KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

INFORMACIJOS SISTEMŲ KATEDRA

Justinas Grėbliūnas, Monika Pažereckaitė

Veiklos ir reikalavimų modeliavimo metodas įvertinantis saugumą

Magistro darbas

Darbo vadovas

prof. Saulius Gudas

KAUNAS, 2011

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

INFORMACIJOS SISTEMŲ KATEDRA

Justinas Grėbliūnas, Monika Pažereckaitė

Veiklos ir reikalavimų modeliavimo metodas įvertinantis saugumą

Magistro darbas

Recenzentas

doc. dr. A. Lenkevičius

2011-05-27

Darbo vadovas

prof. Saulius Gudas

2011-05-27

Atliko

IFM - 9/4 gr. Studentai

Justinas Grėbliūnas, Monika Pažereckaitė

2011-05-27

KAUNAS, 2011

SUMMARY

Business and Requirements Modelling Method with Security Assessment

The aim of this work is to create a business process modeling and IS requirements specification method with a security assessment. For this purpose, a three-level organizational security model with assessment of organization's objectives, management structure and business processes was made.

The paper analyzes the security requirements engineering process associated with the business modeling and application management of the organization level. The system security standards ISO / IEC 17799, ISO / IEC 13335, which refer to the essential safety aspects, were analyzed. There was developed business model using BPMN. The IS security requirements specification techniques and models of i * framework, misuse cases were analyzed, analysis of trade-offs was made.

There were selected the security requirements modeling methods - the misuse cases, the goal model, BPMN, which include key performance functions and allow to link business with a possible misuse case model.

Based on MoDAF models a developed business model was created. Using UML Use Case diagrams, which specify information system security requirements, IS model for potential misuse cases was designed.

The Magic Draw profile and plug-in package was created, which is a help for an analyst and projector to ensure the security of the IS.

Operating conditions and simulation method was tested through UAB „Piramidė LT“, requirements specification, which includes the security requirements.

Keywords: IS security requirements, ISO / IEC 17799, ISO / IEC 13335, business model, BPMN, the goal model, MoDAF, misuse cases, UML, Use Case Diagram, MagicDraw plugin.

Turinys

Terminų ir santrumpų žodynas

UML - (angl. *Unified Modeling language*) – unifikuota modeliavimo kalba

PĮ – programinė įranga

IS – informacinė sistema

IT – informacinės technologijos

ISO/IEC 17799 – standartas padeda nustatyti saugumo reikalavimus

ISO/IEC 13335 – standartas apžvelgia informacines technologijas, saugumo technikas ir jų valdymą

ERP - (angl. *Enterprise resource planning*) - verslo valdymo sistema

CRM - (angl. *Customer Relationship Management*) – klientu valdymo sistema

Misuse Case - piktnaudžiavimo atvejai

Security trade-offs - saugumo kompromisai

BPMN (angl. Business Process Modeling Notation) – veiklos proceso modeliavimo notacija

OMG (angl. *Object Management Group*) – objektų valdymo grupė, konsorciumas, kuris nustato standartus sistemoms, pagrįstoms duomenų struktūromis.

BPQL – (angl. *Business Process Query Language*) – veiklos proceso užklausos kalba

MoDAF - (angl. *British Ministry of Defence Architecture Framework*) - veiklos architektūros karkasas

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

HTTPS – (angl. *Hypertext Transfer Protocol Secure)* – apsaugotas hyperteksto perdavimo protokolas

SSL (angl. *Secure Socket Layer*) - kriptografinis protokolas, skirtas informacijos, sklindančios internete apsaugojimui šifruojant

DdoS – (angl. *distributed denial-of-service attack*) – paskirstyta serviso nepasiekiamumo ataka, apjungianti daugybę kompiuterių

DSL - (angl. *Domain Specific Language*) – srities specifinė kalba, kompiuterinė kalba sukurta tam tikrai sričiai

COBIT - (angl. *Control Objectives for Information and related Technology*) - karkasas, sukurtas informacinių technologijų valdymui. Šis karkasas turi rinkinį įrankių, kurie leidžia valdytojams susieti reikalavimus su techninėmis problemomis ir veiklos rizika

BPD - (angl. *Business Process Development*) – veiklos proceso kūrimas

1. Įvadas

Šiuolaikinis pasaulis tiesiog neįsivaizduojamas be informacinių technologijų (IT), visuomenė tapo labai priklausoma nuo skaitmeninių technologijų, kurios tapo gyvenimo kokybės rodikliais. Informacinių technologijų pagalba yra valdoma daugybė informacinių sistemų, kurios stipriai įtakoja žmonių gyvenimą. Informacinės sistemos (IS) valdo labai svarbią informaciją, jos taikomos įvairiose gyvenimo srityse, nuo IS priklauso netgi žmonių sveikata, todėl yra labai svarbu, užtikrinti IS saugumą. Norėdami sutaupyti laiko ir lėšų saugumo priemonės turėtų būti taikomos organizacijos IS kūrimo proceso pradžioje, tai sudarytų saugesnę IS struktūrą. Informacinės sistemos saugumas yra priklausomas nuo organizacijos saugumo, kurioje ji yra, todėl svarbu užtikrinti saugumą ne tik IS bet ir organizacijos lygmenyse.

Įgyvendinant saugumą verslo procesuose yra svarbu palaipsniui modeliuoti organizaciją detalizuojant jos struktūrą ir procesus. Kuriant IS, aprašant jos kompiuterizuojamas funkcijas (UML, panaudojimo atvejų diagrama) sistemos saugumo aspektai dažnai paliekami saviveiklai. Todėl svarbu sistemingai įgyvendinti saugumą. Egzistuoja keletas standartų ISO/IEC 17799, ISO/IEC 13335, kurie padeda nustatyti tam tikras saugumo taisykles ir principus, kurių reikia laikytis, norint užtikrinti saugumą visose srityse, įskaitant ir IT. Tačiau šie standartai nepateikia jokių metodikų.

Saugumo užtikrinimas yra sudėtingas ir sunkus uždavinys. Saugumo užtikrinimas yra neatsiejamas nuo informacinių sistemų, techninės dalies, žmonių, pačios organizacijos modelio ir dar daugelio kitų aspektų. Norint tinkamai įvertinti reikalingą saugumo lygį, reikia atsižvelgti į anksčiau išvardintus faktorius ir juos išanalizavus, pritaikyti saugumo priemones kuriamame saugumo modelyje.

Taikant saugumo priemones turėtų būti atsižvelgta į vartotojų tikslus ir tai, kad įdiegtos saugumo priemonės netrukdytų vartotojams dirbti su informacine sistema. Atsiranda klausimas ir uždavinys - „Kaip apjungti organizacijos, informacijos sistemos ir vartotojų tikslų modelius, kurie apjungtų saugumo reikalavimus?“

Šis magistro darbas skirtas veiklos ir reikalavimų saugumo metodikos sukūrimui ir koncepcinio modelio sudarymui.

2. Saugumo reikalavimų analizė

2.1. Analizės tikslas

Išnagrinėti sistemos saugumo standartus, saugumo reikalavimo specifikavimo metodus.

2.2. Tyrimo sritis, objektas ir problema

Tyrimo sritis apima saugumo reikalavimų specifikavimą ir jų taikymą modeliavimo kalbose, kurios atvaizduoja organizacijos veiklos procesus, struktūrą.

Nėra nusistovėjusios tvarkos, kaip modeliuojant organizaciją ir jos elementus (IS, darbuotojai ir kt.) įtraukti saugumo reikalavimus nuo pat pradžių.

2.3. Organizacijos UAB „Piramidė LT“ e-parduotuvės informacinės sistemos analizė

Šiame skyriuje pateiksime dalykinės srities aprašymą, kuriuo remiantis bus vykdomas mūsų sukurto metodo testavimas.

Šiuo metu sparčiai vystantis technologijomis, vis labiau dinamiškėja vartotojų paslaugų sektorius. Kuomet visus dalykus tvarkę tiesiogiai, dabar tai darome nuotoliniu būdu, dažniausiai per internetą. Vienas didžiausių paslaugų sektorius, tai prekybininkai, kurie užsiima prekių pardavimų. Vis dažniau esantys mažmeniniai prekybininkai, turintys parduotuves, taip pat kelia verslą ir į internetą – elektronines parduotuves. Kai kurie pradedantys verslininkai, realią alternatyvą mato tik e-parduotuvę, nes ji reikalauja mažiau išlaidų nei įprastą parduotuvė. Taip pat dažnai verslo realizavimas internete susijęs su specifinių vartotojų grupe: gali būti taikomasi tik į mažą vartotojų rinką, todėl norint pasiekti kuo didesnį vartotojų skaičių reikia kurti e-parduotuvę.

2.3.1. Pasirinktos dalykinės srities aprašas

E-parduotuvės kuriamos įvairiais metodais: pasinaudojant įvairių programavimo kalbų šablonais (angl. framework), ar iš karto perkant e-parduotuvės sistemą. Perkant jau paruoštą e-parduotuvės sistemą, gali iškilti kliūčių, dėl jos pritaikymo. Tuo tarpu jei samdomas programuotojas ar įmonė kuria e-parduotuvę, funkcionalumas atitiks visus užsakovo reikalavimus.

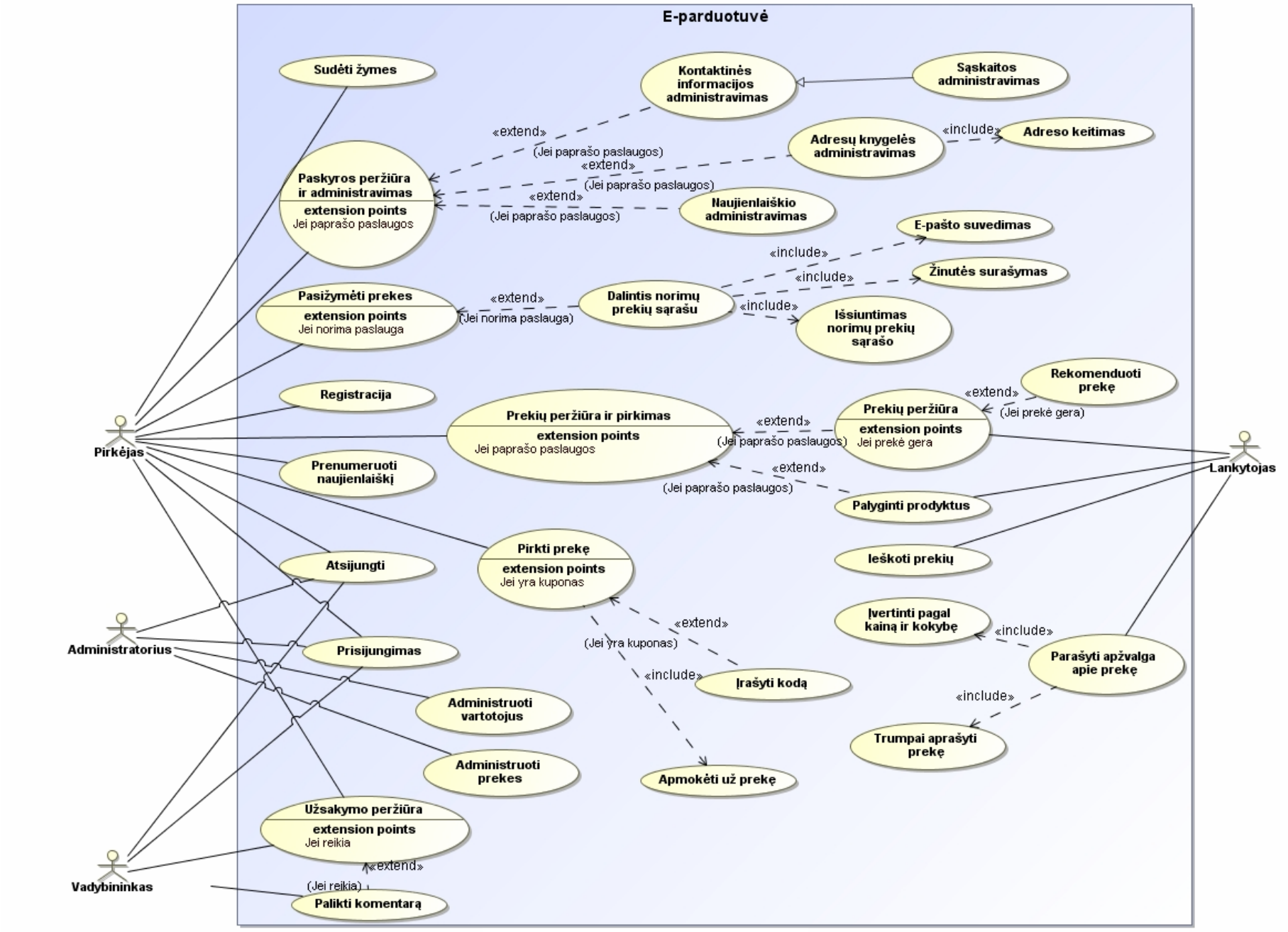
E-parduotuvė yra sudėtinga informacinė sistema, tuo labiau, kad ji gali būti apjungta su VVS – verslo valdymo sistema (angl. ERP - Enterprise resource planning), CRM (angl. Customer

Relationship Management) – klientu valdymo sistema ir kitomis. Kuomet į pardavimo procesą įtraukiama tiekėjai, kurjeriai, finansų valdymas visa organizacinė struktūra pasidaro ypatingai sudėtinga. Todėl tokioje organizacijoje, labai svarbus pasidaro saugumo aspektas. Kad organizacija sėkmingai vykdytų savo veiklą, saugumo priemonės turi būti įdiegtos verslo procesuose.

Taigi nuspręsta modeliuoti organizacijos UAB „Piramidė LT“ užsiimančios kaljanų e-prekyba saugumo modelį. Ši parduotuvė yra pasiekiama adresu http://www.tabakaskaljanui.lt. E-parduotuvėje galima įsigyti įvairių prekių skirtų kaljanams.

2.3.2. E-parduotuvės informacinės sistemos panaudojimo atvejų diagrama

1 paveikslėlyje pavaizduota E-parduotuvės supaprastinta panaudojimo atvejų diagrama. Ši e-parduotuvė sukurta naudojanti „magento community“ (http://www.magentocommerce.com/) - atvirojo kodo web aplikacija, parašyta PHP kalba (angl. Hypertext Preprocessor).



1 pav. Panaudojimo atvejų diagrama

Organizacija yra nedidelė ją sudaro 3 žmonės: e-parduotuvės administratorius ir 2 vadybininkai. Administratoriaus pagrindinė veikla yra susijusi su e-parduotuve: prekių įkėlimas, paprašytų ataskaitų parengimas, vartotojų administravimas, nustatymų ir informacijos keitimas ir kt. Vadybininkai užsiima tik prekių užsakymų vykdymu, jie mato užsakymus e-pašte, tikrina mokėjimus, bei perduoda prekes išsiuntimui.

2.3.3. Organizacijos aprašymas

Įmonė UAB „Piramidė LT“ užsiima prekių skirtų kaljanams prekyba. Taip pat nuomoja kaljanus kavinėms, barams ir paprastiems asmenims. Prekių pristatymas vyksta trimis būdais:

- siuntimas autobusu stoties siuntų skyriumi – prekė pristatoma per 24 valandas;
- siuntimas kurjeriu - prekės pristatomos kitą darbo dieną po užsakymo patvirtinimo;
- siuntimas paštu - siunta pristatoma į namus arba ją reikia atsiimti pašte su gautu lapeliu. Prekė pristatoma per 1-3 darbo dienas po užsakymo patvirtinimo.

Apmokėjimas galimas dviem būdais:

- Apmokėjimas pavedimu į banko sąskaitą - detalesnė informacija apie konkrečios sąskaitos apmokėjimą gaunamas atlikus užsakymą elektroniniu paštu;
- Apmokėjimas grynaisiais - šis apmokėjimo būdas taikomas tuomet kai pasiimamos prekės iš sandėlio Kaune. Atsiimti prekes galima tą pačią dieną, darbo valandomis.

2.4. Vartotojų analizė

2.4.1. Vartotojų aibė, tipai ir savybė

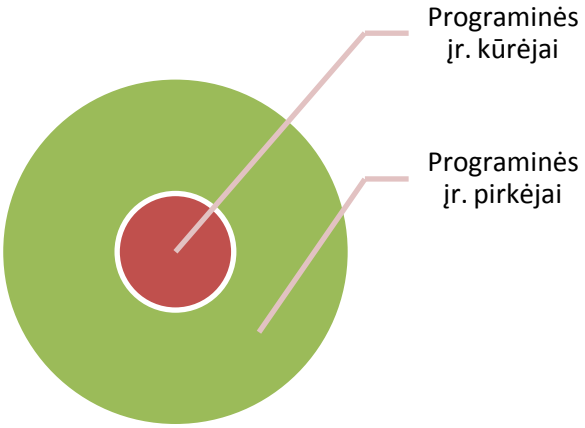
Šis veiklos ir reikalavimų modeliavimo metodas, įvertinantis saugumo kriterijus bus naudingas dvejoms vartotojų grupėms: programinės įrangos kūrėjams ir IT analitikams. PĮ analitikai galės pasinaudoti šia metodika norėdami, pažiūrėti kokio lygio saugumą užtikrina informacinė sistema. Programinės įrangos kūrėjai šį metodą taikys programinės įrangos kūrime, nes šis metodas leis jiems formalizuoti saugumo reikalavimus ir juos panaudoti projektuojant organizacijos ir informacinės sistemos modelius.

Programines įrangos kūrėjai – saugumas yra vienas didžiausiu prioritetų, ypatingai kuriant kritines sistemas lemiančios žmonių saugumą, privatumą, konfidencialumą. Norint sukurti tvirtą

struktūrą turinčią informacinę sistemą reikia saugumo priemones taikyti kuo ankstesnėse kūrimo stadijose, nes taikant vėliau nėra gerai užtikrinamas programinės įrangos integralumas. Taikant šį metodą, bus sutaupomos laiko ir lėšų sąnaudos. Įrodyta, kad saugumą diegiant pradinėse programos kūrimo stadijose greičiau į rinką paleidžiama tvarkinga programa.

IT analitikai – ši vartotojų grupė bus suinteresuota metodu, dėl galimybės patikrinti saugumo lygį. IT analitikai galės patikrinti koks yra saugumo lygis, priderinti saugumo priemones prie sistemai keliamų tikslų.

Nors PĮ kūrėjų yra mažiau (14 pav.), bet programinės įrangos projektavimo metodas, įvertinantis vartojimo saugumo kriterijus bus labiau naudingas PĮ kūrėjams, nes jie galės išnaudoti visas metodo teikiamas galimybes, kadangi kūrėjai yra labiau nusimanantys IS reikalavimų specifikavime.



2 pav. Vartotojai

2.4.2. Vartotojų tikslai ir problemos

Metodikos vartotojų tikslai ir problemos aprašyti 1 lentelėje.

Lentelė 1. Vartotojų tikslai ir problemos.

Vartotojų tipas	Tikslai	Problemos
IT analitikai	Patikrinti esamos IS saugumą	Trūkumas IT žinių
PĮ kūrėjai	Sukurti kokybišką, saugią PĮ, atitinkančią vartotojų reikalavimus Sumodeliuoti kuo galima detalesnį saugumo modelį	Pernelyg supaprastinta grėsmių analizė

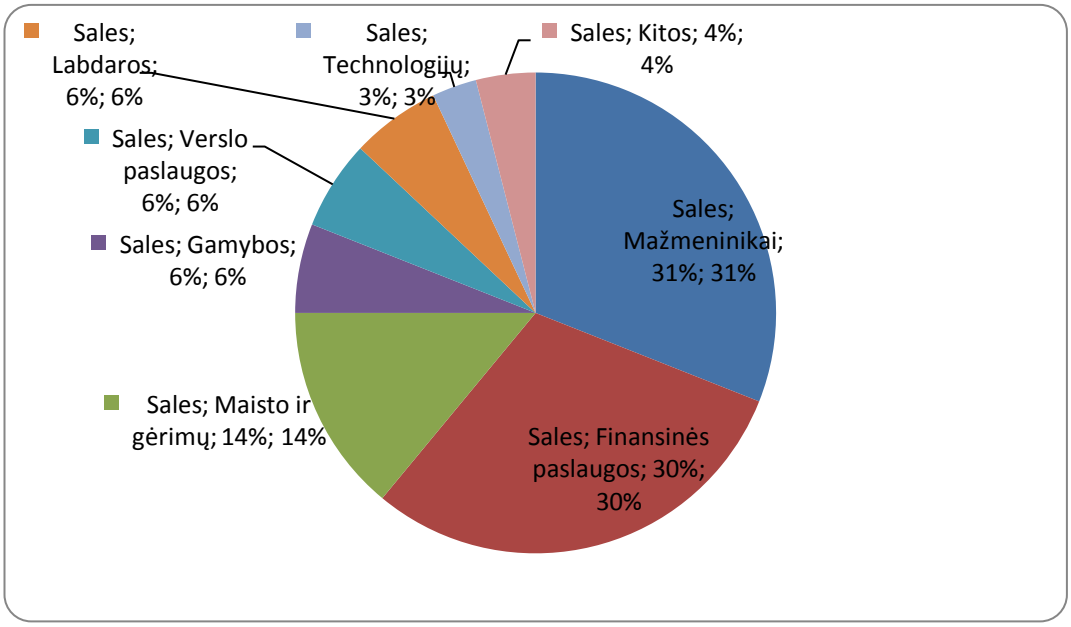
2.5. Problemos sprendimo metodų literatūros šaltiniuose analizė

Už įsilaužimus dažniausiai būna atsakingi ne organizacijos nariai -74 % (lentelė 1, http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf), todėl organizacijos dažniausiai yra puolamos, nežinant jos IT struktūros ir naudojantis jau patikrintais standartiniais metodais. Visi kiti įsilaužimai būna susiję su tam tikru organizacijos struktūros išmanymu, nes tai daro asmenys artimi tai organizacijai. Pagal tą patį atliktą tyrimą buvo nustatyta, kad pažeidimai dažniausiai atsiranda, dėl techninių ar saugumo politikos klaidų, jos nebūvimo. Taip pat didelę dalį – 64 % procentus pažeidimų padaro patys įsilaužėliai. Pažeidimai įvyksta ir dėl naudojamų kenkėjiškų programų. Mažesnė dalis pažeidimų (22 % ir 9 %) atsiranda dėl organizacijos darbuotojų kaltės. Tai dažniausiai vyksta suteikiant per dideles paskyrų teises serveriuose, duomenų bazių sistemoje ar informacinėje sistemoje. Fizinių atakų priežastis būna kuomet darbuotojui yra suteikta per daug teisių pačioje organizacijoje ir jis gali turėdamas bylų sandėlio raktus, nueiti ir jas pavogti ar kitaip pasisavinti informaciją.

Lentelė 2. Pažeidimų statistika.

Kas atsakingi už duomenų apsaugos pažeidimus?	**Kaip pažeidimai atsirado?**
74 % išoriniai šaltiniai	**67 %** buvo įtakoti reikšmingų klaidų
20 %buvo įvykdyta iš vidaus	**64 %** dėl įsilaužimų
32 % susiję verslo partneriai	**38%** naudojant kenkėjiškas programas.
39 % skirtingos šalys	**22 %** dėl privilegijuoto piktnaudžiavimo
	9 % dėl fizinių atakų

Paveikslėlyje 3 pavaizduota pramonės šakos, į kurias dažniausiai laužiasi hakeriai. Pirmiausia tai yra mažmenine prekyba užsiimančios organizacijos – parduotuvės, paskui seka finansines paslaugas teikiančios bendrovės – bankai, valiutų konvertavimo tinklapiai ir kt. Trečioje vietoje pagal pažeidžiamumus atsiduria maisto ir gėrimų kompanijos. Ši diagrama (3 pav.) rodo, kad įsilaužėliai linkę laužtis į kompanijas, kurios savo verslą vykdo internete. Plečiantis IT galimybėmis vis mažesnės kompanijos gali užsiimti verslu, nes IT sutaupo žmoginių resursus. To paties tyrimo (http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf) nustatyta, kad pagal pažeidžiamumus yra arba labai didelės kompanijos (1001 -10000 darbuotojų) – 27% procentai arba mažos – 26% procentai (11-100 darbuotojų).



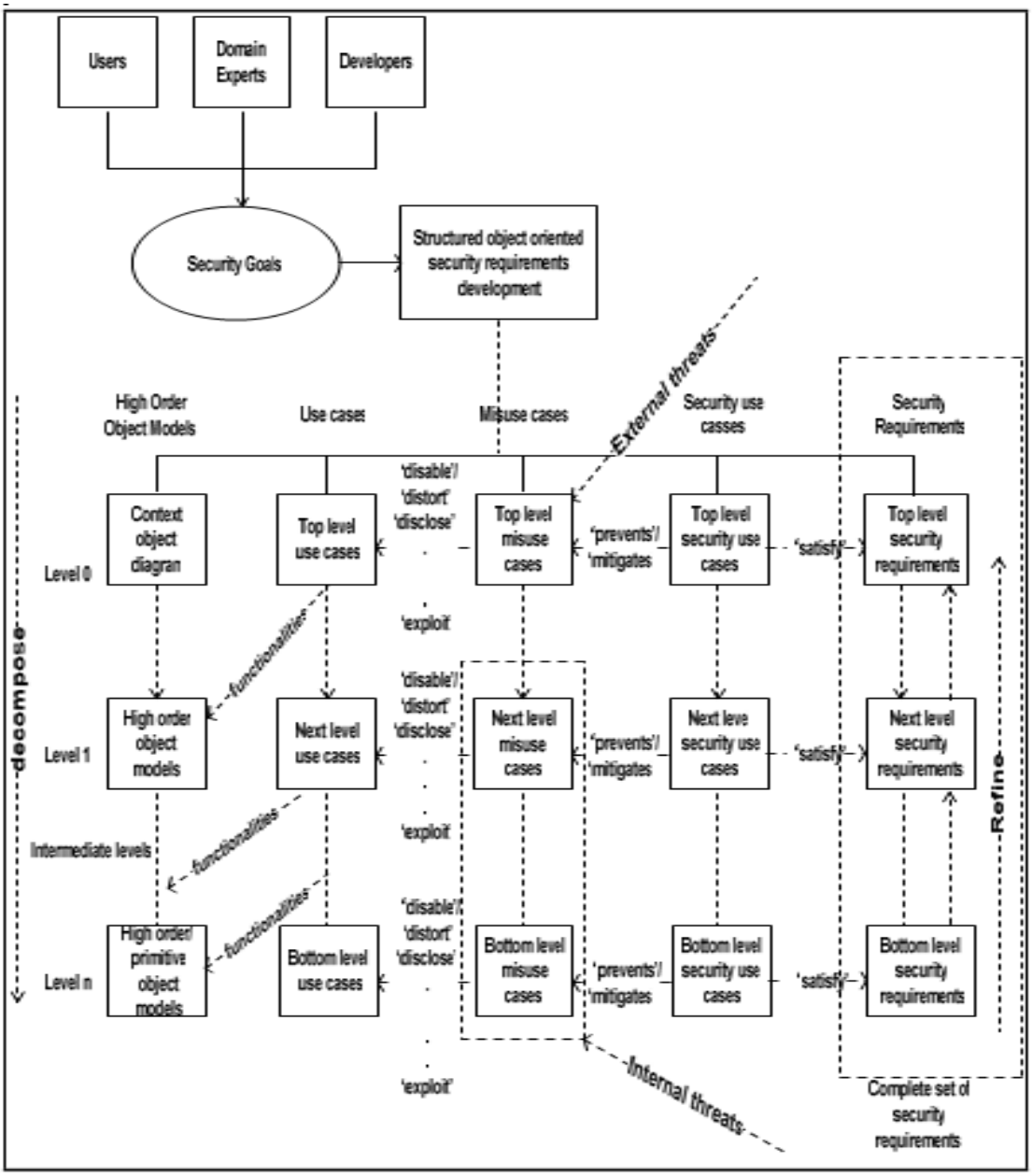
3 pav. Pramonės šakos pagal pažeidžiamumų procentą.

2.6. Panašių modelių analizė

2.6.1. Piktnaudžiavimo atvejų metodas

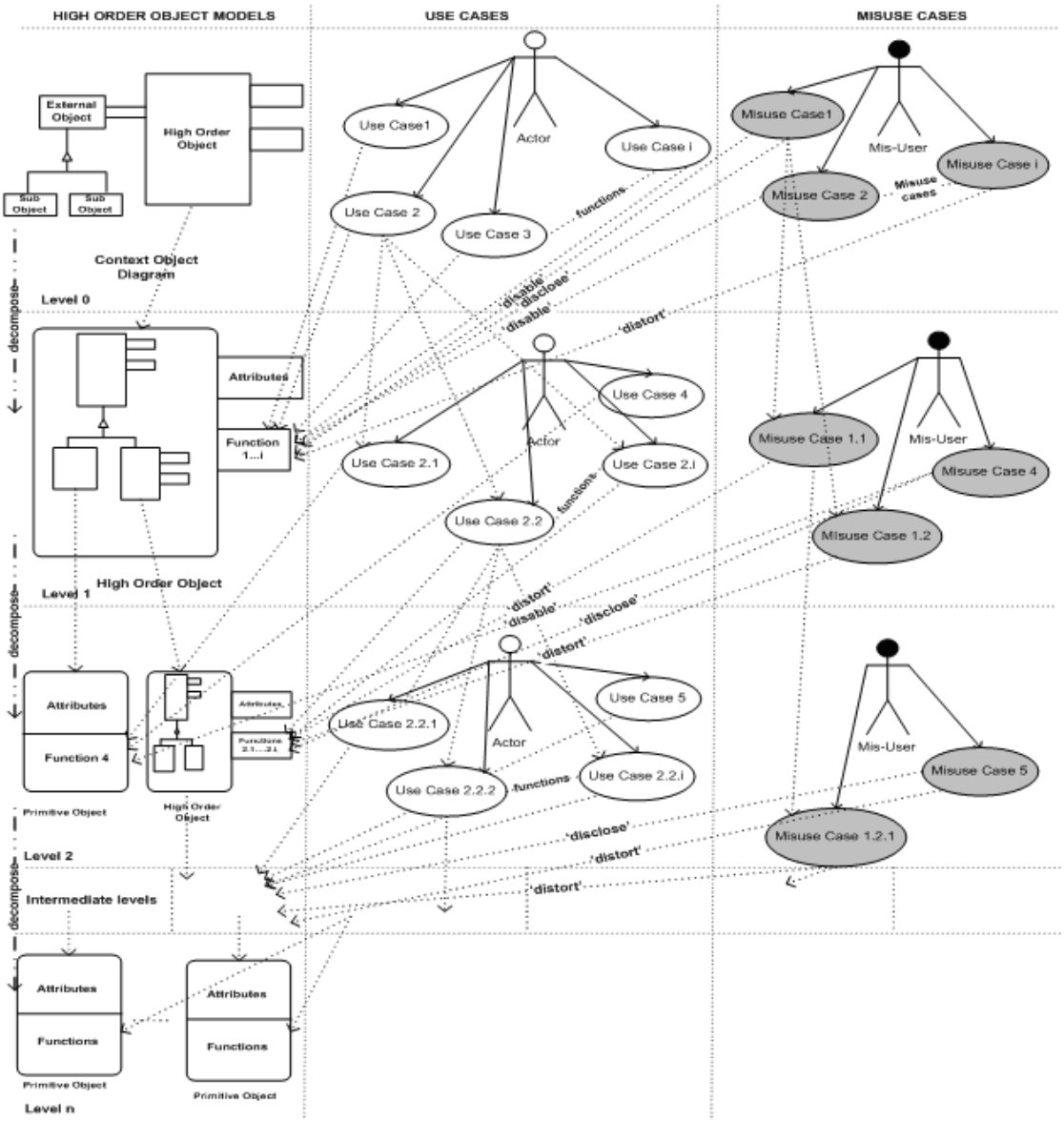
Vienas iš sprendimų, kaip analizuoti informacinę sistemą, yra aprašytas autorių: Sojan Markose, Xiaoqing (Frank) Liu, ir Bruce McMillin. Šio straipsnio autoriai pateikia informacinės sistemos analizės metodologiją, kuri įvertina sistemos saugumą, remiantis panaudojimo ir piktnaudžiavimo atvejų metodu (angl. Use Case and Misuse Case). [1]

Ši metodologija unikali tuo, kad atsižvelgia ne tik į išorines grėsmes sistemai, bet analizuodama sistemą kaip visumą, vėliau ją išskaido į komponentus ir analizuoja kiekvieną komponentą atskirai, taip yra išanalizuojama ir vidinės grėsmės, kurios gali paveikti sistemą. Ši metodologija gali būti panaudota modeliuojant saugumo reikalavimus. Pirmame žingsnyje yra sudaroma kontekstinė sistemos diagrama, kuri parodo sąveikas tarp aukšto lygio objektų ir išorinių objektų. Antrame žingsnyje, kiekviename lygyje panaudojimo atvejai identifikuoja pagrindines objekto funkcijas. Trečiame žingsnyje identifikuojami piktnaudžiavimo atvejai ir piktnaudžiaujantys vartotojai. Visuose lygiuose piktnaudžiaujantys vartotojai gali būti ir išoriniais ir vidiniais aktoriais. Šiame modelyje gali būti įvairių ryšių tarp panaudojimo ir piktnaudžiavimo atvejų. Ryšys tarp panaudojimo ir piktnaudžiavimo atvejų gali būti: „disable“, „distort“, ir „disclose“. „Disable“ ryšys reiškia, kad piktnaudžiavimo atvejis visiškai panaikina panaudojimo atvejo funkcionalumą. „Distort“ ryšys reiškia, kad yra iškraipomas panaudojimo atvejo funkcionalumas, o „disclose“ ryšys parodo, kur atskleidžiama svarbi informacija apie esybes naudojamas panaudojimo atvejyje.



