nustatyti, jog vykstant internetiniam balsavimui rinkėjas internetu gali balsuoti kelis kartus, tačiau turi būti skaičiuojamas tik vėliausiai gautas jo balsas. Sudarius rinkėjui galimybę pakeisti savo balsavimą, naikinamos prielaidos internetu balsuojančių rinkėjų papirkinėjimui. Taip pat buvo siūloma įtvirtinti Vyriausiosios rinkimų komisijos teisę iki rinkimų dienos priimti sprendimą nutraukti balsavimą internetu ir anuliuoti jo metu gautus balsus, pripažinus, jog balsavimo internetu metu gauti duomenys buvo sunaikinti, sugadinti ar neteisėtai pakeisti. Tokios galimybės nustatymas leistų išvengti visų rinkimų rezultatų pripažinimo negaliojančiais dėl to, kad nėra galimybės nustatyti objektyvių balsavimo internetu rezultatų, bei neužkirs kelio internetu balsavusiems rinkėjams pareikšti savo valią įprastiniu būdu rinkimų dieną tais atvejais, kai dėl kokių nors priežasčių internetinio balsavimo sistema susikompromituoja. Įstatymų projektuose siūloma įtvirtinti reikalavimą, kad valdant informacinę sistemą, kurioje bus kaupiami, saugomi ir kitaip apdorojami balsavimo internetu metu gauti duomenys, būtų laikomasi elektroninės informacijos saugai keliamų reikalavimų. Taigi įstatymų pakeitimo įstatymų projektuose siūloma aiškiai apibrėžti balsavimo internetu schemą. Pagal siūlytą teisinį reguliavimą, internetu būtų balsuojama Vyriausiosios rinkimų komisijos interneto tinklalapyje. Balsavimo internetu metu gauti duomenys būtų kaupiami, saugomi ir kitaip

apdorojami VRK valdomos informacinės sistemos pagalba. Internetu galima būtų balsuoti pradedant 144 valandoms ir baigiant likus 79 valandoms iki balsavimo rinkimų apylinkėse pradžios. Pasibaigus balsavimo internetu laikui, nebūtų galima atlikti veiksmų, kuriais papildomi, panaikinami arba pakeičiami informacinėje sistemoje esantys duomenys. Rinkėjas internetu galėtų balsuoti kelis kartus, tačiau skaičiuojamas būtų tik vėliausiai gautas jo balsas. Pasibaigus balsavimo internetu laikui, Vyriausioji rinkimų komisija, pripažindama, kad nėra balsavimo internetu metu gautų balsų anuliavimo pagrindų, per 12 valandų priimtų sprendimą laikyti balsavimą internetu įvykusiu. Priėmusi tokį sprendimą VRK pagal rinkimų apylinkes ir diplomatines atstovybes, į kurių rinkėjų sąrašus įtraukti internetu balsavę rinkėjai, sudarytų internetu balsavusių rinkėjų sąrašus, kuriuos ne vėliau kaip iki balsavimo rinkimų dieną pradžios perduotų atitinkamoms apylinkių rinkimų komisijoms ir diplomatinėms atstovybėms. Balsavimo internetu metu bei jam pasibaigus, bet ne vėliau kaip likus 67 valandoms iki balsavimo rinkimų dieną pradžios, VRK galėtų priimti sprendimą nutraukti balsavimą internetu ir anuliuoti jo metu gautus balsus arba, jei balsavimas internetu yra pasibaigęs, anuliuoti balsavimo internetu metu gautus balsus, jei pripažintų, jog balsavimo internetu metu gauti duomenys buvo sunaikinti, sugadinti ar neteisėtai pakeisti. Įgyvendinant teisinės valstybės principą, numatyta, kad partijos, iškėlusios kandidatus, Vyriausiosios rinkimų komisijos sprendimą laikyti balsavimą internetu įvykusiu arba sprendimą, kuriuo anuliuojami balsavimo internetu metu gauti balsai, ne vėliau kaip per 24 valandas nuo jo priėmimo, bet ne vėliau kaip likus trims dienoms iki rinkimų dienos, galėtų apskųsti Lietuvos vyriausiajam administraciniams teismui. Šie įstatymų projektai, po svarstymų Seimo komitetuose ir plenariniame posėdyje, 2008 m. sausio 17 d. buvo atmesti.

2009 m. spalio 15 d. LR Vyriausybė pateikė Vidaus reikalų ministerijos parengtus atitinkamų įstatymų pakeitimo įstatymų projektus (Nr. XIP-1155/1159). Juose beveik identiškai atkartojamos pirmojo pasiūlymų paketo nuostatos. Papildomai siūloma patikslinti, kad balsuoti internetu turi teisę visi rinkėjai, patvirtinę jų asmens tapatybę elektroninėje erdvėje. Šie projektai buvo grąžinti iniciatoriams tobulinti dar pateikimo stadijoje. 2010 m. birželio 19 d. tos pačios LR Vyriausybės susisiekimo ministro teikimu buvo užregistruoti patobulinti tų pačių įstatymų pakeitimo įstatymų projektai (Nr. XIP-1155(2)/1159(2)). Šiuose projektuose atsisakoma vienos iš pagrindinių balsavimo internetu idėjų – galimybės balsuoti bet kurioje Lietuvos ar pasaulio vietoje. Projektuose siūloma nustatyti, kad balsuoti internetu rinkėjas galėtų bet kurioje *rinkimų apylinkėje*. Balsuoti būtų galima iš anksto (paskutinį trečiadienį ir ketvirtadienį iki rinkimų dienos) ir rinkimų dieną. Siūlyta nustatyti, kad internetu balsuojama iš anksto parengtose ir balsavimui tinkamose patalpose, esančiose pastate, kuriame yra savivaldybės, kurios teritorijoje yra rinkimų apygarda, mero (administracijos direktoriaus) darbo vieta ir rinkimų apylinkės balsavimo patalpoje, laive ar diplomatinėje ir konsulinėje įstaigoje, taip pat nustatyti, kad internetu balsuojama Vyriausiosios

rinkimų komisijos nustatytus reikalavimus atitinkančioje balsavimo kabinoje. Balsuoti internetu ne balsavimo kabinoje būtų draudžiama. Atkreiptinas dėmesys, kad 2010 m. dar nebuvo galimybės balsuoti ne savo rinkimų apylinkėje (rinkimų dieną), todėl tai buvo naujovė. Toks balsavimo internetu įteisinimas, kuomet balsuojama tik tam tikrose specialiai tam skirtose kontrolinėse patalpose ir tik tam tiktu laiku, būtų tarpinis žingsnis link visiško balsavimo internetu įteisinimo. Tokiu būdu tikėtasi išspręsti išankstinio balsavimo metu susidarančių eilių problemą ir po truputį pratinti visuomenę prie naujo balsavimo būdo. Po pateikimo LR Seimo plenariniame posėdyje projektai vėl buvo grąžinti iniciatoriams tobulinti. 2011 m. birželio 20 d. projektai buvo atsiimti LR Vyriausybės nutarimu.

2010 m. gruodžio 23 d. keli LR Seimo nariai, daugiausiai LR Seimo ir Pasaulio lietuvių bendruomenės komisijos nariai, įregistravo atitinkamų įstatymų pakeitimo įstatymų projektus (Nr. XIP-2794/2797), kuriuose siūloma suteikti balsavimo internetu galimybę *tik užsienyje esantiems LR piliečiams.* Siūlyta nustatyti, kad balsavimas internetu prasidėtų 9 valandą, likus 5 dienoms iki rinkimų dienos, ir baigtųsi 24 valandą, likus 3 dienoms iki rinkimų dienos. Balsavimas vyktų VRK interneto svetainėje. Kitos nuostatos (dėl galimybės balsuoti ne tik internetu, dėl balsų skaičiavimo) siūlomos tokios pačios, kaip ir ankstesniuose projektuose. Seimo Valstybės valdymo ir savivaldybių komitetas, kaip pagrindinis komitetas, atsižvelgdamas į papildomų Seimo komitetų (Teisės ir teisėtvarkos komiteto, Užsienio reikalų komiteto, Biudžeto ir finansų komiteto, Informacinės visuomenės plėtros komiteto), Seimo kanceliarijos Teisės departamento, Europos teisės departamento ir kitų ekspertų išvadas ir pasiūlymus, nutarė įstatymo projektus atmesti, nes jie galimai prieštarauja konstituciniam lygios rinkimų teisės principui, kuris reiškia, kad „organizuojant ir vykdant rinkimus visi rinkėjai turi būti traktuojami vienodai, kiekvieno rinkėjo balsas yra lygiavertis bet kurio kito rinkėjo balsui ir turi vienodą reikšmę nustatant balsavimo rezultatus". Projektams aiškia balsų persvara buvo nepritarta ir LR Seimo plenariniame posėdyje 2012 m. rugsėjo 25 d.

2011 m. gegužės 24 d. LR Seimo narys A. Valinskas užregistravo dar vieną atitinkamų įstatymų pakeitimo įstatymų projektų paketą (Nr. XIP-3248/3252). Juose numatytos nuostatos tapačios 2007 m. pateiktiems projektams ir atitinka Balsavimo internetu rinkimuose ir referendumuose koncepcijos nuostatas. Projektams buvo pritarta po pateikimo, tačiau dauguma papildomų komitetų siūlė juos atmesti. Pagrindinis Valstybės valdymo ir savivaldybių komitetas taip ir nepateikė išvados dėl šių įstatymų projektų.

2014 m. gegužės 21 d. LR Seimo nariai ir ministrai Juozas Bernatonis ir Evaldas Sinkevičius užregistravo dar vieną įstatymų pakeitimų paketą dėl balsavimo internetu įteisinimo (Nr. XIIP-1835/1839). Juose atsispindi tos pačios nuostatos, kaip ir ankstesniuose projektuose bei Balsavimo internetu rinkimuose ir referendumuose koncepcijoje. Nauja yra tik nuostata, kad daryti

poveikį rinkėjui, jo apsisprendimui ar skubinti jį balsuoti internetu, draudžiama. Šie įstatymų pakeitimo įstatymų projektai dar nėra pradėti svarstyti Seime, t.y. nėra įvykęs pateikimas plenariniame posėdyje.

Apibendrinant interneto rinkimų teisinį reglamentavimą galima teigti, kad šiuo metu valdžios institucijos tik deklaruoja ketinimą įteisinti interneto rinkimus Lietuvoje. 2006 metais priimta koncepcija apibrėžia interneto rinkimų įteisinimo gaires, tačiau LR Seimui pateikti rinkimų įstatymų pakeitimų įstatymų projektai taip ir nebuvo pabaigti svarstyti.

2.5. Esamos padėties analizė ir perspektyvos Lietuvoje

Prieš kuriant interneto rinkimų modelį, svarbu išsiaiškinti esamą padėtį Lietuvoje. Šiam tikslui naudojama SSGG analizė (Kotler, Keller, 2007). 1 lentelėje išskirtos interneto rinkimų kibernetinio saugumo Lietuvoje stiprybės, silpnybės, galimybės ir grėsmės.

