KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

ROBERTAS ŠUNOKAS

TAIKOMŲJŲ UŽDAVINIŲ KOKYBĖS MODELIAVIMAS SAUGIOJE ELEKTRONINIŲ PASLAUGŲ SISTEMOJE

MAGISTRO DARBAS

Darbo vadovas doc. Valentinas Kiauleikis

KAUNAS, 2004

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

TVIRTINU .....
Katedros vedėjas
doc. dr. E. Kazanavičius
2004 05

TAIKOMŲJŲ UŽDAVINIŲ KOKYBĖS MODELIAVIMAS SAUGIOJE ELEKRONINIŲ PASLAUGŲ SISTEMOJE

INFORMATIKOS MOKSLŲ MAGISTRO BAIGIAMASIS DARBAS

Magistrantas .....
Robertas Šunokas IFM-8/1
2004 05

Vadovas .....
doc. Valentinas Kiauleikis
2004 05

Recenzentas .....
doc. Rimantas Plėštys
2004 05

Lietuvių kalbos konsultantas .....
dr. Jurgita Mikelionienė
2004 05

KAUNAS, 2004

R. Šunokas. Taikomųjų uždavinių kokybės modeliavimas saugioje elektroninių paslaugų sistemoje: magistro baigiamasis darbas / mokslinis vadovas doc. V. Kiauleikis; Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterių katedra.– Kaunas, 2004.– 68 p.

Santrauka

Modeliuojant būsimas elektroninių paslaugų sistemas visuomet aktualūs yra taikomųjų uždavinių kokybės parametrai. Būsima sistema turi būti patikima darbo režime, pakankamai lanksti ir prisitaikanti įvairiose situacijose, bei kuo labiau našesnė. Sistemos kūrėjui labai svarbus parametras yra būsimos sistemos kaina. Apibrėžtas integruotasis kokybės parametras, kuris naudojamas visų atskirai naudojamų parametrų skaičiavimui ir analizei.

Šiame darbe pasirinkta Petri tinklų sistemų projektavimo metodologija. Teoriniame lygmenyje Petri tinklais kuriama ir modeliuojama elektroninių paslaugų sistema – El. Valdžia. Tiriant informacijos apsaugos metodus sistemos projektavimo ir modeliavimo žingsniuose stengiamasi įvertinti šiuos pagrindinius vertinimo kriterijus:

a) Lankstumas b) Patikimumas c) Našumas d) Kaina

Atliekant Petri tinklų analizę pereinama prie kuriamos sistemos teorinio modeliavimo mechanizmo ir aprašymo. Analizuojami geriausių informacijos apsaugos savybių radimo (pasiekimo) būdai ir keliai. Tam naudojami taikomųjų uždavinių kokybės parametrų modeliavimas.

R. Šunokas. Modeling of application quality parameters in a secured electronic service system: master thesis / science guide doc. V. Kiauleikis; Kaunas University of Technology, Informatics Faculty, Department of Computers.- Kaunas, 2004.– 68 p.

Summary

While modeling electronic service systems application quality parameters are always relevant. Future system must be reliable in operating, flexible enough in different situations and to have good efficiency. Price is important for system builder. Integrated quality parameter is defined for measuring and evaluation of all other quality parameters.

In this work Petri nets architecture is picked as projecting methodology. electronic service information system - E-Government, is created and modeled theoretically. While studying information security methods in every projecting and modeling step we try to valuate these parameters: a) flexibility b) reliability c) performance d) price.

While analyzing Petri nets it is required to make and describe information system theoretically. It is analyzed how to find the best way to reach optimal information security features. Application quality parameters are used for that.

TURINYS

ĮVADAS

Kiekvienos sistemos projektuotojui svarbūs yra šie kriterijai: sistemos lankstumas, patikimumas, našumas ir žinoma kaina. Taigi kuriant elektroninių paslaugų sistemą kiekviename žingsnyje yra patogu naudoti standartizuotą projektavimo ir modeliavimo architektūrą.

Būsimos sistemos vartotojui yra svarbu sistemos saugumas ir patikimumas, o sistemos kūrėjui svarbu pasiekti didesnį pelną. Todėl projektuojant sistemas visuomet siekiama optimalaus varianto. Svarbiausiais jo radimo matavimo komponentais yra kuo didesnius sistemos lankstumas, patikimumas bei našumas, ir kuo mažesnė kaina.

Internetas yra viena iš veržliausiai plintančių ir ypatingai efektyvių komunikavimo priemonių, padedančių mums bendrauti neatsižvelgiant į atstumą, laiką, valstybių sienas. Gyvenimas elektroninėje erdvėje tampa vis intensyvesnis. Susijungus į pasaulini tinklą dešimtims ir šimtams milijonų asmeninių kompiuterių, atsiranda ir didėja realus pavojus, jog mūsų asmeninius duomenis, el. pašto korespondenciją tretieji (pašaliniai) asmenys galės stebėti, pakeisti ar perimti, nes interneto kanalais keliaujančią informaciją galima surasti, perskaityti, pakeisti, redaguoti ar sunaikinti. Tokiu būdu, naudodami internetą, mes ne tik gauname naujas komunikavimo galimybes, bet taip pat susiduriame su privačios informacijos ir asmens duomenų nesankcionuoto vartojimo problema.

Klausimai yra aktualūs ne tik asmenims, naudojantiems internetą kaip informacijos apsikeitimo terpę, bet ir informacinių paslaugų – el. verslo, el. prekybos, nuotolinio mokymo, gydymo bei kitų paslaugų elektroninėje erdvėje kūrėjams, teikėjams ir platintojams. Akivaizdu, kad elektroninių paslaugų plitimo tempai didele dalimi priklauso nuo visuomenės narių pasitikėjimo informacinėmis technologijomis lygio, nuo realių garantijų išsaugoti informacijos privatumą, naudojantis interneto paslaugomis.

Taigi elektroninių paslaugų sistemų kūrėjams vis didesnį dėmesį reikia skirti informacijos saugumui užtikrinti. Nes nuo to priklauso el. paslaugų vartotojų pasitikėjimas, tuo pačiu ir el. paslaugų plėtra.

Magistro darbas susideda iš keturių pagrindinių dalių: elektroninių paslaugų kūrimo problemų analizės literatūroje, taikomųjų uždavinių modeliavimo teorinių klausimų, elektroninių paslaugų taikomųjų uždavinių kokybės analizės ir modeliavimo, bei pateiktų išvadų.

Literatūros analizėje gvildenamos problemos, susijusios su informacijos apsaugos metodais, kurie turi būti realizuoti elektroninių paslaugų sistemose. Pateikiama elektroninių

paslaugų ir Elektroninės Valdžios samprata. Analizuojami mokslinėje literatūroje pateikti taikomųjų uždavinių kokybės parametrų vertinimo ypatumai. Išskiriamas Petri tinklų panaudojimas elektroninių paslaugų sistemoms modeliuoti ir kokybės parametrams vertinti..

Antroje darbo dalyje išskiriama problemos analizė. Pateikiami elektroninių paslaugų ypatumai. Svarbiausiu kokybės parametru išskirtas patikimumas. Analizuojami naudojami sistemos patikimumo modeliai. Išskiriamas stochastinių Petri tinklų naudojimas modeliuojant patikimumą.

Trečioje darbo dalyje pateikiamas kokybės parametrų formalizavimas. Pristatomi du elektroninės paslaugos modeliai. Atliekami šių modelių kokybinių parametrų skaičiavimai. Atlikus rezultatų paliginimą realizuojamas kokybės parametrų gerinimo ir integruotojo kokybės parametro didinimo būdas.

Ketvirtoje dalyje pateikiamos tyrimo išvados bei rekomendacijos.

1. ELEKTRONINIŲ PASLAUGŲ KŪRIMO PROBLEMŲ ANALIZĖ LITERATŪROJE

1.1. Informacijos apsaugos svarba

Informacinės saugos problemos tyrinėjamos ir sprendžiamos jau seniai. Ypač jos aktualios dabar, kada plačiai plinta lokalūs ir globalūs tinklai. Informacinės saugos problema yra viena iš pagrindinių atvirųjų sistemų teorijos ir praktikos problemų. Pradžioje šios problemos sprendimu daugiausia užsiiminėjo valstybinės organizacijos, turinčios slaptą informaciją arba užsiimančios saugumo užtikrinimu. 1983 metais JAV gynybos ministerija išleido knygą "Patikimų kompiuterinių sistemų įvertinimo kriterijai" (*Tmsted Computer System Evaluation Criteria*, TCSEC), vadinamą dar „Oranžine knyga", kadangi jos viršelis yra oranžinės spalvos. Ši knyga pradėjo sistematinį žinių apie informacinį saugumą plitimą už valstybinių organizacijų ribų. Devintame dešimtmetyje analogiškos paskirties dokumentai buvo publikuoti daugelyje Europos šalių, pvz., 1991 metais Londone išleista knyga "Informacinių technologijų saugumo įvertinimo kriterijai", paruošta Prancūzijos, Vokietijos, Nyderlandų ir Jungtinės karalystės specialistų (*Information Technology Security Evaluation Criteria,* ITSEC).

Apsaugos priemonės turi užtikrinti informacijos konfidencialumą, aktualumą, prieinamumą. Bet jeigu valstybinėms organizacijoms svarbiausia informacijos konfidencialumas, o informacijos aktualumas suprantamas kaip informacijos pastovumas, tai komercinėms struktūroms svarbiausia informacijos aktualumas ir duomenų bei jų apdorojimo paslaugų prieinamumas [5]. Komercinės organizacijos, palyginti su valstybinėmis, yra atviresnės ir dinamiškesnės, todėl grėsmė joms skiriasi ir kiekybiniu, ir kokybiniu atžvilgiu.

Įvairios paskirties kompiuterinių sistemų informacinės saugos užtikrinimas yra viena iš opiausių informacinių technologijų problemų. Galima konstatuoti, kad nepaisant daugelio organizacijų, dirbančių šioje srityje, pastangų, ši problema nėra išspręsta.

Užfiksuojama vis daugiau informacinės saugos incidentų, turinčių sunkias pasekmes didelėms organizacijoms. Šio augimo pagrindinės priežastys yra dvi [28]:

Augantis informacinių technologijų verslo ir valdymo procesuose vaidmuo, ir to pasekoje didėjantys reikalavimai informacinei saugai kompiuterinėse sistemose. Auganti klaidų ir trikių „kaina" informacinėse sistemose.

Didėja informacinių procesų sudėtingumas. Tai kelia padidintus reikalavimus personalo, atsakingo už informacinę saugą, kvalifikacijai. Adekvačių sprendimų,

užtikrinančių priimtiną informacinę saugą už atitinkamą kainą, priėmimas tampa vis sudėtingesniu uždaviniu.

Pirma priežastis objektyvi, jai galima tik priešpastatyti organizacijos sugebėjimą tenkinti augančius reikalavimus informacinės saugos srityje.

Antros priežasties neutralizavimui būtina atitinkama personalo, atsakingo už informacinę saugą, kvalifikacija ir objektyvus informacinės saugos užtikrinimo posistemės įvertinimas.

Informacijos saugumas yra gyvybiškai svarbus verslo sėkmei. Duomenis apie finansinę padėtį, produktų gamybą, prekes, saugomas sandėlyje, ir kt. ypač svarbu patikimai saugoti. Nuo to priklauso kiekvieno verslo sėkmė. Netgi menkutis informacijos nutekėjimas apie gamybos ir pirkimo planus, apie tiekėjus ir klientus gali privesti įmonę prie bankroto ribos. Pagrindinis saugumo uždavinys – kontroliuoti ir saugoti priėjimą prie bendrų įmonės duomenų.

Informacijos saugumo svarba pabrėžtina ne tik verslui. Informacijos saugumas ypač svarbus valstybinėms organizacijoms, kur duomenų nutekėjimas gali priversti prie katastrofinių padarinių. Taip pat informacija ir jos saugumas yra svarbus dalykas įvairioms kitoms struktūroms, nepelno organizacijoms, viešos paskirties įmonėms bei asmeniniam vartojimui.

Taigi informacijos saugumas yra svarbus uždavinys bet kuriai įmonei, organizacijai ar paprastai sistemai.

Darbe bus apžvelgtos galimos grėsmes informacinės sistemos saugai pradedant fizinėmis ir baigiant kompiuterių tinklo grėsmėmis, taip pat bus analizuojami vartotojų autentifikavimo ir patikimi informacijos perdavimo būdai.

1.1.1. Fizinės grėsmės

Kalbant apie fizines saugumo grėsmes, turime omenyje ne tik tai tinklo įrangą ir serverius, bet taip pat ir klientus ir jų aplinką. Nėra prasmės saugoti konfidencialius failus apsaugotame serveryje, jeigu jo kopija yra vartotojo pamestame diskelyje ar nešiojamame kompiuteryje. Norint apsaugoti informaciją reikia pasirūpinti visos aplinkos fizinės apsaugos priemonėmis.

Kompiuterių tinklas ir visa jame esanti informacija negali būti labiau apsaugota nei patalpos, kuriose yra techninė įranga. Reikia apsaugoti patalpas ir nuolat tikrinti ir analizuoti saugą. Tikrinti, kas lankosi patalpose, turi būti rutininė procedūra.

Priėjimas prie techninės įrangos turi būti leidžiamas tik esant realiems poreikiams, techninėmis priemonėmis turi naudotis tik tie, kam tai yra būtina [17].

Nevykusiai prijungti nešiojami kompiuteriai gali tapti saugos grėsme. Pažeidėjas gali pavogti kompiuterį arba vieną iš jo komponentų, pavyzdžiui, standųjį diską. Be to, dirbant ne kontoroje, aplinkoje esantys žmonės gali „nužiūrėti" informaciją iš kompiuterio [17].

Vidaus susirašinėjimas dažnai gali sukelti rimtą pavojų saugumui. Daugelyje kompanijų pranešimai išsiuntinėjami pagal didelį sąrašą ir prarandama kontrolė, kaip gavėjai elgiasi su pranešimais. Svarbūs užrašai išmėtyti ant stalų ar išmesti į šiukšlių dėžę gali sukelti problemas. Reikia rūpintis laiškais taip pat, kaip ir kompiuteriniais duomenimis. Veiksmai turi būti adekvatūs informacijos svarbai. Reikia apibrėžti darbo su konfidencialia informacija taisykles.

Serveriai – tai tikriausiai patys vertingiausi tinklo įrenginiai. Jų apsaugai reikia skirti ypatingai daug dėmesio.

Kabelinė bei komutacinė įranga taip gali būti lengvai pažeidžiami elementai, jeigu jie yra sumontuoti lengvai prieinamose ir neapsaugotose vietose.

1.1.2. Tinklinės grėsmės

Pagrindinės informacinės (kompiuterinės) saugos sąvokos

Grėsmė kompiuterinės sistemos saugai – tai potencialiai galimas įvykis, tyčinis ar ne, kuris gali nepageidaujamai paveikti pačią sistemą, taip pat joje saugomą informaciją.

Kompiuterinės sistemos pažeidžiamumas – tai tam tikra charakteristika, kuri leidžia įvykti grėsmei. Kitaip sakant, būtent dėl sistemos pažeidžiamumo įvyksta nepageidautini įvykiai.

Kompiuterinės sistemos ataka – tai sąmoningas piktavalio veiksmas, kuriuo siekiama atrasti ir pasinaudoti tuo ar kitu sistemos pažeidžiamumu [17]. Taigi ataka – tai grėsmės realizacija. Beje, atakos gali būti ir atsitiktiniai veiksmai, dažnai būna neįmanoma atskirti sąmoningus ir atsitiktinius veiksmus, ir gera apsaugos sistema turi adekvačiai reaguoti į bet kurį iš jų.

Paprastai skiriamos trys pagrindinės saugos grėsmių rūšys – tai informacijos atskleidimo, integralumo ir aptarnavimo atsakymo grėsmės [17].

Informacijos atskleidimo grėsmė kyla tada , kai informacija tampa žinoma tiems, kurie neturėtų jos žinoti. Kompiuterinės saugos terminais informacijos atskleidimo grėsmė gali būti realizuota tada, kada priėjimas prie konfidencialios informacijos, saugomos kompiuterinėje sistemoje arba perduodamos iš vienos sistemos į kitą tampa galimas.

Integralumo grėsmė – tai bet koks sąmoningas duomenų, saugojamų kompiuterinėje sistemoje arba perduodamų iš vienos į kitą, pakeitimas (modifikavimas arba ištrynimas). Paprastai laikoma, kad informacijos atskleidimo grėsmė būdingesnė valstybinėms struktūroms, o informacijos integralumo grėsmė – verslo ir komercinėms struktūroms.

Aptarnavimo atsakymo grėsmė yra tada, kai dėl kažkokių veiksmų yra blokuojamas priėjimas prie kompiuterinės sistemos resursų. Realiai blokavimas gali būti nuolatinis, todėl reikiamas resursas niekada nebus gautas arba gali pasireikšti reikiamo resurso užlaikymu pakankamai ilgai, kad jis tampa nereikšmingu.

Kompiuterinių tinklų saugumo ypatybės

Tinklinių sistemų pagrindinė ypatybė yra tai, kad jų komponentai paskirstyti erdvėje ir ryšys tarp jų fiziškai atliekamas tinkliniais sujungimais (koksealiniais kabeliais, vytomis poromis, optiniais kabeliais ir t.t.) ir programiškai – pranešimais.

Tinklinėms sistemoms charakteringa tai, kad šalia lokalių atakų, vykdomų vienos kompiuterinės sistemos ribose, joms galimos specifinės atakos, sąlygotos resursų ir informacijos paskirstymo erdvėje [28]. Tai vadinamosios tinklinės (nutolusios) atakos. Joms pirmiausia charakteringa tai, kad įsilaužėlis gali būti už tūkstančių kilometrų nuo objekto ir, antra, atakuojama gali būti ne konkretus kompiuteris, bet informacija perduodama tinklu. Vystantis lokaliems ir globaliems tinklams būtent tinklinės atakos vyrauja ir pagal bandymų kiekį, ir pagal jų sėkmę, todėl būtent informacinės saugos nuo tinklinių atakų užtikrinimas įgauna pagrindinę reikšmę. Paskirstytųjų kompiuterinių sistemų specifika yra tokia, kad jeigu lokalioms kompiuterinėms sistemoms dažniausiai kildavo informacijos atskleidimo ir integralumo grėsmės, tai tinklinėms sistemoms į pirmą vietą išeina aptarnavimo atsakymo grėsmė [28].

1.1.3. Patikimi vartotojų tapatybės atpažinimo būdai

Vartotojų tapatybės atpažinimas arba autentifikacija – vienas pirmų vartotojų registracijos bet kokioje informacijos sistemoje etapų. Visos informacinės sistemos saugumas priklauso nuo to, kaip griežtai ir patikimai atliekamas vartotojų tapatybės atpažinimas [22].

Daugumoje sistemų naudojama standartinė vienpakopė autentifikacija. Vartotojas atpažįstamas jam įrašius vartotojo vardą ir slaptažodį. Šis būdas jau senokai naudojamas, patogus tuo, kad lengvai įgyvendinamas, gali būti naudojami pakankamai sudėtingi slaptažodžiai. Tačiau jis turi begalę trūkumų. Vartotojas gali užsirašyti savo įėjimo į sistemą vardą bei slaptažodį ir prisiklijuoti tokį lapelį visiems matomoje vietoje, gali atsitiktinai jį

pamesti, o gal ir tyčia „paskolinti" draugui. Gali atsitikti ir taip, kad buvęs darbuotojas, net išėjęs iš darbo, ir toliau turės priėjimą prie svarbių įmonės duomenų.

Siekiant didesnio informacijos saugumo gali būti naudojama dvipakopė autentifikacija [22]. Priėjimas prie svarbios informacijos ribojamas ne tik vartotojo vardu ir slaptažodžiu, bet ir dar viena priemone, pavyzdžiui, panaudojant intelektualiąją kortelę ar elektroninį raktą. Šis sprendimas leidžia išvengti minėtų vienpakopės autentifikacijos trūkumų. Pavyzdžiui, prieš išeidamas iš darbo buvęs darbuotojas privalo priduoti elektroninį raktą ir priėjimas prie įmonės duomenų jam užkertamas.

Dauguma šiuo metu naudojamų operacinių sistemų ir programų pritaikytos ir vienpakopei, ir dvipakopei autentifikacijai. Pvz., operacinės sistemos „Microsoft Windows" 2000/XP versijos pagal nutylėjimą pritaikytos vienpakopei autentifikacijai, tačiau jos gali būti lengvai pritaikytos ir dvipakopei autentifikacijai. Šiuo priėjimo prie sistemos atveju vartotojas turi naudotis intelektualiąja kortele ar el. raktu ir turėti savo PIN kodą.

1.1.4. Patikimo informacijos perdavimo užtikrinimo būdai

Vis labiau plintant elektroniniams informacijos saugojimo ir perdavimo būdams, tampa sunkiau garantuoti, kad ją pasieks tik tie, kuriems ji skirta. Atsiranda poreikis tokių priemonių, kurios užkoduoja duomenis, arba suteikia galimybę jais pasinaudoti tik ribotam asmenų skaičiui.

Didžiuliai kiekiai informacijos keliauja ryšio tinklais aplink pasaulį. Jų pralaidumas vis didėja, tačiau jie nėra saugūs. Siunčiančios duomenis organizacijos nenori, kad jų informacija būtų prieinama bet kam. Tam siūlomi sprendimai, užtikrinantys ISDN, GSM, VPN, ATM, radijo, fakso ir kt. ryšio linijų slaptumą vyriausybinėms, gynybos, diplomatinėms bei privačioms organizacijoms [22].

Pokyčiai bankuose vyksta vis greičiau. Sparčiai vystosi telefoninė ir internetinė bankininkystė. Tai suteikia naujas galimybes, tačiau kartu sukelia saugumo ir konfidencialumo problemas. Vis plačiau rinkoje siūlomi sprendimai, naudojant naujausias kriptografijos technologijas. Tai leidžia klientams labai paprastai ir patikimai prisijungti prie sudėtingų sistemų.

Reziumuojant atliktą informacinės saugos analizę galima teigti:

- Apžvelgtos fizinės ir kompiuterinių tinklų grėsmės organizacijose ir jų informacinėse sistemose, tuo pačiu ir išanalizuota informacijos apsaugos taikymo sritys šiose dalyse. Išanalizuotos fizinės apsaugos problemos, taip pat ir kompiuterinių tinklų saugumo ypatybės.

- Išnagrinėti patikimi vartotojų tapatybės atpažinimo būdai. Susipažinta su metodais, taikomais autentifikacijos srityje.
- Susipažinta su patikimo informacijos perdavimo užtikrinimo būdais. Išanalizuota, kokie metodai naudojami kriptografijoje, perduodant informaciją ryšio tinklais.

1.2. Elektroninių paslaugų samprata

1.2.1. Elektroninės viešosios paslaugos

Viešųjų elektroninių paslaugų teikimas pastaruoju metu yra viena iš svarbiausių, o neretai ir pati svarbiausia daugelio pasaulio valstybių vyriausybių strategijos dalis. Daugelio šalių vyriausybės įžvelgia didelę naudą pereinant nuo viešųjų paslaugų teikimo įprastais būdais (daugeliu atvejų grįstų tiesioginiu bendravimu bei popierinių formų pildymu) prie viešųjų paslaugų teikimo elektroninėmis formomis. Jeigu 1996 metais pasaulyje buvo tiktai trijų vyriausybių iniciatyvos, susijusios su viešųjų elektroninių paslaugų teikimu, tai dabar jų priskaičiuojama daugiau nei 500.

Perėjimas nuo viešųjų paslaugų teikimo įprastais būdais prie viešųjų paslaugų teikimo elektroninėmis formomis (daugiausia – internetu), yra ne tik pageidaujamas piliečių, bet ir suteikia pranašumų pačioms vyriausybėms.

Šiame darbe kaip informacinė sistema pasirinkta El. Valdžios sistema. El. Valdžia nagrinėjama kaip sistema, jungianti vidinius, išorinius procesus bei nuotolinį priėjimą prie sistemos. Naudojant informacines technologijas, vidinių procesų pagrindu sąveikauja valdžios institucijos. Išorinių procesų dėka yra galimas verslo, įvairių organizacijų ir bendruomenių pasijungimas prie valdžios institucijų resursų. Piliečiai, naudodami interneto ryšį, turi priėjimo teisę prie valdžios institucijų teikiamos informacijos.

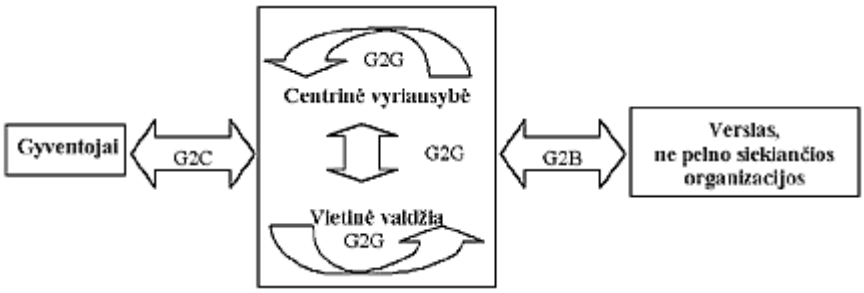
El. Valdžia – tai informacijos ir komunikacijos technologijų (IKT) panaudojimas tam, kad būtų pagerinta viešųjų organizacijų veikla.

Yra trys pagrindinės El. Valdžios sritys:

- Valdžios procesų tobulinimas: el. Administravimas;
- Piliečių pajungimas: el. Piliečiai ir el. Paslaugos;
- Išorinių sąveikų kūrimas: el. Visuomenė;

Pagrindinis viešųjų elektroninių paslaugų teikimo tikslas paprastai yra siekis pagerinti trijų pagrindinių šalių – gyventojų, verslo įmonių ir vyriausybės – poreikių tenkinimą bei

supaprastinti jų tarpusavio bendravimą ir komunikavimą. Žemiau pateiktoje diagramoje pavaizduota daugelio analitikų naudojama bendra elektroninės vyriausybės schema.



1 pav. Elektroninės Valdžios modelis [11]

El. Valdžioje informacijos ir komunikacijos technologijos taikomos šiose srityse [11]:

- Valdžia ir Piliečiai (G2C *Government and Citizens*)
- Valdžia ir Verslas (G2B)
- Valdžia ir Valdžia (G2G)

Įdiegus viešųjų paslaugų teikimą elektroninėmis formomis, gyventojai ir verslo bendrovės gali gauti paslaugas greičiau ir kur kas efektyviau. Be to, elektroninis paslaugų teikimo būdas leidžia išvengti daugelio techninių klaidų.

1.2.2. Elektroninės valdžios samprata

Informacijos technologijų panaudojimo galimybės viešojo administravimo sektoriaus darbo modernizavimui yra labai plačios. Vis didėjantis informacijos technologijų naudojimas, ypač galimybė naudotis internetu, iš esmės keičia valdžios veiklos galimybes.