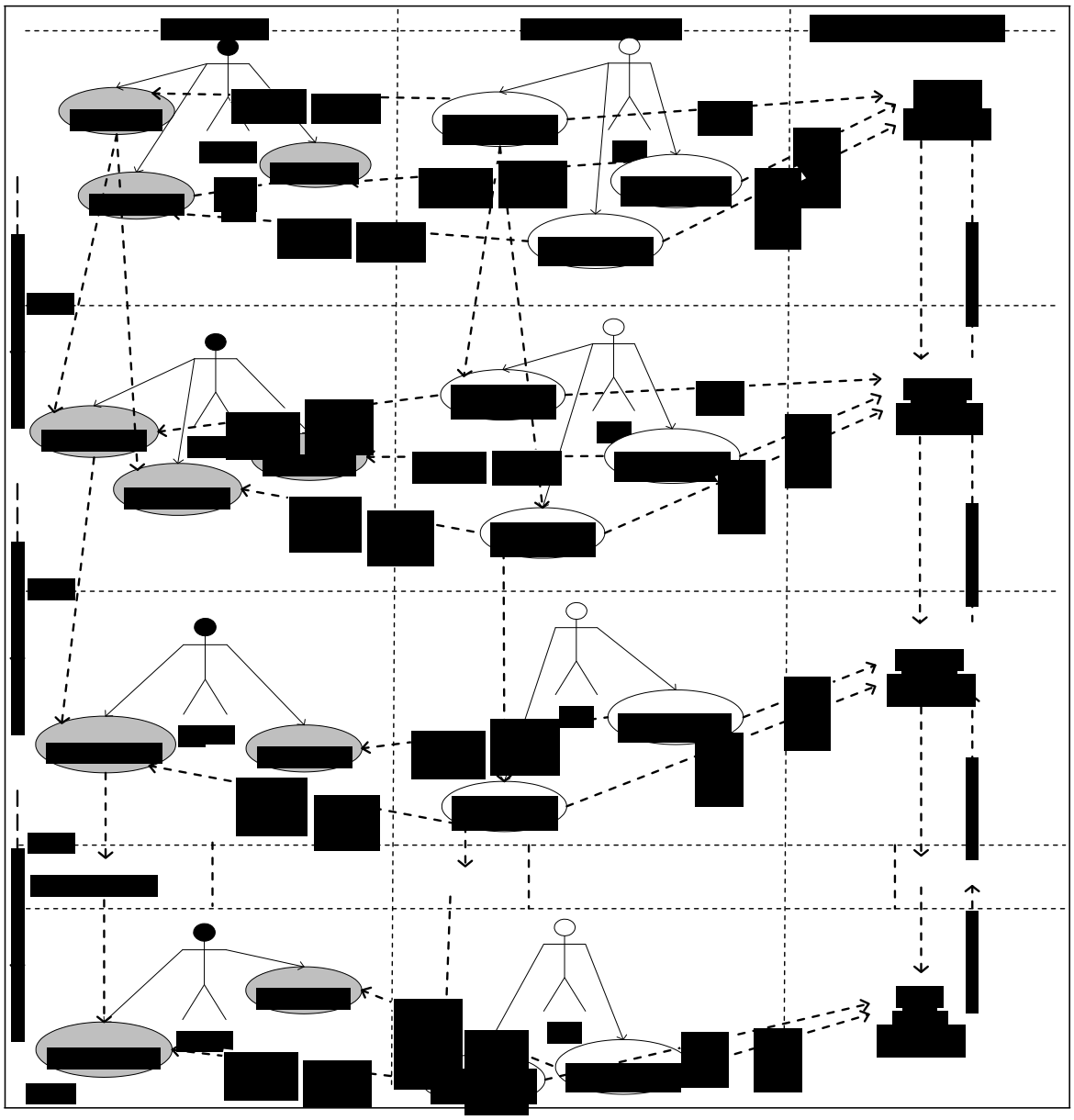
4 pav. Struktūriškai objektinis saugumo reikalavimų procesas. [1]

Detalizuotas proceso pavyzdys pateiktas 4 paveikslėlyje. Aukščiausiame lygyje yra sumodeliuojama kontekstinė diagrama, vėliau ši diagrama yra išskaidoma į smulkesnius objektus. Saugumo panaudojimo atvejai yra kuriami atsakant į piktnaudžiavimo atvejus. Kiekviename lygyje saugumo reikalavimai yra išgaunami iš saugumo panaudojimo atvejų. Išskaidymo procesas tęsiasi, kol objektai pasidaro primityvūs ir yra pilnai išnagrinėjami piktnaudžiavimo ir panaudojimo atvejai.



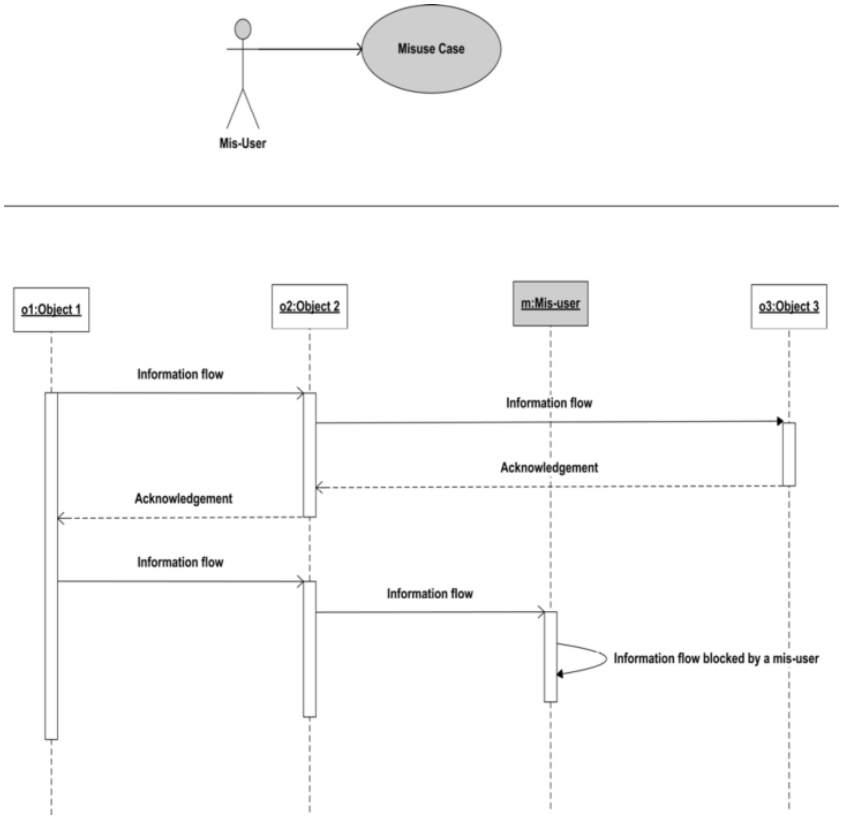
5 pav. Detalizuotas piktnaudžiavimo atvejų ir hierarchinio kūrimo procesas.[1]

Detalizuotas hierarchinio kūrimo ir saugumo reikalavimų analizės procesas pateiktas 5 paveikslėlyje. Saugumo panaudojimo atvejai yra susiję su saugumo reikalavimais naudojant „satisfies“ ryšį. Dekompozicijos procesas yra tęsiamas iki tada, kai yra pasiekiama, kad kiekvienas piktnaudžiavimo panaudojimo atvejis visuose lygiuose yra sustabdomas ar sušvelninimas, naudojant saugumo panaudojimo atvejus, kol galu gale išgaunami saugumo reikalavimai.

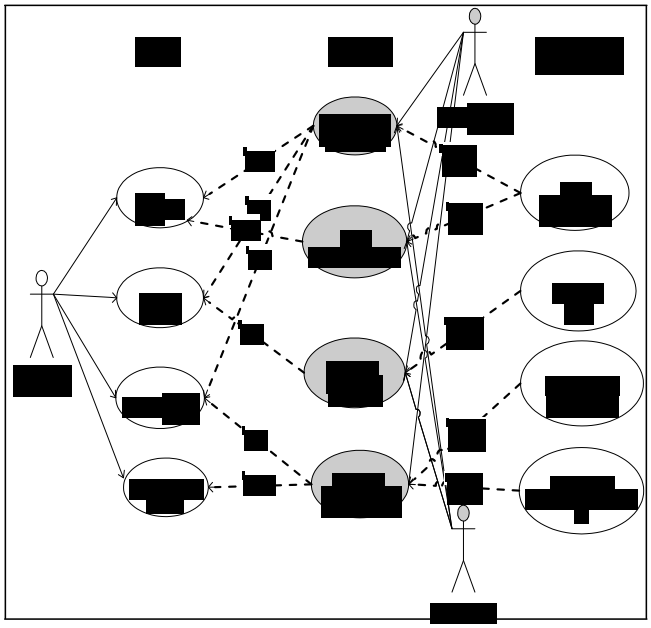


6 pav. Detalizuotas 16 hierarchinio kūrimo ir saugumo reikalavimų analizės procesas [1]

Kiekvienas piktnaudžiavimo panaudojimo atvejis gali būti detalizuotas sekos diagrama (6pav.). Taip pat pavaizduojama atitinkamo lygio panaudojimo ir piktnaudžiavimo atvejai hierarchiškai (7 ir 8 pav.).



7 pav. Piktnaudžiavimo atvejo sekos diagrama [1]



8 pav. Panaudojimo ir piktnaudžiavimo atvejų diagrama [1]

2.6.2. Saugumo kompromisai ir alternatyvūs saugumo sprendimai

Kito šaltinio autoriai siekia išsiaiškinti, kaip saugumo kompromisai ir alternatyvūs saugumo sprendimai veikia kitus kokybės tikslus. Tai jie bando padaryti naudodami saugumo kompromisų analizę (angl. security trade-offs). Kompromisų analizė yra metodiškas nagrinėjimas privalumų ir

trūkumų ir sistemos kūrimo pasirinkimų, kad būtų pasiektas balansas tarp kelių konkuruojančių tikslų. Ši analizė gali būti labai sudėtinga, nes vien metu reikia išspręsti problemas tarp skirtingų vartotojų ir jų skirtingų tikslų, atakų galimybę, apgalvoti saugumo atsakomąsias priemones ir jų poveikius.[3]

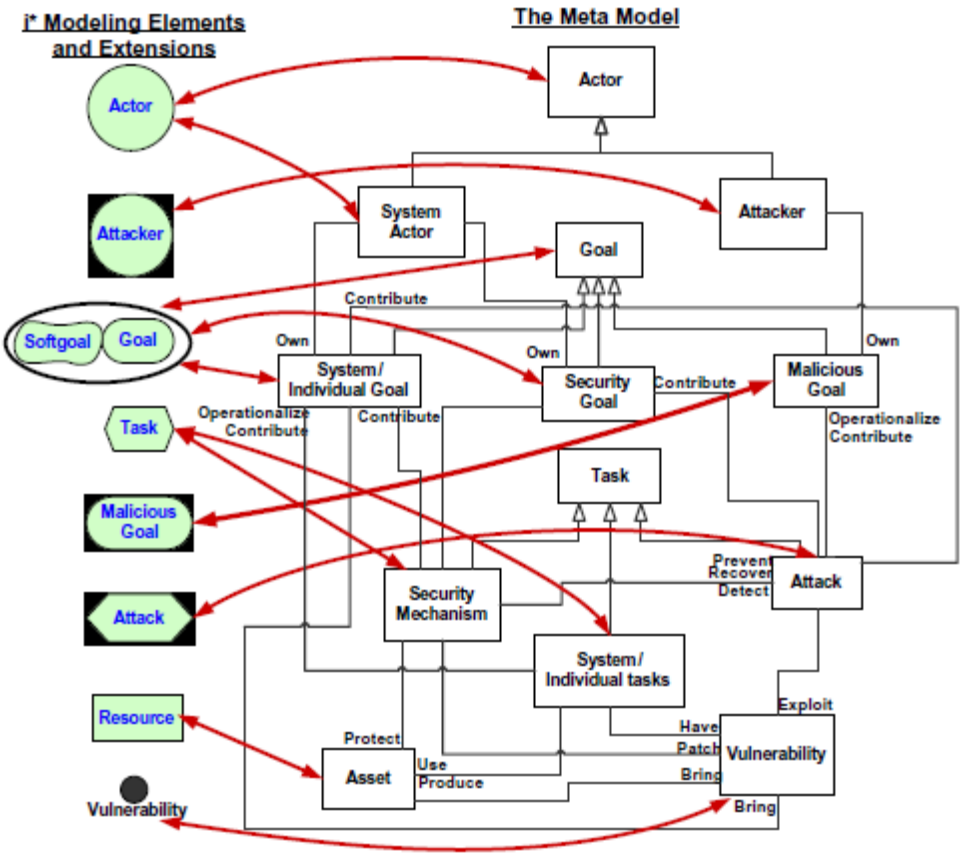
Konceptualiam modeliavimui jie išskiria tris pagrindines kriterijų rūšis: kūrimo tikslai, aktoriai, saugumo-specifiniai konceptai.

Saugumo ir kiti kompromisai užimą pagrindinį branduolį nesutarimų, šalia kūrimo tikslų, kurie kyla iš užsakovų ir vartotojų. Kol pasirinkti tinkamus saugumo sprendimus iš alternatyvų yra sunku, daug didesnė problema būna, kada kūrėjams reikia nuspręsti, kaip pasirinkti tinkamus saugumo mechanizmus, atsižvelgiant į kainą, išleidimą, įvairius ne funkcinius reikalavimus, saugumo politiką, standartus, individualius tikslus skirtingų užsakovų, vartotojų. Atsižvelgiant į tai modeliavimo technika turėtų palaikyti netikslias, neužbaigtas ar subjektyvias žinias apie tikslus.

Antroji kriterijų rūšis yra aktoriai. Dažniausiai kūrimo tikslai kyla iš įvairių suinteresuotų asmenų: sistemos vartotojai, administratoriai, vyriausieji vadovai, projektų vadovai ir vartotojai. Konceptuali modeliavimo technika taip pat turėtų galimybę vaizduoti skirtingus vartotojus.

Saugumo reikalavimai reikalingi, dėl grėsmių kylančių iš piktavališkų aktorių. Saugumo tikslai yra paveikiami grėsmių kylančių iš vidinių ir išorinių aktorių ir egzistuojančių pažeidžiamumų sistemos modelyje.

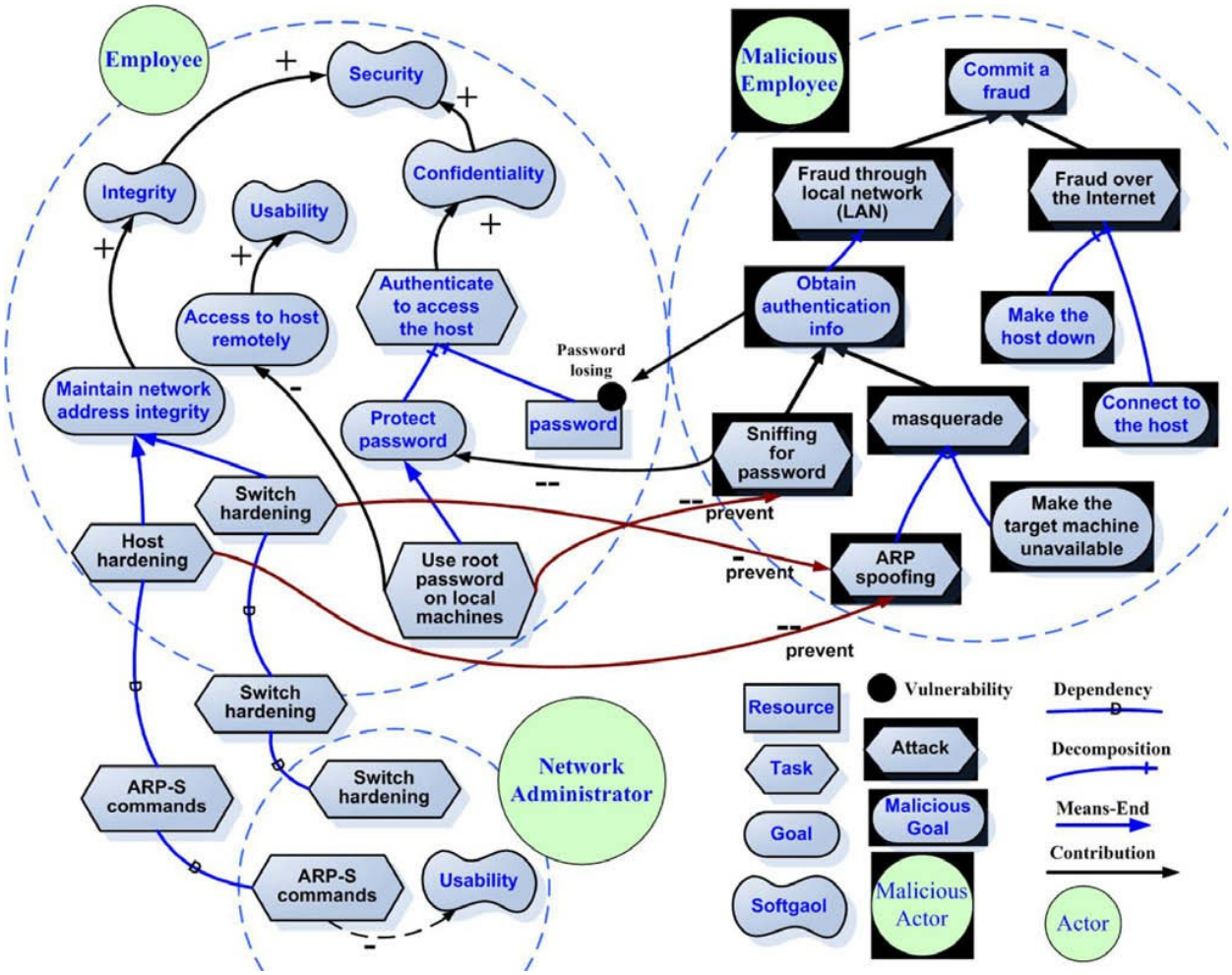
Saugumo kompromisų modeliavimo notacija



9 pav. Sudarytas metamodelis pagal kriterijus [3]

Autoriai papildė i* karkasą, kuris remiasi aktorių, jų tikslų ir iš anksto nustatytų priklausomybių tarp aktorių. Metamodelis parodo, kaip jo elementai yra susiejami su i* modeliavimo konstrukcija (9 pav.). Notacija buvo papildyta ir grėsmę keliantys: tikslai, negriežti tikslai, užduotys ir aktoriai yra pažymėti juodo šešėlio stačiakampiu. Norint atskirti grėsmę keliančius elementus nuo saugių elementų yra analizuojama įsilaužėlių tikslai ir uždaviniai. Tačiau įsilaužėlių elgesys yra nenuspėjamas, todėl labiau kreipiamas dėmesys į įsilaužėlių galimus pasirinkimus, atsižvelgiant į sistemos tipą ir grėsmes sukeltas kitų aktorių tikslams.

Saugumo grėsmė yra bet koks pavojų keliantis elgesys, kuris daro įtaką kitų aktorių tikslams. Pavyzdžiui 10 pav. parodyta aktoriaus – „Malicious Employee“, sukelta grėsmė – įsilaužti, pasinaudojus kieno nors kito vardu.



10 pav. Kenkėjiško vartotojo grėsmė.[3]

Modelyje (10 pav.) yra žymima elementų turtai ir pažeidžiamumai. Turtas (angl. asset) yra bet kas, kas turi vertę organizacijai. Fiziniai resursai, informacija, žmonės. Pažeidžiamumas yra silpnybė, ar galimybė įsilaužti į sistemą. Tarkim slaptažodis yra darbuotojo turtas, o pažeidžiamumas yra slaptažodį pamesti. Saugumo inžinerijoje skirtingi mechanizmai sukelia skirtingus padarinius atakoms. Šie mechanizmai (ryšiai) grupuojami į – uždrausti (angl. prevent), susekti (angl. detect), atstatyti (angl. recover). Norint sėkmingai atremti ataką, ryšys turėtų būti uždrausti. Susekti ir atstatyti ryšiai gali sumažinti atakų padarinius, bet kelio joms užkirsti negali. Ryšys – atstatyti, atstato po atakos įvykusius padarinius.

Kitas pasiūlytos konceptualios struktūros privalumas yra jos galimybė išreikšti kompromisus. Pateikta notacija pateikia priemones tikslų modeliavimui ir jų atsekimui iki aktorių. Šiame pavyzdyje (11 pav.) kompromisai tarp tikslų yra modeliuojami pasinaudojus pagalbinių ryšių: -, - -, +, ++. Konceptuali struktūra taip pat suteikia galimybę modeliuoti kompromisus tarp aukšto lygio tikslų potikslių. Pavyzdžiui darbuotojas gali pasinaudodamas pagrindiniu raktu vietinėje

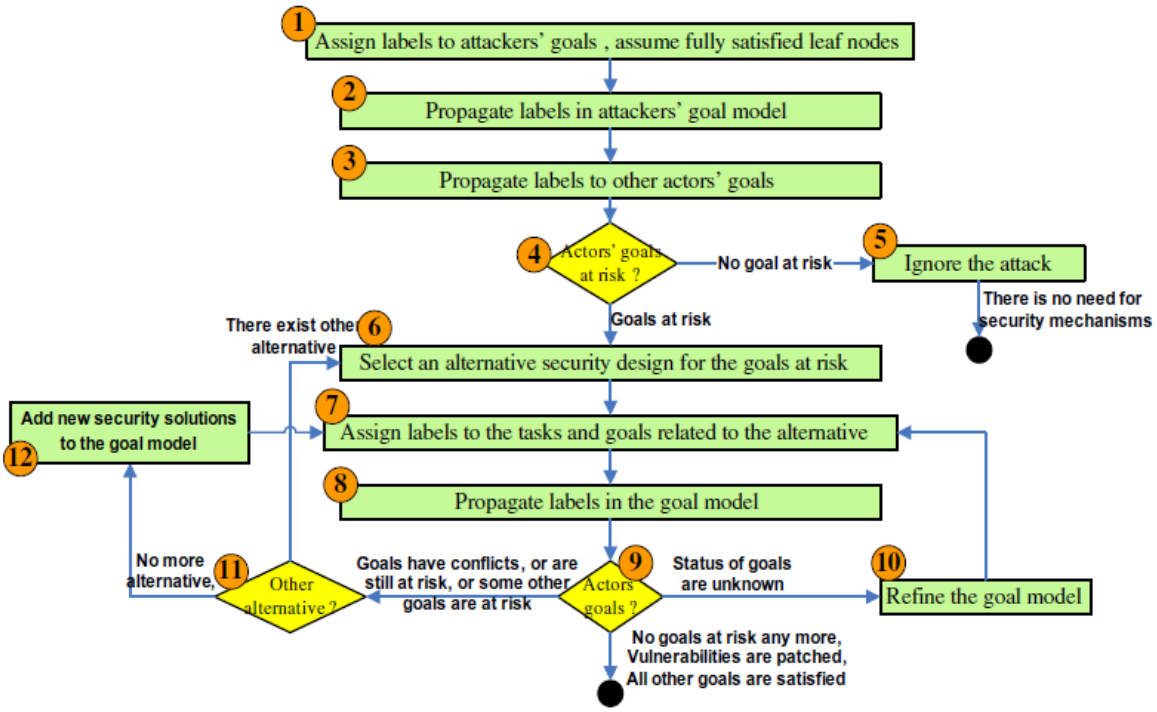
sistemoje (angl. Use root password on local machines) gali visiškai užkirsti kelią atakai – slaptažodžių šnipinėjimas (angl. Sniffing the password). Nepaisant to, šis saugumo sprendimas veikia neigiamai tikslą - prisijungti prie serverio nuotoliniu būtu (angl. Access to host remotely), o šis tuo tarpu turi neigiamą įtaką panaudojamumo (angl. Usability) tikslui.

Kompromisų analizės metodas

Sistemos kūrėjui reikia ištirti visus galimus saugumo sprendimus ir patikrinti kiekvieno jų įtaką atakoms ir tikslams, kad galiausiai būtų galima pasirinkti labiausiai tinkamą skirtingiems aktoriams. Šios metodikos tikslas, kad aktoriai būtų patenkinti savo padarytais sprendimais[8]. Metodika pavaizduota 11 pav.

Pirmajame žingsnyje vertintojas mano, kad įsilaužėliui pavyko įvykdyti užsibrėžtus tikslus. Bet vertintojas nežino jo tikslų, gali būti, kad įsilaužėlio tikslų modelis turi hierarchiją, todėl yra svarbu tiems tikslams suteikti tam tikras etikes, etiketės suteikiamos tik aukščiausiems tikslams. Kai tik etiketės yra sukuriamos visiems pavojų keliantiems aktorių tikslams, vertintojas paskirsto etiketes užduotims ir tikslams, kurie veikia su saugumo mechanizmu (7 žingsnis). Etiketė žymi vertintojo nuosprendį apie atitinkamų aktorių pasisekimą, vykdant saugumo užduotis, ar siekiant saugumo tikslų.

Devintame žingsnyje tikslų modelis nurodo, kurie tikslai yra pilnai ar dalinai patenkinti, ar atmesti analizuojant saugumo sprendimus. Procedūra yra tęsiama tol, kol randamas saugumo sprendimas, paremtas vertintojo suvokimu. Nepaisant to vertintojas gali toliau nagrinėti kitas saugumo alternatyvas, kad būtų patenkinta kuo daugiau tikslų. Įvertinus alternatyvas, kai kurių tikslų statusas gali būti neaiškus, todėl vertintojui reikia nuodugniai ištirti modelį (10 žingsnis). Jei dar yra nesutapimų tarp tikslų, turi būti analizuojamos kitos alternatyvos (11 žingsnis).



11 pav. Saugumo kompromisų analizės procedūra. [8]

Etikečių pavadinimai yra priskiriamai pagal 12 pav.

Child Node		Contribution Type (Prevent)				
Label Name	Symbol	++	+	-	- -	?
Satisfied	✓	✓	✓.	✗.	✗	?.
Weakly Satisfied	✓.	✓.	✓.	✗.	✗.	?.
Conflict	↯	↯	↯	↯	↯	?.
Unknown	?.	?.	?.	?.	?.	?.
Weakly Denied	✗.	✗.	✗.	✓.	✓.	?.
Denied	✗	✗	✗.	✓.	✓.	?.

12 pav. Įvertinimo etiketės ir jų kūrimo taisyklės. [8]

Standartas ISO 17799

ISO 17799 standartas naudojamas informacijos saugumo valdyme. Standartas padeda nustatyti saugumo reikalavimus. Standartas taip pat pateikia kelis aspektus, nuo kurių vertėtų pradėti, vertinant saugumo grėsmes [28]:

- Informacijos saugumo politikos sudarymas;
- Atsakomybės paskirstymas;
- Įspėjimai ir apmokymai apie informacijos saugumo svarbą;

- Teisingas procesų vykdymas;
- Techninių pažeidžiamumų valdymas;
- Veiklos tęstinumo valdymas;
- Informacijos saugumo incidentų valdymas.

Kritiniai saugumo faktoriai:

- Informacijos saugumo politika, tikslai ir veiklos, kurios atspindi veiklos tiksluose;
- Bandymas įdiegti, palaikyti, stebėti ir gerinti informacijos saugumą, kuris yra suderinamas su organizacijos kultūra;
- Įsipareigojimas visuose valdymo lygmenyse;
- Geras supratimas informacijos saugumo reikalavimų, rizikos įvertinimas ir jos valdymas;
- Informacijos saugumo efektyvi rinkodara visų tipų valdytojams, darbuotojams ir kitoms šalims;
- Paskirstymo gairės dėl informacijos saugumo politikos ir standartų visiems vadovams
  darbuotojų ir kitų šalių;
- Steigimas tam tikrų veiklų, kurios valdytų informacijos saugumą;
- Teikiant tinkamą informuotumą, mokymą, švietimą;
- Kuriant veiksmingą informacijos saugumo incidentų valdymo procesą;
- Įvertinimo sistema, kuri vertintų informacijos saugumo valdymą.

ISO 17799 apima beveik visas saugumo sritis: žmogiškųjų resursų sauga, fizinė ir aplinkos sauga, komunikacijų, operacijų saugumas ir kt.

Standartas ISO / IEC 13335

Standartas ISO 13335 apžvelgia informacines technologijas, saugumo technikas ir jų valdymą. ISO 13335 aprašo koncepcinius saugumo valdymo modelius informacijos ir komunikacijos technologijų. Saugumo modeliai apima komunikacijos technologijų saugumo (angl. ICT - communications technology security) planavimą, diegimą ir vykdymo fazes, įskaitant palaikymą. Šis standartas labiausiai orientuotas į informacijos perdavimo apsaugą [29].

Šiuolaikinėje aplinkoje, kuomet organizacijos yra susietos ryšiais, jų generuojama informacija gali būti kritinė ir lengvai pažeidžiama.

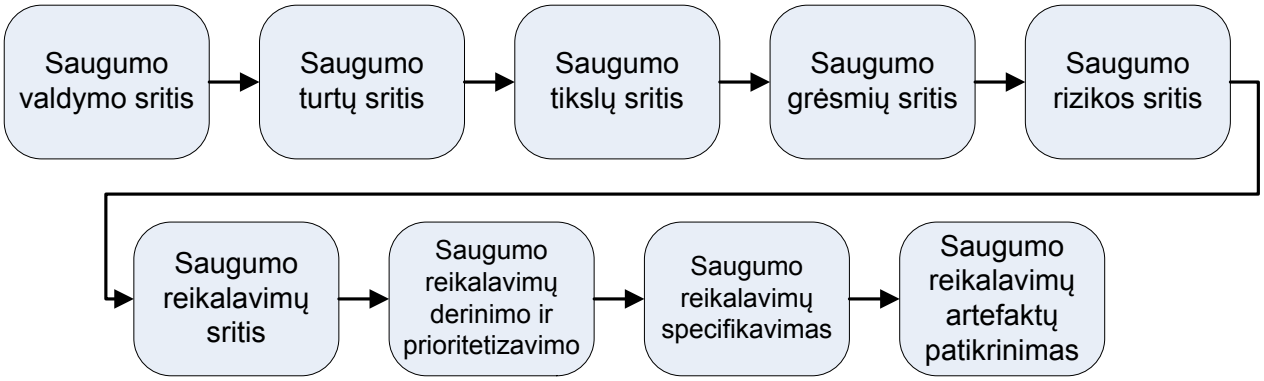
Šis formatas suteikia aukšto lygmens saugumo valdymo apžvalgą. Tai naudinga valdytojams ir tiems, kurie prižiūri informacijos perdavimo kanalus.

ISO 13335 sudėtis:

- Terminų žodynas susijęs su ISO 13335;
- Didžiausių saugumo elementų ir jų ryšių aprašymas;

- Įmonės saugumo tikslų, strategijos ir politikos reikalingumas efektyviam saugumo užtikrinimui;
- Atsakomybė už ryšius;
- ICT saugumo valdymo funkcijų apžvalga.

2.6.3. Saugumo reikalavimų inžinerijos procesas



13 pav. Saugumo reikalavimų inžinerijos procesas [9]

Saugumo vadovavimo apimtis

Paveikslėlyje 13 pažymėta visos saugumo reikalavimų inžinerijos proceso veiklos. Ši veikla sudaryta iš tokių užduočių: saugumo branduolio panaudojimo saugyklos patobulinimas (naujausi artefaktai ir nuorodos); identifikavimas specifikacijos tarpininkų, saugumo apibrėžimų derinimas; saugumo aplinkos identifikavimas (saugumo politika, saugumo reikalavimai, teisės, apribojimai, saugumo reikalingumas ir saugumo prieinamumo kriterijus toks kaip įvertinimo užtikrinimo lygis. Įvairių tipų išteklių įvertinimas ir saugumo tikslai, saugumo požymių nustatymas (bendrumai ir kintamumai), saugumo kaštų įtaka ir rizikos paviršutinis įvertinimas[9].

Saugumo turtų aprašų apimtis

Ši veikla sudaryta iš tokių užduočių: saugumo aprašų identifikavimas kiekvienam aprašui ir aplinkai; saugumo prielaidos, saugumo aprašų apimtis, kurie tikslai identifikuojant komponentus bus panaudojami pakartotinai, pakartotiniai ir kintamieji aprašai; priklausomybių identifikaciją tarp saugumo aprašų.

Saugumo tikslų apimtis

Ši veikla sudaryta iš tokių užduočių: saugumo tikslų identifikavimo (bendroji ir kintamoji analizė) kiekvienam aprašui; saugumo tikslų modeliavimas ir specifikacija; aprašų įvertinimas su jiems susietais saugumo tikslais.

Saugumo grėsmių apimtis

Ši veikla sudaryta iš tokių užduočių: pažeidžiamų vietų nustatymas viešuosiuose domenų šaltiniuose; įsilaužimų medžio identifikavimas, siejant su veiklos modeliu ar saugumo produktų linijos domenu; piktnaudžiavimo atveju identifikacija ir kiekvienam saugumo objekto grėsmei ir aprašui, nes kiekvienas aprašas turi piktnaudžiavimo atvejo galimybę, kuriai turi būti suteikta prevencija, kad saugumo objektas būtų užtikrintas. Piktnaudžiavimo atvejų modeliavimas ir specifikavimas; saugumo tikslų patvirtinimas prieš galimų piktnaudžiavimo atvejų modelius ir sąrašus.

Saugumo rizikos įvertinimas

Ši veikla sudaryta iš tokių užduočių kurios užtikrintų pasiekti 100% rizikos sumažinimą: įvertinama ar grėsmės yra įmanomos specifikuotose saugumo tiksluose; įvertinama saugumo rizika grėsmėse, jų tikėtinumas ir jų potenciali neigiama įtaka, priklausanti nuo įvairių tikslų. Tam nustatyti naudojamas ISO/IEC 13335 (GMITS), paaiškina kaip naudoti rizikos įvertinimo procesą.