1 lentelė. **„Interneto rinkimų kibernetinio saugumo Lietuvoje SSGG analizė“**

STIPRYBĖS	**SILPNYBĖS**
1. Priimtas kibernetinio saugumo įstatymas; 2. Žinyboms padalintos kibernetinio saugumo atsakomybės sferos; 3. Tarpinstitucinis bendradarbiavimas; 4. Elektroninis rinkėjų registras	1. Nepakankamas susidirbimas tarp kibernetinę erdvę saugančių žinybų; 2. Nepriimti visi poįstatyminiai teisės aktai 3. Nacionalinis kibernetinio saugumo centras kol kas dirba ne visu pajėgumu; 4. Visuomenės abejingas požiūris į kibernetinį saugumą.
GALIMYBĖS	**GRĖSMĖS**
1. Perimti patirtį iš kitų šalių, jau įgyvendinusių balsavimą internetu; 2. Vykdyti nuolatinį visuomenės švietimą kibernetinio saugumo srityje; 3. Taikyti naujausius saugumo sprendimus.	**1.** Užsienio valstybių kibernetinių išpuolių grėsmė; **2.** Kibernetinės atakos prieš rinkimų sistemą ir rinkėjus; **3.** Grėsmė sumenkinti visuomenės pasitikėjimą valstybe.

Šaltinis: sudaryta autoriaus

Stiprybės. Viena iš didžiausių stiprybių galima įvardinti 2014 m. gruodžio 11 d. priimtą LR kibernetinio saugumo įstatymą, kuris nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžia kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetencijas, funkcijas, teises ir pareigas, valstybės informacinių išteklių valdytojų ir tvarkytojų, ypatingos svarbos infrastruktūros valdytojų, viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų

pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones. Įstatymas taip pat reglamentuoja tarpinstitucinį bendradarbiavimą tiriant kibernetinius incidentus bei sukuria saugią mainų platformą, kurios paskirtis yra dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir bendradarbiavimą tarp kibernetinio saugumo informacinio tinklo narių kibernetinio saugumo srityje. Neabejotina stiprybė yra jau dabar veikiantis elektroninis rinkėjų registras.

Silpnybės. Kibernetinio saugumo įstatymu (2014) buvo nustatytas kibernetinio saugumo sistemos organizavimas, valdymas ir kontrolė, tačiau pačioms organizacijoms tai vis dar yra nauja sritis. Lietuvoje labai trūksta šios srities specialistų, o esamo personalo mokymai reikalauja nemažai finansinių ir laiko sąnaudų. Kibernetinę erdvę saugančioms žinyboms taip pat reikalingas susidirbimas, kuriam būtini kompleksiniai mokymai. Lietuvoje iki šiol nebuvo didelio masto kibernetinių incidentų, todėl nėra žinoma, kaip suveiktų šalies gynybiniai pajėgumai. Šiuo metu net nėra rekomendacijų, kaip elgtis įvykus kibernetiniam išpuoliui.

Galimybės. Įgyvendindama interneto rinkimus, Lietuva turi galimybę perimti patirtį iš kitų šalių, jau įgyvendinusių šį balsavimo būdą. Vienas iš puikiausių pavyzdžių yra kaimynė Estija, kur balsuoti internetu galima net nuo 2005 metų. Pasinaudojus gerosiomis praktikomis, būtina nustatyti saugumo politikas, sukurti reagavimo į kibernetinius incidentus planus, paskirstyti atsakomybes. Taip pat vykdyti nuolatinį visuomenės švietimą kibernetinio saugumo srityje, rengti reagavimo į kibernetines atakas pratybas, stebėti pasaulines kibernetinio saugumo tendencijas bei esamomis sistemoms taikyti naujausius saugumo sprendimus.

Grėsmės. 2006 metų balsavimo internetu rinkimuose ir referendumuose koncepcijoje nurodytos kelios galimos grėsmės elektroninėms balsavimo sistemoms: technologinis, žmogiškasis faktorius bei nepalanki visuomenės nuomonė. Tačiau, atsižvelgus į šiandienines tendencijas, neatmetama galimybė, kad interneto rinkimai gali tapti nedraugiškų užsienio valstybių taikiniu. Taip pat galimos atakos prieš rinkėjus pasinaudojus socialine inžinerija. Nekontroliuojamą balsavimo aplinką gali bandyti išnaudoti balsų pirkėjai.

Apibendrinant, galima pastebėti, kad kibernetinio saugumo valdymo stiprybės Lietuvoje yra susijusios su kibernetinio saugumo įstatymo priėmimu, kurio pagrindu įkurtas Nacionalinis kibernetinio saugumo centras, valstybės institucijoms paskirstytos atsakomybės sferos bei numatytas tarpinstitucinis bendradarbiavimas. Tačiau dėl laiko stokos išryškėja silpnybės: Nacionalinis kibernetinio saugumo centras dar nedirba pilnu pajėgumu, nepakankamas „susidirbimas“ tarp kibernetinę erdvę saugančių institucijų, nepriimti visi reikalingi poįstatyminiai teisės aktai. Tai nuteikia optimistiškai, nes laikui bėgant šios silpnybės taps stiprybėmis. Tačiau abejingą visuomenės požiūrį į kibernetinį saugumą pakeisti nebus taip lengva. Lietuva turi geras

galimybes perimti interneto rinkimų patirtį iš kitų šalių, vykdyti nuolatinį visuomenės švietimą, taikyti naujausius saugumo sprendimus, tačiau kyla grėsmė, kad, įvykus kibernetiniam išpuoliui prieš elektroninę balsavimo sistemą ar rinkėjus, gali kilti visuomenės nepasitikėjimas valstybe bei jos institucijomis. Nekontroliuojama balsavimo aplinka gali pasinaudoti balsų pirkėjai.

3. KIBERNETINIO SAUGUMO VALDYMO YPATUMŲ VERTINIMAS DIEGIANT INTERNETO RINKIMUS LIETUVOJE

3.1. Tyrimo metodologija

Tyrimui buvo pasirinkta **kokybinio tyrimo metodologijos pusiau struktūrizuotas ekspertinio interviu metodas.** Tai specifinis apklausos metodas, kurio metu apklausiama iš anksto parinkta žmonių grupė, turinti tam tikros srities, tyrimui reikalingų žinių.

Pusiau struktūruotas interviu remiasi planu, kuriame numatyti konkretūs klausimai, jų pateikimo seka, tačiau numatyta, kad tyrimo eigoje tyrėjas gali papildomai užduoti plane neįrašytų klausimų. Papildomus klausimus tyrėjas užduoda esant skirtingoms situacijoms (Morkevičius, Telešienė, Žvaliauskas, 2008):

- *kai interviu metu pastebi, jog numatytieji klausimai nepadengia visų tyrimui svarbių temų;*
- *siekiant surinkti daugiau ar gilesnės informacijos tuomet, kai tiriamasis nepilnai atsako į pateiktuosius klausimus;*
- *kai pastebi, jog tiriamajam nepatogu (jis nenori) atsakinėti į pateiktąjį klausimą – tuomet tyrėjas stengiasi tą pačią informaciją gauti paklausdamas kitaip ar trumpam nukreipdamas tiriamojo dėmesį į kitus, mažiau jautrius klausimus, ir sugrįždamas prie jautraus klausimo kita formuluote.*

Tyrimo organizavimas

Tyrimas buvo atliekamas 2015 m. lapkričio 12 - 20 dienomis.

Šiuo metu Lietuvoje nėra interneto rinkimų kibernetinio saugumo valdymo specialistų, todėl tyrimas buvo atliekamas apklausiant dviejų sričių ekspertus. Buvo apklausiami interneto rinkimų ir kibernetinio saugumo ekspertai, kuriems buvo pateikiami skirtingi klausimai. Interneto rinkimų specialistų buvo klausiama apie balsavimo internetu saugumo problematiką. Kibernetinio saugumo specialistų buvo klausiama, kaip spręsti iškilusias kibernetinio saugumo problemas.

Interneto rinkimų ekspertai:

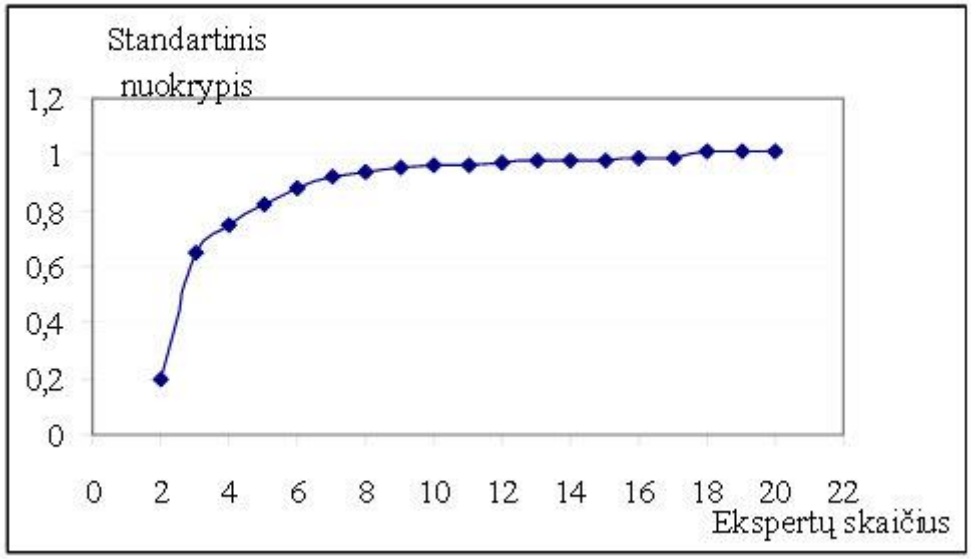
- VRK pirmininkas Zenonas Vaigauskas;
- VRK pirmininko pavaduotoja Laura Matjošaitytė;
- VRK narys Jonas Udris;
- LR Seimo Parlamentinių tyrimų departamento vyr. specialistas Mindaugas Skačkauskas;
- VRK Kompiuterinių technologijų skyriaus vedėja Jurga Augustaitytė;
- „Elektroninio balsavimo studijos“ vadovė, politikos mokslų prof. dr. Ainė Ramonaitė.

Kibernetinio saugumo ekspertai:

- LR Seimo Informacijos technologijų ir telekomunikacijų departamento direktorius Jurgis Bridžius;
- LR Seimo Informacijos sistemų diegimo ir saugos skyriaus vedėjas Rimantas Paliušis;
- VRK Kompiuterinių technologijų skyriaus vedėja Jurga Augustaitytė;
- Nacionalinio kibernetinio saugumo centro darbuotojas Nr. 1;
- Nacionalinio kibernetinio saugumo centro darbuotojas Nr. 2;
- Nacionalinio kibernetinio saugumo centro darbuotojas Nr. 3.

Nacionalinio kibernetinio saugumo centro darbuotojai pageidavo, kad jų tapatybė nebūtų atskleista dėl vidinių centro nuostatų.

