KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Tadas Kiškis

Privatumo ir saugos lygio vertinimo interneto svetainėse metodo parengimas ir taikymas

Magistro darbas

Darbo vadovas
dr. Alfredas Otas

Kaunas, 2012

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Tadas Kiškis

Privatumo ir saugos lygio vertinimo interneto svetainėse metodo parengimas ir taikymas

Magistro darbas

Recenzentas
dr. Renata Danielienė
2012–05–

Darbo vadovas
dr. Alfredas Otas
2012–05–

Atliko
IFN–0/3 gr. stud.
Tadas Kiškis
2012–05–

Kaunas, 2012

TURINYS

Privacy and Security Level Evaluation Method for Web Site Design and Application

SUMMARY

There is a number of ways to ensure privacy and security within an electronic environment: antivirus programs, firewalls, content search systems etc. Each Web browser has its own additional security safeguards (for XXS, *ActiveX* and others) using virus browsers databases. However when using social engineering attacking principles, viruses codes are able to pass by or eliminate such security measures which are being unintentionally and unknowingly installed by an IT user. In resolving common internet user problems, a number of challenges arise. For an example, one person or one user computer is not able to analyse large data packages (such as read all systems used by a private user). For more complex tasks (e.g. with larger data quantities) supercomputers and distributed systems are used (such as GRID which allows federation of computer resources from multiple administrative domains to reach common goal and that allows to process large projects for which local resources are not enough). From information security perspective security mainly depends on each user and their interaction between them. Therefore, the aim of Masters of Information Security Theses, based on the above statements, is to propose a method and an application for a privacy and security of internet browsers setup.

Created privacy and security level assessment for web servers is based on *Java* programming language which runs on the server that connects client–side *Java* based browser. It is also based on: system users and websites Database, and experts, administrators control website.

For the purpose of created system use in various operating systems and internet browsers these technologies have been used: *MySQL* Database, *Java* programing language, Hyper Text Markup Language, *JavaScript*, Cascading Style Sheets.

The system is created using existing models: RSAC content classification system model, TCSEC criterions and Public Information Act; “Internet news portal ranking model”. Internet risks methodologies are used and users awareness development of risk assessment; trusted network creation terminologies are used.

Key words: website, privacy, security tools, knowledge sharing, rating system.

ĮVADAS

Naudojantis internetu susiduriama su asmens duomenų privatumą ir saugą galinčiomis pažeisti grėsmėmis, pradedant nuo nesaugių duomenų perdavimui naudojamų kanalų, saugaus informacijos perdavimo neužtikrinančių informacijos perdavimo protokolų, iki naudojimosi tinkamai saugumo ir privatumo politikos neapibrėžtų internetinių svetainių paslaugomis.

Privatumui ir saugai elektroninėje erdvėje užtikrinti naudojama daugybe priemonių: antivirusinės programos, ugniasienės, turinio parinkimo sistemos ir kt. Kiekviena naršyklė turi papildomas saugumo užtikrinimo priemones (apsaugai nuo XSS, *ActiveX* ir kitas), naudoja kenkėjiškų svetainių duomenų bazes. Tačiau yra kenkėjiški kodai, kurie sugeba „apeiti“ (ir) ar išjungti šias apsaugas, kai taikomi socialinės inžinerijos atakos principai, o nepatyręs IT vartotojas apgaulės būdu pats net nesuvokdamas įsidiegia kenkėjiškas programas. Sprendžiant žmogiškąsias problemas, su kuriomis susiduriame naudojantis internetu, iškyla daugybe sunkumų. Pavyzdžiui, išanalizuoti didelius kiekius duomenų (kaip antai perskaityti visas sistemų kuriomis naudojasi privatumo politikas) vienas žmogus, kaip ir vienas paprastas kompiuteris skirti tiek resursų nepajėgus. Sudėtingiems uždaviniams, (pvz. kai yra dideli kiekiai duomenų) spręsti naudojami superkompiuteriai ar paskirstytosios sistemos (pvz. GRID lokaliųjų skaičiavimų tinklų telkiniai – junginiai leidžia apjungti skaičiavimo resursus, o tai leidžia realizuoti didesnius projektus, kuriems nepakanka lokaliųjų resursų). Informacijos apsauga – žmonių problema, saugumas labiausiai priklauso nuo kiekvieno vartotojo ir jų bendradarbiavimo tarpusavyje.

Probleminė sritis. Rinkoje siūloma pakankamai daug apsaugos priemonių privatumui ir saugai užtikrinti, tačiau vartotojams dažnai trūksta patirties, ypač kai taikomi socialinės inžinerijos metodai juos apgauti, iškyla rizika atskleisti ar sugadinti saugomus asmens duomenis. Saugumo ekspertai, IT darbuotojai, IT mėgėjai ar kiti (dažniausiais jau nukentėję) vartotojai sugeba atpažinti žalingą turinį, bei įvertinti galimas grėsmes. Jaučiamas paprastų ir nesunkiai pritaikomų metodų trūkumas, siekiant užtikrinti įvairių lygių kompiuterių vartotojų veiklos elektroninėje erdvėje saugų ir patikimą darbą.

Žalingą, neteiktiną turinį platinančios interneto svetainės iškeliamos į įstatymiškai palankesnes valstybes, kuriose toks turinys nėra reglamentuotas. Nėra teisinių priemonių jas pašalinti. Tai kas vienose valstybėse traktuojama nusikalstama, neteiktina, kitose tai nereglamentuota ar leistina norma.

Darbo tikslas. Parengti priemones apsaugoti interneto svetainių vartotojus nuo socialinės inžinerijos ir duomenų gavybos atakų keliamų problemų: virusų, šnipinėjimo programų, o tuo pačiu duomenų naikinimo, duomenų vagysčių, privatumo pažeidimų, asmens duomenų ir slaptažodžių

gavybos. Prisidėti apsaugant nuo neteiktinos informacijos globaliame internete plitimo.

Uždaviniai. Suformuluoti naudojantis interneto svetainėmis iškylančių privatumo ir saugos problemų, socialinės inžinerijos ir duomenų gavybos atakų, sprendimo tikslus ir uždavinius. Atliki tam taikomų apsaugos metodų analizę, bei parinkti sprendimo kūrimo metodus ir priemones. Suformuluoti reikalavimus socialinės inžinerijos ir duomenų gavybos atakų problematikos sprendimui, bei parengti sprendimo modelį.

Modeliuojamos probleminės srities aprašymas. Privatumo ir saugos lygio vertinimo interneto svetainėje metodas, kuris padėtų vartotojui nustatyti saugias ir nesaugias interneto svetaines, suteiktų ekspertams galimybę pateikti savo rekomendacijas.

Norint apsaugoti vartotoją nuo internete tykančių grėsmių, reikia jį tinkamai, laiku ir patogiai informuoti apie tykantį pavojų nesaugiose (virusus, neteiktiną turinį platinančiose), nepatikimuose (apgaudinėjančiuose vartotoją) interneto svetainėse. Tai realizuoti galima su specializuotu įrankiu, kuris galėtų būti naudojamas kaip interneto naršyklės papildinys. Šis papildinys tikrintų atidaromas interneto svetaines: aptikęs neigiamai vertinama turinį apie tai informuotų vartotoją, aptikęs ypač grėsmingai vertinamą turinį blokuotų tą svetainę ir informuotų apie galimas pasekmes jei vartotojas norėtų nepaisyti šio draudimo. Kadangi paprastas interneto vartotojas nėra IT saugumo ekspertas, ir jis neturi reikiamos kompetencijos ištirti atsitiktines interneto svetaines, būtų galima teikti vartotojams galimybę vertinti svetaines: ar neapkrėtė jo kompiuterio parsisiųstos programos, ar nenaudojamos automatinės nukreipimo technologijos; ar interneto svetainėje naudojama privatumo politika ir kaip ją vertinti; kokie vartotojų atsiliepimai apie teikiamas (ar tariamai teikiamas) e. komercijos paslaugas; koks interneto svetainėje pateiktas turinys, ar platinama informacija ir teikiamos paslaugos neprieštarauja Lietuvos Respublikos teisės aktams.

Ekspertai galėtų nagrinėti ir analizuoti neigimai vartotojų vertinamas svetaines, teikti pastabas ar jose pateiktas turinys neprieštarauja LR teisinėms normoms, bei imtis kitų reikiamų priemonių.

Privatumo ir saugos lygio vertinimo interneto svetainėse sistema modeliuojama remiantis teiginiais:

1. E. Kazanavičiaus, A. Venčkausko, A. Liutkevičiaus, A. Vrubliausko, mokomojoje knygoje „Informacijos saugos vadyba“ pateiktu teiginiu: „Kompiuterių sujungimas į tinklą labai padidina riziką ir tinklo saugumas labiausiai priklauso nuo kiekvieno vartotojo ir jų bendradarbiavimo tarpusavyje“ [24];

2. Daugiamečio Bendrijos veiksmų plano dėl saugesnio naudojimosi internetu skatinimo kovojant su neteisėtu ir žalingu turiniu pasauliniuose tinkluose įgyvendinimo galutiniu įvertinimu: „Visos suinteresuotosios šalys pripažino, kad turinio žymėjimo ir vertinimo sistemos ir toliau lieka nepaprastai svarbi priemonė darant internetą saugesnį“ [13];

3. Jennifer Golbeck, Bijan Parsia, James Hendler (Merilando universitetas) darbe „Trust Networks on the Semantic Web“ pateiktu teiginiu jog programos su turinio reitingavimo priemonėmis leidžia vartotojui sukonfigūruoti, rodyti pasitikėjimo lygius arba bendruoju lygmeniu arba, atsižvelgiant į tam tikrą temą [21].

Sistemai realizuoti naudojama: RSAC turinio klasifikavimo modelio koncepcija, TCSEC kriterijais ir Lietuvos Respublikos visuomenės informavimo įstatymo pagrindais sukurta turinio klasifikavimo matrica, kuri panaudojama internetinių svetainių reitingavimui (4.2 skyrius); išskirta, „IT žinių portalo reitingavimo modeliu“ paremta, reitinguojamų elementų aibė (4.5 skyrius); susisteminta, remiantis turinio klasifikavimo matrica parengta, metodinė medžiaga apie grėsmes internete, bei grėsmių vertinimą vartotojų sąmoningumo ugdymui (1 priedas); naudojamos pasitikėjimo tinklo kūrimo sąvokos (4 skyrius).

Siekiant, kad sukurtąją sistemą būtų galima pritaikyti naudotis įvairiose operacinėse sistemose ir interneto naršyklėse naudotos šios kūrimo technologijos: *MySQL* duomenų bazės, *Java* programavimo kalba, hiperteksto ženklinimo kalba, *JavaScript*, pakopinių stilių aprašo kalba.

Sukurta privatumo ir saugos lygio vertinimo interneto svetainėse sistema sudaryta iš *Java* programavimo kalba realizuotos sistemos serverio, kuris sudaro ryšį tarp vartotojų klientinės prieigos įrankių (interneto naršyklės papildinio), taip pat iš sistemos naudotojų ir internetinių svetainių vertinimų duomenų bazės, bei iš ekspertams, valdytojams skirtos sistemos valdymo internetinės svetainės.

Darbo struktūra:

1. Pirmajame skyriuje atlikta asmens duomenų privatumą ir saugą, naudojantis internetu, galinčių pažeisti technologijų analizė. Apžvelgiamos už internetinių incidentų tyrimą ir visuomenės informavimą atsakingų institucijų funkcijos, esami ir siūlomi saugumo internete užtikrinimo metodai, rekomendacijos, bei pagrindinės iniciatyvos. Nagrinėjamos taikomos apsaugos nuo kenkėjiškų ir sukčiavimo svetainių priemonės naršyklėse, esami turinio filtravimo ir vertinimo metodai, sprendimai.

2. Antrajame skyriuje, remiantis sistemų modeliais, projektuojamas privatumo ir saugos lygio vertinimo interneto svetainėse metodas. Analizuojamos projektuojamai sistemai reikalingos

priemonės. Įsivardinami projektuojamos sistemos funkciniai ir nefunkciniai reikalavimai. Atliekamas informacinės posistemės projektavimas.

3. Trečiajame skyriuje atliekama eksperimentinės privatumo ir saugos lygio vertinimo sistemos analizė. Pateikiamas veikimo aprašymas, kontrolinis pavyzdys.

4. Ketvirtajame skyriuje pateikiamas privatumo ir saugos lygio vertinimo interneto svetainėse sistemos įvertinimas, palyginimas su esamais taikomais metodais ir sistemomis. Pateikiamos taikymo rekomendacijos, tyrimo išvados.

I. PRIVATUMO IR SAUGOS INTERNETE ANALIZĖ

1. Privatumo ir saugos internete problematikos analizė

1.1. Tiriamoji problema, objektas, sritis

Naudojantis internetu galima susidurti su daugybe asmens duomenų privatumą ir saugą pažeidžiančių priemonių, pradedant nuo nesaugių duomenų perdavimui naudojamų kanalų, informacijos perdavimo protokolų, iki naudojimosi tinkamai saugumo politikos neapibrėžtų internetinių svetainių paslaugomis. Saugumo supratimas nuolat kinta šiandieniame informacinių technologijų pasaulyje. Saugumo politika turėtų apimti organizacines bei technines apsaugos priemones ir turėtų būti nuolatos tikslinama [1].

Naujos komunikavimo galimybės vis labiau domina įvairiausius informacijos vartotojus. Valstybės, savivaldos institucijos, verslo įmonės bei pavieniai asmenys, teikdami informacines paslaugas, naudodami interneto svetaines, siųsdami ir gaudami elektroninius laiškus, įgyvendindami elektroninius atsiskaitymus, vykdydami įvairias marketingines akcijas naudoja (renka, kaupia, apdoroja ir platina) informaciją, tame tarpe ir duomenis apie fizinius bei juridinius asmenis. Šalies informacinių sistemų duomenų bazėse yra kaupiami dideli kiekiai informacijos, kurioje gana žymią dalį sudaro asmens duomenys. Internete platinama reklaminė informacija, siūloma užpildyti įvairias anketas, siūlomos paslaugos ar prekės. Šioje aplinkoje egzistuoja ir toliau tobulinamos naujos efektyvios techninės galimybės automatizuotam informacijos rinkimui, įgalinančios informaciją, keliaujančią interneto kanalais surasti, perskaityti, pakeisti, redaguoti ar sunaikinti. Atsiranda reali galimybė informacinių sistemų duomenų bazėse sukaupti didelius kiekius informacijos apie tai neinformuojant informacijos savininko. Tokiu būdu, dirbdami internete mes ne tik gauname, perduodame informaciją, bet taip pat sudarome tam tikrą realią grėsmę nesankcionuotai gauti ir vartoti mūsų asmeninius duomenis, privačią informaciją, juos analizuoti, grupuoti, sistematizuoti [2].

Interneto suformuotoje virtualioje aplinkoje yra aptinkami bene visi realaus socialinio gyvenimo atributai, tame tarpe ir nusikaltimai. Privačios informacijos ir asmens duomenų išgavimo galimybėmis internete vis labiau domisi ir nusikalstamo pasaulio atstovai. Nusikaltimai, kurie yra atliekamai skaitmeninių technologijų pagalba nėra visiškai nauja nusikalstama veika. Tai tradiciniai nusikaltimai – vagystės, terorizmas, šantažas, asmens teisių pažeidimai ir t.t., kurie informacinių technologijų įtakoje įgavo naują formą. Nors tokiems nusikaltimams atlikti reikia naujų įgūdžių, žinojimo ir įrankių, bet šiuo metu tai nėra problema, nes šią nusikaltimams atlikti reikiama

informaciją ir įrankius galima lengvai rasti internete, ji tapo lengvai prieinama kone kiekvienam individui. Interneto svetainėse apstu pradedantiesiems, potencialiems įstatymų pažeidėjams, detalizuotos medžiagos, kurioje išsamiai išdėstyti algoritmai, kurių procese pralaužiami programų, svetainių ar asmeninių kompiuterių bei skaitmeninių dokumentų kodai. Nusikaltimai, susiję su informacinėmis technologijomis, gali būti susiję su pardavimais internete, bankų sąskaitos pasisavinimu, grasinimu ir šantažu asmenims elektroniniu paštu, didelių sumų pervesti į nurodytas sąskaitas viliojimu, neleistino turinio teksto ar grafikos platinamu, piratavimu bei autorinių teisių pažeidimu ir kitų nusikaltimų, kuriems atlikti internetas yra pagrindinė priemonė [3, 4].

1.2. Tyrimo tikslas ir uždaviniai

Tyrimo tikslas – didinti internetu besinaudojančios visuomenės informuotumą apie asmens duomenų, privačios informacijos rinkimo, saugojimo technologijas, renkamos informacijos panaudojimo galimybes, bei neteisėtą veiklą internete, siekiant padidinti interneto vartotojų supratimą apie grėsmes ir rizikas, saugant bei perduodant internetu privačią informaciją ir asmens duomenis. Įtraukti visuomenę į privataus gyvenimo neliečiamumo ir asmens duomenų apsaugos klausimų internete išsiaiškinimą bei galimų problemos sprendimų aptarimą [1, 2].

Tyrimo uždaviniai – išanalizuoti populiariausias asmens duomenų rinkimo, perdavimo, bei nesankcionuoto panaudojimo problemas internete. Išsiaiškinti už duomenų, informacijos kontrolę, nusikaltimų elektroninėje erdvėje tyrimą atsakingas institucijas, bei aptarti jų veiklą. Pateikti išvadas ir pasiūlymus.

1.3. Asmens duomenų privatumą ir saugą galinčių pažeisti technologijų analizė

Naudojantis internetu, ieškoma reikiamos informacijos, programinės įrangos, muzikos ir kitokio turinio. Naudojamasi elektroniniu paštu, elektroninėmis parduotuvėmis, internetinėmis bankų paslaugomis, bei daugybe kitų elektroninių priemonių sutinkamų interneto erdvėje. Tačiau ne visada susimąstoma apie tykančius internete pavojus: asmens duomenų rinkimą registruojantis įvairiose internetinėse svetainėse, virusus, bei paslaugų teikėjų, naudojamų parsisiųstų programų patikimumą privatumo ir saugos atžvilgiu.

Socialinės inžinerijos ir duomenų gavybos atakos

Apsaugos priemonės neapsiriboja vien tik antivirusinės programinės įrangos naudojimu ar stiprių slaptažodžių parinkimu. Informacijos apsauga apima daugumą kompiuterių ir fizinės saugos temų, socialinės inžinerijos atakas ir privatumo klausimus. Socialinės inžinerijos ir duomenų gavybos atakos yra aktuali problematika naudojantis informacinėmis technologijomis. Tokio

pobūdžio atakose skatinamos teigiamos ar neigiamas emocijos siekiant išgauti duomenys ar kad būtų atliktas tam tikras veiksmas (pvz. apkrėstas virusais kompiuteris, spustelint elementą internetinėje svetainėje). Socialinės inžinerijos ir duomenų gavybos atakos yra vienas iš nusikaltėlių įrankių, kadangi socialinės inžinerijos naudojimas turi finansinę motyvaciją. Pavyzdžiui apkrėsti kompiuterius *botnet* virusais, vėliau pagal užsakymą vykdyti atkirtimo nuo paslaugos atakas (angl. *Denial of Service*, DoS), ar paskirstytas (angl. *Distributed Denial of Service*, DDoS) atakas, kai sistemą – auką puola daug kompiuterių. Taip pat išgauti iš aukos privačia informaciją ir ją pateikti suinteresuotiesiems. Tad socialinės inžinerijos taikymo sritys: įvairaus tipo kritinių duomenų vagystės, pramoninis šnipinėjimas, finansinės machinacijos, sukčiavimas, šantažas, informacijos rinkimas [5, 6, 7, 8].

Naršymas internete

Beveik visos naršyklės kaupia ir gali atskleisti vartotojų apsilankymų interneto svetainėse istoriją. Didžioji dalis interneto naudotojų nėra apsaugoti nuo atakų, galinčių pasisavinti iš jų naršyklių informaciją apie aplankytus tinklapius [9].

Dauguma interneto naudotojų naršo internete naudodami paieškos sistemas. Paieškos sistemos turi ir naudoja gebėjimą sekti ir kaupti duomenis apie kiekvieną paiešką. Pavyzdžiui naudojantis paieškos sistemomis, serverio žurnaluose gali būti kaupiama informacija apie vartotojo užklausas, sąveiką su paslauga, interneto protokolo tipą, naršyklės tipą, naršyklės kalbą, užklausos datą ir laiką bei vieną ar daugiau slapukų, kurie gali unikaliai atpažinti vartotojo interneto naršyklę ar naudojama paskyrą. O kartu, naudojant vietos nustatymo paslaugas (pavyzdžiui žemėlapius), šias paslaugas teikiančios kompanijos gali gauti informacijos apie vartotojo faktinę vietovę (pvz., mobiliojo įrenginio siunčiamus GPS signalus), kurioje jis yra, arba informaciją, kuri gali būti naudojama tai vietovei apytiksliai nustatyti (pavyzdžiui telefono stoties ID)[10]. Kokie duomenys renkami ir kaip jie naudojami apibrėžiama paslaugos teikėjo privatumo politikoje.

E. komercija

Per internetą, firmos gali susisiekti su klientais. Internetas leidžia firmoms identifikuoti, rinkti duomenys ir sužinoti kliento įpročius, kad galėtų pasiūlyti patraukliausius pasiūlymus. Perkant iš neaiškių internetinių parduotuvių iškyla pavojus, netik prarasti pinigus ir negauti prekių, bet ir atskleisti asmens duomenis [6].

Kompanijos užsiimančios elgesio rinkodara, kaip įprasta kontroliuoja vartotojų atliekamas paieškas internete. Interneto svetaines, kurias lanko vartotojai, turinį, kurį jie žiūrį, jų sąveikas su socialinių tinklo svetainėmis, sąveikas su jų elektroninio pašto turiniu, bei produktais ir paslaugomis, kurias jie perka. Toliau, kai vartotojai naudoja mobilius prietaisus, net jų fizinė vieta

gali būti fiksuojama, o surinkti duomenys gali būti analizuojami ir apjungiami su informacija iš autonominių šaltinių, kad sukurtų dar išsamesnius vartotojų profilius [4].

Paslaugas internetu teikiantis bankai naudoja slaptažodžius ir užšifravimo sistemas, kad apsaugotų vartotojo registracijos vardą ir kitą informaciją. Tačiau ir Lietuvoje yra fiksuojami atvejai, kai sukčiai per kenkėjiškas programas bando išvilioti prisijungimo kodus ir slaptažodžius. Šios programos nukreipia į suklastotą internetinio banko svetainę, kuri iš pirmo žvilgsnio niekuo nesiskiria nuo tikrosios. Antivirusinės programos ir ugniasienės neužtikrina šimtaprocentinės apsaugos nuo šios kenkėjiškos programos, kurią lengvai galima apkrėsti kompiuterį atidarant bylas atsisiųstas iš neaiškių interneto svetainių [6].

Nusikalstama veikla ir žalingos programos

Internetiniai nusikaltėliai gali išgauti vartotojų informaciją internete įvairiausiais būdais, apkrėsti vartotojų kompiuterius virusais, Trojos arkliais ir t.t. Piktavaliai hakeriai gali užgrobti kompiuterius ir iš jų sudaryti kompiuterių tinklus – *botnetus*. *Botnetai* yra populiarūs tarp internetinių nusikaltėlių, nes juos galima panaudoti daugybei nusikalstamų reikmių. Apkrėsti kompiuteriai – *botai* gali būti panaudoti siuntinėjant nepageidaujamas laiškus (angl. *SPAM*) ar siuntinėjant el. laiškus vagiančius asmeninę informaciją. *Botnet* tinklai naudojami organizuojant paslaugu blokavimo (angl. *Denial of Service*) atakas, kuriose dalyvauja tūkstančiai pavergtų kompiuterių. Tokios atakos paprastai yra gerai valdomos – jos gali būti paleidžiamos staiga, bei greitai nutraukiamos. Taip pat šie *botnet* kompiuteriai gali tapti naujo viruso proveržio šaltiniu ar būti nutolusia nelegalios informacijos saugykla. Nepageidaujamų laiškų platintojai, duomenų vagių gaujos ir kiti internetiniai nusikaltėliai dažnai išsinuomoja *botnetus* ir naudoja savo reikmėms. Dažniausiai, perėmus kompiuterio valdymą, būna įdiegiama klaviatūros paspaudimus fiksuojanti programa, kuri renka informaciją apie tikrojo kompiuterio savininko veiksmus, pavyzdžiui internetinės bankininkystės naudotojo duomenis ir persiunčianti juos *botneto* savininkui [6, 7, 8].

Nepageidaujamo pobūdžio žinutės (angl. *SPAM*) – tai dideliais kiekiais siunčiamos elektroninio pašto žinutės be gavėjų sutikimo. Nepageidaujamos žinutės dažniausiai yra naudojamos komerciniais ir reklamos tikslais: bandoma įsiūlyti vaistų, programinės įrangos ir kitokių prekių arba paslaugų. Viena kita per dieną gauta žinutė kompiuterių vartotojams gali sukelti susierzinimą, tačiau gaunant nepageidaujamas žinutes dideliais kiekiais, yra veltui eikvojamas vartotojų laikas, apkraunamos dideliais duomenų srautais informacijos perdavimo kanalai, bei jos apdorojimo įranga. Kartu su nepageidaujamomis žinutėmis į kompiuterį gali atkeliauti ir virusai, kirminai arba Trojos arkliai. Dažniausiai tokių virusų taikinys yra kompiuteryje saugomi elektroninio pašto adresai, į kuriuos būtų galima persiųsti nepageidaujamas žinutes. Kartais virusais

yra siekiama perimti kompiuterio valdymą ir iš jo persiųsti didelius kiekius nepageidaujamų žinučių. Kai kuriomis masiškai platinamomis žinutėmis yra bandoma apgaulės būdu sužinoti vartotojų vardus, kodus ir slaptažodžius. Tai – vadinamoji „žvejybos“ ataka (angl. *phishing*). Pavyzdžiui, atsiųstoje žinutėje yra nurodoma, kad dėl daromų pakeitimų elektroninės bankininkystės sistemoje reikia pakartotinai pateikti savo duomenis: vartotojo vardą ir slaptažodį. Vartotojui yra siūloma spustelėti ant nuorodos į banko tinklalapį. Tačiau iš tikrųjų vartotojas yra perkeliamas į apgaulingą tinklalapį, kuris tik vizualiai yra panašus į banko. Tokiame tinklalapyje įvesti tikrieji kodai ir slaptažodžiai patenka į rankas nusikaltėliams, pasinaudodami šia informacija nusikaltėliai gali ištuštinti banko sąskaitą, ar net paimti paskolą šia informaciją atskleidusio vartotojo vardu [6, 7, 8].

Yra daugybe žalingų programų kompiuteriniai virusai, kirminai, Trojos arkliai ir kt., kuriomis dažniausiai kompiuteriai apkrečiami naudojantis internetu. Tai programos, kurios gali sugadinti kompiuterį ir jame laikomus duomenis, sulėtinti kompiuterio darbą, bei interneto ryšį. Šiomis žalingomis programomis apsikrėtęs kompiuteris tampa pavojingas bendradarbių, draugų kompiuteriams ir visiems kitiems interneto vartotojams [6, 8]. Dažniausiai vartotojai susiduria su virusais[7].

Yra daugybė kompiuterinių virusų atmainų. Bendru atveju tai yra kompiuterinio kodo dalis prisijungianti prie failo ar programos, tam kad galėtų platinti save kompiuterių tinklu kartu su siunčiamais duomenimis. Virusai gali padaryti įvairios žalos, kaip antai: sugadinti programinę įrangą, saugomus failus, ar net techninę įrangą [25]. Virusai skirstomi į tam tikrus tipus.

Kirminai yra virusų, kurie patys sugeba daugintis, atmaina. Didžiausias jų keliamas pavojus yra sugebėjimas daugintis dideliais kiekiais. Įprastam virusui reikalingas įsiskverbimas į kitas bylas, tuo tarpu kirminas gali daugintis nesustodamas tol, kol išnaudos kompiuterio duomenų talpą arba išplis po visą tinklą ir sutrikdys jo darbą. Kirminas dažniausiai plinta be vartotojo veiksmų ir platina savo kopijas po tinklus. Kadangi kirminams nereikalinga programa ar failas, prie kurio jie turėtų prisikabinti, jie gali sukurti tunelį į aukos kompiuterį ir leisti kažkam kitam valdyti jį nuotoliniu būdu. Pavyzdžiui, kirminas „MyDoom“ buvo sukurtas suteikti prieigą prie užkrėstų sistemų ir per šias sistemas pulti interneto svetainių serverius. Ne mažiau pavojinga ir viruso atmaina Trojos arklys [6, 7, 8].

Trojos arkliai – kompiuterinės programos, besislepiančios kitose programose ir išoriškai atrodančios kaip naudingos, tačiau realiai sukeliančios kenksmingus padarinius. Gana dažnai Trojos arkliai apsimeta kaip kompiuterio darbą gerinančios programos, ar netgi antivirusinėmis programomis. Tačiau Trojos arklys perleidžia kompiuterio kontrolę nepageidaujamiems asmenimis.

Skirtingai nuo kirminų, Trojos arklys negamina savo kopijų, bet aktyvavus programą, už kurios jie slepiasi, kartu aktyvuojamas ir virusas. Veikiantis Trojos arklys ypatingai pavojingas, nes sudaro virtualų koridorių, per kurį užkrėstasis kompiuteris ir jo resursai tampa prieinami iš išorės įsibrovėliams, kurie naudojasi aukos duomenimis, vagia informaciją ir keičia sistemos parametrus [6, 7, 8].

Yra unikalių virusių kurie gali plisti ne vien internetu — tai HOAX virusai – laiškai siunčiami kaip įprastas elektroninis laiškas. Tokiame laiške dažniausiai nėra jokios žalingos programos (viruso), kuri galėtų užkrėsti vartotojo kompiuterį, tačiau jame yra išgalvoto viruso ar kitokio pavojaus aprašas, kurio tikslas yra įteigti laiško gavėjui šią žinią persiųsti toliau. Kitu atveju dažniausiai, bandoma manipuliuoti žmonių jausmais, kai prašoma padėti sunkiai sergančiam žmogui, ko pasekoje už neva persiųstus laiškus bus surinkta kažkokia suma pinigų. Tokie apgaulingi virusai – laiškai plinta, naudodamiesi žmonių patiklumu, žaisdami jų jausmais. Jų platintojais tampa patys vartotojai. Paprastai visa jų kenkėjiška veikla yra nukreipta į pašto serverių apkrovimą. Tokie virusai neplinta patys ir neapkrauna serverių jie įtikina tai padaryti patį vartotoją [6, 8].

Tad dažniausiai žalingos kompiuteriui ir vartotojo privatumui keliančios grėsmę programos plinta per internetą, apgaudinėjant interneto vartotojus, atidarinėjant jiems virusais apkrėstas bylas ar specialiai tam suformuotas interneto svetaines, parsisiunčiant tariamai naudingas funkcijas atliekančias programas, taip pat per elektrinius laiškus. Saugumo ekspertai, IT darbuotojai sugeba atpažinti žalinga turinį, bei įvertinti galimas grėsmes, bet paprastiems kompiuterių vartotojams tam trūksta žinių ir informacijos „čia ir dabar“.

1.4. Internetinių incidentų tyrimas ir visuomenės informavimas

Lietuvoje yra keletas institucijų, atsakingų už informacijos apsaugą [6]:

- Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos;
- Valstybinė duomenų apsaugos inspekcija;
- Ryšių reguliavimo tarnyba;
- Vidaus reikalų ministerija;
- Valstybės saugumo departamentas.

Vienos institucijos yra atsakingos už informacijos apsaugą tik valstybiniame sektoriuje, kitų veikla apima informacijos apsaugą tiek valstybiniame, tiek privačiame sektoriuose. Dėl skirtingo informacijos pobūdžio skiriasi tokių institucijų užduotys, funkcijos ir atsakomybė [6].

Vienas pagrindinių Informacinės visuomenės plėtros komiteto (IVPK) prie Susisiekimo

ministerijos uždavinių – dalyvauti koordinuojant valstybės informacijos technologijų ir telekomunikacijų Lietuvos Respublikoje įgyvendinimą. Įgyvendindamas šį uždavinį, IVPK inicijuoja valstybės informacinių sistemų ir valstybės registrų kūrimo ir jų saugos užtikrinimo privalomųjų reikalavimų ir standartų rengimą. Vienas iš didesnių IVPK projektų yra elektroninio parašo diegimas Lietuvoje. IVPK formuoja ir įgyvendina elektroninio dokumento ir elektroninio parašo naudojimo politiką ir vykdo elektroninio parašo priežiūros institucijos funkcijas [6]..