Saugumo reikalavimų apimtis

Ši veikla sudaryta iš tokių užduočių: saugumo reikalavimų išgavimas, tinkami saugumo reikalavimai ir tinkamas saugumo reikalavimų paketas, kurie sumažina piktnaudžiavimo atvejų grėsmes iki tinkamo naudoti lygio dėl atitinkamos rizikos įvertinimo. Pagrindinių saugumo reikalavimų identifikavimas, atsižvelgiant į pasirinktus ankstesnių analizių reikalavimus; apibrėžiami įvairūs reikalavimai kintamumo priklausomybes; saugumo reikalavimų modeliavimas; leidžiamų CC operacijų aprašymas CC (iteracija, užduotys, atrankos išgryninimas); saugumo metrikų, testų apibrėžimai ir atsakomoji priemonė kiekvienam saugos reikalavimui. Vadinasi, šios veiklos pabaigoje turi būti identifikuoti atsižvelgiant į ISO/IEC 17799:2005 funkcionalumas, užtikrinimas, ir organizacijos saugumo reikalavimai, kartu su saugumo reikalavimai IT vystymuisi ir operacine aplinka turi būti specifikuota.

Saugumo reikalavimų derinimas ir prioritizavimas

Ši veikla sudaryta iš tokių užduočių: tarpusavio priklausomybės su kitais funkciniais ir nefunkciniais reikalavimai ir kompromisai saugumo modelio nepastovume ir stačiakampiame nepastovumo modelyje; balansuojama ekonominės įtakos rizika su atsakomosiomis priemonėmis.

Saugumo reikalavimų specifikavimas

Ši veikla sudaryta iš tokių užduočių: saugumo reikalavimų modeliavimas ir saugumo reikalavimų specifikacija.

Saugumo reikalavimų artefaktų aptikimas

Ši veikla sudaryta iš tokių užduočių: patikrinti ar saugumo reikalavimai atitinka ISO/IEC27001 kontrolės tikslus ir ISO/IEC15408 užtikrina reikalavimus IEEE830-1998 standartui, nes atsižvelgiant į šį standartą, kokybės reikalavimai turi būti teisingi, nedviprasmiški, išbaigti, nuoseklūs, surūšiuoti, stabilūs, tvirtinami, modifikuojami ir atsekami.

2.6.4. Veiklos procesų saugumas

Veiklos procesai yra laikomi svarbiu klausimu daugeliui įmonių, nes jos yra pagrindas siekiant išsaugoti konkurencingumą. Be to, veiklos procesai yra svarbūs programinės įrangos kūrėjams, nes jie turi būti užfiksuoti programinės įrangos projektavime ir kūrime. Be to, veiklos procesų modeliavimas yra pačiame centre, norint pagerinti verslą. Saugumas yra svarbus veiklos efektyvumui, tačiau tradiciškai jis sprendžiamas po veiklos procesų apibrėžimo. Empiriniai tyrimai rodo, kad veiklos procesų lygyje vartotojai, galutiniai vartotojai ir verslo analitikai gali nustatyti savo saugumo poreikius. [13]

Sėkmingas organizacijos raktas - išlaikyti organizacijos konkurencingumą yra bendrovės sugebėjimas aprašyti, standartizuoti ir pritaikyti tai, kaip ji reaguoja į tam tikrus verslo įvykius ir kaip ji sąveikauja su tiekėjais, partneriais, konkurentais, ir klientais. Veiklos procesai, apibrėžti kaip veikla procedūrų ar veiklų, kuri bendrai skatina veiklos tikslo siekimą ar tikslą, tai labai geras atsakymas į aplinkos daugialipyškumą, naujų produktų greičio augimą ir didesnį skaičių dalyvaujančių subjektų organizacijos veikloje.[14]

Nauja veiklos scena, kur yra daug dalyvių ir intensyviai naudojamos ryšių ir informacinės technologijos, įtakoja, jog įmonės ne tik plečia savo verslą, bet ir didina įmonės pažeidžiamumą didinančius veiksnius.

Pasekmė gali būti tokia, kad anksčiau ar vėliau didėjant atakų skaičiui sistemoje, bus įsilaužta į sistemą. Ši saugumo pažeidimas sukelia didelius nuostolius. Dėl šios priežasties, būtina

apsaugoti kompiuterius ir jų sistemas. Geriausias galimas saugumas, nebūtinai reiškia visišką saugumą, bet pagrįstas aukštas apsaugos lygis atsižvelgiantis į apribojimus.

Saugumo sąvoka yra dažnai atmetama veiklos procesų modeliuose, kurie paprastai yra sukoncentruoti į modeliavimo procesą taip, kad būtų galima įrodyti funkcinį teisingumą. Priežastis yra dėl to, kad verslo procesų domeno ekspertas nėra saugumo ekspertas. Dažnai, saugumas taikomas po sistemos apibrėžimo.[15]

Šis požiūris dažnai veda prie problemų, kurios patampa saugumo spragomis, kurioms reikia padidinti pasirengimo etapus, kur taisyti klaidas yra žymiai pigiau. Be to, inžinieriai nėra apmokyti visų saugumo reikalavimų, ir tik keletas iš jų kurie buvo mokyti, jiems buvo duota tik apžvalga saugumo architektūros mechanizmų, pavyzdžiui, slaptažodžiai ir šifravimas, bet ne tinkamas mokymas aktualiuose saugumo reikalavimuose.

Empiriniai tyrimai rodo, kad veiklos proceso lygyje klientai ir galutiniai naudotojai galėtų pareikšti savo saugumo reikalavimus tuomet galima lengvai identifikuoti pagal tuos, kurie modeliuos veiklos procesus.[17]

Veiklos procesų modeliavimui yra keletas galimybių juos aprašyti. BPMN (angl. Business Process Modeling Notation) ir UML (angl. Unified Modeling Language) yra nustatyti pagrindiniai standartai, vis dėl to yra galimybė patikrinti saugumo aspektus, kurie nėra įtraukti į veiklos proceso modeliavimą ir yra įtraukti į BPMI (angl. Business Process Management Initiative) arba naujoje versijoje kurią iškėlė OMG (angl. Object Management Group).

Saugumas veiklos procese

Nepaisant veiklos procesų saugumo svarbos, nustatytos dvi problemos. Pirmoji yra tai, kad nebuvo pakankamas modeliavimas, nes tie, kurie specifikuoja saugumo reikalavimus yra reikalavimų inžinieriai, kurie atsitiktinai buvo linkę naudotis architektūros specifiniais apribojimais, o ne saugumo reikalavimais. Ir antroji - saugumas buvo integruotas „ad-hoc“ būdu, dažniausiai faktinio įgyvendinimo procese, sistemos administravimo fazės metu.

Saugumo reikalavimai, kurie gali būti modeliuojami veiklos procesuose, bet kokiame taikomajame abstrakcijos lygyje bus vertinami kaip pažeidžiamasis turtas.

Dar daugiau, reikia pasakyti, kad surinkti visus saugumo reikalavimus yra didelis ir sunkus darbas ir tai turi būti daroma nuo pačios pradinės sistemos kūrimo stadijos. Verslo žinovai siūlo veiklos struktūrą, kuri yra labai tinkama saugumo reikalavimų atrinkimui ir specifikavimui. Veiklos procesų pristatymai tokiu būdu gali parodyti sistemos kūrimo fazes visais skirtingais lygiais. Todėl manoma, kad verslo analitikas gali integruoti savo požiūrį į verslo saugumą į veiklos procesų perspektyvą ir į papildomus saugumo reikalavimus, nes bet kokia aukščiausio lygio taikomoji abstrakcija turės tuos pačius pažeidžiamuosius turtus.

Galiausiai nė viena iš pasiūlymų, susijusių su saugumo specifikacijomis, dėl veiklos procesų ir ar informacinių sistemų, kurie buvo išanalizuoti saugumo reikalavimų specifikacijose, nebuvo sukurtos veiklos analitikų. Manoma, kad tokia perspektyva suteiks saugumo specifikacijoms daugiau reikšmės, kai bus leidžiama saugumo ekspertams įtraukti naujus elementus į analizes. Standartinių kalbų patobulinimas veiklos procesams, gali tik pagelbėti veiklos procesų aprašymus.

Veiklos procesų modeliavime, pagrindinis tikslas yra skatinti realybės aprašymą, pavyzdžiui kaip komercinis sandoris yra atliekamas, jį suprasti ir galiausiai jį pakeisti siekiant jį patobulinti. Kaip pasekmė, yra svarbu turėti žymėjimą, kuris leidžia mums modeliuoti veiklos esmę kuo aiškiau. Šis žymėjimas turi leisti mums įtraukti skirtingas perspektyvas, suteikiant vietą diagramoms, taisyklėms, tikslams, ir ne tik veilos uždavinių ryšiams, bet ir sąveikoms parodyti.[18]

Didžioji modeliavimo sėkmės dalis yra gebėjimas išreikšti veiklos skirtumus ir poreikius, taip pat reikia turėti žymėjimą, kur šie poreikiai gali būti aprašyti. Štai kodėl renkantis metodą ar žymėjimą, modeliuojamo objekto savybės turi būti įtrauktos, į tai turi būti atsižvelgta, kitaip tariant, veiklos procesai, aplinkos ypatumai ir pagrindinės panaudojimo priežastys.

Tarp metodų, kurie buvo naudojami veiklos procesų modeliavimui, galime išskirti šiuos: srautų diagramos (IDEF) integracijos apibrėžtis funkciniam modeliavimui, Petri tinklai, simuliacija, žiniomis grindžiami metodai, ir rolių veiklos diagramos.
Šiuo metu ir atsižvelgiant į veiklos procesų modeliavimo pramonės būklę, galima nustatyti, kad UML ir BPMN yra tarp pagrindinių standartų.

Dėl BPMN, tai yra naujas pasiūlymas žymėjimo aprašymui unikalus procesų diagramų atstovavimas BPD.

Norint užfiksuoti saugumo reikalavimus kartu su veilos procesų modeliavimu, yra naudinga turėti žymėjimą, jis turi turėti grafinį sąvokų rinkinį, kuris leidžia atvaizduoti saugumo semantiką. BPMN siūlo veiklos orientaciją į veiklos analitiko domeną, nes ji sudaro galimybę užfiksuoti saugumo reikalavimų abstrakcijas.18]

BPMN notacijos elementai pateikti prieduose 4 dalyje.

BPMN negali aiškiai aprašyti saugumo reikalavimų mechanizmų. Tačiau, tarp simbolių rinkinio, kurie buvo naudojami BPD (angl. Business Process Development) konstrukcijai, artefaktai gali būti naudojami tokių reikalavimų išreiškimui. Artefaktai buvo sukurti modeliavimo pagrindų žymos išplėtimui, įtraukiant į juos galimybę atvaizduoti specifines situacijas. Jie yra sudaryti iš objektų duomenų, kurie leidžia parodyti reikalaujamą veiklos produkciją, grupė kuri leis sujungti kelias veiklos rūšis, siekiant, kad būtų lengvesnė analizė, pagerinti dokumentų ir teksto anotacijas.. Nepaisant to, kad artefaktai gali būti naudojami išreikšti saugumo reikalavimus, daugiausia per teksto anotacijas, nustačius tikslius jų identifikatorius, bus lengviau modeliuoti.18]

2.7. Architektūros ir galimų įgyvendinimo priemonių variantų analizė

Saugumo reikalavimai skirtingoms informacinėms sistemoms skiriasi. Dažnai saugumo lygis informacinėse sistemose priklauso nuo tos sistemos atliekamo darbo, bei nuo savininkų piniginių išteklių. IS saugumo lygi nustatyti yra taip pat labai sunku, dažniausiai saugumas matuojamas įvairiais koeficientais. Nėra visiškai saugios ar patikimos sistemos. Saugumo lygis gali būti nurodomas koordinačių plokštumoje, kurios skalė būtų nuo 0 iki 1, nuo visiškai nesaugios iki pilnai saugios. Saugi sistema tai tokia, kuriai nulaužti reikia labai daug laiko ir pinigų. Be to rizika būti pagautam yra labai didelė.[20]

Padidintas saugumas dažnai lemia padidintas išlaidas informacinei sistemai. Saugumo kaina susideda iš daugybės faktorių – padidintų sistemos prižiūrėjimo kaštų, padidintų išlaidų sistemos patikimumui. Galima padidinti sistemos saugumo lygį, bet tai sąlygotų sumažintą funkcionalumo lygį. Todėl turint tam tikrą išlaidų normą reikia išlaikyti balansą tarp visų sistemos savybių.

Kai sistemos saugumas artėja prie 100 procentų, eksponentiškai padidėja ir išlaidos.

Saugumo politika

Kiekvienai svarbiai informacinei sistemai turi būti sukuriama saugumo politika. Saugumo politika tai taisyklių rinkiniai, kurie nusako kas yra draudžiama ir kas yra galima sistemoje, jos veikimo metu.

Saugumo politika reguliuoja, kaip esybės gali gauti priėjimą prie sistemos objekto. Saugumo politika turėtų nusakyti gerai subalansuotą, ekonomiškai efektyvią sistemos apsaugą. Kartais saugumo politika yra nusakoma patikimumo atžvilgiu, sudarant sistemos nesėkmių semantiką, kuri nusako kokias atvejais sistema gali pradėti netinkamai veikti.[21]

Grėsmių analizė yra taip pat svarbi pagalba , sudarant saugumo politiką. Grėsmių analizė tai yra procesas, kuriame identifikuojamos visos galimos grėsmės sistemai. Šio proceso metu yra sudaromas grėsmių sąrašas ir kiekvienos grėsmės pavojingumas. Vėliau toks sąrašas, kuriant saugumo politiką, gali būti naudojamas kaip pagrindas.

Kada yra sudaroma saugumo politika, reikia pasirinkti saugumo priemones, spręsti saugumo politikos klausimus. Kuomet saugumo politika yra sukurta, yra svarbu suprasti, kaip taisyklės veikia, galima rinktis saugumo sprendimus. Todėl, kuriant saugumo politiką reikia ją kurti ne tik teisingą, bet, kad ji tenkintų ir praktinius sistemos reikalavimus. Įrankiai naudojami užtikrinti saugumą turi būti pakankamai geri ir tuo pat metu lengvai panaudojami, kad juos galėtų priimti ir naudoti sistemos vartotojai.

Bet koks veiksmas – tyčinis ar netyčinis, kuris pažeidžia taisykles aprašytas saugumo politikoje yra saugumo pažeidimas.

Formalus saugumo modelis yra taisyklių matematinis formalizavimas (aprašymas), kurios paminėtos saugumo politikoje ir gali būti panaudotos matematiškai įrodant įvairias sistemos savybes. Formalus saugumo modelis turi būti aprašytas specifikavimo kalba arba formalia kalba.

Grėsmės

Grėsmės yra potencialūs saugumo pažeidimai ir egzistuoja dėl pažeidžiamumų, tam tikrų trūkumų sistemoje. Egzistuoja du grėsmių tipai: atsitiktinės grėsmės, kurios paviešina konfidencialią sistemos informaciją ar kitaip sutrikdo sistemos darbą ar priverčia ją dirbti ne pagal nustatytas procesus, kitas tipas yra atakos, kurios nusakomos kaip tyčinės grėsmės.[14]

Atsitiktinės grėsmės

Atsitiktinės grėsmės gali būti suprantamos kaip rezultatas objekto paviešinimo arba jo modifikacija. Paviešinimai gali įvykti ir dėl techninių ir dėl programinių nesėkmių, taip pat dėl vartotojo klaidų, taip pažeidžiant objekto konfidencialumą. Tai gali įvykti, kai vartotojas išsiunčia elektroninį laišką ne tam asmeniui.

Atsitiktinė grėsmė gali būti ir tuomet kai pažeidžiamas sistemos objekto integralumas, tai gali įvykti įvedus objektą į neleistiną būseną.

Atakos

Ataka yra tyčinė grėsmė ir ji vykdoma tam, kad būtų pažeidžiamas sistemos saugumas. Atakos gali būti destruktyvios, modifikuojančios, suklastojančios, įsiskverbiančios, užkertančios duomenis. Atakos pasekmė yra informacijos atskleidimas ar modifikavimas objekto integralumo.

Saugumo pažeidimas visada yra neteisėtas priėjimas prie objekto. Įsilaužėlis gali vykdyti savo atakas pažingsniui, kur kiekviename žingsnyje pažeidžiamas sistemos objektas. Pavyzdžiui įsilaužėlis gali iš pradžių bandyti laužtis į vartotojų duomenų bazę, vėliau radus kitas vartotojų paskyras, bandyti įsilaužti į kitas sistemas.[15]

Atakos gali būti tiesioginės ir netiesioginės. Tiesioginė ataka yra nutaikyta tiesiogiai į objektą, keletas sistemos komponentų gali būti prieš tai atakuojami, kol galutinis objektas bus pasiektas. Netiesioginėje atakoje informacija yra gaunama apie objektą, ne atakuojant jo paties. Įsilaužėlis gali kaupti tam tikrą statistiką, kitus duomenis ir iš jų surinkti jam reikalingą informaciją apie objektą. Netiesioginės atakos yra problema sistemose, kur galima netiesioginėmis užklausomis apie objektą iš duomenų bazės surinkti informaciją, kuri apibūdins tą objektą.

Yra aktyvios ir pasyvios atakos. Pasyvios atakos yra užbaigiamos, stebint sistemos veiklą, jos užduotis ir renkant informaciją. Pasyvias atakas aptikti yra labai sunku, nes jos nesąveikauja ir nepaveikia normalaus sistemos darbo. Dažniausiai tokios atakos būna stebint tinklo srautą, procesorių veiklą, diskų vieta ir kitus parametrus.

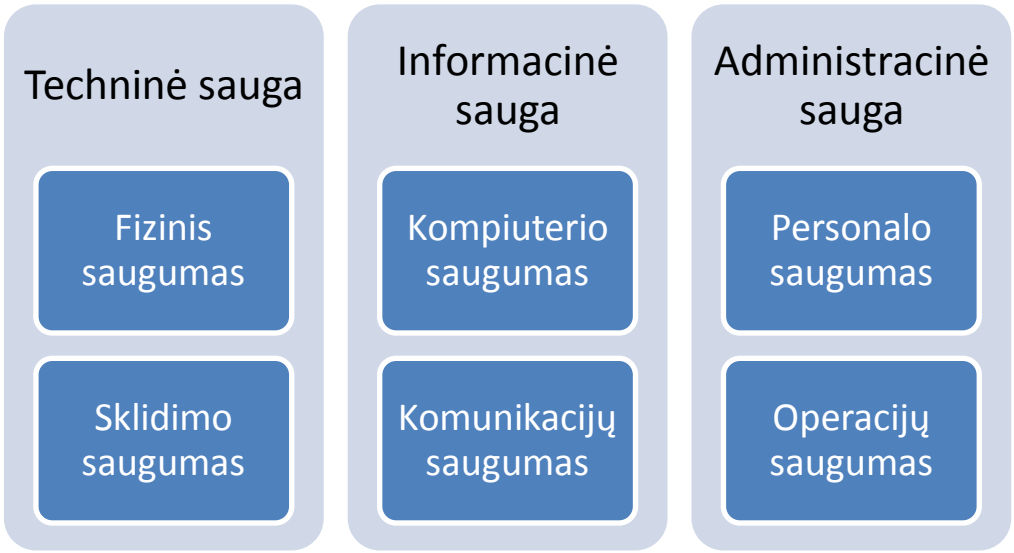
Aktyvi ataka pakeičia sistemos procesus. Tai gali būti tarkim įrašoma papildoma funkcija kuri suteiktų įsilaužėliui tam tikrą naudą.

Saugumo aspektai

Konfidencialumas ir integralumas yra saugumo aspektai. Sistemose, kur patikimumas yra esminis faktorius, visi objektai sistemoje turi būti apsaugoti nuo tyčinių ir netyčinių grėsmių. Vartotojui nėra skirtumo ar kas nors serverį išjungs, nutrauks laidą, ar dings elektra, visi atvejai sustabdys sistemos darbą.

Saugumo formos

Įsilaužėlis gali bandyti laužtis į keletą sistemos objektų, kad rastų jam reikalingos informacijos: gali būti bandoma laužtis į sistemos programinę įrangą, taip pat į fizinę kompiuterio būvimo vietą, gali būti papirkinėjami sistemos vartotojai, todėl reikia saugumą išskirstyti į skirtingas dalis arba saugumo formas (14 pav.), kuriose bus panašių saugumo charakteristikų užtikrinimas. [23]



14 pav. Saugumo formos.

Su techniniais įtaisais susiję saugumo klausimai

Technikos saugumo klausimai susiję su objektų pažeidžiamumu dėl IS techninės įrangos. Techninės įrangos sauga gali būti skirstoma į fizinę ir sklidimo saugumą.

Fizinis saugumas sprendžia techninės įrangos apsaugojimą nuo išorinių fizinių veiksmų, tokių kaip, klastojimo, vagystės, žemės drebėjimų, vandens potvynių ir kitų. Visą įrangą, kuri tvarko ar saugo svarbią informaciją, reikia apsaugoti. Neturi būti sudaryta galimybė įsibrovėliui pasisavinti kietąjį diską ar jį apkeisti kitu, ar pakeisti įrangą, kad ji rinktų duomenis. Šios problemos bus

išspręstos, jei techninę įrangą patalpinsime saugioje tam pritaikytoje aplinkoje (duomenų saugyklose), kur priėjimą turi ne vienas asmuo, bet keletas ir jie prieiti prie techninės įrangos gali tik vienu metu.

Sklidimo saugumas sprendžia problemas susijusias su signalų (informacijos) sklidimu iš sistemos techninių įrenginių. Gali būti garso signalai (spausdintuvų darbas), vaizdinė informacija (tam tikri ekranai gali būti matomi per langą).

Informacinio saugumo klausimai

Informacijos saugumas yra sistemos objektų apsaugojimas per pačios sistemos architektūrą, apjungiant programinę ir techninę įrangą. Informacijos saugumas skirstomas į kompiuterių ir komunikacijų saugumą.[20]

Kompiuterių saugumas susijęs su objektų išviešinimu ir sistemos architektūros pažeidžiamumu. Kompiuterių saugumas sprendžia daugybę klausimų, kaip turėtų veikti programos kompiuteryje, kad vykdytų saugumo politiką, kokia turėtų būti prieigos kontrolė, kokių įrenginių reikia operacinei sistemai ir kt.

Komunikacijų saugumas sprendžia klausimus susijusius su informacijos pernešimo apsaugojimu. Kaip objektai yra pernešami, ar tarp kompiuterių, ar lokaliai. Komunikacijos turi būti apsaugotos, kad įsilaužėlis negalėtų pakeisti informacijos, ar kitaip ja pasinaudoti.

Administracinio saugumo klausimai

Administracinis saugumas yra objektų apsauga nuo vartotojų ir grėsmių tykančių saugumo organizacijoje. Administracinis saugumas yra padalinamas į dvi grupes – personalo ir operacijų saugumą.

Personalo saugumas susijęs su objektų apsaugojimu nuo įgaliotų vartotojų. Sistemos vartotojai turi priėjimą prie įvairių objektų ir saugumo mechanizmai prieš sąmoningai piktnaudžiaujančius vartotojus yra beveik nereikalingi, dažniausiai uždedamos apribojančios teisės. Priežastys, kodėl vartotojai laužtųsi į sistemą yra įvairios: įsilaužėlio papirkinėjimas, apgaudinėjimas, asmeninis pinigų troškimas, tai tarsi protinis iššūkis, asmeninis kompanijos baudimas. Taip pat personalo saugumas apima tokias sritis kaip įgaliotų asmenų pamiršimas atsijungti iš sistemos ir kt.

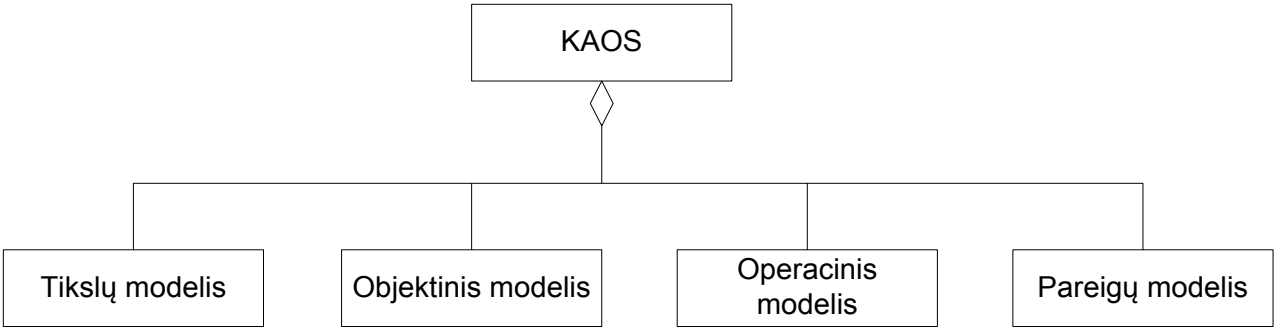
Operacijų saugumas susijęs su objektų saugumu organizacijoje, kuri palaiko saugumą sistemoje. Operacijų saugumas reguliuoja kaip visos kitos saugumo formos turėtų būti įgyvendintos ir kaip sistema turėtų būti valdoma. Operacijų saugumas tai padaro vykdydamas saugumo politikos taisykles, kokias priemones taikyti, kai yra aptinkami pažeidimai, kokius atstatymo mechanizmus taikyti ir pan.

Visos šešios saugumo formos detalizuotos 3 lentelėje.

Lentelė 3. Saugumo formų charakteristikos.

Kategorija	**Saugumo forma**	**Aspektas**	**Atakų taikinys**	**Pavyzdys**	**Pirminis saugumo mechanizmas**
Techninė	Fizinė	Konfidencialus ir intelektualinis	Techninė įranga	Vagystės, modifikacijos	Techninė įranga
	Sklidimo	Konfidencialus	Techninė įranga	Siųstuvai	Techninė įranga
Informacinė	Kompiuterių	Konfidencialus ir intelektualinis	Programinė įranga (techninė įranga)	Programinė įranga modifikavimas	Programinė įranga (techninė įranga)
	Komunikacijų	Konfidencialus	Informacija	Informacijos įrašymas	Kodavimas, techninės įrangos
		Intelektualinis	Programinė įranga	Komunikacijų veikimas	Kodavimas, programinė įranga
Administracinė	Personalo	Konfidencialus ir intelektualinis	Žmonės	Įgalioti vartotojai	Taisyklės, mokymas
	Operacijų	Konfidencialus ir intelektualinis	--	Operacinės klaidos	Taisyklės, rengimas

KAOS



15 pav. KAOS modelių schema.[12]

KAOS objektinis modelis

Objektinis modelis (15 pav.) yra naudojamas dokumentuoti ir apibrėžti pritaikymo srities konceptus. Konceptai turi būti susiję su žinomais reikalavimais, jie turi nustatyti statinius apribojimus vykdomajai sistemai, kuri patenkintų reikalavimus. Dalis objektinio modelio objektų siejasi su kitais objektais, kurie buvo sukurti išreikšti reikalavimus ir vykdomajai sistemai. Kad ir koks būtų objekto tipas modeliuotojai turi suprasti, ką jis reiškia ir kodėl jis buvo sukurtas modelyje.[12]

KAOS objektiniame modelyje naudojami objektai:

- *Esybė* – vaizduoja nepriklausomą, pasyvų objektą. Pavyzdžiui: lifto durys, mygtukai ir kt. Nepriklausomas reiškia, kad šio tipo objektai gali neturėti sąsajų su kitais modelio objektais. Esybės gali turėti atributus, kurių reikšmės apibrėžia būsenų rinkinius, kuriuos esybė gali generuoti. Jei esybė yra – pasyvi, ji negali vykdyti jokių operacijų.
- *Agentas* – vaizduoja nepriklausomą, aktyvų objektą. Pavyzdžiui: lifto kompanija, keleivis, lifto kontrolierius ir kt. Aktyvus – reiškia, kad jis gali atlikti operacijas. Operacijos paprastai reiškia esybių būsenų kitimus.
- *Ryšys (angl. k. association)* - yra priklausomas, pasyvus objektas. Priklausomas nes jo aprašas nurodo (nukreipia) į kitus objektus. Pavyzdžiui ryšys sujungia grindis su siena. Tarkim yra ryšys tarp grindų (g) ir sienos (s). Tada operacija „AtskirtiSienaNuoGrindu“ reikš perėjimą: At(g,s) → not At(g,s).

Objektų identifikacija vyksta vykdant tikslų apibrėžimo procesų. Daugelis tikslų trumpųjų ir ilgųjų apibrėžimų, reiškia srities objektą, kuris turi būti modeliuojamas ir dokumentuojamas. Visi sumodeliuoti objektai, turi turėti savo esybes reikalavimo dokumento žodyno dalyje. Per peržiūras suinteresuotieji asmenys susitars dėl tam tikrų žodyno dalių.

KAOS operacinis modelis aprašo visas galimas elgsenas veikėjų, kurie turi išpildyti reikalavimus. Elgesys yra išreiškiamas operacijų terminais, kurios yra vykdomos veikėjų. Operacijos dirba su objektais (aprašytais objekto modelyje): jie gali kurti objektus, sužadinti objektų būsenas ir aktyvuoti jų operacijas (siunčiant įvykį).

Iš kur ateina operacijos? Yra du būdai jas identifikuoti:

Operacijos gali būti tiesiogiai išreiškiamos tarpininkų pokalbių metu. Tarpininkai yra atsakingi už esamos sistemos procesus pokalbių metu, bet ne už tikslus kurie turi būti pasiekti. Tuomet analitikas turi klausti specifinių klausimų, identifikuoti priežastis esančias už esamų procesų ir galbūt atskleisti tikslus identifikuojančius šiuos procesus.

Operacijos gali būti identifikuojamos žiūrint į egzistuojančius reikalavimus. Jie paaiškina kaip reikalavimai turi būti realizuojami.

Reikalavimas gali būti panaudojamas keleto objektų, arba keleto veikėjų arba abiejų kombinacijoje:

- Reikalavimai kurie aprašo statistines savybes sistemoje yra panaudojamos objektų. Pavyzdžiui, reikalavimas „Liftas įrengiamas su aukšto durimis“ bus panaudojamas su objektu „Aukšto durys“.
- Reikalavimai kurie aprašo dinaminės sistemos savybes yra panaudojami per operacijas.
- Reikalavimai kurie aprašo savybes su dinaminiu ir statiniu aspektu yra panaudojamos su objektais ir operacijomis. Pavyzdžiui, tikimasi kad „stop mygtukas panaudotas“ bus panaudojamas su operacija „spausti mygtuką“ ir „Mygtukas“ esybe.

MODAF

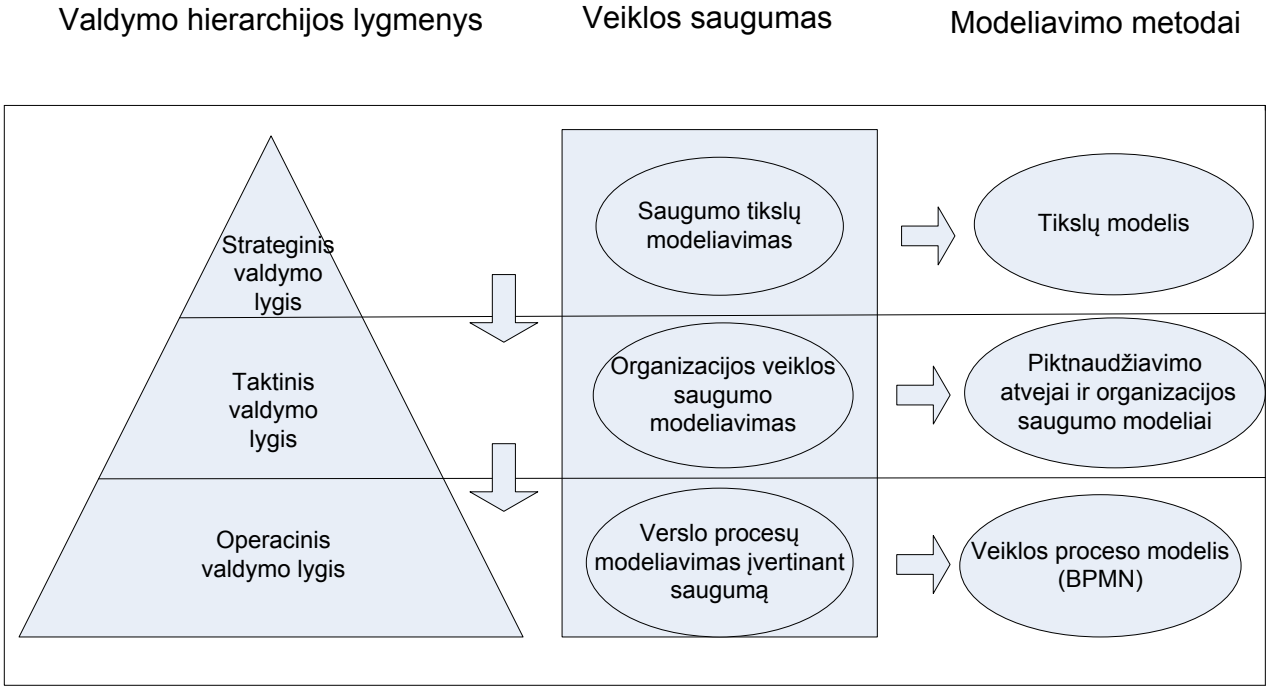
MODAF yra veiklos architektūros karkasas, kuris pateikia gausybę šablonų (notacijų) veiklos proceso gerinimui. Įmonės architektūros kūrimas yra sudėtingas procesas, todėl MODAF išskaido įmonės architektūrą į kelias sritis. Kiekviena sritis architektūra apibrėžia savais aspektais. Tai leidžia įvairių sričių specialistams dirbti, kuriant įmonės architektūrą.