Įgyvendinant elektroninės valdžios projektus, sukuriamos paslaugos per internetą, kurios leidžia patogiau bendrauti su valdžios institucijomis. Be abejo, tai įtakos vartotojų, norinčių gauti valdžios paslaugas patogesniais elektroniniais kanalais, skaičių.

Be abejo, tai pajus tiek paprasti Lietuvos gyventojai, tiek verslo bendrovės, tiek ir pačios viešojo administravimo institucijos.

Vis prieinamesnis internetas ir kompiuterinė technika sparčiai keičia daugelio gyventojų gyvenimą, kuriamos naujos paslaugos, o jau esančios pradedamos teikti naujais būdais. Tinkamai pritaikius informacijos technologijas galima [11]:

- sukurti geresnį priėjimą prie informacijos ir paslaugų;
- ginti piliečių interesus interneto tinkle;

- pagelbėti neįgaliems gyventojams efektyviau integruotis į visuomenę;
- paslaugas teikti įvairiais nuotoliniais kanalais;
- paslaugas suskirstyti pagal rinkos dalies poreikius, geriau tenkinti tikslinių grupių poreikius;
- efektyviau reaguoti į klientų pranešimus apie paslaugų kokybę ir turinį;
- įtraukti vartotojus į paslaugų pertvarkymą ir tobulinimą.

1.2.3. Elektroninės valdžios paslaugų teikimo techniniai sprendimai

Elektroninės valdžios projektų įgyvendinimo sėkmė labai priklauso nuo prieigos prie paslaugos greitaveikos užtikrinimo. Gyventojams turi būti sudarytos sąlygos lengvai ir patogiai naudotis šiomis paslaugomis. Numatoma, kad lengvą prieinamumą prie elektroninės valdžios teikiamos informacijos ir paslaugų užtikrins ir tai, kad sąsajai su vartotoju bus naudojamos paplitusios atviros technologijos.

Įgyvendinant elektroninės valdžios projektus, pasak Lietuvos Vyriausybės, prioritetų nenumatyta teikti jokiems konkretiems techniniams sprendimams, operacinei sistemai ar įrangos gamintojui. Kiekvienu atveju apsisprendimą turi lemti funkcionalumo, saugumo, tolesnio plėtimo galimybių ir kainos veiksniai.

Perkeltos į internetą paslaugos turi būti prieinamos populiariais ir visuotinai naudojamais protokolais bei įrenginiais. Kiekvieno projekto atveju pagal paslaugos gavėjų poreikius, turi būti sprendžiama, kaip paslaugos turi būti teikiamos. Taip bus užtikrinama tinkama paslaugų prieinamumo kokybė, vartotojo „neprisirišimas" prie konkrečių gamintojų.

Viešojo administravimo institucijos sudaro galimybes verslo subjektams turimą viešą informaciją panaudoti komercinėms paslaugoms kurti ir realizuoti.

Informacija turi būti pateikiama atvirais formatais. Valstybės institucijų naudojami bendravimo protokolai ir formatai neturi versti informacijos naudotojų įsigyti mokamas operacines sistemas ar programinę įrangą.

1.2.4. Saugumas, elektroninio dokumento autentiškumo užtikrinimas

El. dokumentas – paruoštas, saugomas ir perduodamas informacinių technologijų priemonėmis, su įstaigos veikla susijęs jos parengtas ar gautas ir į įstaigos dokumentų apskaitos sistemas įtrauktas dokumentas, prie kurio prijungtas elektroninis parašas [3].

El. dokumentą patvirtinusio asmens tapatumo patvirtinimui ir el. dokumento autentiškumui užtikrinti turi būti naudojamas asimetrinių raktų poros tipo elektroninis parašas

patvirtintas sertifikatu. Elektroninio parašo naudojimą nustato Lietuvos Respublikos elektroninio parašo įstatymas ir kiti teisės aktai. Rekomenduojami naudoti elektroninio parašo tipai ir algoritmai. Rekomenduojami naudoti elektroninio parašo tipai ir algoritmai nurodyti 1 Priede.

Elektroninio parašo kūrimą ir tikrinimą bei galiojimo patvirtinimą reglamentuoja elektroninio parašo taisyklės. Elektroninio parašo taisykles rengia ir tvirtina įgaliota el. dokumentų mainų priežiūros institucija.

Elektroninių parašų sertifikatų sudarymą ir naudojimą reglamentuoja sertifikatų taisyklės, kurias rengia ir įgyvendina sertifikavimo paslaugų teikėjas.

Siunčiamas el. dokumentas turi būti pasirašytas elektroniniu parašu. Priedai taip pat gali būti pasirašyti juos rengusių asmenų. El. dokumento bei jo priedų elektroninių parašų kiekis neribojamas.

Suformuotas siuntinys, kuriame yra el. dokumentas, priedai bei jų elektroniniai parašai ir sertifikatai taip pat kiti būtini papildomi duomenys, autentiškumo užtikrinimui turi būti pasirašytas įstaigos vadovo įgalioto asmens elektroniniu parašu. Šiems darbuotojams išduotų sertifikatų duomenys turi būti skelbiami kaip ir įstaigos elektroninio pašto adresas.

El. dokumentų mainų priemonės turi būti atsparios informacijos iškraipymui siuntimo metu, turi būti numatyta apsauga nuo neteisėtų siuntėjų. Rekomenduojama šiuos reikalavimus įgyvendinti darbo stočių, vidinių įstaigos tinklų bei vartotojų teisių administravimo priemonėmis.

Kokiose laikmenose bei kokias informacines technologijas naudojant turi būti kaupiamas el. dokumentų archyvas, kokiais formatais el. dokumentai turi būti saugomi. Rekomenduojamos informacinės technologijos bei el. dokumentų formatai nurodyti 1 Priede.

Siuntinių perdavimui turi būti naudojamas elektroninis paštas. Rekomenduojami siunčiamų el. dokumentų formatai nurodyti 1 Priede.

1.2.5. Virtualaus privataus tinklo panaudojimas elektroninės valdžios sistemoje

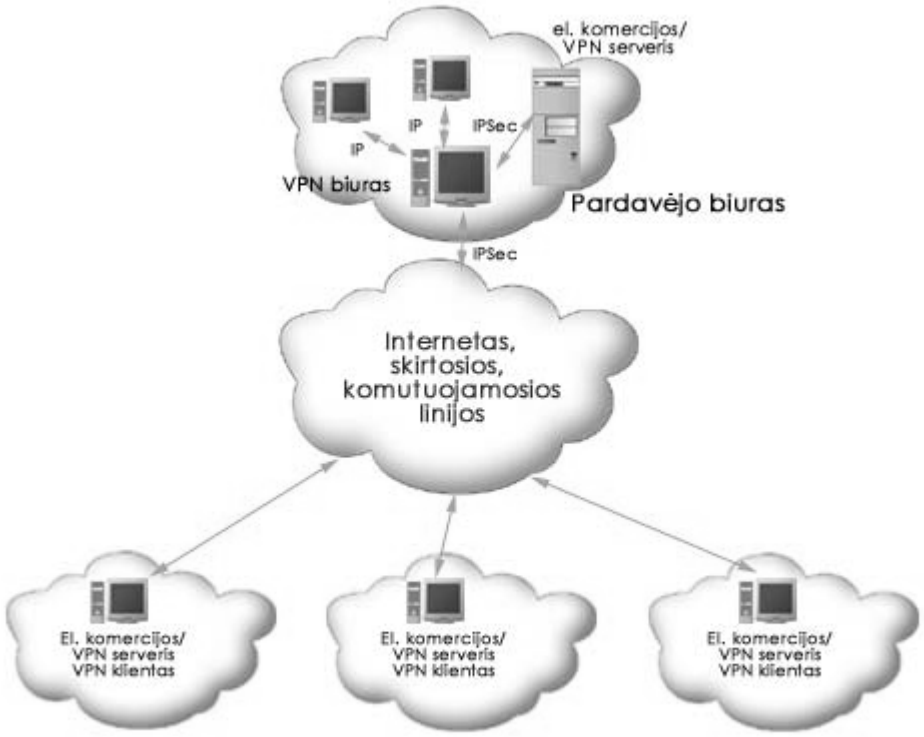
Virtualus privatus tinklas gali būti sėkmingai panaudotas visur, kur reikalinga informacijos ir procesų apsaugo. El. Valdžios sistemoje šie reikalavimai yra ypač aktualūs.

Centrinės vyriausybės ir vietinės valdžios bendradarbiavimui sėkmingai gali būti panaudotas „B2B" VPN sprendimas. Elektroninės komercijos tarp įmonių sistemos („B2B") turi tokių savitumų [35]:

- tam tikrą sistemos vartotojų skaičių (skirtingai nuo sistemos „B2C");

- dideles užsakymų apimtis ir dėl to didelį jautrumą įsibrovimams ir ryšio patikimumui;
- didelę taikomųjų protokolų įvairovę (ne tik HTTP);
- padidintus apsaugos reikalavimus.

Šiuo metu kuriama ir diegiama daug įvairių komercijai skirtų sistemų. 2 paveiksle pavaizduota „B2B" tipo sistemos apsauga.



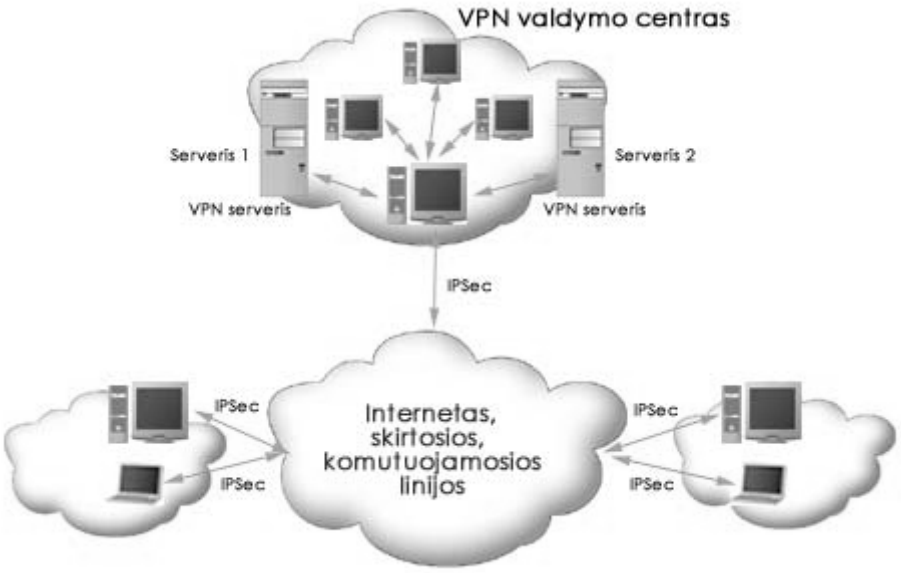
2 pav. „B2B" tipo sistemos apsauga [35]

Tarnybinei stočiai su bet kokio taikomosios sistemos „B2B" programine įranga apsaugoti įdiegiamas produktas "VPN-Server", o klientui priklausančioje sistemos dalyje, kurią turi verslo partneris – „VPN-Client". Produktas "VPN-Office" paslepia vidinio tinklo topologiją ir saugo jį nuo išorinių įsibrovimų iš Interneto bei neleistinos patekties.

Panaudojant kompleksinius VPN produktus galima sudaryti viso tinklo apsaugos sistemą ir tai aiškiai parodo jų privalumą prieš specializuotus VPN produktus, kurie saugo atskirų klasių taikomąsias programas. Plačiau apie VPN panaudojimą skaityti 3 priedą.

Valdžios ir piliečių, o taip pat valdžios ir verslo sąveikai gali būti panaudotas VPN sprendimas informacinių paslaugų tiekėjams.

Kiekvieno kliento darbo vietai apsaugoti įdiegiamas produktas “VPN-Client”, pagrindinėms ir atsarginėms tarnybinėms stotims – “VPN-Server”; nuosavame vidiniame tinkle kompanija tiekėja gali naudoti produktą “VPN-Office”.



3 pav. Patikimą klientų sistemų atskyrimą [35]

3 paveiksle pavaizduotas sprendimas užtikrina patikimą klientų sistemų atskyrimą, t.y. A kliento sistema (taikomoji programa, informacija, vartotojai) apsaugotųjų ryšių būdu yra izoliuota nuo B kliento sistemos. Plačiau apie VPN panaudojimą skaityti 3 priedą.

1.3. Petri tinklų panaudojimas sistemoms modeliuoti

Šiame darbe pasirinkta Petri tinklų sistemų projektavimo architektūra. Petri tinklai yra formalaus specifikavimo architektūra, labai tinkama modeliuoti ir analizuoti tiek lygiagrečius, tiek paskirstytus diskrečius įvykius dinaminėse, tuo pačiu ir el. paslaugų, sistemose. Pateikiami kartu su atitinkamais laiko įvertinimais, Petri tinklai leidžia projektuoti įvairių kokybinių parametrų modelius. Pavyzdžiui projektuojant našumo modelius, kuriuose realus lygiagretumas gali būti aprašomas kartu su sinchronizavimu ir paskirstymu [25**].**

Dar 1962 metais pasirodė pirmas darbas apie Petri tinklus. Jo autorius K. A. Petri (VFR) aprašė naują informacinių srautų sistemos modelį. Modelis buvo sudarytas remiantis prielaida, kad atskiros sistemos dalys funkcionuoja asinchroniškai ir konkuruoja tarpusavyje. Ryšiai tarp atskirų dalių buvo vaizduojami grafu arba tinklu. Dažniausiai Petri tinklai naudojami modeliuojant sistemas, kuriose vienu metu gali įvykti keletas įvykių ir yra apribojimai procesų dažnumui, sekai [24]. Įvykiams yra suteikiami prioriteto įvertinimai. Tai labai patogus informacinių procesų aprašymo būdas, kada valdymo sistemose vyksta konfliktinės situacijos, lygiagretūs atsitiktiniai ir nedeterminuoti procesai.

Petri tinklas yra matematinis metodas. Petri tinklų principas – keletas paprastų objektų, ryšių ir taisyklių, kurių dėka galima atvaizduoti labai sudėtingas elgsenas [24]. Dar tiksliau, Petri tinklas gali būti traktuojamas kaip grafų teorijos įrankis, tinkamas modeliuoti ir analizuoti diskrečių įvykių dinamines sistemas, kurios demonstruoja lygiagretų vystymąsi ir kurių funkcionavimas charakterizuojamas sinchronizacijos ir paskirstymo reiškiniais. Jie naudojami modeliuoti procesus įvairiose veiklos srityse, pavyzdžiui, komunikacijų tinklai, kompiuterinės sistemos ir atskirų dalių gamybos sistemos.

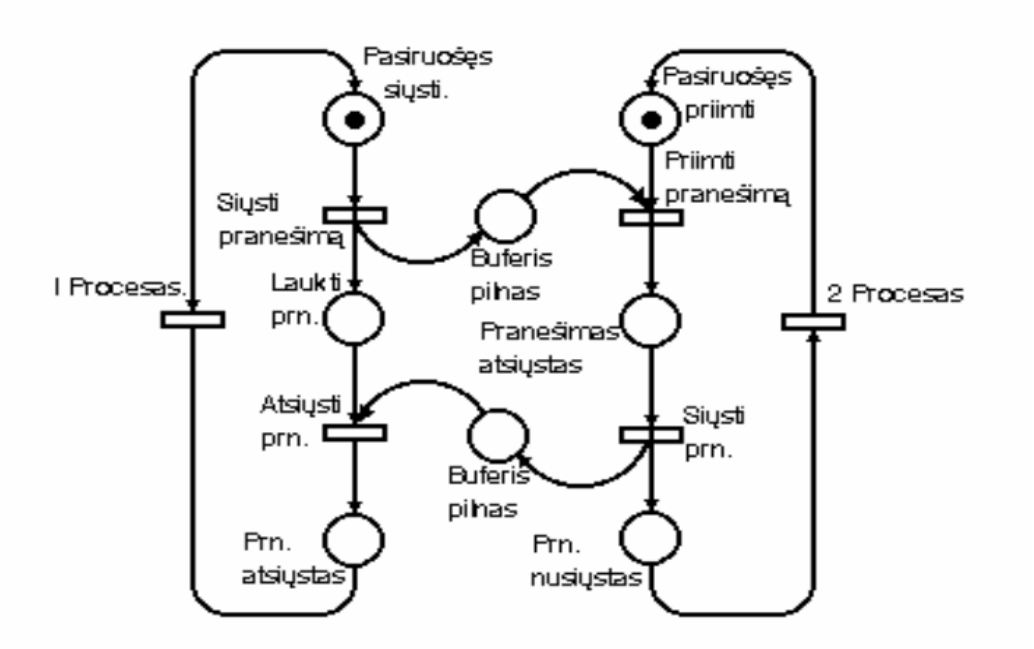
Labai plačios yra Petri tinklų taikymo sritys [24]:

1. Paskirstytosios duomenų bazes. 2. Lygiagretus programavimas. 3. Lanksti gamyba. 4. Diskrečių įvykių sistemos. 5. Daugiaprocesorinės sistemos. 6. Didelio duomenų srauto apdorojimas. 7. Kompiliatoriai ir operacinės sistemos. 8. Loginis programavimas. 9. Neuroniniai tinklai. 10. Formaliosios kalbos. 11. Asinchroninės grandinės ir struktūros.

Loginė (kokybinė) analizė nagrinėja tokias savybes, kaip išlaisvinimas iš mirties taško ar persipildymų nebūvimas. Pagrindinis šios analizės tikslas yra modeliuojamos sistemos korektiškumo įrodymas. Našumo (kiekybinė) analizė nagrinėja tokius matavimo vienetus kaip pralaidumo ar panaudojimo rodikliai. Tai leidžia vertinti modeliuojamos sistemos efektyvumą. Elgsenų, kurios gali būti aprašomos Petri tinklų modeliais, sudėtingumas parodo tai, kad efektyvaus našumo analizės metodika yra pagrįsta loginėmis savybėmis.

Petri tinklai projektuojami naudojant dvi objektų rūšis: būsenas (apskritimai), kurios parodo būsenų kintamuosius ir perėjimus (stačiakampiai), kurie parodo būsenų pasikeitimų veiksmus. Svorinio srauto ryšiai leidžia paprastai atvaizduoti būsenų įėjimus ir išėjimus.

Pateikiamas Petri tinklų panaudojimo pavyzdys. 4 paveiksle pavaizduotas tinklas yra labai paprastas ryšių tarp dviejų procesų Petri tinklo modelis. Jame sistemos būsenos pavaizduotos apskritimais, perėjimai iš vienos būsenos į kita atvaizduoti rodyklėmis ir atitinkamais procesais – stačiakampiais. Taškas apskritime reiškia pradinę sistemos padėtį, šiuo atveju sistema pasiruošusi siųsti ir pasiruošusi priimti pranešimą.



4 pav. Petri tinklų panaudojimo pavyzdys [24]

Šiuolaikinės valdymo sistemos daugiausia yra hibridinės – tolydiniai ar mišrūs objektai valdomi diskretiniais valdikliais. Valdymo algoritmui modeliuoti puikiai tinka spalvotieji Petri tinklai [24]. Ypatingą reikšmę įgauna sąsaja tarp šių modelio dalių ir laiko įvertinimas, nes laikas (laiko momentas) gali būti vienas iš valdančiųjų faktorių.

Projektuojant įvairias informacines sistemas patogu naudoti Petri tinklų architektūrą. Su ja galima nagrinėti sistemą ypač detaliai, nes kiekvienas sistemos žingsnis aprašomas atskirais komponentais.

Projektuojant kiekvieną sistemą, ir užsakovui ir sistemos kūrėjui svarbūs yra šie kriterijai: sistemos lankstumas, patikimumas, našumas ir, žinoma, kaina. Taigi kuriant el. Paslaugų sistemą kiekviename žingsnyje yra naudojama Petri tinklų architektūra.

Kiekviena sistemos posistemė turi būti suskaidoma į komponentus – operacijas ir būsenas. Reikiamose suskaidytos sistemos vietose turi būti realizuoti atitinkami informacijos apsaugos metodai (reikiamos apsaugos operacijos).

Taip pat naudojant Petri tinklus būtina ištirti sistemos lankstumą, patikimumą bei našumą, tam, kad būtų pasiektas optimalus sistemos variantas. Be abejo, iš atskirų sistemos elementų turi būti paskaičiuota sistemos kainą. Jei sistemos kūrėjų ar užsakovų netenkina suprojektuotos sistemos lankstumas, patikimumas, našumas ar kaina, tokia sistema turi būti suprojektuota iš naujo, ir joje turi būti pasiektas optimalus lankstumo, patikimumo, našumo ir kainos variantas.

1.4. Taikomųjų uždavinių kokybės parametrų vertinimo ypatumai

Įmonės kuria el. paslaugas, kurios pasiekiamos per internetą, tam, kad gautų papildomas pajamas iš naujų šaltinių arba tam, kad padidintų įmonės darbo efektyvumą. Mišrios el. paslaugos, kurias sudaro įvairios el. paslaugos teikiamos iš įvairių paslaugų tiekėjų yra labiau priimtinos ir reikiamos vartotojams. Siūloma nauja platforma ar sistema, kuri palaiko el. paslaugų metaduomenis. Ji leidžia mišrių el. paslaugų modeliavimą, kūrimą bei pateikimą ir rekomendavimą vartotojams [13]. Mišrios el. paslaugos yra modeliuojamos naudojant UML (*Unified Model Language*) diagramas, kuriose ECA (*Event/Condition/Action* – Įvykis/Būsena/Procesas) taisyklės naudojamos valdyti el. paslaugų patvirtinimų sekas ir parinkti el. paslaugos tiekėjus. Be to projektuojami dviejų lygių el. paslaugų metaduomenys tam, kad išplėsti universalaus aprašymo, pateikimo ir integravimo (UDDI – *Universal Description, Discovery and Integration*) standartus ir tai įgalinti semantinę el. paslaugų paiešką ir atranką. Galiausiai duomenų surinkimo tikslas yra pasiūlyti surasti dažniausiai ieškomas el. paslaugas ir dažniausius pasirenkamas el. paslaugas. Atsižvelgiant į duomenų atrankos pasiūlytą platformą ar sistemą vartotojui pateikiama dažniausių *N* kiekio mišrių el. paslaugų sąrašų rekomendacijos. Galutinis rezultatas yra tarsi dažniausiai ieškomų arba pasirenkamų el. paslaugų sąrašas.

Taip pat moksliniuose leidiniuose kalbama apie sistemų modeliavimą ir kaip jas reikėtų modeliuoti bei į kokius sistemos vertinimo parametrus reikėtų atkreipti dėmesį prieš jas kuriant. Aiškinama užduočių modelių ir sistemų modelių apjungimo galimybės [21]. Demonstruojama, kaip formalių uždavinių modelio panaudojimas gali pagerinti interaktyvių sistemų projektavimą. Tai daroma pateikiant kiekybinius skaičiavimų rezultatus, kuriais remiantis projektuotojai gali lengviau pasirinkti ir pagrįsti savo sprendimus. Taip pat pateikiama, kad yra galimybė apibūdinti ir uždavinių, ir sistemų modelius ta pačia formalia struktūra ir vertėtų tai daryti. Tai mus pirmiausiai leidžia formaliai įrodyti, kad uždaviniai ir sistemos tarpusavyje susietos struktūriškai, taip pat įgalina vykdyti kiekybinius skaičiavimus ir analizuoti duomenis naudojant uždaviniu ir sistemų modelių kombinacijas. Pateikiamas pavyzdys, leidžiantis vystyti ir uždavinių, ir sistemų modelius, ir atlikti keleta projektavimo proceso iteracijų. Aparatas (galima apibūdinti sistema) ir skaičiavimų uždaviniai yra modeliuojami naudojant ICO (*Interactive Cooperative Objects* – sąveikaujantys bendradarbiaujantys objektai) formalizavimą, kuris pagrįstas „Petri tinklų" modeliavimo architektūra ir objektiškai orientuota logika. „Petri tinklų" architektūra leidžia aksiomiškai patvirtinti izoliuotų ir sąveikaujančių posistemių naudojimą [21].

Analizuojant mokslinę literatūrą, kurioje nagrinėjami kokybės parametrai, pastebima tai, kad jie pasirenkami po viena arba kelis. Pavyzdžiui, kalbama tik apie lankstumą arba tik apie patikimumą, arba našumo ir patikimumo tarpusavio sąveika ir panašiai. Kai kuriuose moksliniuose leidiniuose paminimi ir visi keturi kokybės parametrai (lankstumas, patikimumas, našumas, kaina), tačiau detalaus jų tarpusavio vertinimo nėra.

Lankstumo analizė

Lankstumą tiriančiuose straipsniuose nagrinėjami įvairūs vertinimo būdai. Apibūdinama pasiūla pagrįsta lanksčios perdavimo linijos scheminio projektavimo sistema (*FTL – flexible transfer line*) [33]. Yra pasiūlyta lanksčios perdavimo linijos scheminio projektavimo sistemos architektūra (FTLSDS). Sistemą susidaro keturi procesai: dalinių charakteristikų modeliavimo, procesų planavimo, FTL galimybių pateikimo ir FTL skaičiavimų. FTL scheminiam projektavimui yra pasiūlyta penkių lygių procesų planavimo strategija, kuri vadinama hierarchiniu procesų planavimo modeliu. Metodas paremtas apdorojimo operacijos parinkimu, dalinės struktūros planavimu, savybių seka, operacijų seka ir procesų plano generavimu. Didžiausias dėmesys skiriamas struktūros planavimui. Realizuota modulinė mechanizmo projektavimo sistema palaikanti mechanizmo reikalavimus projektuojant FTL. Skaičiavimo procese analizuojama kokybė, lankstumas, patikimumas, mechanizmo užkrovimas ir kaina.

Pastebimi naujoviškų būdų tyrimai, kurie leidžia pasiekti programinės įrangos lankstumą nuoseklių sistemų (workflow) aplinkoje. Manoma, kad apjungus nuoseklių sistemų (workflow) ir „protingųjų agentų“ (intelligent agent) technologijas į modernią informacinę sistemą, programinė įranga gali būti pagaminama tvirtesnė ar patikimesnė, labiau naši kainos ir palaikymo kaštų atžvilgiu ir lengviau koreguojama [33].

Nelson‘as yra išskyręs technologinį lankstumo vertinimą. Technologinis lankstumas apibūdinamas kaip techninės charakteristikos, kurios leidžia ar įgalina dalykinių procesų koregavimus ar kitokius pakeitimus. Pasiūlyta technologinio lankstumo įvertinimo struktūra, kuri apima modeliavimą, pakitimų priėmimą, struktūrinio lankstumo aspektų nuoseklumą, reakcijų (atsakymų) greitį (dažnį), įvertinimą ir procesų lankstumo įvertinimo veiksmų suderinimą.

Zhao pasiūlė dvi susietas programinės įrangos lankstumo sąvokas: sistemos prisitaikymas ir sistemos universalumą (įvairiapusiškumą). Sistemos prisitaikymas – tai gebėjimas modifikuoti sistemą tam, kad susitvarkyti su pagrindiniais pakitimais dalykiniuose

procesuose kuo mažiau įtakojant ir nepertraukiant dalykinių operacijų. Sistemos universalumas (tvirtumas) – tai sistemos gebėjimas leisti lanksčioms procedūroms reaguoti į procesų ar procedūrų prieštaravimus.