Pagrindinis Valstybinės duomenų apsaugos inspekcijos uždavinys yra užtikrinti asmens duomenų apsaugą. Ši institucija atlieka šias funkcijas: tvarko asmens duomenų valdytojų valstybės registrą, viešai skelbia jo duomenis ir vykdo registruotų duomenų valdytojų veiklos, susijusios su asmens duomenų tvarkymu, priežiūrą; tikrina asmens duomenų tvarkymo teisėtumą ir priima sprendimus dėl asmens duomenų tvarkymo pažeidimų; teikia konsultacijas duomenų valdytojams, taip pat rengia metodines rekomendacijas dėl asmens duomenų apsaugos ir jas viešai skelbia internete; asmens duomenų teisinės apsaugos įstatymo nustatytais atvejais atlieka išankstinę patikrą ir teikia išvadas duomenų valdytojui apie numatomą duomenų tvarkymą; vertina duomenų valdytojų pateiktas asmens duomenų tvarkymo taisykles [6].

Ryšių reguliavimo tarnyba (RRT) siekia užtikrinti kiekvienam Lietuvos gyventojui technologiškai pažangių, kokybiškų, saugių ir įperkamų informacijos ir ryšių technologijų bei pašto paslaugų (produktų) pasirinkimo įvairovę, sudaryti galimybes informacijos ir ryšių technologijų bei pašto verslo plėtrai, taip spartinant informacinės ir žinių visuomenės plėtrą [6].

Vidaus reikalų ministerija (VRM) yra viena iš pagrindinių institucijų, užsiimančių informacinių sistemų apsauga valstybiniame sektoriuje. VRM, formuodama valstybės politiką informacinių technologijų saugos srityje, organizuoja, koordinuoja ir kontroliuoja jos įgyvendinimą.

Valstybės saugumo departamentas (VSD) be pagrindinių savo funkcijų – žvalgybos, kontržvalgybos ir kovos su terorizmu yra taip pat atsakingas už įslaptintos informacijos apsaugos kontrolę. Įtraukdamas ir kitas valstybines institucijas VSD rengia reikalavimus dėl valstybės ir tarnybos paslapčių, apdorojamų informacinėse sistemose, apsaugos [6].

Kai 1988 m., kai vienas pirmųjų „interneto kirminų“ apkeliavo visą pasaulinį interneto tinklą ir sutrikdė daugelio sistemų veiklą JAV Gynybos departamento Pažangių tyrimų projektų agentūra (angl. *Defence Advanced Research Projects Agency of the US Department of Defence*) sukūrė pirmąjį CERT (*angl. Computer Emergency Response Team*) IT saugumo incidentų tyrimo grupės modelį. Sukurtas CERT veiklos modelis buvo sėkminga idėja ir tapo svarbiausiu įrankiu vykdant IT saugumo incidentų valdymą elektroninių ryšių tinkluose. Šiuo metu pasaulyje egzistuoja keletas šimtų įvairaus dydžio valstybinių, komercinių bei akademinių CERT. 2005 m. kovo 24 d.

Lietuvos Respublikos Vyriausybės nutarimu dėl Lietuvos Respublikos Vyriausybės 2004 – 2008 m. programos įgyvendinimo priemonių patvirtinimo numatė įsteigti kompiuterinių incidentų tyrimo padalinį CERT Lietuvos Respublikos ryšių reguliavimo tarnyboje [7].

Lietuvoje veikiantis nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT–LT atlieka elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimus, veiksmų koordinavimą, sprendžia incidentus, rengia rekomendacijas apie grėsmes, organizuoja seminarus, skelbia incidentų statistiką [7].

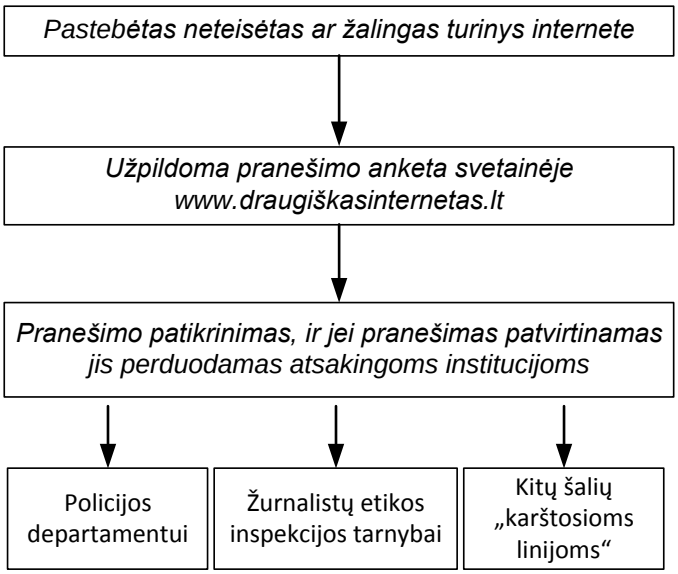
CERT–LT nagrinėja vartotojų pateiktus (elektroninių paštu ar interneto svetainėje https://www.cert.lt/pranesti.html užpildytus) pranešimus, atlieka tyrimus, kai yra įvykdyta ar vis dar vykdoma:

- Elektroninės paslaugos trikdymo ataka (angl.*DoS*);
- Neleidžiamasis prisijungimas – neteisėtas prisijungimas prie informacinės sistemos ar elektroninių ryšių tinkle;
- Neleidžiamasis naudojimasis informacinės sistemos ištekliais – neteisėtas informacinės sistemos išteklių naudojimas;
- Manipuliacija elektroniniais duomenimis – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.;
- Neteisėtas turinys – elektroniniai duomenys, kurių kūrimas, saugojimas ar platinimas yra draudžiamas pagal Lietuvos Respublikos įstatymus;
- Kenkėjiška programinė įranga (angl. *Virus, Worm, Spyware*);
- Nepageidaujamas elektroninis paštas (angl. *SPAM*);
- Elektroninių duomenų klastojimas – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.

CERT−LT nenagrinėja pranešimų apie žalingą turinį internete, tačiau apie šį turinį galima pranešti svetainėje www.draugiskasinternetas.lt.

Vadovaujantis Europos komisijos Informacinės visuomenės direktorato programa, Lietuvoje vykdomas projektas ,,Saugesnis Internetas LT AN–HL“. Jo pagrindiniai uždaviniai yra šie [15]:

- Visuomenės švietimas saugaus interneto klausimais (vykdo švietimo IT centras ir RRT);
- „Karštosios linijos“ funkcijų vykdymas (vykdo RRT). Jos veikimo schema pavaizduota 1 pav.



1 pav. „Karštosios linijos" veikimo schema [9]

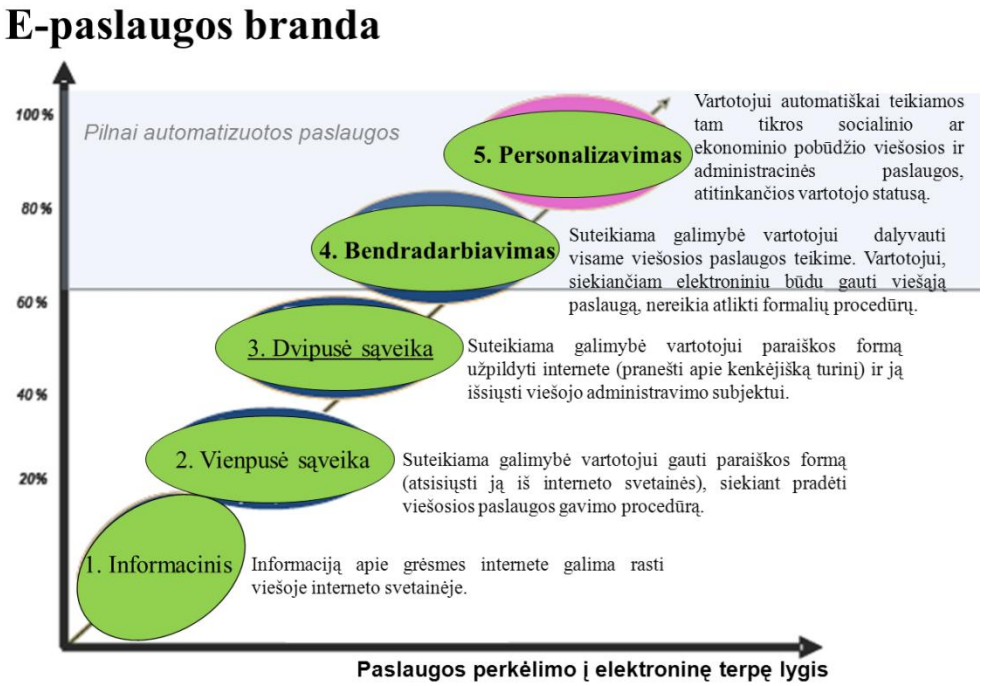
Interneto svetainėje http://www.draugiskasinternetas.lt/lt/misc/report_form bet kada galima pranešti apie pastebėtą neteisėtą ar žalingą informaciją internete (pedofiline, pornografine, rasinę ir tautinę nesantaiką kurstančią), kuri bus patikrinama ir perduodama atsakingoms institucijoms.

Šiuo metu 33 pasaulio šalyse veikia 38 „karštosios linijos“ (3 pav.), kurias jungia INHOPE asociacija http://www.inhope.org/. RRT „karštoji linija" buvo priimta į INHOPE 2008 m. gegužės 28–29 d. Dubline vykusioje šios asociacijos Generalinėje Asamblėjoje.

3 pav. Į INHOPE asociacija prisijungusių šalių žemėlapis [inhope.org, 2010 m.]

Visuomenei besinaudojančiai internetu sudaryta galimybė pranešti ir gauti atsakymą iš atsakingos institucijos apie pastebėta kenkėjiška turinį, tad pagal e. paslaugų brandos modulį [11] šioje sferoje yra pasiektas dvipusės sąveikos lygis (2 pav.). Tačiau norint judėti į prieki reikalinga

taikyti įnovatyvius bendradarbiavimo metodus užtikrinant netik vartotojas − už e. saugą atsakinga institucija ryšį, bet trišalius ryšius. Taip artėjant prie bendradarbiavimo ir personalizavimo paslaugų lygio.



2 pav. E. paslaugų brandos modulis

Lietuvoje vykdoma ECDL (Europos kompiuterio vartotojo pažymėjimo) programa. ECDL standarte remiamasi tuo, ką kompiuterio vartotojas turi žinoti apie informacijos technologijas ir asmeninius kompiuterius, bei kokius asmeninių kompiuterių ir populiariausios jų taikomosios programinės įrangos panaudojimo įgūdžius jis turi įgyti. Nuo 2009 metų partnerinės programos licencija patvirtintą ECDL fondo „e-Guardian“ programa, kurios naudojimo ir sklaidos teisės priklauso Lietuvos kompiuterininkų sąjungai (LIKS). Yra dvi šios programos versijos:

- „e-Guardian“ v.1 yra aukštesnio lygio ECDL sertifikavimo programa skirta asmenims, kurie nori apsaugoti vaikus nuo galimų pavojų internete ir informaciją nuo nepageidaujamos prieigos, t. y. tėvams, IT administratoriams vidurinėse ir aukštosiose mokyklose;

- „e-GUARDIAN“ v.2 saugos modulis skirtas visiems mokytojams (t y. ne tik IT mokytojams). Jis orientuotas į saugias informacines technologijas ir kibernetinių pavojų prevenciją [12].

1.5. Išvados

Internetas yra plačiai naudojamas tiek darbe, tiek namuose. Kiekviena kompiuterizuota darbo vieta, turinti interneto prieigą, gauna ne tik naudingą informaciją ir informacines paslaugas,

jai taip pat gręsią visi internete slypintys pavojai. Tarp tokių grėsmių gali būti kompiuteriniai virusai, interneto kirminai – piktavališkos programos, sugebančios save platinti. Dažnai virusai bei kirminai atlieka žalingus veiksmus: sunaikina informaciją, atlieka kompiuterines atakas prieš kitus kompiuterius, kompiuteriai ir tinklai patiria perkrovas. Taip pat iškyla pavojus prarasti informaciją. Įsilaužėliai, gavę nesankcionuotą priėjimą prie kompiuterio, gali sunaikinti arba pavogti (perimti) privačią, svarbią informaciją. Dažnai įsilaužėlių tikslas – perimti vartotojų slaptažodžius, banko (mokėjimo kortelių) informaciją, el. pašto adresus ir kt. Įsilaužėliai, perėmę kompiuterio valdymą, gali panaudoti jį kitokiems piktavališkiems tikslams, pavyzdžiui, kompiuteris gali būti paverstas naujų atakų vykdymo priemone, ištekliu ar tiesiog piratinės programinės įrangos saugykla.

Galima išvardinti tokias priežastis, dėl kurių pažeidžiami kompiuteriai: vartotojams dažnai trūksta žinių apie interneto pavojus (tokius vartotojus ypač lengva apgauti); kompiuteriai dažnai nėra pakankamai apsaugomi nuo interneto grėsmių; vartotojai nesinaudoja (galimai dėl žinių trūkumo) pigiomis ar nemokamomis programinėmis priemonėmis, skirtomis padidinti kompiuterio saugumą.

Lietuvoje veikia daug už informacijos apsaugą atsakingų institucijų, žinių apie jų rengiamas rekomendacijas platinimas nepasiekia dalies tikslinių grupių, trūksta informacijos į kuria instituciją kreiptis atsiradus tokiam poreikiui.

2. Esamų ir siūlomų saugumo internete metodų bei rekomendacijų apžvalga

2.1. Esamos rekomendacijos

Europos Bendrijų Komisijos veiksmų plano dėl saugesnio naudojimosi internetu skatinimo kovojant su neteisėtu ir žalingu turiniu pasauliniuose tinkluose įgyvendinimo galutinio įvertinimo išvadose skelbiama jog filtravimo technologijos visų suinteresuotųjų šalių laikomos esminiu elementu, kurio svarba vis didėja. Filtravimo technologijų srityje sektorius yra padaręs nemažą technologinę pažangą, ir galutiniams vartotojams dabar yra siūlomi įvairiausi sprendimai. Yra tokių filtravimo technologijų, kurias naudodami galutiniai vartotojai, ypač tėvai, gali panaikinti vaikams prieigą prie tinklalapių su žalingu turiniu. Tačiau tėvai vis dar per mažai žino apie tai, kaip naudotis filtravimo programine įranga vartotojo lygmeniu. Visos suinteresuotosios šalys pripažino, kad turinio žymėjimo ir vertinimo sistemos ir toliau lieka nepaprastai svarbi priemonė darant internetą saugesnį [13].

Manoma, jog asmens duomenų apsaugos problemos neįmanoma įveikti, jeigu su tuo

nesistengs kovoti patys žmonės. Įvairūs atlikti tyrimai rodo, kad didžioji visuomenės dalis labai mažai žino savo ir valstybės institucijų teises asmens duomenų tvarkymo srityje. Todėl labai svarbi yra švietėjiška veikla visuomenę informuojant apie jų asmens duomenų apsaugą ir teises šioje srityje [14].

2.2. Egzistuojančių metodų ir priemonių apžvalga

2.2.1. Pagrindinės iniciatyvos

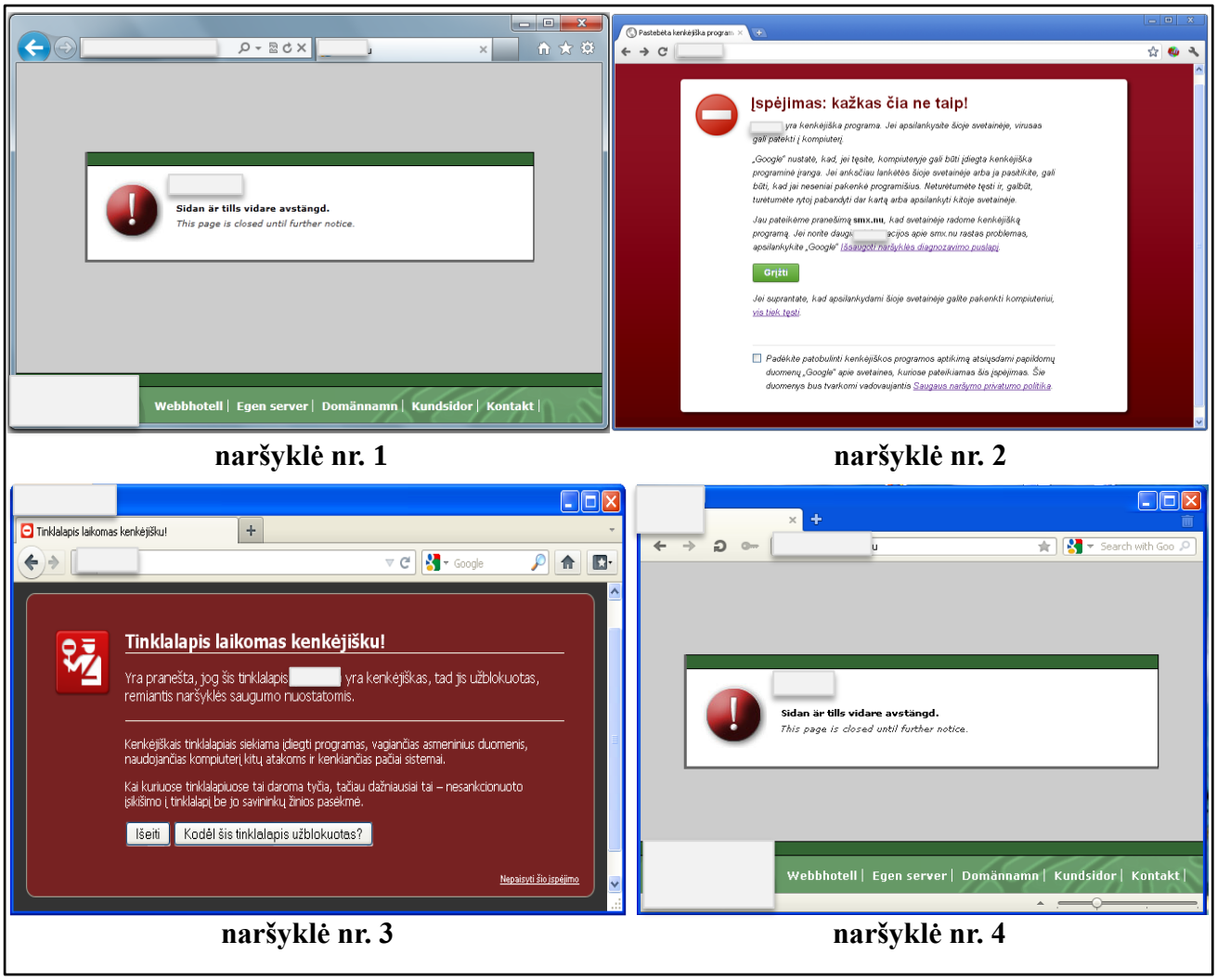
Insafe tinklas koordinuoja veiksmus, gerinančius informuotumą interneto saugumo klausimais Europoje, ir yra remiamas Europos Komisijos, bendradarbiaujant su nacionaliniais informacijos apie saugesnį internetą skleidimo taškais. *Insafe* siekia paremti ir paskatinti ne tik nacionalinių taškų, bet ir visų asmenų, organizacijų bei agentūrų, veikiančių Europoje ir už jos ribų, veiklą. Tikslas yra prisidėti prie informuotumo gerinimo ir sudaryti galimybę piliečiams veiksmingai bei etiškai naudotis naujomis informacijos ir ryšių technologijomis, tuo pat metu išryškinant su tuo susijusius pavojus ir užtikrinant teisę į privatumą bei saugumą.

Tarptautinė interneto „karštųjų linijų“ asociacija INHOPE atstovauja 34 šalių interneto „karštosioms linijoms“ įvairiuose pasaulio regionuose. Jų tikslas – priimti ir nagrinėti pranešimus apie neteisėtą ar žalingą turinį ir (arba) neteisėtą veiklą internete. LR ryšių reguliavimo tarnybos įsteigta interneto „karštoji linija“ yra INHOPE narė nuo 2008 metų [15].

W3C koordinuoja iniciatyvą, vadinamą interneto turinio parinkimo platforma (angl. *Platform for Internet Content Selection,* PICS) [16]. PICS tai iniciatyva, kurios tikslas sudaryti infrastruktūrą žymių suteikimui turiniui, tačiau ši iniciatyva yra neutrali tuo aspektu, kad ji nenurodo žymių turinio. Nurodomas tik žymės formatas ir aprašoma, kaip tam tikros žymės gali būti perduodamos. Tai yra platforma, kuria remiantis konstruojama programinė įranga, skirta turinio filtravimui bei turinio reitingavimui.

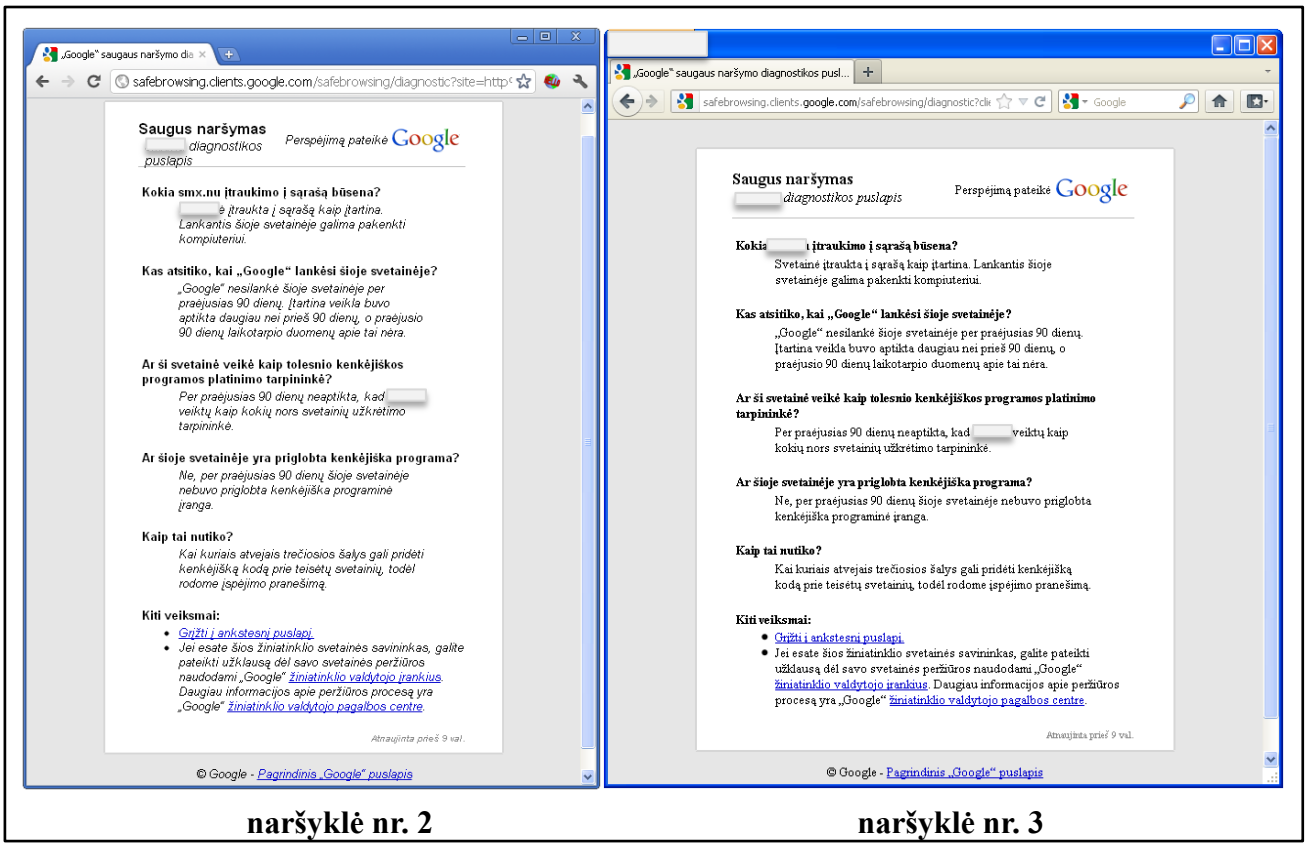
2.2.2. Apsauga nuo kenkėjiškų ir sukčiavimo svetainių naršyklėse

Apžvelkime kaip reaguoja keturios populiaresnės naršyklės į kenkėjiškas ir (ar) sukčiavimo svetaines. Atlikime pirmąjį testą panaudodami internetinio tinklapio adresą, kuris skelbiama jog yra laikomas kenkėjišku. Pastebime jog interneto naršyklės elgęsi skirtingai (4 pav.).



4 pav. Interneto naršyklių reakcija į kenkėjiška svetainę

Dvi bandytos naršyklės (44 pav**.** nr. 1, 4) tiesiog bandė atvaizduot internetine svetainę, tačiau ji jau buvo „uždaryta iki tolesnio pranešimo“ (angl. „*This page is closed until further notice.*“). Kitos dvi (44 pav**.** nr. 2 ir 3) naršyklės elgėsi panašiai. Pirmoji įspėjo jog „yra pranešta, jog šis tinklalapis [redacted] yra kenkėjiškas, tad jis užblokuotas, remiantis naršyklės saugumo nuostatomis. O antroji įspėjo jog „[redacted] yra kenkėjiška programa. Jei apsilankysite šioje svetainėje, virusas gali patekti į kompiuterį.“. Paspaudus nuorodas abejuose naršyklėse, kad būtų pateikta daugiau informacijos pastebime, jog „Perspėjimą pateikė Google“ (5 pav.). Jame sužinome, kad „Google nesilankė šioje svetainėje per praėjusias 90 dienų. Įtartina veikla buvo aptikta daugiau nei prieš 90 dienų, o praėjusio 90 dienų laikotarpio duomenų apie tai nėra.“.



naršyklė nr. 2 **naršyklė nr. 3**

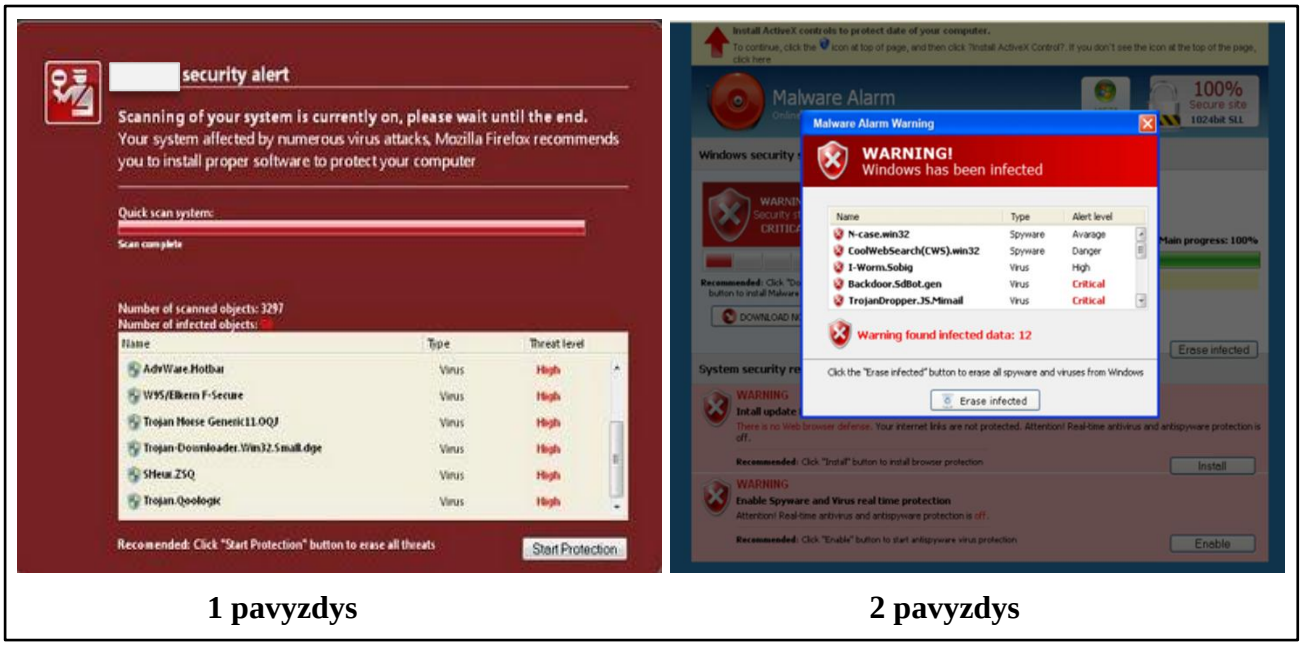
5 pav. Perspėjimo apie internetine svetainę aprašas

Be to buvo pastebėta, kad naršyklė nr. 3 naudoja „StopBadware“ teikiamomis paslaugomis. „StopBadware“ kompanijai galima pranešti apie kenkėjiškas internetines svetaines. Ši kompanija teigia, kad jos partneriai „Google“, „Mozilla“, „PayPal“ sistema, ir kt. [17].

Atlikus bandymą, atidarant internetine svetainę, kurioje įrašytas kenkėjiškas kodas (*Trojan:JS/Aseljo.K*) interneto naršyklės elgėsi skirtingai. Vienos naršyklės internetine svetainę atvaizdavo iškart, kitos parodė pranešimus apie galimas grėsmes. Tačiau visais šiais atvejais, naudota ta pati antivirusinė programa, aptiko kenkėjišką kodą.

Dar keli bandymai parodė tapačius rezultatus, tik naršyklės, kurios pirmame bandyme iškart atvaizdavo užklausta internetinę svetainę taip pat parodydavo pranešimus apie galimas grėsmes.

Kiekviena naršyklė turi papildomas saugumo užtikrinimo priemones (apsaugai nuo XSS, *ActiveX* ir kt.), kai kuriose naršyklėse jas reikia suaktyvinti. Tačiau yra kenkėjiški kodai, kurie sugeba „apeiti“ (ir) ar išjungti šias apsaugas. O kai taikomos socialinės inžinerijos atakos principai nepatyręs IT vartotojas apgaulės būdų pats net nesuvokdamas įsidiegia kenkėjiškas programas. Štai (6 pav.) keletas socialinės inžinerijos atakos pavyzdžių.



1 pavyzdys **2 pavyzdys**

6 pav. Socialinės inžinerijos atakų internetinių svetainių pavyzdžiai

Abejais šiais variantais buvo siūloma parsisiųsti tariamai naudingas funkcijas atliekančias („antivirusines“ ir pan.) programas – virusus. Taip gali būti apkrečiami kompiuteriai ir *Botnet* virusais. Atsiranda galimybė taikyti *Botnet* tinklus vykdant DoS ar DDoS atakas.

Naršyklių tyrimas nėra išsamus (naudotos dviejų versijų operacinės sistemos, bet vienos kompanijos ir viena antivirusinė programa tos pačios kompanijos), tačiau atskleidžia dalį veikimo principų. Iš analizės rezultatų galima teigti jog yra kaupiamos ir naudojamas kenkėjiškų svetainių duomenų bazės. Tuo įsitikiname ir susipažinę su vienos naršyklės gamintojo skelbiama privatumo politika „... siųs į „[redacted]“ tam tikrą informaciją, įskaitant puslapio URL, kad būtų papildomi sukčiavimo ir kenkėjiškų programų sąrašai“.

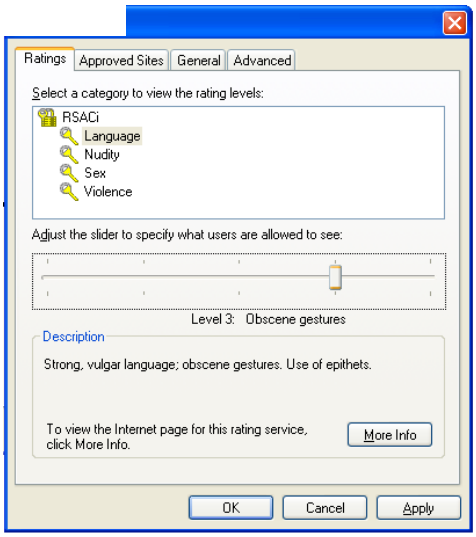
Vienos naršyklės gamintojas teigia: „[redacted]“ (operacinės sistemos) aplinkoje „[redacted]“ (naršyklė) tvarkingai integruojasi su Jūsų naudojama apsaugos nuo virusų programine įranga. Jums parsisiuntus failą, kompiuteryje esanti antivirusinė programa automatiškai patikrins, ar jame nėra virusų ar kitų kenksmingų programų.“ Galima pastebėti jog tai turi atgalinį ryšį ir apie aptiktą kenkėjišką kodą internetinės svetainės turinyje informuojami suinteresuoti, naršyklės gamintojo įvardytos institucijos (ir) ar asmenys.

2.2.3. Esami turinio vertinimo ir filtravimo sprendimai

Programos „turinio patarėjai“

Su interneto naršyklėmis veikiančios turinio valdymo priemonės gali valdyti turinio tipus, kuriuos interneto naršytojas gali pasiekti internete. Įjungus turinio patarėją, gali būti rodomas tik įvertintas turinys, kuris atitinka arba viršija kriterijus (pvz. 1 lent.). 7 pav. pateiktas turinio patarėjo

langas, kuriame galima keist informacijos filtravimo lygį.