MODAF sudarytas iš septynių požiūrių (angl. views):

- Strateginis požiūris (angl. Strategic View) – skirtas aprašyti veiklos gebėjimus, reikalingus valdymo procesui. Sudarytas iš šešių produktų- StV. Produktai aprašo tikslus, veiklos gebėjimus, veiklos fazes. StV-1 yra veiklos vizija, kuri aprašoma veiklos tikslais ir veiklos fazėmis. Šis produktas yra aukščiausio abstrakcijos lygio, todėl modeliuojamas pirmas, kiti strateginio požiūrio produktai naudoja šios veiklos vizijos elementus.
- Operacinis požiūris (angl. Operational View) – skirtas aprašyti loginiams mazgams, veikloms procesams ir informacijos srautams tarp procesų. Šį požiūri sudaro septyni produktai.
- Paslaugų požiūris (angl. Service View) – skirtas aprašyti paslaugoms, kurių reikalauja tam tikras architektūrinis dalyvis.
- Sisteminis požiūris (angl. System View) – skirtas aprašyti problemos sprendimui, iškeltai operaciniame lygmenyje. Sudarytas iš 12 produktų.
- Projektinis požiūris (angl. Ascuisition View) – aprašo programas, kurios vykdomos realizuojant strateginius gebėjimus. Programos siejamos su sisteminiais ir organizaciniais resursais. Sudarytas iš dviejų produktų.
- Techninių standartų požiūris (angl. Technical Standards View) – skirtas aprašyti techniniams ir netechniniams standartams, naudojamiems architektūroje. Sudarytas iš 2 produktų.
- Bendrasis požiūris (angl. All View) – šio požiūrio produktai pateikia informaciją, kuri yra susijusi su visa modeliuojama architektūra. Bendrojo požiūrio produktai:
    - AV-1- architektūros apžvalga ir santrauka, kuri identifikuoja architektūros tikslus, požiūrius, rekomendacijas, išvadas.
    - AV-2 – terminų žodynas, naudojamų architektūroje. [27]

2.8. Siekiamos sistemos apibrėžimas

Tyrimo tikslas yra sukurti metodiką, koncepcinį modelį, kuriuo remiantis būtų galima atvaizduoti vartotojų saugumo reikalavimų atitikimą organizaciniame ir sisteminiame (informacinės sistemos) lygiuose.



16 pav. Koncepcinis modelis.

Koncepciniame modelyje 16 pav. pavaizduota organizacijos valdymo hierarchijos lygmenys. Kiekvienam hierarchijos lygmeniui yra parinkti skirtingi modeliavimo modeliai. Strateginis valdymo lygis, kuris yra aukščiausio abstrakcijos lygio, yra pasirinktas saugumo tikslų modeliavimas, modeliuojamas tikslų modeliavimo metodu. Vidurinis hierarchijos lygmuo – taktinis valdymo lygis, jame modeliuojamas organizacijos veiklos saugumas panaudojant piktnaudžiavimo atvejų ir organizacijos saugumo modelius. Detaliausias hierarchijos lygmuo – operacinis valdymo lygis, jame modeliuojami veiklos procesai įvertinant saugumą, modeliuojant BPMN kalba.
Visi šie modeliai atitinka organizacijos hierarchijos lygius ir tarpusavyje yra lengvai siejami.

2.9.Darbo tikslas ir siekiami privalumai

Darbo tikslas yra sukurti metodiką, koncepcinį modelį, kuriuo remiantis būtų galima atvaizduoti vartotojų saugumo reikalavimų atitikimą organizaciniame ir sisteminiame (informacinės sistemos) lygiuose.

Palyginamojoje lentelėje (lentelė 4) lyginami piktnaudžiavimo atvejų ir i* karkaso saugumo reikalavimų aspektai. Iš palyginimo matosi, kad nė vienas metodas neišveda saugumo reikalavimų iš tikslų, o tai yra svarbu, nes nustatyti tam tikri saugumo tikslai organizaciją padarys patikimesnę. Taip pat lyginami metodai detaliai neišskaido saugumo reikalavimų.

Lentelė 4. Palyginamoji lentelė.

Palyginimo kriterijai	Piktnaudžiavimo atvejai	i* karkasas
Ar nagrinėja saugumo reikalavimus?	Taip	Taip
Ar nagrinėja saugumo reikalavimų priklausomybes?	Taip	Taip
Ar išveda saugumo reikalavimus iš tikslų?	Ne	Ne
Ar išskaido saugumo reikalavimus iki atominių vienetų?	Ne	Ne
Ar turi šablonus saugumo reikalavimams specifikuoti?	Taip	Ne
Ar gali būti atvaizduojami organizacijos objektai?	Taip	Ne
Ar gali būti atvaizduojami organizacijos objektai?	Taip	Ne

2.10. Analizės išvados

Išanalizuoti saugumo karkasai yra sunkiai pritaikomi praktikoje, nes kylančias grėsmes aprašo pernelyg abstrakčiai. Modeliuose sunku susigaudyti ne ekspertui, o programinės įrangos kūrėjams, kurie naudojo per daugelį metų nusistovėjusias saugumo reikalavimų metodikas, saugumo karkasai yra nepriimtini. Piktnaudžiavimo atvejus galima pritaikyti detalizuotoms sistemos dalims.

1. Piktnaudžiavimo atvejai leidžia atvaizduoti IS grėsmes.

2. Modeliuojant saugumo grėsmes yra svarbu pažymėti iš kur jos kyla – aktorių, kokius elementus pažeidžia ir kokie aktorių tikslai.
3. Piktnaudžiavimo atvejus galima pritaikyti detalizuotoms sistemos dalims.
4. Modeliuojamos saugumo priemonės turi būti nedviprasmiškos.
5. Saugumo užtikrinimo klausimas turi būti sprendžiamas IS modeliavimo pradžioje, nes tiesiogiai veikia IS efektyvumą.

3. Saugumo reikalavimų specifikacija ir analizė

3.1 Reikalavimų specifikacija

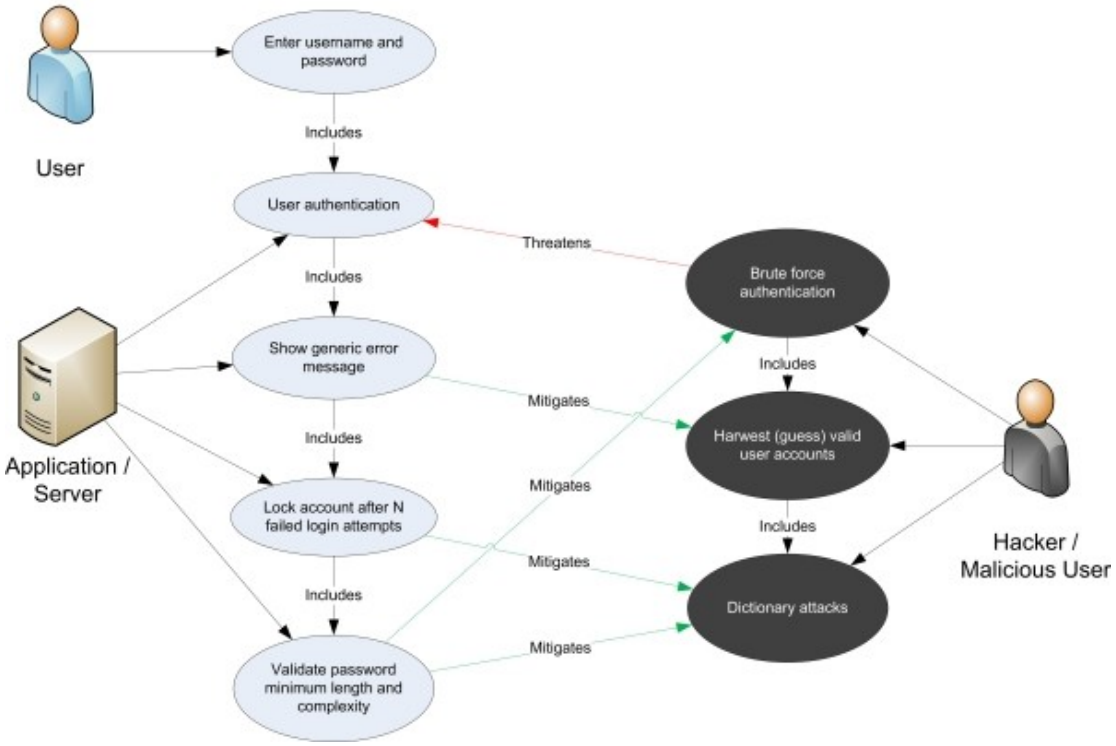
3.1.1. Piktnaudžiavimo atvejai

Panaudojimo atvejų modeliai tapo vienu dažniausiai naudojamų grafinių vaizdavimo būdų reikalavimų inžinerijoje. Bet jie neturi pakankamai atributų norint sumodeliuoti saugumo reikalavimus, grėsmes. Įprastuose panaudojimo atvejuose yra modeliuojamos sistemos funkcijos ir vartotojų priklausomybė nuo tų funkcijų. Piktnaudžiavimo atvejai apibrėžia ne funkcijas, o nepageidaujamą sistemos elgseną. Jie kuriami beveik tokia pat eiga kaip ir paprasti panaudojimo atvejai, didžiausias skirtumas, kad panaudojimo atvejai sukuria tam tikrą vertę sistemos savininkui, ar sistema suinteresuotiems asmenims, tuo tarpu saugumas yra nepaliečiamas.

Piktnaudžiavimo atvejų elementai:

Piktnaudžiavimo atvejis – seka veiksmų, kuriuos sistema ar kita esybė gali vykdyti, dažniausiai susijusi su piktnaudžiautojais (pažeidėjais) ir padaranti žalą jei ta seka bus įvykdyta (17 pav.).

Piktnaudžiautojas (pažeidėjas) – veikėjas, kuris tyčia ar netyčia sužadina piktnaudžiavimo atvejus.



17 pav. Piktnaudžiavimo atvejų pavyzdys [8]

Įprasti panaudojimo atvejų ryšiai: „include“, „extend“ ir „generalize“, gali būti panaudoti ir tarp piktnaudžiavimo atvejų, kaip ir asociacijų ryšiai tarp pažeidėjo ir piktnaudžiavimo atvejų. Bet yra ir specifinių ryšių piktnaudžiavimo atvejų diagramoje. Ryšys sumažinti (angl. mitigate) naudojamas tarp piktnaudžiavimo ir paprastų panaudojimo atvejų, kuomet tam tikras panašus atvejis sumažina vieno piktnaudžiavimo atvejo grėsmę. Ryšys grasinti (angl. threaten) naudojamas, kai piktnaudžiavimo atvejis trukdo arba pasinaudoja paprastu panašiu atveju.

Piktnaudžiavimo kaip ir paprasti panaudojimo atvejai turi savo specifikacijas – paprastą (5 lentelė) ir išplėstą (6 lentelė). Paprastoji specifikacija yra gaunama pridėjus lauką grėsmės (angl. threats).

Lentelė 5. Paprastoji piktnaudžiavimo atvejų specifikacija.

Pavadinimas	PA pavadinimas
Tikslas	nurodomas tikslas ir laukiami rezultatai
Aprašymas	PA aprašymas
Pagrindinis įvykių sąrašas	aprašomi PS veiksmai vykdant šį PA
Alternatyvūs scenarijai	nurodomi scenarijai, kurie gali vykti aktoriui pasirinkus ne pagrindinį, o kurį nors alternatyvų

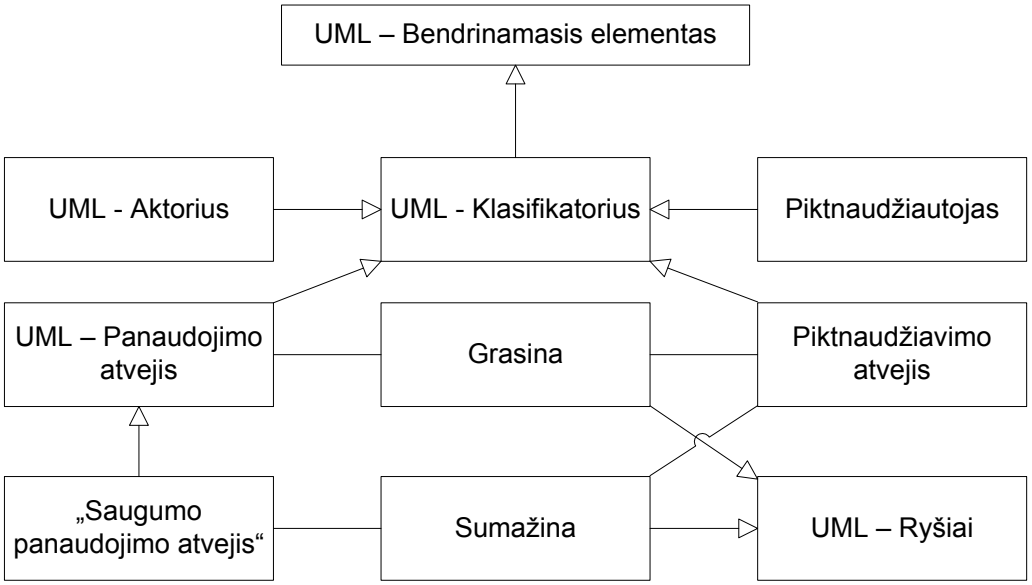
	arba neteisingą veiksmą
Pastabos	PA pastabos
Sužadinimo sąlyga	aprašomas įvykis, tiesiogiai inicijuojantis PA vykdymą
Prielaidos	PA prielaidos
Prieš sąlyga	aprašomos sąlygos, prie kurių vykdomas šis PA
Po sąlyga	aprašoma situacija (būsenos pokyčiai) įvykdžius šį PA
Veiklos taisyklė	Taisyklė aprašanti tam tikrus veiklos aspektus
Grėsmės	Grėsmės galinčios paveikti PA
Autorius	PA autorius
Data	Sukūrimo data

Praplėstoje piktnaudžiavimo atvejų specifikacijoje naudojami papildomi laukai:

Lentelė 6. Paprastoji piktnaudžiavimo atvejų išplėstoji specifikacija.

Piktnaudžiautojo profilis	prielaidos apie pažeidėją, tyčia ar netyčia veikia, ar asmuo iš vidaus, ar iš išorės veikia, kaip techniškai įgudęs gali būti
Sritis	taikinys, aprašytas piktnaudžiavimo atvejyje, detalus aprašymas kas yra taikinys, ar visas verslas, programinė įranga, žmonės ar kiti
Lygis	abstraktus lygis , kuris identifikuoja specifikaciją
Suinteresuoti asmenys ir rizikos	visas rizikas, kurios liečia veikėjus, įtrauktus į piktnaudžiavimo atvejus
Technologijų ir duomenų variantai	pažeidėjas gali naudoti skirtingas technologijas kiekvienam piktnaudžiavimo atvejui, čia aprašomos tos technologijos (WAP, kompiuteris, ...).
Technologijos ir paaiškinimai	žodynas techninių terminų ir kitų žodžių

Kaip UML panaudojimo atvejų metamodelis siejasi su piktnaudžiavimo atvejų metamodeliu pavaizduota 18 pav. Papildomai prie paprastų panaudojimo atvejų metamodelio yra pridėta „Piktnaudžiavimo atvejai“ ir „Piktnaudžiautojai“, todėl piktnaudžiavimo atvejai gali grasinti paprastiems atvejams. Taip pat metamodelis papildomas „Saugumo panaudojimo atveju“, kuris gali sumažinti žalą daromą piktnaudžiavimo atvejo. Saugumo panaudojimo atvejis UML klasių diagramoje užtikrina tam tikrų sistemos elementų saugumą.



18 pav. Piktnaudžiavimo atvejų metamodelis [2]

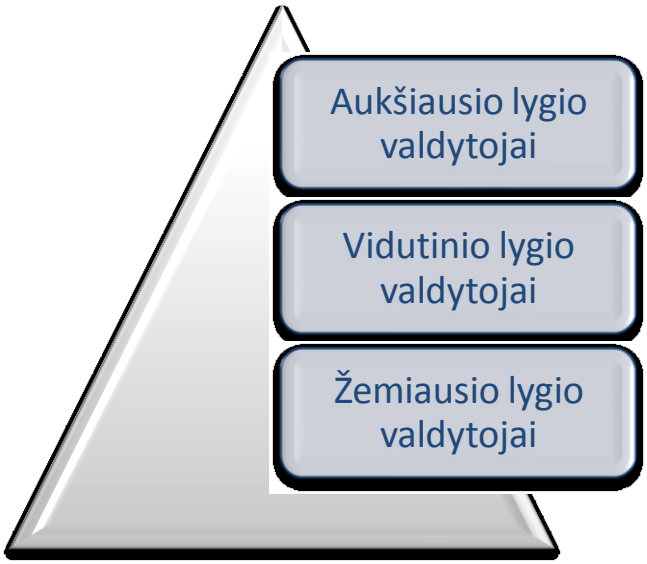
Taigi piktnaudžiavimo atvejai papildo saugumo reikalavimų procesą.

Saugumo reikalavimu inžinerijoje svarbu ne tik pasiekti sistemos atskirų elementų saugumą, bet ir užtikrinti jų saugumo elementų suderinamumą įvairiais lygiais – sisteminiu ir organizaciniu. I saugumo problemas yra svarbu pažvelgti ir iš organizacijos pusės (18 pav.). Organizacija pagal valdymo lygius skirstoma į tris lygius (19 pav.):

- aukščiausio lygio valdytojai – yra atsakingi už visos organizacijos veiklą. Jie nustato tikslus, veiklos kryptis, kurios turi vykdyti organizacijos misiją. Aukščiausio lygio valdytojai praleidžia daug laiko planuodami ir spręsdami didžiausias organizacijos problemas. Šio lygio valdytojai reprezentuoja įmonę prieš kitas įmones ar kitas organizacijas.

- vidutinio lygio valdytojai – šie valdytojai atsiskaitinėja aukščiausio lygio valdytojams ir prižiūri žemiausio lygio valdytojų veiklas. Šie valdytojai kuria ir įgyvendina įvairias veiklas, surasdami joms resursus, kad veiklos pasiektų tam tikrų rezultatų.
- žemiausio lygio valdytojai – prižiūri darbuotojus, koordinuoja jų veiklas, kad atliktas darbas tenkintų kompaniją. Jie mažiau įtraukti į planavimą ir labiau įtraukti į kasdienes operacijas.

Įvairiuose literatūriniuose šaltiniuose lygių pavadinimai būna nevienodi, bet jie atitinka tuos pačius abstrakcinius lygius.



19 pav. Organizacijos valdymo lygiai

Organizacijos valdymo lygiai yra abstraktūs ir reiškia ne tik žmones, bet ir visą jų aplinką. Todėl dažnai šie lygiai yra skirstomi taip:

Strateginis lygis (aukščiausias) – Ko mes siekiame ir kodėl?

Taktinis lygis (vidurinysis) – Ką verta daryti ir kada?

Operacinis lygis (žemiausias) – Kaip taisyklingai atlikti?

Kylant lygiais į piramidės viršų mažėja detalumo lygis ir didėja atsakomybė už ilgalaikius tikslus ir sprendimus. Leidžiantis piramidės lygiais žemyn didėja resursų poreikis, kasdienis priežiūros valdymas ir darbo atsakomybė.

Dažniausiai pažeidžiami komponentai - 7 lentelė (http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf):

Lentelė 7. Dažniausiai atakuojami komponentai.

Dažniausiai pažeidžiami komponentai
Pardavimo vietos sistema (angl. POS system)
Duomenų serveris
Aplikacijų serveris (angl. Applicationserver)
Interneto serveris (angl. Webserver)
Failų serveris
Vieša kiosko sistema (angl. publickiosksystem)
Autentifikacijos ar nuorodų serveris (angl. Authentication / Directory serve)
Atsarginė laikmena (juostos)
Dokumentai
Kompiuterizuotos darbo vietos
Nešiojami kompiuteriai
PIN kodu apsaugoti įrenginiai

Rizikos įvertinimo procesas yra būtinas, norint nustatyti, reikiamas naudoti saugumo priemones.

Rizikos nustatymo žingsniai:

- Grėsmių identifikavimas;
- Pažeidžiamumų identifikavimas;
- Kontrolės analizė;
- Galimybių nustatymas;
- Rizikos nustatymas.

4. Veiklos proceso saugumo modeliavimo projektas

4.1. Saugumo grėsmių identifikavimas

Taigi saugumo grėsmes suskirstėme į tris grupes: techninę, informacinę ir administracijos. Kiekviena ši grupė turi dar ir pogrupių. Techninės saugos grupė yra sudaryta IT technikos grupės. Svarbiausias IT technikos grupės elementas yra kompiuteris, nesvarbu koks būtų jo tipas (nešiojamas, mini ir kt.)

Daugelis įsilaužėlių turėdami kokį nors tikslą, dažniausiai atakuoja būtent kompiuterius ar serverius. Todėl yra sukurta daugybė kenkėjiškų programų ir būdų kaip apeiti šias sistemas. Svarbiausi jų tipai pavaizduoti 8 lentelėje.

Lentelė 8. Saugumo grėsmės.

ID	Grėsmė	Aprašymas	Grupė
1	Virusai (angl. Viruses)	Save platinti sugebanti kompiuterio programa. Kai kurie virusai atlieka kenksmingus veiksmus: trina persiunčia vartotojo duomenis, naudoja kompiuterio resursus ir kt. (http://lt.wikipedia.org/wiki/Virusas_(programa)).	Techninė
2	Duomenų nutekėjimai (angl. Data Leakage)	Tai informaciniai duomenų praradimai, per nešiojamas laikmenas ar internete (tinkle).	Techninė, Organizacinė
3	Trojanai (angl. Trojans)	Programa, atliekanti nepageidautinus veiksmus be kompiuterio naudotojo žinios, dažniausiai apsimesdama kita programa (http://lt.wikipedia.org/wiki/Trojos_arklys_(programa)).	Techninė
4	Web grėsmės (angl. Web Threats)	Tai su internetu susijusios grėsmės, kuomet naudojantis HTTP, HTTPS protokolais, el. paštu ir kt. metodais yra i6gaunama konfidenciali informacija (http://en.wikipedia.org/wiki/Web_threat).	Techninė
5	Šnipinėjimo programos (angl. Spyware)	Programa, kuri renka informaciją apie vartotojo naršymo įpročius ar kita informaciją, be jo sutikimo.	Techninė
6	Farmingas (angl. Pharming)	Vartotojų nukreipimas į netikrus puslapius, taip pasisavinant suvedamą informaciją. Gali būti atakuojami maršrutizatoriai, kuriuose keičiant adresus, vartotojas per savo maršrutizatorių automatiškai pasiektų fiktyvų puslapį.	Techninė
7	Fišingas (angl. Phishing)	Siekia išgauti konfidencialią informaciją pasinaudojant puslapių pavadinimais panašiais į jau egzistuojančių patikimų svetainių.	Organizacinė
8	Brukalas (angl.	Masiškai siunčiami laiškai, kurie fiktyviai bando ką	Organizacinė

	Spam)	nors įsiūlyti.	
9	SQL injekcija (SQL)	SQL kodo įrašymo metodas, kuris išnaudoja duomenų bazės sluoksnio pažeidžiamumus informacinėje sistemoje. Dažniausiai išnaudojama, kuomet į įvedimo laukus įrašoma SQL užklausa.	Techninė
10	Nutolusių skriptų pažeidžiamumas (angl. Cross-site scripting)	Pažeidėjas gali į neapsaugotus tinklapius įdėti java skriptus ar interneto adresus, kuriuos paspaudęs klientas nukeliaus į kenksmingą tinklapį, nors jis ir atrodys taip kaip originalus tinklapis.	Techninė
11	Automatinio įsilaužimo testas (angl. Brute force)	Šis būdas išnaudoja neapsaugotus laukelius formose, bandydamas visas įmanomas kombinacijas (dažniausiai slaptažodžių ir prisijungimo vardų), todėl jei duomenys saugomi duomenų bazėje yra šifruoti, tai netrukdo.	Techninė
12	Resursų perpildymas (angl. Buffer overflow)	Metodas, kuris išnaudoja laikinąją atmintį (angl. buffer), kuomet rašydamas į laikinąją atmintį, pasiekia jos dydžio ribas ir perrašo gretimą atmintį (angl. adjacent memory). Išnaudojamas per įvedimo laukelius. To pasėkoje sistema gali išmetinėti klaidų pranešimus, nustoti veikti, ar tapti pažeidžiama įsilaužimui.	Techninė
13	Sesijos kintamųjų išnaudojimas	Metodas, kuris išnaudoja sesijos metu sukurtus kintamuosius. Dažniausiai tai vartotojo ID, kuris gali būti generuojamas automatiškai ar tiesiog priskiriamas vartotojo vardas.	Techninė

4.2. Saugumo priemonės

Lentelė 9. Saugumo priemonių lentelė.

ID	Aprašymas	
Autentifikacija		
1	Visi puslapiai turi turėti įvedimo ir išvedimo laukų filtravimą. Būtų negalima įvesti arba apsaugota nuo simbolių: ?<>‘=()”.	9
2	Vietoj paprastų užklausų įvedimo laukams, naudoti patalpintas procedūras (angl. stored procedures).	9
3	Apriboti teises užklausoms ar patalpintoms procedūroms (kad prisijungimo formoje nebūtų galima ištrinti lentelės ar duomenų).	9
4	Nepavykus prisijungti, neturėtų būti gražinama žinutė, kuri nurodytų kas buvo netiksliai įvesta – vartotojo vardas ar slaptažodis, nes įsilaužėliai taip spėliodami, vėliau gali panaudoti automatinio įsilaužimo testus.	9
5	Testines paskyras vertėtų ištrinti.	2
6	Reikia ištrinti paskyras, kurios gražina sistemoje klaidas ar kitaip trikdo darbą.	9
7	Suteikti prieigos teises prie duomenų bazės tik	2

	patikimiems žmonės.	
8	Nenaudotinų portų blokavimas.	2
9	Panaikinti „HTTP Trace“ funkciją (ši funkcija gražina atgal vartotojui įvedimo duomenis) serveryje, kuri įgalina pasinaudoti nuotolinių skriptų vykdymu. Pasinaudojant „HTTP Trace“ galima išgauti tinklapio duomenis ar sausainukus (angl. cookies) http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf	10
10	Panaikinti nereikalingas paskyras IIS (angl. Internet Information Services), kad įsilaužėlis negalėtų pasinaudoti sprinterių ar kitomis paskyromis.	2
11	Klaidų pranešimų apsaugojimas (nerodymas), kai vykdant SQL užklausas tinklapyje parodoma, kokia klaida ištiko.	9
12	Blokuoti papildomus servisus, kuriais įsilaužėlis gali pasinaudoti.	2, 1
13	Šifruoti svarbius duomenis duomenų bazėje.	12, 5, 3, 2, 1
14	Reikia ištrinti paskyras, kurios gražina sistemoje klaidas ar kitaip trikdo darbą.	2, 10, 12, 13
15	Suteikti prieigos teises prie duomenų bazės tik patikimiems žmonės.	6, 7
Tinklo Saugumas		
16	Visada laiku atnaujinti serverio programinę įrangą.	2
17	Serverio programinę įrangą ir OS, laikyti skirtinguose fiziniuose ar loginiuose diskuose.	2
18	Panaikinti visus įdiegtus, bet nenaudojamus servisus.	10
19	Pašalinti ar panaikinti numatytąsias paskyras.	2
20	Apriboti vartotojų nuotolinio prisijungimo teises.	2
21	Apriboti vietas (IP adresus) iš kurių būtų galima jungtis.	2
22	Naudoti saugius protokolus jungimuisi prie FTP – SSH, HTTPS, atsisakyti naudoti – FTP, NFS, HTTP.	13
23	Jei duomenys ypatingai svarbus, įdiegti papildomus saugumo mechanizmus nuotoliniu jungimuisi.	2
24	Įdiegti TCP ir UDP portų sekimo įrangą.	4
25	Įdiegti brukalo tvarkymo programą.	8

Autentifikacija

Tikslas – užtikrinti tinkamą autentifikacijos procesą ir su gera slaptažodžių saugumo politika.

Netinkamai tvarkomos įvedimo reikšmės, gali būti įsilaužimo priežastis. Išnaudojant šį pažeidžiamumą, galima nukopijuoti sesijos ID adresą ir nusiųsti kitam žmogui.

Pažeidžiamumai:

- Duomenų bazės, vykdant SQL injekcijas. SQL užklausos dažniausiai vykdomos per vartotojo ir slaptažodžio paskyros prisijungimo duomenis. Kai kuriais atvejais įsilaužiama į tinklapį, kartais per įvedimo laukus ištrinamos duomenų bazės lentelės.
- Tinklapis, vykdant nutolusių skriptų atakas (angl. Cross-site scripting). Pažeidėjas gali į neapsaugotus tinklapius įdėti java skriptus ar interneto adresus, kuriuos paspaudęs klientas nukeliaus į kenksmingą tinklapį, nors jis ir atrodys taip kaip originalus tinklapis.
- Tinklapis, kuomet bet koks URL adreso įvedimas į formą, gali būti pavojingas.
- Tinklapis, vykdant automatinio įsilaužimo testą (angl. brute force).

Tinklo saugumas

Saugumo priemonės:

- Tinklapiui naudoti HTTPS protokolą.
- Naudoti antivirusinę programą.
- Naudoti Ugniasienę.
- Naudoti SSL (angl. Secure Socket Layer) sertifikatą.

Serverio saugumo priemonės:

Organizacijos saugumas:

Pažeidžiamumai:

- Slaptažodžių rašymas ant lapelių ir jų pakabinimas ofise.

DDOS atakos:

Saugumo priemonės:

- Viena pigesnių prevencinių priemonių nuo DDoS atakų yra „kliento dėlionė“, kuomet serveris apskaičiuodamas per nelyk didelį užklausų kiekį, klientams (klientai siunčiantys užklausas) pradeda pateikinėti klientų dėliones. Klientų dėlionės tai

įvairūs uždaviniai klientui, kuriuos jis turi išspręsti prieš siunčiant paketus (informacija) gavėjui (serveriui). Nors klientas užtrunka mažą dalį spręsdamas uždavinį, bet daugelis klientų užtrunka pakankamą laiką, kad serveris paruoštų resursus, taip sumažinama DDoS atakos pasisekimo galimybė.

- Kuriami įvairūs metodai užkirsti DDoS atakas. Metodas naudojantis siunčiamą slaptažodžių rinkinį aprašytas [8].

ORGANIZACIJA

Organizacijoje, kur vyrauja įvairūs IT sprendimai dažnai kartojasi tam tikri elementai: kompiuteriai, serveriai, maršrutizatoriai ir kt. Todėl patiems dažniausiems reikia sudaryti tam tikrą saugumo specifikaciją. Duomenų bazių serveriai, saugojantys svarbią informaciją, privalo būti saugumo užtikrinimo proceso priekyje, nes didžiausias duomenų nutekėjimas (http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf) yra duomenų pasiekiamų internetu (angl. online data).

Duomenų serveriai turi būti apsaugoti nuo:

- Duomenų vagysčių;
- Duomenų nutekėjimo;
- Neautorizuotų pakeitimų.

Serveriams gali būti taikomi įvairūs standartai – COBIT (angl. Control Objectives for Information and related Technology), ISO/IEC 27002 ir kiti, kurie apibrėžia serverių valdymo ribas.

Prie serverių gali būti jungiamasi trimis būdais:

- Tiesiogiai (jungiamasi iš karto į serverį);
- Lokaliai (organizacijos viduje);
- Globaliai (internetu).

Norint užtikrinti serverių saugumą reikia:

- Apsaugoti nuo SQL injekcijų;
- Kontroliuoti autorizuotus vartotojus;
- Užtikrinti keitimų kontrolę;

- Įvertinti realaus laiko pavojus.

Serverių specifikacijų vertinimai:

- Stebėjimas esamų versijų ir atnaujinimų;
- Pagal nutylėjimus paliktų paskyrų, slaptažodžių keitimas;
- Teisių mažinimas;
- Teises suteikinėti ne vartotojams, o vartotojų grupėms;
- Pagal nutylėjimus paliktų portų keitimas;
- Veiksmų atsekamumas, pagal vartotoją;
- Jungčių stebėjimas;
- Įtartinų šablonų kūrimas;
- DB keitimų stebėjimas;
- Kontroliavimas programų, kurios gali jungtis su duomenų bazę;
- Vartotojų, turinčių daug teisių, patikra;
- Procesų stebėjimas;
- Susijungimų su DB šifravimas;
- Ypatingai svarbių duomenų apsauga;
- Failų, laikomų serveryje, teisių peržiūra;
- Operacinės sistemos konfigūracija (prisijungimo saugumo užtikrinimas).

4.3 Organizacijos pažeidžiamumų identifikavimas

Organizacijos aplinkoje be jau aprašytų techninės grupės pažeidimų įvyksta kiti pažeidimai susiję su organizacijos saugumo politika. Saugumo politika būna fizinė ir techninė. Techninė saugumo politika gali būti tinkama išoriniams įsilaužėliams ir vidiniams (darbuotojams). Tuo tarpu fizinė saugumo politika dažniausiai būna susijusi tik su darbuotojais ar asmenimis, kurie gali pasiekti organizacijos resursus iš vidaus. Fizinė saugumo politika nurodo fizinių organizacijos elementų saugą, tuo tarpu techninė saugumo politika būna susijusi su informacinių sistemų, paskyrų ir kt. elementais.

Vis labiau Įsivyraujant informacinėms technologijoms, fizinė sauga tampa mažiau svarbi nei techninė. Dokumentai, pinigai ir visi kiti svarbūs elementai organizacijai dabar yra įgavę skaitmeninę formą. Jei anksčiau informacijos naudojimui ir saugojimui darbuotojai naudodavo

paprastus lapus, užrašines ar kitas fizines laikmenas, tai dabar esant greitam internetui ir neišsenkamoms saugojimo laikmenoms galima informaciją pasiekti iš bet kur ir bet kada. Popierines formas daugelyje organizacijų pakeitė skaitmeninės.

10 lentelėje pateiktas sąrašas fizinių saugumo priemonių. Sąrašas buvo sudarytas atsižvelgiant į
e-parduotuvių tipą, todėl jame figūruoja saugumo priemonės naudojamos pastatų viduje (saugyklose, sandėliuose, darbo patalpose).