Deiter‘is, Goesmann‘as ir Loffeler‘is sutaria dėl idėjos lankstumą traktuoti kaip techninį, organizacinį ir žmogiškąjį. Jie lankstumą klasifikavo keturiais dėmenimis: procesų lankstumas, tarp-organizacinis lankstumas, lankstus valdymas ir žinios bei lankstus užduočių paskirstymas.

Viso šio programinės įrangos lankstumo vertinimo sąvokos buvo praplėstos ir apjungtos, o taip pat šie suvienyti rezultatai buvo pritaikyti lanksčių procesų technologijos vystymui [34].

Lanksčios nuoseklios sistemos

Nuoseklių sistemų technologijos ir tokių sistemų valdymo tyrimai yra susiję su lanksčių nuoseklų sistemų vystymu. Tokių teorijų pradininkai yra Klein‘as, Dellarocas‘as ir Bernstein‘as (2000). Jie teigia: „Nuoseklios sistemos turi būti adaptyvios tam, kad efektyviai palaikytų šiuolaikines dinamines, neapibrėžtas ir klaidų neišvengiančias bendradarbiavimu pagrįstas veiklos terpes. Nuoseklios sistemos šiuo metu mažai išnaudojamos palaikyti adaptyvius procesus. Dažniausiai sistemos neleidžia modifikuoti procesų, jei jie tuo metu vykdomi. Klaidos ar išimtys valdomos naudojant nuosekliai iš anksto apibrėžtomis sąlyginėmis šakomis visiems galimiems atsitiktinumams.” [34]

Tyrimų pagrindu yra pateikta keletas svarbių nurodymų kaip pasiekti nuoseklių sistemų lankstumą [34]:

a) Išimčių valdymas: klaidos toleravimas yra pagrindinis reikalavimas procesus palaikančioms sistemoms įskaitant nuoseklias sistemas. Hagen‘as ir Alonso (2000) pateikia sprendimą kaip realizuoti labiau patikimus procesus naudojant išimčių valdymo technologiją taip, kaip daroma programavimo kalbose.

b) Dinaminio modelio įvertinimas: besikeičiančių procesų modeliai turi būti valdomi dinaminis nuosekliais pakeitimas. Ellis ir Keddara (2000), pasinaudodami poslinkių modalumo sistematika ir procedūrinių pakeitimų nedviprasmiška specifikavimo kalba, pateikia nedviprasmiškai specifikuotų procesų pasikeitimo modelį.

c) Staiga iškylančių (*Emergent*) procesų modeliavimas: dar vienas bendrinis požiūris į dinaminę adaptaciją. Jis pagrįstas dalinai specifikuotų procesų

modeliu ir priklauso nuo lanksčių priėmimo sistemų, kuris tobulinamas ir koreguojamas vykdymo eigoje. (Kumar‘as ir Zhao, 1999, Faustmann‘as, 2000)

Mokslinėje literatūroje nuolat nagrinėjamos el. paslaugų (ir nuoseklių sistemų) specifikavimo patvirtinimo problemos. Norima sukurti efektyvias technologijas, kurios leistų konstruoti mišrias el. Paslaugas [13]. Taip pat būtina užtikrinti atitinkamas savybes (pvz., mirties taško išvengimas, resursų naudojimo ribos, užklausų ir atsakymų ribiniai laikai). Čia pateikiamas labai paprastas el. paslaugų modelis skirtas tyrimui ir išvadų patvirtinimui. Šis modelis pagrįstas tokiomis nuosekliomis el. paslaugų sistemomis, kaip AZTEC ir el. FLow [13]. Pirmiausia pateikiamas aprašymas, kaip trijų skirtingų modelio tyrimo metodikos panaudojamos, kai vykdomų procesų skaičius sistemoje yra ribotas ir iš anksto nustatytas. Toliau pateikiamas „pid skaičiavimų apribojimas” – naujas simbolinis išmatavimų pateikimo būdas, kuris gali užkoduoti neribotą sistemos būsenų skaičių. Šis būdas leidžia patikrinti sistemas, kurios neturi apibrėžtų ribų ir yra sudarytos iš dinaminių procesų. Manoma, kad tai įvairiapusė ir lanksti metodika, kuri tinkama el. paslaugų specifikacijom patvirtinti. Šią metodiką naudojant kartu su kitomis, pavyzdžiui, abstrakcija ir išplėtimu, įmanoma išspręsti įvairias el. paslaugų patvirtinimo problemas.

El. paslaugų sutrikimai ar gedimai potencialiai gali turėti skaudžius padarinius. Net paprasta el. paslauga dažniausiai susideda iš keletos, o kartais ir labai daug lygiagrečiai vykstančių procesų, pavyzdžiui, inventorizacijos valdymo, elektroninių apmokėjimų ar tiesioginių gaminių reklamavimų visuotiniame tinkle. Todėl el. paslaugų procesų projektavimas tampa vis sudėtingesnis. Projektavimo klaidos gali iškilti dėl įsiterpiančių kreipinių į bendrai naudojamus duomenis, procesų sinchronizacijos, dinaminių specifikuotų pasikeitimų ir labai dažnai dėl „žmogiškojo veiksnio”, kai įvyksta nesusipratimai programuotojams neteisingai interpretuojant verslo logikos specifikacijas. Taigi čia galimas įdomus sprendimas – vystyti savitus įrankius, skirtus padėti projektuoti el. paslaugų architektūras ir specifikacijas.

Pateikiamas supaprastintas el. paslaugų sistemos modelis [13]. Tokiame modelyje yra nuosekliose sistemose vyraujančios savybės, tuo pačiu jis yra pakankamai paprastas formaliam verifikavimui. Modelyje leidžiami dinaminiai procesai, įvairūs duomenų tipai, globalūs kintamieji, kuriuos naudoja lygiagretūs procesai, ir įvairiapusiškas tarpprocesinis sinchronizavimas.

Patikimumo ir našumo analizė

Kuriamos paslaugų sistemos išankstinis našumo apskaičiavimas padeda projektuoti sistemas, kadangi pateikia atsakomąsias reakcijas ir projektavimo sprendimai lengvai gali būti pataisomi. Tačiau paskirstytos ir lygiagrečios paslaugų sistemos našumo modelio konstravimas reikalauja didelių pastangų. Yra siūlomi įvairūs šių pastangų mažinimo būdai. Siūlomas našumo modelio konstravimo pastangų sumažinimo būdas, pagrįstas lengvai specifikuojamais našumo kriterijais, empiriniais modelio parametrų skaičiavimais, automatiniu modelio generavimu ir įvairių modelio tipų palaikymu [16]. Prototipas naudojamas objektiškai orientuotos sistemos, kurioje priežastiniai (*causal, augio*) sistemos vykdymo eigos duomenys yra registruojami, apibūdinimui. Šie duomenys toliau apdorojami ir gaunamos resursų poreikių (*workthreads*) sekos. Taip pat sudaromi sistemos veikimo aprašymai (*workthread classes*) ir generuojami našumo modeliai. Ši metodika taip pat gali būti pritaikyta kituose sistemos kūrimo etapuose, tuo pačiu ir egzistuojančios sistemos perprojektavime.

Internetiniai portalai, kaip el. paslaugų sistemos, vis plačiau panaudojami, ir paslaugų įvairovė nuolat didėja. Šiomis dienomis plačiai naudojami internetiniai puslapiai, kuriuose vartotojai labai paprastais būdais gali atsisiųsti ir įdiegti programinę įrangą. Aprašomas tokių tinklapių našumas [21]. Jis gali būti prastas, jei naudojamasi bevieliais tinklais. Priežastis yra ta, kad reikiami resursai neadekvačiai panaudojami. Jei tokio tipo sistema suprojektuota naudojant mobilių agentų technologiją, tuomet problemos galima išvengti.

Dažniausiai našumas yra pagrindinė problema projektuojant, tobulinant ir konfigūruojant sistemas. Ne visuomet pakanka žinoti, kad sistema dirba tinkamai, taip pat svarbus ir jos efektyvumas. Yra daugybė sričių, kaip pavyzdžiui elektroninių paslaugų, kompiuterių ir telekomunikacijų sistemos, gamyba, krašto apsauga, sveikatos rūpyba ar transportavimas, kur sutrumpinamas veikimo laikas, sumažinama kaina, tuo pačiu taupomi pinigai ar netgi žmonių gyvybės gali būti išgelbėtos pagerinus sistemų našumą. Našumo analizė ir studijavimas remiasi egzistuojamų ar planuojamų sistemų skaičiavimu ir vertinimu, alternatyvių konfigūracijų palyginimu ar optimalios sistemos konfigūracijos radimu. Galima išskirti tris pagrindinius kriterijus, pagal kuriuos vertinamas sistemų našumas. Tai matavimas, analitiniai modeliai ir imitaciniai modeliai.

Pabrėžiamas spalvotųjų Petri tinklų panaudojimas analizuojant našumą [32]. Čia nagrinėjamos imituojamos sistemos. Spalvotieji Petri tinklai ypač tinkami modeliuoti ir analizuoti dideles ir sudėtingas sistemas dėl keletos priežasčių: jie remiasi intuityviu grafiniu

atvaizdavimu; jie yra įvykdomi; gali būti konstruojami hierarchiniai modeliai; yra galimybė modeliuoti įvairių sistemos procesų sugaištą laiką; ir egzistuoja pagrįsti bei išbandyti įrankiai, kurie skirti spalvotųjų Petri tinklų modelių kūrimui, imitavimui ir analizei.

Stochastiniai Petri tinklai yra naudingas modeliavimo įrankis, leidžiantis analizuoti sistemų našumą ir patikimumą. Kaip bebūtų, viena iš šių Petri tinklų panaudojimo problemų yra ta, kad įvykių pasiskirstymo laikai dažniausiai yra ribojami. Tai daroma tam, kad sukurti sistemos modelį labiau skaitinį-analitinį nei simuliuojamą.

Sistemos našumo matavimas gali pateikti tikslius vertinimo atsakymus. Projektuojama sistema matuojama tiesiogiai – nepaliekama jokių nefiksuotų smulkmenų ir nereikia jokių supaprastintų prielaidų. Kaip bebūtų matavimas yra vienintelis pasirinkimas, jei projektuojama sistema egzistuos realiai. Vykdomi matavimai gali būti tikslūs arba ne visiškai tikslūs. Tai priklauso nuo konkrečios sistemos būsenos. Pavyzdžiui, jei tinklo išnaudojimas matuojamas ne piko metu, tuomet negalima pateikti vidutinių tinklo išnaudojimo galimybių išvadų. Lygiai taip pat ir atliekant matavimus tik piko metu.

Analitiniai modeliai, tokie kaip Markovo modeliai, gali pateikti tikslius rezultatus skaičiuojant sistemų našumą. Rezultatai yra tikslūs, tuo pačiu jie nėra sistemos našumo įvertinimas. Kaip bebūtų, analitinių modelių pateikiami rezultatai gali būti tikslūs arba ne priklausomai nuo prielaidų, kurios buvo naudojamos kuriant patį modelį. Daugeliu atvejų yra sunku tiksliai modeliuoti realias pramonines sistemas naudojant analitinius modelius. Netgi yra nustatyta, kad analizuojant kompiuterines sistemas analitinis modeliavimas reikalauja tiek daug supaprastinimų ir prielaidų, kad net analitikai nustemba, jei gaunamas tikslus rezultatas [32].

Imitavimu pagrįsto našumo analizė gali būti naudojama kaip alternatyva analitiniams metodams. Imitavimas retai pateikia tikslius duomenis, tačiau taip įmanoma paskaičiuoti kokiu tikslumu gaunami paskaičiavimai. Be to gali būti sukurti ir analizuojami didesni ir labiau sudėtingi modeliai. Ir tam nereikia sistemą ribojančių prielaidų. Yra du pagrindiniai imitavimų naudojimo trūkumai: galimas laiko trūkumas vykdant reikiamus imitavimus, gali būti sudėtinga pasiekti pakankamai tikslius rezultatus. Imitavimu pagrįsto našumo modelio analizė pateikia statistiškai ištiriamus sistemos išėjimų duomenis, didelius tiriamų duomenų kiekius, atitinkamus atvaizdavimus ir imituojamų tyrimų pripažinimą bei patvirtinimą.

Našumo tyrimas tai ir menas ir mokslas. Vienas iš našumo analizės tyrimo menų yra žinojimas, kurią iš trijų analizės metodikų naudoti konkrečioje situacijoje. Išmatavimas tikrai negali būti naudojamas sistemose, kuriuos neegzistuoja. Imitavimas tikriausiai nenaudotinas sistemose, kuriose yra keletas tarnybinių stočių ir įėjimo signalų. Tokiu atveju labiau

tinkamas tinklų tyrimo metodas. Imitavimas ir analizė dažnai yra papildantys vienas kitą. Analitiniai modeliai puikiai tinka nedidelėms sistemoms, kurios atitinka būtinus reikalavimus, tokius kaip eksponentiškai paskirstyti lygiagretaus signalų priėmimo periodai ir apdorojimo laikai. Imitavimo modeliai labiau taikytini didelėms ir sudėtingoms (sudėtinėms) sistemoms, kurių charakteristikos padaro jas nepriimtinas analitiniams modeliams. Našumo analitikai turi būti susipažinę su įvairiomis metodikomis, modeliais, formalizavimo architektūromis ir projektavimo bei analizės įrankiais. Sukurti modelį, kuris turėtų atitinkama detalizacijos lygį, taip pat yra menas. Labai svarbu turėti pakankamai informacijos ir žinių. Tik tuomet galima sukurti tinkamą sistemos atvaizdavimą. Be to labai svarbu nuspręsti kurie elementai ar sistemos savybės yra nereikšmingos ir nereikalingos.

Pagrindinis dėmesys sutelktas imitavimu pagrįstai našumo analizei [32]. Jame aprašomas vienas iš mokslų, kuris tiria imitavimus. Tai atitinkamų statistinių metodų taikymas analizuojant imitavimo išėjimų duomenis. Kai modelis sukuriamas ir patvirtinamas dar daugybė sprendimų turi būti priimtų ir tik tuomet galima pradėti tyrimą.

Reziumuojant galima teigti, kad mokslinėje literatūroje analizuojami taikomųjų uždavinių kokybės parametrai dažniausiai išskiriami po vieną. Atliekami: patikimumo modeliavimas, lankstumo analizė, našumo didinimo operacijos ar kainos skaičiavimai. Galima pastebėti ir keletos kokybės parametrų sąveikos modeliavimą.

Norint išskirti visų kokybės parametrų sąveiką, pirmiausiai jie tiriami atskirai. Tuomet reikia įvesti integruotojo kokybės parametro sąvoką. Šis parametras turėtų padėti paskaičiuoti visus kokybės parametrus kartu.

2. TAIKOMŲJŲ UŽDAVINIŲ MODELIAVIMO TEORINIAI KLAUSIMAI

2.1. Problemos analizė

Magistro tiriamojo darbo tikslas yra surasti būdą, kaip modeliuoti kuriamą sistemą, joje nagrinėjant pagrindines taikomųjų uždavinių kokybės charakteristikas: lankstumą, patikimumą, našumą ir kainą.

Šiame darbe būtent šios savybės išskiriamos pagrindinėmis.

Jei mes kalbame apie el. paslaugų sistemą, turime žinoti kas svarbu jos vartotojams. El. Valdžios sistemoje galima išskirti platų vartotojų ratą. Tai ir vidiniai sistemos vartotojai – grupė dirbančiųjų sistemos viduje. Turima omenyje tai, kad sąveikauja įvairios valdžios institucijos, taigi jos nuolat keičiasi įvairiais duomenimis arba kitaip tariant naudoja elektronines paslaugas. Kiti vartotojai vadinami išoriniais. Juos taip pat galima suskirstyti į Verslą ir Piliečius. Verslas nuolatos turi bendrauti su Valdžia, todėl El. Valdžios sistemoje verslo vartotojai nuolat naudojasi šios sistemos el. paslaugomis. Piliečiai taip pat turi teisę naudotis sistema ir jos el. paslaugomis. Svarbiausia vartotojui, kad sistema būtų saugi. Kiekvienas vartotojas nori gauti teisingus duomenis iš sistemos, ir taip pat nori žinoti, kad jo siunčiami sistemai duomenys saugiai pasieks ją. Tai ypač aktualu naudojant nuotolinę prieigą prie sistemos, kitaip tariant naudojantis internetu.

Tik saugios ir patikimos sistemos vartotojas gali nebijodamas naudotis el. paslaugomis, ypač tada, kai sistema siunčiami asmeniniai ar įmonės privatūs duomenys. Taigi modeliuojant sistemą, būtina atkreipti dėmesį į jos patikimumą.

Kitos trys charakteristikos aktualesnės sistemos užsakovui ir sistemos kūrėjui. Užsakovui visuomet yra svarbi kaina. Bet kuri organizacija ar įmonė planuoja savo biudžetą ir visuomet stengiasi mažinti kaštus. Taigi būsimos sistemos kaina turi būti kiek galima mažesnė.

Sistemos lankstumas ir našumas yra taip pat labai svarbios charakteristikos. Sistemos kūrėjai ir projektuotojai turi įvertinti visas šias charakteristikas. Sistema turi būti lanksti, nes reikia numatyti įvairius galimus sistemos veikimo variantus. Labai paprastas sistemos pavyzdys yra kavos aparatas, kuris klientui įpila kavos į puodelį už, pavyzdžiui, 1 Lt. Klientas gali įmesti į aparatą iš karto 1 Lito vertės monetą arba dvi monetas po 50 ct., arba penkias monetas po 20 ct. ir t.t. Taigi čia atsispindi sistemos lankstumas. Projektuojant būsimą

sistemą reikia kiekviename jos žingsnyje įvertinti galimybę pereiti į vieną ar kitą sekantį žingsnį.

Našumas dažniausiai apibūdinamas sugaištu tam tikro veiksmo atlikimo laiku. Sistemos projektuotojas, analizuodamas modeliuojamą sistemą, turėtų paskaičiuoti kiekvieno sistemos žingsnio, kitaip tariant operacijos, sugaištą laiką. Bendras sistemos našumas paskaičiuojamas labai paprastai – sudedant visus operacijų laikus. Didesnis dėmesys turėtų būti skiriamas sistemos našumui didinti. Šiuo atveju reikėtų spręsti problemą, kaip naikinti ar pakeisti kitomis tas operacijas, kurioms sugaištama perdaug laiko.

Sistemos projektuotojui svarbiausias uždavinys būtų visų šių charakteristikų optimalus vertinimas. Projektuojant sistemą neužtenka, kad jos kaina būtų maža, sistema būtų tiesiog patikima arba tik labai lanksti ar naši. Svarbūs visi šie parametrai. Juos reikėtų paskaičiuoti kiekybiškai ir, analizuojant gautus duomenis, spręsti, kurias charakteristikas reikėtų tobulinti ar kurias priešingai – sumažinti kitų charakteristikų naudai.

Taigi labai svarbi problema yra optimalios sistemos radimas, kuri tenkintų pagrindines charakteristikas. Lankstumas, patikimumas, našumas ir kaina turi būti nuolat analizuojami modeliuojant būsimą el. paslaugų sistema.

2.2. Elektroninių paslaugų ypatumai

Elektroninė paslauga yra ta paslauga, kuri gaunama per tinklą ir kuri įvykdo užduotis, sprendžia problemas arba atlieka duomenų perdavimus. Elektronines paslaugas gali vartoti žmonės, verslas ir kitos elektroninės paslaugos ir jos gali būti pasiekiamos įvairiais informacijos įtaisais.

Informacinės visuomenės plėtros komitetas pateikia tokį laikiną elektroninės paslaugos apibrėžimą: „Elektroninė viešoji paslauga – paslauga, suteikianti asmeniui galimybę jo buvimo vietoje skaitmeniniu pavidalu viešaisiais kompiuterių tinklais atlikti jo poreikius tenkinančias įvairias procedūras ir gauti informaciją.”

Informacinės visuomenės paslaugų apibrėžimas aprėpia bet kokią paslaugą, paprastai teikiamą už atlygį per nuotolį, elektroninėmis priemonėmis atskiru paslaugos gavėjo prašymu duomenims apdoroti (įskaitant skaitmeninį sutankinimą) ir saugoti (vertimas neoficialus) [pagal ES direktyvą 2000/31/EB].

Elektroninių paslaugų sistemos pasižymi ir išsiskiria iš kitų tuo, kad jų vykdomoji terpė yra internetas. Taip pat čia labai svarbi duomenų apsauga ir tokių sistemų vartotojų

klaidų išvengimo galimybės. Nagrinėjant konkrečiai pasirinktą El. Valdžios sistemą galima išskirtis tokius išskirtinius jos bruožus:

- Internetas
- Platus paslaugų asortimentas
- Duomenų apsauga
- Vartotojų klaidos

Elektroninių paslaugų sistemose turi būti užtikrintas patikimumas, pasiekiamumas ir informacinis saugumas. Pagrindinėmis šių užtikrinimų problemomis yra [11,27]:

- Konfidencialumas – informacijos pasiekimas yra apribotas, ir tik specifikuoti, aiškūs vartotojai turi teise ja naudotis.
- Integralumas – informacijos tikslumo ir užbaigtumo įgyvendinimas.
- Tinkamumas – informacijos suteikimo, autorizuotiems vartotojams pareikalavus, užtikrinimas.

Kuriant bei modeliuojant elektroninių paslaugų sistemas būtina siekti maksimalios informacijos apsaugos. Siekiama užtikrinti:

- Tinkamą informacinių sistemų saugumą;
- Konfidencialumo, integralumo ir tinkamumo palaikymą;
- Sistemų personalo informavimą apie jų atsakomybę, vaidmenis ir įsipareigojimus;
- Saugumo spragų nustatymo ir išsprendimo procedūras;
- Informacijos apsaugos būdų atitikimą valdžios reikalavimams.

Elektroninių paslaugų sistemų ypatumui tirti skirtos tokios disciplinos: procesų tyrimai (PT), valdymo mokslas (VM) ir taikomosios sistemos (TS). Jos siūlo griežtus kiekybinius skaičiavimo metodus.

El. Valdžios projektai gali būti charakterizuojami hibridinėmis sistemomis. Didžioji dalis tokių projektų yra programinės sistemos, kurios dažnai sukelia nesuderinamumus tarp projektuotojų ir vartotojų. Tai dažnai lemia paprasčiausią sistemos žlugimą. Tokios sistemos turi atitikti nuolat dėl įstatymų kintančius ryšius tarp valdžios institucijų, verslo ir piliečių. Analizuojant El. Valdžios sistemą reikia atkreipti dėmesį į keletą pagrindinių charakteristikų, suteikiančių galimybę suprasti ir modeliuoti sudėtingas problemas, suvienyti skirtingus požiūrius į problemą, ir mokytis iš klaidų.

El. Valdžios informacinę sistemą turėtų sudaryti daug ir įvairių paslaugų. Keletui paslaugų realizuoti naudojami portalai. El. Valdžios portale teikiamas viešąsias paslaugas galima būtų suskirstyti į skirtas piliečiams, verslui ir valstybės valdymui. Šios paslaugos plačiau skirstomos taip [11]:

Viešosios paslaugos piliečiams:

- Mokesčiu mokėjimas/deklaravimas
- Įvairių vienkartinių mokesčių ir baudų apmokėjimas, mokesčiai už komunalinius patarnavimus.
- Pareiškimas socialinėms lengvatoms gauti ir gavimas (stipendijos, pašalpos ir kitos išmokos).
- Automobilio registracija / mokesčiai.
- Paso keitimas nustojus galioti arba pametus / gavimas.
- Vairuotojo teisių gavimas / keitimas / gavimas pametus.
- Sužinojimas apie naujas darbo vietas bei pagalba persikvalifikuojant.
- Socialinio draudimo pažymėjimo gavimas / gavimas pametus.
- Liudijimų išdavimas arba įrašų apie įvykius fiksavimas (gimimas, santuoka, mirtis).
- Pranešimas apie ligos atvejį ir išmokų iš socialinio draudimo gavimas.
- Pranešimas apie gyvenamosios vietos pakeitimą.
- Savivaldybių teikiamos paslaugos, t.y. informacija apie renginius, naujas tvarkas, informavimai apie laisvas vietas automobilių aikštelėse.

Viešosios paslaugos verslui:

- Mokesčių mokėjimas ir deklaravimas: pelno / pajamų, PVM, muitai, akcizai ir kiti mokesčiai. Socialinio draudimo įmokų deklaravimas ir mokėjimas.
- Naujos įmonės registracija.
- Duomenų pateikimas statistikos departamentui.
- Įvairių leidimų, licencijų, patentų gavimas.
- Valstybės tarnautojų duomenų bazė.

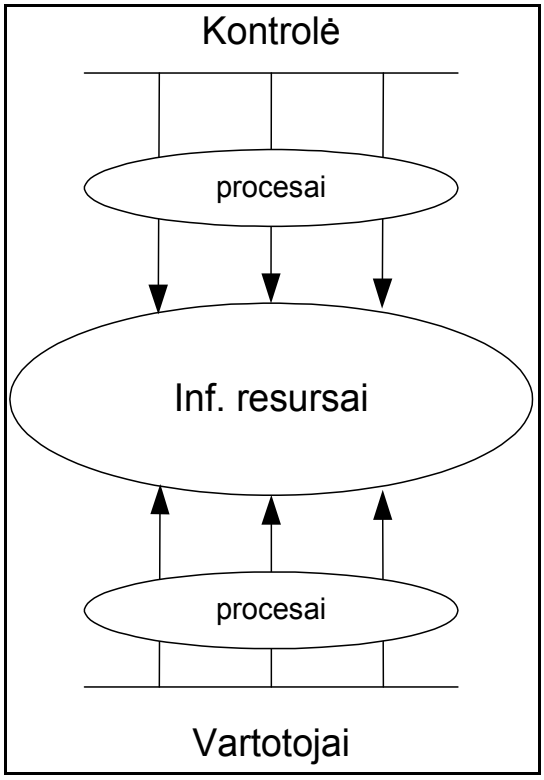
Viešosios paslaugos valstybės valdymui:

- Bendra duomenų bazė arba galimybė prieiti prie tam tikrų duomenų reikiamoms institucijoms.

- Reikiamų duomenų valstybės valdymui surinkimas per statistikos departamentą efektyviu būdu.
- Paslaugų ir atsakingų asmenų duomenų bazė.
- Elektroninių įrašų įteisinimas.
- Elektroninio pašto paplitimas.

Ši klasifikacija pateikta remiantis Lietuvos Valstybės institucijų bei įmonių ir kitų įstaigų elektroninių viešųjų paslaugų, teikiamų viešaisiais kompiuterių tinklais, svarbiausių paslaugų procedūrų tyrimu ir paslaugų teikimo galimybių analize, kurią parengė informacinės visuomenės plėtros komitetas prie LRV.