7 pav. Turinio patarėjo programos langas informacijos filtravimo lygiui nustatyti

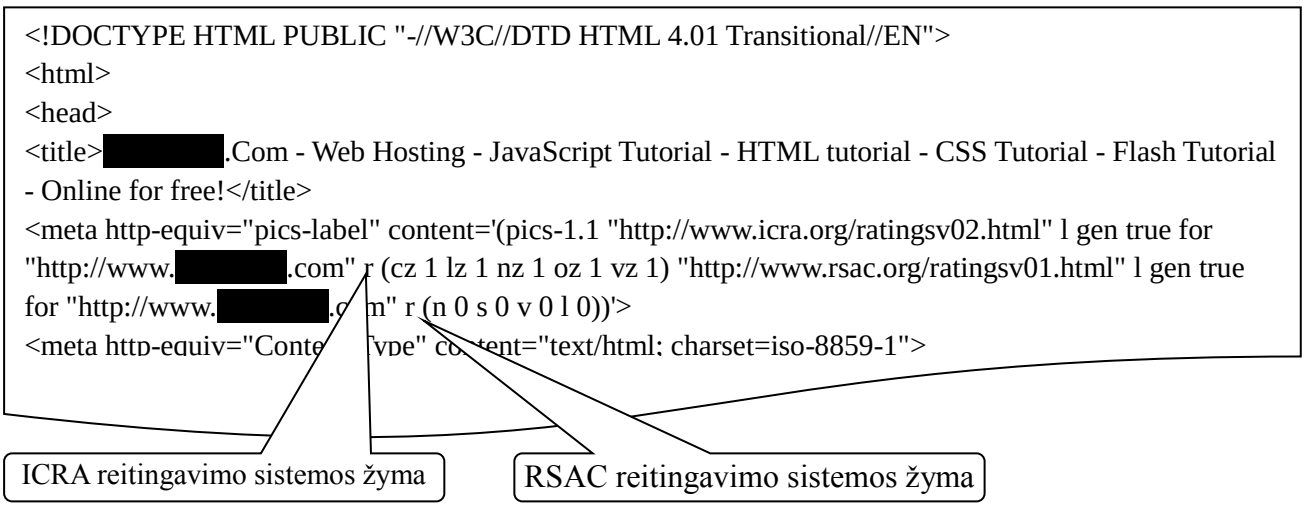
Šio tipo programose galima nustatyti informacijos filtravimą pagal savo poreikius, atlikti šiuos veiksmus: rodyti ir nustatyti įvertinimų parametrus, norint apriboti arba leisti turinį kiekvienoje iš šių kategorijų: kalba, nuogumas, seksas ir smurtas; kurti svetainių, kurios visada turėtų būti blokuojamos, nepaisant jų turinio įvertinimo, sąrašą; rodyti ir keisti įvertinimų sistemas, kurias naudoja Turinio patarėjas.

Dauguma tokio tipo programų naudojama interneto turinio parinkimo platforma (angl. *Platform for Internet Content Selection,* PICS) pagrįsta žymių skaitymu įterptų į turinį [16, 18]. Galima rinktis keletą turinio reitingavimo sistemų (pvz.: RSACi, ICRA, ar kt.), kurios viena nuo kitos skiriasi vertinimo kriterijais ir jų vertinimo lygiais. Pavyzdžiui, RSACi sukurta *Recreational Software Advisory Council* pateikia vartotojams informaciją apie smurto, nuogybės, sekso, įžeidžiančios kalbos lygį interneto svetainėse. RSACi lygiai yra pateikti 1 lentelėje.

1 lentelė. RSACi vertinimo lygiai [19]

Lygis	Smurto reitingo aprašymas	Nuogybės reitingo aprašymas	Sekso reitingo aprašymas	Įžeidžiančios kalbos reitingo aprašymas
4	Prievarta arba ištvirkimas, nepelnytas smurtas.	Nuogumas iš priekio (klasifikuojamas kaip provokuojantis rodymas).	Atviri lytiniai aktai arba lytiniai nusikaltimai.	Šiurkšti, vulgari kalba arba radikali neapykantos kalba.
3	Agresyvus smurtas arba žmonių mirtis.	Nuogumas iš priekio.	Ne atviri lytiniai aktai.	Mažiau vulgari kalba arba neapykantos kalba.
2	Realistiškų objektų naikinimas.	Dalinis nuogumas.	Apsirengusių lytiniai veiksmai.	Vidutinio stiprumo keiksmažodžiai ar neapykanta.
1	Žmogaus sužeidimas.	Per daug apnuoginantys drabužiai.	Aistringas bučiavimasis.	Švelnūs keiksmažodžiai.
0	Nei vienas iš anksčiau paminėtų arba su sportu susijęs dalykas.	Nei vienas iš anksčiau minėtų.	Nei vienas ir anksčiau minėtų arba nekaltas bučiavimasis ar romantika.	Nei vienas iš anksčiau minėtų.

Pagal vartotojo nustatyta lygi turinio atrinkimo programa atrenka kurias interneto svetaines publikuoti vartotojui, skaitydamas specialias žymas (8 pav.) įtrauktas į turinį.



8 pav. Specialiosios turinio įvertinimo žymos HTML faile

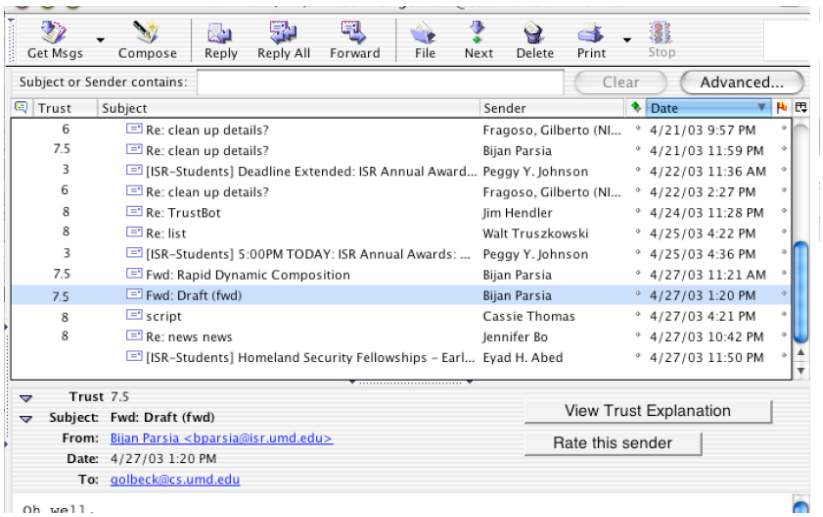
Tačiau šias žymas į failą turi įterpti patys turinio kūrėjai. Tad ne visomis žymėmis galima pasitikėti. Vien tik kūrėjo turinio žymėjimas negali duoti visiško nepageidaujamo turinio blokavimo, nes kūrėjas gali ignoruoti kai kurias žymes, ar žymėti jas neteisingai [13, 19].

Programos „tarpiniai serveriai“

Programos „tarpiniai serveriai“ − tai tarpinis interneto serveris su filtravimo galimybėmis, skirtas privatumui apsaugoti, interneto puslapio turiniui keisti, slapukams tvarkyti, prieigai kontroliuoti, reklamai, reklaminėms antraštėms, laikiniesiems langams ir kitam interneto šlamštui šalinti [6, 8, 27]. Programos „tarpiniai serveriai“ ganėtinai lanksčiai konfigūruojamos ir gali būti pritaikomos asmeniniams poreikiams. Tačiau nepatyrusiam vartotojui sudėtinga keisti filtravimo nustatymus, bet to reikalingas pritaikymas nacionalinio turinio filtravimui. Programos poveikio ribos: vienam kompiuteriui ar vidiniam kompiuterių tinklui (panaudojant kaip tarpini serverį informacijos srautui perduoti).

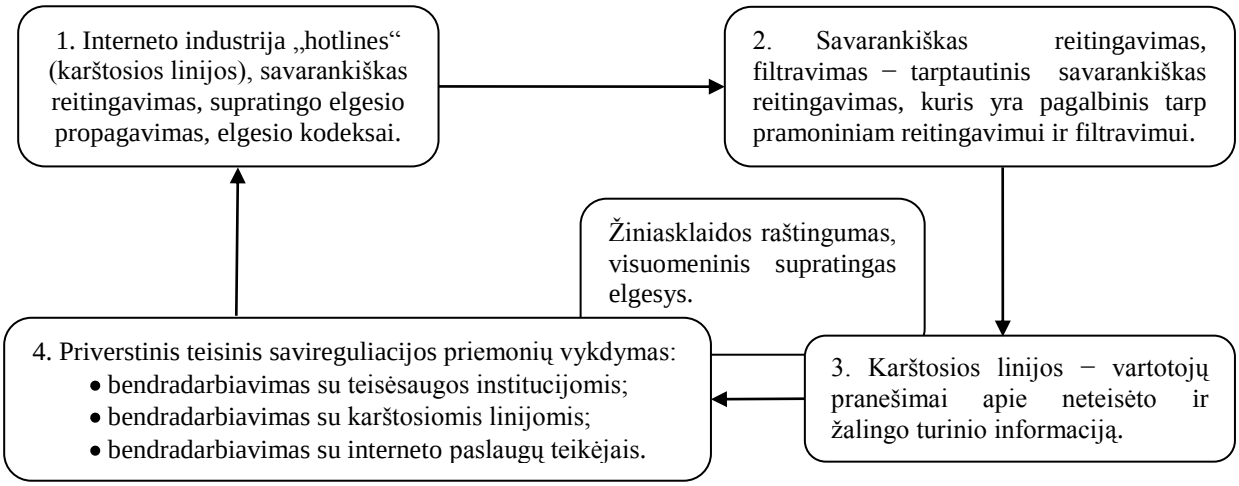
Programos su turinio reitingavimo priemonėm

Programos su turinio reitingavimo priemonėm leidžia vartotojui sukonfigūruoti, rodyti pasitikėjimo lygius arba bendruoju lygmeniu arba, atsižvelgiant į tam tikrą temą. Pavyzdžiui elektroninio pašto programa (9 pav. pateiktas programos langas), kuri rodo laiško siuntėjo reputaciją ir suteikia galimybę reitinguoti siuntėją. Kiekvienas vartotojas gali sukonfigūruoti, rodyti pasitikėjimo lygius laiško siuntėjui arba bendruoju lygmeniu arba, atsižvelgiant į tam tikrą temą. Skirtingai nuo šlamšto filtrų, kurie nurodo, kurie pranešimai ignoruotini, reputacijų reitingas taip pat gali pasakyti vartotojams, kurie pranešimai yra svarbus perskaityti [21, 22].



9 pav. Programos langas su pasitikėjimo reitingais [21]

Apibendrinant galima pateikti tokia vyraujančia interneto turinio reguliacijos schemą (10 pav.).



10 pav. Interneto turinio reguliacijos schema [23]

2.3. Išvados

Kai prieinama įvairiausio turinio informacija, iškyla atrankos klausimas. Interneto auditorija – visas pasaulis, tačiau nepageidaujamas turinys įvairiose šalyse apibrėžiamas skirtingai. Interneto filtravimo technologijų srityje sektorius yra padaręs nemažą technologinę pažangą, ir galutiniams vartotojams dabar yra siūlomi įvairiausi sprendimai.

Kiekviena naršyklė turi papildomas saugumo užtikrinimo priemones (apsaugai nuo XSS, *ActiveX* ir kt.) ir naudoja kenkėjiškų svetainių duomenų bazes. Tačiau yra kenkėjiški kodai, kurie sugeba „apeiti“ (ir) ar išjungti šias apsaugas, kai taikomi socialinės inžinerijos atakos principai, o nepatyręs IT vartotojas apgaulės būdų pats net nesuvokdamas įsidiegia kenkėjiškas programas.

Apžvelgus įvairias turinio vertinimo ir filtravimo programas galime teigti jog su nepageidautinu turiniu kovojama įvairiai. Turinio patarėjai naudojasi interneto turinio parinkimo platforma PICS, kuri pagrįsta įterptų į turinį žymenų skaitymu, tačiau ne visomis žymėmis galima pasitikėti. Pavyzdžiui, kompiuterinio viruso kūrėjas gali labai lengvai sukurti ir platinti žymę, sakančią, kad jo kompiuterinė programa yra saugi, nors išties ji yra užkrėsta virusu. Naudojant žymių tikrinimą klausimą ar pasitikėti turinio kūrėju, keičia klausimas ar pasitikėti žymės kūrėju? Jei abu šie kūrėjai yra tas pats asmuo – pasitikėti žyme nėra saugiau nei pačiu turiniu. Tad vien tik kūrėjo turinio žymėjimas negali privesti iki visiško nepageidaujamo turinio blokavimo, nes jis gali nuspręsti ignoruoti kai kuriuos žymenis, ar žymėti juos neteisingai.

Naudojant tarpinio serverio technologiją paremtas programas galima efektyviai kontroliuoti turinį. Tačiau nepatyrusiam vartotojui sudėtinga paruošti ją darbui. Be to reikia pritaikyti filtruoti nacionalinį turinį. Filtravimo veikimas dažniausiai taikomas vieno kompiuterio ar vietinio kompiuterių tinklo ribose.

Programos su turinio reitingavimo priemonėmis leidžia vartotojui sukonfigūruoti, rodyti pasitikėjimo lygius arba bendruoju lygmeniu arba, atsižvelgiant į tam tikrą temą.

Yra manoma, jog asmens duomenų apsaugos elektroninėje erdvėje problemos neįmanoma įveikti, jeigu su tuo nesistengs kovoti patys interneto vartotojai.

3. Pasiūlymai

Nors Lietuvoje ir veikia daug už informacijos apsaugą atsakingų institucijų skelbiančių informaciją apie incidentus ir grėsmes elektroninėje erdvėje, tačiau vartotojai mažai savarankiškai domisi informacijos saugos, bei privatumo klausimais. O naršant globaliame internete, atidarinėjant nežinomas vartotojui interneto svetaines, dažnai iškyla klausimas ar ši svetainė saugi, ar neapkrės vartotojo kompiuterio kenkėjiškomis programomis, kiek ji yra patikima. Plečiantis e. paslaugų rinkai, tobulėjant mašininiam vertimui, ši problematika tampa vis aktualesne. Šią problematiką galima būtų spręsti panaudojant įrankį, kuris padėtų vartotojui atrinkti saugius ir nesaugius tinklapius, ir kuris taip pat galėtų teikti duomenis ekspertams situacijos analizei, bei galimybę pranešti apie kenkėjiškas svetaines, kurių dėl vienokių ar kitokių priežasčių nėra galimybės pašalinti.

Norint apsaugoti vartotoją nuo grėsmių tykančių internete, reikia jį tinkamai, laiku ir patogiai informuoti apie tykantį pavojų nesaugiose, nepatikimuose interneto svetainėse. Tai realizuoti galima su specializuotu įrankiu, kuris galėtų būti naudojamas kaip naršyklės papildinys. Šis papildinys tikrintų atidaromos interneto svetaines: aptikęs neigiamai vertinama turinį apie tai informuotų vartotoją, aptikęs ypač grėsmingai vertinamą turinį blokuotų tą svetainę ir informuotų apie galimas pasekmes jei vartotojas norėtų nepaisyti šio draudimo. Nors paprastas interneto vartotojas nėra saugumo ekspertas, ir jis neturi reikiamos kompetencijos ištirti atsitiktines interneto svetaines, tačiau būtų galima teikti vartotojams galimybe vertinti svetaines (t. y. pasidalinti savo patirtimi). Kad padidinti šio vertinimo patikimumą sistemos naudotojus – vertintojus galima grupuoti į kelias roles, kurių dalyviai turėtų savitą internetinių svetainių vertinimo svorį, įtakos sistemai matą. Iškart neužpildant sistemos rolių dalyviais (asmenimis įrodančiais savo kvalifikaciją) visas šio vertinimo patikimumas iš pradžių priklausytų nuo sistemos valdytojų. Vėliau susiformavus visoms vartotojų rolėms kiekviena jų kontroliuotų, atsvertų žemesnės rolės pateiktus vertinimus, jų teisingumą ir šitaip padėtų mažiau patyrusiems vartotojams vengti saugumo grėsmių, bei matyti vyraujančias problematikas, aktualijas ir taip tobulėti patys. O nepatyrę vartotojai galėtų įgyti patirties iš pažengusiųjų IT naudotojų apie interneto svetainėse tykančius pavojus. Šiuo metų vykdomo projekto Lietuvoje „Saugesnis internetas LT AN–HL“ efektyvumas nėra pilnai

panaudojamas. Per ataskaitinį nuo 2009 m. balandžio 1 d. iki 2010 m. kovo 31 d. laikotarpį ištirtų 402 pranešimų apie neteisėtą ar žalingą turinį buvo imtasi šių veiksmų:

- 1 pranešimas persiųstas Policijos departamentui;
- 14 pranešimų persiųsta Žurnalistų etikos inspektoriaus tarnybai;
- 15 pranešimų persiųsta kitų šalių, kurios priklauso INHOPE, karštosioms linijoms;
- 31 pranešimas persiųsta atitinkamiems interneto paslaugų teikėjams.

O dėl 341 pranešimo (t. y. beveik 85 %) nebuvo imtasi jokių tolesnių veiksmų, nes turinys nebuvo neteisėtas arba buvo aptiktas šalyse, kuriose toks turinys nėra laikomas neteisėtu [15]. Tad apie tokias svetaines reikiamu momentu būtų galima informuoti vartotoją, naudojant naująjį specializuotąjį įrankį. Į šio specializuotojo įrankio duombazes būtų galima įtraukti jau žinomų valstybinių ir kt. institucijų išanalizuotų netinkamo, žalingo turinio interneto svetaines.

Naudojant internetinių paslaugų teikėjų vertinimo metodiką, kai netik ekspertai formuoja, bei vertina internetines svetaines, nereikalinga daug aukštos kvalifikacijos specialistų. Naudojant hierarchinę vertintojų klasifikaciją galima kontroliuoti vertintojų sąžiningumą. Visuomenės informavimas taptų efektyvesnis, nes vartotojas galėtų gauti informaciją reikiamu momentu prieš susiduriant su netinkamu, žalingu turiniu internete ir jo išvengti.

II. PRIVATUMO IR SAUGOS INTERNETE METODIKOS KŪRIMAS

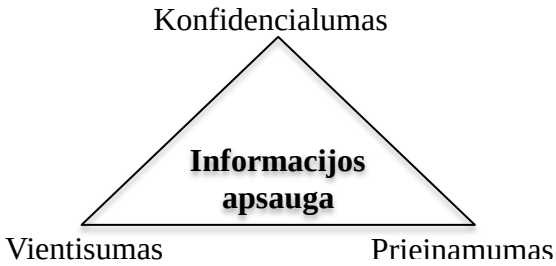
4. Privatumo ir saugos užtikrinimo sprendimo kūrimo metodai

Elektroninėje erdvėje privatumui ir saugumui užtikrinti kompleksiškai turi būti nuolat naudojamos programinės, techninės priemonės. Būtina įvertinti resursus, kuriuos stengiamasi apsaugoti. Šimtaprocentinis saugumas neegzistuoja, o bandymas jo siekti yra labai brangus ir sudėtingas procesas.

Literatūroje [24] galima rasti teiginių jog saugumas labiausiai priklauso nuo kiekvieno vartotojo ir jų bendradarbiavimo tarpusavyje: „***Informacijos apsauga – žmonių problema.*** Dauguma technikos specialistų kompiuterių apsaugą apibrėžia kaip technologinę problemą. Tikrovė rodo, kad kompiuterių apsauga pirmiausia yra žmonių problema. Kompiuterių sujungimas į tinklą labai padidina riziką ir tinklo saugumas labiausiai priklauso nuo kiekvieno vartotojo ir jų bendradarbiavimo tarpusavyje. Saugumo lygis yra toks, koks jis yra silpniausios grandies, ir autorizacija ir identifikacija tampa bevertės, jeigu nors vienas vartotojas nepripažįsta informacijos, kuri turi būti apsaugota, vertės ir leidžia sistemai patekti į pavojų.“

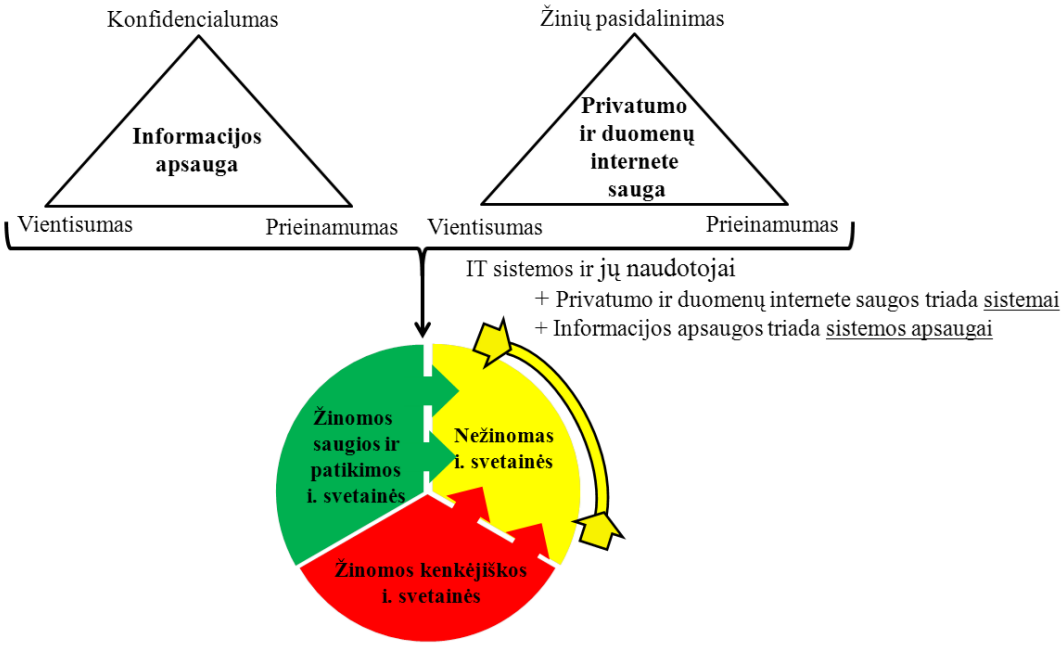
Sprendžiant žmogiškąsias problemas su kuriomis susiduriame naudojantis internetu iškyla daugybę sunkumų. Pavyzdžiui išanalizuoti didelius kiekius duomenų (kaip antai perskaityti visas privatumo politikas sistemų kuriomis naudojasi) vienas žmogus, kaip ir vienas paprastas kompiuteris skirti tiek resursų nepajėgus. Sudėtingiems uždaviniams (pvz. kai yra dideli kiekiai duomenų) spręsti naudojami superkompiuteriai ar paskirstytosios sistemos (pvz. GRID lokaliųjų skaičiavimų tinklų telkiniai – junginiai leidžia apjungti skaičiavimo resursus, o tai leidžia realizuoti didesnius projektus, kuriems nepakanka lokaliųjų resursų).

Informacijos apsaugos teorija teigia jog „informacijos apsauga − tai ne tik informacijos konfidencialumo užtikrinimas. Informacija gali būti prarasta ir niekam jos neatskleidus, pavyzdžiui sugedus tarnybinei stočiai, praradus duomenų laikmenas, pažeidus duomenų bazėse esančius įrašus ar tokių teisių neturintiems asmenims pakeitus informaciją. Tai yra turi būti užtikrinamas ir informacijos prieinamumas bei vientisumas“ [6]. Tai atvaizduojama šia (11 pav.) informacijos apsaugos triada.



11 pav. Informacijos saugos triada

Kone kasdien išleidžiami antivirusinių programų, kas savaitei operacinių sistemų naujinimai. Informacijos sauga ypač greitai kintanti terpė. Kone kasdien atsiranda naujų grėsmių (virusų, duomenų išgavimo internetinių svetainių). Privatumo ir duomenų apsaugos problemoms, su kuriomis susiduriama naudojantis internetinėmis svetainėmis, spręsti reikalingi įnovatyvūs sprendimai. Dažnai žmonės apgaulės būdu, atskleidžia savo privačius duomenis, parsisiunčia tariamai naudingas funkcijas atliekančias programas – virusus. Ne visas jų (ypač naujas) identifikuoja antivirusinės programos. Saugumo ekspertai, IT darbuotojai, IT mėgėjai ar kiti (dažniausiais jau nukentėję) vartotojai sugeba atpažinti žalinga turinį, bei įvertinti galimas grėsmes. Tad jaučiamas metodų trūkumas, siekiant užtikrinti įvairių lygių kompiuterių vartotojų veiklos elektroninėje erdvėje saugų ir patikimą darbą. Tad šioms problemoms spręsti minėtąją informacijos apsaugos triadą, galima interpretuoti ir pritaikyti privatumo ir duomenų saugos internete problematikai spręsti (12 pav.).



12 pav. Informacijos apsaugos triada ir jos interpretacija kuriant pasitikėjimo tinklą

Panaudojant informacijos apsaugos triadą sistemos apsaugai, o duomenų apsaugos internete triada sistemai galima kurti „pasitikėjimo tinklą“ [21], kuriame būtų galima dalintis privatumo, duomenų saugumo užsitikrinimo, naudojantis interneto svetainėmis, patirtimi taip išskiriant „geras“

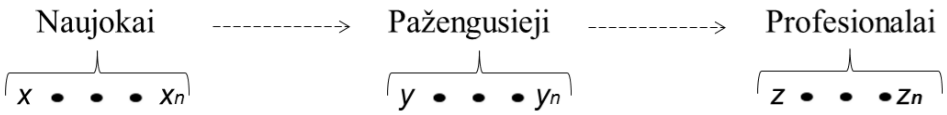
ir „blogas“ internetines svetaines. Tai leistų greičiau pastebėti ir imtis priemonių prieš netinkamą turinį internete, į kovą su juo įtraukiant dar didesnę visuomenės dalį.

4.1. Vartotojų rolės

Apžvelgus privatumo ir saugos užtikrinimui elektroninėje erdvėje naudojamas kompiuterinės priemonės, bei analizės išvadose nustatytus sistemų trūkumus, galime teikti šiuos problematikos sprendimo metodus. Projektuojama sistema turėtų leisti jos vartotojams atrinkti saugias ir nesaugias interneto svetaines. Sistema turėtų būti sudaryta iš kelių skirtingo pasitikėjimo vartotojų rolių (15 pav.): profesionalų, pažengusiųjų, naujokų (t. y. reitinguojamų sistemos naudotojų); bei ekspertų, sistemos valdytojų. Sistema galėtų apjungti įvairius savo mokslo šakų (informacijos saugos, teisės, ir kt.) specialistus, visuomenės saugumu el. erdvėje besirūpinančias organizacijas („Insafe“, „INHOPE“, valstybines organizacijas ir kt.) ir visą visuomenę. Toliau apžvelkime kiekviena sistemos vartotojų grupę.

Sistemos valdytojai, ekspertai tvarkytų ir tobulintų sistemą, galėtų administruoti visų rolių dalyvių (profesionalų, pažengusiųjų ir naujokų) įtaką sistemai, eliminuoti sistemos vartotojų piktybiškus kėslus, formuoti interneto svetainių įverčius – pranešimus, peržvelgti neigiamų, bei teigiamų įverčių susilaukiančias internetinių svetainių sąrašus.

Kitoms vartotojų rolėms (13 pav.) vartotojai prisikrami užsiregistravus sistemoje ir tinkamai (patvirtinus aukštesnės grupės nariams) įvertinus tam tikrą svetainių skaičių. Jie vis kiltų į aukštesnę rolę, kartu didėtų ir jų įtaka (vertinimo svoris) sistemai. Taip pat galima pritaikyti ir kitas variacijas, tarkim vartotojus įrodančius savo kvalifikaciją įtraukiant į aukštesnes roles, bei priskiriant atitinkama vertinimo svorio koeficientą.



13 pav. Vartotojų rolių dalyviai su individualiais vertinimo svoriais

Čia: x – naujoko rolės svoris; y – pažengusiojo rolės svoris; z – profesionalo rolės svoris; $x<y<z$.

Rolė profesionalai – tai būtų ypač patyrę sistemos vartotojai – specialistai, seniai naudojantys šį privatumo ir saugos lygio vertinimo įrankį, teisingai įvertinę tam tikrą internetinių svetainių skaičių, jų įvertinimai sudarytų ženklesne vertę, nei „pažengusiųjų“, bei dar ženklesne nei „naujokų“. Taip pat šios rolės vartotojai turėtų teisę vertinti žemesnės rolės vartotojų vertinimo teisingumą, o to vertinimo įtaka turėtų atsverti žemesnių rolių vertinimus. Į šią rolę iš kart būtų galima priskirti ir naujus vartotojus, įvairius savo mokslo šakų (informacijos saugos, teisės, ir kt.)

specialistus.

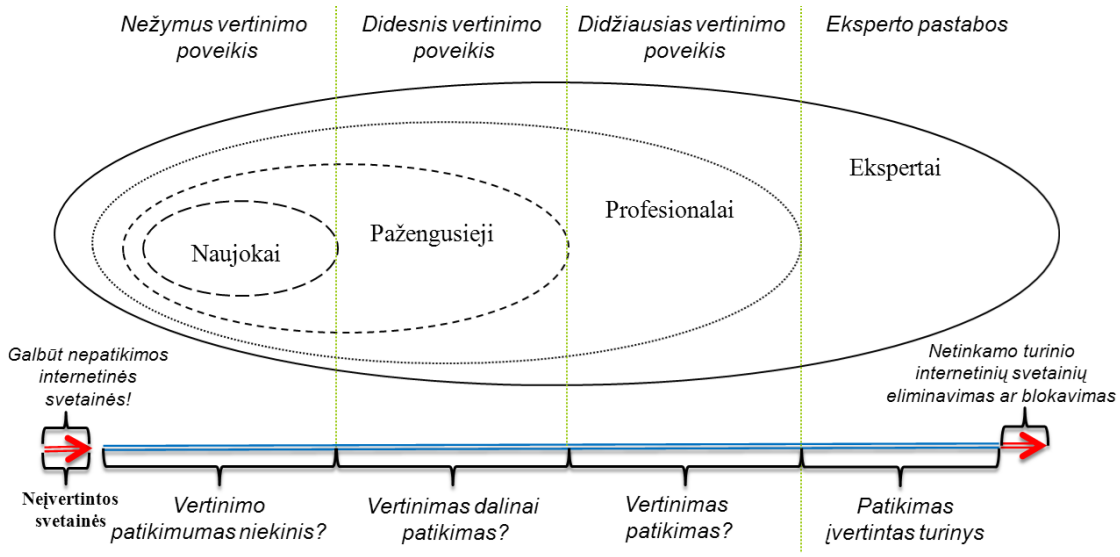
Rolė pažengusieji – tai vidutinio lygmens, tarp ekspertų ir naujokų, vartotojai kurie vertina svetaines palygintinai neilgą laiką, jų vertinimas sudarytu menkesne vertę nei vartotojų ekspertų. Šios rolės vartotojai turėtų teisę vertinti žemesnės ir aukštesnės rolės vartotojų vertinimo teisingumą, tik šio vertinimo svoris būtų didesnis nei naujokų rolės dalyvių ir mažesnis nei profesionalų rolės dalyvių.

Į pažengusiųjų rolę galėtų patekti ir naujai sistemoje užsiregistravę vartotojai jau įgiję žinių pavyzdžiui „e-GUARDIAN“ v.2 mokymo programoje (ir gavę tai įrodantį dokumentą). Minėtoji programa apjungia turimą įdirbį saugaus interneto mokymo srityje ir pateikia pilną produktą skirtą Europos mokytojams, padedantį įgyti daugiau žinių apie interneto grėsmes ir būdus apsaugoti vaikus nuo žalingo interneto poveikio [12].

Rolė naujokai – nepatyrę, nauji vartotojai. Šios rolės vartotojų atliekami vertinimai teiktų mažiausia poveikį sistemai. Į kitą, aukštesnę rolę (ar rolės grupę) pereitų tik patvirtinus aukštesnės rolės (grupės) vartotojams *y* jo vertinimų.

Literatūroje [25] sutinkame jog kompiuterio „procesoriuje skiriami keturi privilegijų lygiai. Labiausiai privilegijuotos yra „0“ lygio programos. Programų, kurios gali būti vykdomos aukštesniu privilegijų lygiu, mažėja nuo 3 lygio iki 0 lygio. 0 lygiu veikia operacinės sistemos branduolio programos. Todėl privilegijų lygiai paprastai vaizduojami keturių apsaugos žiedų pavidalu.“. Šiais principais yra nuolatos kontroliuojama ar vykdoma programa turi pakankamas privilegijas.