10 lentelė. Fizinės saugumo priemonės

ID	**Priemonė**	**Aprašymas**	
1	Garsinis signalas (aliarmas)	Garso signalas, kuris įsijungia pagal kitų daviklių gautus duomenis.	
2	Biometrinis skaitymo prietaisas	Gali atpažinti asmens fiziologijos ar elgsenos pakitimus. Biometrinis prietaisas gali skaityti pirštų antspaudus, atpažinti veidą, DNR, rankos forma, rašymo greičio ar balso atpažinimo.	
3	Užtvaros (stulpeliai)	Užtvaros ribojančios pravažumą arba praeinamumą.	
4	Signalizacija	Apsaugos priemonė, kuri pagal turimus daviklius (vibracijos, magnetinio lauko pakitimų, garso pakitimų, mikrobangų pakitimų ir kt.) gali paleisti garsinį signalą, pranešti apsaugos tarnybai ar kitaip informuoti.	
5	Stebėjimo kameros	Stebėjimo kameros jungiamos į stebėjimo tinklą, kartu su peržiūros monitoriais ir įrašymo įrenginiais.	

6	ID kortelė	Identifikavimo kortelė, kuri pagal įdiegtą nuskaitymo technologiją (magnetinė, brūkšninio kodo, ir kt.), leidžia identifikuoti asmenį.	
7	Durų saugumo priemonės	Durų grandinėlės, metaliniai sustiprinimai staktai, vidinės spynos, žiūrėjimo akutė, ilgesni vyriai, neleidžianti lengvai nuimti durų, slankiojančios durys.	
8	Elektrinė spyna	Spyna, kuriai atrakinti gali būti panaudoti kodo, slaptažodžio įvedimas, kortelė, biometrinių duomenų ar RFID skaitytuvas.	
9	Elektrinė užtvara	Užtvara (tvora) su leidžiama elektros srove ja.	
10	Kriptografinis raktas	Nedidelis prietaisas, kuriam išsaugomas šifruotas kodas, o paveikus raktą spyna kodas yra patikrinamas.	
11	Magnetinės juostelės kortelė	Kortelė, kurios nuskaitymas vyksta per magnetinę juostelę.	
12	Praėjimo vartai	Vartai (sukamieji), kurie gali riboti greitą įsibrovimą.	
13	Identifikavimas pagal dokumentą (nuotrauką)	Metodas, kuomet asmuo identifikuojamas, pagal jo asmens dokumentą ir nuotrauką jame.	
14	Artumo kortelė	Tai bekontaktė kortelė, kuria galima nuskaityti per nedidelį atstumą.	
15	Seifas	Tvirta,, nedeganti iš metalo padaryta dėžė ar spinta	

		vertingiems daiktams laikyti.	
16	Judėjimo sensoriai	Davikliai kurie reaguoja į judesį.	
17	Dūmų sensoriai	Gaisrą nustatantys sensoriai.	
18	Metalo detektorius	Detektoriai skirti aptikti metalinius daiktus, gali būti rankiniai ar įmontuoti perėjimo vartuose.	

4.4 Organizacijos elementų identifikavimas

Abstrakčiai žiūrint į organizaciją iš karto galima išskirti žmones, kurie yra susiję su ja ir įvairius įrankius skirtus darbui atlikti, vykdyti. Taip pat organizacija yra suvokiama kaip sistema susidedanti iš smulkesnių struktūrinių vienetų.

Žmones galima skaidyti į smulkesnes grupes. Tiesiogiai su organizacija susiję yra darbuotojai, veiklos partneriai ir klientai, todėl šios trys grupės bus pagrindinės. Ir vienas svarbiausių elementų saugumo modeliavime tai piktybinis vartotojas (įsilaužėlis), kuri bando neteisėtais būdais gauti sau naudos.

Visos atakos dažniausiai būna nukreiptos į IT techniką, todėl pirmiausiai reiktų išskirti IT technikos elementus. Dažniausiai laužiamasi į duomenis saugančius IT elementus, todėl reikia juos išskirti. Tai būtų:

- Duomenų bazių serveris,
- Serveris,
- Tinklo įrenginys.

Saugumo modeliavime taip pat reikia pridėti pažeidžiamumo ir saugumo priemonės elementus. Pažeidžiamumo elementas nurodys organizacijos elementą, kuriam kyla grėsmė, o saugumo priemonės elementas parodys kaip tą grėsmę įveikti.

5. Metodo koncepcinis modelis

Remiantis atlikta analize, buvo išskirti svarbiausi elementai, kurie buvo panaudoti sudarant saugumo metamodelį (20 pav.). Modelyje yra du vartotojų tipai: vartotojas ir piktybinis vartotojas. Piktybinis vartotojas žymi bet kurį asmenį, kuris bando pakenkti organizacijos turtui – resursui. Vartotojas turi tam tikras jam nustatytas teises, taip pat jis gali būti apibūdinamas vartotojo tipu.

Resursu gali būti bet koks organizacijai svarbus elementas – IT ūkio vienetas, organizacijos struktūros dalis ar kt. Kiekvienas vartotojas gali būti įsilaužėlis (pikto siekiantis vartotojas), kuris visuomet turi tikslą, taip pat gali būti apibūdinamas vieta iš kurios jis laužiasi.

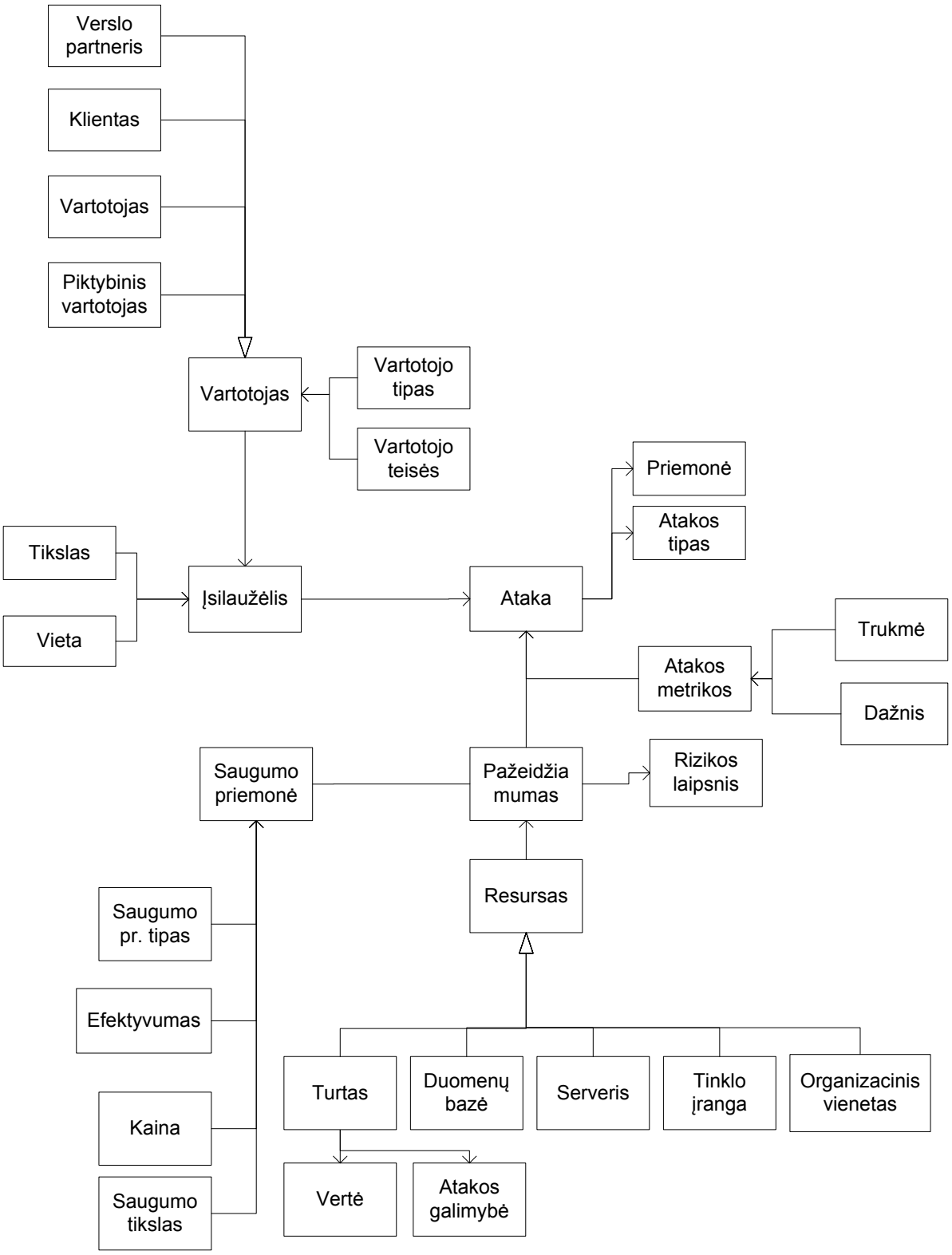
Metamodelio tikslas yra aiškiai pavaizduoti įvairius atakų tipus. Todėl ataka yra aprašoma labai tiksliai – identifikacinis numeris, pavadinimas, tipas. Galima nurodyti atakos trukmę ir dažnį. Atakos priemonė yra elementas, kuris padeda įvykdyti ataką (yra pagrindinis įsilaužimo įrankis): personalinis kompiuteris, skriptas, fizinė ataka, viešai platinama programinė įranga. Atakos tipas nurodo, kuo paremta ataka ir kokiu būdu ji sutrikdo resurso darbą.

Atakos tipas:

- Skenavimas;
- Srauto perpildymas;
- Įsilaužimo skriptai;
- Informacijos ištrynimas;
- Informacijos nuskaitymas;
- Apėjimas;
- Identifikavimo išnaudojimas.

Resursas gali būti pažeistas atakos metu, todėl turi pažeidžiamumo elementą, nurodantį, koks tai pažeidžiamumas. Rizikos laipsnis nurodo tikimybę, kad bus išnaudojamas būtent tas resurso pažeidžiamumas.

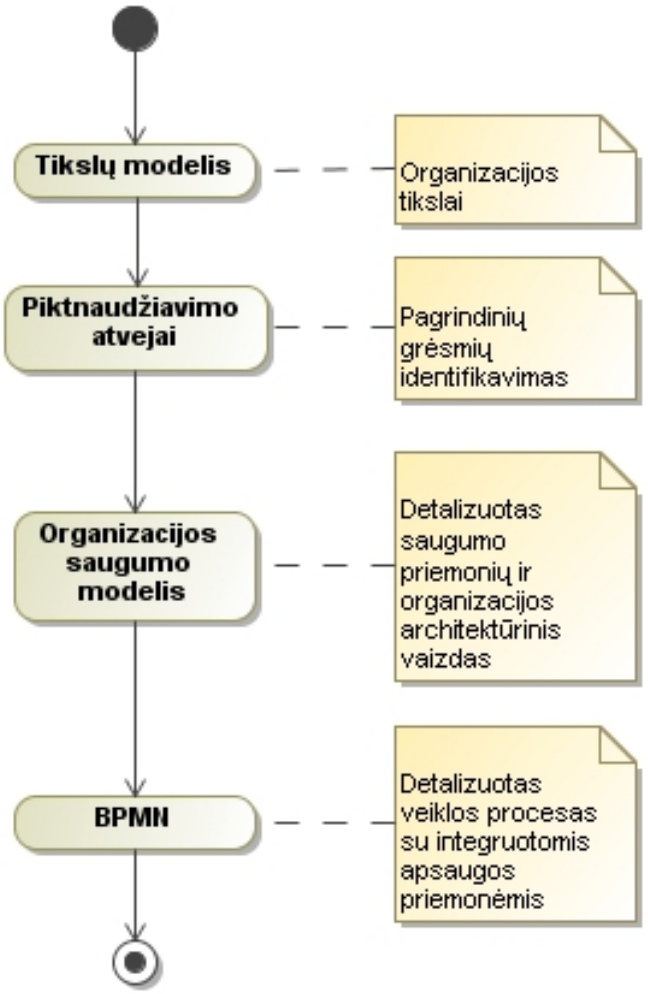
Saugumo priemonė yra skirta užtikrinti resurso saugumą. Saugumo priemonė gali būti skirtingų tipų ir turi metrikas: efektyvumas ir kaina. Visuomet saugumo priemonė yra apibūdinama ir jos siekiamu tikslu – saugumo priemonės tikslas.



20 pav. Saugumo metodo koncepcinis modelis.

Sukurto saugumo metodo procesas pavaizduotas 20 pav., modeliuojant organizacijos saugumo struktūrą. Šiame paveikslėlyje parodyta, kokios svarbiausios dalys paimamos iš kiekvieno elemento. Piktnaudžiavimo atvejai suteikia pagrindinius grėsmių sąrašus, saugumo priemonių

modeliavimas tai struktūrizuoja, o BPMN diagramoje matomas konkretus veiklos procesas ir jam taikomos saugumo priemonės.



21 pav. Grėsmės yra įvairios, detalus jų sąrašas

Saugumo metodą sudaro trys pagrindiniai žingsniai:

1. organizacijos tikslų sudarymas (strateginio lygio uždavinys),
2. piktnaudžiavimo atvejų ir organizacinio modelio sudarymas (taktinio lygio uždaviniai),
3. veiklos procesų sudarymas (operacinio lygio BPMN diagramos).

5.1. Tikslų sudarymo procesas

Šio proceso metu yra nustatomi organizacijos tikslai. Tikslai gali būti sudaryti iš smulkesnių tikslų (potikslių).

Tikslų sudarymo procesas susideda iš: (1) Tikslų indentifikavimo, (2) Potikslių indentifikavimo, (3) Saugumo tikslų indentifikavimo, (4) Vizijos aprašymo. Tikslų sudarymo procesas pateiktas 20 pav.

22 pav. Grėsmės yra įvairios, detalus jų sąrašas

Tikslų indentifikavimas – tikslų nustatymas, kurie apibrėžia organizacijos siekius.

Potikslių indentifikavimas – kartais tikslai gali būti sudaryti iš smulkesnių tikslų, tokie tikslai vadinami potiksliais.

Saugumo tikslų indentifikavimas – vykdant metodą, svarbu išskirti saugumo tikslus, kad vėliau juos būtų galima detaliau apibrėžti piktnaudžiavimo atvejų diagramoje ir organizacinio saugumo modelyje.

Vizijos parašymas – vizija tai organizacijos požiūris į vykdomą veiklą ir jos veiklos misija.

5.2. Organizacinio modelio sudarymas

Organizacinio modelio sudarymo tikslas yra organizacijos pažeidžiamumų indentifikavimas pagal jos struktūrą ir IS funkcijas.

Organizacinio modelio sudarymas susideda iš: (1) Panaudojimo atvejų sudarymo, (2) Piktnaudžiavimo atvejų sudarymo, (3) Organizacijos saugumo modelio sudarymo.

Panaudojimo atvejų sudarymas – jei organizacija turi IS, sudaroma jos panaudojimo atvejų diagrama.

Piktnaudžiavimo atvejų sudarymas – panaudojimo atvejų diagramoje kuriami piktnaudžiavimo atvejai, atsižvelgiant į saugumo tikslus MODAF modelyje ir sudaromi piktnaudžiavimo atvejų aprašai.

Organizacijos saugumo modelio sudarymas – sudaromas organizacijos saugumo modelis. Šis modelis turi aktorius, organizacijos turtų, saugumo priemonių ir pažeidžiamumų elementus. Iš šių elementu sudaroma organizacinio modelio saugumo diagrama, modeliuojant aktorius susietais su turtais, saugumo priemones su pažeidžiamumais, o pažeidžiamumus su turtais. Modeliuojami pažeidžiamumai ęsantys piktnaudžiavimo atvejų diagramoje.

5.3. Veiklos procesų sudarymas

Veiklos procesų modelio sudarymo tikslas yra pavaizduoti detalias saugumo priemones, taikomas organizacijos veiklos procese.

Veiklos procesų sudarymas susideda iš: (1) Veiklos proceso indentifikavimo, (2) Saugumo priemonės taikymas.

Veiklos proceso indentifikavimas – nustatoma veikla, kurios metu kyla pažeidžiamumai organizacijos turtams (pvz. prekės įdėjimas į e-parduotuvę, pirkimas ir kt.), tuomet ši veikla yra sumodeliuojama BPMN kalba.

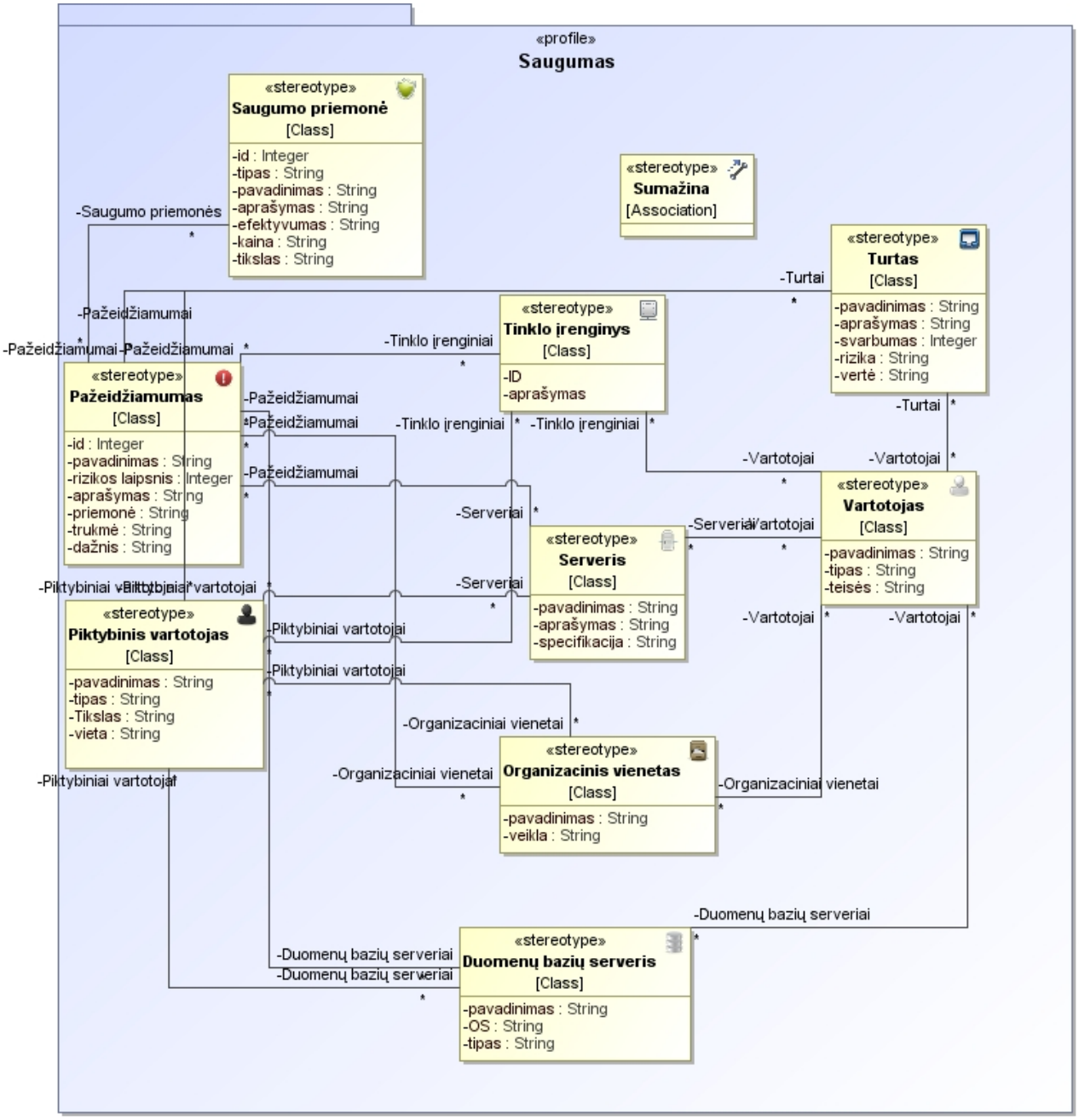
Saugumo priemonės taikymas – sumodeliuotoje BPMN diagramoje, parenkame konkrečią taikomą saugumo priemonę ir ja įterpiame diagramoje, tuo metu kai ji suveikia. Saugumo priemonė turi atitikti organizaciniame modelyje modeliuotas saugumo priemones.

Atlikus analizę sukonkretinome dažniausiai kylančias grėsmes (lentelė 11). Kurios vėliau bus priskirtos piktnaudžiavimo elemento tipui.

Lentelė 11. Grėsmės pavadinamas.

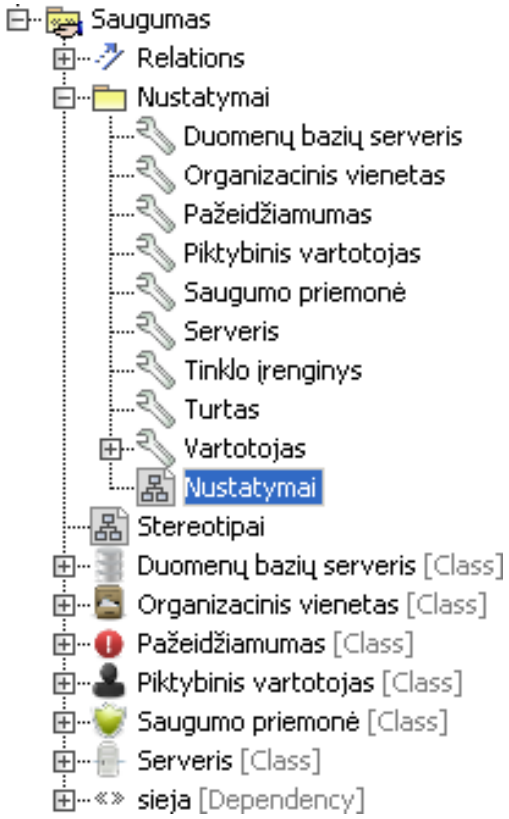
Grėsmės pavadinamas (angl.)
Neteisėta prieiga per numatytuosius ar bendrai prieinamus duomenis (angl. unauthorized access)
SQL Injekcija
Neteisingo dėl apribojimų ar dėl blogos prieigos kontrolės kylanti grėsmė (angl. poor Access control lists - ACLs)
Neteisėta prieiga per pavogtus duomenis
Autentifikacijos apėjimas (angl. bypass)
Automatinis įsilaužimo testas (angl. Brute-Force)
Pernelyg dideli įgaliojimai
Sesijos kintamųjų išnaudojimas
Resursų perpildymas (angl. BufferOverflow)
Nutolusių skriptų pažeidžiamumas (angl. Cross-SiteScripting)

Saugumo koncepcinio modelio atvaizdavimas UML parodytas 23 pav. Tai yra pirminis etapas, kuriant MagicDraw profilį. Jame sužymima ryšiai, atributai.



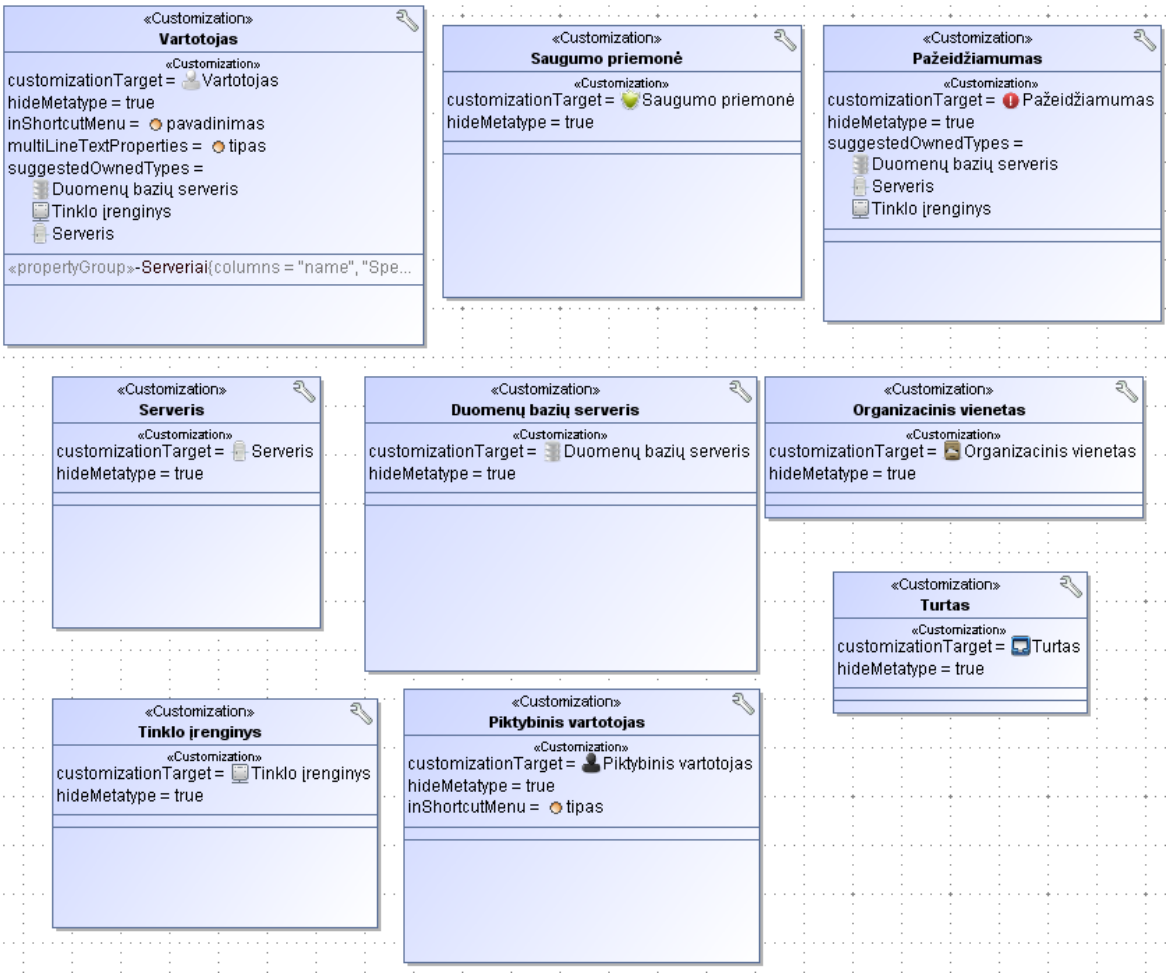
23 pav. Saugumo metodo UML klasių modelis.

Kiekvienas naujas elementas, DSL (angl. Domain Specific Language) kalboje yra aprašomas (specifikuojamas) UML kalba. DSL kalba leidžia susikurti savo individualizuotos diagramas, elementų savybes, semantines taisykles ir kt. Kiekvienas naujas elementas DSL kalboje yra specifikuojamas stereotipų, su jų nustatymais ir ikonomis. Stereotipai yra sujungiami vienas su kitu asociacijos ryšiu (angl. Association link) ir nurodomi ryšiai. Sukurtiems stereotipams sukuriamos savybės (atributai) su nurodytais tipais (23 pav.). Visi sukurti elementai yra saugomi viename kataloge, o kitame kataloge „Nustatymai“ yra patalpinta nustatymų klasės, sukurtos kiekvienam stereotipui.



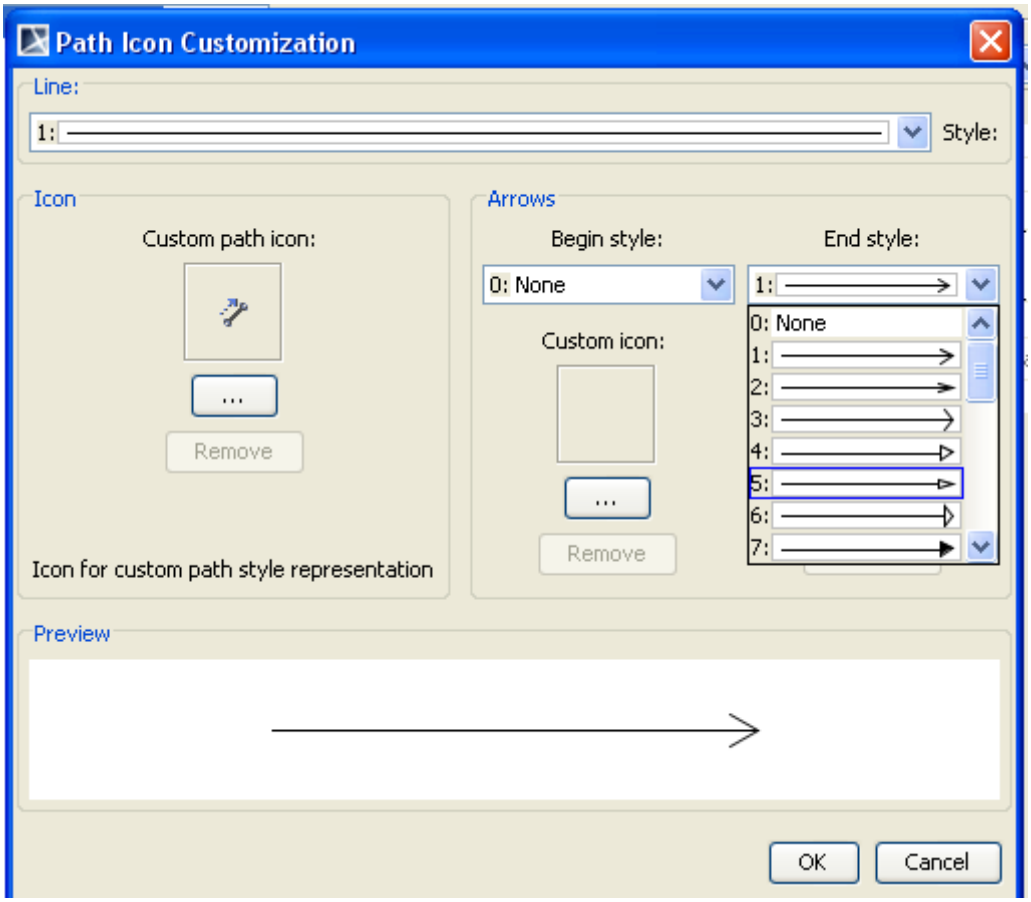
24 pav. Elementų struktūra.

Kuriant MagicDraw profilį svarbus yra profilio stereotipų nustatymo modelis (25 pav.). Jame sužymima tėvinės bei vaikinės klasės (paveldimumas), matomi nustatymo parametrai. DSL nustatymo taisyklės yra talpinamos klasėse su nustatymo (angl. Customization) stereotipu (25 pav.). Elementų saugoma struktūra pavaizduota (24 pav.) paveikslėlyje.



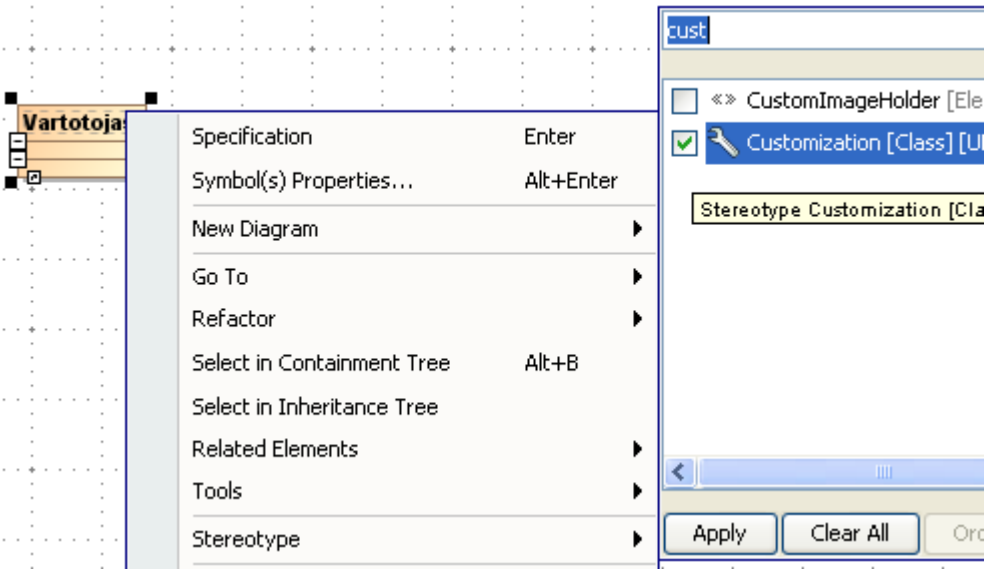
25 pav. Profilio stereotipų nustatymo modelis

Ryšiams kurti yra daug pasirenkamų nustatymų (26 pav.). Galima parinkti linijos stilių – brūkšniuota, taškuota ir kt. Taip pat pradžios ir pabaigos linijos simbolius.



26 pav. Ryšio nustatymai.

Profilio nustatymų kūrimas pradedamas, sukūrus UML klasių modelį (27 pav.) Todėl sukurkime naują nustatymų klasę elementui - vartotojas (27 pav.).