Šiame darbe nebus tiriama visa el. Valdžios sistema, kadangi ji sudaryta iš daugelio el. paslaugų. Susikoncentruota ties uždavinio modeliu, kurį atvaizduoja 5 paveikslas. Informacinės sistemos resursais gali naudotis tiek išoriniai vartotojai, tiek vidiniai kontrolieriai. Vartotojai, nuotoliniu būdu jungdamiesi prie informacinės sistemos, atlieka įvairius veiksmus, kuriuos galima apibūdinti "išoriniais vartotojų procesais". Vidinės kontrolės metu taip pat atliekami atitinkami veiksmai – „vidiniai kontrolės procesai".

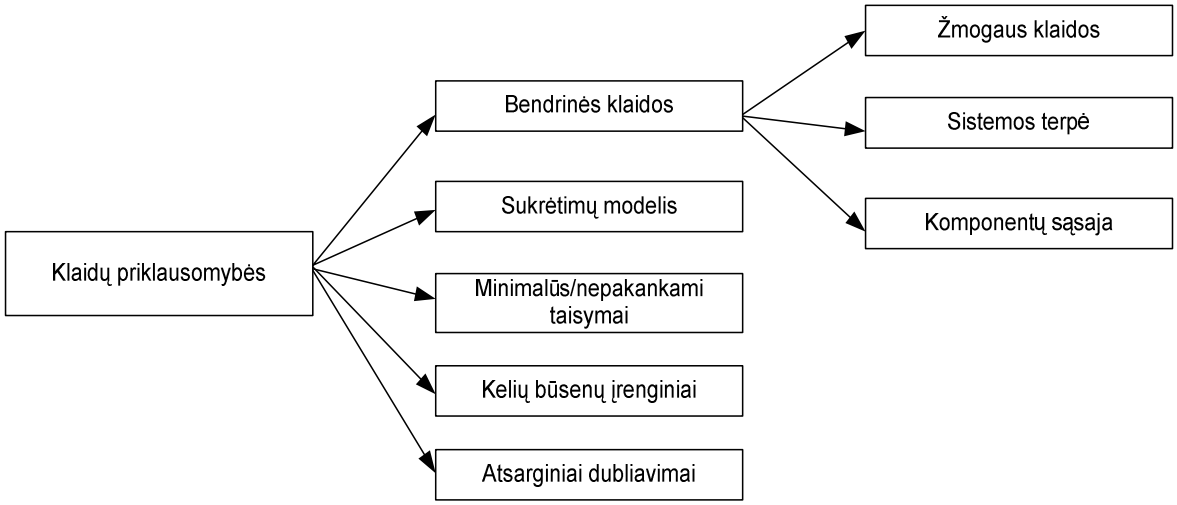


5 pav. El. paslaugų sistemos informacinių resursų panaudojimas

2.3. Sistemos patikimumo modeliavimas

Patikimumo problema el. paslaugų sistemose yra labai aktuali. Patikimumas dažniausiai siejamas su klaidų priklausomybe. Šioje dalyje kaip tik ir aprašoma klaidų priklausomybė patikimumo modeliuose. Tam naudojami stochastiniai Petri tinklai ir nuoseklios laiko atžvilgiu Markovo grandinės [12]. Taip pat yra pasiūlyta pagrindinių klaidų priklausomybių klasifikavimo struktūra. Dauguma nustatytų klasių iliustruojamos realaus laiko kompiuterinėmis sistemomis.

Klaidų priklausomybės sistematika pavaizduota 6 paveiksle.



6 pav. Klaidų priklausomybės sistematika [12]

Bendrinės klaidos – tai bet kokia būklė ar įvykis, kuris paveikia keletą komponentų įskaitant jų sinchronines klaidas arba veikimo sutrikimus. Nors ir yra paprastas, šis apibrėžimas sunkiai pritaikomas, kadangi yra problematiška nustatyti ar sudėtinės-kartotinos klaidos buvo priklausomos ar ne. Taip pat nėra aiškus ir apibrėžimas „sinchroninis". Taigi praktikoje bendrinės klaidos ir sudėtinės-kartotinos klaidos traktuojamos kaip sinonimai. Tai daroma, nes klaidų priklausomybės nežinomos arba sunkiai modeliuojamos. Bendrinės klaidos dar skirstomos į [12]:

a) Žmogaus klaidos: tai žmogaus įvykdomos specifinės užduoties klaidos (arba uždrausto veiksmo įvykdymas), kurios gali sugadinti įrangą ir sužlugdyti planines užduotis. Jos yra didžiausias bendrinių klaidų šaltinis ir gali būti įvykdomos daugelyje sistemos veikimo ciklo vietų.
b) Sistemos terpė: tai aplinkos, kurioje veikia sistema, charakteristikų įtempimai ar sukrėtimai, žmonių sukelti pavojai ir paskirstyta infrastruktūra, įskaitant ir natūraliuosius faktorius (pavyzdžiui potvynis, žaibas, žemės drebėjimas, gaisras ir t.t.).

c) Komponentų sąsaja: komponento gedimas gali neigiamai paveikti kitus komponentus grandininiu ar domino principu, kitaip vadinimu kaskadiniu gedimu. Komponentų sąsajos priklausomybės pavyzdžiais galima laikyti funkcionalius trūkumus, kuriuos sukelia netinkamai suprojektuotas apsauginis veiksmas arba programinės įrangos ir aparatūros tarpusavio priklausomybė. Programinės įrangos gedimai dažniausiai nepaveikia aparatūros iš esmės, taigi aparatūrą gali toliau naudoti kitos programos. Tačiau aparatūros gedimas automatiškai paveikia veikiančias programas. Programos numatytas aparatūros veikimas bus nepasiekiamas.

Priklausantis gedimas egzistuoja tuo pat metu keliuose sistemos komponentuose. Tokio gedimo tikėtinumas negali būti paskaičiuotas taip paprastai, kaip besąlyginis individualaus komponento gedimo tikėtinumas. Bendrinės klaidos yra tipiškiausi gedimų priklausomybės pavyzdžiai. Tačiau kartais gedimai yra statiškai priklausomi be jokio sąryšio su kitais siejamais įvykiais.

Sukrėtimų modeliai. Sistemos komponentai gali būti paveikiami išoriniais sukrėtimais. Tokie išoriniai poveikiai tarsi priskaičiuojami iki tam tikro laiko kada įvyksta gedimas. Žala kaupiasi tol, kol komponentas (ar visa sistema) pakeičiamas ar sugenda. Laiko tarpai tarp išorinių sukrėtimų ir žalos poveikio gali priklausyti nuo kaupiamos žalos apibrėžtuoju laiku *t*. Kai to paties išorinio šaltinio sukrėtimas paveikia kelis komponentus lygiagrečiai, tuomet tokie poveikiai traktuojami kaip sistemos terpę veikiančios bendrinės klaidos.

Minimalūs ar nepakankami taisymai. Vietoj to, kad pakeisti sugedusį komponentą nauju (arba atstatyti iki tokio „kaip naujas”), atliekami minimalūs komponentų, kurie nusidėvi iki tam tikro lygio, taisymai. Jei sugedusio komponento taisymas atstato visą sistemos funkcionalumą, o sistemos galimybės sugesti lygis išlieka koks buvo prieš komponentui sugendant, toks taisymas vadinamas minimaliu. Panašiai ir netobulų atitaisymų sukeliamos klaidos neatnaujina sistemos komponentų. Tokie atitaisymų būdai gali netgi didinti sistemos gedimų lygį ir, todėl laiko tarpai tarp nuoseklių gedimų nebūtinai yra nepriklausomi.

Kelių būsenų įrenginiai. Tipiniai sistemos komponentai būna dvinariai, susieti su priklausomomis charakteristikomis, t.y. bet kuris komponentas yra veikiantis arba ne. Tačiau tokie įtaisai kaip skystos srovės vožtuvas ar puslaidininkinis diodas turi du gedimų būdus, o ne vieną. Taip yra, nes jie gali sugesti būdami atvirame (atviroji grandinė) arba uždarame (trumpojo jungimo) būvyje. Kadangi trijų būvių įtaisas negali sugesti vienu metu abiejose atvirame ir uždarame būvyje, todėl gedimai yra abipusiai išskirtiniai įvykiai. Kiti komponentų tipai gali turėti netgi sudėtines išskirtines gedimų būsenas. Pavyzdžiui duomenų transliavimas

(nuoseklus perdavimas) gali sutrikti dėl: a) ryšio problemų: atviro ar uždaro ryšio blokavimas, sulėtinimas atidarant ar uždarant ryšį, trumpas jungimas įžeminant, nuo šaltinio ar tarp kontaktų, triukšmų (pertraukimų), kibirkščiavimo ar lanko įsižiebimo; b) ryšio linijos problemų: atviroji grandinė ar trumpasis jungimas, aukštos ar žemos varžos, perkaitimo; c) pernelyg didelės histerezės kilpos ar permagnetinimo.

Atsarginiai dubliavimai. Atsargų ribojimas susideda iš dinaminės sistemos komponentų rekonfigūracijos, priklausomos nuo gedimų. Aptikus ar nustačius gedimo vietą rekonfigūracijos mechanizmas pakeičia reikiamą komponentą atsarginiu. Sugedus darbiniam komponentui jis gali būti pakeistas labiau atsparesniu trikdžiams komponentu, taigi komponentų gedimai negali būti statistiškai nepriklausomi.

2.4. Stochastiniai Petri tinklai patikimumui modeliuoti

Jei atkreipsime dėmesį į pagrindinius sistemų patikimumo programinės įrangos platintojus neabejotinai pastebėsime tai, kad tik patikimumo blokinės diagramos (*Reliability Block Diagrams RBD*) ir klaidų (sutrikimų) medžių analizė (*Fault Tree Analysis FTA*) plačiai naudojamos modeliuojant patikimumą kiekybiniais matais [30]. Dabartiniai tokių standartinių įrankių išplėtimai apima vis daugiau ir daugiau dinaminių savybių tokių, kaip priklausomi įvykiai ir atsarginis modeliavimas, kuris leidžia beveik nenaudoti alternatyvių, iš esmės dinaminių, įrankių. Anksčiau buvo privaloma naudoti Markovo grandines tam, kad modeliuoti sudėtingas dinamines sąveikas tarp įvairių sutrikimų. Tačiau tiesioginis Markovo būsenų modeliavimas neįmanomas visoms, o ypač labai mažoms, gradacijos skalės atžvilgiu, problemoms, kurias patogiau nagrinėti stochastiniais Petri tinklais (TPT).

Stochastiniai Petri tinklai siūlomi, kaip potencialiai patogi alternatyva modeliuoti patikimumui. Tačiau modernios dinaminės klaidų medžių analizė (FTA) arba patobulintos patikimumo blokinės diagramos (RBD) taip pat gali būti panaudotos panašiu būdu. Tikriausiai taip galima paaiškinti faktą, kad TPT taikomieji uždaviniai, kurie naudojami sistemos patikimumui modeliuoti, yra uždrausti tyrimuose (neskaitant keletos išimčių). Šiuo metu Petri tinklai yra labai paplitę modeliavimo srityje, o tuo pačiu atsiranda ir vis daugiau įvairių TPT „praplėtimų“. Daugybė egzistuojančių Petri tinklų architektūros variacijų turi dideles modeliavimo galimybes įvairiose srityse, tačiau tuo pačiu gali turėti suvienyto standarto trukumų. Taigi tai, kas traktuojama kaip stochastiniai Petri tinklai, gali drastiškai skirtis vienuose ar kituose modeliuose, aprašymuose ar taikymuose. Nereikia nė sakyti, kad toks dviprasmiškumas gali būti ganėtinai painus patikimumo specialistams, ir kad tokie didelių galimybių TPT suvokiami kaip galingi, tačiau griozdiški ir kažkaip paslaptingi [30].

Toks TPT charakterizavimas parodo, kad juose dažnai trūksta sistemų priklausomumo (sistemos našumo, kuris apima patikimumą, pasiekiamumą ir saugumą, matas) metodų palyginimų.

Kita vertus stochastiniai Petri tinklai išsivystė į galingus ir efektyvius operatyvinių tyrimų metodus, kurie plačiai naudojami tokiose srityse kaip optiniai ar kompiuteriniai tinklai ir lanksčios gamybinės sistemos. Taigi atliktos pastangos, kurios padėjo pasiekti aiškumą priklausomybių stochastiniais Petri tinklais modeliavime išasocijuotoje terminijoje.

Galima įžvelgti dar vieną priežastį praktinio TPT taikymo trūkumuose. Aprašoma galimybė išspręsti TPT trūkumus naudojant diskrečių įvykių imitavimą. Remiantis faktu, kad kiekybiniai diferencialinių lygčių, kurios daro įtaką stochastiniams procesams, sprendimai gali būti papildyti „Monte Carlo“ metodais. „Monte Carlo“ skaičiavimų metodas gali panaikinti bet kokius modeliuojamo proceso apribojimus ir leidžia susikoncentruoti ne ties patikimumo inžinierių poreikiais, o ties modelio kompleksiniais veiksmų planais kompaktiškoje ir suprantamoje formoje [20,29]. Stengiamasi apibrėžti esamų stochastinių Petri tinklų papildymų suderinamumą su moderniais ne Markovo metodais, tame tarpe ir kitais „tiesioginių” sprendimų stochastiniams procesams metodais. Tačiau tai išlieka įdomiu klausimu tolesniems tyrimams ateityje.

Stochastinių Petri tinklų su išlaikymo leksema pagrindinė savybė yra žymės su atmintimi (arba išlaikymo leksema). Leksemos žymės gali nuosekliai kisti per laiko periodą, kada galimas perėjimas iš būsenos į būseną. Tokios žymės gali egzistuoti konjunkcijoje su paprastomis spalvotomis ar nespalvotomis leksemomis. Tokių skaitiklių duomenys gali paveikti perėjimų tarp būsenų politiką. Kaip ir spalvotuose Petri tinkluose čia viena leksema gali turėti daugiau nei vieną priklausomą skaitiklį. Tokiu pavyzdžiu gali būti realus skaičius nuo 0 iki 1, indikuojantis gyvavimo trukmės laiko dalį, ar realus laikas kada būsena pradeda perėjimą. Tokie nuosekliai besikeičiantys skaitikliai gali natūraliai palengvinti kaupiamosios žalos ar kokios kitos nuosekliai besikeičiančios savybės modeliavimą. Tokie būsenų skaitikliai gali būti papildyti egzistuojančiais spalvotuose tinkluose, pavyzdžiui konkrečios dalies atitaisymų kiekis. Būsenos išlaikymas vyksta tuomet, kai prasideda perėjimas iš būsenos. Akivaizdu, kad su bet kuria užduota žyme būsena su išlaikymu gali įvykdyti tik vieną perėjimą į kitą būseną (nėra galimybės pereiti vienu metu į kelias kitas būsenas). Pateikiama keletas būsenų su išlaikymu režimų (stochastinių ar apibrėžtinių), kurių dėka parenkami tolesni perėjimai [12]:

a) Standartinis režimas. Kai parenkamas perėjimas, užduodamas atsitiktinis pasiskirstymas ar numatomas sąlyginis vėlinimas, o taip pat paleidžiamas asocijuotas laikmatis. Kai šis užduotas laikas išsenka esamoji būsena parenka

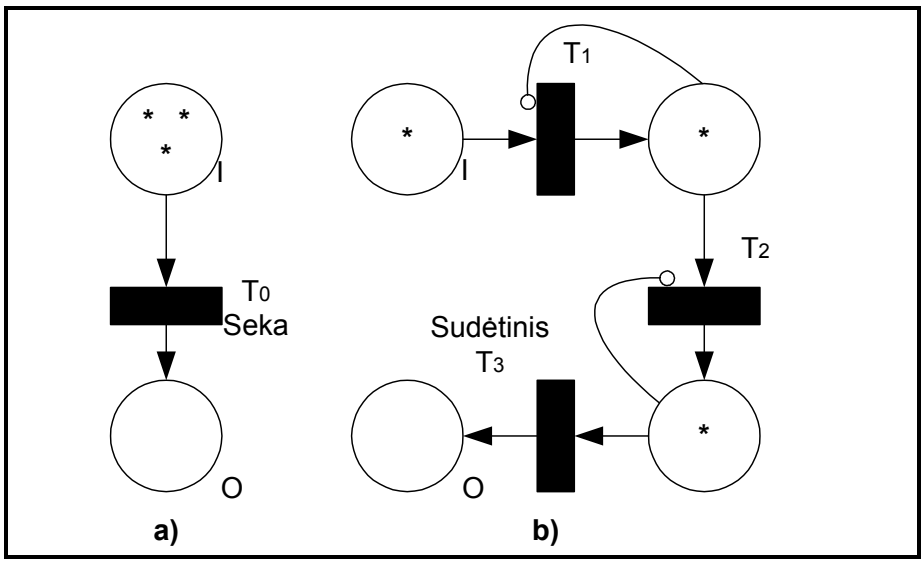
tiek perėjimų kiek yra atitinkamų išėjimų. Šie perėjimai parenkami atsitiktine tvarka priklausomai nuo įėjimo. Ši procedūra kartojama tol, kol perėjimas yra veiksnus.

b) „Seka" arba FIFO būvis (*first-in-first-out* – pirmas įėjęs išeina pirmas). Šis režimas panašus į standartinį tuo, kad tik vienas perėjimo laikmatis yra aktyvus bet kuriuo laiko momentu. Tačiau perėjimai parenkami tokia tvarka, kokia paduodami įėjimo signalai. Skirtumas tarp FIFO ir standartinio režimų aktualus tik tuomet kai nagrinėjami pažymėtosios būsenos.

c) „Sudėtinis" (arba lygiagretus) režimas. Jis naudingas labiau kompaktiškiems paprastų procesų apibūdinimams. Kiekvienam perėjimui įėjime, jo aktyvavimo laikas nustatomas nepriklausomai nuo kitų ir nustatomas atitinkamas laikmatis (skaitliukas). Esminis šio režimo skirtumas yra tas, kad įvykdymo laikų nustatymai yra artimai susiję ir su būsenomis ir su perėjimais. Taigi galima surasti panašumą su raktu ir spyna, kur raktas – būsena, o spyna – perėjimas. Ir sudėtiniai ryšiai standartiniuose perėjimuose ir sudėtiniai perėjimai projektuojami tam, kad sujungti keletą būsenų tuo pat metu.

Sudėtinis režimas yra dažniausiai naudojamas stochastiniuose Petri tinkluose su išlaikymo būsenomis. Iš tiesų jis gali būti naudojamas imituoti kitų dviejų režimų elgseną. Tiesa sakant nuosekliems perėjimams šis modeliavimo režimas yra gana tiesmukiškas (žiūrėti 7 paveikslą). Sekų režimas pateikia kompaktiškesnį atvaizdavimą (7 pav. a)), ypač jei įėjimo būsena, aprašyta kaip *I*, taip pat naudojama ir kitiems perėjimams.

Būsenų su išlaikymų panaudojimas Petri tinkluose turi didelę reikšmę sistemos patikimumo modeliavime [30]. Daug aiškiau gali būti modeliuojamos keletas pagrindinių realiai naudojamų sistemų savybių tokių kaip: išlaikančios sistemos su krūvio paskirstymu, daugiafaziai paskirstymai, kaupiamųjų dalių netobuli pataisymai ir pan. Sąsajoje su jau egzistuojančiomis Petri tinklų savybėmis gaunamas labai galingas sistemų patikimumo modeliavimo įrankis.



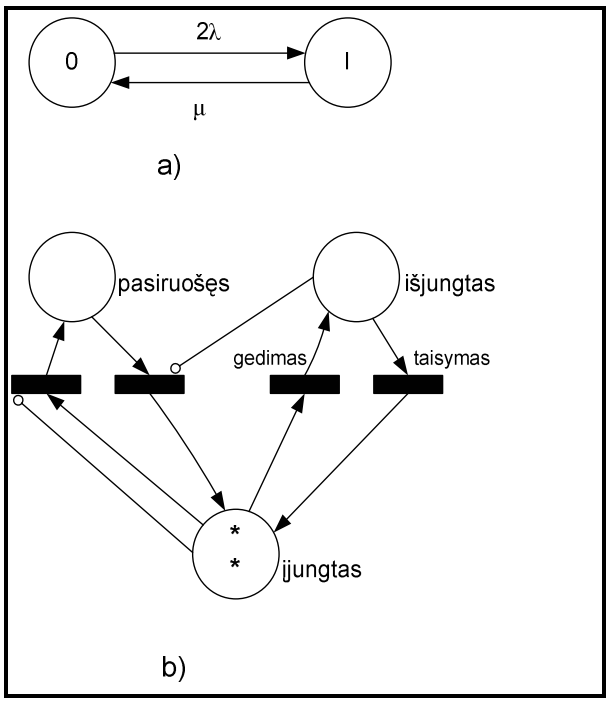
7 pav. Nuoseklus perėjimas į tris būsenas: a) modeliavimas naudojant Sekos režimą b) atitinkamas modeliavimas naudojant sudėtinį režimą [30]

7 paveiksle pavaizduoti perėjimai iš būsenos *I* į būseną *0* atitinkamai „Sekos" ir „Sudėtiniu" režimais. Čia T_i – perėjimai iš būsenų. Būsenoje * reiškia išėjimų iš jos skaičių.

2.5. Būsenų su išlaikymu taikymas

Norėdami paaiškinti šį taikymą pasirinkime du taisomus komponentus, kurie sujungti į seką. Kiekvieno komponento gedimas turi įtaką visos sistemos gedimui. Tai yra dažnai naudojamas būdas modeliuojant tokias sistemas kaip RBD blokų sąjungos ar klaidų medis su dviem pagrindiniais įvykiais susietais loginiu „ARBA" ryšiu [30]. Mažiau pastebima tai, kad prielaida, jog šių dviejų komponentų gedimas nesusijęs. Tikriausiai suprantama tai, kad įvykus vieno komponento klaidai ir dėl to išėjus iš rikiuotės sistemai, kito komponento klaidos galimybė turėtų pasikeisti (pavyzdžiui nustatoma lygi 0).

Pirmiausiai tarkime, kad klaidos ir taisymo galimybės yra konstantos abiems komponentams. Ir mes galime modeliuoti tokią sistemą Markovo grandinių metodu (kur atitinkamai klaida ir taisymas yra λ ir μ). 8 paveikslo a) dalyje pavaizduotos dvi galimos būsenos: *0* – kai abu komponentai yra veikiantys, ir *I* – kai viename iš komponentų įvyko klaida, o kitas tuo metu dirba tuščia eiga. Akivaizdu, kad perėjimas iš *0* į *I* yra lygus 2λ (atsižvelgiant į vieno iš komponentų gedimą), tuo tarpo perėjimas iš *I* į *0* yra lygus μ.



8pav. Du nuosekliai sujungti komponentai: a) modeliavimas naudojant Markovo grandines b) modeliavimas naudojant stochastinius Petri tinklus [30]

Stochastinių Petri tinklų modeliavimas atvaizduotas 8 paveikslo b) dalyje. Kiekvienas iš dviejų komponentų gali būti trijose pozicijose: įjungtas, pasiruošęs ir išjungtas. Tuo pačiu yra trys būsenos atitinkančios šias pozicijas, ir du „perėjimai" pažymintis kiekvieną iš komponentų. „Perėjimo" buvimas duotoje pozicijoje reiškia komponento buvimą atitinkamoje būsenoje. Duotame paveiksle abu „perėjimai" yra pozicijoje „įjungtas". Tai reiškia kad abu komponentai yra veikiantys, taigi „gedimo" procesas gali būti aktyvuotas. Šis procesas yra daugialypis. Čia negalima įžvelgti panašumo su Markovo grandine. Kuomet komponentas sugenda, kas lemia vieno iš dviejų laikmačių išsijungimą, tuomet įvykdomas atitinkamas „perėjimas" ir komponentas pereina į būsena „išjungtas". Šis įvykis turi dvi pasekmes: „taisymo" procesas aktyvuojamas ir gali būti panaudotas, o taip pat nustatomas atitinkamas laikmatis (skaitliukas iki taisymo veiksmo). Antrasis komponentas iškart nustatomas į „pasiruošusio" būseną. Jis išlieka šioje būsenoje tol, kol sugedęs komponentas nepataisomas. Tuomet atitinkamai pereina į „įjungto" būseną.

Šis pavyzdys parodo, kad Markovo grandinių modeliavimo metodas yra kompaktiškesnis, tačiau stochastinių Petri tinklų modelis yra pritaikomas ne tik dviems bet ir pasirenkamam komponentų skaičiui. Taigi komponentų kiekiui padidėjus modelis išliks nepakitęs. O atitinkamai Markovo grandinių modelis išsiplės.

2.5.1. Patikimumo, našumo skaičiavimas

Modeliuojant sistemos elgseną stochastiniai Petri tinklai leidžia aprašyti daug skirtingų matavimo vienetų, kuriais galima matuoti sistemos patikimumo ir našumo savybes.

Petri tinklo būsenų „perėjimų" loginės ar algebrinės funkcijos leidžia specifikuoti išėjimo rezultatus (pavyzdžiui, sugedusioje būsenoje nėra nei vieno „perėjimo"). Aibėje apibrėžiamas būsenų, kurių išėjimo rezultatai teigiami, poaibis S. Išėjimas matuojamas taip:

$Q_S(t)$ = Tikėtinumas {išėjimo rezultatas teigiamas atitinkamu laiku t} [30]

$$Q_S(t) = \Sigma q_S(t) \quad (1)\ [30]$$

čia $q_S(t)$ – tikėtinumas būti *s* būsenoje atitinkamu laiku *t*. Jeigu S yra operaciniu būsenų rinkinys, $Q_S(t)$ pagal 1 formule yra paprastas patikimumo (ar pasiekiamumo) apibrežimas.