Apžvelgus visas išsivardintas roles ir remiantis sistemų kūrimo modeliais galime sudaryti šių rolių įtakos sistemai diagramą (14 pav.).



14 pav. Vartotojų rolių įtaka privatumo ir saugos lygio vertinimo sistemai

Kaip matome (14 pav.) visa sistema sukasi aplink „naujokus“ – interneto vartotojus galimai turinčius menkiausia žinių apie grėsmes, bei kaip jas atpažinti lygį. Judant šioje diagramoje iš centro į sistemos pakraštį žinių lygis, o kartu ir įtaka sistemai didėja. Toliau išskirsime internetinių svetainių vertinimo aspektus.

4.2. Internetinių svetainių vertinimo aspektai

Interneto svetainių vertinimui reiktų išskirti kelias vertinimų kategorijas, tai yra didžiausius privatumui ir saugai keliančius grėsmę aspektus:

- Žalingos programos ir veika − virusais, Trojos arkliais ir kitos žalingos programos, taip pat tarptinklapinių užklausų klastojimas, slapukų perėmimas ir kt.;

- Privatumo politika – kokia privatumo politika apie interneto svetainėje renkamus duomenis, kur ir kaip jie naudojami, saugomi;

- E. komercija – vartotojų pasitenkinimo teikiamomis (tariamai teikiamomis) komercinėmis paslaugomis atsiliepimai. Tai aktualu, nes apgavystės vykdomos ir kai „e. verslas“ perkeliamas į mažiau įstatymais reglamentuotas ir (ar) palankias jį vystyti valstybes, kur taikant teisines priemones teisėsaugos institucijoms netinkamos, kenkėjiškos interneto svetaines pašalinti nepavyksta;

- Neteiktinas turinys – tai draudžiama skelbti informacija, kurioje raginama prievarta keisti Lietuvos Respublikos (LR) konstitucinę santvarką, skatinama kėsintis į LR suverenitetą, jos teritorijos vientisumą, politinę nepriklausomybę, kurstomas karas ar neapykanta, tyčiojimasis, niekinimas, kurstoma diskriminuoti, smurtauti, fiziškai susidoroti su žmonių grupe ar jai priklausančiu asmeniu dėl lyties, seksualines orientacijos, rasės, tautybės, kalbos, kilmės, socialines padėties, tikėjimo, įsitikinimų ar pažiūrų, platinama, propaguojama ar reklamuojama pornografija, taip pat propaguojamos ir (ar) reklamuojamos seksualinės paslaugos, lytiniai iškrypimai, propaguojami ir (ar) reklamuojami žalingi įpročiai ir narkotinės ar psichotropines medžiagos. Taip pat draudžiama platinti dezinformacija ir informacija, šmeižianti, įžeidžianti žmogų, žeminanti jo garbę ir orumą, pažeidžianti nekaltumo prezumpciją ir kliudanti teismines valdžios nešališkumui [39].

Istoriškai pirmuoju vertinimo standartu, plačiai paplitusiu ir padariusiu didelį poveikį kompiuterių saugumo standartizavimui daugelyje šalių, tapo JAV gynybos ministerijos standartas „Patikimų kompiuterinių sistemų vertinimo kriterijai“ (*Trusted Computer System Evaluation Criteria*, TCSEC) [25]. Joje apibrėžti keturi sistemų saugumo lygiai (nuo žemiausio iki aukščiausio). Taipogi prisimenant *Recreational Software Advisory Council* turinio klasifikavimo

sistemą (apžvelgta 2.2.3 skyriuje), galime projektuojamoje sistemoje sugrupuot saugumo grėsmių lygius su kuriais susiduriama naudojantis internetinėmis svetainėmis, pagal jų poveikį vartotojo sistemai ar pačiam vartotojui (jo privatumui ir saugumui).

2 lentelė. Išskiriami saugumo grėsmių lygiai su kuriais susiduriama naršant i. svetainėse

Grėsmės lygis	Saugumas	Privatumas	E. komercija	Turinys
3	Aukščiausias virusų, kenkėjiško kodo grėsmės lygis (automatins užkrėtimas).	Kaupia duomenis neapibrėžtą laiką, neaiškiem tikslam. Neužtikrinamas duomenų konfidencialumas.	Sukčiavimas.	Raginama prievarta, prieštaraujama LR santvarkai, propaguojama ar reklamuojama pornografija, žalingi įpročiai ir jų medžiagos.
2	Vidutinis virusų, kenkėjiško kodo grėsmės lygis (užkrėtimas po atlikto veiksmo).	Teikia vartotojų duomenis tretiesiems asmenims.	Nepatenkinamai vykdoma veikla.	Autorių teisių ir gretutinių teisių pažeidimai.
1	Nedidelis virusų, kenkėjiško kodo grėsmės lygis (neprašyta veikla).	Neskelbia privatumo politikos.	Yra nusiskundimų vykdoma veikla.	Dezinformacija.
0	Nėra virusų, kenkėjiško kodo grėsmės.	Atitinka lūkesčius.	Veikla vykdoma puikiai.	Atitinka leistinas normas.

4.3. Didesnio vertinimo patikimumo užtikrinimas

Reitinguojamam vartotojui įvertinus *n* interneto svetainių aukštesnės rolės vartotojas turi būti patikrinęs (įvertinęs) bent *n–x* jo įvertinimų, tik tada vartotojas būtų priskirtas aukštesnei rolei, kurioje vertinimai turėtų ženklesnę reikšmę sistemai.

Vartotojo interneto svetainės įvertinimus turėtų vertinti kiti vartotojai (nedaugiau kaip po vieną vertinimą vienam interneto svetainės vertinimui). Šio vertinimo poveikis sistemai būtų didinamas priklausomai nuo kitų vartotojų ir pačių vertintojų individualaus svorio sistemai, tai yra jų suteikiamo vertinimui svarumo.

Vartotojui atverčiant internetinę svetainę, kurią jis pats įvertino, turi būti atsižvelgiama į jo vertinimus, tai yra jei jis ją įvertino trečio lygio grėsmės įverčiu, tai jam bus svetainė blokuojama ir prašoma patvirtinimo tęsti, nors ir iš kitų vartotojų nesulauktą tokių vertinimų.

Vienam vartotojui internetinę svetainę įvertinti visais pateiktais aspektais (saugumas,

privatumas, e. komercija, turinys) reikia leisti tik vieną kartą, vėliau leidžiant tik juos keisti, tai leistų išvengti piktnaudžiavimo.

4.4. Pranešimai sistemos vartotojams

Literatūroje [24] sutinkame teiginių jog saugumo ugdymo progamos turinyje turi atsispinėti rizika, pagrindinės atsakomybės priemonės, atsakomybė, kontaktinė informacija:

„***Kontaktinė informacija*.** Ugdymo medžiagoje turi būti nurodyti kontaktiniai duomenys – kam pranešti apie incidentą, ko klausti apie slaptumo dalykus ir kam pateikti siūlymus. Žmonės turi žinoti *kas, kaip, ką* ir *kada*:

Kas – apsaugos personalo, kuris rūpinasi apsauga nuo incidentų, pagalbos tarnybos personalo kontaktinė informacija: telefono numeris, e. pašto adresas, tinklapio adresas.

Ką – informacijos tipai, apie kurių problemų įtarimus reikia pranešti, pvz.:

- pažeistos sistemos ar tinklapiai;
- techninė įranga ir operacinės sistemos;
- požymiai;
- data, laikas, incidento trukmė;
- ryšys su sistemomis, kurios buvo paveiktos;
- vykdyti veiksmai;
- pažeidimai;
- reikalinga pagalba.

Kaip – instrukcijos, kaip pranešti apie įtariamas problemas telefonu, e. paštu, t. y. naudojant sistemą, kuri yra pakankamai atspari atakoms.

Kada – vartotojai turi žinoti, kokioms situacijoms yra svarbus laiko veiksnys. Jeigu skubus pranešimas gali apsaugoti nuo būsimo pažeidimo, vartotojai turi žinoti, jog negalima delsti.“

Tad kuriamoje sistemoje pranešimus vartotojams turėtų teisę rašyti tik ekspertai, sistemos valdytojai. Jais galima būtų pranešti apie kenkėjiškas internetines svetaines, elektroninėmis sistemomis tiek ir kitomis priemonėmis greitai plintančias grėsmes privatumui, duomenims ir kt., pagal vartotojų grupes ar individualiai. Kitų rolių vartotojai, naudodamiesi pranešimų funkciją, turėtų tik teisę pranešti apie sukčiavimą vertinant turinį sistemos valdytojams, o taip pat ir apie aptiktą neteiktiną Lietuvos Respublikoje turinį atsakingoms institucijoms.

4.5. Sistemos funkcionavimo metodo parinkimas

Kiekvienas sistemos dalyvis turi turėti savitą patikimumo lygį, kaip ir jo pateiktas įvertis nustatant internetinės svetainės saugumo lygį. Šio skyrelio tikslas atrinkti tinkamiausius metodus sistemos kiek galima geresniam funkcionavimui.

Paprasta tiesinė vartotojų reitingų skaičiavimo sistema nepakankamai išpildo lūkesčius, nes ji augina skaitliuką, tačiau neatsižvelgia į laiko, bei kokybiškumo klausimus[28].

Vidurkio principu grindžiamame metode atsiranda galimybės nesąžiningam reitingavimui. Jei kiti vartotojai norės, kad reitinguojamas vienetas neiškiltų, jie gali tyčia skirti mažus balus. To pasekoje reitinguojamo vieneto galutinis rezultatas mažės nuo savo vidurkio normos. Taip pat ši reitingavimo sistema yra labai lengvai perprantama ir nesuteikia jokio intelektualumo pojūčio reitinguojamiems vienetams bei patiems reitinguotojams [28].

ELO reitingavimo sistemos taškų skaičiavimo principai yra ganėtinai teisingi ir priimtini norint nustatyti reitinguojamo vieneto kokybiškumą, tačiau ši sistema plačiau naudojama rungtynėse, kur varžovai varžosi poromis vienas prieš kitą [28].

Glicko reitingavimo sistemos praktinis pritaikomumas yra toks pats kaip ir ELO reitingavimo sistemos. Priešingai nei ELO reitingavimo sistema, Glicko įvertina vartotojo patikimumo faktorių. ELO sistemoje, jei rungiasi du žaidėjai su tokiu pačiu reitingo dydžiu, tai pergalės atveju, vienam žaidėjui taškų skaičius sumažėja per *n* vienetų, o kitam žaidėjui atitinkamai padidėja per *n* vienetų. Glicko reitingavimo modelyje išlieka reitinguojamų objektų aibės mažas išplečiamumas – čia reitinguojami tik tarpusavyje besivaržantys objektai, veiksmas vyksta poromis [28, 29].

Glicko–2 reitingavimo sistema turi ne tik objekto reitingą, reitingo nuokrypį, bet dar vieną papildomą parametrą – reitingo nepastovumą [28, 30]. Glicko–2 reitingų skaičiavimo būdas įgalina sekti reitinguojamų objektų intelektualinius šuolius, kurie galbūt yra pagrįsti apgaule ar melu. Turinčius didelį reitingo nepastovumą vartotojus galima labiau stebėti ir vertinti jų atliekamus veiksmus [28, 31]. Glicko–2 reitingo skaičiavimo papildomi parametrai labiausiai reikalingi sistemą prižiūrinčiajam valdytojui. Turint šias reikšmes galima bandyti ieškoti galimų taškų nesutapimų ar pervertinimų. Tačiau Glicko–2 reitingavimo modelyje taip pat išlieka reitinguojamų objektų aibės mažas išplečiamumas, tai yra reitinguojami tik tarpusavyje besivaržantys objektai, veiksmas vyksta poromis [28].

Kuriamajai sistemai reikia realizuoti tokį metodą, kurio darbui atlikti būtų kuo mažiau naudojamas žmogiškasis valdytojo įsikišimas. Kuo platesnė reitingavimo galimybių aibė, tuo labiau

atsiranda didesnis stimulas varžytis ir lenktyniauti siekiant teisingiausio – geriausio rezultato. Reikia įvertinti sistemos dalyvio patikimumo lygį, bei patvirtinti ar paneigti internetinių svetainių įverčių patikimumą. Šiems tikslams pasiekti galima pasiremti sukurtu IT žinių portalo reitingavimo modeliu [28].

4.5.1. Sistemos dalyvio patikimumo lygio nustatymas

Tam, kad pasiekti didesnes galimybes reitingų skaičiavimo variacijose vertinant svetainių įverčius, reitingavimo modeliuose naudojami svorių mažinimo koeficientai bei patys svoriai. Koeficientų dydžiai priklauso nuo įvykio naujumo ar kokybiškumo.

Kiekvienam sistemoje registruotam vartotojui pradžioje reikia sukurti pradinį jo reitingą. Sistemoje yra trys vartotojų lygiai. Visi lygiai turi savo svorinius koeficientus, kurie naudojami skaičiuojant atitinkamus vartotojo veiksmų įvertinimus. Kiekvienam lygiui yra nustatyta taisyklė, kas gali į jį pakliūti. Taisyklėse apibrėžti skaičių intervalai, kurie reiškia vartotojo tinkamumą į vieną ar kitą lygį. Lygių intervalai turėtų būti padalinti norimais intervalais [0;1] ribose, pvz. [0; 0.5); [0.5;0.8); [0.8;1]. Tokiu atveju, naujo vartotojo pradinis reitingas lygus nuliui ir jis patenka į naujoko lygį.

Reitingavimo elementai vartotojui gali būti pradinis vartotojo reitingas, jo įvertintų internetinių svetainių, paneigtų ar patvirtintų, įverčių skaičius. Pradinis vartotojo reitingas yra vienas iš reitingų elementų, todėl jį apskaičiuojant naudojama standartinė procedūra išgaunant reitingo elemento svorį pagal periodą bei maksimumo reikšmę bei ją padauginant iš vartotojo lygio svorinio koeficiento:

$$ir^{user} = \frac{rire^{number}}{rem^{value}} \cdot re^{weight} \cdot ul \quad (1)$$

Čia: ir^{user} – vartotojo patikimumo lygis (svoris); $rire^{number}$ – už laisvos formos vertinimus surinktas teigiamų recenzijų skaičius; rem^{value} – sistemoje įvertintų interneto svetainių skaičius; re^{weight} – už laisvos formos įverčius sukauptas svoris; ul – vartotojo lygio svoris.

Vartotojo lygis gali kilti atitinkamai dėl atliekamų veiksmų. Kiekvieną kartą pasikeitus bendram vartotojo patikimumo lygiui, jo reikšmė yra lyginama su lygių intervalų reikšmėmis ir pagal sulyginimo rezultatą vartotojo lygis paliekamas toks koks buvo arba pakeičiamas. Pasikeitus vartotojo lygiui, pradinis vartotojo reitingas neperskaičiuojamas. Atitinkamai už visus reitinguojamus elementus konkretiems vartotojams yra kaupiamas surinktas įvykių kiekis, kuris vėliau dalyvauja bendruose rezultatų skaičiavimo algoritmuose.

4.5.2. Įverčių patikimumo nustatymas

Internetinių svetainių įverčiai pagrindžiami laisvos formos komentaru kaip ir vartotojai, turi

jiems pritaikytus reitingavimo elementus (svariausi vertinimai bus pateikiami geriausiai matomoje vietoje). Tad pradinis komentaro reitingas, teigiamų ir neigiamų įvertinimų santykio svoris, kuris skirtingas kiekvienam vertinančiam sistemos dalyviui.

$$w^{reviewsWeight} = -1 \cdot \sum_{i=0}^{m} ir_i^{userF} + \sum_{i=0}^{m} ir_i^{userT} \quad (2)$$

Čia: $w^{reviewsWeight}$ – vartotojo atlikto laisvos formos įverčio svarumas po atliktų recenzijų ($w^{reviewsWeight} \geq 0$); ir_i^{userF} – i-tojo svorio recenzento įvertinimas neigiamai; ir_i^{userT}– i-tojo svorio recenzento įvertinimas teigiamai; *m* – vertinimų skaičius.

Skaičiuojant internetinės svetainės laisvos formos įverčio reitingą yra įvertinamas autoriaus lygis, internetinų svetainių įverčių recenzijų svorio koeficientas, recenzijų įvertinimas.

$$ir^{assessment} = ir^{user} + w^{reviewsWeight} + re^{reviewsT} \quad (3)$$

Čia: $ir^{assessment}$– internetinės svetainės laisvos formos įverčio svarumas; ir^{user} – vartotojo rašiusio laisvos formos įvertį patikimumo reitingas (svoris); $w^{reviewsWeight}$ – vartotojo atlikto įverčio svoris po atliktų recenzijų; $re^{reviewsT}$– recenzentų suteiktas teigiamų įverčių skaičius.

4.5.3. Grėsmės lygio internetinėje svetainėje nustatymas

Norint apibendrinti ir pateikti grėsmės saugumui, privatumui, e. komercijos (teikiamom, tariamai teikiamom) paslaugom, turinio tinkamumo ir patikimumo lygius tikslinga pasiremti sistemos vartotojų įverčiais ir išskirti stiprausią kiekvienos vertinamos kategorijos įvertį.

$$G_0 = \sum_{i=0}^{m} ir_i^{user}, \ldots, G_3 = \sum_{i=0}^{m} ir_i^{user} \quad (4)$$

Čia: G_n – grėsmes vertinimui suformuotas svarumas; ir_i^{user} – vartotojo atlikusio įvertinimą svoris; *i*-tojo svorio recenzento įvertinimas; *m* – vertinimų skaičius.

Tikslinga sistemos dalyviam pateikti bendrą internetinės svetainės įvertį, grėsmingiausia įvertį. Esant internetinės svetainės eksperto įvertinimui tikslingiausia pateikti pastarąjį, jei jo nėra pateikti internetinės svetainės lankytojų suformuota stipriausią grėsmės įvertį. O tik užklausius pateikti suformuota esamą išsamia ekspertų ir vartotojų nuomonę – informaciją.

5. Privatumo ir saugos internete tyrimui reikalingų aparatūrinių – programinių – informacinių priemonių apžvalga

Tokiai privatumo ir saugos internete vertinimo sistemai realizuoti bus reikalinga klientinės prieigos programa, kuria naudodamiesi vartotojai galės valdyti visas jiems suteiktas funkcijas. O programinės įrangos funkcionalumui užtikrinti bus reikalinga serverio programinė įranga. Ji bus

prieinama tik administratoriams ir patalpinta projekto serveryje kartu su duomenų bazėmis. Serveris perduos parametrus, reikalingus duomenis tarp vartotojų klientinės prieigos programinės įrangos ir duomenų bazės.

Projektui reikalinga aparatūrinė įranga: kompiuteriai paruošti darbui, interneto prieiga suteikianti aparatūra. Taip pat reikalinga interneto naršyklė, UML diagramų kūrimo programa, programavimo paketai, žiniatinklio serveris, duomenų bazių valdymo programinė įranga.

Privatumo ir saugos internete vertinimo informacinės posistemės projektavimui naudosime UML. UML – tai modeliavimo kalba, standartinė projektavimo priemonė, kuri visuotinai naudojama pasaulyje ir praktiškai neturi rimtesnių „konkurentų“. UML apibrėžia 12 rūšių diagramas, kurios leidžia specifikuoti įvairius architektūros aspektus. Nedideliuose projektuose galima braižyti UML diagramas bendrais diagramų modeliavimo įrankiais, pavyzdžiui „MagicDraw UML“, „Microsoft Visio“, arba tiesiog tekstų rengykle. Visgi didesniuose projektuose specializuotų UML įrankių naudojimas leidžia dirbti daug efektyviau. Naudojant UML, galima modeliuoti sistemą skirtingais abstrakcijos lygiais. Pavyzdžiui, kuriamos sistemos esybes ir jų ryšius vaizduojanti klasių diagrama gali būti naudojama reikalavimų analizės metu, o vėliau pagal ją gali būti sukuriama detali realizacijos klasių diagrama, kurioje nurodomi specifiniai realizacijos kalbos duomenų tipai, atliekamos reikalingos ryšių transformacijos, pridedamos tik realizacijai reikalingos savybės, tokios kaip identifikaciniai kodai. Modeliavimas skirtingais abstrakcijos lygiais leidžia glaudžiau susieti programinės įrangos architektūros projektavimą su reikalavimų analizės veikla.

5.1. Programavimo kalba *Java*

Privatumo ir saugos internete vertinimo sistemos serverio dalies programinei įrangai kurti naudosime *Java* programavimo kalbą. Norint, kad ji galėtų veikti daugelyje sistemų − tai *Java* programavimo kalba tiks labiausiai, nes šioje programavimo sistemoje programuotojo parašytas kodas kompiliuojamas ne į procesoriui specifinę, o į tarpinę formą, kuri nepriklauso nuo procesoriaus tipo ar operacinės sistemos, todėl iškart tinka vykdyti įvairiose operacinėse sistemose ir kompiuterių architektūrose.

Java – objektiškai orientuota programavimo kalba, 1991 metais sukurta „Sun Microsystems“ inžinierių Džeimso Goslingo ir Patriko Naughtono. Apie ją oficialiai paskelbta 1995 metų gegužės 23 d., o išleista tų pačių metų lapkritį. *Java* sudaryta iš kelių platformų:

- *J2SE – Java 2 Platform, Standard Edition*. Šioje platformoje yra pateikiamos visos bazinės bibliotekos ir įrankiai, kurie naudojami komandines eilutes ir grafinę sąsają turinčioms programoms kurti;

- *J2EE – Java 2 Platform, Enterprise Edition*. *J2SE* yra papildoma įvairiomis technologijomis, suteikiančiomis galimybę kurti internetines programas (*Java Servlet, JavaServer Pages, JavaServer Faces* ir kt.), paskirstytas sistemas, apibrėžia daugkartinio panaudojimo komponentus kaip *Enterprise JavaBeans*;

- *J2ME – Java 2 Platform, Micro Edition*. Tai platforma, kuri pateikia įrankių rinkinį kurti programas tokiems mobiliems įrenginiams, kaip mobilieji telefonai, delniniai kompiuteriai ir kitiems.

Java programavimo sistemoje programuotojo parašytas kodas kompiliuojamas ne į procesoriui specifinę, o į tarpinę formą. Ši tarpinė forma nepriklauso nuo procesoriaus tipo ar operacinės sistemos, todėl iškart tinka vykdyti įvairiose aplinkose. Pirmosiose *Java* versijose tarpinis kodas buvo interpretuojamas, todėl *Java* pelnė lėtai dirbančios platformos reputaciją. Dabartinės sistemos tarpinį kodą paprastai prieš vykdydamos kompiliuoja, todėl vykdymo greitis panašus ar tik nežymiai mažesnis. *Java* turi gimtąją sąsają (angl. *native interface*), kurios pagalba nesunku ją jungti ir su esančiomis *C, C++* bibliotekomis. Dažniausiai to prireikia jei būtina naudoti šiomis kalbomis parašytas matematines ar kitokias bibliotekas.

Svarbi *Java* sistemos dalis yra šiukšlių surinktuvas. Programuotojas turi rašyti kodą, kuris atėjus laikui naikina nebereikalingas duomenų struktūras, išlaisvindamas jų užimamą atmintį. Klaidos neretai sutrikdydavo programą, o senesniais laikais paprastai ir visą operacinę sistemą. *Java* šiukšlių surinkėjas pats nustato, jog struktūra nebenaudojama ir jos užimama atmintis gali būti atlaisvinama.

Įvairios *Java* programos dalys nesunkiai gali būti vykdomos lygiagrečiai (angl. *multithreading*).

Pradedant naujesne 1.5 versija, *Java* kalba palaiko bendrybes (angl. *generics*), kurios primena aiškesnį, paprastesnį praeityje kai kuriose programavimo kalbose buvusių makrokomandų variantą. Nuo 1.6 versijos *Java* palaiko scenarijus (angl. *script*) – galimybę vykdyti simbolių eilutės, kintamajame esantį kitos programos tekstą, jam keičiantis duomenimis su gaubiančiąja programa.

Šiuo metu esama tiek komercinių, tiek ir atviro kodo (*GNU Classpath, Apache Harmony*) *Java* programų vykdymo sistemų. *Java* sukūrusi „Sun Microsystems“ 2006 m lapkričio mėnesį paskelbė, jog palaipsniui pereina prie atviro kodo modelio, pateikiant visas *Java* programai vykdyti reikalingas dalis su *GPL* licencija [32, 33].

5.2. Interneto naršyklės papildinio kūrimas

Siekiant jog sukurtąją sistema būtų galima naudotis įvairiuose operacinėse sistemose kūrimo priemonės turėtų būti universalios. Sistemos klientine dalį galima realizuoti naudojant interneto naršyklių papildinių kūrimo priemones. Populiaresnėse naršyklėse [34] „Chrome“, „Firefox“, „Safari“, „Opera“ papildiniai gali būti rašomi naudojant interneto technologijas, kaip antai HTML, *Javascript* ir CSS.

Yra dviejų tipų scenarijai (angl *script*). Internete *JavaScript* vykdomi tinklalapio turinio kontekste, ir turi prieiga prie tų puslapių DOM (angl. *Document Object Model*) turinio. Tai leidžia kviesti funkcijas, pavyzdžiui:

window.alert("Labas");

Papildinio pagrindiniame scenarijuje, to padaryti negalime, nes papildinio kodas nėra skirtas vykdyti puslapio turinį ir DOM, todėl nėra pasiekiamas. Norint prieiti prie konkretaus puslapio DOM, reikia naudoti turinio scenarijus.

Taigi, yra dviejų skirtingų rūšių *JavaScript* scenarijai, galima įtraukti juos į naršyklės papildinį, ir jie turės prieigą prie skirtingų taikomųjų programų programavimo sąsajų (angl. *Application Programming Interface*, API). SDK (angl. *Software Development Kit*) dokumentacijoje jie vadinami atitinkamai papildinio kodu (*„add–on code“)* ir turinio scenarijumi (*„content scripts“).*

Papildinio kodas − tai vieta, kurioje įgyvendinama pagrindinė interneto naršyklės papildinio logika. Papildinys yra įgyvendinamas kaip vieno ar daugiau bendrų *JavaScript* modulių kolekcija.

Turinio scenarijus**.** Papildinys visada turės viena pagrindinį modulį (pavyzdžiui: „Firefox“ − *main.js*; „Google Chrome“ − *manifest.json*;), tereikia parašyti turinio scenarijus, jei papildiniui reikia manipuliuoti interneto turiniu. Turinio scenarijus yra įterpiamas į interneto puslapius, naudojant API, apibrėžtų kaip SDK moduliais, pavyzdžiui „*page–mod*“, skydeliu (angl. *panel*) ir valdikliu (angl. *widget*).

API prieiga prie papildinio kodo ir turinio scenarijų yra skirtinga. Toliau pateiktoje 3 lentelėje apibendrinama, kurie yra prieinami kiekvieno tipo scenarijų API.

3 lentelė. API prieiga prie papildinio kodo ir turinio scenarijų

Taikomųjų programų programavimo sąsaja (API)	**Papildinio kodas**	**Turinio scenarijus**
Globalus objektai apibrėžti branduolyje *JavaScript* kalba, tokie kaip *Math*, *Array*, ir JSON (angl. *JavaScript Object Notation*)	+	+
require() ir *exports* globaliais apibrėžti bendrojoje *JavaScript* specifikacijoje. Galima naudoti *require()* importuoti funkcionalumą iš kito modulio ir *export* eksportuoti funkcionalumą iš modulio. Jei *require()* yra prieinami, tai yra tiekiami SDK modulio.	+	−
Pultas (angl. *console*) globaliai teikiamas SDK.	+	+
Globaliais HTML5 specifikacijoje apibrėžti, tokie kaip *window*, *document*, ir *localStorage*.	−	+
Globalus *self* naudojamas komunikuoti su turinio scenarijais ir papildinio kodu.	−	+

Naršyklės papildiniams reikia bendrauti su interneto turiniu ar naršyklės vartotojo sąsaja. Pavyzdžiui, papildiniai (*add–ons*) gali pasiekti ir keisti tinklalapių turinį ar pranešti, kai vartotojas paspaudžia nuorodą.

SDK numato keletą pagrindinių modulių:

- *„Panel“* − skirtas kurti dialogui, kuris gali priimti tinklo turinį;
- *„Page–worker“* − skirtas parsisiųsti puslapį ir naudotis jo turiniu, nerodant vartotojui;
- *„Page–mod“* − naudojamas vykdyti pasirinktų interneto puslapių scenarijus;
- *„Widget“* − priimančiojo papildinio vartotojo sąsajos, apimančios tinklo turinį, valdiklis;
- *„Context–meniu“* yra skirtas pridėti elementus į naršyklės kontekstinį menių.

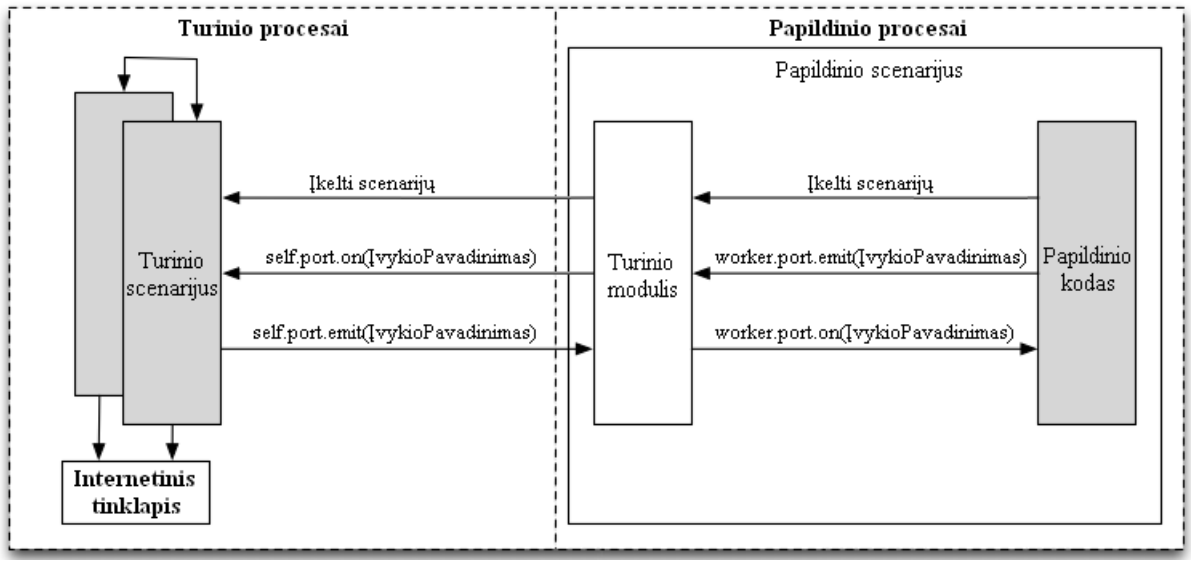
Pagrindia interneto naršyklės naudoja atskirus procesus rodyti vartotojo sąsają, tvarkyti interneto turinį ir vykdyti papildinius. Pagrindinis papildinio kodas bus vykdomas papildinio procesų ir neturės tiesioginės prieigos prie bet kurios interneto turinio. Tai reiškia, kad papildiniai, kurie turi bendrauti su interneto turiniu, turi būti sudaryti iš dviejų dalių:

- pagrindinis scenarijus (angl. *main script*) vykdomas papildinio proceso;
- bet koks kodas, kuris turi bendrauti su interneto turiniu yra pakraunamas į interneto turinio procesą, kaip atskiras scenarijus. Šie atskiri scenarijai yra vadinami turinio scenarijais.

Vieną papildinį gali naudoti keletą turinio scenarijų, ir turinio scenarijai pakrauti į ta patį kontekstą gali veikti kartu tiesiogiai vienas su kitu taip pat kaip su tinklo turiniu, savarankiškai.

Papildinio scenarijus ir turinio scenarijus negali tiesiogiai gauti prieigą vienas prie kito būsenos. Vietoj to, galima nustatyti savo įvykius, kuriuos kiekviena pusė gali skleisti, ir kitoje pusėje gali registruoti, bei su jais dirbti.

Diagrama pateikta 15 pav. rodo, apžvelgtus pagrindinius komponentus ir jų santykius. Pilka spalva užpildytos dalys − tai kodas parašytas papildinio kūrėjo [35].



15 pav. Turinio scenarijaus ir papildinio principinė komunikavimo schema

Norint gauti įvykį iš papildinio kodo naudojamas metodas *self.port.on(ĮvykioPavadinimas)*. Turinio scenarijuje prievado (angl. *port*) objektas yra pasisekamas kaip ypatybė globalaus savarankiško objekto. Tad skleisti įvykį iš turinio scenarijaus naudojamas metodas *self.port.emit(ĮvykioPavadinimas)*.