Nustatant pasirinktą ekspertų skaičių buvo pasiremta klasikinėje testų teorijoje suformuotomis metodologinėmis prielaidomis, kuriomis teigiama, kad agreguotų sprendimų patikimumą ir priimančių sprendimą (šiuo atveju ekspertų) skaičių sieja greitai gęstantis netiesinis ryšys (Baležentis, Žalimaitė, 2011).



Šaltinis: Baležentis, Žalimaitė, 2011

11 pav. **Ekspertų vertinimo standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus**

Pagal pateiktą grafiką (11 pav.) matome, kad 7 ekspertų vertinimo tikslumas yra pakankamai tikslus. Toliau daugėjant informantų skaičiui vertinimo tikslumas kyla labai nežymiai. Todėl galima daryti prielaidą, kad tyrimo patikimumas yra pakankamas.

Tyrimo tikslas - pasitelkiant ekspertų žinias, išsiaiškinti interneto rinkimų kibernetinio saugumo problematiką bei pateikti galimus identifikuotų problemų sprendimo būdus.

Tyrimo uždaviniai:

- Išsiaiškinti interneto rinkimų Lietuvoje problematiką.
- Aptarti pasaulyje naudojamas interneto rinkimų sistemas bei sužinoti ekspertų nuomonę apie interneto rinkimų modelių taikymo galimybes Lietuvoje.
- Aptarti interneto rinkimų etapus ir identifikuoti problemines saugumo vietas.
- Sužinoti kibernetinio saugumo ekspertų nuomonę apie identifikuotas problemas ir aptarti galimus jų sprendimo būdus.
- Išsiaiškinti kibernetinio saugumo ekspertų nuomonę apie interneto rinkimų kibernetinio saugumo valdymo probleminius aspektus.

Tyrimo objektas – interneto rinkimų kibernetinio saugumo valdymo ypatumai.

3.2. Tyrimo duomenų analizė

Interneto rinkimų problematika. Trys iš keturių interneto rinkimų ekspertų teigė, kad Lietuvoje interneto rinkimai yra neįteisinti daugiausiai dėl „*politinės valios trūkumo*“. Buvo parengtas ne vienas įstatymų pakeitimų įstatymų projektas, siūlantis įteisinti balsavimą internetu Prezidento, LR Seimo, savivaldybių tarybų, Europos Parlamento rinkimų bei referendumų metu, tačiau visi buvo „nugesinti“ LR Seime. Tačiau M. Skačkauskas ir J. Augustaitytė nelinkę sutikti su šia nuomone. Ekspertai teigia, kad šiuo metu didžiausia interneto rinkimų problema yra neaiškumas. LR Seimui siūlomuose įstatymų pakeitimų įstatymų projektuose dėl galimybės balsuoti internetu rinkimuose ir referendumuose iš esmės numatyta, kad balsavimas internetu neribos rinkėjų teisių balsuoti tradiciniais būdais ir atitiks visus teisės aktų nustatytus balsavimo principus ir reikalavimus, rinkėjas internetu galės balsuoti kelis kartus, tačiau bus skaičiuojamas tik vėliausiai gautas rinkėjo balsas (įstatymų projektai XIIP – 1835/1839). Kaip vyks visas interneto rinkimų procesas nėra aišku iki šiol. Ekspertai teigė, kad prieš įteisinant balsavimą internetu turėtų būti užtikrinamas visiškas aiškumas, kokio pobūdžio sistema bus įgyvendinama. Taip pat ekspertai rekomendavo, jog įstatymuose būtų aiškiau įvardinami ir detalizuojami sistemos veikimo principai bei pagrindinės savybės, užtikrintas aiškus atsakomybių pasiskirstymas tarp susijusių institucijų ir numatyti išorinės kontrolės mechanizmai, kurie užtikrintų kompetentingus ir nepriklausomus kokybės patikrinimus. Kiti ekspertai pastebi, kad susidaro įspūdis, jog interneto rinkimus politikai naudoja kaip politinę reklamą, tačiau norint įgyvendinti interneto rinkimus Lietuvoje neužtenka vien inicijuoti įstatymų pakeitimus – būtina atlikti daug „*techninio*“ darbo. VRK Kompiuterinių technologijų skyriaus vedėja teigia, kad informacinėse sistemose neįmanoma užtikrinti 100 proc. saugumo – dėl to turi būti atliktas išsamus rizikų vertinimas bei nustatyta toleruojama rizika. Iki šiol Lietuvoje neatlikta interneto rinkimų rizikos analizė. Interneto rinkimų toleruojama rizika turi būti

suderinama su visuomene. Apie visuomenės įtraukimą į interneto rinkimų procesą užsiminė ir A. Ramonaitė. Dėl ypatingos specifikos, interneto rinkimų stebėtojais gali būti tik informacinių technologijų specialistai. Profesorė pabrėžė, kad dėl šios priežasties interneto rinkimai yra ypač priklausomi nuo visuomenės pasitikėjimo. Todėl būtina rengti įvairias diskusijas, konferencijas interneto rinkimų tema. A. Ramonaitė prisiminė atsitikimą, kai per LR Prezidento rinkimus rungėsi K. Prunskienė ir V. Adamkus. Tuomet visuomenė apie rezultatus buvo informuojama per televiziją (besikeičiantys rezultatai buvo matomi ekrano apačioje). Skaičiuojant balsus, iš pradžių užtikrintai pirmavo K. Prunskienė ir tada dėl techninių kliūčių apie porą valandų rezultatai nebuvo atnaujinami. Kai kliūtys buvo pašalintos, jau užtikrintai pirmavo V. Adamkus. VRK pirmininkas teigia, kad iki šiol yra manančių, jog tuo metu buvo „*sufabrikuoti*“ rinkimų rezultatai, tačiau tiesa ta, kad V. Adamkų labiau palaikė didieji miestai, kurių rinkimų apylinkės yra didelės ir rezultatai ateina vėliau. Tai dar kartą įrodo, koks svarbus visuomenės pasitikėjimas.

Apibendrinant ekspertų atsakymus į pirmąją klausimų dalį, galima daryti prielaidą, kad interneto rinkimai Lietuvoje neįteisinti dėl keturių pagrindinių aspektų:

- LR Seimo narių politinės valios trūkumo – nepriimti įstatymų pakeitimai;
- Nėra bendro sutarimo, kaip turėtų atrodyti interneto rinkimų mechanizmas;
- Neatliktas rizikų vertinimas, nenustatyta toleruojama rizika;
- Nepakankamas visuomenės įtraukimas į interneto rinkimų įgyvendinimą. Trūksta visuomenės informavimo interneto rinkimų tema (diskusijų, konferencijų).

Interneto rinkimų modelių taikymo galimybės Lietuvoje. VRK Kompiuterinių technologijų skyriaus vedėja Jurga Augustaitytė pabrėžė, kad neabejotinai svarbu, jog balsavimas internetu būtų įterptas į visą Lietuvoje veikiančią rinkimų sistemą kaip vientisas darinys. Tai būtina sąlyga siekiant sukurti gerai veikiantį, nenutrūkstamą balsavimo procesą. Interneto rinkimų ekspertų nuomonės išsiskyrė ir dėl galimo interneto rinkimų modelio Lietuvoje taikymo galimybės. VRK narys J. Udris vienintelis užtikrintai siūlė Lietuvoje pasinaudoti „Scytl“ teikiamomis galimybėmis. Ekspertas išskyrė „Scytl“ interneto modelio privalumus: galima įdiegti skirtingus rinkėjo asmenybės nustatymo mechanizmus, yra lengvai suderinamas su Google, Android, Blackberry ir Apple IOS operacinėmis sistemomis bei užtikrina tą patį saugumo lygį, kaip ir naudojantis asmeniniu kompiuteriu. Tačiau kiti ekspertai atsargiau šnekėjo apie J. Udrio propaguojamą modelį. M. Skačkauskas, kaip labiausiai Lietuvai tinkantį, išskyrė „Cybernetica“ rinkimų modelį. Estijoje šis modelis puikiai tiko dėl gerai išvystytos elektroninio parašo infrastruktūros. Tuo tarpu Lietuvoje, nors ir didžioji dalis gyventojų turi elektroninį parašą asmens tapatybės kortelėje, retas naudojasi šia galimybe. Likę 5 ekspertai negalėjo pasakyti, kokį interneto rinkimų modelį geriausiai būtų taikyti rinkimams ir referendumams Lietuvoje. J. Augustaitytė mano, kad LR Seimui priėmus atitinkamus įstatymus, greičiausiai VRK organizuotų konkursą, kuriame galėtų dalyvauti įvairios įmonės. Tokiu

atveju, greičiausiai, interneto rinkimų organizavime dalyvautų ne viena įmonė. Ekspertai pabrėžia, kad kuriant Lietuvos interneto rinkimų modelį, būtina aiškiai nustatyti reikalavimus, atitinkančius Lietuvos Respublikos įstatymus bei viešojo administravimo specifiką.

Apibendrinant galima teigti, kad interneto rinkimų specialistai nesutaria, kokį rinkimų modelį reikėtų pasirinkti įgyvendinant interneto rinkimus Lietuvoje. Ekspertai siūlė pasinaudoti „Scytl“ ir Estijoje naudojamu „Cybernetica“ modeliais. Taip pat buvo manančių, kad Lietuva, pasinaudodama pasaulinėmis praktikomis, turėtų susikurti savo interneto rinkimų modelį, kuris būtų pritaikytas prie Lietuvos teisinės bazės bei viešojo administravimo specifikos.

Probleminės interneto rinkimų saugumo vietos. Vienos iš svarbiausių sąlygų, vykdant interneto rinkimus, yra užtikrinti, kad balsuoti galėtų tik teisę tam turintys Lietuvos piliečiai ir kad balsuojantis asmuo yra tas, kas iš tikrųjų yra. VRK pirmininkas Z. Vaigauskas teigia, kad interneto rinkimai labai panašūs į išankstinį balsavimą (balsavimą paštu). „*Rinkėjo tapatybė turi būti tiksliai nustatyta, bet negali būti susieta su jo balsu - tam naudojamas dvigubo voko principas. Į vidinį voką įdedamas rinkėjo balsas, o išoriniame voke pridedama rinkėjo tapatybė. Viskas užklijuojama, užantspauduojama ir siunčiama į rinkimų apylinkę“*. Rinkimų apylinkė atplėšia išorinį voką, randa tapatybę ir rinkėjų sąraše tikrina, ar rinkėjas balsavo. Taip pat tikrinama, ar rinkėjas priklauso tai apylinkei, kur balsavo, ar nėra balsuota antrą kartą. Kai viskas patikrinama, rinkėjų sąraše pažymima, kad rinkėjas balsavo, o vidinis vokas įmetamas į balsadėžę prie kitų vokų ir sumaišomas. Visi šie principai turi išlikti ir balsuojant internetu panaudojant kriptografines priemones. Visi kalbinti interneto rinkimų ekspertai vieningai pasisakė prieš elektroninės bankininkystės sistemos naudojimą interneto rinkimuose Lietuvoje. VRK pirmininkas pabrėžė, kad konfidencialumas banke suprantamas kaip informacijos apsauga nuo trečiųjų asmenų. Tuo tarpu bankas žino ir mato visus savo klientų žingsnius. Slaptas balsavimas remiasi tuo, kad sistema nežino, kaip balsavo rinkėjas. Ji žino, kad buvo balsuota, bet už kurią partiją ar už kurį kandidatą balsuota – nežino. Pasak VRK pirmininko, tai yra „žymiai aukštesnis sistemos slaptumo lygmuo“. Ekspertai teigė, kad rinkėjo asmens tapatybė Lietuvos interneto rinkimuose galėtų būti nustatoma pasinaudojant elektroniniu parašu, mobiliuoju parašu. Išsiskyrė ekspertų nuomonė dėl asmens tapatybės kortelės panaudojimo galimybės. Trys iš septynių ekspertų teigė, kad tai yra nepavykęs projektas. Tačiau neneigė, kad tai saugus būdas tiek identifikuoti tapatybę, tiek balsuoti. Tuo tarpu kiti trys teigė, kad būtina rinkėjams pateikti kuo platesnį pasirinkimą, svarbu, kad tai būtų saugu ir patikima.