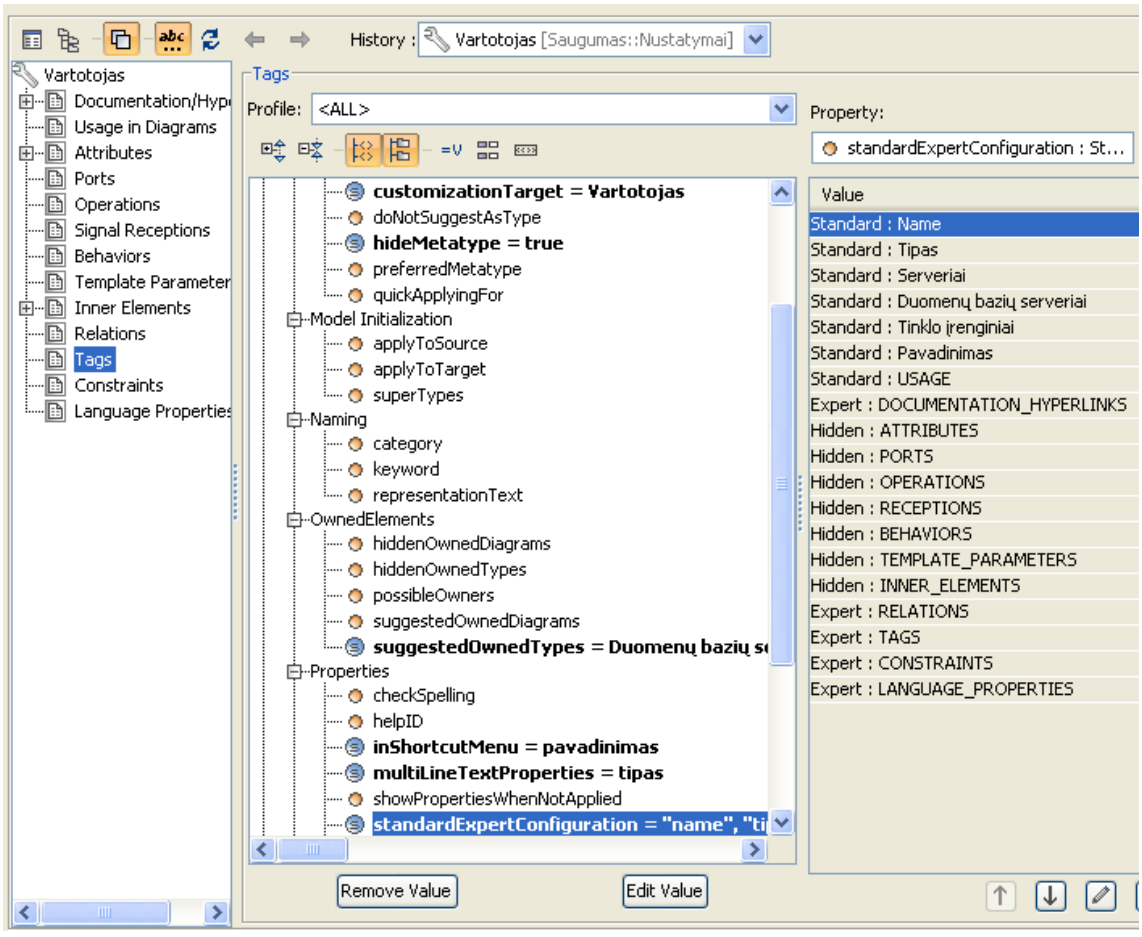
27 pav. Stereotipo „Customization“ priskyrimas.

Pagrindiniai nustatymai elementui vykdomi žymių (angl. Tags) meniu punkte. Skyriuje pagrindinis (angl. General), punkte „customizationTarget“ nurodomas stereotipas, kuriam atliksim

nustatymus (27 pav.), taip pat reikia pažymėti savybę „hideMetatype“ į „true“, jei norime, kad stereotipas veiktų kaip naujas standartinis elementas.

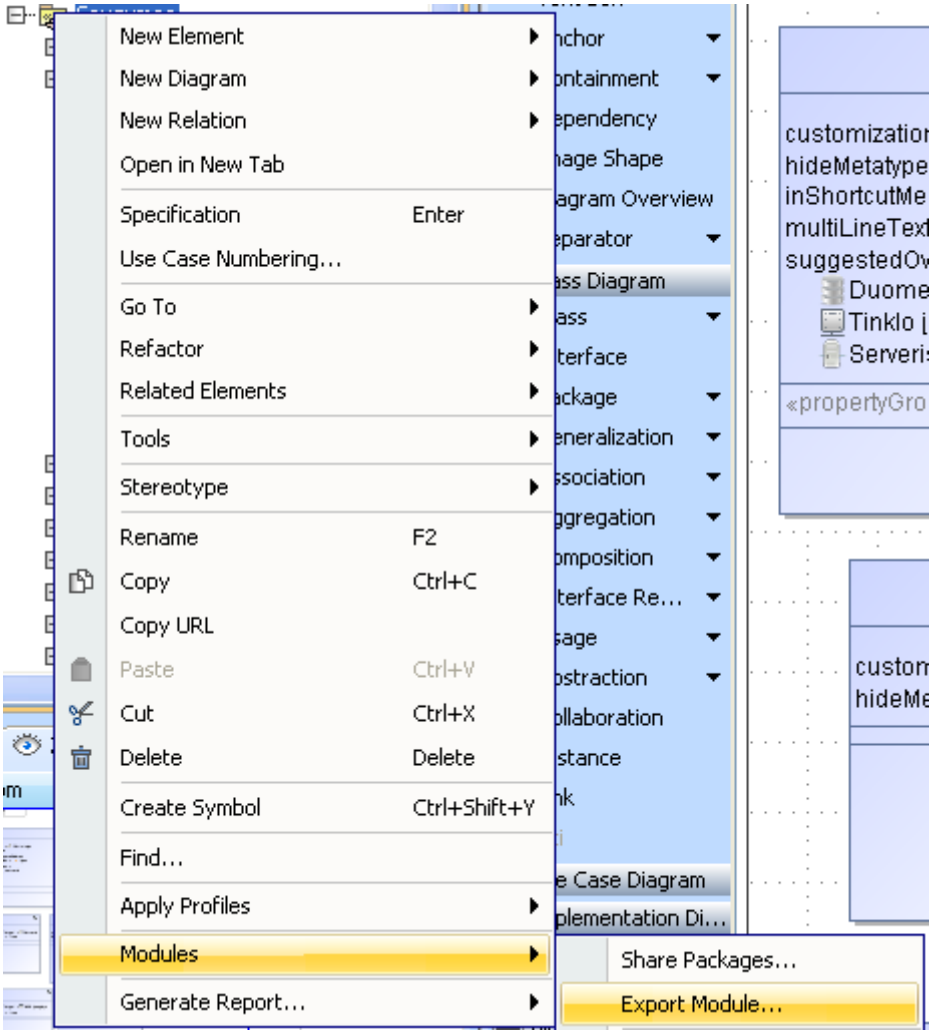
Skyriuje „Connection Rules“ atliekami nustatymai susiję su ryšiais, koks elementas gali būti sujungiamas su kitu ir kokie ryšiai negalimi. „Naming“ srityje atliekami nustatymai susiję su elemento vardu, koks bus vaizduojamas elemento vardas ir kas bus atvaizduojama būsenos juostoje, lentelėse ir pan. „OwnedElements“ skyriuje nurodoma, kada tam tikras elementą, bus galima sukurti tik kito elemento viduje (28 pav.).

„Properties“ skyriuje (28 pav.) nurodomi laukai, kurie bus matomi elemento „Specification“ nustatymų lange.



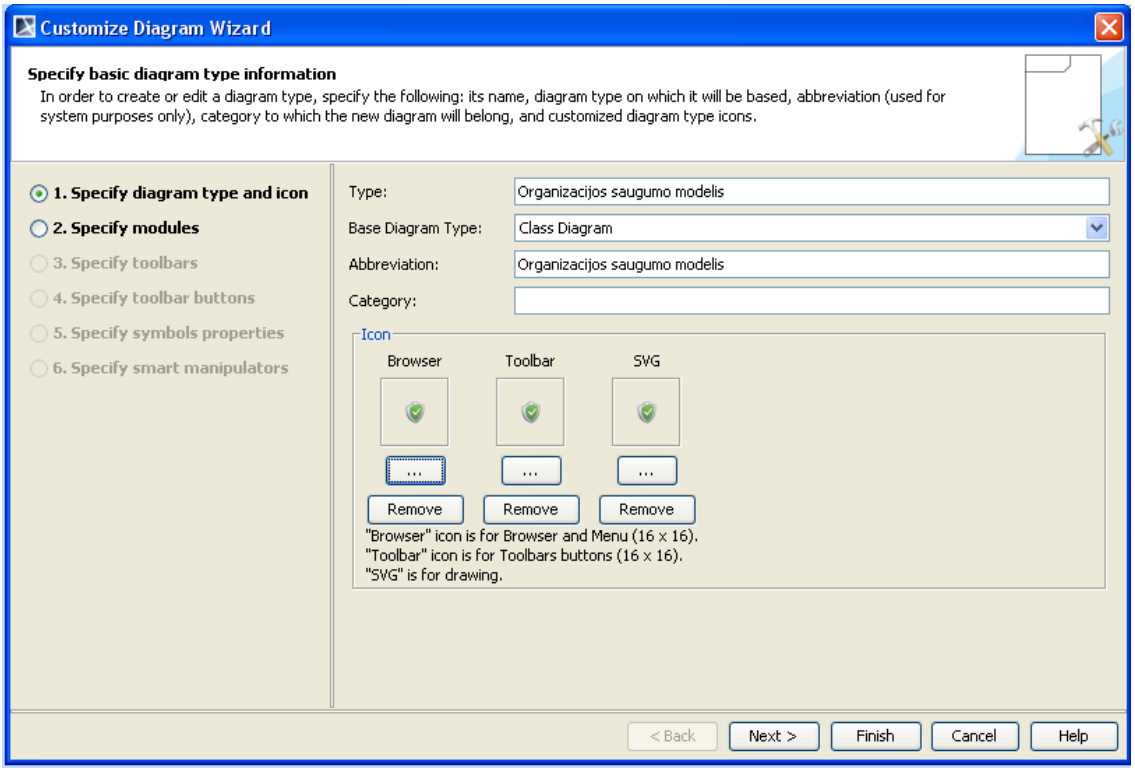
28 pav. Elemento nustatymai pagal žymes.

Tokia pačia tvarka elementams sukuriamos „Customization“ klasės. Sukurtas profilis eksportuojamas (28 pav.)



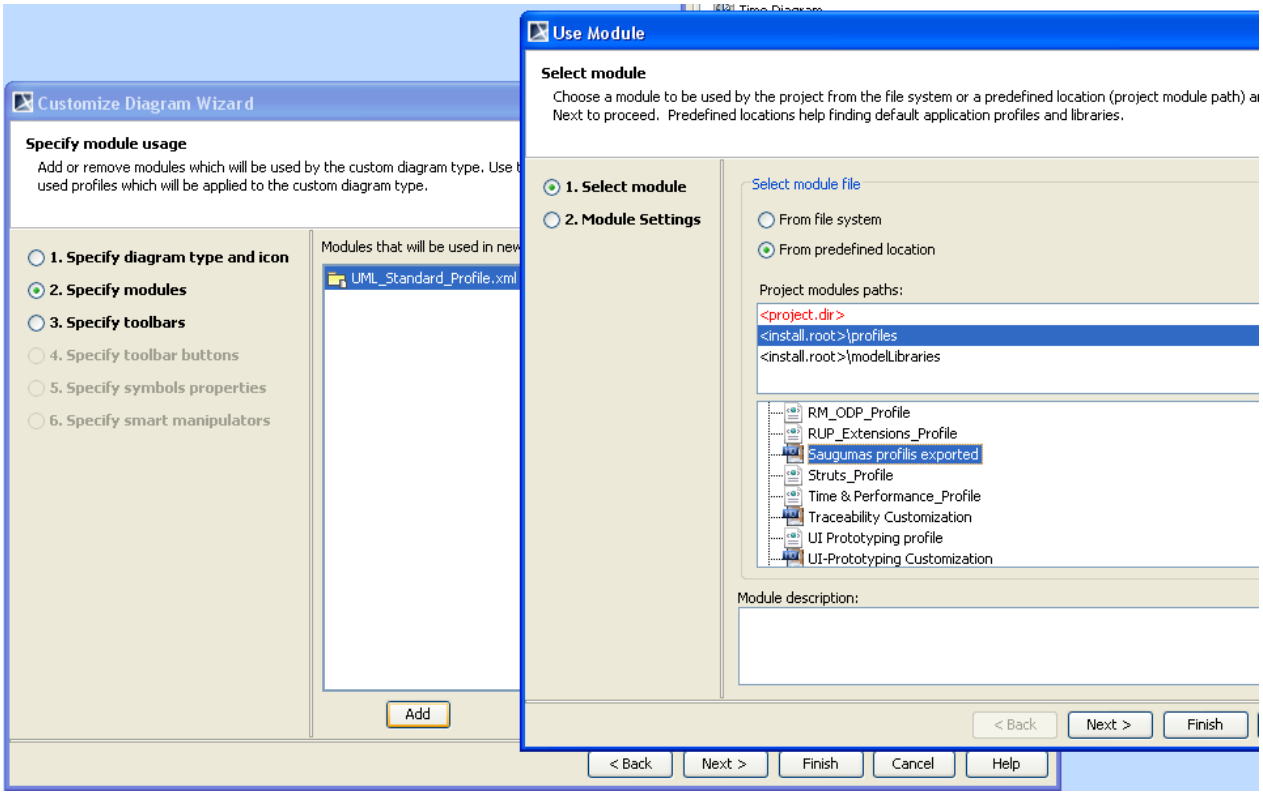
29 pav. Profilio eksportavimas.

Sukūrus profilį, reikia kurti diagramą. Diagrama kuriama per diagramų meniu punktą pasirinkus „Customize“. Atsidaro diagramų administravimo langas, kuriame paspaudus „Create“ mygtuką atsidaro naujos diagramos nustatymo pildymų langas (29 pav).



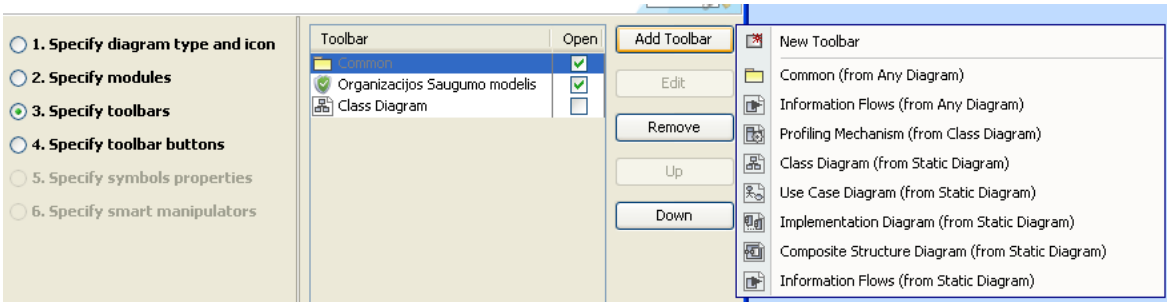
30 pav. Diagramos kūrimo langas.

Diagramos kūrimo vedlyje nustatymai suskirstyti į 6 žingsnius. Pirmame žingsnyje nurodome diagramos tipą, pavadinimą, aprašymą ir diagramos ikonas (30 pav.). Toliau reikia nurodyti profilį, pagal kurį kursime diagramą. Paspaudus „Add“ mygtuką (31 pav.) parenkame sukurtą profilį ir pagal nutylėtuosius nustatymus pridedame profilį. Naujai kuriama diagrama gali būti paremta ne vienu profiliu, bet keliais, iš jų pasirenkant elementus, kurių reikia.



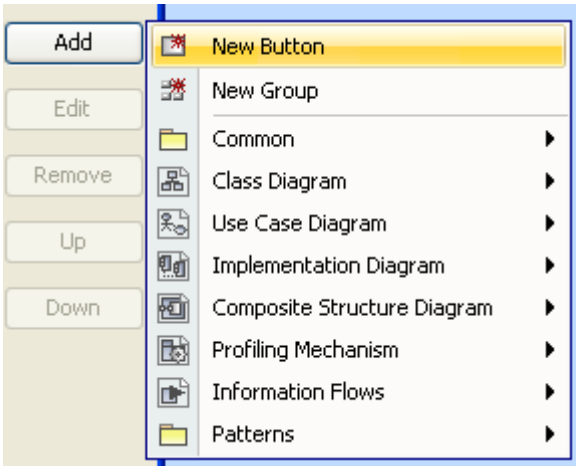
31 pav. Profilio parinkimas.

Kuomet parinktas profilis, 3 žingsnyje reikia specifikuoti įrankių juosta (32 pav.). Prieš tai įrašius diagramos pavadinimą, į įrankių juosta automatiškai yra įtraukiama diagramos pavadinimo įrankių juosta. Galima naudoti daugiau negu vienos diagramos įrankių juosta, jei reikia, galima įsidėti klasių, panaudojimo atvejų ar kitų diagramų įrankių juostas. Norint, kad nebūtų perkrauta elementais pagrindinė įrankių juosta, galima parinkti, kad kai kurios juostos pagal nutylėjimą būtų sutrauktos, o vartotojui prireikus, išskleidžiamos. Taip pat galima nustatyti įrankių juostų išdėstymo eiliškumą.



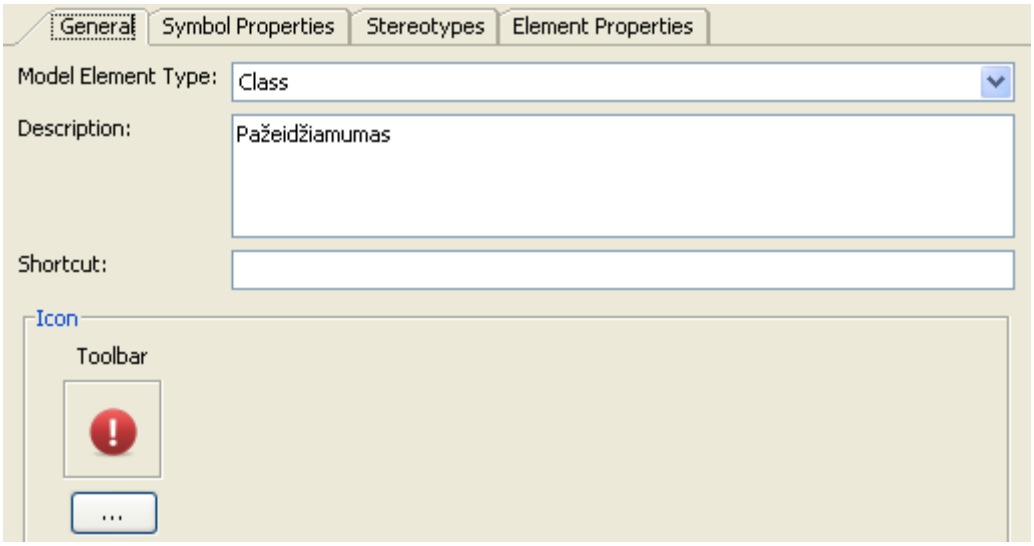
32 pav. Įrankių juostos specifikavimas.

Ketvirtame žingsnyje yra kuriami mygtukai. Naujas mygtukas pridedamas „Add“ mygtuku ir pasirinkus „New Button“ punktą (33 pav.).



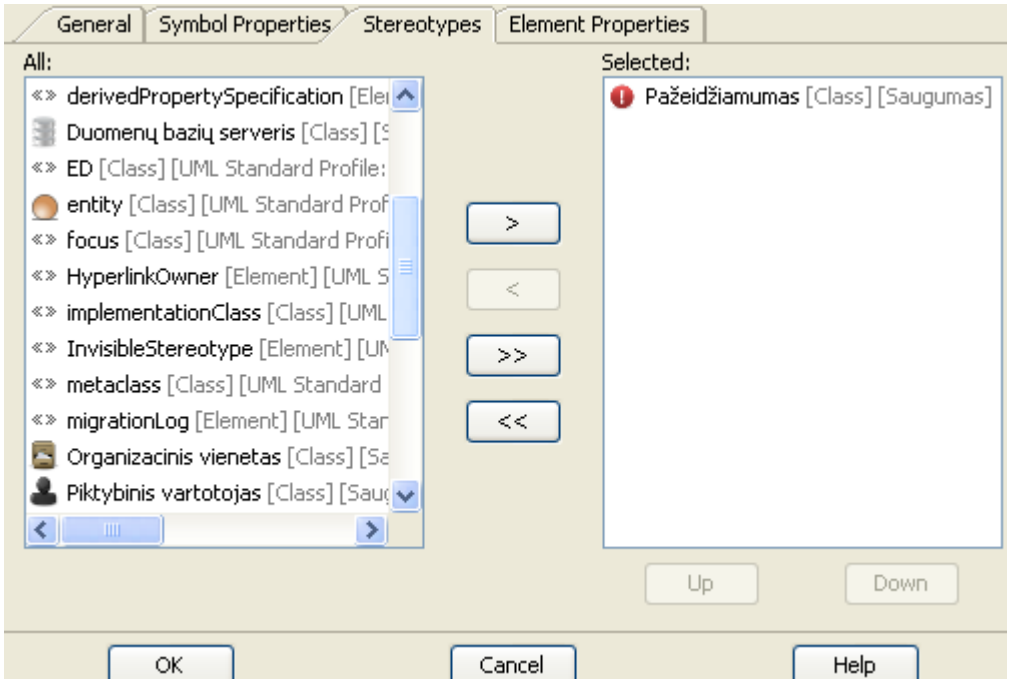
33 pav. Naujo mygtuko pridėjimas.

Atsidaro mygtuko nustatymo langas, kuriame reikia nurodyti elemento tipą, aprašymą ir ikonas (pav 34).



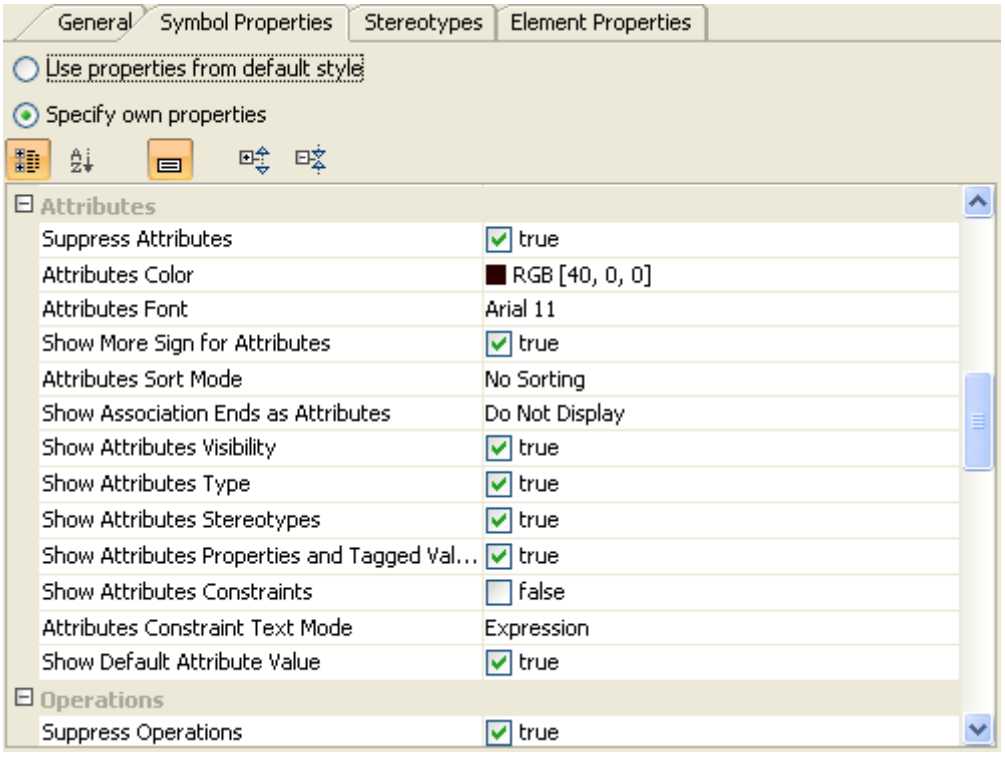
34 pav. Mygtuko „General“ skiltis.

Stereotipų meniu punkte parenkame elementą, kuriam norime sukurti mygtuką. (pav 35).



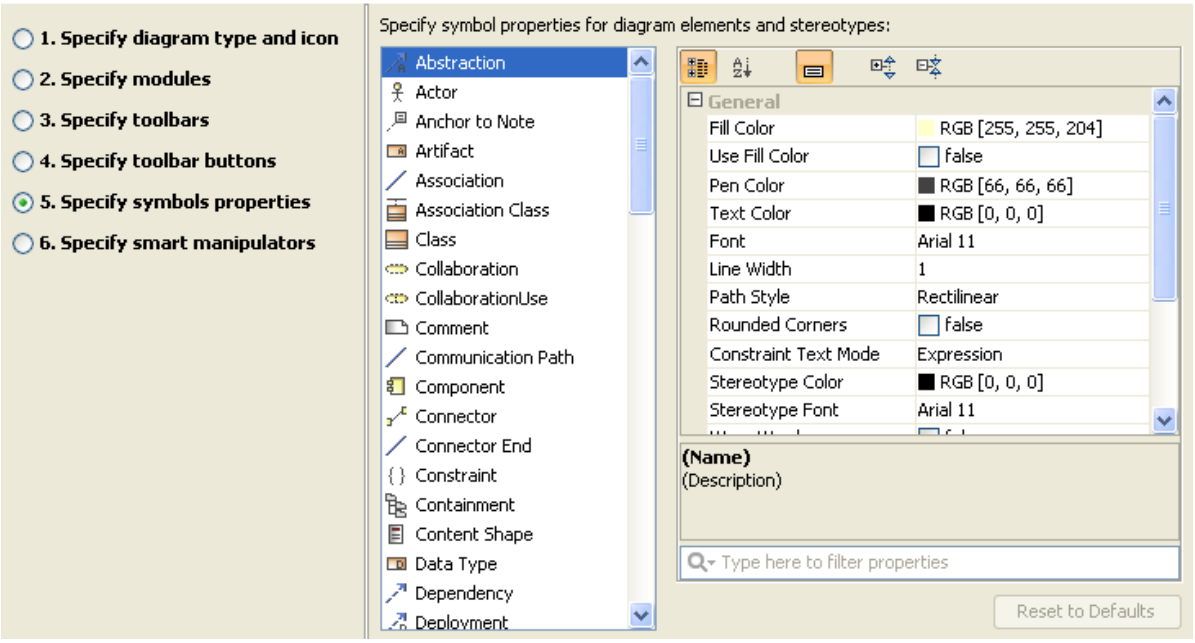
35 pav. Elemento parinkimas.

Meniu punkte „Symbol Properties“ (36 pav.) reikia pažymėti „false“ laukeliuose „attributes“ ir „operations“, kad elementuose paremtuose UML klasės tipu, atributų ir operacijų laukeliai pagal nutylėjimą būtų paslėpti. Tada spaudžiame mygtuką „OK“ ir naujas elementas atsiras įrankių juostoje. Tokiu pačiu būdu pridedame visus elementus.



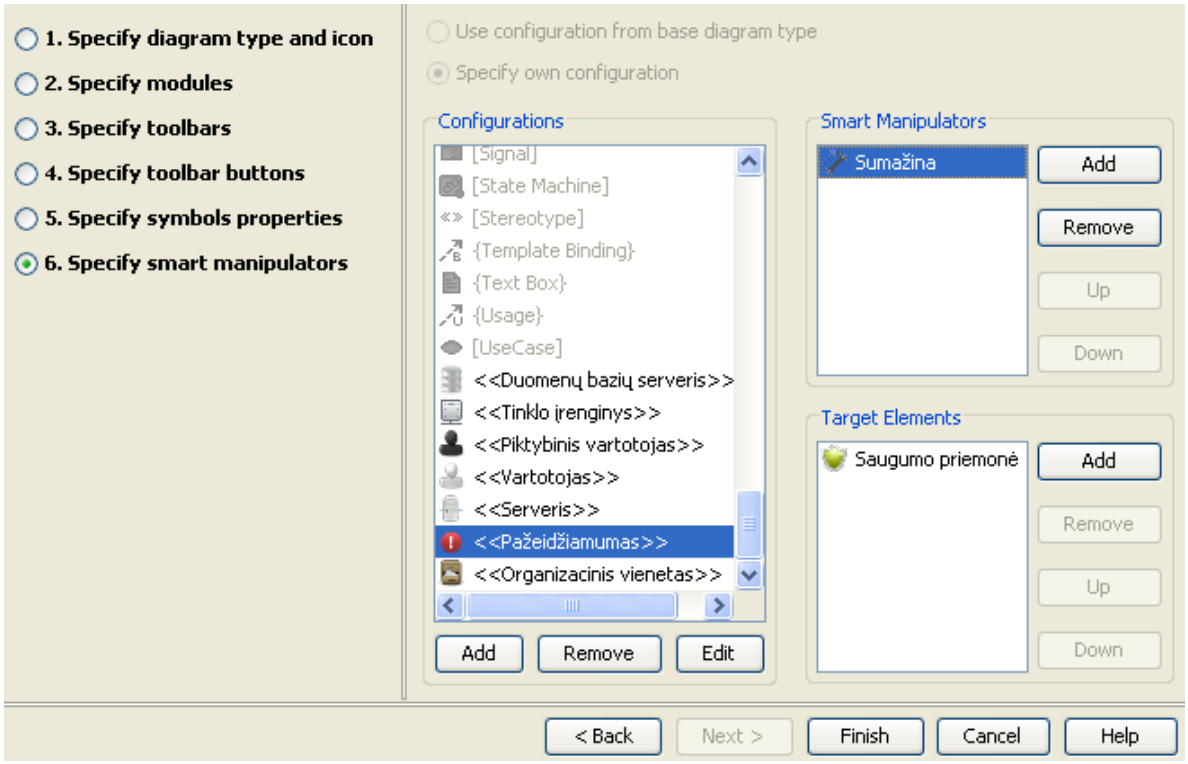
36 pav. Įdedamo elemento nustatymų keitimas.

Penktame žingsnyje galima keisti nustatymus standartiniams UML elementams (37 pav.).



37 pav. Nustatymų keitimas UML elementams.

Norint, kad elementai būtai greičiau paišomi, reikia nurodyti ryšius, kurie bus pasiūlyti, įdėjus elementą į diagramą. Pirmiausia reikia pasirinkti elementą „Configurations“ lange (38 pav.), jei tai naujai sukurtas profilis elementą reikia įsidėti su „Add“ mygtuku. Tuomet „Smart Manipulators“ lange pridedame ryšius, kurie bus pasiūlyti, nubraižius elementą. Pridėjus ryšius, parenkame vieną ryšį ir „Target Elements“ lange įdedame elementą, kurį bus pasiūlyta nubraižyt su šiuo ryšiu. Taip sutvarkome visus elementus. Spaudžiame „Finish“. Ir iš naujo atidarome Magicdraw, norėdami dirbti su naujai sukurta diagrama.

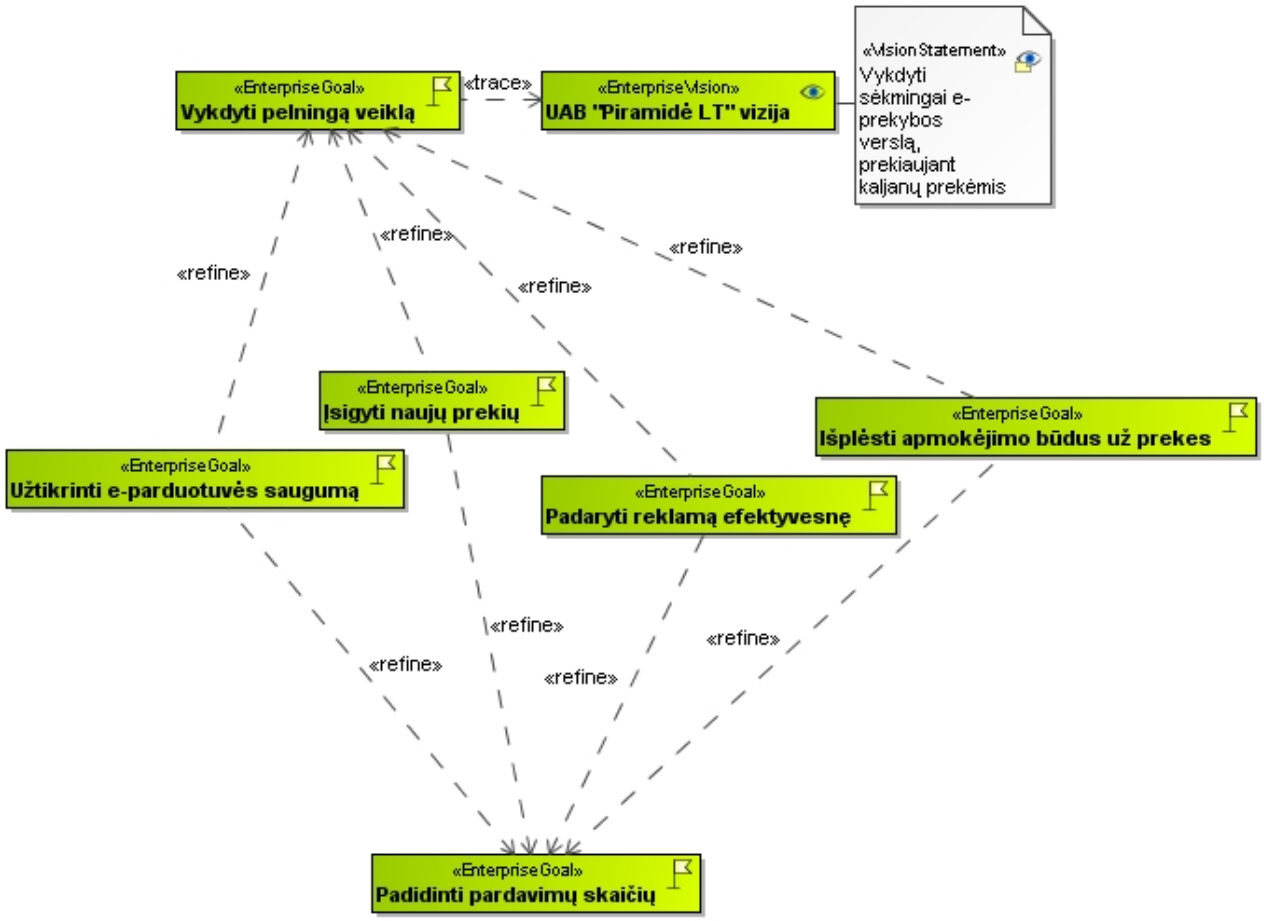


38 pav. „Smart Manipulators“ nustatymai.

6. Realizacija

6.1. Strateginio lygio saugumo tikslų identifikavimas

Strateginime lygyje, organizacijos valdytojai nustato tikslus. Įmonės UAB „Piramidė LT“ nustatyti tikslai pavaizduoti 39 paveikslėlyje. Tikslų modelį sudaro 2 tikslai – pelningos veiklos vykdymas, padidinti pardavimų skaičių. Tikslai turi potikslių, kurie detalizuoja tikslus: užtikrinti e-parduotuvės saugumą, įsigyti naujų prekių, padaryti reklamą efektyvesnę ir išplėsti apmokėjimo būdus už prekes. Tikslai ir potiksliai kartu sudaro viziją – sėkmingas veiklos vykdymas.