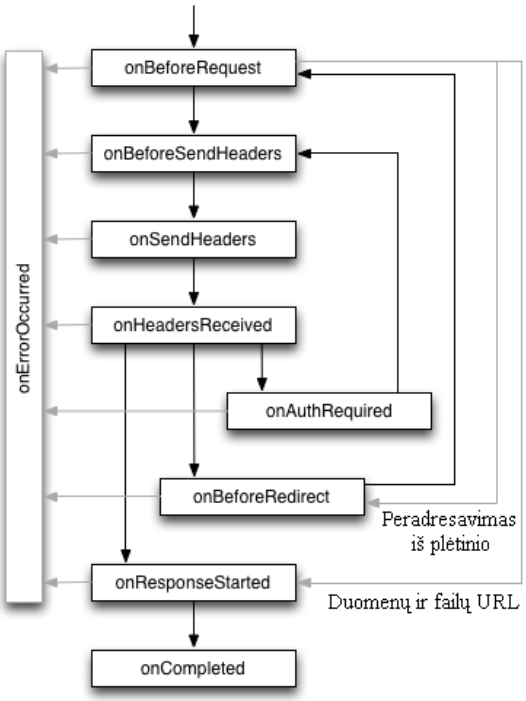
„Page–mod“ nėra tiesiogiai integruoti aplikacijų programavimo sąsajoje (angl. *application programming interface*, API) darbuotojo (angl. *worker*). Vietoj to, kiekvieną kartą, turinio scenarijus yra pridedamas į puslapį. *Worker* susijęs su puslapio tiekimu į „page–mod“ savo *onAttach* funkciją. Pateikiant tikslą šiai funkcijai į „page–mod“ konstruktorius gali užsiregistruoti, bei gauti įvykius iš turinio scenarijaus ir nurodyti į darbuotoją taip, kad skleisti įvykius, pavyzdžiui:

```
var pageMod = require('page–mod').PageMod({
  include: ['*'],
  contentScript: pageModScript,
  onAttach: function(worker) {
    worker.port.on('click', function(html) {
      worker.port.emit('warning', 'Spustelėti dar karta negalima');
    });
```

Turinio scenarijus naudoja anotacijas, kurti vartotojo sąsajas, gauti vartotojo įvestis ir išnagrinėti DOM (angl. *Document Object Model*), puslapių kuriuos vartotojas užkrauna. DOM yra

akronimas reiškiantis dokumentų objektų modelį. DOM standartizuoja W3C standartai. Bet kurį HTML dokumentą galima suprasti kaip dokumentą pilną objektų. CSS ir *JavaScript* kalbos keičia HTML objektų parametrus, tai yra HTML DOM leidžia pasiekti, keisti, pridėti ar trinti HTML elementus HTML dokumente. Pagal DOM visas HTML dokumentas yra objektas, o kiekvienas HTML elementas yra vidinis objektas. Pagrindinis modulis yra logika, kuri tarpininkauja tarp skirtingų SDK objektų sąveikos.

Internetinio tinklapio prašymą programavimo sąsaja apibrėžia kaip komplektą įvykių, kurie seka tinklo prašymo gyvavimo ciklą. Galima panaudoti šiuos įvykius, kad stebėti ir analizuoti srautą [36]. Tam tikri sinchroniniai įvykiai (kurie pateikti 16 pav.) leidžia perimti, blokuoti, ar pakeisti prašymą.



16 pav. Internetinio tinklapio prašymo gyvavimo ciklas

5.3. Reliacinių duomenų bazių valdymo sistema *MySQL*

Darbui su duomenimis privatumo ir saugos lygio interneto svetainėse vertinimo sistemos programinės įrangos funkcionavimui užtikrinti naudosime reliacinę duomenų bazių valdymo sistema *MySQL*, nes *MySQL* atviro kodo, lengvai įdiegiama ir administruojama, orientuota į interneto svetainių kūrėjų poreikius, efektyviai dirbanti duomenų bazių valdymo sistema. Ji tiks darbui su duomenimis tiek klientinės prieigos programai, tiek ir visai privatumo ir saugos internete vertinimo sistemos darbui su duomenimis.

MySQL − viena iš reliacinių duomenų bazių valdymo sistemų (liet. santrumpa RDBVS,

angl. RDBMS), palaikanti daugelį naudotojų, dirbanti SQL kalbos pagrindu. *MySQL* yra atviro kodo programinė įranga (GPL ir kitos licencijos). *MySQL* RDBVS veikia daugelyje platformų [37].

Prieigai prie *MySQL* duomenų bazių dažniausiai pasirenkama PHP kalba, ją taip pat galima pasiekti įvairiomis kitomis programinėmis priemonėmis – *C*, *C++*, *C#*, *Java*, *Perl*, *Python* ir kitomis. Kiekvienai šių kalbų sukurtos specialios bibliotekos. Taip pat *MySQL* duomenų bazėms yra sukurta ODBC sąsaja *MyODBC*, leidžianti duomenis pasiekti bet kuria kalba, neturinčia specialios bibliotekos, tačiau palaikančia ODBC komunikavimo mechanizmą. PHP kalba jai parašytas valdymo įrankis *phpMyAdmin*.

Kaip ir kiekvienos reliacinės duomenų bazių valdymo sistemos taip ir *MySQL*‘e duomenis prieinami per lentelių abstrakcijas ir kintamuosius dėmenis, aprašomi ryšiais tarp skirtingų lentelių ar jų dalių. Duomenims įvesti, keisti, ieškoti bei lentelėms ir duomenų bazei valdyti yra naudojama kalba SQL (angl. *Structured Query Language*).

5.4. Paprastasis objekto prieigos protokolas SOAP

Projektuojant kliento ir serverio architektūrą kyla klausimas kaip saugiai keistis pranešimais? Sistemose, kai yra naudojamos ne tik vieno gamintojo technologijos, pranešimus perduoti galima pasinaudojant SOAP standartu. Visa tai leistų ateityje atsiradus poreikiui apjungti su kitomis, netgi heterogeninėmis, sistemomis.

SOAP (angl. *Simple Object Access Protocol*) – standartas nustatantis kaip dvi programos gali tarpusavyje keistis pranešimais. Keli SOAP pranešimai gali būti sinchroniškai arba asinchroniškai susieti tarpusavyje realizuojant užklausą – atsakymas funkcionalumą. Keletas pranešimų gali būti susieti į bendravimą (angl. *Conversation*). SOAP pranešimas sukuriamas programos perduodamus duomenis įvelkant (angl. *wraped*) į standartinį XML pagrindu sukurtą voką. SOAP yra aukštesnio lygio protokolas nei taikomųjų programų, todėl pranešimus gali „nešti“ HTTP, JMS (angl. *Java Messaging Service*), FTP ar net SMTP transporto protokolai.

SOAP pranešimas tai XML dokumentas, kurio struktūra tokia:

- vokas (angl. *Envelope*):
  - antraštė (angl. *Header*) − papildoma informacija, saugos informacija, nuorodos į kitus SOAP pranešimus;
  - kūnas (angl. *Body*) − informacija kurią viena programa perduoda kitai.

SOAP numato standarto išplėtimus panaudojant antraštes. Pats SOAP nedokumentuoja jokių antraščių, tačiau SOAP pateikia nurodymus (angl. *Framework*) pagal kuriuos antraštės turi būti

kuriamos, talpinamos į pranešimus ir apdorojamos. O antraščių turinys ir naudojimas yra tik paslaugos tiekėjo ir jos naudotojo susitarimo reikalas. Pavyzdžiui projekto serveryje gali būti naudojamos tam tikros antraštės užtikrinančias vidaus saugos politikos taisykles (auditą). Kad antraštės nebūtų naudojamos visiškai chaotiškai, standartus kuriančios organizacijos pateikia antraščių panaudojimo tam tikrose plačiai paplitusiose srityse standartus (pvz., OASIS ir WS–Security)

SOAP kūnas − šis SOAP pranešimo elementas yra būtinas. Jame ir patalpinamas SOAP pranešimas skirtas galutiniam tikslui (angl. *Ultimate Endpoint*).

Tam kad dvi bendraujančios programos viena kitą suprastų reikalinga bendra kalba, kuri formaliai aprašytų paslaugą. SOAP atveju tam naudojama WSDL (angl. *Web Service Definition Language*). Galima paskelbti savo paslaugą ir ieškoti reikiamų paslaugų naudojant UDDI (angl. *Universal Description, Discovery and Integration*) paslaugą.

WSDL yra XML dokumentas, kuris aprašo paslaugą. Jos pasiekimo adresą, metodus, jų parametrus ir rezultatus. Dalis aprašų yra abstraktūs (nepriklausantys nuo to kur realiai paslauga yra įdiegta), kita dalis aprašo konkretaus paslaugos įdiegimo parametrus.

SOAP standartas tiesiogiai nereglamentuoja jokių saugos klausimų. Jis visiškai nekelia jokių reikalavimų pranešimų perdavimo patikimumui, konfidencialumui, integralumui, tranzakcijų palaikymui. Standartas tik numato išplėtimo mechanizmus kurie gali padėti išspręsti įvairias ateityje kylančias problemas, tame tarpe ir saugos.

SOAP numato du esminius pranešimo apdorojimo mazgus – pirminį siuntėją ir galutinį gavėją (angl. *Initial Sender and Ultimate Receiver*). Pranešimą papildomai apdoroja ir persiunčia tarpininkai. Jie gali peržiūrėti, bet negali keisti kūno. Kūnas skirtas tik galutiniam gavėjui.

Saugos priemonės SOAP gali būti panaudotos: taikomųjų programų lygyje (paslauga – klientas); SOAP pranešimų lygyje (žiniatinklio paslaugų variklyje), transporto lygyje (HTTP, FTP, SMTP, JMS ir kt., per IP, TCP, SSL) [38]

Yra galimybė panaudoti WS–Security (angl. *Web Services Security*, WSS) – SOAP standarto išplėtimą, kuris aprašo saugos išplėtimus naudojamus SOAP pranešimuose. WSS aprašo saugos antraštes SOAP pranešimuose, kurių pagalba perduodami saugos tvirtinimai (angl. *Security Claim*) skirti pranešimų lygio saugai organizuoti. Be to WSS nustato kaip pasirašyti SOAP pranešimus užtikrinant jų integralumą ir neišsigynimą. Nustato kaip užšifruoti SOAP pranešimą užtikrinant jo konfidencialumą ir palaiko daug įvairių pasirašymo ir šifravimo metodų. WSS apibrėžia kaip prie SOAP pranešimo pridėti saugos žymes (angl. *Security Tokens*): X.509 sertifikatą, kerberos bilietą,

vardą ir slaptažodį, SAML (angl. *Security Assertion Markup Language*) patvirtinimą (kuris aprašo kaip turi būti pateikta autentifikavimo, autorizavimo ir atributų informacija, kuri gali būti panaudota paskirstytos architektūros sistemose). Kadangi WSS veikia pranešimų lygyje, tai jo panaudojimas užtikrina pranešimo saugą nuo siuntėjo iki galutinio gavėjo.

5.5. Išvados

Siekiant, kad kuriama privatumo ir saugos lygio vertinimo interneto svetainėse sistema galėtų būti pritaikoma veikti daugelyje sistemų, tai *Java* programavimo kalba tiks realizuoti serverio daliai, nes šioje programavimo sistemoje programuotojo parašytas kodas kompiliuojamas ne į procesoriui specifinę, o į tarpinę formą, kuri nepriklauso nuo procesoriaus tipo ar operacinės sistemos (OS), todėl iškart tinka vykdyti įvairiose OS ir kompiuterių architektūrose.

Kiekvienai interneto naršyklei reikalingas individualus klientinės privatumo ir saugos lygio vertinimo sistemos dalies pritaikymas. Tad norint, jog kuriama sistema galima būtų naudotis daugelyje operacinių sistemų, realizuojant sistemą pirmiausiai reikia pasirink perspektyvią, populiaria interneto naršyklę, veikiančia daugelyje OS.

MySQL atviro kodo, lengvai įdiegiama ir administruojama, turinti saugumo užtikrinimo priemones, veikianti daugelyje platformų duomenų bazių valdymo sistema. Ji tiks darbui su duomenimis tiek klientinės prieigos programai, tiek ir visam privatumo ir saugos internete vertinimo sistemos darbui su duomenimis.

Kliento ir serverio architektūroje yra poreikis keistis pranešimais. SOAP – standartas nustato kaip dvi programos gali tarpusavyje keistis pranešimais. Šis standartas tinkamas ir heterogeninių sistemų komunikacijai. Keli SOAP pranešimai gali būti sinchroniškai arba asinchroniškai susieti tarpusavyje realizuojant užklausą – atsakymas funkcionalumą. Yra galimybė standartizuotu, kompiuterinei programai suprantamu protokolu, suformuluoti užklausos parametrus. Užklausos rezultatai yra taip pat suformuojami kompiuterinei programai suprantamu protokolu ir siunčiami atgal klausiančiajai sistemai. Be to naudojant SOAP yra galimybė realizuoti saugos priemonės tiek taikomųjų programų lygyje (paslauga – klientas), tiek SOAP pranešimų lygyje (žiniatinklio paslaugų variklyje), tiek ir transporto lygyje (HTTP, FTP, SMTP, JMS, ..., per IP, TCP, SSL). Taip pat yra galimybė pasinaudoti SOAP standarto išplėtimais kaip antai WSS (angl. *Web Services Security*), kuris užtikrina pranešimo saugą nuo siuntėjo iki galutinio gavėjo.

6. Reikalavimai privatumo ir saugos lygio interneto svetainėse vertinimo sistemai

6.1. Funkciniai reikalavimai

1. Kiekvienas vartotojas turi būti priskirtas atitinkamai rolei (eksperto, profesionalo, pažengusiojo, naujoko).

2. Ekspertai, valdytojai turi tūrėti galimybę gauti pranešimus iš sistemos naudotojų.

3. Vartotojai turi turėti galimybę atliktį interneto svetainių vertinimo veiksmus, bei peržvelgti svetainių vertinimo formas.

4. Vartotojui įvertinus *n* interneto svetainių aukštesnės rolės vartotojas turi būti patikrinęs (įvertinęs) bent *n–x* jo įvertinimų, tik tada vartotojas gali būti priskirtas aukštesnei rolei, kurioje vertinimai turi tūrėti ženklesnę reikšmę sistemai.

5. Vartotojų interneto svetainės įvertinimus turi būti galimybė įvertinti kitiems vartotojams (nedaugiau kaip po vieną vertinimą vienai interneto svetainei).

6. Vartotojui atverčiant svetainę, kuria jis pats įvertino turi būti atsižvelgiama į jo vertinimus, tai yra jei jis ją įvertino trečios grėsmės lygio įverčiu, tai šiam vartotojui ši svetainė turi būti blokuojama ir prašoma patvirtinimo tęsti, nors ir iš kitų vartotojų nesulauktą aukšto grėsmės lygio vertinimų.

7. Eksperto vertinimai turi būti išskirti ir pateikiami geriausiai matomoje vietoje.

8. Vienas vartotojas turi turėti teisę įvertinti internetinę svetainę po viena įvertį kiekvienai kategorijai (saugumas, privatumas, e. komercija, turinys).

9. Vienas vartotojas turi turėti teisę įvertinti internetinę svetainę tik viena kartą, vėliau šį įvertinimą jis turi turėti galimybę pakeisti.

10. Projekto programinėje įrangoje turi būti galimybė atšaukti neteisingus vertinimus.

11. Ekspertai turi tūrėti galimybę atrinkti ir peržiūrėti pagal įvairius kriterijus (interneto svetainę, vartotoją) interneto svetainių vertinimo duomenis.

12. Projekto programinė įranga turi turėti galimybę nustatyti ir automatiškai įvesti reikiamus duomenų laukus, taip pat vartotojas turi turėti galimybę juos lengvai ir greitai pakeisti.

6.2. Nefunkciniai reikalavimai

13. Turi būti užtikrinamas informacijos konfidencialumas, prieinamumas ir vientisumas.

14. Sukurta sistema turi dirbti stabiliai, įvertinti vartotojo daromas klaidas (kaip antai: neteisingai įvestus duomenis, ar neleistinų operacijų atlikimą) ir suformuoti vartotojui suprantama klaidos pranešimą.

15. Programa turi naudoti nedidelius sistemos resursus. Ji neturi trukdyti sklandaus kitų programinių paketų, ar operacinės sistemos veikimo.

16. Programa privalo turėti galimybę dirbti nepertraukiamu rėžimu.

17. Programa neturi pažeisti vartotojo teisių į privatumą ir saugumą. Taip pat joje neturi būti žalingų vartotojui programos kodo intarpų (kaip antai: virusų, šnipinėjimų intarpų, saugumo spragų).

18. Programa privalo naudoti tik tuos sisteminius kreipinius, kurie būtini, t.y. prašymus išskirti atmintį, naudotis sistemos resursais. Tačiau joje neturi būti jokių nesankcionuotų sistemos panaudojimų, dėl kurių galėtų sutrikti vartotojo kompiuterio, darbinės stoties ar serverio darbas.

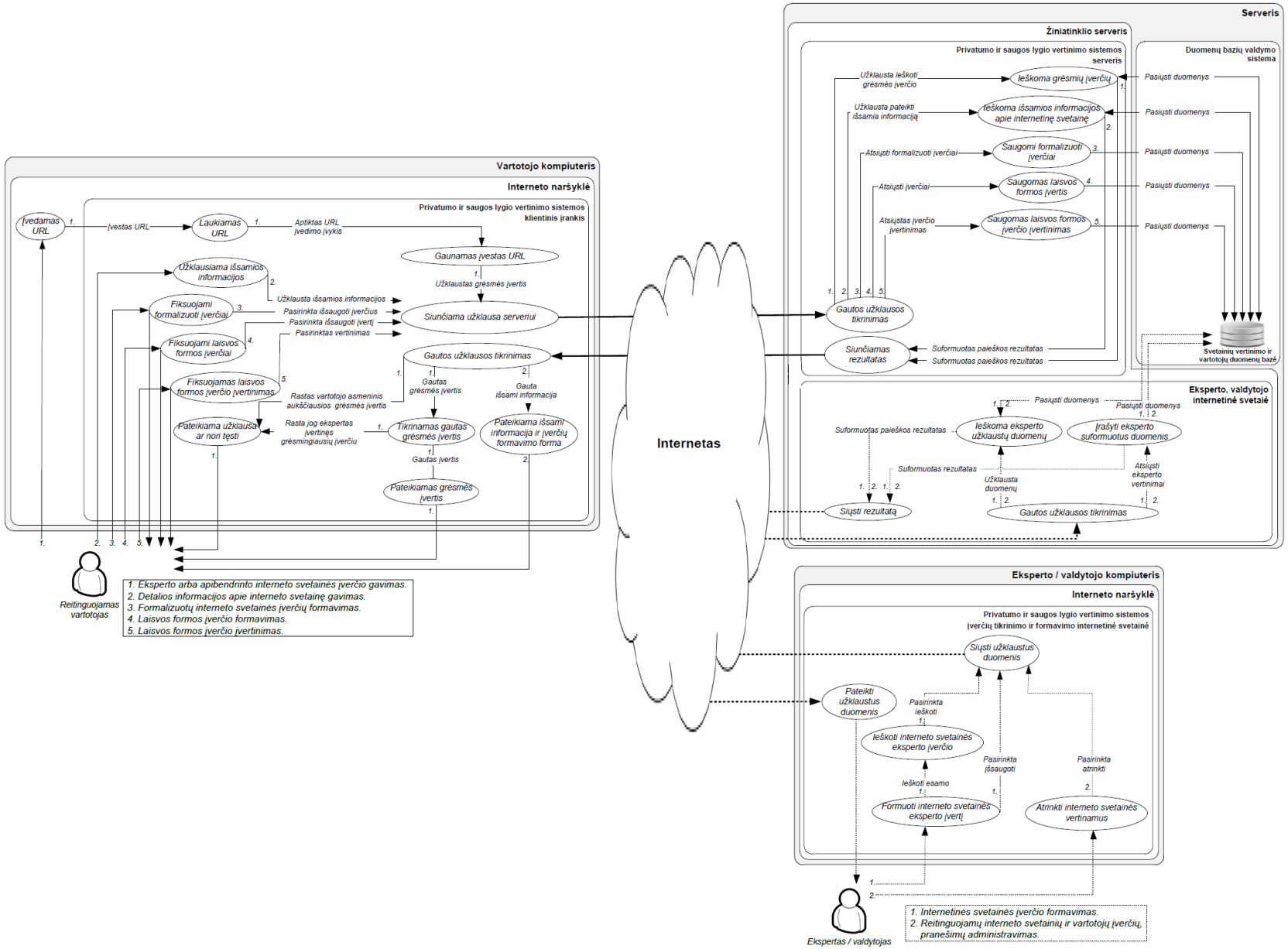
19. Programinė įranga turi būti mobili, patalpinta serveryje ir pasiekiama vartotojams per internetą naudojantis interneto naršykle.

20. Programa turėtu veikti populiariosiose operacinėse sistemose: *Windows*, *Linux*, *Mac OS*.

7. Informacinės posistemės projektas

7.1. Koncepcinis modelis

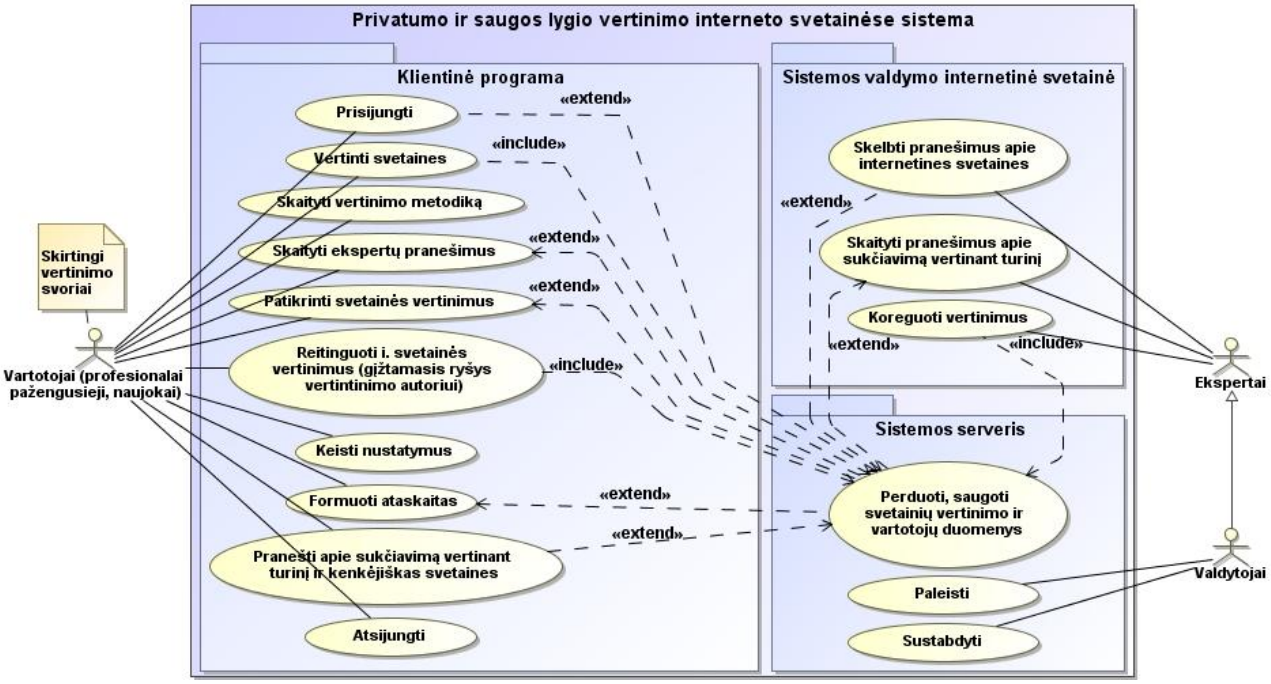
Privatumo ir saugos lygio interneto svetainėse vertinimo sistema bus sudaryta iš serverio programos, kuri apjungs vartotojų klientines programas ir sistemos duomenų bazes į vieningą sistemą. Pateikiame sistemos įrangos išdėstymo ir funkcijų pasikirstymo koncepcinį modelį (17 pav.). Šis sistemos koncepcinis modelis atspindi sistemos techninės realizacijos infrastruktūrą, sąryšius, bei pagrindinius projektuojamos programinės įrangos komponentus.



17 pav. Funkcijų paskirstymo ir įrangos išdėstymo koncepciniais modelis

7.2. Panaudojimo atvejai

Pateikiame (18 pav.) privatumo ir saugos lygio vertinimo sistemos panaudos atvejų diagramą. Ši UML diagrama aprašo ką projektuojama sistema gali atlikti. Pagrindinis šios diagramos elementas – panaudos atvejis.

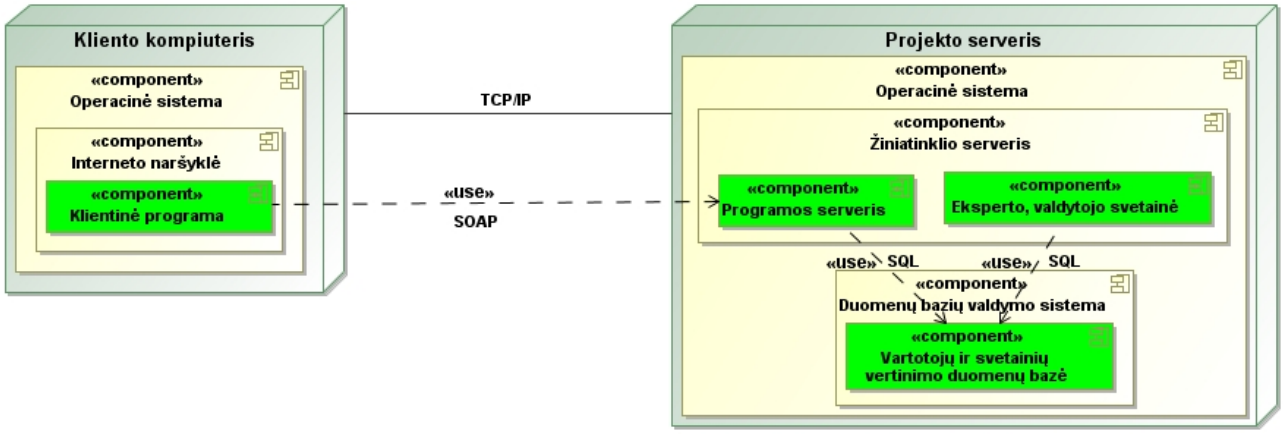


18 pav. Klientinės programos panaudojimo atvejų diagrama

Programos funkcionavimui bus reikalingas serveris, kuris sudarys ryšį tarp vartotojų klientinių programų bei interneto svetainių vertinimo ir sistemos vartotojų *MySQL* duomenų bazių. Ji atliks vartotojų autentifikavimą, interneto svetainių vertinimų įrašymo, modifikavimo, bei duomenų perdavimo klientinės prieigos įrankiui funkcijas. Sistemos valdytojo, panaudos funkcijų atžvilgiu, serverio programa turės paleidimo ir sustabdymo galimybę.

7.3. Sistemos išskaidymas į modulius

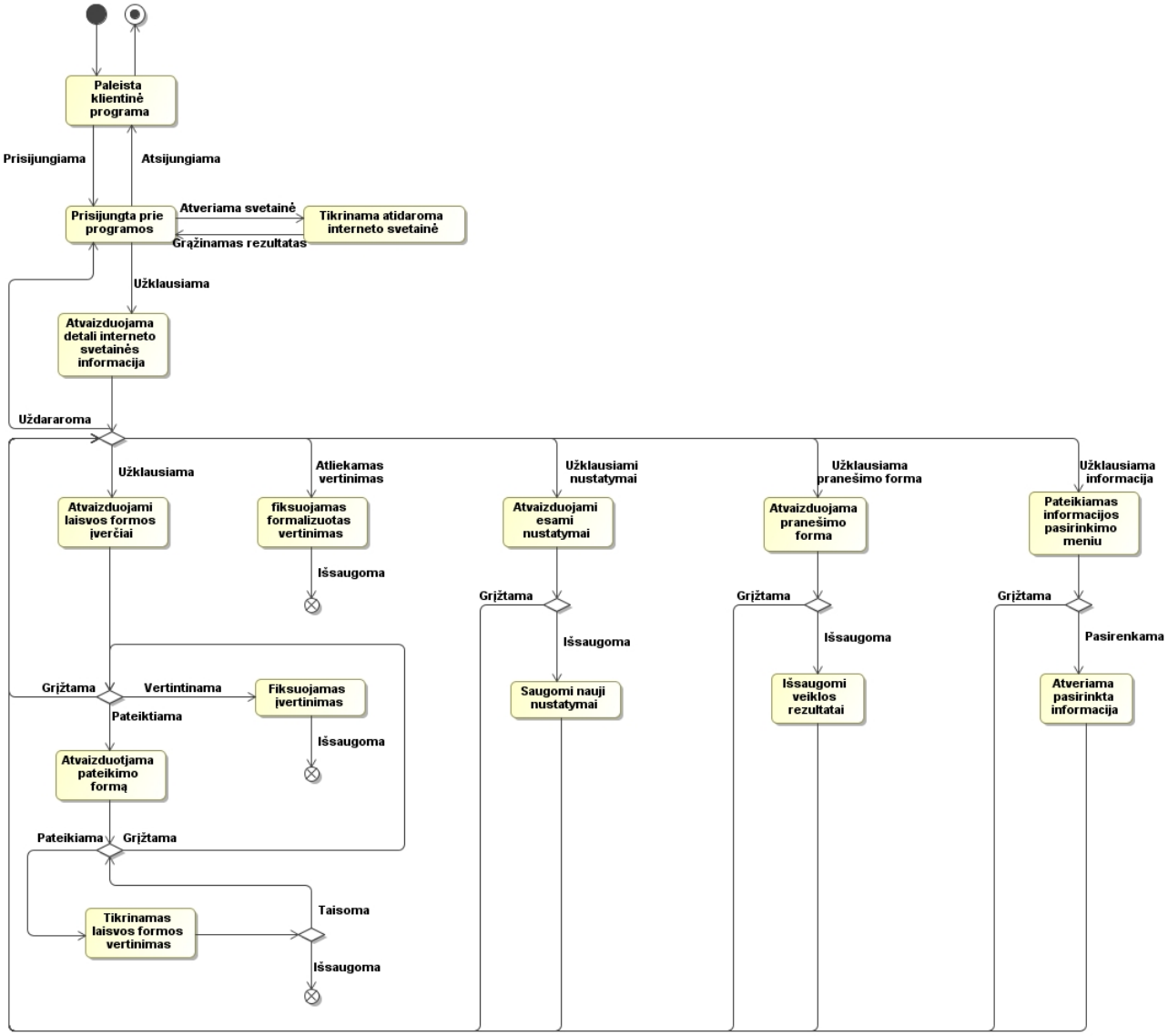
Pateikiame projektuojamos internetinių svetainių vertinimo sistemos išskaidymo į modulius schemą (19 pav.). Joje atvaizduota sistemos techninės realizacijos infrastruktūra, pagrindiniai programinės įrangos komponentai, jų priklausomybės ryšiai, realizacijos technologijos bei protokolai, kuriais jie komunikuos.



19 pav. Svetainių vertinimo sistemos išskaidymo į modulius schema

7.4. Būsenų diagrama

Būsenų diagrama grafiškai atvaizduoja ir parodo modeliuojamų objektų dinamišką elgseną. Šioje (20 pav.) klientinės programos būsenų diagramoje atvaizduojamos būsenų sekos, sąlygos, prie kurių pereinama iš vienos būsenos į kitą, o taip pat veiksmai, kurie atliekami esant konkrečioje būsenoje arba perėjimo metu. Būsenų diagramoje sumodeliuoti, bei atvaizduoti šio projekto objektų gyvavimo etapai.