Ekspertai kaip probleminį klausimą paminėjo rinkėjo galimybę pasitikrinti savo atiduotą balsą. Ši galimybė numatyta rinkimų įstatymų pakeitimų įstatymų projektuose. VRK narys J. Udris teigė, kad šiuo metu geriausią balso patikrinimo metodą taiko „Scytl“ interneto rinkimų modelis. Rinkėjas, atlikęs kelis veiksmus, gali sužinoti, ar jo balsas buvo įskaitytas bei įskaitytas

kaip numatytas. Z. Vaigauskas ir M. Skačkauskas paminėjo Estijos interneto rinkimų modelyje naudojamą balso patikrinimo metodą. Tačiau J. Udris šį metodą sukritikavo dėl balsavimo turinio atskleidimo, kas suteikia galimybę parduoti balsą.

A. Ramonaitė nuogąstavo, kad balsavimas internetu suteiks dar vieną galimybę pirkti/parduoti balsus. Tuo tarpu kiti ekspertai pastebėjo, kad balsų pirkimas vyksta jau ne vienerius metus, tuo tarpu galimybė balsuoti „n“ kartų internetu, o vėliau dar ir rinkimų dieną rinkimų apylinkėje, eliminuotų papirkimo galimybę.

Apibendrinant galima daryti išvadą, kad yra penki pagrindiniai interneto rinkimų probleminiai taškai: rinkėjo registracija ir asmens tapatybės elektroninėje erdvėje nustatymas, galimybė rinkėjui pasitikrinti savo balsą, atsirandanti papildoma galimybė papirkti rinkėjus ir interneto rinkimų audito problematika.

Kibernetinio saugumo ekspertai, paklausti apie *interneto rinkimų kibernetinio saugumo valdymo problematiką,* vieningai pabrėžė, kad šiuo metu, nepažeidžiant rinkėjo privatumo, neįmanoma užtikrinti interneto rinkimams naudojamo rinkėjo įrenginio saugumo. Ekspertai pastebi, kad dar dažnas Lietuvos pilietis asmeniniame kompiuteryje naudoja „piratinę“ programinę įrangą, neturi „palaikomos“ antivirusinės programos. Nacionaliniame kibernetinio saugumo centre dirbantis ekspertas pasijuokė, kad yra žmonių, kurie bandydami „*jaustis saugiau*“ įsidiegia „piratines“ antivirusines programas, kurios nėra atnaujinamos ir negali atpažinti naujausių virusų. Sprendžiant nesaugaus rinkėjo įrenginio problemą, keli ekspertai siūlė, diegiant interneto rinkimų programą, įdiegti Java skribtą (angl. Java script), kuris balsavimo metu blokuotų kitas programas. Tačiau kiti pastebėjo, kad tai galėtų pažeisti rinkėjo privatumą. Ekspertai pateikė rekomendacijas rinkėjui, kuriomis jis turėtų vadovautis balsuojant internetu:

- Interneto rinkimų adresą rašyti ranka (spaudžiant nuorodą galima „pakliūti” į socialinės inžinerijos paspęstus spąstus);
- Įsitikinti, kad jungiantis naudojamas saugus šifruotas HTTPS ryšys;
- Patikrinti, ar galioja svetainės apsaugos sertifikatas.

Kibernetinio išpuolio galima tikėtis ir rinkėjui komunikuojant su elektronine rinkimų sistema. Visi ekspertai rekomendavo naudoti tik saugų šifruotą kanalą, kuris garantuotų siunčiamų duomenų konfidencialumą bei vientisumą.

LR Seimo kanceliarijos Informacijos technologijų ir telekomunikacijų departamento direktorius J. Bridžius teigia, kad, visų pirma, visa interneto rinkimų informacinės sistemos programinė įranga privalo būti sertifikuota. Siekiant užtikrinti elektroninės informacinės sistemos apsaugą būtina parengti bei vadovautis:

- Saugos nuostatus;
- Saugaus elektroninės informacijos tvarkymo taisykles;

- Informacinės sistemos veiklos tęstinumo valdymo planą;
- Informacinės sistemos naudotojų administravimo taisykles.

Nacionalinio kibernetinio saugumo centro darbuotojai, diegiant saugią informacinės sistemos infrastruktūrą, komunikacijai su rinkėjais (nesaugia aplinka) rekomenduoja naudoti DMZ, kur komunikacija vykdoma tik iš vidaus.

Pasak kibernetinio saugumo specialistų, absoliutus saugumas egzistuoja tik teoriškai - net labiausiai apsaugotose sistemose visada išlieka klaidos ir įsilaužimo tikimybė, kurios neįmanoma eliminuoti. Todėl prieš diegiant rinkimų sistemą būtina atlikti išsamią rizikų analizę (nustatyti rizikas, tikimybę, kad ji įvyks, kokią žalą gali padaryti, kokie ištekliai reikalingi, norint sumažinti riziką ir pan.) bei nusistatyti toleruojamą riziką.

Apibendrinant galima konstatuoti, kad šiuo metu, nepažeidžiant asmens privatumo, nėra techninių galimybių užtikrinti rinkėjo įrenginio saugumą – galima tik pateikti rekomendacijas rinkėjui. Saugią komunikacijai tarp rinkėjo ir elektroninės balsavimo sistemos galima užtikrinti naudojant saugų šifruotą (TSL, SSL) ryšį. Elektroninės balsavimo sistemos apsaugai ekspertai rekomendavo taikyti technines, organizacines bei teisines saugumo priemones.

Tyrime gautų ekspertų atsakymų į pateiktus klausimus apibendrinimas pateiktas 2 lentelėje.

2 lentelė. **Ekspertų atsakymų į tyrimo klausimus apibendrinimas**

Klausimai	Ekspertų atsakymų apibendrinimai
Interneto rinkimų problematika	• Nepriimti įstatymų pakeitimų įstatymų projektai
	• Nėra bendro sutarimo, kaip turėtų atrodyti interneto rinkimų mechanizmas
	• Neatliktas rizikų vertinimas, nenustatyta toleruojama rizika
	• Nepakankamas visuomenės įtraukimas į interneto rinkimų įgyvendinimą. Trūksta visuomenės informavimo interneto rinkimų tema (diskusijų, konferencijų).
Interneto rinkimų modelių taikymo galimybės Lietuvoje	• Rinktis lengvai priderinamą „Scytl“ modelį
	• Remtis Estijos patirtimi, priderinant jų interneto rinkimų modelį Lietuvos rinkimams
	• Kurti savo interneto modelį, pasinaudojant geriausiomis užsienio praktikomis
Probleminės interneto rinkimų vietos	• Rinkėjo registracija
	• Asmens tapatybės nustatymas
	• Galimybė patikrinti balsą
	• Interneto rinkimų audito problematika
	• Rinkėjų papirkinėjimo galimybės
Interneto rinkimų kibernetinio saugumo valdymo problematika	• Nesaugus rinkėjo įrenginys
	• Saugios komunikacijos užtikrinimas
	• Saugi elektroninės informacinės sistemos infrastruktūra

Šaltinis: sudaryta autoriaus

4. INTERNETO RINKIMŲ MODELIO KŪRIMAS

4.1. Modeliavimo metodologija ir modelio analizė

Plikauskas (2011) modelį apibūdina kaip abstrakčią instrukciją, kuria mėginama atkartoti kai kurias realios sistemos savybes. Interneto rinkimų kibernetinio saugumo valdymo modeliui kurti buvo pasirinkta *procesų modelio* metodika.

Kuriant modelį pasirinktas į veiklas orientuotas požiūris – koncentruojamasi ties proceso veiklomis bei ryšius tarp jų. Kiti proceso elementai neapibrėžiami arba analizuojami proceso veiklų kontekste.

Modeliavimo tikslas – sukurti interneto rinkimų kibernetinio saugumo valdymo modelį.

Modeliavimo uždaviniai:

- Sukurti elektroninės balsavimo sistemos infrastruktūrą;
- Nubraižyti loginę balsavimo internetu schemą;
- Į gautą modelį integruoti kibernetinio saugumo valdymo priemones.

Prieš pradedant nagrinėti interneto rinkimų kibernetinio saugumo valdymo modelį**,** įsivaizduokime, kad internetu balsuojančio asmens įrenginys turi legalią, reguliariai atnaujinamą operacinę sistemą su legaliomis bei gamintojo palaikomomis programomis. Įrenginys yra saugiai sukonfigūruotas, įdiegta gera kiekvieną dieną atnaujinama antivirusinė programa ir t.t. Tačiau, kaip teigė Nacionalinio kibernetinio saugumo centro ekspertas – yra žmonių, kurie bandydami „*jaustis saugiau*“ įsidiegia „piratines“ antivirusines programas.

Pradedant modelio analizę, prisiminkime kibernetinio saugumo ekspertų pateiktas rekomendacijas, kurios galėtų padėti išvengti socialinės inžinerijos paspęstų spąstų:

- Interneto rinkimų adresą rašyti ranka;
- Įsitikinti, kad jungiantis naudojamas saugus šifruotas HTTPS ryšys;
- Patikrinti, ar galioja svetainės apsaugos sertifikatas.

Pagal sukurtą interneto rinkimų kibernetinio saugumo valdymo modelį (žr. 12 pav.), rinkėjas, pasinaudodamas savo turimu įrenginiu, darbo vieta, viešųjų bibliotekų teikiamomis interneto paslaugomis ar kitomis vietomis, kur galima pasinaudoti interneto ryšį turinčiu įrenginiu, saugiu (TSL) ryšiu prisijungia prie elektroninės balsavimo svetainės. Rinkėjas atsisiunčia interneto balsavimui skirtą programėlę bei įsidiegia ją į naudojamą įrenginį. Pasinaudodamas mobiliuoju parašu ar kitu saugiu elektroniniu parašu, patvirtina savo asmens tapatybę ir registruojasi elektroninėje balsavimo sistemoje.