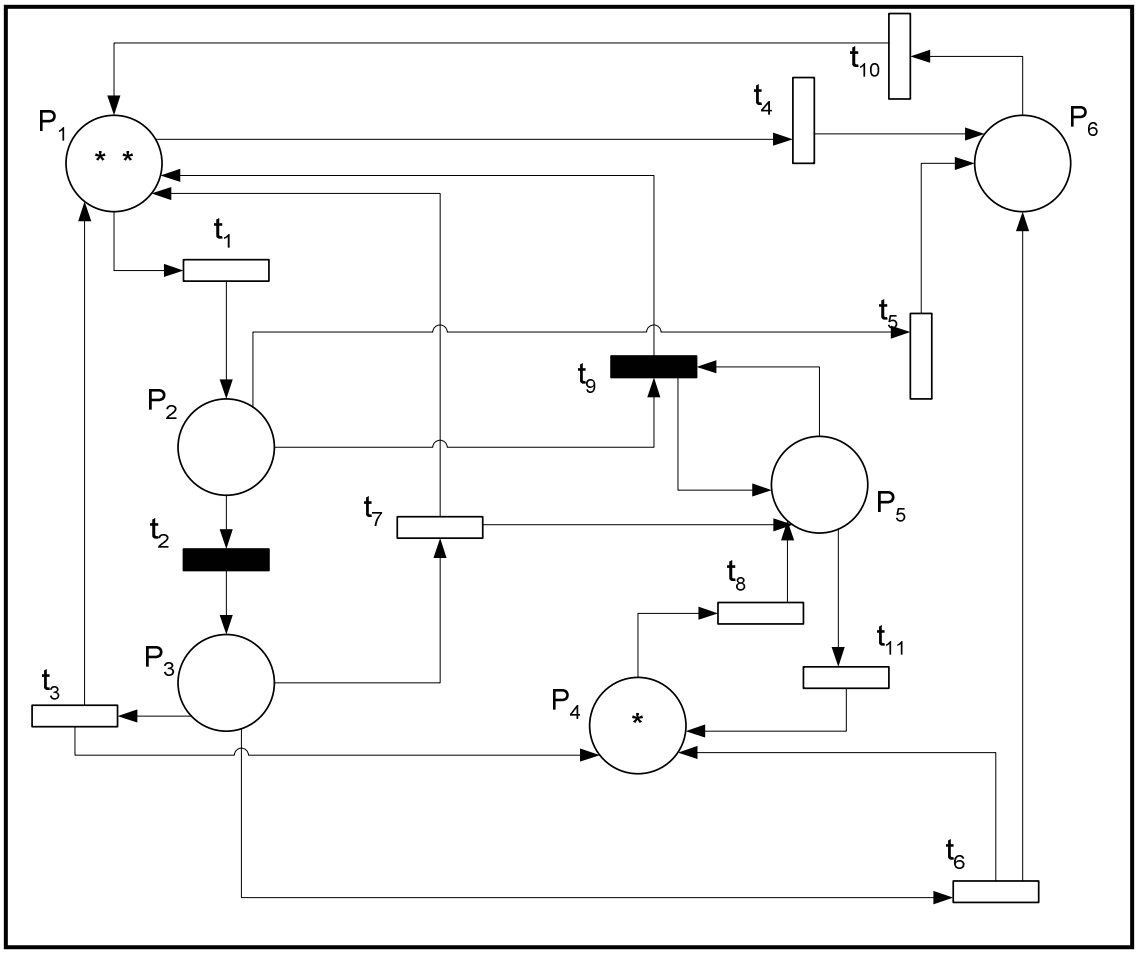
Labai naudingas pavyzdys iškeliamas tada, kai norima skaičiuoti trumpalaikius tikėtinumus, kuomet sąlyga yra tenkinanti pradžioje. Naudojant standartinius tikimybinių procesų analizės mechanizmus, būsenos $s \in S$ absorbuojamos, ir šis dydis įvertinamas sustabdant procesą būsenoje S.

Būsenos perėjimų paskirstymas

Tarkime, kad p_i yra bendrinė Petri tinklo būsena. Kumuliacinė p_i būsenos „perėjimų" skaičiaus atitinkamame laike *t* pasiskirstymo funkcija (Kdf) yra laiptinė funkcija, kurios *k*-tojo žingsnio amplitudė gaunama sumuojant visus aibės, atitinkamu laiku *t* turinčios perėjimų skaičių *k* būsenoje p_i, tikėtinumus. Tankis $f_i(k,t)$ yra lygus *k*-tojo žingsnio amplitudei. Tikėtinas p_i būsenos „perėjimų" skaičius atitinkamu laiku *t* yra lygus:

$$E[m_i(t)] = \sum_{k=0}^{\infty} k f_i(k,t) \quad (2)\ [30]$$

Pavyzdžiui, jei būsenoje p_i atvaizduoti identiški komponentai, laukiantys to paties resurso, tuomet tikėtinas „perėjimų" skaičius yra lygus Kdf ir tikėtinam komponentų skaičiui eilėje atitinkamu laiku. Kuomet būsena p_i reiškia sugedusį komponentą, tuomet šis dydis parodo Kdf ir tikėtiną sugedusių komponentų skaičių atitinkamu laiku.



9 pav. Sistema su gedimais ir atitaisymais [30]

Sistemos su gedimais ir atitaisymais būsenos ir procesai aprašomi sekančiose lentelėse.

1 lentelė 9 paveikslo būsenų reikšmės

Būsena	Aprašymas
P_1	Komponentas veikia nepriklausomai
P_2	Laukiama resurso
P_3	Resursas vykdomas
P_4	Resursas paleidžiamas
P_5	Resurso klaida
P_6	Komponentas sugedęs

2 lentelė 9 paveikslo procesų reikšmės

Procesas	Aprašymas
t_1	Resurso prašymas
t_2	Resurso priėmimas
t_3	Resurso paleidimas
t_4	Komponento gedimas pradinėje būsenoje
t_5	Komponento gedimas belaukiant
t_6	Komponento gedimas naudojant resursą
t_7	Resurso klaida vykdant
t_8	Resurso klaida paleidžiant
t_9	Grįžimas į pradinę būseną įvykus resurso klaidai
t_{10}	Komponento taisymas
t_{11}	Resurso taisymas

9 paveiksle pavaizduoti lygiagretūs komponentai naudojantys paskirstytus resursus. Daroma prielaida, kad šie komponentai yra identiški. Stochastiniais Petri tinklais sumodeliuota klaidų ištaisymo operacija sistemoje. Čia nagrinėjami resursų klaidos ir komponentų gedimai bei jų ištaisymai.

Sistemos našumo/patikimumo skaičiavimas atliekamas matuojant komponentų atliekamą naudingą darbą laike *t*. Sistemos patikimumas (tuo pačiu ir našumas) mažėja dėl įvairių priežasčių: perpildymo vėlinimo dėl paskirstytų resursų naudojimo, duomenų persiuntimo iš kiekvieno komponento naudojant konkretų resursą, gedimų ir taisymų ciklų.

Šis patikimumo matas sutampa su tikėtinu perėjimu skaičiumi P_1 būsenoje, ir patikimumas gali būti aprašytas Petri tinklais ir paskaičiuotas naudojantis 2 formule.

3. ELEKTRONINIŲ PASLAUGŲ TAIKOMŲJŲ UŽDAVINIŲ KOKYBĖS ANALIZĖ IR MODELIAVIMAS

3.1. Kokybės parametrų formalizavimas

Lankstumo, patikimumo, našumo ir kainos vertinimo kriterijai ir optimalaus varianto radimo būdai.

3.1.1. Patikimumo formalizavimas

Naudojant Petri tinklų architektūrą, šio parametro įvertinimui taip pat naudojamos būsenos ir jų savybės. Dažniausiai patikimumą apskaičiuoti tiesiogiai yra labai sunku, todėl patikimumo skaičiavimams naudojamos klaidų įverčiai. Patikimumas yra atvirkščiai proporcingas būsenos klaidoms. Darbe įvestas apibrėžimas klaidos tikimybė. Ji reiškia, kad būsenoje įvyks arba neįvyks klaida sistemos darbo režime. Reikia nustatyti kiekvienos sistemos būsenos perėjimų klaidų tikimybes. Klaidos tikimybės įvertinimas taipogi yra labai problematiškas. Tik patyręs analitikas (ekspertas) gali nustatyti būsenos klaidos tikimybę, ją įvertinti, o tuo pačiu ir paskaičiuoti visos sistemos ar atskiros tiriamos procedūros patikimumą.

Žinant būsenos klaidos tikimybę *kl*, būsenos patikimumas P gali būti paskaičiuotas naudojant tokią formulę:

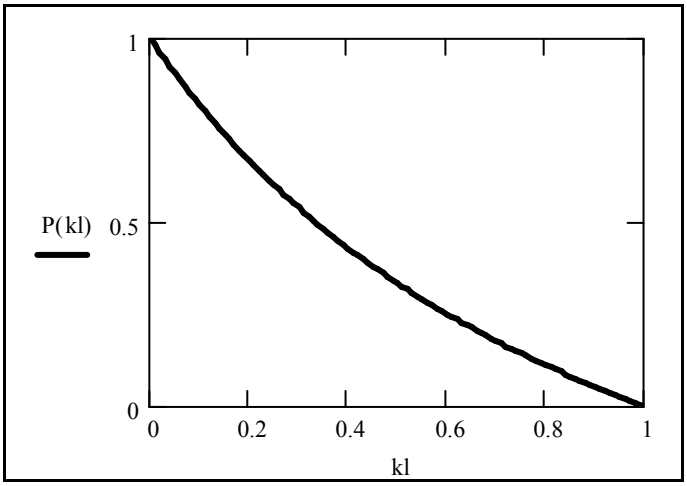
$$P = \frac{1 - kl}{1 + kl}; \tag{3}$$

čia klaidos tikimybė yra $0 \le kl \le 1$.

Klaidos tikimybė gali svyruoti nuo 0, jei būsenoje klaidų būti negali, iki 1, jei būsenoje tikrai įvyks klaida. Žinoma dažniausiai būsenos klaidos tikimybės įvertis bus tarp 0 ir 1, nes garantuoti 100 procentų, kad klaida neįvyks, yra labai sunku, o nustačius, kad būsenoje klaida įvyks tikrai, būtina koreguoti sistemos architektūrą ir atsisakyti tokių sistemos būsenų. Taigi, remiantis patyrusio analitiko pateiktais duomenimis apie būsenų klaidų tikimybes, mes žinome – $0 \le kl \le 1$.

Jeigu klaidos tikimybė atitinkamoje būsenoje būtų lygi 0, tuomet jos patikimumas būtų lygus 1, o tai reiškią absoliutų būsenos patikimumą. Jeigu klaidos tikimybė atitinkamoje būsenoje būtų lygi 1, tuomet jos patikimumas būtų lygus 0, o tai reiškia, kad būsena yra

visiškai nepatikima. Tačiau, jei sistemos analitikas nustatė būsenos klaidos tikimybę lygią 0,5, tuomet sistemos patikimumas nėra lygus 0,5, o atitinkamai 0,33. Taigi galima sakyti, kad esant didesnei klaidos galimybei būsenoje proporcingai mažėja tos būsenos patikimumas. Patikimumo priklausomybės nuo klaidos galimybės grafikas patektas 10 paveiksle.



10 pav. Patikimumo priklausomybė nuo klaidos galimybės

Didėjant sistemai, problemų daugėja; kai kurie dalykai, nesvarbūs mažoje sistemoje, staiga tampa aktualūs. Analizuojant visą sumodeliuotą elektroninę sistemą (arba didesnę jos dalį) skaičiuojama užduoties įvykdymo tikimybė:

$$P_U(t) = \sum_{i=1}^{B} P_i(t) P_{Ui}(t); \qquad (4)\ [10]$$

čia P_{Ui} – užduoties įvykdymo tikimybė esant *i*-tajai būsenai; P_i – *i*-tosios elektroninės sistemos būsenos tikimybė; B – būsenų skaičius.

Jei sistemos būsenos sujungtos nuosekliai, tuomet ryšys tarp galinių būsenų bus užtikrintas tuomet, jei veiks būsenos bei jas jungiantys komponentai.

Ryšio tarp galinių būsenų tikimybė:

$$P_{1\text{-}n} = P_1 * P_2 * \ldots * P_{n;}; \qquad (5)\ [10]$$

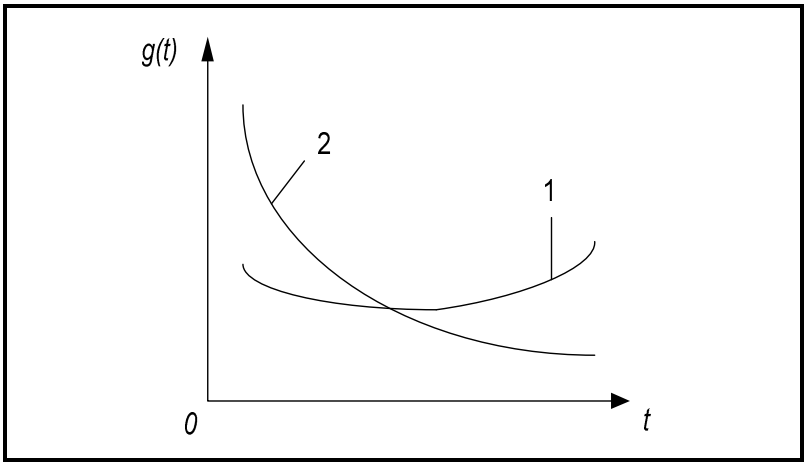
čia P1, P2,…Pn – atitinkamų sistemos būsenų negendamumo tikimybės, n – būsenų skaičius.

Jei būsenos jungiamos lygiagrečiai, tuomet skaičiuojant patikimumą pirmiausiai reikia paskaičiuoti klaidų galimybes lygiagretaus jungimo metodu. Šis metodas nusakomas taip:

Jei dvi būsenos sujungtos lygiagrečiai, tuomet bendroji dviejų būsenų klaidos galimybė paskaičiuojama pagal šią formulę:

$$k = \frac{k1 * k2}{k1 + k2}; \qquad (6)$$

Analizuojant patikimumą, kai sistemose naudojama kompiuterinė įranga, reikia įvertinti ne tik aparatūros, bet ir programinės įrangos patikimumą. Programinės įrangos patikimumą taip pat galima apibrėžti kaip gebėjimą tam tikromis eksploatacijos sąlygomis atlikti numatytas funkcijas. Esminis programinės įrangos patikimumo skirtumas tas, kad programos nesidėvi, nelūžta, todėl jų veikimas priklauso tik nuo kokybės, kurią lemia kūrimo procesas. 11 paveiksle pavaizduoti gedimų intensyvumo grafikai eksploatacijos metu:



11 pav. Gedimų intensyvumo grafikas: 1 – aparatūros eksploatacijos metu; 2 – programų eksploatacijos metu [10]

3.1.2. Lankstumo formalizavimas

Naudojant Petri tinklų architektūrą, šio parametro įvertinimui naudojamos būsenos ir jų savybės. Pirmiausiai reikia įvertinti kiek „išėjimų" į kitas sistemos būsenas turi tiriamoji būsena. Tam tiesiog reikia suskaičiuoti ryšius, vedančius į sekančias būsenas (kitaip tariant procesų skaičius). Turint omenyje tai, kad mes projektuojame informacinę sistema ir siekiama optimalaus sistemos varianto, vertinant pagrindinius kriterijus, mes galime numatyti keletą sistemos architektūros variantų, o tuo pačiu ir kiekvienos sistemos būsenos, bei jos įėjimų ir išėjimų skaičius. Taigi mes galime numatyti kiek "išėjimų" gali turėti tiriamoji būsena. Reikia atkreipti dėmesį, kad bus vertinami visi pagrindiniai sistemos kriterijai, todėl mums nėra būtina siekti kuo didesnio sistemos lankstumo, t.y. suprojektuoti kuo daugiau išėjimų.

Pereikime prie konkrečių vertinimų ir kiekybinių skaičiavimų.

a. Pirmasis vertinimas. Tarkime, kad tiriamoji būsena *i* turi maksimalų skaičių „išėjimų" (analizuojant visas suprojektuotas sistemos architektūras). Tuomet šiai būsenai rašome įvertį atitinkanti „išėjimų" skaičių:

n_i = iš.sk.; (7)

Jei būsena gali turėti daugiau išėjimų, nei turi šioje architektūroje, jai rašome įvertį „išėjimų" skaičius minus papildomai galimų „išėjimų" skaičius:

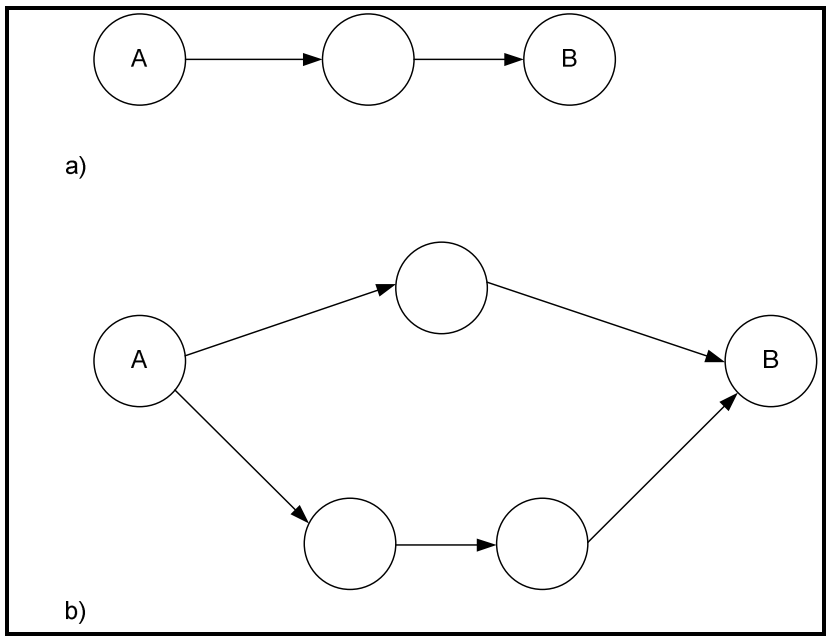
n_i = iš.sk. – pap.iš.sk.; (8)

Papildomai galimi išėjimai gaunami tuomet, kai projektuojant sistemos architektūrą galima modeliuoti kelis sistemos variantus. Toks pavyzdys pateiktas 12 paveiksle. Čia pavaizduotas perėjimas iš būsenos A į būseną B. Pirmuoju atveju a) iš būsenos A seka tik vienas „išėjimas". Tuo tarpu b) atveju iš būsenos A seka du „išėjimai". Taigi yra galimybė pereiti iš vienos būsenos į kitą keliais būdais (tuos būdus nustato sistemų projektuotojai). Jeigu pasirinkta modeliuojama sistema, kurioje iš būsenos A pereinama į būseną B taip kaip pavaizduota a) atveju, tuomet A būsenos lankstumas paskaičiuojamas taip:

$n_A = 1 - 1 = 0$.

Jeigu pasirinkta modeliuojama sistema, kurioje iš būsenos A pereinama į būseną B taip kaip pavaizduota a) atveju, tuomet A būsenos lankstumas paskaičiuojamas taip:

$n_A = 2$.



12 pav. Lankstumas. a) Perėjimas iš A būsenos į B vienu „išėjimu", b) Perėjimas iš A būsenos į B dviem „išėjimais".

Taip turime įvertinti kiekvieną sistemos būseną. Visos sistemos lankstumas gaunamas susumavus visus būsenų lankstumo įverčius (arba paskaičiavus visų įverčių vidurkį, kai visų būsenų lankstumo įverčių suma padalinama iš būsenų kiekio).

$$N = \frac{\sum_{i=1}^{B} n_i}{B}; \quad (9)$$

Čia N – bendras sistemos lankstumas, n_i – i-tosios būsenos lankstumas, B – būsenų skaičius.

b. Antrasis vertinimas. Naudojamas procentinis skaičiavimas. Tiriamosios būsenos lankstumas lygus n=100%, jei būsena negali turėti daugiau „išėjimų", arba esamų „išėjimų" skaičius padalintas iš galimų „išėjimų" skaičiaus išreikštas procentais, jei sistema gali turėti daugiau „išėjimų" kitose projektuojamose architektūrose (n= iš.sk/g.iš.sk * 100%).

3.1.3. Našumo formalizavimas

Skaičiavimai atliekami matuojant kiekvieno proceso ar procesų grupės atlikimo laikus *t*. Našumas yra atvirkščiai proporcingas atlikimo laikams. Jis matuojamas atvirkščiu proceso atlikimo laiku ir paskaičiuojamas 1/t. Šiuos laikus gali išmatuoti ar nustatyti tik patyręs sistemų analitikas. Kiekvieno proceso atlikimo laikas turi būti paskaičiuotas praktiškai. Tam gali būti naudojamos sistemų imitacijos arba realiai veikiančios sistemos. Elementarūs procesai gali būti naudojami įvairiose sistemos, todėl jų našumo įverčiai gali būti žinomi iš anksčiau atliktų modeliavimų bei analizės.

Visos sistemos (ar analizuojamos procedūros) atlikimo laikas paskaičiuojamas sudedant elementariųjų procesų atlikimo laikus.

$$T = \sum_{i=1}^{R} t_i; \quad (10)$$

Čia T – bendras sistemos atlikimo laikas, t_i – i-tojo proceso atlikimo laikas, R – procesų skaičius.

Bendras sistemos našumas yra lygus $\frac{1}{T}$.

3.1.4. Kainos formalizavimas

Kainos įvertinimui turime atsižvelgti į suprojektuotus sistemos procesus. Konkretus procesai gali turėti savo kainą, kaip tarkim vartotojo autentifikavimo procesas, kai žinoma jog jis išmatuojamos konkrečiu kainos vienetu. Projektuojant informacinę sistemą privaloma paskaičiuoti kiekvieno proceso kainą. Jei procesai yra sudėtiniai ir konkretaus proceso kainos

neįmanoma atskirai paskaičiuoti, galima nustatyti šios procesų grupės kainą, o ne kiekvieną procesą atskirai. Tuo pačių turi būti paskaičiuota visos projektuojamos sistemos kaina. Pereikime prie konkrečių kainos vertinimų.

c. Pirmas vertinimas. Kaina gali būti išreikšta sąlyginiais kainos vienetais s. Kadangi turi būti įvertinti visi sistemos procesai atskirai (arba atskiros procesų grupės), bendra projektuojamos sistemos kaina gaunama sudėjus visų procesų kainas.

$$S = \sum_{i=1}^{R} s_i ; \qquad (11)$$

Čia S – sistemos kaina, s_i – i-tojo proceso kaina, R – procesų skaičius.

Šiuo atveju paskaičiavus vieno modeliuojamo sistemos varianto kainą ją reikėtų lyginti su kitų sistemų variantų kainomis. Taip atrenkamas geriausias kainos variantas.

d. Antrasis vertinimas. Kaina gali būti išreikšta konkrečia valiuta, tačiau vertinimo principas išlieka kaip ir pirmuoju atveju, t.y. turi būti skaičiuojamos atskirų procesų kainos.

Įveskime naują sistemos analizės matavimą – integruotąjį kokybės parametrą IKP. Šiame parametre apjungiami visi aukščiau aprašyti kokybės parametrai. Tai tarsi bendras sistemos kokybės parametras.

Jis gali būti skaičiuojamas pagal sekančią formule:

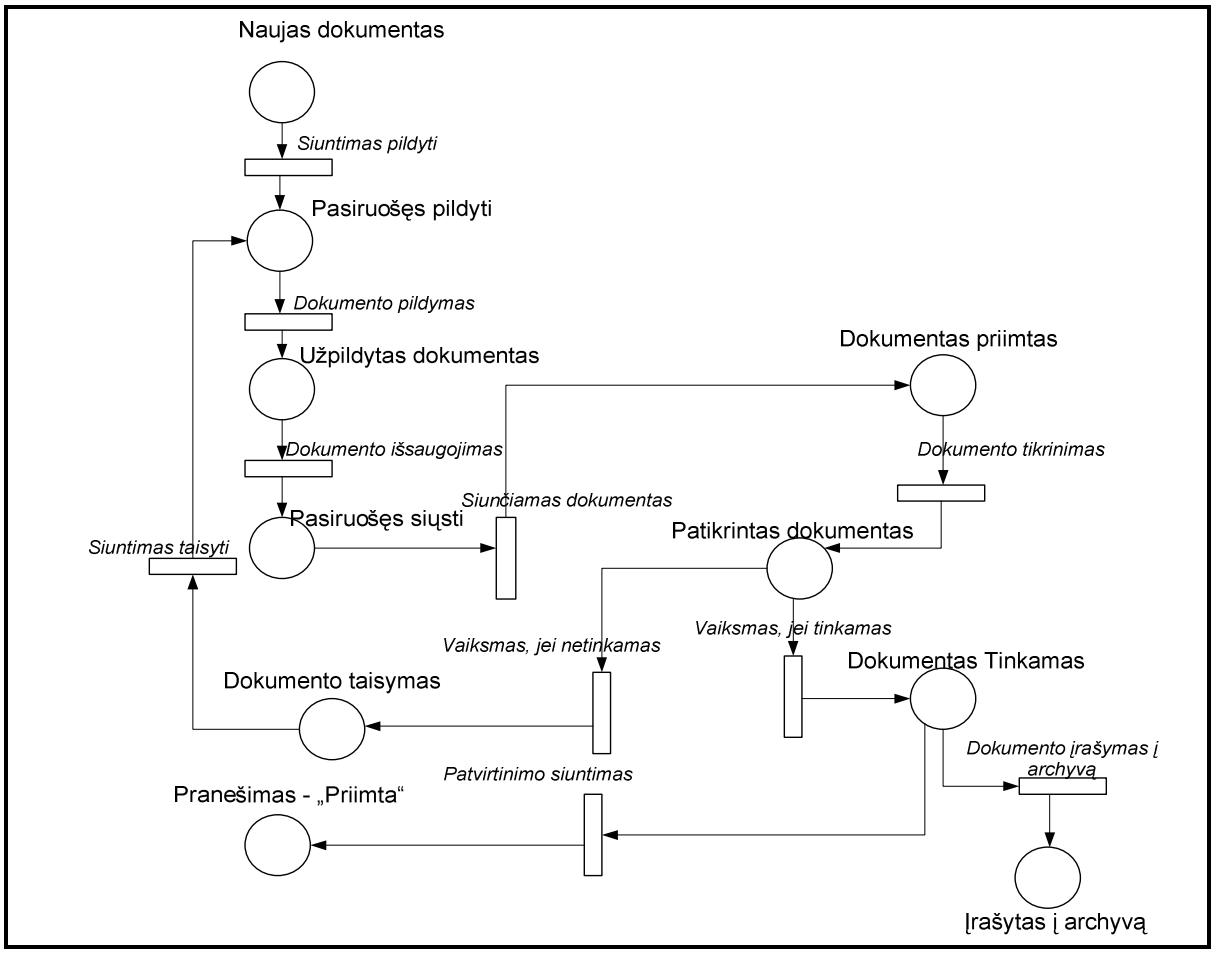
$$IKP = \frac{P * N * \frac{1}{T}}{S} \qquad (12)$$

Analizuodami kuriamą sistemą šis IKP turi būti paskaičiuotas visiems galimiems sistemoms modeliams. IKP naudojami patikimumas, lankstumas, našumas ir kaina į formulę įtraukiami skirtingais svoriais: patikimumo reikšmė yra tarp 0 ir1, lankstumas matuojamais sveikaisiais skaičiais, našumas arba atlikimo laikai tiesiogiai priklauso nuo sistemos dydžio ir joje esančių procesų atlikimo laikų, kaina taip pat priklauso nuo sistemoje realizuotų procesų kainos. Toliau IKP naudojamas tik modelių palyginimui, kadangi tiesioginė jo reikšmė praktinės naudos neduoda. Tik palyginę atskirų modelių IKP galime daryti išvadas, kurie modeliai yra tinkamesni.