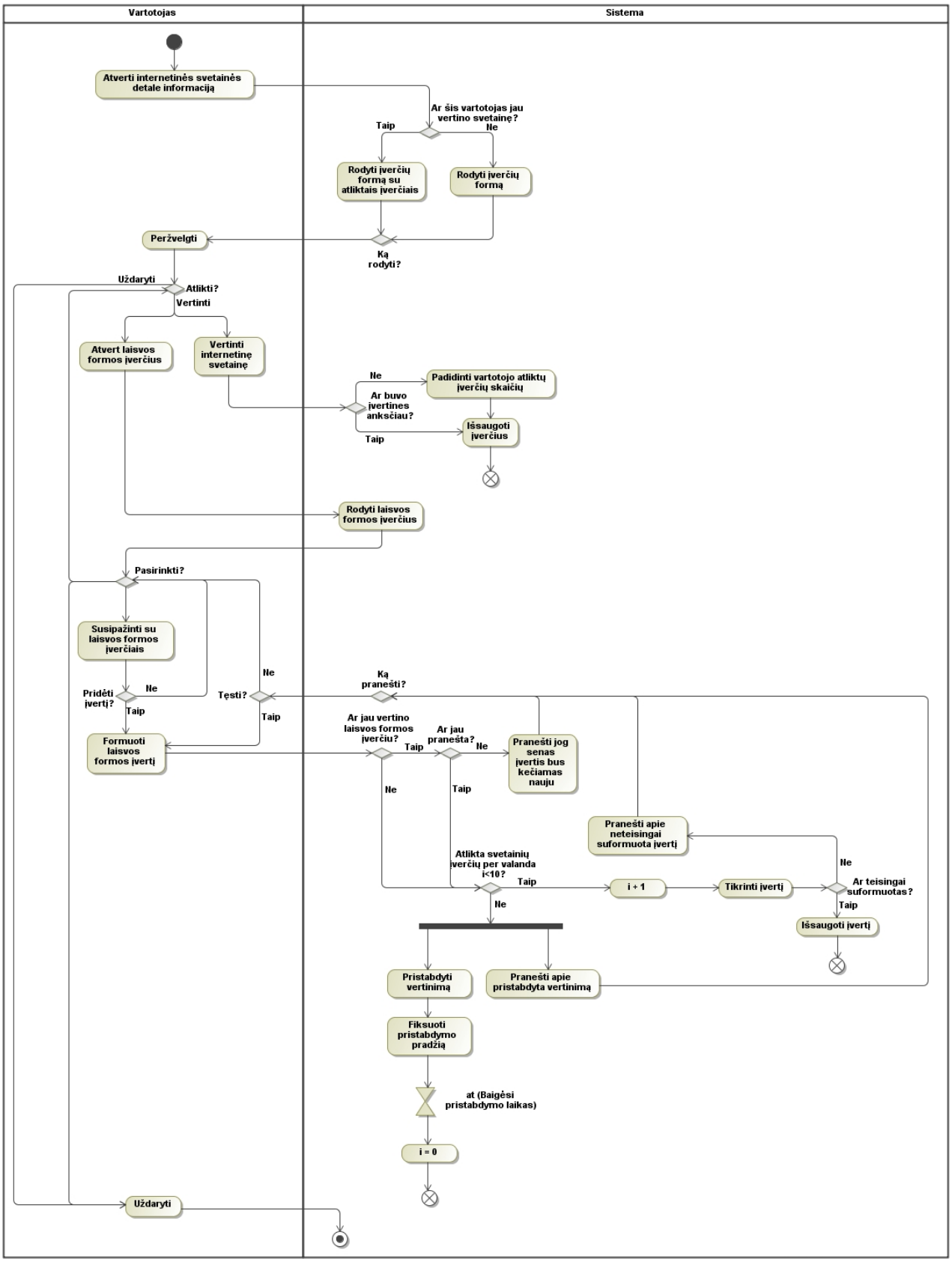


20 pav. Klientinės programos būsenų diagrama

7.5. Veiklos diagramos

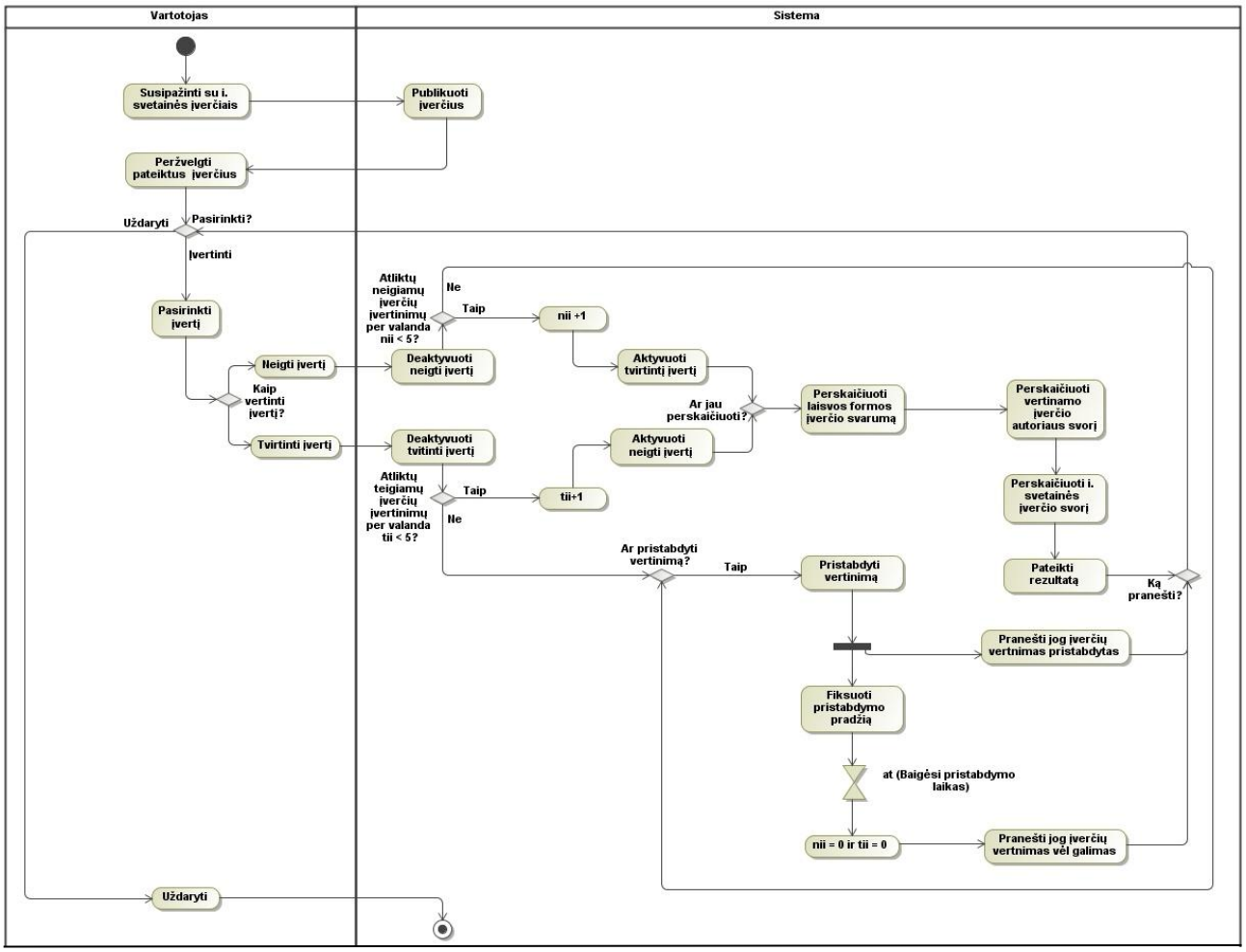
Veikla yra parametrizuota elgesio sekos specifikacija. Ši veiklos diagrama parodo darbų seką nuo pradžios iki pabaigos taško, detalizuojant sprendimo kelius, kurie egzistuoja įvykių, sudarančių veiklą progresijoje. Svetainės įvertinimo (kurio veiklos diagrama pavaizduota 21 pav.)

veikla vyksta taip. Vartotojas paleidęs vykdyti projektinę sistemą ir prie jos prisijungiąs gali parametrizuotai įvertinti internetines svetaines saugumas, privatumas, e. komercija, turinys aspektais. Taip pat jis gali pateikti laisvos formos įvertį.



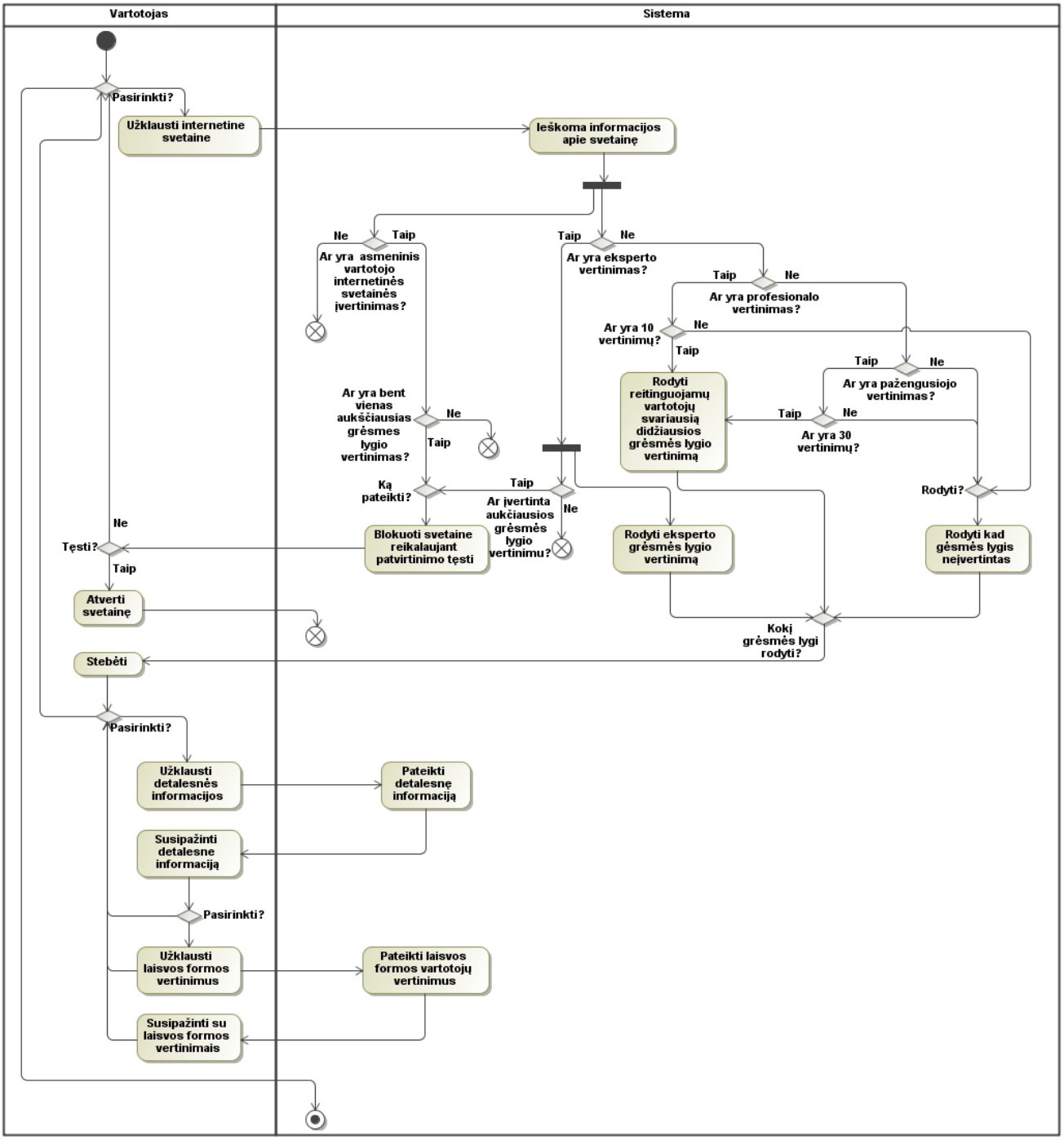
21 pav. Svetainės įvertinimo veiklos diagrama

Sistemos dalyvis gali įvertinti kitų atliktus laisvos formos vertinimus savo svorio koeficientu ir taip padidinti juos atlikusių vertintojų įtaką sistemai. Tai atvaizduoja 22 pav. pateikta veiklos diagrama vartotojo ir projektuojamos sistemos atžvilgiu.



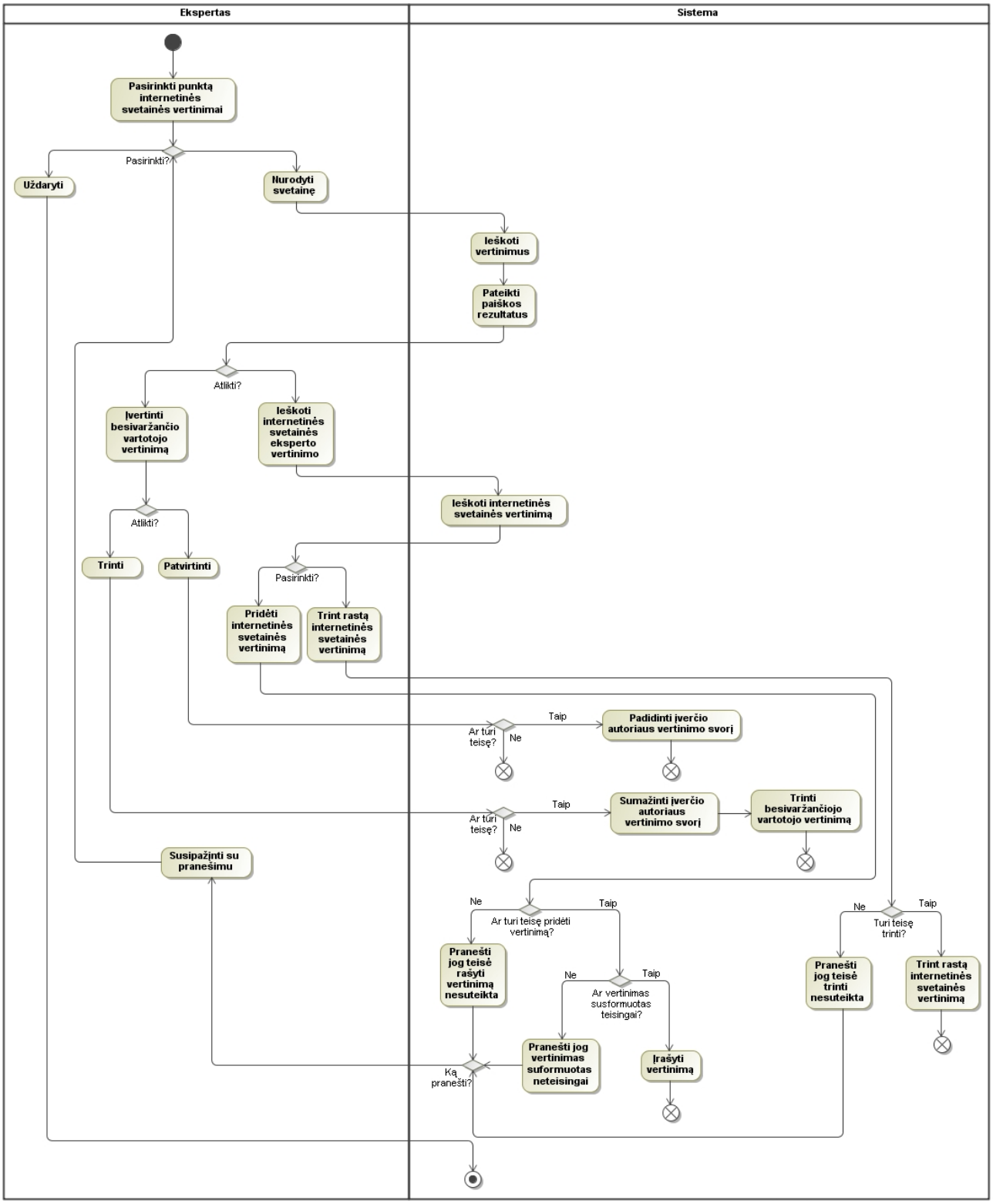
22 pav. Internetinių svetainių laisvos formos įverčių vertinimo veiklos diagrama

Internetinės svetainės grėsmės lygio vertinimo analizės veiklos diagrama, vartotojo ir projektuojamos sistemos atžvilgiu, pavaizduota 23 pav. Čia atsispindi svetainės įverčių glaustos ir išsamios informacijos pateikimo veiklos loginė struktūra.



23 pav. Internetinės svetainės grėsmės lygio vertinimo analizės veiklos diagrama

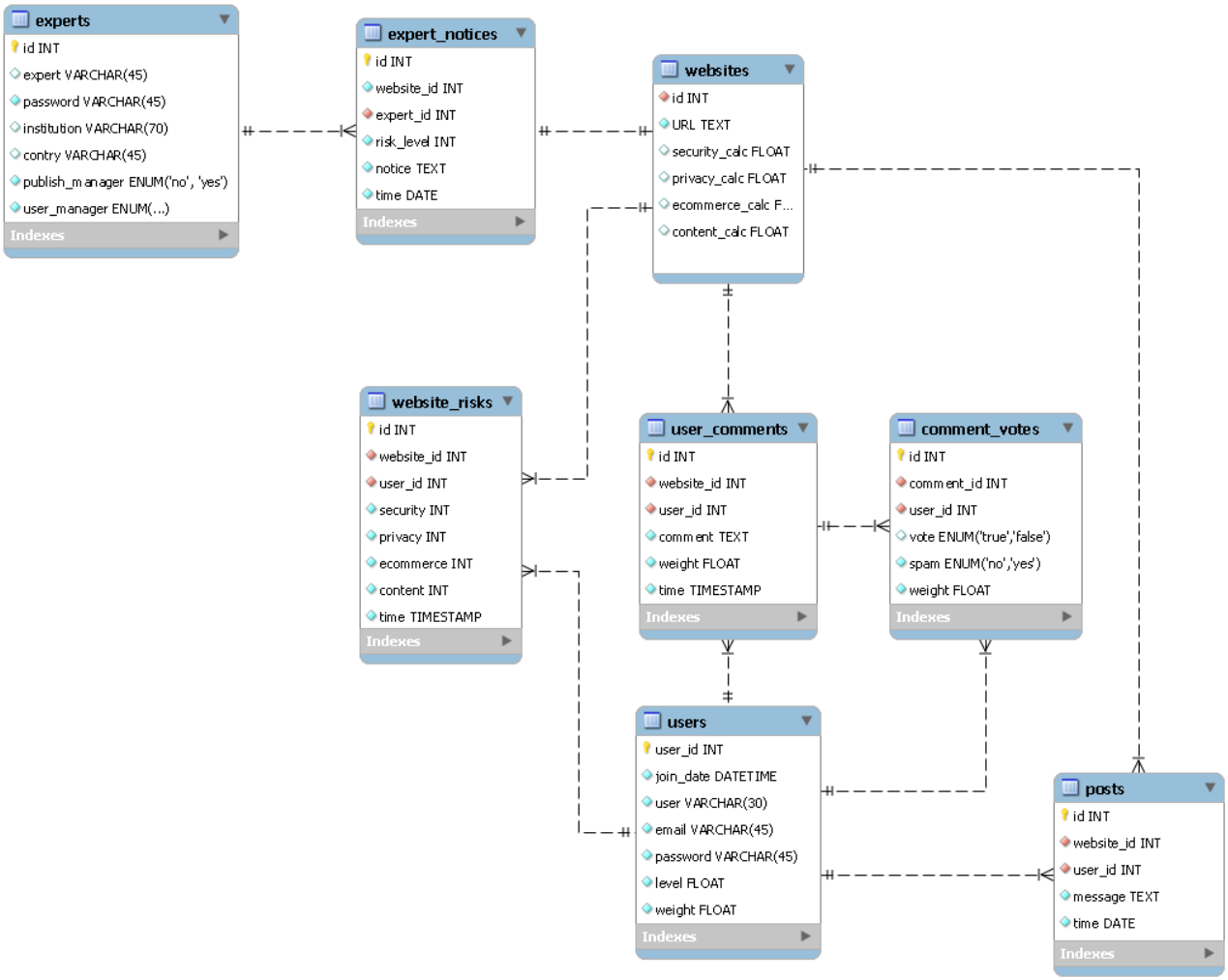
Sistemoje autentifikuoto, turinčio šią privilegiją eksperto internetinės svetainės įvertinimo formavimo, bei besivaržančių vartotojų vertinimo kontrolės veiklos diagrama sistemos atžvilgiu atvaizduota 24 pav.



24 pav. Eksperto vertinimų formavimo veiklos diagrama

7.6. Duomenų bazės schema

Privatumo ir saugos lygio interneto svetainėse vertinimo sistemos projekto duomenų bazė saugos vartotojų vertinimas svetaines, jų vertinimus ir vartotojų sąrašus. Šios duomenų bazės schema pateikta 25 pav. Pastarajame paveikslėlyje pateikti lentelių pavadinimai ir saugomi įrašai, bei ryšys tarp šių lentelių.



25 pav. Vartotojų ir svetainės vertinimų duomenų bazės schema

Lentelė *websites* saugos vertinamų interneto svetainių sąrašus. Ją sudarys tokie atributai:

- *id* − esybės identifikavimui, jos išskyrimui iš kitų tos esybės objektų, vartojamas raktas, kuris vienareikšmiškai apibrėš bet kurį esybės objektą (atributą);
- *URL* − atributas saugosiantis svetainės URL;
- *security_calc* – atributas saugosiantis apskaičiuotą saugumo reitingą;
- *privacy_calc* − atributas saugosiantis apskaičiuotą privatumo reitingą;
- *ecommerce_calc* − atributas saugosiantis apskaičiuotą e. komercijos reitingą;

- *content_calc* − atributas saugosiantis apskaičiuotą interneto svetainėje pateikto turinio reitingą.

Lentelė *experts* saugos ekspertų ir valdytojų sąrašus. Ją sudarys tokie atributai:

- *id* − esybės identifikavimui, jos išskyrimui iš kitų tos esybės objektų, vartojamas raktas, kuris vienareikšmiškai apibrėš bet kurį esybės objektą (atributą);
- *expert* − atributas saugosiantis naudotojo tapatybę;
- *passsword* − atributas saugosiantis naudotojo slaptažodį;
- *institution* − atributas saugosiantis naudotojo atstovaujamos institucijos pavadinimą;
- *contry* − atributas saugosiantis naudotojo atstovaujama šalį;
- *publish_manager* − atributas saugosiantis ar naudotojas gali skelbti, trinti, redaguoti ekspertų pranešimus;
- *user_manager* − atributas saugosiantis ar naudotojas galį valdyti kitų reitinguojamų vartotojų vertinimus.

Lentelė *expert_notices* saugos ekspertų pranešimus, apie internetines svetaines. Ją sudarys tokie atributai:

- *id* − esybės identifikavimui, jos išskyrimui iš kitų tos esybės objektų, vartojamas raktas, kuris vienareikšmiškai apibrėš bet kurį esybės objektą (atributą);
- *website_id* − atributas saugosiantis eksperto vertinamos interneto svetainės identifikacinį numerį;
- *risk_level* − atributas saugosiantis eksperto įvertinta saugumo lygį;
- *notice* − atributas saugosiantis eksperto pranešimą;
- *time* − atributas saugosiantis eksperto pranešimo laiką.

Lentelė *users* saugos sistemos vartotojų sąrašus. Ją sudarys tokie atributai:

- *user_id* − esybės identifikavimui, jos išskyrimui iš kitų tos esybės objektų, vartojamas raktas, kuris vienareikšmiškai apibrėš bet kurį esybės objektą (atributą);
- *join_date* − atributas saugosiantis vartotojo pirmojo prisijungimo data, laiką prie projekto svetainės;
- *user* – atributas saugosiantis vartotojo vardą;
- *email* – atributas saugosiantis vartotojo elektroninio pašto adresą;
- *password* – atributas saugosiantis vartotojo slaptažodį;
- *level* – atributas saugosiantis reitinguojamo vartotojo lygio reikšmę (įtakos sistemai dydį);

- *weight* – atributas saugosiantis apskaičiuota reitinguojamo vartotojo svorį (įtakos sistemai matą);

Lentelė *website_risks* saugos interneto svetainės lankytojų formalizuotos formos vertinimus. Ją sudarys tokie atributai:

- *id* − esybės identifikavimui, jos išskyrimui iš kitų tos esybės objektų, vartojamas raktas, kuris vienareikšmiškai apibrėš bet kurį esybės objektą (atributą);
- *website_id* − atributas saugosiantis reitinguojamos interneto svetainės identifikacinį numerį;
- *user_id* − atributas saugosiantis įvertį atlikusio sistemos vartotojo identifikacinį numerį;
- *security* − atributas saugosiantis saugumo grėsmės lygio įvertį;
- *privacy* − atributas saugosiantis privatumo grėsmės lygio įvertį;
- *ecommerce* − atributas saugosiantis e. komercijos grėsmės lygio įvertį;
- *content* − atributas saugosiantis turinio grėsmės lygio įvertį;
- *time* − atributas saugosiantis įverčio suformavimo laiką.

Lentelė *user_comments* saugos laisvos formos interneto svetainės lankytojų vertinimus. Ją sudarys tokie atributai:

- *id* − esybės identifikavimui, jos išskyrimui iš kitų tos esybės objektų, vartojamas raktas, kuris vienareikšmiškai apibrėš bet kurį esybės objektą (atributą);
- *website_id* − atributas saugosiantis reitinguojamos interneto svetainės identifikacinį numerį;
- *user_id* − atributas saugosiantis laisvos formos įvertį atlikusio vartotojo identifikacinį numerį;
- *comment* – atributas saugosiantis reitinguojamo vartotojo laisvos formos įvertį;
- *weight* − atributas saugosiantis laisvos formos įverčio svorį, kuris bus apskaičiuojamas iš komentarą įvertinusių reitinguojamų vartotojo svorio koeficiento;
- *time* − atributas saugosiantis laisvos formos įverčio suformavimo laiką.

Lentelė *comment_votes* saugos laisvos formos interneto svetainės lankytojų vertinimų vertinimus. Ją sudarys tokie atributai:

- *id* − esybės identifikavimui, jos išskyrimui iš kitų tos esybės objektų, vartojamas raktas, kuris vienareikšmiškai apibrėš bet kurį esybės objektą (atributą);
- *comment_id* − atributas saugosiantis laisvos formos įverčio identifikacinį numerį;

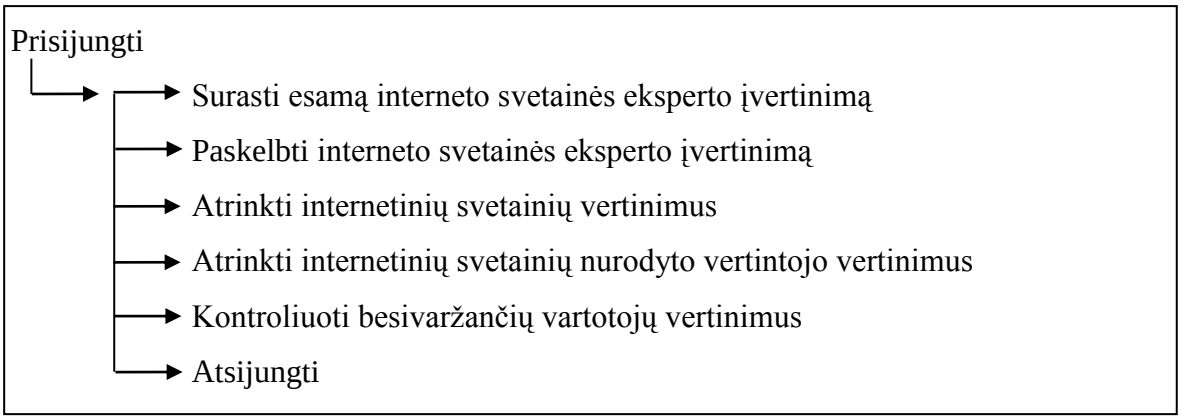
- *user_id* − atributas saugosiantis vartotojo atlikusio laisvos formos įverčio vertinimą identifikacinį numerį;
- *vote* − atributas saugosiantis laisvos formos įverčio, reitinguojamo vartotojo išreikštą, vertinimą;
- *spam* − atributas saugosiantis žymą ar šis laisvos formos įvertis neprieštarauja etikos, moralės normoms.
- *weight* − atributas saugosiantis laisvos formos įverčiui formuojama svorį.

Lentelė *posts* saugos vartotojų prašytus pranešimus, projekto valdytojam. Ją sudarys tokie atributai:

- *id* − esybės identifikavimui, jos išskyrimui iš kitų tos esybės objektų, vartojamas raktas, kuris vienareikšmiškai apibrėš bet kurį esybės objektą (atributą);
- *website_id* − atributas saugosiantis reitinguojamos interneto svetainės identifikacinį numerį;
- *user_id* − atributas saugosiantis vartotojo paskelbusio pranešimą sistemos valdytojam identifikacinį numerį;
- *message* − atributas saugosiantis vartotojo pranešimą sistemos valdytojam;
- *time* − atributas saugosiantis pranešimą data ir laiką.

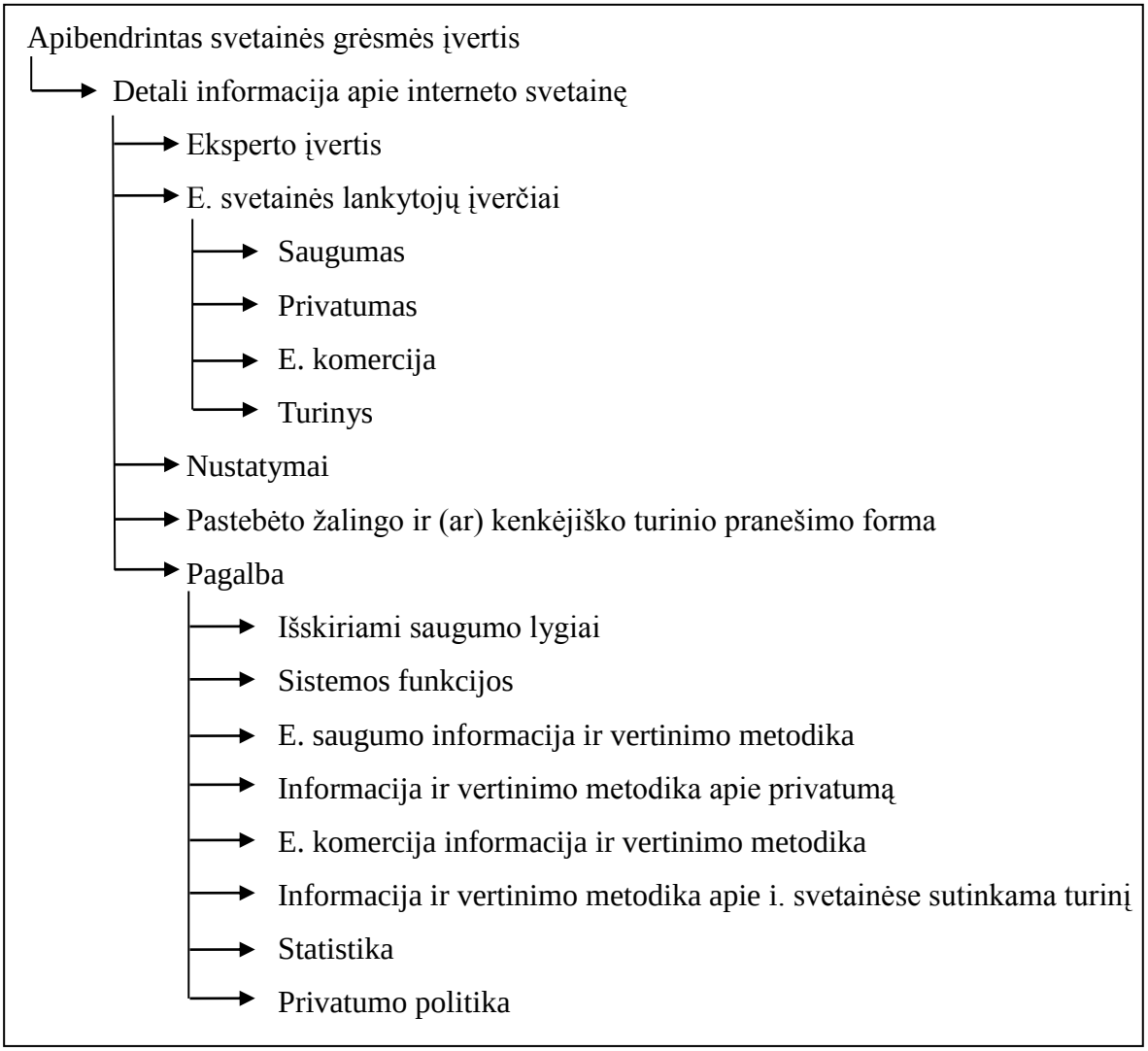
7.7. Langų išdėstymo projektai

Ekspertams, valdytojams skirtoje sistemos valdymo svetainėje. Ekspertai galės atrinkti svetainių vertinimus, bei paskelbti savo pranešimus apie interneto svetaines 26 pav.



26 pav. Ekspertų, valdytojų meniu

Klientinę programą paleidę ir prie jos prisijungę vartotojai galės matyti, valdyti visas pavaizduotas funkcijas pavaizduotas 27 pav.