Elektroninė balsavimo sistema, saugumo sumetimais, su išorine (nesaugia) aplinka komunikuoja tik per demilitarizuotą zoną (DMZ). Visa komunikacija vyksta tik iš vidaus. Kitaip

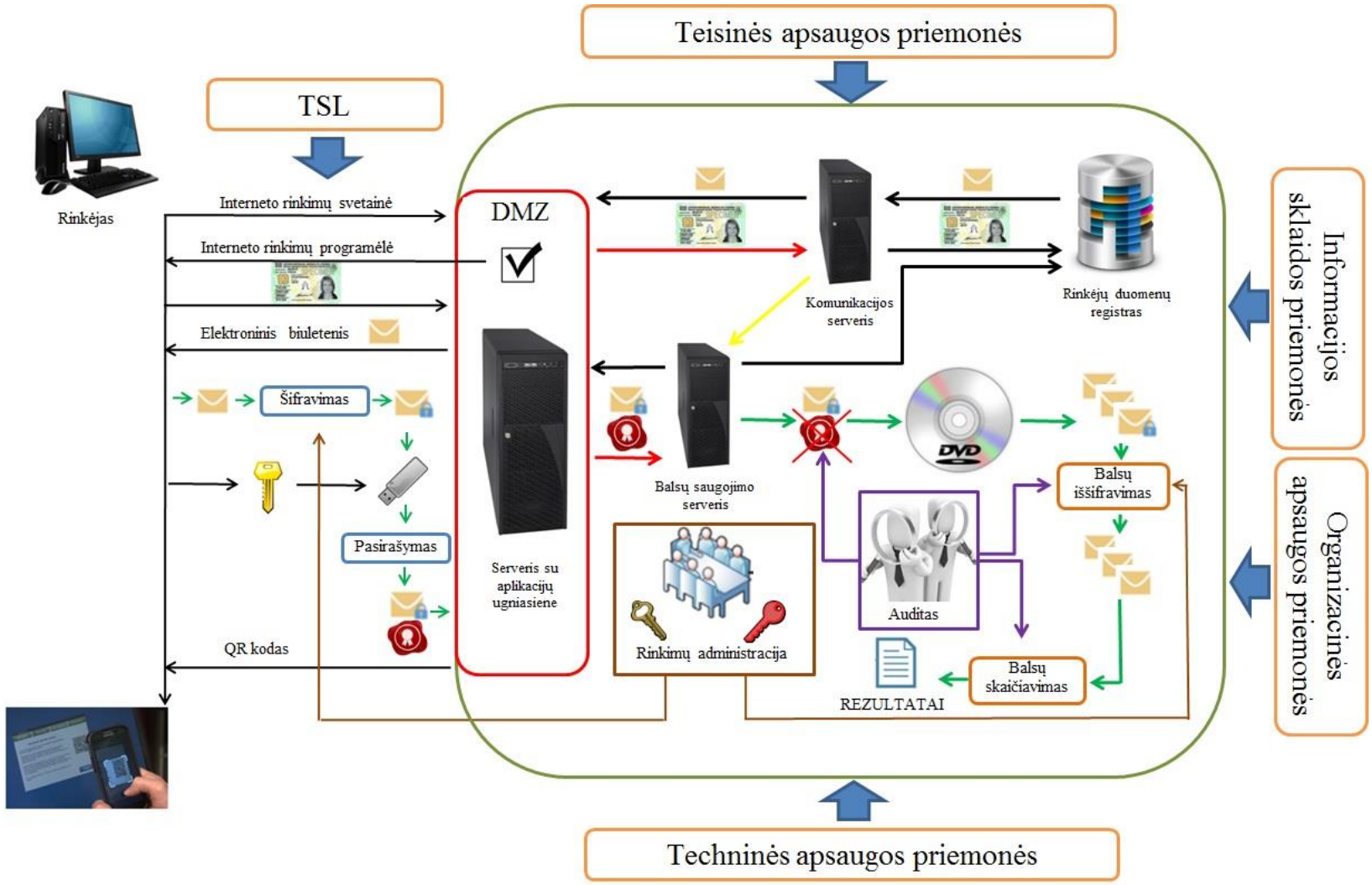
tariant, iš išorės neįmanoma užmegzti ryšio su informacinės sistemos vidumi. DMZ zonoje yra serveris su aplikacijų ugniasiene, kuri praleidžia tik numatyto dydžio ir tipo užklausas bei stebi srautus. Vykstant DDoS atakai, aplikacijų ugniasienė blokuoja informacinę sistemą atakuojančius įrenginius taip leisdama prie sistemos prisijungti teisėtiems vartotojams. Komunikacijos serveris siunčia nuolatines užklausas į DMZ zoną. Kai rinkėjas atsiunčia užklausą dėl registracijos, komunikacijos serveris ją priima ir patikrina rinkėjo tinkamumą (pagal rinkėjo viešąjį raktą). Atsižvelgiant į rinkimų apylinkę, kuriai priklauso rinkėjas, siunčiamas elektroninis rinkimų biuletenis. Jeigu rinkėjas internetu balsuoja ne pirmą kartą, elektroninė balsavimo sistema išima iš balsų saugojimo serverio paskutinįjį rinkėjo balsą ir siunčia jam naują elektroninį biuletenį.

Rinkėjui užpildžius elektroninį balsavimo biuletenį, jis užšifruojamas viešuoju rinkimų raktu (vidinis vokas). Patvirtindamas savo pasirinkimą, rinkėjas pasirašo jį savo privačiuoju raktu (išorinis vokas). Sertifikatas užtikrina, kad atiduotas balsas yra būtent to rinkėjo. Tuomet balsas saugiu šifruotu kanalu siunčiamas į elektroninę balsavimo sistemą.

Atsiųstas balsas patenka į DMZ zoną. Balsų saugojimo serveris siunčia nuolatines užklausas į DMZ zonoje esantį serverį (vienos krypties komunikacija). Gautą rinkimų viešuoju raktu užšifruotą balsą su rinkėjo sertifikatu, balsų saugojimo serveris pasiima iš DMZ zonos ir išsiunčia informaciją į rinkėjų duomenų bazę, kad rinkėjas balsavo. Rinkėjui siunčiamas balso įskaitymo patvirtinimas su unikaliu QR kodu, kuris galioja 30 min. Vartotojas, naudodamas išmaniajame telefone įrašytą programėlę (angl. App), gali pasitikrinti, ar jo balsas buvo teisingai įrašytas.

Užšifruotas balsas balsų saugojimo serveryje saugomas iki balsavimo rinkimų apylinkėse pabaigos. Uždarius balsavimo apylinkes, nuo užšifruotų balsų „nugarinami“ rinkėjų sertifikatai (vidinis vokas išimamas iš išorinio voko). Balsų nuasmeninimo procesą stebi rinkimų auditas. Užšifruoti balsai įrašomi į DVD diską ir perkeliami į saugią aplinką, kur balsai, panaudojus rinkimų privatųjį raktą, iššifruojami ir suskaičiuojami. Balsų iššifravimo ir skaičiavimo procesus stebi rinkimų auditas. Skelbiami rinkimų rezultatai.

Visa komunikacija tarp rinkėjo ir elektroninės balsavimo sistemos balsavimo procesų metu vyksta naudojant saugų šifruotą TSL ryšį. Balsavimo internetu sistema prieš naudojimą turi būti testuojama. Ji privalo būti sertifikuota. Užtikrinant balsavimo sistemos saugumą nuo išorinių bei vidinių grėsmių, turi būti sukurta saugumo politika, kurioje būtų numatytos techninės, organizacinės bei teisinės saugumo priemonės. Įgyvendinant LR Vyriausybės nutarimą (2013 m. liepos 24 d. Nr. 716) dėl Bendrųjų elektroninės informacijos saugos reikalavimų, turi būti parengti ir patvirtinti saugos nuostatai, saugaus elektroninės informacijos tvarkymo taisyklės, informacinės sistemos veiklos tęstinumo valdymo planas bei informacinės sistemos administravimo taisyklės.



Šaltinis: sudaryta autoriaus

12 pav. **Interneto rinkimų kibernetinio saugumo valdymo modelis**

4.2. Modelio taikymo galimybės ir perspektyva

Interneto rinkimų kibernetinio saugumo valdymo modelis sukurtas remiantis teorinėmis ir praktinėmis pasaulinėmis gerosiomis praktikomis (buvo išanalizuoti Prancūzijoje, Jungtinėje Karalystėje, Norvegijoje, Austrijoje ir kt. pasaulio šalyse naudojamas „Scytl“, Estijoje sėkmingai veikiantis „Cybernetica“ bei Šveicarijos Ženevos kontone „Geneva solution“ naudojami interneto rinkimų modeliai). Interneto rinkimų problematika buvo aptarta su 7 interneto rinkimų ekspertais ir 6 kibernetinio saugumo ekspertais, kurie pateikė rekomendacijas dėl kibernetinio saugumo valdymo modelio. Kuriant modelį buvo atsižvelgta į egzistuojančią viešojo administravimo specifiką bei Lietuvoje galiojantį teisinį reglamentavimą (išnagrinėti elektroninės informacijos saugą, kibernetinį saugumą Lietuvoje reglamentuojantys teisės aktai bei Seimo rinkimų, Prezidento rinkimų, savivaldybių tarybų rinkimų, Rinkimų į Europos Parlamentą ir Referendumo įstatymai bei penki šių įstatymų pakeitimų įstatymų projektų paketai, numatantys galimybę balsuoti internetu). Todėl galima teigti, kad šis interneto rinkimų kibernetinio saugumo valdymo modelis galėtų būti taikomas įgyvendinant interneto rinkimus ne tik Lietuvoje, bet ir, atsižvelgiant į panašų kibernetinio saugumo bei interneto rinkimų teisinį reglamentavimą, kitose Europos Sąjungos valstybėse narėse.

2006 metais buvo priimta Balsavimo internetu rinkimuose ir referendumuose koncepcija, 2007 m. LR Vyriausybės nutarimu patvirtinta Balsavimo internetu diegimo programa buvo skirta sukurti ir įdiegti balsavimo internetu sistemą. Koncepcija morališkai paseno, o Programa taip ir liko neįgyvendinta. Interneto rinkimų kibernetinio saugumo valdymo modelio perspektyvą Lietuvoje riboja tai, kad šiuo metu interneto rinkimai nėra įteisinti, t.y. nėra įstatymų, reglamentuojančių balsavimą internetu Seimo, Prezidento, Europos Parlamento, savivaldybių tarybų rinkimuose ir referendumuose. Tačiau priėmus minėtų rinkimų įstatymų pakeitimus, modelis galėtų būti pritaikytas vykdant interneto rinkimus Lietuvoje.