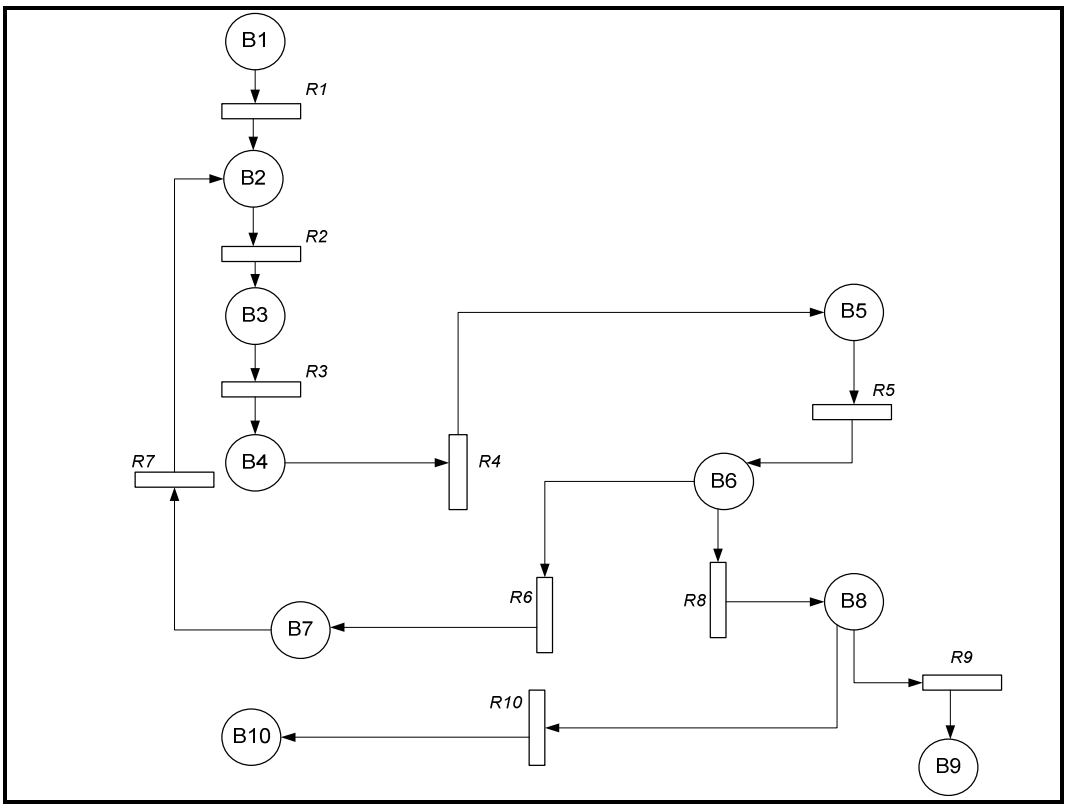
3.2. Elektroninės paslaugos modeliavimas Petri tinklu. Modelis Nr.1

Pateikiami du atskiros elektroninių paslaugų sistemos procedūros modeliai. Abiejuose modeliuose nagrinėjamas elektroninio dokumento, kurį turi nutolęs sistemos vartotojas,

siuntimas sistemai ir jo patikrinimas. 13 paveiksle pavaizduotas paprasčiausiais paslaugos modelis – pavadintas Nr.1, kuriame atliekami elementarūs dokumento pildymo, siuntimo ir tikrinimo veiksmai. Vartotojas pirmiausiai turi užpildyti siunčiamą dokumentą, išsaugoti jį ir tik tuomet siųsti nutolusiai sistemai. Sistemoje atliekama patikrinimo procedūra. Jei dokumentas netinkamas, jis siunčiamas atgal vartotojui ir prašoma jį pakoreguoti. Jei dokumentas tinkamas, jis įrašomas į dokumentų archyvą, o vartotojui siunčiamas pranešimas, jog dokumentas priimtas. 14 paveiksle pavaizduotas tas pats sistemos paslaugos modelis, tačiau būsenos ir procesai pavadinti nuosekliais trumpinimais, kurie bus naudojami tolesniuose skaičiavimuose.



13 pav. Dokumento siuntimas elektroninių paslaugų sistemai Nr.1



14 pav. Dokumento siuntimas elektroninių paslaugų sistemai Nr.1. Atvaizdavimas būsenomis ir procesais

Išanalizavus 14 paveikslą pateikiamos jame pavaizduotos paslaugos būsenų ir procesų patikimumo, lankstumo, našumo ir kainos įverčių lentelės.

3 lentelė Modelio Nr.1 Būsenų patikimumas ir lankstumas

Būsena	Klaidos galimybė *kl*	Patikimumas pagal 3 formulę	Lankstumas *n*
B1	kl1	P1	n1
B2	kl2	P2	n2
B3	kl3	P3	n3
B4	kl4	P4	n4
B5	kl5	P5	n5
B6	kl6	P6	n6
B7	kl7	P7	n7
B8	kl8	P8	n8
B9	kl9	P9	n9
B10	kl10	P10	n10

3.2.1. Modelio Nr.1 kokybės parametrų skaičiavimai

Akivaizdu tai, kad bendras sistemos patikimumas bus ne didesnis už bet kurios iš būsenų patikimumą. Tai yra todėl, kad esant nuosekliam ryšiui tarp dviejų būsenų, jų bendras patikimumas gaunamas sudauginant atskirus tų būsenų patikimumo įverčius. O konkrečios būsenos patikimumas negali būti didesnis už vienetą.

Pirmojo modelio bendras patikimumas būtų skaičiuojamas naudojant 5 formulę taip:

$$P_{Nr.1} = P1*P2*...*Pn = P1*P2*P3*P4*P5*P6*P7*P8*P9*P10; \quad (13)$$

Tačiau šiuo atveju mes negalime visiškai pasikliauti šiuo skaičiavimu, kadangi pastebimas lygiagretaus būsenų jungimo būdas. Taigi čia reikėtų pirmiausiai paskaičiuoti bendrą lygiagrečiai sujungtų būsenų klaidos galimybę ir tik tuomet paskaičiuoti bendrą patikimumą tose būsenose.

Taigi pirmiausiai paskaičiuojama bendroji lygiagrečių B9 ir B10 būsenų klaidos galimybė (naudojama 6 formulė):

$$kl_{9,10} = \frac{kl_9 * kl_{10}}{kl_9 + kl_{10}}; \quad (14)$$

Tuomet turi būti paskaičiuota bendroji lygiagrečių B7 ir B8 būsenų klaidos galimybė (6):

$$kl_{7,8} = \frac{kl_7 * (kl_8 + kl_{9,10})}{kl_7 + kl_8 + kl_{9,10}}; \quad (15)$$

Taigi būsenų B7, B8, B9 ir B10, kurios sujungtos lygiagrečiai, patikimumas paskaičiuojamas pagal 3 formulę taip:

$$P_{7,8,9,10} = \frac{1 - kl_{7,8}}{1 + kl_{7,8}}; \quad (16)$$

Tuomet pirmojo modelio bendras patikimumas, remiantis 5 formule, paskaičiuojamas taip:

$$P_{Nr.1} = P1*P2*...*Pn = P1*P2*P3*P4*P5*P6*P_{7,8,9,10}; \quad (17)$$

Pirmojo modelio bendras lankstumas skaičiuojamas remiantis vidutiniu lankstumu (9):

$$N_{Nr.1} = \frac{\sum_{i=1}^{B} n_i}{B} = \frac{n1 + n2 + n3 + n4 + n5 + n6 + n7 + n8 + n9 + n10}{10}; \quad (18)$$

4 lentelė Modelio Nr.1 Procesų našumas ir kaina

Procesas	Našumas *t*	Kaina s
R1	t1	s1
R2	t2	s2
R3	t3	s3
R4	t4	s4
R5	t5	s5
R6	t6	s6
R7	t7	s7
R8	t8	s8
R9	t9	s9
R10	t10	s10

Pirmojo modelio bendras našumas skaičiuojamas naudojant 10 formulę taip:

$$T_{Nr.1} = \sum_{i=1}^{R} t_i = t1+t2+t3+t4+t5+t6+t7+t8+t9+t10; \quad (19)$$

Bendra kaina paskaičiuojama naudojant 11 formulę sekančiai:

$$S_{Nr.1} = \sum_{i=1}^{R} s_i = s1+s2+s3+s4+s5+s6+s7+s8+s9+s10; \quad (20)$$

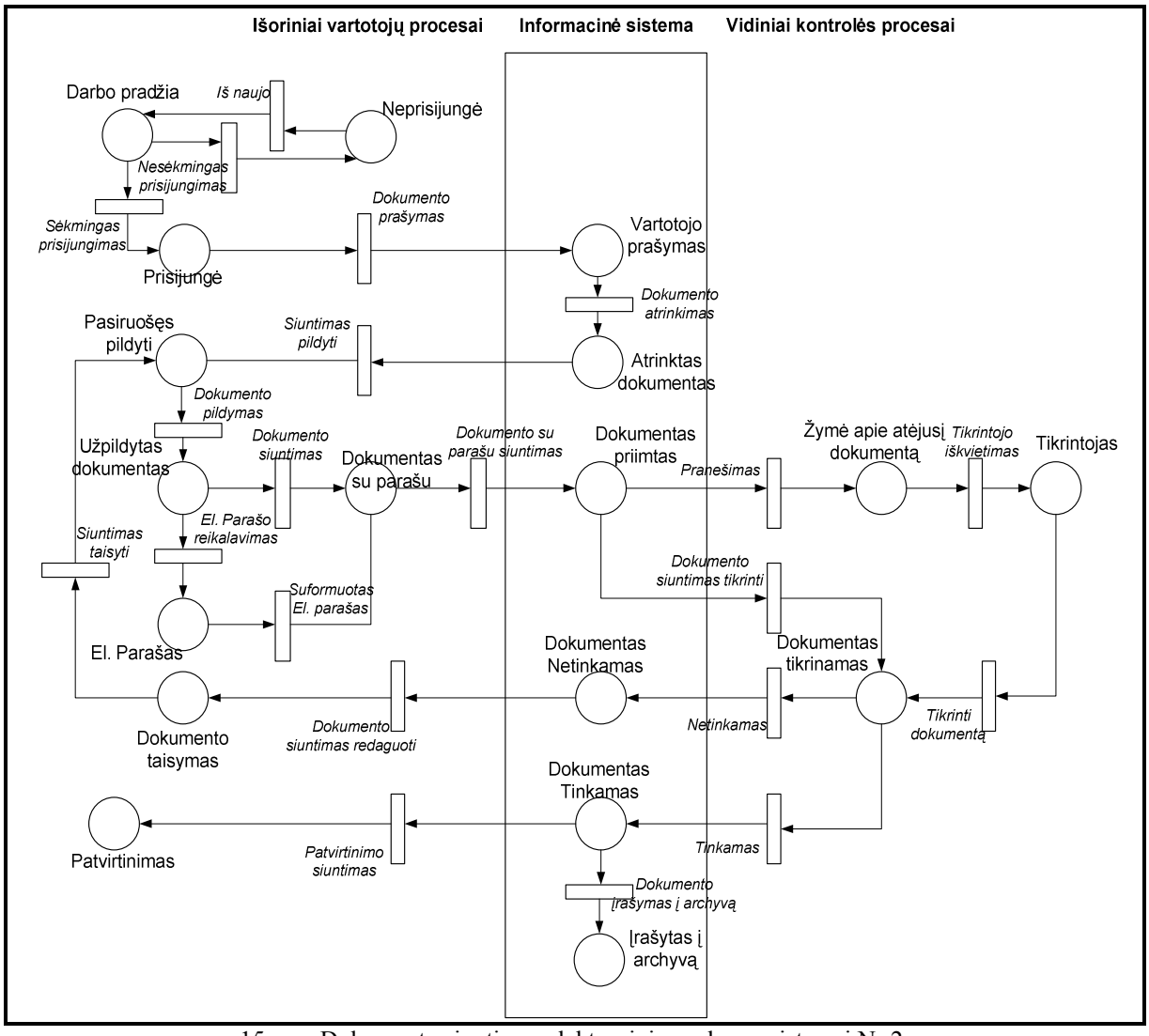
Paskaičiuojame pirmojo modelio IKP (12):

$$IKP_{Nr.1} = \frac{P_{Nr.1} * N_{Nr.1} * \frac{1}{T_{Nr.1}}}{S_{Nr.1}}; \quad (21)$$

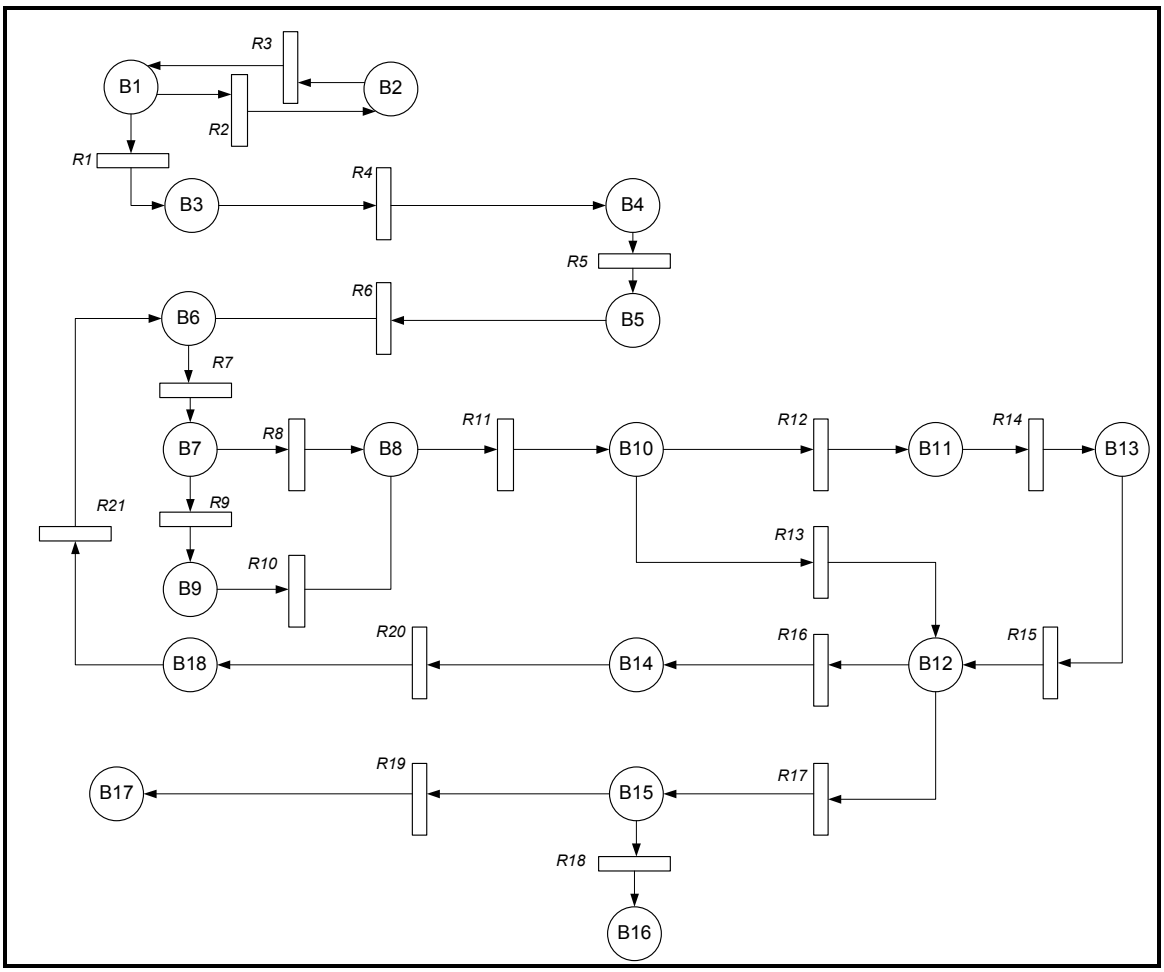
3.3. Elektroninės paslaugos modeliavimas Petri tinklu. Modelis Nr.2

15 paveiksle pavaizduotas sudėtingesnis elektroninės paslaugos modelis – pavadintas Nr.2, kuriame atliekami elementarūs dokumento pildymo, siuntimo ir tikrinimo veiksmai. Taip pat šiame modelyje reikalaujama vartotojo registracija, t.y. darbo pradžioje vartotojas turi prisijungti prie sistemos (nuotoliniu būdu tai dažniausiai daroma įvedant vartotojo vardą ir slaptažodį). Sekančiame žingsnyje vartotojas pateikia nutolusiai sistemai dokumento prašymą ir jį gauna. Ši dokumentą jis turi užpildyti, išsaugoti jį ir tik tuomet siųsti nutolusiai sistemai. Čia pirmiausiai formuojamas ir kartu su dokumentu siunčiamas vartotojo

elektroninis parašas, užtikrinantis dokumento priklausomumą konkrečiam vartotojui. Sistemoje iškviečiama dokumento tikrinimo procedūra, kuri tikrina atsiųstą elektroninį dokumentą. Jei dokumentas netinkamas, jis siunčiamas atgal vartotojui ir prašoma jį pakoreguoti. Jei dokumentas tinkamas, jis įrašomas į dokumentų archyvą, o vartotojui siunčiamas pranešimas, jog dokumentas priimtas. 16 paveiksle pavaizduotas tas pats sistemos paslaugos modelis, tačiau būsenos ir procesai pavadinti nuosekliais trumpinimais, kurie bus naudojami tolesniuose skaičiavimuose.



15 pav. Dokumento siuntimas elektroninių paslaugų sistemai Nr.2



16 pav. Dokumento siuntimas elektroninių paslaugų sistemai Nr.2. Atvaizdavimas būsenomis ir procesais

Išanalizavus 16 paveikslą pateikiamos jame pavaizduotos paslaugos būsenų ir procesų patikimumo, lankstumo, našumo ir kainos įverčių lentelės.

5 lentelė Modelio Nr.2 Būsenų patikimumas ir lankstumas

Būsena	Klaidos galimybė *kl*	Patikimumas pagal 3 formulę	Lankstumas *n*
B1	kl1	P1	n1
B2	kl2	P2	n2
B3	kl3	P3	n3
B4	kl4	P4	n4
B5	kl5	P5	n5
B6	kl6	P6	n6
B7	kl7	P7	n7
B8	kl8	P8	n8
B9	kl9	P9	n9
B10	kl10	P10	n10
B11	kl11	P1	n11
B12	kl12	P12	n12
B13	kl13	P13	n13
B14	kl14	P14	n14
B15	kl15	P15	n15
B16	kl16	P16	n16
B17	kl17	P17	n17
B18	kl18	P18	n18

3.3.1. Modelio Nr.2 kokybės parametrų skaičiavimai

Antrojo modelio bendras patikimumas būtų skaičiuojamas taip:

$$P_{Nr.2} = P1*P2*...*Pn = \quad (22)$$
$$= P1*P2*P3*P4*P5*P6*P7*P8*P9*P10*P11*P12*P13*P14*P15*P16*P17*P18;$$

Tačiau, kaip ir pirmojo modelio atveju, čia pastebimas lygiagretus būsenų jungimas. Taigi čia pagal 6 formulę turi būti paskaičiuoti sekantys elementai:

$$kl_{2,3} = \frac{kl_2 * kl_3}{kl_2 + kl_3}; \quad (23)$$

$$kl_{8,9} = \frac{kl_9 * kl_8}{kl_9 + kl_8}; \quad (24)$$

$$kl_{11,12,13} = \frac{kl_{11} * (kl_{12} + kl_{13})}{kl_{11} + kl_{12} + kl_{13}}; \quad (25)$$

$$kl_{16,17} = \frac{kl_{16} * kl_{17}}{kl_{16} + kl_{17}}; \quad (26)$$

$$kl_{14,15} = \frac{kl_{14} * (kl_{15} + kl_{16,17})}{kl_{14} + kl_{15} + kl_{16,17}}; \quad (27)$$

Tuomet, naudojant 3 formulę, gauname:

$$P_{2,3} = \frac{1 - kl_{2,3}}{1 + kl_{2,3}}; \quad (28)$$

$$P_{8,9} = \frac{1 - kl_{8,9}}{1 + kl_{8,9}}; \quad (29)$$

$$P_{11,12,13} = \frac{1 - kl_{11,12,13}}{1 + kl_{11,12,13}}; \quad (30)$$

$$P_{14,15} = \frac{1 - kl_{14,15}}{1 + kl_{14,15}}; \quad (31)$$

Taigi pirmojo modelio bendras patikimumas paskaičiuojamas taip (5):

$$P_{Nr.2} = P1*P2*...*Pn = P1*P_{2,3}*P4*P5*P6*P7*P_{8,9}*P10*P_{11,12,13}*P_{14,15}*P18; \quad (32)$$

Antrojo modelio bendras lankstumas skaičiuojamas sekančiai (9):

$$N_{Nr.1} = \frac{\sum_{i=1}^{B} n_i}{B} = \quad (33)$$

$$= \frac{n1 + n2 + n3 + n4 + n5 + n6 + n7 + n8 + n9 + n10 + n11 + n12 + n13 + n14 + n15 + n16 + n17 + n18}{B}$$

6 lentelė Modelio Nr.2 Procesų našumas ir kaina

Procesas	Našumas *t*	Kainas
R1	t1	s1
R2	t2	s2
R3	t3	s3
R4	t4	s4
R5	t5	s5
R6	t6	s6
R7	t7	s7
R8	t8	s8
R9	t9	s9
R10	t10	s10
R11	t11	s11
R12	t12	s12
R13	t13	s13
R14	t14	s14
R15	t15	s15
R16	t16	s16
R17	t17	s17
R18	t18	s18
R19	t19	s19
R20	t20	s20
R21	t21	s21

Antrojo modelio bendras našumas skaičiuojamas taip (10):

$$T_{Nr.2} = \sum_{i=1}^{R} t_i = \quad (34)$$

= t1+t2+t3+t4+t5+t6+t7+t8+t9+t10+t11+t12+t13+t14+t15+t16+t17+t18+t19+t20+t21;

Antrojo modelio bendra kaina paskaičiuojama sekančiai (11):

$$S_{Nr.2} = \sum_{i=1}^{R} s_i = \quad (35)$$

= s1+s2+s3+s4+s5+s6+s7+s8+s9+s10+s11+s12+s13+s14+s15+s16+s17+s18+s19+s20+s21;

Paskaičiuojame antrojo modelio IKP (12):

$$IKP_{Nr.2} = \frac{P_{Nr.2} * N_{Nr.2} * \frac{1}{T_{Nr.2}}}{S_{Nr.2}}; \quad (36)$$

3.4. Praktiniai modelių Nr.1 ir Nr.2 skaičiavimai

Atliksime bandomąjį IKP skaičiavimą pasirinkę atsitiktinius būsenų ir procesų kokybinių parametrų įverčius. Vertinant realius sistemų modelius šie kokybinių parametrų įverčiai turi būti tiksliai apibrėžti ir paskaičiuoti.

Tarkime, kad kiekvienos būsenos klaidos galimybė tiek Nr.1, tiek Nr.2 modeliuose yra vienoda ir lygi 0,5 – t.y. klaida vienodai tikėtinai gali įvykti arba ne. Tuomet būsenos patikimumas pagal 3 formulę yra lygus 0,67.

Modelio būsenų lankstumas įvertinamas atlikus Petri tinklo analizę taip, kaip aprašyta 3.1.2. skyrelyje. Taigi atlikus abiejų modelių Petri tinklo analizę gauname rezultatus, kurie pateikti 7 lentelėje.

7 lentelė Modelių Nr.1 ir Nr.2 būsenų lankstumai

Nr.2 modelis		**Nr.1 modelis**	
Būsena	Lankstumas	Atitinkanti Būsena	Lankstumas
B1	2	-	-
B2	1	-	-
B3	1	-	-
B4	1	-	-
B5	1	B1	1
B6	1	B2	1
B7	2	B3	0
B8	1	B4	1
B9	1	-	-
B10	2	B5	0
B11	1	-	-
B12	2	B6	2
B13	1	-	-
B14	1	-	-
B15	2	B8	2
B16	0	B9	0
B17	0	B10	0
B18	1	B7	1

Skaičiuojant modelių našumą laiko vertinimui nenaudosime jokių matavimo vienetų. Tarkime, kad kiekvieno proceso atlikimo laikai yra vienetiniai, t.y. lygūs 1.

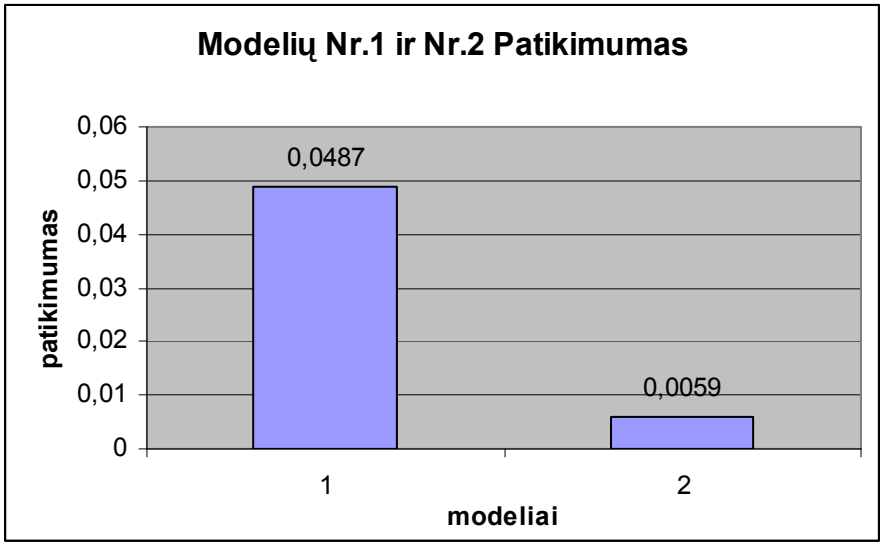
Modelio kainos skaičiavime taip pat laikomės prielaidos, jog kiekvieno proceso kaina yra vienetinė, t.y. lygi 1.