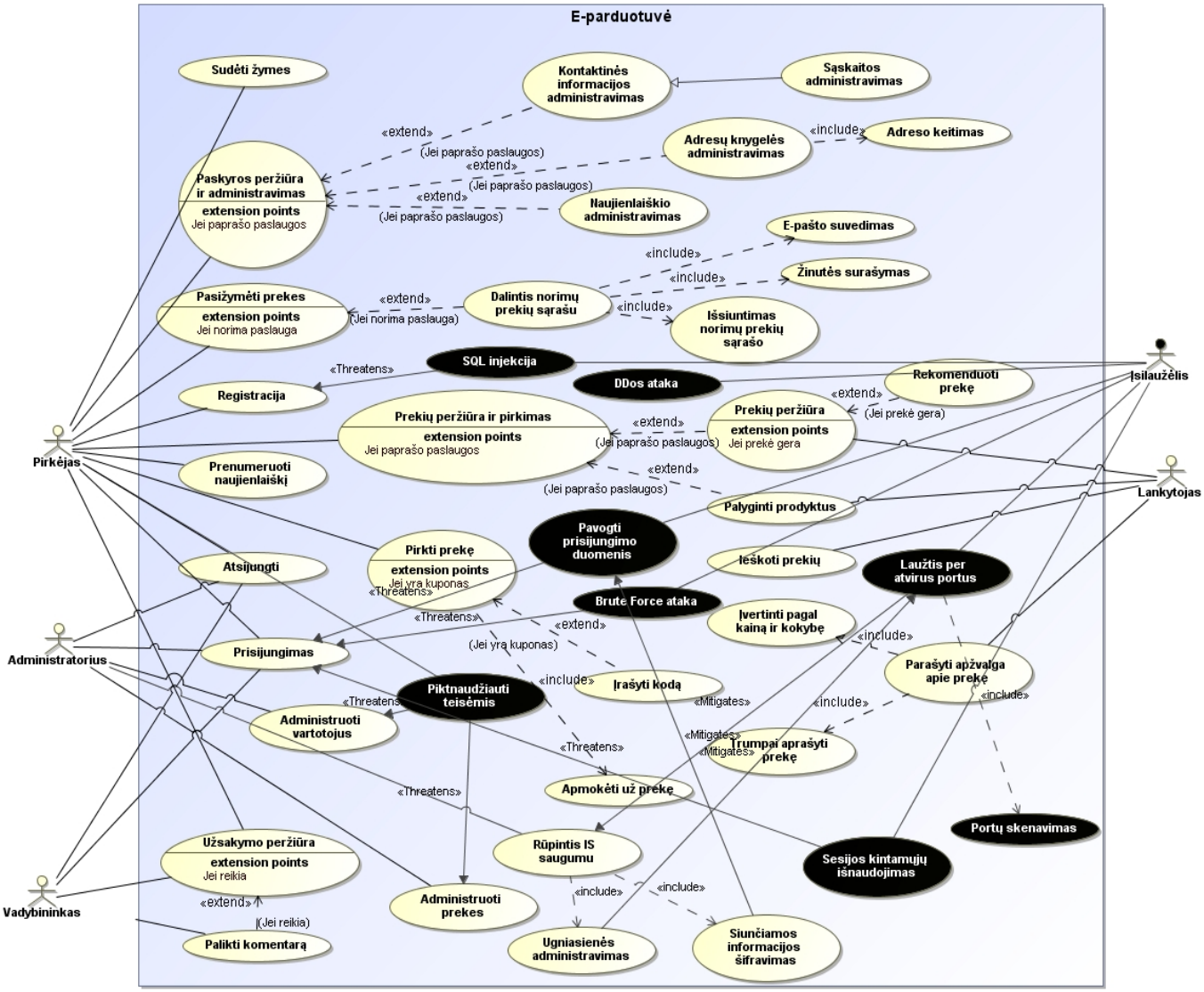


39 pav. MoDAF tikslų modelis

6.2. Taktinio lygio saugumo identifikavimas

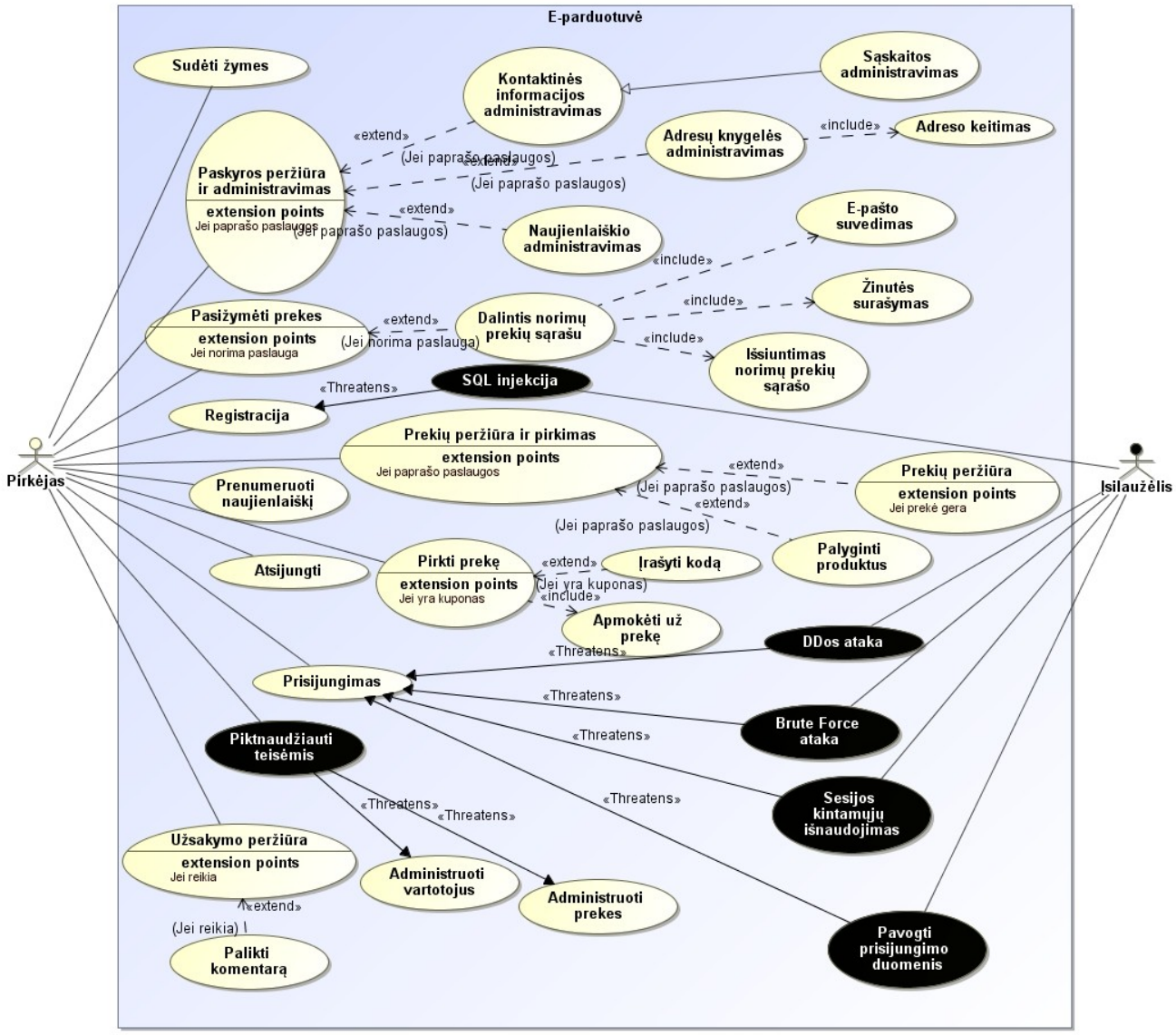
6.2.1. Piktnaudžiavimo atvejų sudarymas

Taktiniame organizacijos lygyje braižomos piktnaudžiavimo atvejų ir organizacijos modelis. Piktnaudžiavimo atvejai braižomi IS (e-parduotuvės) panaudojimo atvejų diagramoje (40 pav.). Piktnaudžiavimo atvejai kuriami atsižvelgiant į panaudojimo atvejo funkcijos pažeidžiamumą – pikt. atvejis „SQL injekcija“ jungiamas su pan. atveju „Registracija“. Taip sujungiami visi pikt. atvejai su panaudojimo atvejais. Piktnaudžiavimo atvejai jungiami ryšiu „Threatens“ (grėsti), kuomet kelia grėsmę panaudojimo atvejo funkcijai. Jei panaudojimo atvejis mažina piktnaudžiavimo atvejo keliamą grėsmę panaudojimo atvejis su pikt. atveju jungiamas ryšiu „Mitigates“ (švelninti, mažinti) – „Ugniasienės administravimas“ mažina grėsmę keliamą pan. atvejo „Laužtis per portus“. Piktnaudžiavimo atvejų spalva yra juoda, o aktoriaus vykdančio pikt. atvejus žmogeliuko galvos simbolis yra taip pat juodas. Panaudojimo ir piktnaudžiavimo atvejai yra aprašyti priedų 1 dalyje. Piktnaudžiavimo atvejų aprašo pavyzdžiai pateikti 5 ir 6 lentelėse.



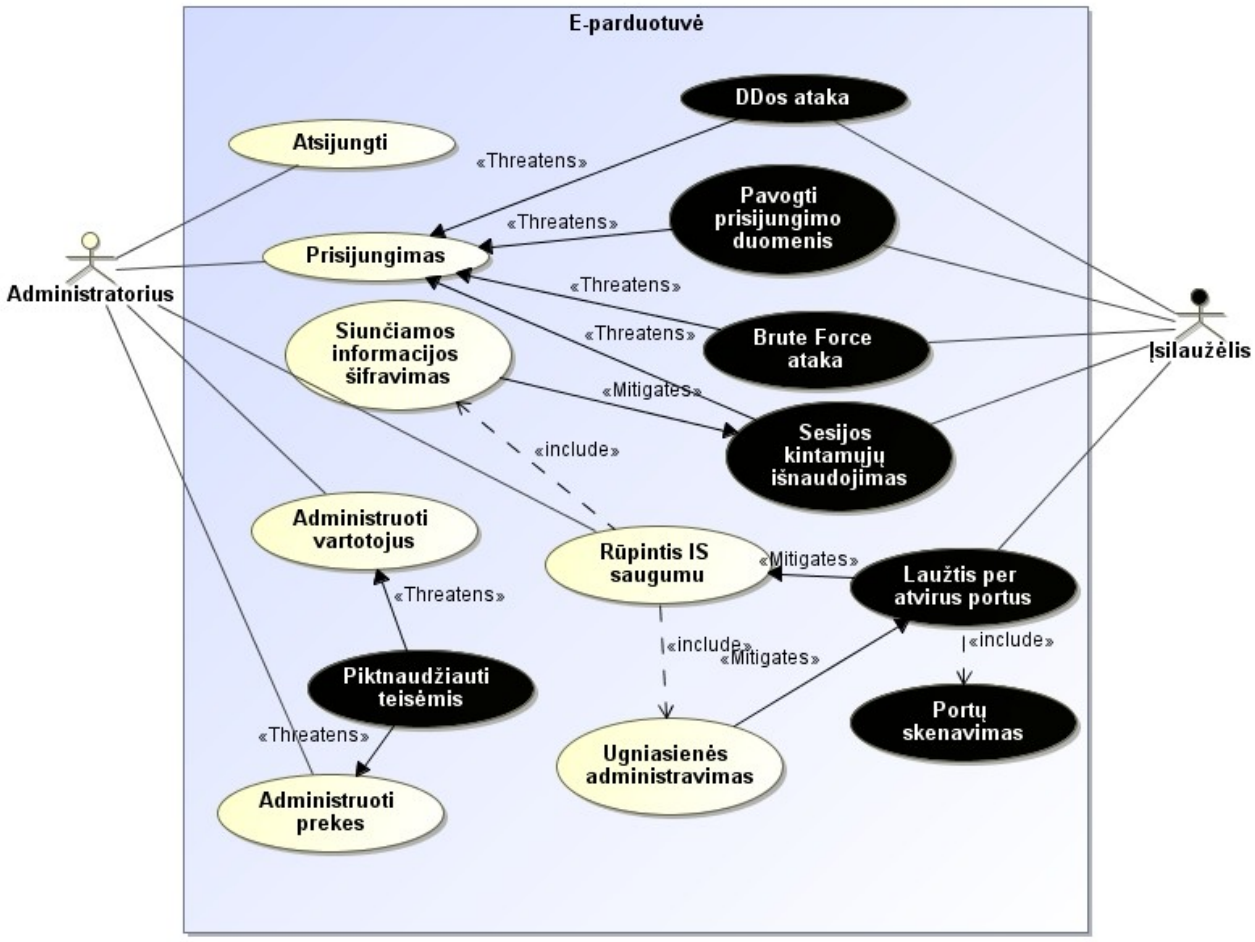
40 pav. Piktnaudžiavimo atvejų diagrama.

Pirkėjo panaudojimo atvejams keliamos grėsmės pavaizduotos 41 pav. Ši diagrama yra išskirta iš bendros piktnaudžiavimo atvejų diagramos (40 pav.).



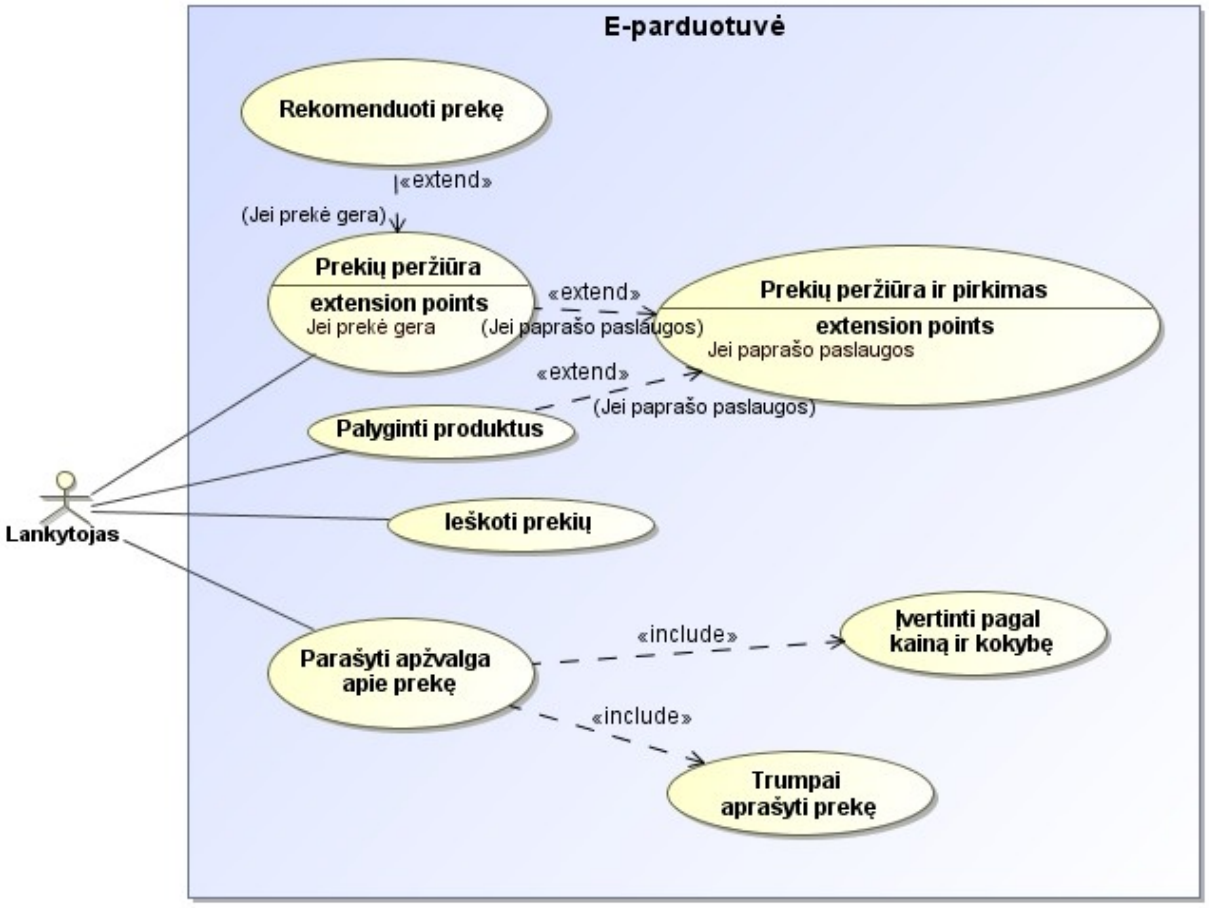
41 pav. Piktnaudžiavimo atvejų pirkėjo diagrama.

Administratoriaus panaudojimo atvejai ir jiems kylančios grėsmės pavaizduotos 42 pav. Piktnaudžiavimo atvejų yra daug, tai rodo, kad įsilaužėlis yra linkęs trikdyti IS valdymo funkcijas.



42 pav. Piktnaudžiavimo atvejų administratoriaus diagrama.

Lankytojo panaudojimo atvejai pavaizduoti 43 pav.



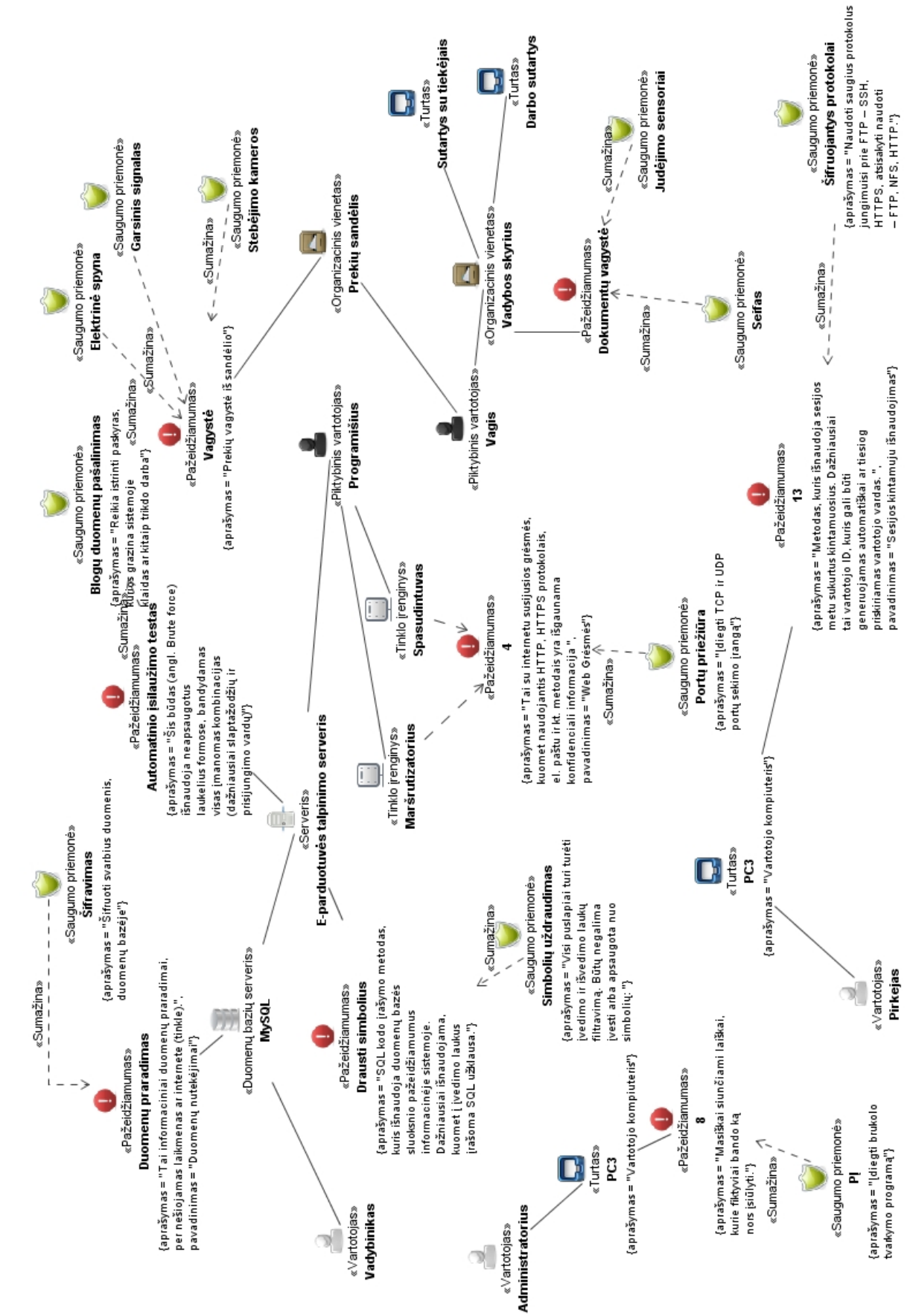
43 pav. Piktnaudžiavimo atvejų administratoriaus diagrama.

6.2.2. Organizacijos modelio sudarymas

Saugumo organizacinis modelis yra piktnaudžiavimo atvejų diagramos papildymas. Organizacinis modelis yra struktūriškas ir neapsiriboja vien tik informacinės sistemos funkcijų saugumo užtikrinimu, kaip piktnaudžiavimo atvejuose, bet leidžia pažvelgti modeliuotojui iš paprastesnės pusės – organizacijos struktūros. Šis saugumo modelis neapsiriboja ne tik metodo parinktomis saugumo priemonėmis ir grėsmėmis, bet ir paties modeliuotojo nuožiūra priskirtais naujais saugumo elementais.

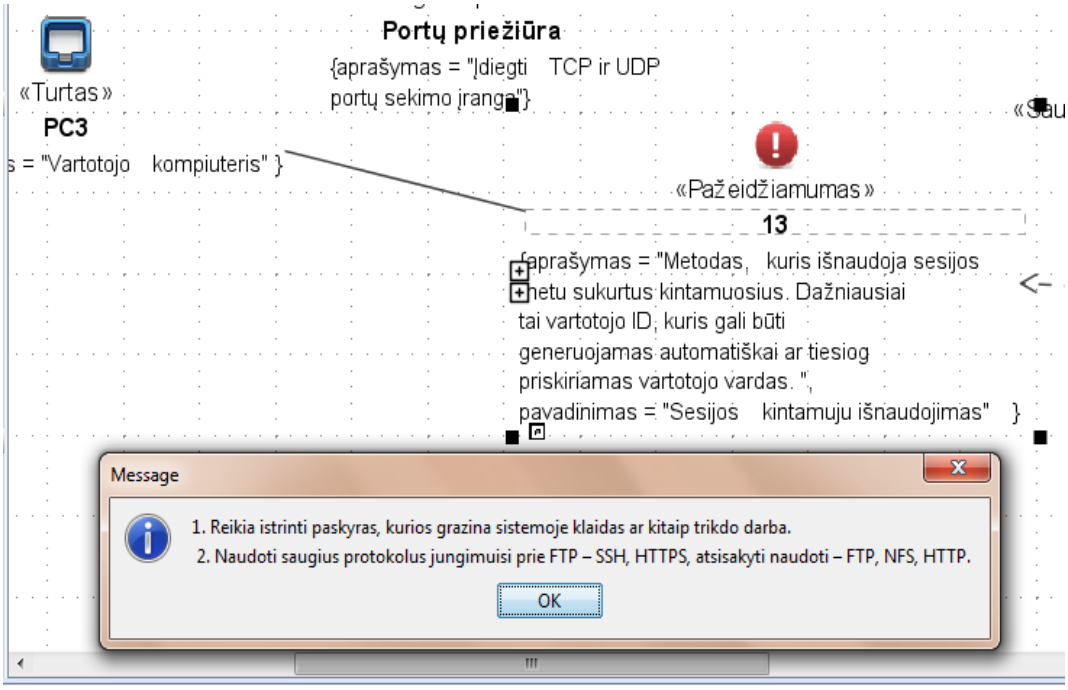
Įmonės „Piramidė LT“ organizacijos saugumo modelis pateiktas 44 pav. Jame pavaizduoti 2 piktybiniai vartotojai – vagis ir programišius, kurie kėsinasi į skirtingą įmonės turtą. Vagis – į fizinį turtą, svarbius dokumentus ir sandėlyje laikomas prekes. Programišius kėsinasi į įmonės turtą kuris yra prieinamas per internetą. Prie kiekvieno elemento, kuriam kyla pažeidimo grėsmė yra prijungiama pažeidžiamumo savybė, kuri galioja tam elementui. Prie pažeidžiamumo jungiama saugumo priemonė, kuri mažina efektą keliamo pažeidžiamumo.

Modelyje pavaizduoti trys nekenksmingi vartotojai administratorius, pirkėjas ir vadybininkas, kuriems saugumo grėsmės kyla per įmonės kompiuterius. Kompiuteriams pavaizduoti panaudoti „turto“ elementai. Modeliuojant ne visada būna pateikiami reikalingi elementai, todėl šiam saugumo modeliui buvo sukurtas turto elementas, kuriuo galima aprašyti organizacijoje esančius daiktus, tiek fizines tiek materialias vertybes.



44 pav. Saugumo organizacinis modelis

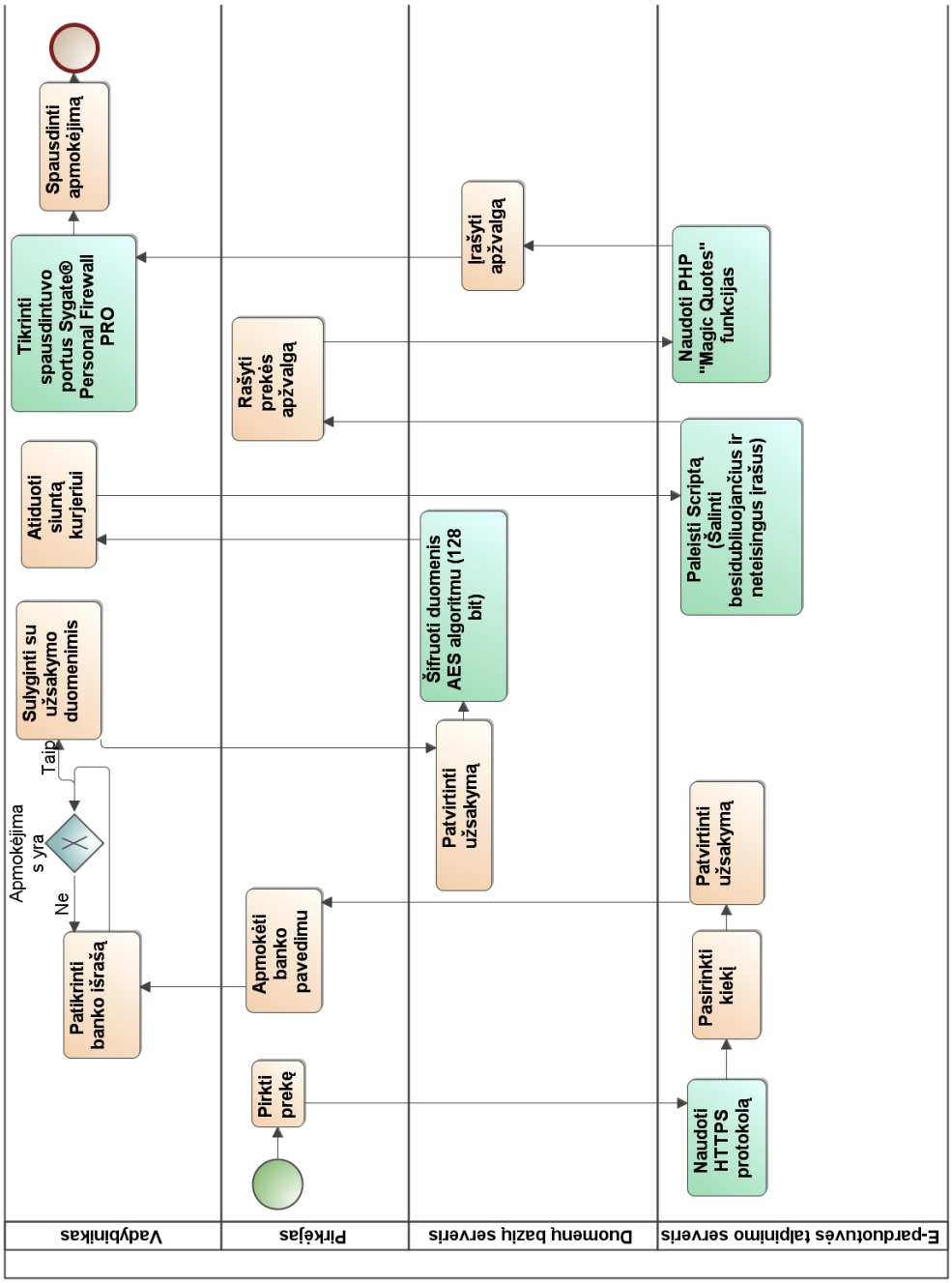
Sukurtas įskiepis leidžia pagal pažeidžiamumų sąrašą (lentelė 8) gauti tam tikras šablonines saugumo priemonės (lentelė 9). Įskiepio veikimas pademonstruotas 45 pav.



45 pav. Įskiepio panaudojimas.

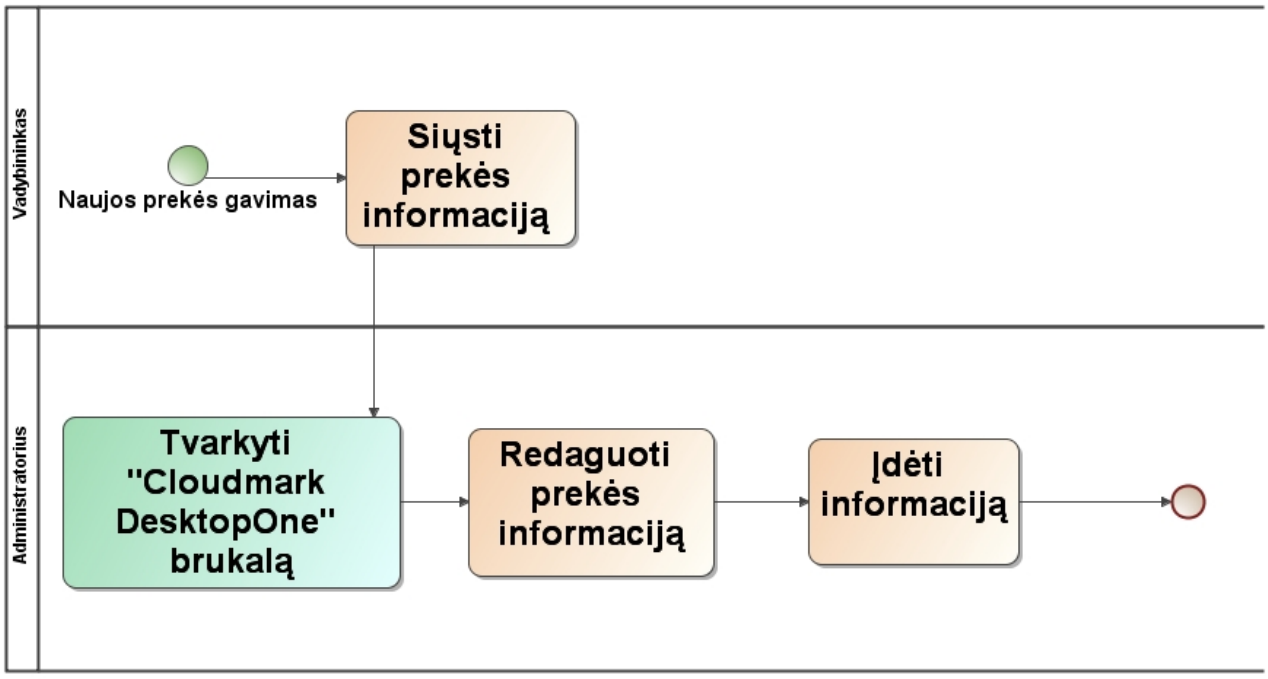
6.3. Organizacinio lygio saugumo identifikavimas

Organizaciniame lygyje braižomos BPMN diagramos, kurios detalizuoja organizacijos taktinio lygio saugumo grėsmes. Prekės pirkimo veiklos procesas pavaizduotas 46 pav, kuriame saugumo priemonės yra parinktos konkrečios – „Duomenų šifravimas AES algoritmu (128 bit)“, taikoma užsakymo patvirtinimui ir jo informacijos šifravimui duomenų bazėje. Taktiniame lygyje ši saugumo priemonė buvo pažymėta – Šifravimas (šifruoti svarbius duomenis duomenų bazėje).



46 pav. Saugumo priemonių indentifikavimas BPMN

Prekės įdėjimo veiklos procese (46 pav.) parduotuvės vadybininkas gavęs prekes persiunčia jų informaciją (nuotraukos, aprašymas) administratoriui. Administratorius prieš dėdamas į e-parduotuvę redaguoja informaciją. BPMN diagramoje saugumo priemonė pavaizduota žalia spalva (47 pav.) – „Cloudmark DesktopOne“ brukalo tvarkymas. Ši programa tvarko gaunamus brukalo laiškus



47 pav. Prekės įdėjimo veiklos procesas.

6.4.Eksperimento išvados

1. Saugumo reikalavimų modeliavimo metodas apima svarbiausius organizacijos veiklos aspektus.
2. Saugumo reikalavimai modeliuojami trimis etapais yra išbaigtesni ir detalesni.
3. Naudojant sukurtą MagicDraw profilį buvo sumodeliuota UAB „Piramide LT“ organizacijos struktūra su fizinemis ir materialiomis grėsmėmis.
4. Modeliavimas buvo paprastas, patogus nes buvo galima sumodeliuoti net tik standartinius elementus (serverius,spausdintuvus ir kt.), bet ir organizacijos struktūrines dalis

Lentelėje 12 pavaizduotas sukurtas veiklos reikalavimų modeliavimo metodo palyginimas su piktnaudžiavimo atvejais ir i* karkasu. Palyginus matosi, kad veiklos reikalavimų modeliavimo metodas yra geresnis už kitus, nes modeliuojant saugumo reikalavimus atsižvelgiama į tikslus ir saugumo reikalavimai yra skaidomi iki konkrečių saugumo priemonių.