27 pav. Klientinės vartotojų programos langų navigacija

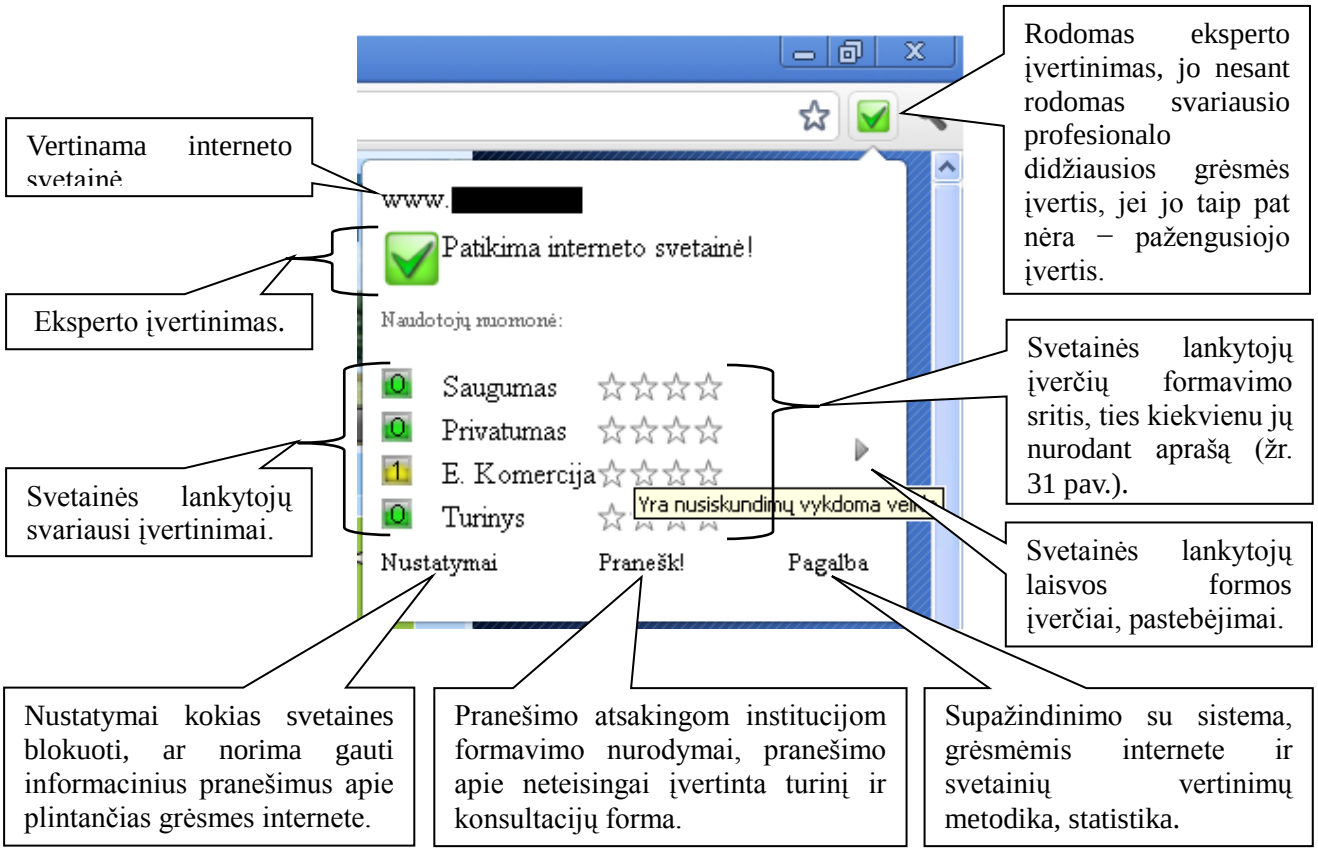
III. EKSPERIMENTINIS PRIVATUMO IR SAUGOS INTERNETE APSAUGOS MODELIS

8. Veikimo aprašymas

Sistemos veikimas pagrįstas principu, jog informacijos apsauga – žmonių problema, saugumas labiausiai priklauso nuo kiekvieno vartotojo ir jų bendradarbiavimo tarpusavyje. Sistemos dalyviai dalinasi patirtimi apie konkrečias interneto svetaines. Sistemoje išskiriamos vartotojų rolės. Atsižvelgiama į aukščiausių rolių vertinimus pateikiant grėsmės lygi interneto svetainėse. Vartotojų – vertintojų įtaka sistemai didėja, kai jo vertinimą patvirtina kitas atitinkamo reitingo vartotojas savo vertinimo svorio koeficientu. Tikimasi jog svetainių vertinimai leis greičiau pastebėti netinkamo turinio, kenkėjiškas internetines svetaines ir imtis reikiamų priemonių.

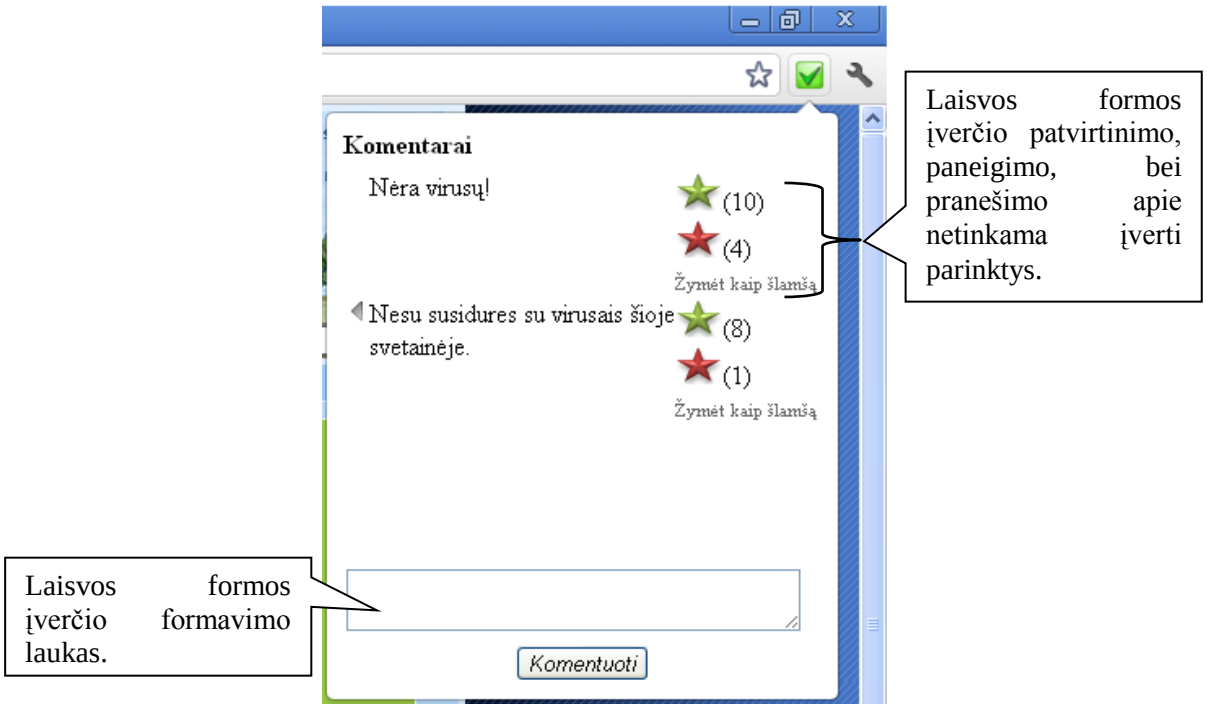
9. Savybių analizė

Atverdami privatumo ir saugos lygio vertinimo įrankį interneto naršyklėje (28 pav.) jo vartotojai gali susipažinti su šiomis savybėmis: interneto svetainės detalizuota grėsmės įverčių ataskaita, ekspertų ir svetainės lankytojų įverčiai. Taip pat gali įvertinti tuo metu naršyklėje atidarytą internetinę svetainę.



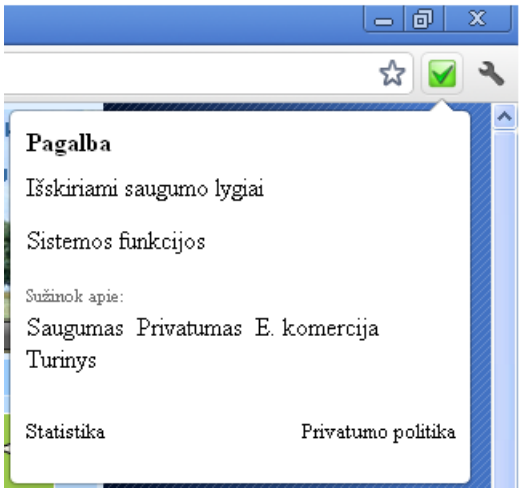
28 pav. Svetainės įverčių peržiūros ir formavimo langas

Privatumo ir saugos lygio vertinimo sistemos naudotojai taip pat gali pateikti laisvos formos įverčius, pastebėjimus (29 pav.). Peržiūrėti kitų naudotojų pastebėjimus, bei juos partvirtinti, paneigti ir taip suteikti įverti atlikusio naudotojo vertinimui ir pačiam vartotojui atitinkama įtaka sistemai (padidinti ar sumažinti vartotojo vertinimo svorį savo svorio koeficientu).



29 pav. Svetainės lankytojų laisvos formos įverčiai, pastebėjimai

Atvėrus langą „pagalba“ (30 pav.) galima sužinoti išskiriamus grėsmių lygius (31 pav.), sistemos funkcijas, susipažinti su e. erdvėje sutinkamomis grėsmėmis ir internetinių svetainių vertinimo metodika (žr. 1 priedas).



30 pav. Programos langas „pagalba“

Internetinių svetainių vertinimo aspektai

Išskiriami saugumo grėsmių lygiai su kuriais susiduriama naršant internetinėse svetainėse.

Grėsmės lygis: vatotojų vertinimai / atsakingų institucijų pranešimai	Saugumas	Privatumas	E. komercija	Turinys
3: 3 / STOP	Aukščiausias virusų, kenkėjiško kodo grėsmės lygis (automatins užkrėtimas)	Kaupia duomenis neapibrėžtą laiką, neaiškiem tikslam. Neužtikrinamas duomenų konfidencialumas	Sukčiavimas	Raginama prievarta, prieštaraujama LR santvarkai, propaguojama ar reklamuojama pornografija, žalingi įpročiai ir jų medžiagos
2: 2 / !	Vidutinis virusų, kenkėjiško kodo grėsmės lygis (užkrėtimas po atlikto veiksmo)	Teikia vartotojų duomenis tretiesiems asmenims	Nepatenkinamai vykdoma veikla	Autorių teisių ir gretutinių teisių pažeidimai
1: 1 / !	Nedidelis virusų, kenkėjiško kodo grėsmės lygis (neprašyta veikla)	Neskelbia privatumo politikos	Yra nusiskundimų vykdoma veikla	Dezinformacija
0: 0 / ✓	Nėra virusų, kenkėjiško kodo grėsmės	Atitinka lūkesčius	Veikla vykdoma puikiai	Atitinka leistinas normas
?: ? / -	Nėra vertinimų!			

31 pav. Išskiriami grėsmių lygiai ir jų žymėjimas sistemoje

10. Testavimo modelis ir duomenys, kontrolinis pavyzdys

Ekspertas naudodamasis privatumo ir saugos lygio vertinimo sistemą gali atlikti svetainės įvertinimą atskirai nuo kitų sistemos naudotojų įrašydamas duomenų bazėje interneto svetainės domeną, grėsmės lygį ir komentarą (32 pav.).

Sistemos teisingumo valdymas

Kontroliuokite šioje sistemoje pateikiamų įverčių teisingumą.

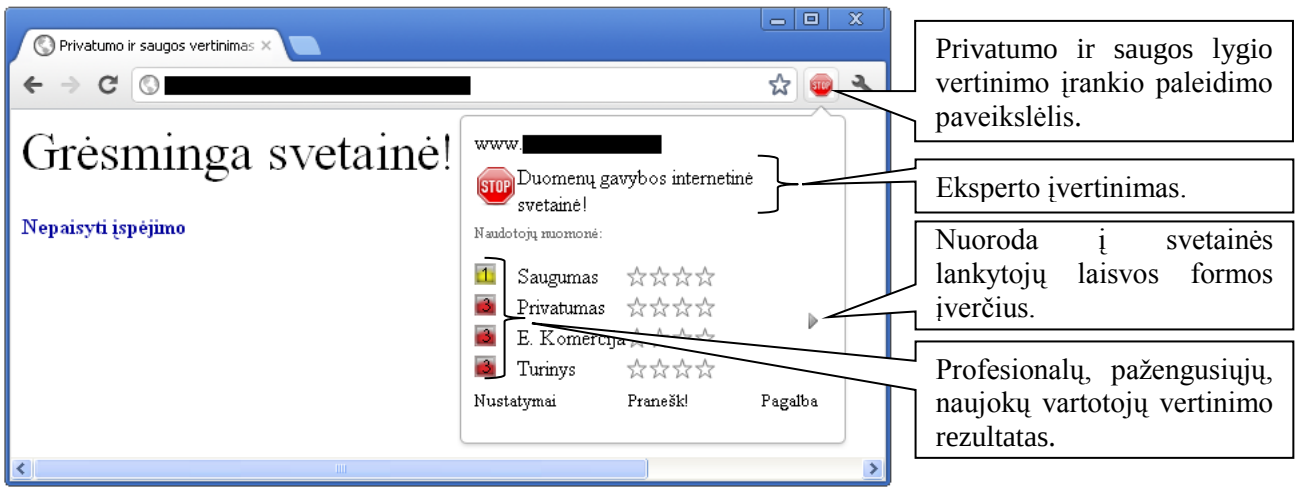
Pateikti vertinimą:

Internetinės svetaiės domenas	Grėsmės lygis	Komentaras	Veiksmai
[redacted] Ieškoti	3	Duomenų gavybos internetinė svetainė!	Pridėti Trinti

32 pav. Eksperto svetainės vertinimo langas

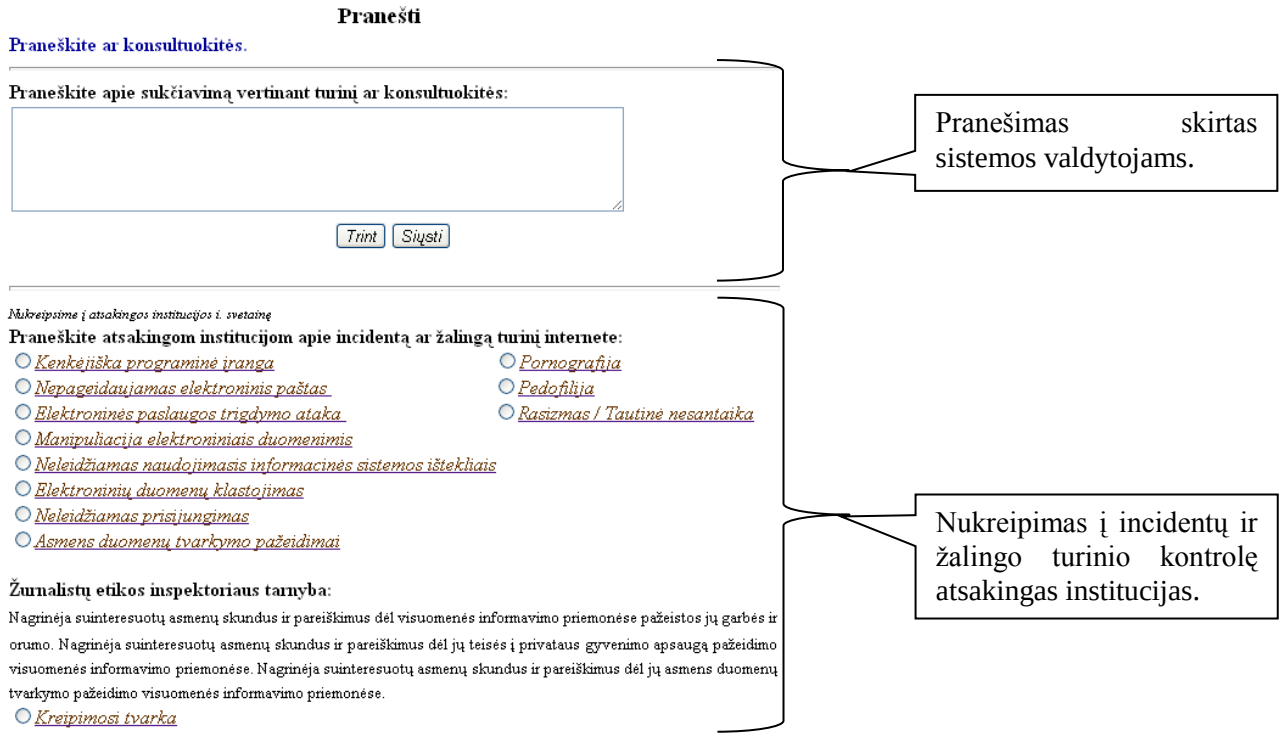
Klientinė privatumo ir saugos lygio vertinimo programa veikianti vartotojo naršyklėje stebi atverčiamus internetinius puslapius ir tikrina ar duomenų bazėje nėra atsiliepimų. Aptikus jog užklausiama internetinė svetainė, kuri įvertinta eksperto aukščiausia 3 lygio grėsme (žr. 31 pav.) internetinė svetainė blokuojama ir reikalaujama patvirtinimo tęsti (pvz. 33 pav.). Kitu grėsmės

įverčių atvejų (taip pat visų kitų sistemos dalyvių vertinimo atvejų) keičiamas tik grėsmės lygį atspindintis privatumo ir saugos lygio vertinimo įrankio paleidimo paveikslėlis.



33 pav. Eksperto įvertintos grėsmingiausiu lygiu internetinės svetainės blokavimas

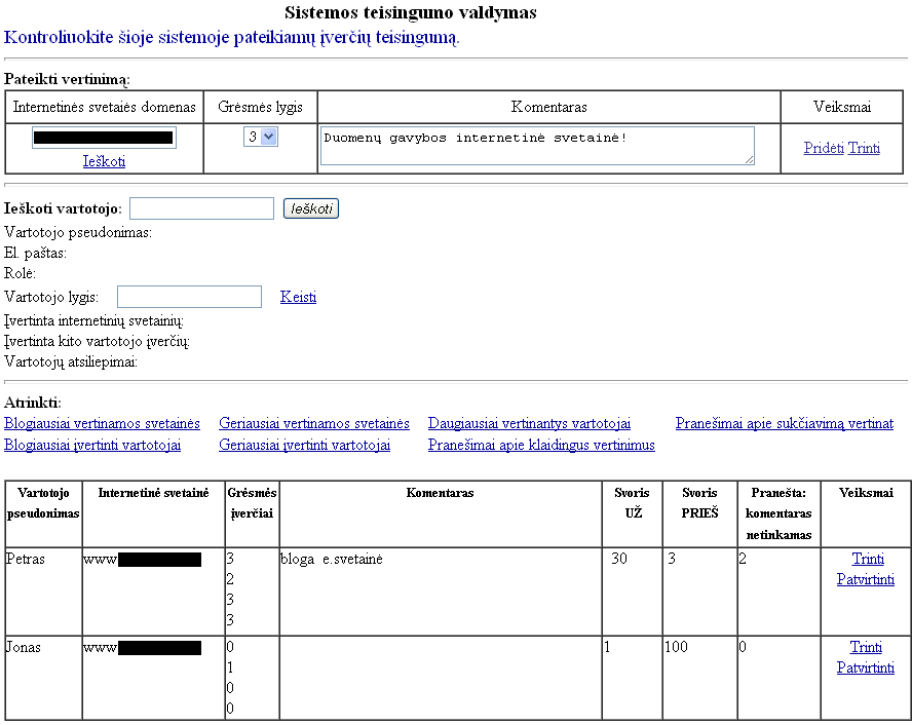
Sistemos naudotojas naršydamas internete gali įvertinti svetainę, t. y. pranešti apie neteisinga privatumo ir saugos lygio vertinimo sistemos veikimą (34 pav.), pranešti atsakingosiom institucijom apie incidentą ar žalingą turinį internete (nukreipiama į atsakinga instituciją).



34 pav. Svetainės su ypač blogu įverčiu blokavimas

Realizuota galimybė atrinkti stipriausius vartotojų vertinimus, peržiūrėti jų teisingumą, apsvarstyti reikalingų priemonių taikymą interneto svetainės, ar tik šio vertinimo (taikant gįžtamąjį ryšį ir sumažinant neteisingą įvertį atlikusio vartotojo įtaką sistemai) pašalinimui. Esant poreikiui

sistemos valdytojai gali valdyti sistemos teisingumą keisti besivaržančių vartotojų (profesionalų, pažengusiųjų, naujokų) įtaką sistemai keisdami vertinimo svorius (35 pav).



Sistemos teisingumo valdymas

Kontroliuokite šioje sistemoje pateikiamų įverčių teisingumą.

Pateikti vertinimą:

Internetinės svetainės domenas	Grėsmės lygis	Komentaras	Veiksmai
[redacted] Ieškoti	3	Duomenų gavybos internetinė svetainė!	Pridėti Trinti

Ieškoti vartotojo: Ieškoti

Vartotojo pseudonimas:
El. paštas:
Rolė:
Vartotojo lygis: Keisti
Įvertinta internetinių svetainių:
Įvertinta kito vartotojo įverčių:
Vartotojų atsiliepimai:

Atrinkti:

Blogiausiai vertinamos svetainės | Geriausiai vertinamos svetainės | Daugiausiai vertinantys vartotojai | Pranešimai apie sukčiavimą vertinat
Blogiausiai įvertinti vartotojai | Geriausiai įvertinti vartotojai | Pranešimai apie klaidingus vertinimus

Vartotojo pseudonimas	Internetinė svetainė	Grėsmės įverčiai	Komentaras	Svoris UŽ	Svoris PRIEŠ	Pranešta: komentaras netinkamas	Veiksmai
Petras	www[redacted]	3 2 3 3	bloga e.svetainė	30	3	2	Trinti Patvirtinti
Jonas	www[redacted]	0 1 0 0		1	100	0	Trinti Patvirtinti

35 pav. Teisingo sistemos veikimo kontroliavimo langas

IV. EKSPERIMENTINĖS PRIVATUMO IR SAUGOS LYGIO INTERNETO SVETAINĖSE VERTINIMO SISTEMOS TYRIMAS

11. Privatumo ir saugos lygio interneto svetainėse vertinimo sistemos įvertinimas

Naudojantis eksperimentine privatumo ir saugos lygio interneto svetainėse vertinimo sistema yra galimybė publikuoti esama ekspertų informaciją reikiamu momentu (užklausiant konkrečią internetinę svetainę). Tokiu būdu visuomenei ekspertai gali pateikti ir informaciją apie neteisėtą turinį aptiktą šalyse, kuriose toks turinys nėra laikomas neteisėtu.

Eksperimentinėje privatumo ir saugos lygio interneto svetainėse vertinimo sistemoje vartotojai turi galimybe įvertinti, išreikšti nuomone apie konkrečia internetinę svetainę. Yra galimybė šios sistemos valdytojams atrinkti stipriausius vartotojų vertinimus, peržiūrėti jų teisingumą, apsvarstyti reikalingų priemonių taikymą interneto svetainės, ar tik šio vertinimo pašalinimui. Esant poreikiui, sistemos valdytojai gali valdyti sistemos teisingumą, koreguoti besivaržančių vartotojų − vertintojų (profesionalų, pažengusiųjų, naujokų) įtaka sistemai keisdami vertinimo svorius.

Eksperimentinėje privatumo ir saugos lygio interneto svetainėse vertinimo sistemoje turinį sureitinguoja patys vartotojai. Tuo tarpu turinio parinkėjai naudojantys interneto turinio parinkimo platformą (angl. *Platform for Internet Content Selection*) pagrįsti žymų skaitymu įterptų į turinį, kurias įterpia patys turinio kūrėjai. Vien tik turinio kūrėjo žymėjimas negali duoti visiško nepageidaujamo turinio blokavimo, nes kūrėjas gali nuspręsti ignoruoti, ar tiesiog žymėti neteisingai kai kurias žymes.

Privatumo ir saugos lygio interneto svetainėse vertinimo sistema suteikia galimybę visuomenei dalyvauti visame viešosios paslaugos (kovos su neteiktinu turiniu internete) teikime jį reitinguojant. Vartotojui, siekiančiam elektroniniu būdu gauti viešąją paslaugą (informaciją apie lankomą internetine svetainę), nereikia atlikti ilgai trunkančių formalių procedūrų.

4 lentelė. Panašių sistemų savybių palyginimas

	Interneto turinio parinkimo platforma (PICS) pagrįsti turinio parinkėjai*	**Turinio parinkėjai pargrįsti žodyno filtravimo taikymu***	**Privatumo ir saugos lygio interneto svetainėse vertinimo sistema**
Klaidingo suveikimo rizika	Klaidingas turinio žymėjimas ir nežymėtas turinys	Žodžiai paveikslėliuose, bei filtravimo pagal žymenis netobulumas (klaidingi žymenys, ar klaidingas suveikimas)	Neteisingas vertinimas (nežymėtas turinys ir žymėtas naujoko laikomas (t. y. žymimas) įtartinu)
Informacijos pateikimas apie užklaustą internetine svetainę	Blokuojama nepageidaujamo turinio interneto svetainė	Blokuojama nepageidaujamo turinio interneto svetainė	Esant pateikiamas eksperto vertinimas, pateikiami svariausių vertintojų svariausi vertinimai
Turinio klasifikavimo, kuri atlieka vartotojas, poveikis	Vietinis**	Vietinis	Vietinis (blokuojama aukščiausia grėsme įvertintos svetainės), globalus (pridedamas prie kitų vertinimų)
Žinių, patirties sklaida	Ne	Ne	Taip (formalizuoti ir laisvos formos įverčiai)

* Pateikta remiantis bendrais veikimo principai, tad galimos išimtys konkrečios sistemos atveju.

** Interneto turinio parinkimo platforma (PICS) pagrįsti turinio parinkėjai turi tik papildomas žodyno ir URL filtravimo galimybes, t. y. turinio klasifikavimo, kuri atlieka vartotojas pagal asmeninius poreikius poveikis tik jam pačiam.

Privatumo ir saugos lygio vertinimo sistema kaip ir bet kuri sistema turi riziką būti pažeista. Taip pat ši sistema gali susilaukti piktybiškų vertinimų, tad gali būti reikalingas pastovus sistemos valdytojų įsikišimas kontroliuojant sistemos teisingumą.

12. Sistemos taikymo rekomendacijos

Interneto svetainių reitingavimas leidžia stebėti neigiamų atsiliepimų sulaukiančias svetaines, dėl kurių piliečiai nepraneša atsakingom institucijom. Sistemą galima taikyti neigiamų atsiliepimų sulaukiančių internetinių svetainių peržiūrai ar jos neprieštarauja LR nustatytoms normoms.

Privatumo ir saugos lygio interneto svetainėse vertinimo sistemą galima taikyti informuojant piliečius, naršančius globaliame internete, apie internetinių svetainių turinį, dėl kurio atsakingos LR

institucijos turi informacijos, o teisinėmis priemonės jo pašalinti nėra galimybės. Informacija pateikiant reikiamu momentu, tai yra atveriant tokia internetinę svetainę.

Sukurtąją sistemą galima bandyti taikyti, siekiant užtikrinti įvairių lygių kompiuterių vartotojų veiklos elektroninėje erdvėje saugų ir patikimą darbą, apjungiant įvairius savo mokslo šakų (informacijos saugos, teisės, ir kt.) specialistus, visuomenės saugumu el. erdvėje besirūpinančias organizacijas, įtraukiant visuomenę į atviras diskusijas.

Sukurtąją sistemą galima kartu naudoti kaip priemonę informuoti dar didesnę visuomenės dalį, kaip metodinę priemonę interneto naudotojų sąmojingumui apie grėsmes internete ugdyti, pateikiant metodines priemones apie grėsmes internete, svetainių įverčių formavimo metodiką, bei nurodant viešai prieinamus šaltinius internete galimų grėsmių rizikos sumažinimui ir teikiant interneto svetainių vertinimo − informavimo sistemos savybes.

13. Tyrimo išvados

1. Duomenų gavybos svetainės (angl. *Phishing Sites*), kurios suformuotos kaip priedanga oficialių internetinių svetainių (t. y. naudojami elementai bemaž identiški oficialiai interneto svetainei) lankomumas mažesnis, nei oficialių. Taip pat dažnu atveju URL turi sąryšį su oficialios interneto svetainės domenu. Be to galima iškirti dažnai klastojamus internetinių svetainių sąrašus, o didėjant duomenų kiekiui sistemoje būtų galima grupuoti pagal rizikas interneto svetainių prieglobos paslaugas teikiančių šaltinių patikimumą. Šie teiginiai gali būti jų automatinio atpažinimo privatumo ir saugos lygio vertinimo sistemoje metodikos sudedamoji dalis.

2. Socialinės inžinerijos metodais paremtos atakos skatina vartotojui teigiamas ar neigiamas emocijas siekiant, kad būtų atliktas tam tikras veiksmas, taip apkrečiant vartotojo interneto prieigos įrenginį virusais, kenkėjiškomis programomis, sukeliant duomenų naikinimo, duomenų vagystės, privatumo pažeidimų problemas. Socialinės inžinerijos atakų problemos interneto svetainėse sprendimas, taikant turinio vertinimą, efektyvus tuo, jog galima pateikti ir nepatyrusiems vartotojams remtis atsakingų institucijų ekspertų pateikiamais įspėjimais reikiamu momentu, tai yra atverčiant internetine svetainę. Be to, jei vyresnieji (patikimesnieji, t. y. praėję atranką) sistemos dalyviai (kurių vertinimo svoris didesnis) nėra įvertinę interneto svetainės, jos patikimumas nėra žinomas ir tai jau gali būti informacija.

3. Kadangi globaliame internete sutinkamas įvairus turinys, esant teisinėm priemonėm neteiktinas, prieštaraujantis Lietuvos Respublikos teisės aktams turinis yra šalinamas. Bet tai sunku padaryti kai turinys iškeliamas į įstatymiškai palankesnes valstybes, į valstybes, kuriose toks turinys

nėra reglamentuotas. Tada nėra teisinių priemonių jas pašalinti. Tai, kas vienose valstybėse traktuojama nusikalstama, neteiktina, kitose tai nereglamentuota ar leistina norma. Turinio reitingavimas leidžia greičiau pastebėti neigiamai vertinamas interneto svetaines globaliame internete. O šis sprendimas – sistema leidžia įspėti vartotoją apie interneto svetaines prieštaraujančioms LR teisės aktuose išdėstytoms normoms informaciją pateikiant reikiamų momentu, užklausiant internetinės svetainės.

4. Grėsmingiausi virusai gali perimti kompiuterio valdymą ir įtraukti jį į bendrą, trečios šalies valdomų kompiuterių tinklą (angl. *botnet*), dažnai panaudojamą kaip priemonę kitoms saugumo atakoms vykdyti: asmens duomenų vagystėms, konfidencialių duomenų vagystėms skirtiems tinklalapiams kurti, nepageidaujamiems elektroninio pašto pranešimams siųsti, paskirstytoms atsisakymo aptarnauti atakoms ir kitai nelegaliai veiklai elektroninėje erdvėje vykdyti. CERT–LT registruoja lietuviškus IP adresus įtrauktus į *botnet* veiklą ir nedelsdamas persiunčia informaciją interneto paslaugų teikėjams apie jų tinkluose aptiktus tokius IP adresus. Kompiuterio naudotojas dažniausiai nežino, kad jo kompiuteris veikia *botnet* tinkle kaip kompiuteris – zombis, valdomas pašalinių asmenų, tačiau kilus įtarimui interneto vartotojas pasinaudodamas CERT–LT patikra, turi galimybę pasitikrinti, ar per pastarąsias 15 dienų jo kompiuterio IP adresas nėra užfiksuotas minėtų tinklų duomenų bazėje [40]. Yra teigiama, kad vienas iš šių grėsmingų virusų požymių, jog jie neleidžia atidaryti apsaugos nuo virusų priemones, rekomendacijas teikiančių internetinių svetainių [41]. Po vienu išoriniu IP adresų gali būti didelis vietinis kompiuterių tinklas. Tad galima bandyti privatumo ir saugos lygio vertinimo interneto svetainėse sistemą papildyti metodu simuliuojančių šį procesą (pvz. užklausiančių e. apsaugos priemones teikiančių internetinių svetainių) ir pranešti vartotojui, jei minėtasis požymis tenkinamas, jog jo kompiuteryje galimai veikia kenkėjiška programinė įranga, taip operatyviai be tarpininkų informuojant konkretu sistemos vartotoją.

IŠVADOS

Asmens duomenų privatumą ir saugą galinčių pažeisti technologijų analizė parodė, jog didžiausią grėsmę privatumui ir duomenų saugai, naudojantis interneto svetainėmis, kelia asmens duomenų, slaptažodžių gavybos atakos taikant socialinės inžinerijos metodus ir skatinant teigiamas ar neigiamas emocijas internetinės svetainės lankytojui paveikti. Kaip antai parsisiųsti tariamai naudingas funkcijas atliekančias programas – virusus. Taip gali būti virusais apkrečiami kompiuteriai. Apkrėtus kompiuterį, įvairiais virusais iškyla grėsmė prarasti, atskleisti duomenis, atsiranda galimybė piktavaliams taikyti *Botnet* tinklus vykdant DoS ar DDoS atakas, platinti nepageidaujamas laiškus ir konfidencialių duomenų vagystėms skirtas interneto svetaines.