Interneto rinkimų kibernetinio saugumo valdymo modelis panašus į „Scytl“ ir „Cybernetinca“ modelius. Modelius vienija tie patys interneto rinkimų procesų etapai (registracija, asmens tapatybės patvirtinimas, rinkėjo balso šifravimas, balsavimo patvirtinimas, balso įskaitymas ir saugojimas, balsų nuasmeninimas, iššifravimas bei suskaičiavimas). Autoriaus sukurtame modelyje, kaip ir „Scytl“, naudojama tokia pati asmens tapatybės nustatymo metodika. Balsų šifravimas vyksta pasinaudojant viešojo rakto infrastruktūros metodika, sukuriant „dvigubo voko“ analogą (šią metodiką naudoja „Scytl“ ir „Cybernetica“). Rinkėjo balso pasitikrinimo metodas toks pat, kaip ir „Cybernetica“ interneto rinkimų modelyje (panaudojant QR kodą).

Nagrinėti „Scytl“ ir „Cybernetica“ modeliai apėmė tik interneto rinkimų procesą, numatydami saugią komunikaciją tarp rinkėjo ir elektroninės balsavimo sistemos. Autorius viešai

prieinamuose šaltiniuose nerado informacijos apie šių modelių kibernetinio saugumo valdymą. Interneto rinkimų kibernetinio saugumo valdymo modelyje interneto rinkimų procesą apima visuma teisinių, techninių bei organizacinių saugumo priemonių. Šios priemonės padeda išvengti incidentų, juos aptikti, analizuoti, reaguoti į juos, taip pat įprastinei veiklai, įvykus šiems incidentams, atkurti.

Siekiant įvertinti sukurto interneto rinkimų kibernetinio saugumo valdymo modelio taikymo galimybes bei perspektyvą, atlikta SSGG analizė (žr. 3 lentelę).

3 lentelė. **Interneto rinkimų kibernetinio saugumo valdymo modelio SSGG analizė**

STIPRYBĖS	**SILPNYBĖS**
1. Pasinaudota gerosiomis pasaulinėmis praktikomis; 2. Atsižvelgta į dviejų sričių ekspertų (interneto rinkimų ir kibernetinio saugumo) rekomendacijas.	1. Modelyje atsispindi tik interneto rinkimų procesas, tačiau neaiškūs procesų etapuose naudojami metodai bei metodikos.
GALIMYBĖS	**GRĖSMĖS**
1. Modelį galima išskaidyti į scenarijus pagal interneto rinkimų proceso etapus, nurodant taikomus metodus ir metodikas; 2. Atsižvelgiant į viešojo administravimo aspektus, pritaikyti interneto rinkimų kibernetinio saugumo valdymo modelį kt. ES valstybėms narėms.	1. Kibernetinė ataka pasinaudojant nesaugiu asmeniniu rinkėjo įrenginiu.

Šaltinis: sudaryta autoriaus

Interneto rinkimų kibernetinio saugumo valdymo modelio stiprybė yra tai, kad kuriant jį buvo pasinaudota gerosiomis pasaulinėmis praktikomis bei atsižvelgta į interneto rinkimų ir kibernetinio saugumo ekspertų nuomonę bei rekomendacijas. Modelyje nėra nurodyti interneto procesų etapuose naudojami metodai bei metodikos, nes tai apsunkintų modelio suvokimą. Tačiau jį galima išskaidyti į scenarijus pagal interneto rinkimų proceso etapus, kuriuose galima nurodyti naudojamus metodus ir metodikas. Atsižvelgiant į viešojo administravimo aspektus, interneto rinkimų kibernetinio saugumo valdymo modelį galima pritaikyti kitoms ES valstybėms narėms dėl panašaus teisinio reguliavimo.

IŠVADOS

1. Balsavime internetu privalo būti užtikrinami visi demokratinių rinkimų ir referendumų principai, kurių kibernetinio saugumo valdymą užtikrina teisinės, informacijos sklaidos, organizacinės bei techninės priemonės. Šių priemonių visuma padeda apsisaugoti nuo vidinių (administratorių, kitų sistemos vartotojų ir valstybės tarnautojų) bei išorinių (užsienio žvalgybos tarnybų, programišių, tipinių nusikaltėlių ir haktivistų) grėsmių visų balsavimo internetu proceso etapų metu.

2. Šiuo metu valdžios institucijos tik deklaruoja ketinimą įteisinti interneto rinkimus Lietuvoje. Tačiau, atsižvelgiant į Lietuvos Respublikos teisinio reglamentavimo ypatumus, parengtus rinkimų įstatymų pakeitimų įstatymų projektus bei kibernetinio saugumo valdymo specifiką, Lietuvoje įgyvendinamiems interneto rinkimams labiausiai tiktų interneto rinkimų modelis, kuriame būtų tiek „Scytl“, tiek „Cybernetica“ interneto rinkimų modeliuose taikomų metodų ir metodikų.

3. Lietuvoje be techninių kliūčių (nepažeidžiant asmens privatumo, šiuo metu nėra galimybių užtikrinti rinkėjo įrenginio saugumo), įteisinti interneto rinkimus trūksta politinės valios. Šiuo metu nėra bendro sutarimo, koks turėtų būti interneto rinkimų modelis. Iki šiol neatliktas rizikų vertinimas, nenustatytos toleruojamos rizikos. O piliečių nepasitikėjimą elektronine balsavimo sistema lemia nepakankamas visuomenės įtraukimas į interneto rinkimų įgyvendinimą.

4. Interneto rinkimų kibernetinio saugumo valdymo modelis (žr. 12 pav.) sukurtas panaudojant gerąsias „Scytl“ ir „Cybernetica“ modelių savybes, atsižvelgus į interneto rinkimų ir kibernetinio saugumo ekspertų nuomonę bei rekomendacijas. Modelis buvo kuriamas pagal egzistuojančią viešojo administravimo specifiką bei Lietuvoje galiojantį teisinį reglamentavimą. Interneto rinkimų kibernetinio saugumo valdymo modelis galėtų būti taikomas įgyvendinant interneto rinkimus ne tik Lietuvoje, bet ir kitose ES valstybėse narėse dėl panašaus teisinio reguliavimo.

REKOMENDACIJOS

- Įteisinant balsavimą internetu būtina užtikrinti visišką aiškumą, kokio pobūdžio modelis bus įgyvendintas.
- Įstatymuose reikia įvardinti ir detalizuoti modelio veikimo principus, pagrindines savybes bei užtikrinti aiškų atsakomybių pasiskirstymą tarp susijusių institucijų.

- Būtina atlikti išsamų interneto rinkimų informacinės sistemos rizikų vertinimą bei nustatyti toleruojamą riziką, kuri turi būti suderinta su visuomene.
- Būtina skleisti informaciją visuomenei apie interneto rinkimus bei kibernetinio saugumo aspektus.
- Siekiant sukurti vientisą nenutrūkstantį balsavimo procesą, balsavimą internetu reikia integruoti į Lietuvos rinkimų sistemą kaip vientisą darinį.
- Pateikti rekomendacijas rinkėjui, kurios padėtų saugiai prisijungti prie interneto rinkimų svetainės.

LITERATŪROS SĄRAŠAS

Įstatymai ir kiti teisės aktai:

1. Lietuvos Respublikos Konstitucija (1992). *Valstybės žinios*, 33(1014).
2. Lietuvos Respublikos kibernetinio saugumo įstatymas (2014). *Teisės aktų registras*, 20553.
3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (2011). *Valstybės žinios*, 163(7739).
4. Lietuvos Respublikos elektroninio parašo įstatymas (2000). *Valstybės žinios*, 61(1827).
5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (1996). *Valstybės žinios*, 63(1479).
6. Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo (2011). *Valstybės žinios*, 83(4033).
7. Lietuvos Respublikos Seimo 2006 m. lapkričio 16 d. nutarimas Nr. X-912 Dėl balsavimo internetu rinkimuose ir referendumuose koncepcijos patvirtinimo (2006). *Valstybės žinios*, 127(4827).
8. Lietuvos Respublikos Vyriausybės 2007 m. liepos 11 d. nutarimas Dėl balsavimo internetu diegimo programos patvirtinimo (2007). *Valstybės žinios*, 81(3332).
9. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo (2013). *Valstybės žinios*, 86(4310).
10. Lietuvos Respublikos Vyriausybės 2015 m. balandžio 23 d. nutarimas Nr. 422 Dėl Kibernetinio saugumo tarybos sudarymo ir jos reglamento patvirtinimo (2015). *Teisės aktų registras*, 6486.
11. Lietuvos policijos generalinio komisaro 2015 m. vasario 2 d. įsakymas Nr. 5-V-101 Dėl Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetinių incidentų tyrimo tvarkos aprašo patvirtinimo (2015). *Teisės aktų registras*, 1654.
12. Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės generalinio direktoriaus 2009 m. rugsėjo 7 d. įsakymas Nr. V-60 Dėl elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos ADOC-V1.0 patvirtinimo (2009). *Valstybės žinios*, 108(4574).

13. Europos Komisijos 2013 m. vasario 7 d. bendras komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“ JOIN(2013)1 final. Prieiga per internetą: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/join/com_join(2013)0001_/com_join(2013)0001_lt.pdf.
14. Recommendation Rec(2004)11 of the Committe of Ministers to member states of legal, operational and technical standards for e-voting. Council of Europe, 2004. Prieiga per internetą: https://wcd.coe.int/ViewDoc.jsp?id=778189.

Įstatymų projektai:

15. Rinkimų į Europos Parlamentą įstatymo 6, 27, 31, 32, 33, 34, 56, 60, 62, 67, 76 ir 80 straipsnių pakeitimo, 63 ir 66 straipsnių papildymo bei Įstatymo papildymo 64(1) ir 79(1) straipsniais įstatymo projektas Nr. XP-2193.
16. Seimo rinkimų įstatymo 5, 6, 28, 29, 31, 32, 33, 34, 35, 58, 59, 62, 64, 69, 78 ir 82 straipsnių pakeitimo, 65 ir 70 straipsnių papildymo bei Įstatymo papildymo 66(1) ir 81(1) straipsniais įstatymo projektas Nr. XP-2194.
17. Referendumo įstatymo 39, 40, 41, 42, 43, 51, 56, 64, 68 ir 69 straipsnių pakeitimo, 52 ir 55 straipsnių papildymo, 36 straipsnio 2 dalies pripažinimo netekusia galios bei Įstatymo papildymo 53(1) ir 67(1) straipsniais įstatymo projektas Nr. XP-2195.
18. Prezidento rinkimų įstatymo 23(3), 23(6), 23(7), 23(8), 23(9), 23(10), 49, 51, 54(2), 64, 68 ir 69 straipsnių pakeitimo, 52 ir 54(1) straipsnių papildymo bei Įstatymo papildymo 53(1) ir 67(1) straipsniais įstatymo projektas Nr. XP-2196.
19. Rinkimų į Europos Parlamentą įstatymo 27, 28, 32, 33, 34, 56, 60, 62, 63, 66, 67, 76, 80 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 64(1), 79(1) straipsniais įstatymo projektas Nr. XIP-1155 ir XIP-1155(2).
20. Prezidento rinkimų įstatymo 26, 31, 32, 33, 52, 54, 55, 58 , 59, 68, 72 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 56(1), 71(1) straipsniais įstatymo projektas Nr. XIP-1156 ir XIP-1156(2).
21. Seimo rinkimų įstatymo 28, 29, 33, 34, 35, 58, 59, 62, 64, 65, 69, 70, 78, 82 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 66(1), 81(1) straipsniais įstatymo projektas Nr. XIP-1157 ir XIP-1157(2).
22. Savivaldybių tarybų rinkimų įstatymo 32, 59, 61, 62, 73, 77 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 64(1), 76(1) straipsniais įstatymo projektas Nr. XIP-1158 ir XIP-1158(2).