3.5. Modelių Nr.1 ir Nr.2 palyginimas

Atlikus skaičiavimus naudojant 5, 9, 10, 11, 12 formules, gauti tokie rezultatai:

$P_{Nr.1} = 0,0487;$

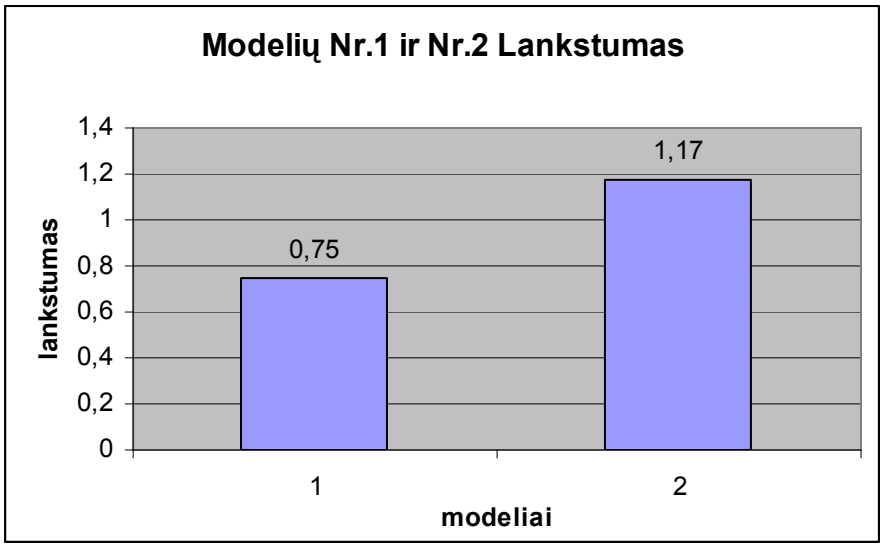
$P_{Nr.2} = 0,0059;$



17 pav. Modelių Nr.1 ir Nr.2 patikimumas

$N_{Nr.1} = 0,75;$

$N_{Nr.2} = 1,17;$



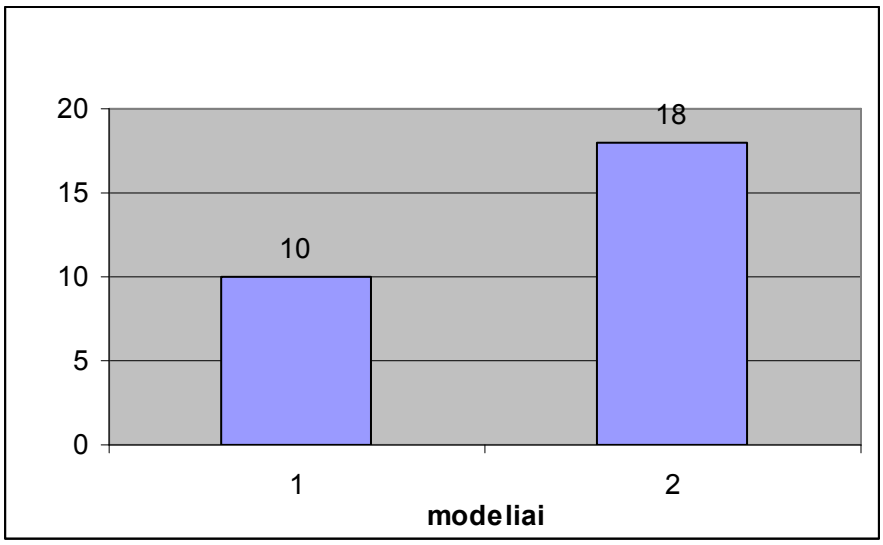
18 pav. Modelių Nr.1 ir Nr.2 lankstumas

$T_{Nr.1} = 10;$

$T_{Nr.2} = 18;$

$S_{Nr.1} = 10;$

$S_{Nr.2} = 18;$

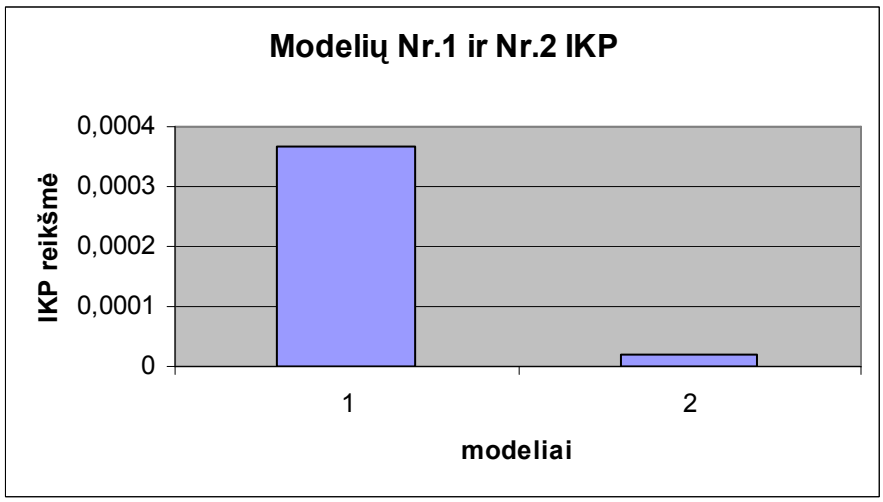


19 pav. Modelių Nr.1 ir Nr.2 kainos ir procesų atlikimo laikų reikšmės

Pateikiami gauti abiejų modelių IKP rezultatai:

$$IKP_{Nr.1} = \frac{0,0487 * 0,75}{10 * 10} = 0,00036525;$$

$$IKP_{Nr.2} = \frac{0,0059 * 1,17}{18 * 18} = 0,0000213056;$$



20 pav. Modelių Nr.1 ir Nr.2 IKP

Analizuojant 20 paveiksle pateiktą grafiką pastebėta, jog pirmojo modelio IKP yra žymiai didesnis už antrojo. Iš 17 paveikslo matyti, kad modelių paskaičiuotas patikimumas taip pat yra žymei didesnis pirmajame modelyje. Kaina ir našumas yra didesni antrajame modelyje (žiūrėti 19 paveikslą).

3.6. Kokybės parametru gerinimas ir IKP didinimas

Galima pastebėti, kad sistemos kainą sumažinti galima tik mažinant procesų skaičių. Ji tiesiogiai priklauso nuo kiekvieno iš sistemoje realizuotų procesų kainos. Taip pat yra ir su sistemos našumu. Jis tiesiogiai priklauso nuo sistemoje realizuotų procesų našumo. Kuriant sistemą turi būti apibrėžti reikalavimai būsimiems procesams. Jei proceso galima atsisakyti, tuomet sistemoje gali būti pasiektas didesnis našumas ir mažesnė kaina.

Tuo tarpu sistemos lankstumas pasiektas kurkas didesnis antrajame modelyje. Tai yra todėl, kad antrasis modelis yra kur kas didesnis ir jame numatytos įvairios sistemos veikimo galimybės esant atitinkamoms būsenoms.

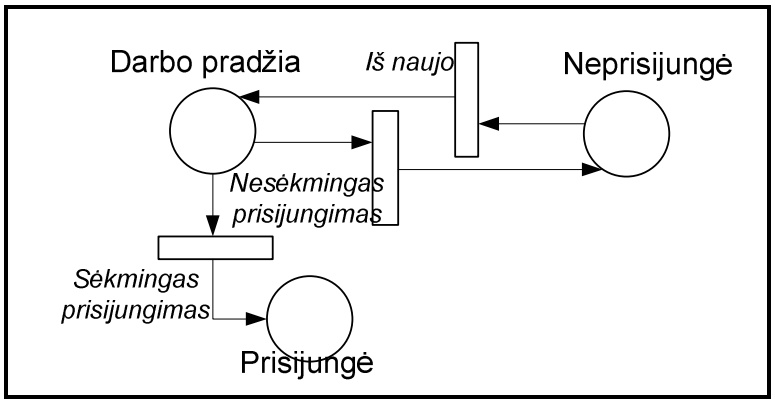
Taigi norint pasiekti didesnį IKP reikia didinti sistemos patikimumą lankstumą ir našumą (mažinti procesų atlikimo laikus), bei mažinti sistemos kainą.

Sistemos našumas ir kaina tiesiogiai priklauso nuo realizuotų procesų, o jie savo ruožtu būna privalomi arba ne, priklausomai nuo keliamų reikalavimų būsimai sistemai. Taigi siekiant geresnių šių kokybės parametrų IKP ženkliai padidinti negalima.

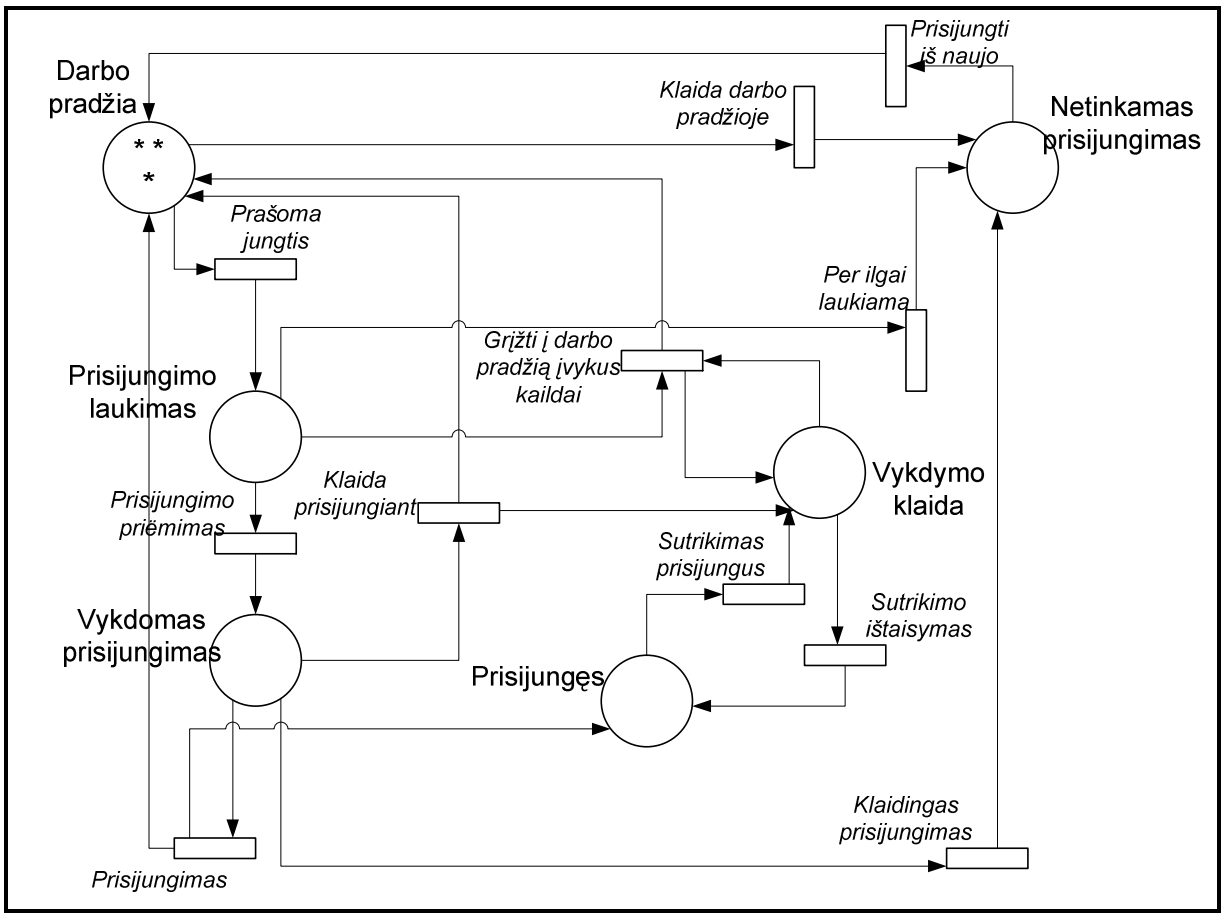
Tuo tarpu siekiant geresnių patikimumo ir lankstumo galima ženkliai padidinti IKP. Lankstumas tiesiogiai priklauso nuo kuriamos sistemos architektūros, o patikimumas gali būti pasiektas mažinant konkrečių būsenų klaidų galimybes.

Norint pasiekti maksimalų patikimumą atitinkamoje būsenoje, reikia numatyti ir realizuoti visas įmanomas situacijas, kurios gali įvykti sistemos darbo režime. Patikimumo didinimui galima pasinaudoti 2.5.1. skyrelyje aprašytu metodu.

Realizuojamas maksimalus patikimumas. Išskiriama 15 paveiksle pavaizduoto Nr.2 modelio vartotojo prisijungimui prie sistemos procedūra. Atliekama detali procedūros būsenų galimų situacijų analizė. Pateikiami du šios procedūros modeliai. A modelyje atliktas pats paprasčiausias vartotojo prisijungimas. B modelyje atliktas patikimas vartotojo prisijungimas.



21 pav. Vartotojo prisijungimas prie sistemos. Modelis A



22 pav. Patikima vartotojo prisijungimo prie sistemos procedūra. Modelis B

Taigi atlikus veiksmus, kurie pavaizduoti 22 paveiksle, gaunamas patikimos vartotojo prisijungimo procedūros Petri tinklo modelis. Šiuo atveju kiekvienoje būsenoje yra apibrėžtos visos galimų procedūros klaidų situacijos, todėl būsenų patikimumas yra maksimalus, t.y. lygus 1.

Paskaičiavus 21 ir 22 paveiksluose pavaizduotų A ir B modelių procedūrų kokybinius parametrus, naudojant 5, 9, 10, 11, 12 formules, gauti tokie rezultatai:

$P_B = 1;$ $N_B = 2;$

$P_A = 0,625;$ $N_A = 0,67;$

$T_B = 6;$ $S_B = 6;$

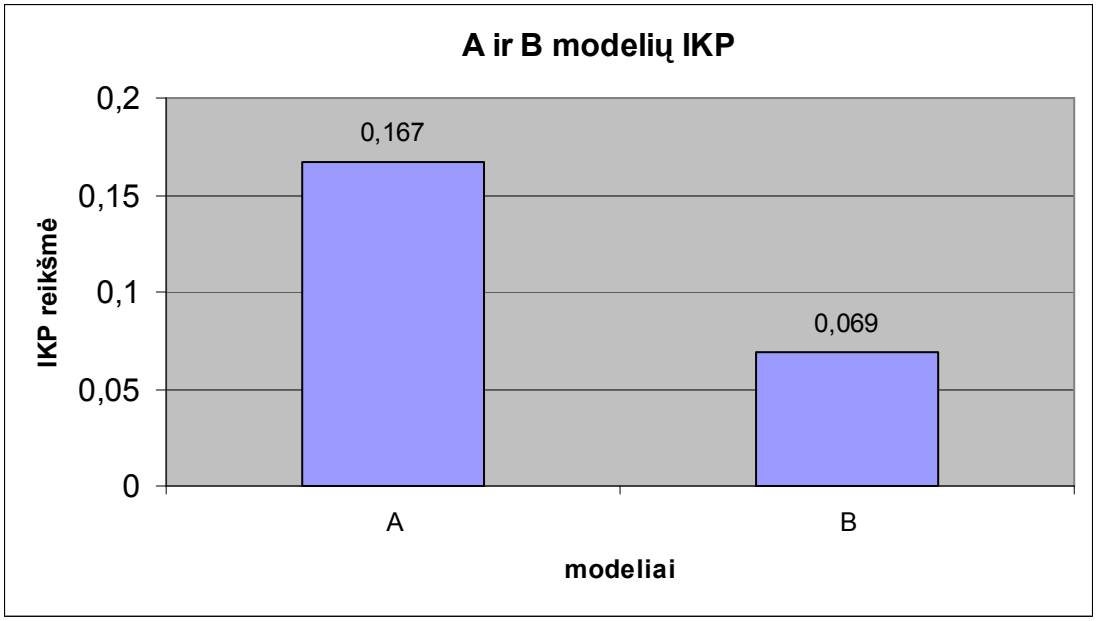
$T_A = 3;$ $S_A = 3;$

$$IKP_B = \frac{1*2}{6*6} = 0,167;$$

$$IKP_A = \frac{0,625*0,67}{3*3} = 0,069;$$

Detalūs šių kokybinių parametrų skaičiavimai pateikti 2 priede.

Akivaizdu, jog B modelio tiek patikimumas, kuris yra maksimalus, tiek lankstumas yra žymiai geresni nei A modelio. Todėl, esant nedideliam kainos ir našumo skirtumui, IKP taip pat pasiektas kur kas didesnis. Tai atvaizduota 23 paveiksle.



23 pav. Modelių A ir B IKP

Reziumuojant galima daryti išvadą, jog IKP didžiausią įtaką turi patikimumas bei lankstumas, o kainos ir našumo parametrai yra mažiau reikšmingi. Tai yra todėl, kad turint kuriamos sistemos reikalavimus, yra būtina realizuoti tam tikrus procesus, kurių atlikimo laikai ir kaina tiesiogiai priklauso nuo pačių procesų, tuo tarpu sistemos projektuotojas gali numatyti būsimą sistemos struktūrą ir ją koreguoti. Teisingų korekcijų dėka galima padidinti būsenų patikimumą ir lankstumą.

Siekiant kuo didesnio sistemos patikimumo, turi būti įvertintos visos galimos klaidos sistemos būsenose ir tų klaidų sprendimo būdai.

Pasiekus didesnį patikimumą pastebimai padidėja ir sistemos lankstumas. Tai įvyksta todėl, kad konkrečioje būsenoje numatomi įvairūs klaidų sprendimo procesai ir perėjimai. Kuo didesnis būsenos išėjimų skaičius, tuo didesnis būsenos lankstumas.

Kainos ir našumo kokybės parametrai tiesiogiai priklauso nuo sistemoje realizuojamų procesų. Šie procesai turi būti specifikuodami prieš kuriant sistemą. Turi būti aprašyti procesai, kurie yra privalomi, o kurių gali ir nebūti. Kiekvienas procesas turi savo kainą ir našumo įvertį, kurie gali būti paskaičiuojami praktiškai arba analizės metu. Bendra sistemos kaina susideda iš visų procesų. Bendras našumas taip pat paskaičiuojamas iš visų procesų našumo įverčių.

IŠVADOS

1. Informacinės saugos problema yra viena iš pagrindinių atvirųjų sistemų teorijos ir praktikos problemų. Taigi informacijos saugumas yra svarbus uždavinys bet kuriai įmonei, organizacijai ar paprastai sistemai.

2. Atlikta fizinių ir tinklinių grėsmių elektroninių paslaugų sistemai, patikimų vartotojų tapatybės atpažinimo ir patikimo informacijos perdavimo užtikrinimo būdų analizė.

3. Viešųjų elektroninių paslaugų teikimas pastaruoju metu yra viena iš svarbiausių, o neretai ir pati svarbiausia daugelio pasaulio valstybių vyriausybių strategijos dalis. Daugelio šalių vyriausybės įžvelgia didelę naudą pereinant nuo viešųjų paslaugų teikimo įprastais būdais prie viešųjų paslaugų teikimo elektroninėmis formomis.

4. Informacijos technologijų panaudojimo galimybės viešojo administravimo sektoriaus darbo modernizavimui yra labai plačios. Vis didėjantis informacijos technologijų naudojimas, ypač galimybė naudotis internetu, iš esmės keičia valdžios veiklos galimybes. Kuriamos Elektroninės Valdžios sistemos.

5. Pateikti elektroninės valdžios paslaugų teikimo techniniai sprendimai. Išanalizuotas elektroninio dokumento autentiškumo užtikrinimas ir virtualaus privataus tinklo panaudojimas saugumui užtikrinti elektroninės valdžios sistemoje.

6. Išanalizuoti taikomųjų uždavinių kokybės parametrų modeliavimo, skaičiavimo ir vertinimo ypatumai.

7. Lankstumas, patikimumas, našumas ir kaina turi būti nuolat analizuojami modeliuojant būsimą el. paslaugų sistemą.

8. Sistemos patikimumas pasirinktas kaip pagrindinis taikomųjų uždavinių kokybės parametras. Atlikta jo modeliavimo analizė, stochastinių Petri tinklų panaudojimas patikimumui modeliuoti bei patikimumo ir našumo skaičiavimų analizė.

9. Sukurtas pagrindinių taikomųjų uždavinių kokybės parametrų formalizavimas. Pasirinkti patikimumo, lankstumo, našumo ir kainos skaičiavimų mechanizmai. Apibrėžtas integruotasis kokybės parametras, naudojamas modelių palyginimui apjungiant visus naudojamus kokybės parametrus.

10. Pateikti du elektroninės paslaugos modeliai. Atlikti šių modelių kokybės parametrų skaičiavimai ir palyginimai.

11. Pasirinktas taikomųjų uždavinių kokybės parametrų gerinimo ir integruotojo kokybės parametro didinimo būdas. Šis būdas sėkmingai padėjo pagerinti atitinkamus parametrus.

LITERATŪRA

[1]. Bartkevičius S., Spalvotųjų Petri tinklų taikymas valdymo sistemoms modeliuoti/ S. Bartkevičius, V. Mačerauskas, K. Šarkauskas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2003. – Nr. 4(46). – P. 7-11.

[2]. Bastine R. Synergistic modelling of tasks, users and systems using formal specification techniques/ P. Palanque, R. Bastine// Iš „Interacting with Computers 9 (2)" [online]. p. 129-153. Toulouse, France, 1997. Prieiga per internetą: < http://liihs.univ-tlse1.fr/bastide/Research/Papers/bastide_IWC_1998.pdf >

[3]. Bendrųjų dokumentų saugojimo terminų rodykle, patvirtinta Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės 1997 m. rugpjūčio 15 d. įsakymu Nr. 38 (Žin., 1997, Nr. 78-2006; 2001, Nr. Nr.99-3577)

[4]. Billington J., Application of Petri Nets to Communication Networks: Advances in Petri Nets/ J. Billington, G. Rozenberg, J. Hartmanis, G. Goos, M. Diaz// Springer-Verlag New York, LLC, 1999. p. 310. ISBN: 354065870X

[5]. Blatchford C., Information security, business and the internet — Part 1, Network Security Volume 2000, Issue 1 , January 2000, p. 8-12. Available online 10 March 2000. Prieiga per internetą: < www.sciencedirect.com >

[6]. Bobbio A. System modelling with petri nets, Istituto Elettrotecnico Nazionale Galileo Ferraris, Italy, 1999. p. 41.

[7]. Cadle J., Project management for information systems / edited by James Cadle, Donald Yeates// Harlow [etc.] : Pearson Education, 2001. 384 p.

[8]. Cassidy A., A practical guide to information systems process improvement / A. Cassidy, K. Guggenberger// Boca Raton [etc.] : St. Lucie Press, 2001. 269 p.

[9]. Choi H., Performance and reliability modeling using Markov regenerative stochastic Petri nets, Department of Computer Science Duke University, 1993. p. 162.

[10]. Eidukas D., Nuotolinis pastato sistemų valdymas/ D. Eidukas, A. Valinevi c ius, Š. Kilius, M. Žilys// ISSN 1392 – 1215 Elektronika ir elektrotechnika. 2003. nr.6(48), t 170 Elektronika, 2003 p. 38-42. Prieiga per internetą:
< http://www.ktu.lt/lt/mokslas/zurnalai/elektr/z48/Eidukas.pdf >

[11]. Elektroninė Valdžia Lietuvoje. Prieiga per internetą:
< http://www.evaldzia.lt > ir < http://www.lietuva.lt/IMI/i_lt.jsp?nr=iv_evaldzia >

[12]. Fricks R.M., Modeling failure dependencies in reliability anglysis using stochastic Petri nets/ R. M. Fricks, K. S. Trivedi// Duke university, 1999. p. 21

[13]. Fu X. Formal Verification of El. services and Workflow/ X. Fu, T. Bultan, J. Su // Proceedings of Workshop on "Web Services, el. Business, and the Semantic Web (WES): Foundations, Models, Architecture, Engineering and Applications" [Toronto, Ontario, Canada, May 2002; Lecture Notes in Computer Science, Vol 2512.]. Santa Barbara, USA. 2002. 20 p.

[14]. Ghosh S., Principles of secure network systems design / Sumit Ghosh ; with a foreword by Harold Lawson// New York : Springer-Verlag, 2002. 209 p.

[15]. Gupta M.P., E-government evaluation: a framework and case study/ M. P. Gupta, J. Debashish// Government Information Quarterly Volume 20, Issue 4, 2003. p. 365-387. Available online 11 December 2003. Prieiga per internetą: http://www.sciencedirect.com

[16]. Hrischuk C., Automatic generation of a software performance model using an object-oriented prototype/ C. Hrischuk, J. Rolia, C.M. Woodside// 3rd International Workshop on Modeling, Analysis, and Simulation Durham, North Carolina ,January 18 - 20, 1995. p. 399.

[17]. Jastramskas V., Informacijos apsaugos pagrindai : mokomoji knyga; Kauno technologijos universitetas. Telekomunikacijų katedra. Kaunas : Technologija, 1999. 181 p.

[18]. Lindemann C. Performance modelling with deterministic and stochasic petri nets. Chichester: John Wiley & Sons, 1998. 405 p.

[19]. Liu D. Designing a composite el. service platform with recomendation function [online]/ D. Liu, M. Shen, C. Liao// Computer Standards & Interfaces Volume 25, Issue 2, May 2003, p. 103-117.

[20]. Marseguerra M., A concept paper on dynamic reliability via Monte Carlo simulation/ M.Marseguerra, E.Zio, J.Devooght, P.E.Labeau// Mathematics and Computers in Simulation 47, 1998. p. 371 –382.

[21]. Marsequer J. Performance analysis of internet based sofware retrieval systems using Petri nets [online]/ J. Marsequer, J. Campos, E. Mena// 2001. p. 47 – 56. ISBN:1-58113-378-2. Prieiga per internetą:
< http://portal.acm.org/citation.cfm?id=381604&dl=ACM&coll=portal >

[22]. Northcutt S., Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems/ S. Northcutt, L. Zeltser, S. Winters// Pearso education, 2002. p. 678. ISBN: 0735712328

[23]. O'Connor P.D.T., Practical reliability engineering / Patrick D.T. O'Connor, David Newton, Richard Bromley// Chichester : Wiley, 2003. 513 p.

[24]. Petri Nets. Petri tinklai. Prieiga per internetą:
< http://pdv.cs.tu-berlin.de/~azi/petri.html > ir
< http://vejas.pit.ktu.lt/~kazysba/ds/ds96r/petri_t/petri.htm >

[25]. Silva M. Performance models based on Petri nets/ M. Silva, J. Campos // IFAC Second International Symposium on Mathematical and Intelligent Models in System Simulation, [Brussels, Belgium: Proceedings of the IMACS, April 1993.]. Zaragosa,1993. p. 14-21.

[26]. Stallings W., Cryptography and network security : principles and practice. Upper Saddle River : Prentice Hall, 1999. 569 p.

[27]. Tardugno A.F., IT Services: Costs, Metrics, Benchmarking and Marketing/ A. F. Tardugno, R. E. Matthews, T. R. DiPasquale// Pearson education, 2000. p. 208. ISBN: 0130191957.

[28]. Tipton H., Information Security Management Handbook/ H. Tipton, M. Krause// CRC Press, 2003. p. 2000. ISBN: 0849319978.

[29]. V.F.Nicola V.F., Techniques for fast simulation of models of highly dependable systems/ V.F.Nicola, P.Shahabuddin,M.K.Nakayama// IEEE Transactions of Reliability 50 (3), 2001. p. 246 –264.

[30]. Volovoi V. Modeling of system reliability using Petri nets with aging tokens Reliability engineering and system safety, 2003. 10 p.

[31]. Wadlow T.A., The process of network security : designing and managing a safe network. Reading [etc.] : Addison-Wesley, 2000. 283 p.

[32]. Wells L. Performance analysis using Coloured Petri nets: daktaro disertacija, University of Aarhus, 2002. 152 p.

[33]. Zhang G.W., Research on flexible transfer line schematic design using hierarchical process planning/ G. W. Zhang, S. C. Zhang, Y. S. Xu//. Journal of Materials Processing Technology, Volume 129, Issues 1-3, 11 October 2002, p. 629-633. Available online 24 September 2002. Prieiga per internetą:
< www.sciencedirect.com >

[34]. Zheng D., Achieving software flexibility via inteligent workflow techniques/ D. Zheng, J. Zhao// 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 1 Big Island, Hawaii, January 07 - 10, 2002. p.43.