Atlikus internetinių incidentų tyrimo ir visuomenės informavimo modelio analizę pastebėta, jog nėra teisinių priemonių žalingų, prieštaraujančių Lietuvos Respublikos įstatymams interneto svetainių pašalinimui, kai internetinės svetainės aptinkamos, bei yra iškeliamos į įstatymiškai palankesnes valstybes, į valstybes kuriose toks turinys nėra reglamentuotas. Projekto „Saugesnis internetas LT AN–HL“ ataskaitoje pastebėta, jog jei interneto svetainės aptinkamos šalyse, kuriose toks turinys nėra laikomas neteisėtu, nesiimama jokių tolesnių veiksmų.

Privatumo ir saugos internete analizė parodė, kad yra metodų trūkumas, siekiant užtikrinti įvairių lygių kompiuterių vartotojų veiklos elektroninėje erdvėje saugų ir patikimą darbą.

Egzistuojančių turinio filtravimo, reitingavimo metodų analizė parodė, jog šie sprendimai neapima norimo informacijos prieinamumo lygio, bei saugumo ir privatumo vertinimo. Įvairiuose šalyse turinys klasifikuojamas skirtingai. Naudoti turinio atrinkimo programas, reikalingas pritaikymas nacionalinei rinkai. O atsakingų institucijų pranešimai nepasiekia dalies tikslinės auditorijos.

Europos Bendrijų Komisijos veiksmų plano dėl saugesnio naudojimosi internetu skatinimo kovojant su neteisėtu ir žalingu turiniu pasauliniuose tinkluose įgyvendinimo galutinio įvertinimo analizė, parodė jog turinio žymėjimas ir vertinimas svarbi priemonė darant internetą saugesnį.

„Trust Networks on the Semantic Web“ darbo analizė parodė, jog programos su turinio reitingavimo priemonėmis leidžia vartotojui sukonfigūruoti, rodyti pasitikėjimo lygius arba bendruoju lygmeniu arba, atsižvelgiant į tam tikrą temą.

Reitingavimo modelių analizė parodė, jog projektuojamos sistemos vartotojų žinioms reitinguoti tikslingiausia pasiremti „IT žinių portalo reitingavimo modeliu“, kuris išskiria kiekvieno sistemos dalyvio ir jų reitinguojamų elementų svorius.

Sudaryta, naudojantis interneto svetainėmis iškylančių saugumo ir privatumo grėsmių lygio vertinimo matrica, įverčių formavimo metodika, kuri panaudojama privatumo ir saugos lygio vertinimui interneto svetainėse.

Suformuota daugiapakopė (turinio vertinimo, turinio vertintojų vertinimo) reitingavimo sistema, kurioje įvertinami privatumo ir saugumo lygiai, bei išskiriami jų nustatymo patikimumo lygmenys, dalinantis sistemos dalyviams patirtimi.

Panašių sistemų savybių palyginimas (žr. 11 skyrių, 4 lentelę) parodė, jog suprojektuota privatumo ir saugos lygio interneto svetainėse vertinimo sistema išsiskiria tuo jog: nežymėtas turinys ir žymėtas naujoko laikomas (t. y. žymimas) įtartinu. Esant visada pateikiamas eksperto vertinimas, pateikiami svariausių vertintojų svariausi vertinimai. Yra žinių ir patirties sklaidos galimybė.

Suformuoto, socialinės inžinerijos atakų problemos interneto svetainėse, sprendimo tyrimas parodė, jog taikant turinio vertinimą, galima pateikti ir nepatyrusiems vartotojams remtis atsakingų institucijų, ekspertų pateikiamais įspėjimais reikiamu momentu, tai yra atverčiant internetine svetainę. Be to, jei vyresnieji (patikimesnieji, t. y. praėję atranką) sistemos dalyviai (kurių vertinimo svoris didesnis) nėra įvertinę interneto svetainės, jos patikimumas nėra žinomas ir tai jau yra informacija.

Suformuotoje sistemoje numatyta galimybė įspėti vartotoją apie interneto svetaines prieštaraujančioms LR teisės aktuose išdėstytoms normoms informaciją pateikiant reikiamų momentu (užklausiant internetinės svetainės), t. y. nereikia atlikti ilgai trunkančių formalių procedūrų.

Kadangi literatūroje [24] teigiama, jog tinklo saugumas labiausiai priklauso nuo kiekvieno vartotojo ir jų bendradarbiavimo tarpusavyje, bei suprojektuotoje sistemoje reitinguojamos sistemos vartotojų žinios, o vertinant internetines svetaines atsižvelgiama ne į įverčių kiekį, o į kiekvieno vertintojo „žodžio“ svarumą (t. y. simuliuojamas realaus gyvenimo modelis), sukurtąją sistemą galima bandyti taikyti, siekiant užtikrinti įvairių lygių kompiuterių vartotojų veiklos elektroninėje erdvėje saugų ir patikimą darbą, apjungiant įvairius savo mokslo šakų (informacijos saugos, teisės, ir kt.) specialistus, visuomenės saugumu el. erdvėje besirūpinančias organizacijas, įtraukiant visuomenę į atviras diskusijas.

LITERATŪRA

[1] Valstybinė duomenų apsaugos inspekcija, Informacijos ir technologijų vyr. specialistas Zigmantas Medutis. Rekomendacijos dėl viešųjų elektroninių ryšių paslaugų ir tinklų saugumo užtikrinimo. 2005-04-20. Prieiga per internetą: http://www.ada.lt/images/cms/File/rekomendacija%20del%20saugumo.pdf

[2] Lietuvos kompiuterininkų sąjunga. Privatumo ir saugumo lietuviškame internete tyrimas (pirmas etapas), dalykinė ataskaita. Tyrimo vadovas dr. Alfredas OTAS. Vilnius, 2002 m., 49 p. Prieiga per internetą: http://politika.osf.lt/inf_visuomene/dokumentai/PrivatumasIrSaugumas/1EtapoAtaskaita.pdf

[3] Europe's Information Society. Safer Internet Programme: the main framework for European policy [interaktyvus], [žiūrėta 2011-05-30]. Prieiga per internetą: http://ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm#currentprog

[4] SafeSurf. Birthplace of the Internet's voluntary rating Standard [interaktyvus], [žiūrėta 2010-06-05]. Prieiga per internetą: http://www.safesurf.com/

[5] US-CERT. Mindi McDowell, Cyber Security Tip ST04-014: Avoiding Social Engineering and Phishing Attacks [interaktyvus], [žiūrėta 2010-10-10]. Prieiga per internetą: http://www.us-cert.gov/cas/tips/ST04-014.html

[6] Lietuvos Respublikos ryšių reguliavimo tarnyba. E. saugumas [interaktyvus], [žiūrėta 2010-10-10]. Prieiga per internetą: http://www.esaugumas.lt/

[7] Lietuvos Respublikos ryšių reguliavimo tarnyba. CERT-LT [interaktyvus], [žiūrėta 2010-10-10]. Prieiga per internetą: https://www.cert.lt/

[8] LITNET CERT. Dokumentai [interaktyvus], [žiūrėta 2010-12-19]. Prieiga per internetą: http://cert.litnet.lt/dokumentai/index.html

[9] Valstybinė duomenų apsaugos inspekcija. Rekomendacijos asmens duomenų apsaugai internete. Prieiga per internetą: www.ada.lt/images/cms/File/rekomendacijos%20asmens%20duomenu%20apsaugai%20inernete.pdf

[10] Google. Privatumo centras [interaktyvus], [žiūrėta 2010-10-10]. Prieiga per internetą: http://www.google.lt/intl/lt/privacypolicy.html

[11] Capgemini, IDC, Rand Europe, Sogeti and DTi. Digitizing Public Services in Europe: Putting ambition into action. 9th Benchmark Measurement. For: European Commission, Directorate General for Information Society and Media. 2010 m., 272 p.

[12] VšĮ Informacinių technologijų institutas. ECDL, e-Guardian programa [interaktyvus], [žiūrėta 2010-01-25]. Prieiga per internetą: http://www.ecdl.lt

[13] Europos Bendrijų Komisija. Daugiamečio Bendrijos veiksmų plano dėl saugesnio naudojimosi internetu skatinimo kovojant su neteisėtu ir žalingu turiniu pasauliniuose tinkluose įgyvendinimo galutinis įvertinimas. Briuselis, 2006 m. Prieiga per internetą: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0663:FIN:LT:PDF

[14] Andrius Gedgaudas. Lietuvos valstybės institucijų privatumo politika internete. Vilnius, 2006 m. Prieiga per internetą: http://vddb.library.lt/fedora/get/LT-eLABa-0001:E.02~2006~D_20061219_142248-89079/DS.005.0.01.ETD

[15] European Commission Information Society and Media, Lietuvos Respublikos ryšių reguliavimo tarnyba, Švietimo informacinių technologijų centras. Saugesnis internetas LT AN-HL. Metinė viešoji ataskaita 2009 m. Prieiga per internetą: http://www.draugiskasinternetas.lt/repository/dokumentai/Metine%20ataskaita%20SIP%202009.pdf

[16] W3S. Platform for Internet Content Selection [interaktyvus], [žiūrėta 2011-05-15]. Prieiga per internetą: http://www.w3.org/PICS

[17] StopBadware. StopBadware kompanijos interneto svetainė [interaktyvus], [žiūrėta 2010-05-30]. Prieiga per internetą: http://www.stopbadware.org/

[18] Viktors Berstis, Herman Rodriguez. BLOCKING SAVES TO WEB BROWSER CACHE BASED ON CONTENT RATING. Patent No.: US 6,510,458 B1. Date of Patent: Jan. 21, 2003.

[19] Vilniaus universitetas, Matematikos ir informatikos fakultetas, Jaunesnysis dėstytojas Žilvinas Ledas. Interneto cenzūravimas [interaktyvus], [žiūrėta 2011-12-10]. Prieiga per internetą: http://sapnotaka.blogspot.com/2011/03/interneto-cenzuravimas.html

[20] Varghese Jacob, Ramayya Krishnan, Young U. Ryu, R. Chandrasekaran, Sungchul Hong. Filtering objectionable internet content. Carnegie Mellon University, University of Texas at Dallas, USA. Prieiga per internetą: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.143.625&rep=rep1&type=pdf

[21] Jennifer Golbeck, Bijan Parsia, James Hendler. Trust Networks on the Semantic Web. University of Maryland. Prieiga per internetą: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.62.8205&rep=rep1&type=pdf

[22] Jennifer Golbeck, James Hendler. Accuracy of Metrics for Inferring Trust and Reputation in Semantic Web-based Social Networks. University of Maryland. Prieiga per internetą: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.9.7009&rep=rep1&type=pdf

[23] Ignas Vajega. Elgesio kodeksai: jų vieta ir reikšmė reguliuojant neteisėtos ir žalingos informacijos platinimą kompiuteriniuose tinkluose. Vilnius, 2007 m. Prieiga per internetą: http://vddb.library.lt/fedora/get/LT-eLABa-0001:E.02~2007~D_20080207_135241-93697/DS.005.0.02.ETD

[24] E. Kazanavičius, A. Venčkauskas, A. Liutkevičius, A. Vrubliauskas. Informacijos saugos vadyba, mokomoji knyga. Kauno technologijos universitetas, Kaunas, 2008 m., 170 p.

[25] A. Venčkauskas, J. Toldinas. Kompiuterių ir operacinių sistemų sauga, mokomoji knyga. Kauno technologijos universitetas, Kaunas, 2008 m., 202 p.

[26] E. Weisstein. Normal Distribution. 2004 m. Prieiga per internetą: http://mathworld.wolfram.com /NormalDistribution.html

[27] Programos „PRIVOXY 3.0.3“ naudotojo vadovas. Prieiga per internetą: http://www.esaugumas.lt/storage/cd/cd/docs/PRIVOXY.pdf

[28] Kęstutis Vanagas. IT žinių portalo reitingavimo modelis, magistro darbas. Kauno technologijos universitetas, Informatikos fakultetas, Informacijos sistemų katedra. Kaunas, 2007 m., 55 p.

[29] Professor Mark E. Glickman. The Glicko system. Boston University, 2001 m. Prieiga per internetą: http://www.glicko.net/glicko/glicko.doc/glicko.html

[30] Professor Mark E. Glickman. The Glicko 2 system. Boston University, 2001 m. Prieiga per internetą: http://www.glicko.net/glicko/glicko2.doc/example.html

[31] Y. Shi; P. Specht; J. Stolen. A consensus ranking for information system requirements. Information Management & Computer Security. 1996 m. Prieiga per internetą: http://www.emeraldinsight.com/Insight/viewContentItem.do?contentType=Article&contentId=862639

[32] Java™ 2 SDK, Standard Edition documentation, version 1.4.2 [interaktyvus]. [žiūrėta 2010-01-13]. Prieiga per Internetą: http://download.oracle.com/javase/1.4.2/docs/

[33] Oracle. Java Technology [interaktyvus], [žiūrėta 2010-05-20]. Prieiga per internetą: http://www.sun.com/java/

[34] W3Schools. Browser Statistics [interaktyvus], [žiūrėta 2012-02-09]. Prieiga per internetą: http://www.w3schools.com/browsers/browsers_stats.asp

[35] Mozilla. Add-on SDK, Developer Guide [interaktyvus], [žiūrėta 2012-02-15]. Prieiga per internetą: https://addons.mozilla.org/en-US/developers/docs/sdk/latest/

[36] Google. Google Chrome Extensions, Developer's Guide. [interaktyvus], [žiūrėta 2012-02-15]. Prieiga per internetą: http://code.google.com/chrome/extensions/getstarted.html

[37] Oracle. MySQL open source database web site [interaktyvus], [žiūrėta 2010-05-23]. Prieiga per internetą: http://www.mysql.com/

[38] W3C. Latest SOAP versions, SOAP Version 1.2 [interaktyvus], [žiūrėta 2010-05-26]. Prieiga per internetą: http://www.w3.org/TR/soap/

[39] Lietuvos Respublikos Visuomenės informavimo įstatymas Nr. I-1418, 2011-12-20. Teisės aktą priėmė − Lietuvos Respublikos Seimas. Prieiga per internetą: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=416353&p_query=&p_tr2=2

[40] Ryšių reguliavimo tarnyba. Metinė veiklos ataskaita. Vilnius, 2008 m., 80 p. Prieiga per internetą: http://www.lrv.lt/Posed_medz/2009/090506/13_papildymas.pdf

[41] Jonas Juknius, Antanas Čenys. Botnet prevencija interneto paslaugu teikėjų lygmenyje. 11-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis“ straipsniu rinkinys. Vilniaus Gedimino technikos universitetas, Vilnius, 2008 m., 7 p. Prieiga per internetą: http://leidykla.vgtu.lt/conferences/jmk_informatika_2008/files/pdf/juknius_405-411.pdf

TERMINŲ IR SANTRUMPŲ ŽODYNAS

API (angl. *Application Programming Interface*) − aplikacijų programavimo sąsaja.

DDoS (angl. *Distributed Denial of Service*) − paskirtsytas atkirtimas nuo paslaugos.

DOM (angl. *Document Object Model*) − dokumento objektinis modelis.

DoS (angl. *Denial of Service*) − atkirtimas nuo paslaugos.

ELO − Elo reitingavimo sistema.

FTP (angl. *File Transfer Protocol*) − failų persiuntimo protokolas.

GRID − lokaliųjų skaičiavimų tinklų (telkiniai) junginiai.

HTML (angl. *HyperText Markup Language*) − hiperteksto ženklinimo kalba.

ICRA (angl. *Internet Content Rating Association*) − interneto turinio reitingavimo asociacija.

JMS (angl. *Java Messaging Service*) − *Java* pranešimų paslauga.

JSON (angl. *JavaScript Object Notation*) − *JavaSript* objektų notacija.

LR − Lietuvos Respublika.

ODBC (angl. *Open Database Connectivity*) − atviru duomenų bazių jungiamumas.

OS (angl. *Operating System*) − operacinė sistema.

PICS (angl. *Platform for Internet Content Selection*) − interneto turinio parinkimo platforma.

RDBMS (angl. *Relational DataBase Management System*) − realiacinė duomenu baziu valdymo sistema.

RSACi (angl. *Recreational Software Advisory Council on the Internet*) − pramoginės programos patariamoji taryba internete.

SDK (angl. *Software Development Kit*) − programinės įrangos kūrimo rinkinys.

SMTP (angl. *Simple Mail Transfer Protocol*) − paprastas pašto perdavimo protokolas.

SOAP (angl. *Simple Object Access Protocol*) − paprastasis objekto prieigos protokolas.

SQL (angl. *Structured Query Language*) − struktūrizuota užklausų kalba.

SSL (angl. *Secure Sockets Layer*) − saugiųjų jungimų lygmens.

TCP (angl. *Transport Control Protocol*) − transporto valdymo protokolas.

TCSEC (angl. *Trusted Computer System Evaluation Criteria*) − patikimų kompiuterinių sistemų vertinimo kriterijai.

UDDI (angl. *Universal Description, Discovery and Integration*) − universalaus apibūdinimo, suradimo ir integracijos.

UML (angl. *Unified Modeling Language*) − universali modeliavimo kalba.

URL (angl. *Universal Resource Locator*) – universalusis adresas.

WSDL (angl. *Web Service Definition Language*) − žiniatinklio paslaugų apibrėžimo kalba.

WSS (angl. *Web Services Security*) − žiniatinklio paslaugų saugumas.

XML (angl. *Extensible Markup Language*) − universali dokumentų ženklinimo kalba.

PRIEDAI

1 priedas

E. ERDVĖJE SUTINKAMŲ GRĖSMIŲ IR INTERNETINIŲ SVETAINIŲ ĮVERČIŲ FORMAVIMO METODIKA

SAUGUMAS

Virusai − tai kompiuterinės programos. Nuo įprastų programų jos skiriasi tuo, kad yra piktavališkos ir sugeba pačios plisti, dažnai įgaudamos epidemijos mastus. Dėl pastarojo bruožo kompiuteriniai virusai yra labai panašūs į biologinius virusus. Kompiuteriniai virusai sukelia žalingus padarinius, pavyzdžiui, sunaikina ar sugadina kompiuteryje esančią informaciją, taip pat gali atlikti kompiuterines atakas prieš kitus kompiuterius, nulemti kompiuterių ir tinklų perkrovas arba perimti kompiuterio valdymą.

Kirminai (angl. *worms*) – yra virusų, kurie patys sugeba daugintis, atmaina. Didžiausias jų keliamas pavojus yra sugebėjimas daugintis dideliais kiekiais. Įprastam virusui reikalingas įsiskverbimas į kitas bylas, tuo tarpu kirminas gali daugintis nesustodamas tol, kol išnaudos kompiuterio duomenų laikmenos talpą arba išplis po visą tinklą ir sutrikdys jo darbą. Daugiausia kirminai plinta elektroniniu paštu ir aktyvuojami atidarius bylą, pridedamą prie laiško.

Trojos arkliai (angl. *Trojan horses*) – virusų atmaina, kuri veikia panašiai kaip mitologijoje minimas Trojos arklys. Trojanai į kompiuterį dažniausiai patenka per kitas užkrėstas programas, kurios išoriškai atrodo kaip naudingos, tačiau realiai sukeliančios kenksmingus padarinius. Šie virusai negamina savo kopijų kaip kirminai ir neplinta užkrėsdami failus kaip virusai, bet aktyvavus programą, už kurios jie slepiasi, kartu aktyvuojamas ir virusas. Užpuolę sistemą jie turi galimybę ištrinti bylas, sunaikinti kitą kietojo disko informaciją bei atidaryti prieigą pašaliniams vartotojams, pasiekti ir vogti informaciją iš užkrėsto kompiuterio. Pastaroji virusų galimybė ypač pavojinga, kadangi įmanoma jog svarbi informacija pateks į svetimas rankas, kompiuteris nebus kontroliuojamas jo šeimininko. Populiariausi yra paslėpti trojanai (angl. *backdoors torjans*), trojanai šnipai (angl. *Trojan spies*), slaptažodžius vagiantys ir įgaliojantys trojanai (angl. *Trojan proxies*), kurie užkrėstą kompiuterį paverčia brukalų (angl. *spam*) platinimo priemone.

Šnipinėjimo programos (angl. *Spyware*) vadinama šnipinėjimo programinė įranga. Tai tokios programos, kurios, dažniausiai jums nežinant, renka informaciją apie lankomus tinklalapius, vartotojo vardą, elektroninio pašto adresus, programas ar bylas, esančias kompiuteryje, arba registruoja vartotojo atliekamus veiksmus internete (pvz., dirbant su banko sąskaitomis) ir siunčia šiuos duomenis tretiesiems asmenims (programų gamintojams ar kitiems suinteresuotiems asmenims) be vartotojo leidimo ir netgi be jo žinios.

Tarptinklapinių užklausų klastojimas (angl. *Cross Site Request Forgery*) – tai veiksmų (dažniausiai kenkėjiškų) atlikimas nežinant vartotojui ir naudojantis jo autentifikavimo informacija. Tam panaudojant naršyklėje saugoma įvairią automatinės autentifikacijos informaciją. CSRF pažeidžiamos internetinės programos, kurios autentifikacijos procedūrą atlieka automatiškai be papildomų vartotojo veiksmų.

Programinio kodo įterpimas į vartotojo peržiūrimą tinklapį (angl. *Cross–site scripting*, XSS) – IT sistemų pažeidžiamumas, dažniausiai aptinkamas tinklalapiuose, kuris leidžia įterpti papildomą programinį kodą į vartotojų peržiūrimą puslapį. Toks pažeidžiamumas atsiranda dėl nepakankamo įvedamos informacijos filtravimo. Tinkamai įvykdytos XSS atakos gali pridaryti daug žalos. XSS rezultatu gali tapti nulaužtos paskyros ir seansai, slapukų vagystė, neteisingas nukreipimas, organizacijos firmos ženklo iškraipymas ir kt.

Kodo įterpimas (angl. *Code Injection*) – dažnas programų saugumo pažeidimas, kuomet įvairiais būdais atliekamos netinkamos operacijos. Kodo įterpimas leidžia pakeisti programos vykdymo eigą, modifikuoti duomenis, gauti priėjimą prie slaptų duomenų ir kt. Kodo įterpimas dažnai naudojamas įvairių piktaviliškų programų platinimui.

Slapukų ir/ar sesijų perėmimas. Slapukas – tai mažas duomenų rinkinėlis (failas), kuriame yra svetainės naudojama informacija (pvz., jūsų svetainės nuostatos). Kai lankoma svetainė, kuri naudoja slapukus, ji gali paprašyti, kad naršyklė įrašytų vieną ar kelis slapukus į lankytojo kompiuterio diską. Kai tą pačią svetainę lankysite kitą kartą, naršyklė siųs slapukus atgal. Tokiu būdu svetainė prisiderins prie jūsų reikmių, pasinaudodama slapukuose esančia informacija.

Slapuke taip pat gali būti asmeniniai tapatumo duomenys. Tai tokie duomenys, kurie gali būti panaudoti jūsų tapatumui patvirtinti arba ryšiams reikalingi duomenys (pvz., asmenvardis, el. pašto adresas, darbo ar namų adresas, telefono numeris). Tačiau svetainė gali prieiti tik prie tų asmeninių duomenų, kuriuos jai patys pateikiate. Pavyzdžiui, svetainė negali sužinoti jūsų el. pašto adreso, nebent jį nurodytumėte. Taip pat svetainė negali prieiti prie kitų duomenų, laikomų jūsų kompiuteryje.

Interneto naršyklių nuostatose yra nustatyta, kad darbas su slapukais yra nematomas: slapukai įrašomi bei išsiunčiami be jūsų žinios. Suinteresuoti asmenys gali perimti juos. Patarimas: galima pakeisti slapukų nuostatas, kad naršyklė, prieš įrašydama slapuką, atsiklaustų jūsų. Taip pat galima nurodyti, kad slapukai būtų priimami tik vienam naršyklės seansui.

Iššokantys langai / automatinis nukreipimas. Iššokantys langai yra papildomi naršyklės langai, atsidarantys automatiškai, kai spustelite internetinės svetainės objektą arba tiesiog atidarote internetine svetainę. Dažniausiai šie iššokantys langai yra reklamos.

Tai taip pat gali būti piktybinės programos, kuri įdiegta jūsų kompiuteryje, ženklas. Galite taip pat pastebėti:

- ✓ nepageidaujamus peradresavimus į kitas interneto svetaines;
- ✓ pakeistus paieškos rezultatus;
- ✓ nepageidaujamas įrankių juostas ar šonines juostas interneto naršyklėje;
- ✓ sumažėjusi kompiuterio greitį.

Piktybinės programos paveikia galimybę valdyti jūsų paties kompiuterį. Į jų sudėtį gali įeiti programų, galinčių ištrinti duomenis jūsų kompiuteryje, pavogti kreditinės kortelės numerius ir pasiekti kitą asmeninę informaciją.

Kita. Visas kitas kenkėjiškas kodas, kuris nepriskiriamas paminėtoms kategorijoms.

NAUDINGOS NUORODOS:

Nemokamos antivirusinės:

- www.microsoft.com/security_essentials/
- www.avast.com
- www.avg.com
- www.comodo.com/

Kenkėjiškų programų aptikimo ir pašalinimo programos:

- www.safer-networking.org
- www.lavasoft.com/products/ad-aware_se_personal.php

Talpyklos ir slapukų valymas įvairiose naršyklėse:

- www.google.com/support/accounts/bin/answer.py?hl=lt&answer=32050&ctx=cb&src=cb&cbid=1ms20ypmk8gus&cbrank=1

_____

PRIVATUMAS

Dauguma mūsų naršome internete naudodami paieškos sistemas. Paieškos sistemos turi ir naudoja gebėjimą sekti ir kaupti duomenis apie kiekvieną paiešką. Pavyzdžiui naudojantis paieškos sistemomis, serverio žurnaluose gali būti kaupiama informacija apie jūsų užklausas, sąveiką su paslauga, interneto protokolo tipą, naršyklės tipą, naršyklės kalbą, užklausos datą ir laiką bei vieną ar daugiau slapukų, kurie gali unikaliai atpažinti jūsų naršyklę ar naudojama paskyrą. O kartu naudojant vietos nustatymo paslaugas (pavyzdžiui žemėlapius), šias paslaugas teikiančios kompanijos gali gauti informacijos apie jūsų faktinę vietovę (pvz., mobiliojo įrenginio siunčiamus GPS signalus), kurioje esate, arba informacijos, kuri gali būti naudojama tai vietovei apytiksliai nustatyti (pavyzdžiui telefono stoties ID).

Interneto svetainėse skelbiama kokios privatumo politikos jose laikomasi, tačiau nevisi atsivertę ir (ar) registruodamiesi ją skaito. Kaip naudojami jūsų duomenis? Ar jie perduodami tretiesiems asmenims?

PATARIMAI:

- Peržiūrėkite tinklapių privatumo politiką. Būtinai perskaitykite prieš pateikdami savo asmeninius duomenis registruodamiesi tinklapiuose, rašydami komentarus ir kitais atvejais.
- Nustatykite jog interneto naršyklės nesaugotų slapukų ir nekauptų interneto turinio ilgiau nei vienam naršyklės seansui.

NAUDINGOS NUORODOS:

Rekomendacijos privatumo užtikrinimui:

- www.esaugumas.lt/index.php?1831428302

Rekomendacijos asmens duomenų apsaugai internete:

- www.ada.lt/images/cms/File/rekomendacijos%20asmens%20duomenu%20apsaugai%20inernete.pdf

Duomenų apsauga darbo vietoje:

- www.ada.lt/images/cms/File/Duomenu%20apsauga%20darbo%20vietoje.pdf

_____

E. KOMERCIJA

Per internetą, firmos gali susisiekti su klientais. Internetas leidžia firmoms identifikuoti, rinkti duomenys ir sužinoti kliento įpročius, kad galėtų pasiūlyti patraukliausius pasiūlymus. Perkant iš neaiškių internetinių parduotuvių iškyla pavojus, netik prarasti pinigus ir negauti prekių, bet ir atskleisti asmens duomenis.

Kompanijos užsiimančios elgesio rinkodara, kaip įprasta kontroliuoja vartotojų atliekamas paieškas internete. Interneto svetaines, kurias lanko vartotojai, turinį, kurį jie žiūrį, jų sąveikas su socialinių tinklo svetainėmis, sąveikas su jų elektroninio pašto turiniu, produktais ir paslaugomis, kurias jie perka. Toliau, kai vartotojai naudoja mobilius prietaisus, net jų fizinė vieta gali būti fiksuojama, o surinkti duomenys gali būti analizuojami ir apjungiami su informacija iš autonominių šaltinių, kad sukurtų dar išsamesnius vartotojų profilius.

Asmeninės, konfidencialios informacijos perėmimas arba „phishing“ (angl. terminas „phishing“ kilęs nuo žodžių „password fishing“ – slaptažodžių žvejyba) – tai tokia sukčiavimo forma, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis. Dažniausiai tokio pobūdžio atakos būna nukreiptos prieš bankų klientus, siekiant sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Vėliau tokiu būdu gauta informacija gali būti panaudota pasipelnymo tikslais vykdant nusikalstamas veikas: neteisėtus prisijungimus prie informacinių sistemų, pinigų vagystes iš sąskaitų ar elektroninėje erdvėje atsiskaitant už prekes svetimomis kortelėmis.

PATARIMAI:

- Peržiūrėkite tinklapių privatumo politiką. Būtinai perskaitykite prieš pateikdami savo asmeninius duomenis registruodamiesi e. komercijos paslaugas teikiančiuose tinklapiuose.
- Pirkite iš jums gerai žinomų elektroninių parduotuvių. Jeigu norite pirkti jums negirdėtoje internetinėje parduotuvėje, reikėtų paieškoti informacijos apie ją paieškos sistemose (pvz.: „Google“, „Yahoo“).
- Prieš įvesdami asmens duomenis atkreipkite dėmesį, ar internetinėje svetainėje naudojami saugumo protokolai SSL, HTTPS, ir pan.
- Visada įsitikinkite ar veikia kompiuterio antivirusinė programa.

NAUDINGOS NUORODOS:

E. saugumas:

- www.esaugumas.lt/

Valstybinės duomenų apsaugos inspekcijos rekomendacijos**:**

- www.ada.lt/index.php?lng=lt&action=page&id=55

_____

TURINYS

Globaliame internete sutinkamas įvairus turinis, esant teisinėm priemonėm neteiktinas, prieštaraujantis Lietuvos Respublikos teisės aktams turinis yra šalinamas. Tai sunku padaryti kai turinys iškeliamas į įstatymiškai palankesnes valstybes, į valstybes kuriose toks turinys nėra reglamentuotas. Nėra teisinių priemonių jas pašalinti. Tai kas vienose valstybėse traktuojama nusikalstama, neteiktina, kitose tai nereglamentuota ar leistina norma. Rekomenduojame reitinguoti turinį.

Atitinka leistinas normas − visa kas neprieštarauja žemiau išvardytoms normoms.

Dezinformacija − draudžiama platinti dezinformacija ir informacija, šmeižianti, įžeidžianti žmogų, žeminanti jo garbę ir orumą. Draudžiama skleisti informacija, pažeidžianti nekaltumo prezumpciją.

Autorių teisių ir gretutinių teisių pažeidimai − literatūros, mokslo, meno ir kitų kūrinių platinimas be autoriaus sutikimo, autorių teisių ir gretutinių teisių įstatymų ir kitų įstatymų bei teisės aktų pažeidimai.

Neskelbtina informacija − informacija, kurioje:

1) raginama prievarta keisti Lietuvos Respublikos konstitucinę santvarką;
2) skatinama kėsintis į Lietuvos Respublikos suverenitetą, jos teritorijos vientisumą, politinę nepriklausomybę;
3) kurstomas karas ar neapykanta, tyčiojimasis, niekinimas, kurstoma diskriminuoti, smurtauti, fiziškai susidoroti su žmonių grupe ar jai priklausančiu asmeniu dėl lyties, seksualinės orientacijos, rasės, tautybės, kalbos, kilmės, socialinės padėtis, tikėjimo, įsitikinimų ar pažiūrų;
4) platinama, propaguojama ar reklamuojama pornografija, taip pat propaguojamos ir (ar) reklamuojamos seksualinės paslaugos, lytiniai iškrypimai;
5) propaguojami ir (ar) reklamuojami žalingi įpročiai ir narkotinės ar psichotropinės medžiagos.

NAUDINGOS NUORODOS:

Lietuvos Respublikos visuomenės informavimo įstatymas:

- www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=280580&p_query=&p_tr2=

Nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas:

- www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=183129

Saugaus interneto vaikams kūrimas:

- www.childcentre.info/vaikai-ir-internetas-2
- www.draugiskasinternetas.lt/

Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas

- www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=207199