23. Referendumo įstatymo 36, 41, 42, 43, 51, 52, 55, 56, 64, 68 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 54(1), 67(1) straipsniais įstatymo projektas Nr. XIP-1159 ir XIP-1159(2).
24. Rinkimų į Europos Parlamentą įstatymo 28, 32, 56, 60 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 64(1), 79(1) straipsniais įstatymo projektas Nr. XIP-2794.
25. Prezidento rinkimų įstatymo 31, 50, 52, straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 58(1), 68(1) straipsniais įstatymo projektas Nr.XIP-2795.
26. Referendumo įstatymo 41, 46, 50 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 50(1), 67(1) straipsniais įstatymo projektas Nr. XIP-2796.
27. Seimo rinkimų įstatymo 29, 33, 58, 59, 62 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 70(1), 81(1) straipsniais įstatymo projektas Nr.XIP-2797.
28. Rinkimų į Europos Parlamentą įstatymo 27, 28, 32, 33, 34, 56, 60, 62, 63, 64, 66, 67, 76, 80 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 64(1), 79(1) straipsniais įstatymo projektas Nr. XIP-3248.
29. Prezidento rinkimų įstatymo 26, 31, 32, 33, 50, 52, 54, 55, 56, 58, 59, 68, 72 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 56(1), 71(1) straipsniais įstatymo projektas Nr. XIP-3249.
30. Referendumo įstatymo 36, 41, 42, 43, 46, 51, 52, 53, 55, 56, 64, 68 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 54(1), 67(1) straipsniais įstatymo projektas Nr. XIP-3250.
31. Savivaldybių tarybų rinkimų įstatymo 32, 55, 59, 61, 62, 63, 73, 77 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 64(1), 76(1) straipsniais įstatymo projektas Nr. XIP-3251.
32. Seimo rinkimų įstatymo 28, 29, 33, 34, 35, 58, 59, 62, 64, 65, 66, 69, 70, 78, 82 straipsnių pakeitimo ir papildymo bei Įstatymo papildymo 66(1), 81(1) straipsniais įstatymo projektas Nr. XIP-3252.
33. Prezidento rinkimų įstatymo Nr. I-28 26, 31, 32, 33, 52, 54, 56, 58, 59, 72 straipsnių pakeitimo ir papildymo 56(1), 71(1) straipsniais įstatymo projektas Nr. XIIP-1835.
34. Referendumo įstatymo Nr. IX-929 36, 41, 42, 43, 51, 53, 55, 56, 68 straipsnių pakeitimo ir papildymo 54(1), 67(1) straipsniais įstatymo projektas Nr. XIIP-1836.
35. Rinkimų į Europos Parlamentą įstatymo Nr. IX-1837 28, 33, 34, 35, 58, 62, 64, 66, 69, 70, 83 straipsnių pakeitimo ir papildymo 66(1), 82(1) straipsniais įstatymo projektas Nr. XIIP-1837.
36. Savivaldybių tarybų rinkimų įstatymo Nr. I-532 32, 55, 59, 61, 63, 77 straipsnių pakeitimo ir papildymo 64(1), 76(1) straipsniais įstatymo projektas Nr. XIIP-1838.

37. Seimo rinkimų įstatymo Nr. I-2721 28, 29, 33, 34, 35, 58, 59, 62, 64, 66, 69, 70, 82 straipsnių pakeitimo ir papildymo 66(1), 81(1) straipsniais įstatymo projektas Nr. XIIP-1839.

Knygos:

38. Kiškis M. ir kt. (2006). *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas.
39. Kotler P. ir Keller, K.L. (2007). *Marketingo valdymo pagrindai.* Klaipėda: Logitema.
40. Štitilis D. (2011). *Elektroniniai nusikaltimai (mokomasis leidinys).* Vilnius: Mykolo Romerio universitetas.
41. Virbalienė A. (2011). *Vidinė organizacijos komunikacija*. Klaipėda: Socialinių mokslų kolegija. Prieiga per internetą: http://www.esparama.lt/es_parama_pletra/failai/ESFproduktai/2011_Vidine_organizacijos_komunikacija.pdf.

Straipsniai moksliniuose žurnaluose:

42. Abdalla Al-Ameen ir Samani A. Talab. (2013). E-Voting Systems Security Issues. *IJNCM: International Journal of Networked Computing and Advanced Information Management*, Vol. 3, No. 1, p. 25-34.
43. Hampson Noah C. N. (2012). Hacktivism: A New Breed of Protest in a Networked World. *Boston College Internwtional and comparitive Law Review*, 511, p. 511-542.
44. Jastiuginas S. (2011). Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. *Informacijos mokslai*, 57, p. 7-25.
45. Repečka G. (2007). Elektroninis parašas. *Naujoji komunikacija*, 16 (212), p. 22-24.
46. Repečka G. (2007). Saugus duomenų perdavimas internetu: SSL/TLS. *Naujoji komunikacija*, 12 (208), p. 15-16.
47. Springall D. ir kt. (2014). Security Analysis of the Estonian Internet Voting System. *University of Michigan.* Prieiga per internetą: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf.
48. Štitilis D. (2013). Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos. *Socialinės technologijos*, 3(1), p. 189-207.

Organizacijų ir oficialių įstaigų leidiniai:

49. ACM U.S. Public Policy Council (2006). *Statewide Databases of Registered Voters.* Prieiga per internetą: http://usacm.acm.org/evoting/details.cfm?type=Reports%2FWhite%20Papers&id=123&cat=14&E-Voting.
50. Elections BC. A non-partisan Office of the Legislature (2011). *Discussion Paper: Internet Voting*. Prieiga per internetą: http://www.elections.bc.ca/docs/Internet-Voting-Discussion-Paper.pdf.
51. Independent Panel on internet Voting (2014). *Recommendations Report the Legislative Assembly of British Columbia*. Prieiga per internetą: https://www.verifiedvoting.org/wp-content/uploads/2014/10/CA-BC-2014-recommendations-final-report.pdf.
52. LR Seimo Parlamentinių tyrimų departamentas (2015). *Balsavimas internetu: užsienio patirtis ir perspektyvos Lietuvoje*. Prieiga per internetą: http://www.vrk.lt/documents/10180/556540/Balsavimas+internetu.pdf/a5247fe6-d96e-437d-8135-5db76da1f66f.
53. LR Seimo Parlamentinių tyrimų departamentas (2002). *Elektroninio parašo infrastruktūros išplėstinė samprata*.
54. U.S. Vote Foundation (2015). *The Future of Voting. End-to-end verifiable internet voting*. Prieiga per internetą: https://people.csail.mit.edu/rivest/pubs/OVF15.pdf.
55. Valstybės saugumo departamentas (2014). *Kas, kaip ir kodėl šnipinėja Lietuvoje*. Prieiga per internetą: http://www.vsd.lt/Files/Documents/635465490532338750.pdf.

Interneto šaltiniai:

56. Cybernetica (2015). *For greater safety and security in the world*. Prieiga per internetą: http://cyber.ee/en/about-us/.
57. Elektroninis.lt (2015). *Kaip sudarytas elektroninis.lt parašas*. Prieiga per internetą: http://www.elektroninis.lt/lt/apie/nid-513.
58. ELTA (2015-05-12). KAM perspėja dėl internete platinamo šauktinių sąrašo. *Delfi.lt.* Prieiga per internetą: http://www.delfi.lt/news/daily/lithuania/kam-perspeja-del-internete-platinamo-sauktiniu-saraso.d?id=67945790.
59. Estonia.eu (2015). *Estonian Internet voting system*. Prieiga per internetą: http://estonia.eu/about-estonia/economy-a-it/e-voting.html.
60. Jefferson D. ir kt. (2004). *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE).* Prieiga per internetą: http://www.servesecurityreport.org/.
61. Lietuvos bankas (2015). *Lietuvos banko valdybos nutarimai*. Prieiga per internetą: https://www.lb.lt/lietuvos_banko_valdybos_nutarimai_101.

62. LR ryšių reguliavimo tarnyba (2015). *Atmintinė vartotojui apie elektroninį parašą*. Prieiga per internetą: http://rrt.lt/lt/vartotojui/elektroninis-parasas_358/apie-e-parasa_7/atmintine_980.html.
63. LR ryšių reguliavimo tarnyba (2015). *Tinklų ir informacijos saugumas*. Prieiga per internetą: http://www.rrt.lt/lt/verslui/tinklu-ir-informacijos-saugumas.html.
64. LR vidaus reikalų ministerija (2015). *Asmens tapatybės kortelė ir elektroninis parašas*. Prieiga per internetą: http://www.nsc.vrm.lt/.
65. LR vidaus reikalų ministerija (2005). *Informacijos sauga valstybės institucijų ir įstaigų darbuotojams.* Prieiga per internet: http://www.vipt.lt/infosauga/pdf/3skyrius.pdf.
66. National Initiative for Cybersecurity and Careers and Studie (2015). *Explore Terms: A Glossary of Common Cybersecurity Terminology*. Prieiga per internetą: https://niccs.us-cert.gov/glossary#cybersecurity.
67. Paul N. ir kti. *Autentification for Remote Voting*. Prieiga per internetą: http://www.cs.virginia.edu/~evans/pubs/remote-voting.pdf.
68. SANS Institute InfoSec Reading Room (2001). *Understanding Intrusion Detection Systems*. Prieiga per internetą: https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337.
69. Scytl Innovating Democracy (2013). *On the Radar: Scytl. An End-to-end election modernization platform*. Prieiga per internetą: http://www.scytl.com/wp-content/uploads/2013/05/Ovum_On-the-Radar_Scytl_April-20131.pdf.
70. Scytl Innovating Democracy (2015). *Scytl Voter Registration*. Prieiga per internetą: http://www.scytl.com/en/products/pre-election/scytl-voter-registration/.
71. Skaitmeninio sertifikavimo centras (2015). *Susipažinimas su skaitmeniniais sertifikatais*. Prieiga per internetą: http://www.ssc.lt/?name=menu&act=show&do=17,108&L=lt.
72. Transparency International Lietuvos skyrius (2015). *Trys ekspertų rekomendacijos saugiam balsavimui internetu*. Prieiga per internetą: http://transparency.lt/media/filer_public/2015/03/10/rekomendacijos_balsavimui_internetu.pdf.
73. University of Tartu. (2015). *E-voting*. Prieiga per internetą: https://courses.cs.ut.ee/2015/infsec/fall/Main/E-voting.
74. Urmanavičiūtė I. (2010). *Duomenų apsaugos priemonių kompiuterizuoto parinkimo ir įvertinimo metodika* (magistro baigiamasis darbas). Prieiga per internetą: http://vddb.laba.lt/fedora/get/LT-eLABa-0001:E.02~2010~D_20110709_152451-76770/DS.005.1.01.ETD.