[35]. VPN (Virtualusis privatus tinklas). Prieiga per internetą:
< http://security.5ci.lt/default.asp?DL=L&TopicID=36 >

P R I E D A I

1 Priedas.

Informacinių technologijų taikymo reikalavimai

1. El. dokumentams rengti rekomenduojama naudoti MS Office paketo (ne žemesnę kaip MS Office 97 versiją) ar atvirojo kodo (pavyzdžiui, Open Office) programų priemones. Rekomenduojami el. dokumentų formatai, kuriuos atpažįsta bent viena iš minėtų programų taip pat PDF, JPG ir kitus plačiausiai paplitusius formatus, kuriuos galės atpažinti mainų dalyvis.

2. Rekomenduojama naudoti elektroninio parašo algoritmą DSA-SHA1. DSA – Digital Signature Algorithm – algoritmas, naudojamas skaitmeniniam parašui suformuoti, o SHA1 - Secure Hash Algorithm 1 – algoritmas, naudojamas pranešimo santrumpai suformuoti. Pagal XML-Signature Syntax and Processing specifikaciją programinė įranga, realizuojanti šią specifikaciją, turi būtinai realizuoti DSA-SHA1 algoritmą.

3. Siuntinio formavimo kalba XML. Siuntinio elektroninis parašas – XML skaitmeninis parašas, kuris apibrėžtas W3C XML-Signature Syntax and Processing specifikacijoje.

4. Failų vardams negalima naudoti simbolių iš aibės - {/,\,:,*,?,”,<,>,|}

5. Pagal XML Schema 1.0 specifikaciją dvejetainės informacijos kodavimui naudotinas base64Binary kodavimo būdas.

6. Talpinant el. dokumentą į siuntinį būtinai reikia nurodyti, ar jo formatas tekstinis ar dvejetainis. Jei el. dokumento formatas tekstinis, turi būti nurodoma kodavimo lentelė.

7. Senesnių siųstų bei gautų siuntinių archyvams rekomenduojama naudoti elektronines laikmenas, į kurias informacija tik įrašoma, bet negali būti keičiama ar šalinama, pavyzdžiui, kompaktinis diskas (CD-R).

2 Priedas.

A ir B modelių skaičiavimai

Atliekami 21 ir 22 paveiksluose pavaizduotų A ir B modelių procedūrų kokybinių parametrų skaičiavimai, naudojant 5, 9, 10, 11, 12 formules, gauti tokie rezultatai:

Tarkime, kad A modelio kiekvienos iš trijų būsenų klaidos tikimybė lygi 0,33, tuomet kiekvienos būsenos patikimumas bus lygus 0,5 pagal 6 formulę. Bendras procedūros patikimumas lygus:

$P_A = P1*P2*P3 = 0,5*0,5*0,5 = 0,625$

Tuo tarpu B modelyję realizuotas visiškas patikimumas, todėl $P_A = 1$.

Skaičiuojant lankstuma buvo atlikta 21 ir 22 paveikslų analizė ir palyginimas. Pateikiama išanalizuotų būsenų ir jų lankstumų įverčiai.

B modelis		**A modelis**	
Būsena	Lankstumas	Atitinkanti Būsena	Lankstumas
B1	2	B1	2
B2	3	-	
B3	3	-	
B4	1	B2	-1
B5	2	-	
B6	1	B3	1

B modelio bendras lankstumas skaičiuojamas sekančiai (9):

$$N_B = \frac{\sum_{i=1}^{B} n_i}{B} = (2+3+3+1+2+1)/6 = 2$$

B modelio bendras lankstumas skaičiuojamas sekančiai (9):

$$N_A = \frac{\sum_{i=1}^{B} n_i}{B} = (2-1+1)/3 = 0,67$$

Tarkime, kad tiek modelyję A, tiek ir B procesų atlikimo laikai yra vienetinei, ir procesų kainos taip pat vienetinės. Tuomet:

$$T_B = \sum_{i=1}^{R} t_i = t1+t2+t3+t4+t5+t6 = 6;$$

$$T_A = \sum_{i=1}^{R} t_i = t1+t2+t3 = 6;$$

$$S_B = \sum_{i=1}^{R} s_i = s1+s2+s3+s4+s5+s6 = 6;$$

$$S_A = \sum_{i=1}^{R} s_i = s1+s2+s3 = 3;$$

$$IKP = \frac{P * N * \frac{1}{T}}{S};$$

Atlikti elementarūs skaičiavimai ir gautas rezultatas:

$$IKP_B = \frac{1*2}{6*6} = 0{,}167;$$

$$IKP_A = \frac{0{,}625*0{,}67}{3*3} = 0{,}069;$$

3 Priedas.

Virtualusis privatus tinklas

Šiuolaikiniame versle keliami aukšti reikalavimai visų informacijos išteklių apsaugos sistemoms:

- Biurų sujungimas į saugų tinklą;
- Saugi tolimųjų ir mobiliųjų vartotojų prieiga;
- Apsaugos priemonių centralizuoto valdymo sistema;
- Pašto sistemos apsauga;
- Taikomųjų išskirstytų sistemų apsauga;
- Elektroninei komercijai skirtas sprendimas „B2B";
- Prekybos kompanijai skirtas sprendimas;
- Informacinių paslaugų tiekėjams skirtas sprendimas;
- Finansinių organizacijų informacinių išteklių apsaugai skirtas sprendimas;

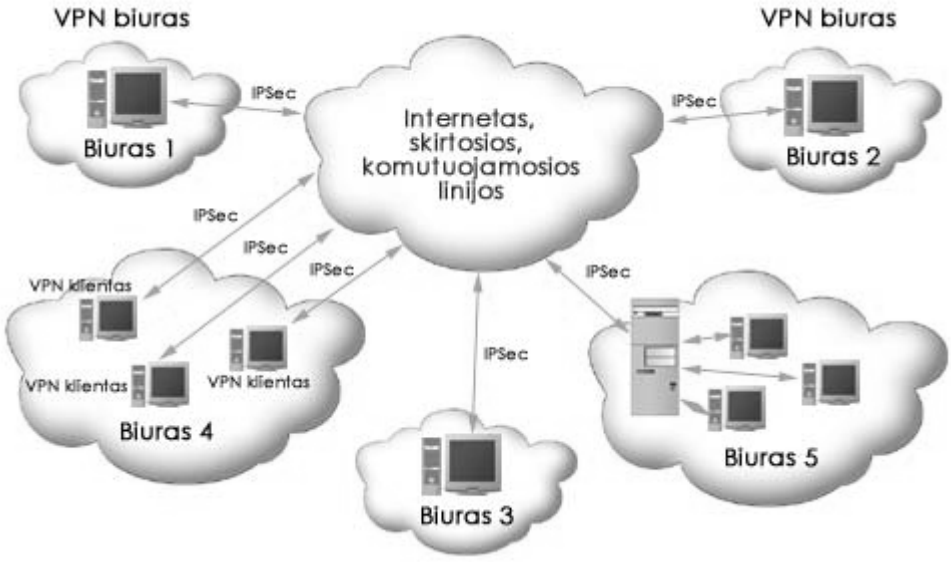
Didelis apsauginių programinių sprendimų mobilumas ir išplečiamumas, pritaikant įvairioms sisteminėms-techninėms sistemoms, įdiegimo, konfigūravimo ir eksploatavimo paprastumas, galimybė jas valdyti derinant su centralizuota apsaugos strategija – tai svarbūs stambių korporacijų, taip pat vidutiniojo ir smulkaus verslo įmonių keliami reikalavimai.

Įmonių tinkle esančių informacijos išteklių apsaugos ir atviraisiais tinklais perduodamos informacijos apsaugos sprendimai gali būti realizuoti panaudojant sertifikuotus VPN produktus, kuriuose naudojama technologija *FireWall* – saugiai sąveikai su išorine aplinka elektronines leksemas (*e-token)* – tinklo vartotojų tapatybei patvirtinti.

Nedidelėms įmonėms, naudojančioms iki dešimties tinklo punktų, tinka VPN produktai su patogia grafine sąsaja, kuriuos galima konfigūruoti vietoje, nenaudojant centralizuoto valdymo.

Stambioms įmonėms geriau tiktų sistemos su operatyviai tinklo punktus valdančiu valdymo centru, kuris leidžia sudaryti daugiasluoksnę vartotojų pažymėjimų (sertifikatų) struktūrą.

Kompanijai augant, VPN technologija leidžia nesudėtingai didinti pajėgumą ir pereiti prie centralizuoto valdymo.



„Virtualusis privatus tinklas"

Nagrinėjami įvairioms paskirtims naudojami tipiniai sprendimai, kurie daugiausia priklauso nuo: verslo procesų topologijos (ne tik nuo tinklų topologijos); verslo procesų specifikos su lanksčiai taikoma apsaugos strategija.

Siūlomiems sprendimams galima naudoti gamą išplečiamųjų produktų, turinčių šias galimybes:

- informacijos apsauga, nepriklausanti nuo jos perdavimo būdų ir aplinkos (palydovinės, optinės, telefono, radiorelinės linijos);
- bet kokių taikomųjų programų apsauga, dėl kurios nereikia jų keisti;
- visiškas „skaidrumas" galutiniams vartotojams;
- išplečiamųjų apsaugos sistemų realizavimas ir jų plėtra;
- informacinės sistemos apsauga nuo įsibrovimo iš išorinės aplinkos;
- garantuota apsauga nuo informacijos perėmimo ir pakeitimo ne tik išorinėse jungtyse bet ir korporacijos vidaus tinkluose;
- šifravimo algoritmų naudojimas per keičiamąsias plokštes;
- atskirų VPN vartotojų tapatybės patvirtinimas, panaudojant bet kokias priemones: elektronines korteles, USB įtaisus ir kt.

Biurų sujungimas į saugų tinklą

Kai verslas yra išskirstytas ir valdomas iš keleto biurų, reikia ne tik apsaugoti kiekvieną iš tokių skyrių, bet ir sujungti visus juos į sistemą su bendra informacine erdve.

Siūlomas sprendimas saugaus korporacinio tinklo perimetrui sudaryti remiantis VPN technologija (2 paveikslas). Sprendimas pagrįstas tuo, kad kiekvieno biuro tinklo kompiuterių tinklo apsaugai ir apsaugai nuo neleistino pasinaudojimo iš išorinių tinklų naudojama programinė įranga „VPN-Office". Duomenų srautui tarp centrinio biuro ir filialų apsaugoti kiekviename vietinio tinklo šliuze įdiegiama „VPN-Office", paslepianti biurų tinklų vidinę topologiją.

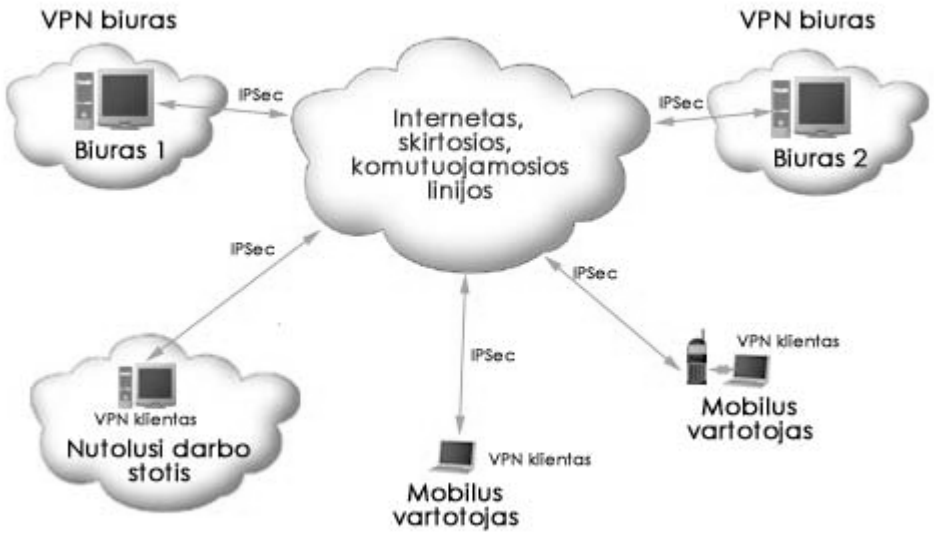
Tokio sprendimo privalumas yra išplečiamumas – prieigą tolimiesiems ir mobiliesiems vartotojams galima suteikti tuomet, kai to prireikia. Kai susijungiama su nedideliu filialu, kuriame kompiuterių nėra daug, kiekvienoje darbo vietoje galima įdiegti programinę įrangą „VPN-Client" arba tarnybinėje stotyje, kurioje laikoma svarbi informacija – „VPN-Server". Kiekvienu konkrečiu atveju nusprendžiama atsižvelgiant į vieno ar kito produktų komplekto ekonominį pagrįstumą.

Saugi tolimųjų ir mobiliųjų vartotojų prieiga

Rinkos sąlygomis kompanijos atstovams dažnai tenka būti pačiose tolimiausiuose geografinėse vietose. Ten atsiradusiems reikalams tvarkyti būtinas ne tik transportas, bet ir ryšio priemonės.

Tokiais atvejais korporacijos tinkle reikia įdiegti saugias mobiliąsias darbo vietas keliaujantiems darbuotojams ir užtikrinti jiems galimybę prisijungti prie kompanijos tinklo per saugų kanalą. Kitaip tariant, korporacijos tinklo apsaugotasis perimetras turi gebėti „išsitempti" ir pereiti per bet kokius bendro naudojimo IP tinklus, bet kartu išlikti toks saugus, lyg niekas iš darbuotojų nebūtų išvykęs iš biuro, t.y. užtikrinti nustatytą konfidencialumo ir nepažeidžiamumo lygmenį.

Tinklo įeigos šliuze įdiegus programinę įrangą „VPN-Office" arba korporacijos tarnybinėje stotyje (pašto, duomenų bazės, Interneto) – „VPN-Server", o mobiliojoje darbo vietoje – „VPN-Client", vartotojas per saugų kanalą gali pasiekti būtiną kompanijos informaciją nepriklausomai nuo savo buvimo vietos ir prisijungimo prie interneto būdo.



„VPN biuro pasiekiamumas“

3 paveiksle pavaizduotas sprendimas suteikia galimybę pasiekti tinklą iš bet kurios pasaulio vietos, taip pat ir mobiliuoju telefonu. Šio sprendimo išskirtinė savybė – saugaus ryšio galimybė su kintamus IP adresus turinčiais vartotojais pagal jų pažymėjimus.

Jei kompiuteris būtų pavogtas arba pamestas, pašaliniai asmenys negalėtų pasinaudoti informacija, kadangi tapatybė patvirtinama slaptažodžiu arba elektronine kortele, kuri leidžia naudotis VPN konkrečiam vartotojui. Visa informacija apie vartotoją, įskaitant ir jo pažymėjimą bei jam priskirtą VPN konfigūraciją, laikoma ne kompiuteryje, o elektroninėje kortelėje. Ištraukus elektroninę kortelę, visa informacija panaikinama ir lieka tik programinė įranga, neleidžianti patekti į VPN.

Apsaugos priemonių centralizuoto valdymo sistema

Šiuolaikinė verslo strategija pasižymi ne tik tuo, kad įsivyrauja elektroninė komercija (*e-commerce*), bet ir tuo, kad pradedama realizuoti elektroninio verslo (*e-business*) koncepcija. Tuo tikslu svarbiausia apjungti esamus ir tradicinius Interneto informacinius išteklius.

Šiems tikslams įgyvendinti naudojamos apsaugos priemonės pritaikytos naudoti šifravimo raktus (simetrinį ir asimetrinį). Kuo sudėtingesnė apsaugos sistema, kuo daugiau yra informacinės sistemos vartotojų, tuo sudėtingiau valdyti visus būtinus sistemos raktus, juos skirstyti ir atnaujinti.

Netgi tuomet, kai informacinės sistemos, turinčios visus pagrindinius apsaugos posistemės komponentus, vartotojų skaičius nėra didesnis kaip šimtas, realizuoti visas būtinas raktų valdymo operacijas be specialių programinių priemonių yra praktiškai neįmanoma. Be to, kai kurių šiuolaikinių informacinės apsaugos technologijų neįmanoma naudoti be visų būtinų raktų valdymo operacijų kompiuterinio palaikymo. Būtent todėl viena tinklų informacijos apsaugos problemų yra apsaugos priemonių valdymas, o būtent – generuojant, skirstant, atnaujinant raktus, o taip pat konfigūruojant apsaugos priemones.

VPN kompleksiniai produktai leidžia surasti veiksmingiausią sprendimą ir užtikrina:

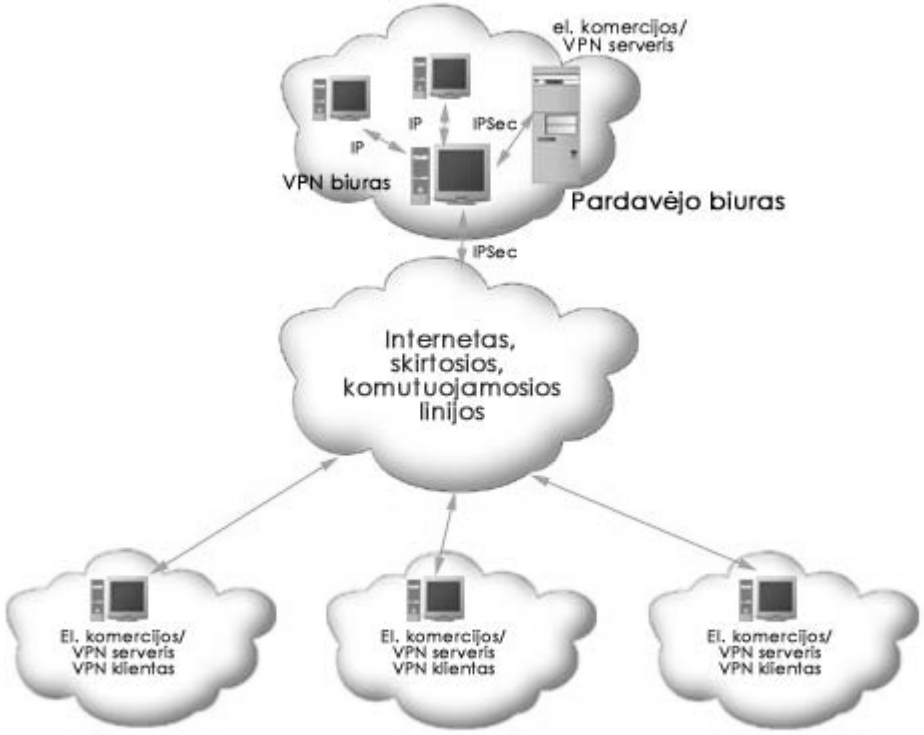
- vieningą apsaugotąją infrastruktūrą (apsaugą tinklo ir taikomajame lygmenyse, PKI, tapatybės patvirtinimą, protokolų sudarymo ir audito sistemą);
- vieningų apsaugos sprendimų sukūrimą visiems filialams, dukterinėms ir pavaldžioms kompanijoms;
- galimybę plėsti apsaugos infrastruktūrą.
- visos sistemos centralizuotą valdymą ir apsaugos strategijos nustatymą;

Elektroninei komercijai skirtas sprendimas „B2B”

Elektroninės komercijos tarp įmonių sistemos („B2B”) turi tokių savitumų:

- tam tikrą sistemos vartotojų skaičių (skirtingai nuo sistemos „B2C”);
- dideles užsakymų apimtis ir dėl to didelį jautrumą įsibrovimams ir ryšio patikimumui;
- didelę taikomųjų protokolų įvairovę (ne tik HTTP);
- padidintus apsaugos reikalavimus.

Šiuo metu kuriama ir diegiama daug įvairių komercijai skirtų sistemų. 4 paveiksle pavaizduota „B2B” tipo sistemos apsauga.



„*B2B* tipo sistemos apsauga“

Tarnybinei stočiai su bet kokio taikomosios sistemos „B2B” programine įranga apsaugoti įdiegiamas produktas “VPN-Server”, o klientui priklausančioje sistemos dalyje, kurią turi verslo partneris – “VPN-Client”. Produktas “VPN-Office” paslepia vidinio tinklo topologiją ir saugo jį nuo išorinių įsibrovimų iš Interneto bei neleistinos patekties.

Panaudojant kompleksinius VPN produktus galima sudaryti viso tinklo apsaugos sistemą ir tai aiškiai parodo jų privalumą prieš specializuotus VPN produktus, kurie saugo atskirų klasių taikomąsias programas.

Štai kai kuriuose žinomuose programiniuose produktuose tapatybei patvirtinti ir duomenų srautams apsaugoti naudojamas protokolas SSL (*Secure Socket Layer*), kurio trūkumas tas, jog jis “prisiriša” prie tam tikros rūšies taikomųjų programų ir todėl neatitinka įvairių reikalavimų apsaugos sistemoms, kuriuos kelia stambios korporacijos ir interneto tiekėjai.

Jei informacinę sistemą saugo atskiros informacijos apsaugos priemonės (šifravimas, elektroninis skaitmeninis parašas), tai VPN vis tiek reikalingas, kadangi tik jis apsaugos sistemą nuo įsibrovimų iš tinklo, pavyzdžiui, DoS. Vien tik SSL paremta sistema neapsaugos taip visapusiškai, kaip VPN produktai. VPN leis į tinklą tik tuos paketus, kurie nurodyti sistemai leistinuose pažymėjimuose.

Reiktų pažymėti dar vieną labai svarbią elektroninės sistemos “B2B” savybę – išvystytas vartotojų tapatybės patvirtinimo priemones:

- panaudojant slaptažodį;
- panaudojant įrenginius SecurID;
- panaudojant elektronines korteles, elektroninių leksemų įrenginius, palaikančius standartinę sąsają PKCS Nr.11.
- Neįvedus slaptažodžio arba nepateikus išorinės laikmenos (elektroninės leksemos), patvirtinančių prieigos teisę, negalima gauti jokios informacijos, išskyrus prieinamą visiems vartotojams.

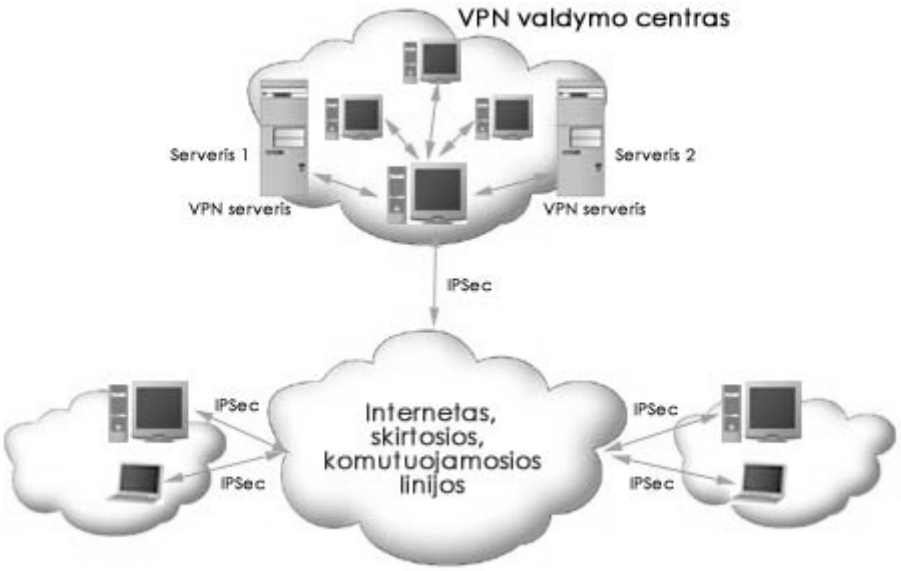
Informacinių paslaugų tiekėjams skirtas sprendimas

Sparčiai besiplečianti komunikacijų rinka suteikia naujų galimybių ir paslaugų. Viena tokių paslaugų yra įvairių taikomųjų programų nuoma, dėl kurios vartotojams nebereikia išleisti daug pinigų brangiai programinei įrangai, papildomai įrangai jų ir techniniam palaikymui įsigyti.

Kreipimasis į programas tiesioginio operatyvaus ryšio su programinių paslaugų tiekėjais (ASP) kanalais labai patrauklu, tačiau yra ir tam tikrų sunkumų. Svarbiausias jų – būtina užtikrinti pakankamą kiekvieno kliento informacijos apsaugos lygį, be to sistema turi būti atspari bandymams įsiterpti iš išorės.

Šiuos sunkumus taip pat galima nugalėti panaudojant VPN programinius produktus, kurie apsaugo nuo įvairiausių įsibrovimų iš tinklo ir leidžia tiekėjams teikti aukštos klasės paslaugas.

Kiekvieno kliento darbo vietai apsaugoti įdiegiamas produktas “VPN-Client”, pagrindinėms ir atsarginėms tarnybinėms stotims – “VPN-Server”; nuosavame vidiniame tinkle kompanija tiekėja gali naudoti produktą “VPN-Office”.



„Patikimą klientų sistemų atskyrimą”

5 paveiksle pavaizduotas sprendimas užtikrina patikimą klientų sistemų atskyrimą, t.y. A kliento sistema (taikomoji programa, informacija, vartotojai) apsaugotųjų ryšių būdu yra izoliuota nuo B kliento sistemos.

Kiekviena konkretaus „Kliento“ vartotojų grupė yra apibrėžta jų viešųjų pažymėjimų sąraše ir pavadinta „Kliento Nr. n vartotojai“. Analogiškai ir kiekviena pagrindinės bei atsarginės tarnybinių stočių taikomųjų programų pora konkrečiam klientui apibrėžiama jų viešaisiais pažymėjimais ir IP adresais – „Taikomųjų programų Nr. n tarnybinė stotis“.

Tokiu būdu susidaro, pavyzdžiui, 30 objektų: “Kliento Nr. 1 vartotojai”, ..., “Kliento Nr. 30 vartotojai”, taip pat 30 juos atitinkančių objektų: “Taikomųjų programų Nr. 1 tarnybinė stotis”, ..., “Taikomųjų programų Nr. 30 tarnybinė stotis”. Sistemos apsaugos strategiją apibrėžia taisyklių rinkinys. Apsaugos administratoriui nereikia jos nustatyti kiekvienam atskiram sistemos elementui – užtenka nustatyti bendrą verslo objektų rinkiniui “Kliento Nr. n vartotojas” ir “Taikomųjų programų Nr. n tarnybinė stotis” skirtą strategiją.

Kiti sprendimo ypatumai: pasinaudodama juo kompanija tiekėja gali sudaryti savo korporaciniams vartotojams keliaujančiųjų vartotojų skaidraus palaikymo galimybę nesumažinant apsaugos bei paslaugos lygio ir nepriklausomai nuo jų geografinės padėties.

Sprendimo veiksmingumas, išplečiamumas ir patikimumas leidžia kompanijai tiekėjai palaikyti greitai auganti klientų kontingentą turint nedidelį administruojantįjį personalą.