Paukštė L. Kibernetinio saugumo valdymo ypatumai įgyvendinant interneto rinkimus / Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas doc. dr. T. Limba – Vilnius: Mykolo Romerio universitetas, verslo ir medijų mokykla, 2015 - 83 p.

ANOTACIJA

Magistro baigiamajame darbe, remiantis teorinėmis ir praktinėmis pasaulinėmis gerosiomis praktikomis, atsižvelgus į Lietuvos kibernetinio saugumo valdymo įgyvendinimo aspektus ir interneto rinkimų teisinio reglamentavimo ypatumus bei dviejų sričių ekspertų (interneto rinkimų ir kibernetinio saugumo valdymo) rekomendacijas, pasiūlytas interneto rinkimų kibernetinio saugumo valdymo modelis, kuris galėtų būti pritaikytas įgyvendinus interneto rinkimus Lietuvoje. Darbą sudaro 4 dalys. *Pirmoje* dalyje pateikiami kibernetinio saugumo valdymo, kūrimo ir diegimo interneto rinkimuose teoriniai aspektai: apibrėžiama kibernetinio saugumo valdymo sąvoka, nagrinėjami interneto rinkimų kibernetinio saugumo valdymo principai bei problematika, aprašomas balsavimo internetu kibernetinio saugumo valdymo įgyvendinimas. *Antroje* dalyje pateikiama kibernetinio saugumo valdymo įgyvendinimo pasaulinės patirties analizė: analizuojami „Scytl“, „Cybernetica“ ir „Geneva soliution“ interneto rinkimų modeliai, atliekama šių modelių lyginamoji analizė. Taip pat nagrinėjami kibernetinio saugumo valdymo įgyvendinimo aspektai Lietuvoje, aptariami interneto rinkimų teisinio reglamentavimo ypatumai bei atliekama esamos padėties (SSGG) analizė. *Trečioje* dalyje atliekamas kokybinis tyrimas, panaudojant ekspertinio interviu metodą. Apklausus 7 interneto rinkimų bei 6 kibernetinio saugumo ekspertus, nustatomi probleminiai interneto rinkimų aspektai, pateikiamos galimų sprendimų rekomendacijos. *Ketvirtoje* dalyje pasiūlytas interneto rinkimų kibernetinio saugumo valdymo modelis interneto rinkimams Lietuvoje.

Pagrindiniai žodžiai: i. rinkimai, e. rinkimai, kibernetinio saugumo valdymas, interneto rinkimų modeliai, elektroninės rinkimų sistemos, elektroninių rinkimų principai.

Paukštė L. Cyber security Management Peculiarities During Internet Voting / Master‘s Work in Cyber security Management. Supervisor: assoc. prof. T. Limba – Vilnius: Mykolas Romeris University, Business and Media School, 2015 - 83 p.

ANNOTATION

The final Master’s paper, based on theoretical and practical global good practices, in consideration of Lithuania’s cyber security management implementation aspects and peculiarities of internet voting legal regulations as well as recommendations of two field experts (internet voting and cyber security management), presents cyber security management model of internet voting, which could be adjusted during the implementation of Lithuania’s online voting. The paper comprises four parts. The first part provides theoretical aspects of cyber security management, development and implementation in internet voting: cyber security management definition, internet voting cyber security management principles and issues. The implementation of internet voting cyber security management is described. The second part presents the analyses of global practices of cyber security management implementation: analysis of internet voting models (systems) of „Scytl“, „Cybernetica“ and „Geneva solution“, qualitative comparative analysis of the models (systems) mentioned. The research is made in cyber security management implementation aspects in Lithuania, and in peculiarities of internet voting legal regulations, after that the SWOT analysis is performed. Third part introduces qualitative research applying expert interview method. Internet voting issues were identified, potential solution recommendations were proposed after seven online voting and six cyber security experts had been interviewed. The fourth part introduces the internet voting cyber security management model suggestions for internet voting in Lithuania.

Keywords: internet voting, e-voting, cyber security management, internet voting models, electronic voting systems, electronic voting principles.

Paukštė L. Kibernetinio saugumo valdymo ypatumai įgyvendinant interneto rinkimus / Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas doc. dr. T. Limba – Vilnius: Mykolo Romerio universitetas, verslo ir medijų mokykla, 2015 - 83 p.

SANTRAUKA

Magistrinio baigiamojo darbo tikslas – išanalizavus kibernetinio saugumo valdymo ypatumus, atlikus interneto rinkimų sistemų kibernetinio saugumo analizę, pasinaudojus gerosiomis pasaulinėmis praktikomis, sukurti kibernetinio saugumo valdymo modelį interneto rinkimams Lietuvoje.

Interneto rinkimai yra labai specifinė bei labai svarbi demokratijos išraiška, kuriai itin svarbu apsisaugoti tiek nuo vidaus, tiek nuo išorės pavojų. Sėkminga kibernetinė ataka prieš tokį svarbų valstybei procesą gali ne tik būti priežastimi, dėl kurios rinkimai būtų pripažinti negaliojantys, bet taip pat gali sukompromituoti valstybę bei sugriauti žmonių pasitikėjimą ja. Mokslo šaltiniuose yra nepakankamai ištirtos pasaulyje sėkmingai veikiančios interneto rinkimų sistemos, grėsmių šaltiniai, galimi atakų vektoriai, metodai bei metodikos.

Darbe taikoma mokslinės literatūros analizė ir sintezė, kitų šalių gerajai praktikai palyginti naudojama lyginamoji analizė, renkant bei analizuojant statistinius duomenis apie kibernetinius incidentus panaudota antrinių duomenų analizė. Tyrimui pasirenkamas pusiau struktūrizuotas giluminio interviu metodas – apklausta 13 ekspertų. Išanalizavus kibernetinio saugumo valdymo ypatumus bei atlikus interneto rinkimų sistemų kibernetinio saugumo analizę, sukurtas kibernetinio saugumo valdymo modelis interneto rinkimams Lietuvoje.

Magistro darbą sudaro 4 dalys. *Pirmoje* dalyje pateikiami kibernetinio saugumo valdymo, kūrimo ir diegimo interneto rinkimuose teoriniai aspektai: apibrėžiama kibernetinio saugumo valdymo sąvoka, nagrinėjami interneto rinkimų kibernetinio saugumo valdymo principai bei problematika, aprašomas balsavimo internetu kibernetinio saugumo valdymo įgyvendinimas. *Antroje* dalyje pateikiama kibernetinio saugumo valdymo įgyvendinimo pasaulinės patirties analizė: analizuojami „Scytl“, „Cybernetica“ ir „Geneva soliution“ interneto rinkimų modeliai, atliekama šių modelių lyginamoji analizė. Taip pat nagrinėjami kibernetinio saugumo valdymo įgyvendinimo aspektai Lietuvoje, aptariami interneto rinkimų teisinio reglamentavimo ypatumai bei atliekama esamos padėties (SSGG) analizė. *Trečioje* dalyje atliekamas kokybinis tyrimas, panaudojant ekspertinio interviu metodą. Apklausus 7 interneto rinkimų bei 6 kibernetinio saugumo ekspertus, nustatomi probleminiai interneto rinkimų aspektai, pateikiamos galimų sprendimų rekomendacijos. *Ketvirtoje* dalyje pasiūlytas interneto rinkimų kibernetinio saugumo valdymo modelis.

Paukštė L. Cyber security Management Peculiarities During Internet Voting / Master‘s Work in Cyber security Management. Supervisor: assoc. prof. T. Limba – Vilnius: Mykolas Romeris University, Business and Media School, 2015 - 83 p.

SUMMARY

The aim of final Master’s paper is, after analyzing peculiarities of cyber security management, carrying out a cyber security analysis of internet voting systems, studying legal regulations of Lithuania’s cyber security management and internet voting, interviewing internet voting and cyber security management experts, to develop a cyber security management model for internet voting in Lithuania.

Internet voting is a specific and very important aspect of democracy, which must be protected equally from the inside or outside risks. Successful cyber attack against such an important process for a state can become a reason not only to declare elections invalid but also to compromise a state and to ruin people’s reliance on it. There are few researches made about global successfully operating internet voting systems, threats, possible attack vectors, methods and methodologies.

There are applied scientific literature analysis and synthesis, comparative analysis in order to compare good practices of other states, statistical data analysis, used during compilation and analysis of statistical data related to cyber incidents, in the paper. The research is made by choosing half structured qualitative interview method: 13 experts were interviewed. After analysing peculiarities of cyber security management and carrying out internet voting cyber security analyses, a cyber security management model for the internet voting in Lithuania was developed.

The paper comprises four parts. The first part provides theoretical aspects of cyber security management, development and implementation in internet voting: cyber security management definition, internet voting cyber security management principles and issues. The implementation of internet voting cyber security management is described. The second part presents the analyses of global practices of cyber security management implementation: analysis of internet voting models (systems) of „Scytl“, „Cybernetica“ and „Geneva solution“, qualitative comparative analysis of the models (systems) mentioned. The research is made in cyber security management implementation aspects in Lithuania, and in peculiarities of internet voting legal regulations, after that the SWOT analysis is performed. Third part introduces qualitative research applying expert interview method. Interne voting issues were identified, potential solution recommendations were proposed after seven internet voting and six cyber security experts had been interviewed. The fourth part introduces the internet voting cyber security management model suggestions.

PRIEDAI

Klausimai interneto rinkimų specialistams

1. Interneto rinkimų problematika Lietuvoje.
    - Kodėl Lietuvoje iki šiol neįgyvendinta galimybė balsuoti internetu?
    - Ko trūksta sklandžiam interneto rinkimų įgyvendinimui Lietuvoje?
2. Interneto rinkimų modelio taikymas Lietuvoje.
    - Pasiremti kitų šalių patirtimi, ar kurti savo interneto rinkimų modelį? Kodėl?
    - Koks rinkimų modelis labiausiai tiktų Lietuvoje? Kodėl?
3. Interneto rinkimų problematika.
    - Pavojai interneto rinkimų proceso etapuose. Kokie pavojai slypi? Kokie galimi sprendimų variantai?
    - Kokių dar problemų gali kilti?

Klausimai kibernetinio saugumo specialistams

1. Interneto rinkimų kibernetinio saugumo valdymo problematika
    - Nesaugaus rinkėjo įrenginio problema. Kokie galimi sprendimo būdai?
    - Kaip užtikrinti saugią komunikaciją?
    - Saugi interneto rinkimų informacinės sistemos infrastruktūra.