Lentelė 12. Sukurto metodo palyginimas

Palyginimo kriterijai	Piktnaudžiavimo atvejai	i* karkasas	sukurtas veiklos reikalavimų modeliavimo metodo
Ar nagrinėja saugumo reikalavimus?	Taip	Taip	Taip
Ar nagrinėja saugumo reikalavimų priklausomybes?	Taip	Taip	Taip
Ar išveda saugumo reikalavimus iš tikslų?	Ne	Ne	Taip
Ar išskaido saugumo reikalavimus iki atominių vienetų?	Ne	Ne	Taip
Ar turi šablonus saugumo reikalavimams specifikuoti?	Taip	Ne	Taip
Ar gali būti atvaizduojami organizacijos objektai?	Taip	Ne	Taip

7. Išvados

Įgyvendinant saugumą veiklos procesuose yra svarbu palaipsniui modeliuoti organizaciją detalizuojant jos struktūrą ir procesus. Sukurtas saugumo priemonių projektavimo metodas detaliai atvaizduoja organizacijos struktūrai kylančias grėsmes. Kuriant IS, aprašant jos kompiuterizuojamas funkcijas (UML, panaudojimo atvejų diagrama) sistemos saugumo aspektai dažnai paliekami saviveiklai.

Pagrindiniai rezultatai ir išvados:

1. Darbe sukurtas praktinis saugumo reikalavimų užtikrinimo metodas, siejantis veiklos modelius su reikalavimų specifikacija. Išnagrinėti IS saugumo standartų reikalavimai, kitų autorių sprendimai specifikuojant saugumo reikalavimus.

2. Darbe panaudoti šie modeliai: UML Use Case; MODAF metodologijos modelis STV1 strategijoms modeliuoti, reikalavimų IS modeliavimo būdas įvertinantis piktnaudžiavimo atvejus.

3. UML Use Case diagrama (panaudojimo atvejų modelis) labai gerai pasiteisino ieškant neleistinų veiksmų, nes piktnaudžiavimo atvejai suintegruoja tiesioginių sistemos funkcijų ir saugumo reikalavimų modeliavimą.

4. Darbe pasiūlyta piktnaudžiavimo atvejų specifikacija leistų generuoti klases saugumo reikalavimams užtikrinti.

5. Gauti rezultatai gali būti panaudoti praktiškai. Siūlome katedrai įtraukti piktnaudžiavimo atvejų modeliavimą į metodikas rengiant bakalauro baigiamuosius darbus, nes panaudojimo atvejai apibrėžia tik galimas sistemos funkcijas, bet nėra kreipiamas dėmesys saugumo funkcijoms.

8. Literatūra

1. Sojan Markose, Xiaoqing (Frank) Liu, and Bruce McMillin. A Systematic Framework for Structured Object-Oriented Security Requirements Analysis in Embedded Systems. Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on 17-20 Dec. 2008, Vol. 1, 75 – 81.
2. Guttom Sindre, Andreas L. Opdahl. Eliciting security requirements with misuse cases. Requirements Eng (2005) 10: 34–44.
3. G. Elahi, E. Yu. Data & Knowledge Engineering 68 (2009) 579–598.
4. John McDermott, Chris Fox . Using Abuse Case Models for Security Requirements Analysis. Proceedings of the 15th Annual Computer Security Applications Conference, 1999, 55.
5. Thomas A. Horan, Ph.D., Tarun Abhichandani, Raghuvira Rayalu, School of Information, Systems and Technology, Claremont Graduate University, Claremont, CA, USA "Assessing User Satisfaction of E-Government Services: Development and Testing of Quality-in-Use Satisfaction with Advanced Traveler Information Systems (ATIS)" Proceedings of the 39th Hawaii International Conference on System Sciences – 2006.
6. Tomas Olovsson. A Structured Approach to Computer Security. Technical Report No 122, 1992.
7. Doug Rosenberg and Matt Stephens. Use Case Driven Object Modeling with UML – Theory and Practice (2007)
8. Ma, M. Mitigating Denial of Service Attacks with Password Puzzles. Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on 4-6 April 2005, Vol. 2, 621
9. Daniel Mellado, Eduardo Fernández-Medina and Mario Piattini. Towards security requirements management for software product lines: A security domain requirements engineering process. Computer Standards & Interfaces Volume 30, Issue 6, August 2008, Pages 361-371
   Special Issue: State of standards in the information systems security area
10. Daniel Mellado, Carlos Blanco, Luis E. Sánchez and Eduardo Fernández-Medina. A systematic review of security requirements engineering. Computer Standards & Interfaces Volume 32, Issue 4, June 2010, Pages 153-165

11. Travis D. Breaux, and David L. Baumer Legally “reasonable” security requirements: A 10-year FTC retrospective Computers & Security Volume 30, Issue 4, June 2011, Pages 178-193
12. KAOS tutorial, puslapiai 12-20 psl. Prieiga per internetą: http://www.objectiver.com/fileadmin/download/documents/KaosTutorial.pdf
13. Miguel A. Martínez , Joaquín Lasheras, Eduardo Fernández-Medina, Ambrosio Toval and Mario Piattini A Personal Data Audit Method through Requirements Engineering Computer Standards & Interfaces Volume 32, Issue 4, June 2010, Pages 166-178
14. Andreas L. Opdahl and Guttorm Sindre. Experimental comparison of attack trees and misuse cases for security threat identification. Information and Software Technology Volume 51, Issue 5, May 2009, Pages 916-932 SPECIAL ISSUE: Model-Driven Development for Secure Information Systems
15. Haralambos Mouratidis and Paolo Giorgini. Security Attack Testing (SAT)—testing the security of information systems at design time. Information Systems Volume 32, Issue 8, December 2007, Pages 1166-1183
16. Lars Grunske, and David Joyce. Quantitative risk-based security prediction for component-based systems with explicitly modeled attack profile. Journal of Systems and Software Volume 81, Issue 8, August 2008, Pages 1327-1345
17. Teodor Sommestad, Mathias Ekstedt and Pontus Johnson. A probabilistic relational model for security risk analysis. Computers & Security Volume 29, Issue 6, September 2010, Pages 659-679
18. Tsai, Ching-Hong ; Luo, How-Jen ; Wang, Feng-Jian. Constructing a BPM Environment with BPMN. Future Trends of Distributed Computing Systems, 2007.
19. Michael E. Shin and Hassan Gomaa. Software requirements and architecture modeling for evolving non-secure applications into secure applications. Science of Computer Programming Volume 66, Issue 1, 15 April 2007, Pages 60-70
20. Elias Pimenidis and Christos K. Georgiadis. Web services for rural areas—Security challenges in development and use. Computers and Electronics in Agriculture Volume 70, Issue 2, March 2010, Pages 348-354 Special issue on Information and Communication Technologies in Bio and Earth Sciences

21. Robert Booker. Re-engineering enterprise security. Computers & Security Volume 25, Issue 1, February 2006, Pages 13-17
22. Omar F. El-Gayar and Brian D. Fritz. A web-based multi-perspective decision support system for information security planning. Decision Support Systems Volume 50, Issue 1, December 2010, Pages 43-54
23. Mikko Siponen and Robert Willison. Information security management standards: Problems and solutions. Information & Management Volume 46, Issue 5, June 2009, Pages 267-270
24. Serap Atay and Marcelo Masera. Challenges for the security analysis of Next Generation Networks. Volume 15, Issue 3, Pages 77-136 August 2010
25. Albin Zuccato. Holistic security requirement engineering for electronic commerce. Computers & Security
Volume 23, Issue 1, February 2004, Pages 63-76
26. Daniel Mellado, Eduardo Fernández-Medina and Mario Piattini. Security requirements engineering framework for software product lines. Information and Software Technology. Volume 52, Issue 10, October 2010, Pages 1094-1117
27. MODAF tutorial, Prieiga per internetą: http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/InformationManagement/MODAF/
28. International Standard ISO/IEC 17799. Prieiga per internetą: http://engweb.info/courses/ens/extra/ISO-IEC%2017799-2005.pdf
29. International Standard ISO 13335. Prieiga per internetą: http://webstore.iec.ch/preview/info_isoiec13335-1%7Bed1.0%7Den.pdf

9. Priedai

1 priedas. Panaudojimo atvejų detalizavimas

Panaudojimo atvejo „Registracija“ detalizavimas

1. PANAUDOJIMO ATVEJIS:	Registracija
Vartotojas/Aktorius:	Pirkėjas
Aprašas:	Vartotojo registracijos procesas, kurio metu suvedami duomenys.
Prioritetas	Labai svarbus
Prieš sąlyga:	Vartotojas neregistruotas sistemoje.
Pagrindinis scenarijus:	Vartotojas suveda vardą, pavardę, el. pašto adresą.
Po-sąlyga:	Vartotojas užregistruotas sistemoje.
Alternatyvus scenarijus	Vartotojas pats atšaukė operaciją.

Panaudojimo atvejo „Administruoti vartotojus“ detalizavimas

2. PANAUDOJIMO ATVEJIS:	Administruoti vartotojus
Vartotojas/Aktorius:	Administratorius
Aprašas:	Procesas kuomet administratorius peržiūri vartotojus ir keičią jų informaciją.
Prioritetas	Labai svarbus
Prieš sąlyga:	Vartotojas turi būt registruotas sistemoje.
Pagrindinis scenarijus:	Administratorius šalina neaktyvius vartotojus, su neteisingais duomenimis, ar vartotojų pageidavimu keičia jų informaciją.
Po-sąlyga:	Redaguotas vartotojas.
Alternatyvus scenarijus	

Panaudojimo atvejo „Administruoti prekes“ detalizavimas

3. PANAUDOJIMO ATVEJIS:	Administruoti prekes
Vartotojas/Aktorius:	Administratorius.
Aprašas:	Apima procesą, kurio metu administratorius rūpinasi asortimento pateikimu.
Prioritetas	Labai svarbus
Prieš sąlyga:	Administratorius prisijungęs.
Pagrindinis scenarijus:	Administratorius įdeda naujas prekes į el. parduotuvę, su visa jų informacija (paveikslėliais, aprašymu), išima nebeprekiaujamas prekes ir redaguoja esamų informaciją.
Po-sąlyga:	Prekės informacija atnaujinta.
Alternatyvus scenarijus	Jei reikia prekių nuotraukos redaguojamos.

Panaudojimo atvejo „Siunčiamos informacijos šifravimas“ detalizavimas

4. PANAUDOJIMO ATVEJIS:	Siunčiamos informacijos šifravimas.
Vartotojas/Aktorius:	Administratorius
Aprašas:	Procesas, kurio metu siunčiama informacija yra šifruojama.
Prioritetas	Svarbus
Prieš sąlyga:	Norima išsiusti informaciją.
Pagrindinis scenarijus:	Siunčiama informacija yra koduojama HTTPS protokolu.
Po-sąlyga:	Gauta šifruota informacija.
Alternatyvus scenarijus	

Panaudojimo atvejo „Rūpintis IS saugumu“ detalizavimas

5. PANAUDOJIMO ATVEJIS:	Rūpintis IS saugumu
Vartotojas/Aktorius:	Administratorius
Aprašas:	Apima procesą, kurio metu administratorius rūpinasi, kad sistema veiktų.
Prioritetas	Labai svarbus
Prieš sąlyga:	
Pagrindinis scenarijus:	Administratorius prižiūri, kad IS veiktų sklandžiai ir nuolatos.
Po-sąlyga:	Veikianti IS sistema.
Alternatyvus scenarijus	

Panaudojimo atvejo „Ugniasienės administravimas“ detalizavimas

6. PANAUDOJIMO ATVEJIS:	Ugniasienės administravimas
Vartotojas/Aktorius:	Administratorius
Aprašas:	Apima procesą, kurio metu ugniasienės veikla prižiūrima.
Prioritetas	Labai svarbus
Prieš sąlyga:	
Pagrindinis scenarijus:	Administratorius konfigūruoja ugniasienę, kad prireikus ji neapribotų e-parduotuvės funkcionalumo, o ir saugotų nuo įsilaužimų.
Po-sąlyga:	Tinkamai veikianti ugniasienė.
Alternatyvus scenarijus	Paliktas automatinis ugniasienės konfiguravimas.

Piktnaudžiavimo atvejo „SQL injekcija“ detalizavimas

7. PIKTNAUDŽIAVIMO ATVEJIS:	SQL injekcija

Vartotojas/Aktorius:	Įsilaužėlis
Piktnaudžiautojo profilis:	Vartotojas elgiasi tyčia, norėdamas išgauti duomenis arba pažeisti duomenų bazę.
Aprašas:	Apima procesą, kurio metu įsilaužėlis bando įsilaužti pasinaudojęs SQL injekcijomis.
Prioritetas	Labai svarbus
Prieš sąlyga:	Yra įvedimo laukeliai.
Pagrindinis scenarijus:	Įsilaužėlis naudodamas įvedimo laukelius, vykdo SQL injekcijas.
Po-sąlyga:	Prisijungta kitu asmeniu arba pažeista duomenų bazė.
Alternatyvus scenarijus	
Sušvelninimo taškai:	1. Vartotojui neparodoma duomenų bazės žinutė, su lentelių pavadinimais ar laukų. 2. Priimant duomenis iš laukelių patikrinama ar juose nėra neleistinų simbolių.
Sušvelninimo garantija:	Vartotojas negali valdyti duomenų bazės per formos laukus.

Piktnaudžiavimo atvejo „Piktnaudžiauti teisėmis“ detalizavimas

8. PIKTNAUDŽIAVIMO ATVEJIS:	Piktnaudžiauti teisėmis
Vartotojas/Aktorius:	Pirkėjas
Piktnaudžiautojo profilis:	Vartotojas elgiasi tyčia.
Aprašas:	Apima procesą, kurio metu vartotojas pateikia neteisingus duomenis.
Prioritetas	Svarbus
Prieš sąlyga:	Užregistruotas vartotojas.
Pagrindinis scenarijus:	Vartotojas pateikia neteisingus duomenis apie save, prekių atsiliepimuose pateikia taip pat neigiamus arba

	nesantūrius atsiliepimus.
Po-sąlyga:	Informacija apie prekes ar vartotoja yra dezinformatyvi.
Sušvelninimo taškai:	1. Apsaugos įdėjimas, kuri filtruotų nesantūrius žodžius.

Piktnaudžiavimo atvejo „Pavogti prisijungimo duomenis“ detalizavimas

9. PIKTNAUDŽIAVIMO ATVEJIS:	Pavogti prisijungimo duomenis
Vartotojas/Aktorius:	Įsilaužėlis
Piktnaudžiautojo profilis:	Vartotojas elgiasi tyčia, norėdamas gauti duomenis, kuriais galėtų manipuliuoti.
Aprašas:	Apima procesą, kurio metu įsilaužėlis pavagia nesaugius prisijungimo duomenis ir su jais prisijungia.
Prioritetas	Svarbus
Prieš sąlyga:	Registruoti vartotojai yra naudojęsi sistema.
Pagrindinis scenarijus:	Įsilaužėlis fiziškai suseka prisijungimo duomenis arba įrašęs kenkėjišką programą į vartotojo kompiuterį.
Po-sąlyga:	Prisijungta kitu asmeniu.
Alternatyvus scenarijus	
Sušvelninimo taškai:	1. Vartotojui prisijungiant reiktų suvesti kodą iš kodų kortelės.

Piktnaudžiavimo atvejo „Brute Force ataka“ detalizavimas

10. PIKTNAUDŽIAVIMO ATVEJIS:	Brute Force ataka
Vartotojas/Aktorius:	Įsilaužėlis
Piktnaudžiautojo profilis:	Vartotojas elgiasi tyčia, norėdamas atspėti prisijungimo duomenis.

Aprašas:	Apima procesą, kurio metu įsilaužėlis pasinaudodamas priemonėmis bando atspėti prisijungimo duomenis (dažniausiai vartotojo prisijungimo vardas būna žinomas).
Prioritetas	Svarbus
Prieš sąlyga:	Vartotojas yra registruotas sistemoje.
Pagrindinis scenarijus:	Įsilaužėlis paleidžia programą, kuri spėja slaptažodį.
Po-sąlyga:	Įsilaužėlis prisijungia kitu vartotoju.
Alternatyvus scenarijus	Įsilaužėlis bando nulaužti ir prisijungimo vardą ir slaptažodį.
Sušvelninimo taškai:	1. Sistemoje apribotas prisijungimų skaičius vieno vartotojo per tam tikrą nustatytą laiką. 2. Apribotas bendras sistemos vartotojų prisijungimo skaičius per tam tikrą. 1. Sistemoje įdiegti slaptažodžių sudėtingumo tikrinimą. 2. Padaryti privalomus simbolius (raidė, skaičius, skyrybos ženklai), kurie būtų įtraukti į slaptažodžius taip juos padarant sudėtingesniais.
Technologijų ir duomenų variantai:	1. Įsilaužėlis pasitelkęs lietuvių kalbos žodyną ar anglų. 2. Įsilaužėlis gali naudotis sudarytais sąrašais pagal dažniausiais naudojamus slaptažodžius.

Piktnaudžiavimo atvejo „DDos ataka“ detalizavimas

11. PIKTNAUDŽIAVIMO ATVEJIS:	DDos ataka
Vartotojas/Aktorius:	Įsilaužėlis
Piktnaudžiautojo profilis:	Vartotojas elgiasi tyčia, norėdamas atspėti sutrikdyti e-parduotuvės darbą, dažnai tai daro šantažuodamas.
Sritis:	Ši ataka nukreipta į serverį.
Aprašas:	Apima procesą, kurio metu įsilaužėlis pasinaudodamas

	priemonėmis bando sutrikdyti e-parduotuvės darbą.
Prioritetas	Svarbus
Pagrindinis scenarijus:	Įsilaužėlis sukuria didelį kompiuterių tinklą, kurie siunčia užklausas į e-parduotuvės sistemą, taip sutrikdant normalų jos darbą.
Po-sąlyga:	E-parduotuvėje negalima atlikti pirkimų.
Sušvelninimo taškai:	1. Įdiegti programinę įrangą, kuri atpažintų DDoS ataką ir tuomet paleistų IP tikrinimo programą, kuri neleistų kenkėjiškiems IP užduoti užklausų.
Technologijų ir duomenų variantai:	1. Dideli kompiuteriu tinklas (dažnai užkrėstų kompiuterių), kurie valdomi vieno pažeidėjo.

Piktnaudžiavimo atvejo „Sesijos kintamųjų išnaudojimas“ detalizavimas

12. PIKTNAUDŽIAVIMO ATVEJIS:	Sesijos kintamųjų išnaudojimas
Vartotojas/Aktorius:	Įsilaužėlis
Aprašas:	Apima procesą, kurio metu įsilaužėlis pasinaudodamas priemonėmis bando gauti sesijos kintamuosius.
Prioritetas	Labai svarbus
Prieš sąlyga:	Vartotojas buvo prisijungęs sistemoje.
Pagrindinis scenarijus:	Įsilaužėlis pavogdamas vartotojui IS sugeneruotą (priskirtą) ID gali juo pasinaudoti, taip apsimesdamas kitu asmeniu.
Po-sąlyga:	Įsilaužėlis prisijungia kitu asmeniu.
Sušvelninimo taškai:	1. Siunčiama informacija yra koduojama HTTPS protokolu. 2. Sudaromi sesijos ID, kurie būna susieti su tam tikru kompiuteriu.

Piktnaudžiavimo atvejo „Laužtis per atvirus portus“ detalizavimas

13. PIKTNAUDŽIAVIMO ATVEJIS:	Laužtis per atvirus portus

Vartotojas/Aktorius:	Įsilaužėlis
Piktnaudžiautojo profilis:	Įsilaužėlis tyčia bando laužtis per pažeidžiamus portus.
Aprašas:	Apima procesą, kurio metu įsilaužėlis išnaudoja atvirus portus.
Prioritetas	Svarbus
Prieš sąlyga:	Įsilaužėlis radęs pažeidžiamus portus.
Pagrindinis scenarijus:	Įsilaužėlis išnaudoja pažeidžiamo serviso portą, taip gaudamas naudingos informacijos.
Po-sąlyga:	Pažeista IS apsauga.
Sušvelninimo taškai:	1. Rankiniu būdu nustatyti naudojami portai, nepalikti pagal nutylėjimą.
Technologijų ir duomenų variantai:	1. Naudojama programinė įranga portų skenavimui.

Piktnaudžiavimo atvejo „Portų skenavimas“ detalizavimas

14. PIKTNAUDŽIAVIMO ATVEJIS:	Portų skenavimas
Vartotojas/Aktorius:	Įsilaužėlis
Aprašas:	Apima procesą, kurio Įsilaužėlis skenuoja portus.
Prioritetas	Svarbus
Pagrindinis scenarijus:	Įsilaužėlis skenuoja atvirus portus.
Po-sąlyga:	Rasti atviri portai.
Sušvelninimo taškai:	1. Rankiniu būdu nustatyti naudojami portai, nepalikti pagal nutylėjimą.
Technologijų ir duomenų variantai:	1. Naudojama programinė įranga portų skenavimui.

2 priedas. Magic Draw įskiepio kodas

DiagramAction.Java

```
package myplugin;

import com.nomagic.magicdraw.ui.actions.DefaultDiagramAction;
import com.nomagic.magicdraw.ui.dialogs.MDDialogParentProvider;
import com.nomagic.magicdraw.properties.Property;
import com.nomagic.magicdraw.properties.PropertyManager;

import com.nomagic.magicdraw.openapi.uml.SessionManager;
import com.nomagic.magicdraw.uml.symbols.PresentationElement;
import com.nomagic.uml2.impl.PropertyNames;

import com.nomagic.uml2.ext.magicdraw.classes.mdkernel.Element;
import com.nomagic.magicdraw.properties.StringProperty;
import com.nomagic.magicdraw.properties.PropertyID;
import com.nomagic.uml2.ext.magicdraw.classes.mdkernel.NamedElement;

import com.nomagic.uml2.impl.ElementsFactory;
import com.nomagic.uml2.ext.magicdraw.classes.mdkernel.Class;
import com.nomagic.magicdraw.core.Application;


import javax.swing.*;
import java.awt.event.ActionEvent;
import java.awt.event.KeyEvent;

import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;

public class DiagramAction extends DefaultDiagramAction
{

    public DiagramAction()
    {
        super("Tinkinti", "Tinkinti", KeyStroke.getKeyStroke(KeyEvent.VK_E,
KeyEvent.SHIFT_MASK+KeyEvent.ALT_MASK), null);
    }


    public void actionPerformed(ActionEvent e)
    {
       String tipas = getFirstSelected().getHumanType(); // Gaunamas elemento vardas
pazeidziamumas
         String text5 = getFirstSelected().getHumanType() + " tipas" +
getFirstSelected().getName() + "Name \n";


String[] anArrayOfStrings;
anArrayOfStrings = new String[50]; //sukuriamas masyvas
               anArrayOfStrings[0] = "nera"; // initialize first element
         anArrayOfStrings[1] = "1. Blokuoti papildomus servisus, kuriais isilauzelis
gali pasinaudoti.\n  2. Sifruoti svarbius duomenis duomenu bazeje."; // initialize second
element
          anArrayOfStrings[2] = "1. Testines paskyras vertetu istrinti.\n 2. Suteikti
prieigos teises prie duomenu bazes tik patikimimiems zmonems\n 3. Nenaudotinu portu
blokavimas.\n 4. Blokuoti papildomus servisus, kuriais isilauzelis gali pasinaudoti.\n 5.
```

```
Sifruoti svarbius duomenis duomenu bazeje.\n 6. Reikia istrinti paskyras, kurios grazina
sistemoje klaidas ar kitaip trikdo darba.\n 7. Visada laiku atnaujinti serverio
programine iranga.\n 8. Serverio programine iranga ir OS, laikyti skirtinguose fiziniuose
ar loginiuose diskuose.\n 9. Pasalinti ar panaikinti numatytasias paskyras.\n 10.
Apriboti vartotoju nuotolinio prisijungimo teises.\n 11. Apriboti vietas (IP adresus) is
kuriu butu galima jungtis.\n 12. Jei duomenys ypatingai svarbus, idiegti papildomus
saugumo mechanizmus nuotoliniui jungimuisi."; // etc.
          anArrayOfStrings[3] = "1. Sifruoti svarbius duomenis duomenu bazeje. ";
          anArrayOfStrings[4] = "1. Idiegti TCP ir UDP portu sekimo iranga.";
          anArrayOfStrings[5] = "1. Sifruoti svarbius duomenis duomenu bazeje. ";
          anArrayOfStrings[6] = "1. Suteikti prieigos teises prie duomenø bazes tik
patikimimiems zmonems. ";
          anArrayOfStrings[7] = "1. Suteikti prieigos teises prie duomenu bazes tik
patikimimiems zmonems. ";
          anArrayOfStrings[8] = "1. Idiegti brukalo tvarkymo programa.";
          anArrayOfStrings[9] = "1. Visi puslapiai turi tureti ivedimo ir isvedimo lauku
filtravima. Butu negalima vesti arba apsaugota nuo neleistinø simboliu.".\n 2. Vietoj
paprastu uzklausu ivedimo laukams, naudoti patalpintas proceduras (stored procedures).\n
3. Apriboti teises uzklausoms ar patalpintoms proceduroms (kad prisijungimo formoje
nebutu galima istrinti lenteles ar duomenu).\n 4. Nepavykus prisijungti, neturetu buti
grazinama zinute, kuri nurodytu kas buvo netiksliai ivesta – vartotojo vardas ar
slaptazodis.\n 5. Reikia istrinti paskyras, kurios grazina sistemoje klaidas ar kitaip
trikdo darba.\n 6. Suteikti prieigos teises prie duomenu bazes tik patikimimiems
zmonems.\n 7. Klaidu pranesimu apsaugojimas (nerodymas), kai vykdant SQL uzlausas
tinklapyje parodoma, kokia klaida istiko.\n";
               anArrayOfStrings[10] = "1. Panaikinti HTTP Trace funkcija (si funkcija
grazina atgal vartotojui ivedimo duomenis) serveryje.\n 2. Panaikinti nereikalingas
paskyras IIS (Internet Information Services.\n 3. Reikia istrinti paskyras, kurios
grazina sistemoje klaidas ar kitaip trikdo darba.\n 4. Panaikinti visus idiegtus, bet
nenaudojamus servisus.\n";
               anArrayOfStrings[11] = "1. Idiegti brukalo tvarkymo programa.";
               anArrayOfStrings[12] = "1. Sifruoti svarbius duomenis duomenu bazeje.\n
2. Reikia istrinti paskyras, kurios grazina sistemoje klaidas ar kitaip trikdo darba.";
               anArrayOfStrings[13] = "1. Reikia istrinti paskyras, kurios grazina
sistemoje klaidas ar kitaip trikdo darba.\n 2. Naudoti saugius protokolus jungimuisi prie
FTP – SSH, HTTPS, atsisakyti naudoti – FTP, NFS, HTTP. ";
            String name = getFirstSelected().getName();
            String getThreat  = "";
            Integer i = Integer.parseInt( name );
            if (tipas.equals("Pažeidžiamumas")){
            getThreat = anArrayOfStrings[i];

            }else {
            getThreat = "nera" + tipas + "Pažeidžiamumas";
            }



}*/String yra = "";



JOptionPane.showMessageDialog(MDDialogParentProvider.getProvider().getDialogParent(),
getThreat);


    }
```

```
    public void updateState()
    {
        setEnabled(getSelected().size()>0);
    }
}
```

DiagramConfigurator.Java

```
package myplugin;

import com.nomagic.actions.AMConfigurator;
import com.nomagic.actions.ActionsCategory;
import com.nomagic.actions.ActionsManager;
import com.nomagic.magicdraw.actions.ActionsID;
import com.nomagic.magicdraw.actions.DiagramContextAMConfigurator;
import com.nomagic.magicdraw.actions.MDActionsCategory;
import com.nomagic.magicdraw.ui.actions.DefaultDiagramAction;
import com.nomagic.magicdraw.uml.symbols.DiagramPresentationElement;
import com.nomagic.magicdraw.uml.symbols.PresentationElement;

public class DiagramConfigurator implements DiagramContextAMConfigurator, AMConfigurator
{
       private DefaultDiagramAction action;

       public DiagramConfigurator(DefaultDiagramAction action)
       {
              this.action = action;
       }

       public void configure(ActionsManager mngr,DiagramPresentationElement
diagram,PresentationElement[] selected, PresentationElement requestor)
       {
                     ActionsCategory category = new MDActionsCategory(null, null);
                     category.addAction(action);
                     mngr.addCategory(category);
       }

       public void configure(ActionsManager mngr)
       {
                     if( mngr.getActionFor(action.getID())==null)
                     {
                            ActionsCategory category = (ActionsCategory)
mngr.getActionFor( ActionsID.CLASS_DIAGRAM_ELEMENTS);
                            if(category != null )
                            {
                                   category.addAction(action);
                            }
                     }
       }
       public int getPriority()
       {
              return AMConfigurator.MEDIUM_PRIORITY;
       }

}
```

MyPlugin.Java

```
package myplugin;

import java.util.List;

import javax.swing.ImageIcon;

import com.nomagic.magicdraw.actions.*;
import com.nomagic.magicdraw.plugins.Plugin;
import com.nomagic.magicdraw.ui.browser.actions.DefaultBrowserAction;
import com.nomagic.magicdraw.uml.DiagramType;

public class MyPlugin extends Plugin
{

    public void init()
    {
        ActionsConfiguratorsManager manager = ActionsConfiguratorsManager.getInstance();

////////////////////////////////////////////////////////////////////////////////
//


        DiagramAction dAction = new DiagramAction();
        DiagramConfigurator diagramConfigurator = new DiagramConfigurator(dAction);
        manager.addDiagramContextConfigurator(DiagramType.UML_CLASS_DIAGRAM,
diagramConfigurator);
        manager.addDiagramShortcutsConfigurator(DiagramType.UML_CLASS_DIAGRAM,
diagramConfigurator);

        manager.addDiagramToolbarConfigurator(DiagramType.UML_CLASS_DIAGRAM,
diagramConfigurator);

    }


    public boolean close()
    {
        return true;
    }


    public boolean isSupported()
    {
        return true;
    }

}
```

3 priedas. Darbų pasiskirstymas

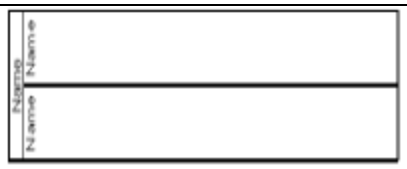
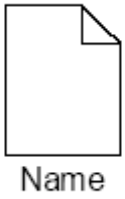
Lentelė 1.

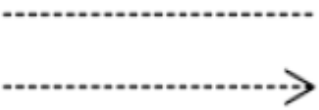
Darbų pasiskirstymas		
Magistro darbo turinys	Justinas Grėbliūnas	Monika Pažereckaitė
Saugumo reikalavimų analizė	**40 %**	**60 %**
Analizės tikslas	40 %	60 %
Tyrimo sritis, objektas ir problema	50%	50 %
Organizacijos UAB „Piramidė LT“ e-parduotuvės informacinės sistemos analizė	60 %	40 %
Vartotojų analizė	40 %	60 %
Problemos sprendimo metodų literatūros šaltiniuose analizė	40 %	60 %
Panašių modelių analizė	45 %	55 %
Architektūros ir galimų įgyvendinimo priemonių variantų analizė	50 %	50 %
Siekiamos sistemos apibrėžimas	60 %	40 %
Darbo tikslas ir siekiami privalumai	50 %	50 %
Analizės išvados	50 %	50 %
Saugumo reikalavimų specifikacija ir analizė	40 %	60 %
Reikalavimų specifikacija	45 %	55 %
Veiklos proceso saugumo modeliavimo projektas	**55 %**	**45 %**
Saugumo grėsmių identifikavimas	55%	45 %
Saugumo priemonės	60 %	40 %
Organizacijos pažeidžiamumų identifikavimas	60 %	40 %
Organizacijos elementų identifikavimas	60 %	40 %
Metodo koncepcinis modelis	60 %	40 %
Tikslų sudarymo procesas	50 %	50 %
Organizacinio modelio sudarymas	55 %	45 %
Veiklos procesų sudarymas	55 %	45 %
Realizacija	**60 %**	**40 %**
Strateginio lygio saugumo tikslų identifikavimas	55 %	45 %
Taktinio lygio saugumo identifikavimas	65 %	35 %
Organizacinio lygio saugumo identifikavimas	50 %	50 %
Eksperimento išvados	60 %	40 %

4 priedas. BPMN notacija

Veiklos procesų modeliavimo žymėjimai (2 lentelė).

Lentelė 2. BPMN notacija. [18]

Elementas	Notacija
Pool: Baseinas parodo, kad dalyvis yra procese. Jis taip pat veikia kaip „Swimlane“ ir grafinis konteineris vaizduojantis rinkinį veiklų kurie vyksta kituose baseinuose, dažniausiai B2B situacijose.	
Lane: Linija yra baseino sub-dalis, kuri tęsiasi per visą baseino ilgį, vertikaliai arba horizontaliai. Linija yra panaudojama organizuoti ir suskirstyti į kategorijas veiklą.	
Data Objects: Duomenų objektai yra laikomi artefaktais, nes jie neturi jokios tiesioginės įtakos nei sekų srautams, nei pranešimų srautams procesuose, bet jie paskirsto informaciją ką reikia daryti veikloms.	
Group: Veiklų grupavimas, kuris neįtakoja sekų srauto. Grupavimas gali būti naudojamas dokumentacijai ar analizės tikslais. Grupės taip pat gali būti identifikuotos transakcijų veiklose.	
Text Annotations: Tai yra mechanizmas modeliuotojui, leidžiantis įtraukti papildomą informaciją skaitytojui, kuris skaitys BPMN diagramą.	

Sequence Flow: Sekų srautas yra naudojamas parodyti, kad veiklos bus naudojamos procese.	
Association: Asociacija yra naudojama susieti informaciją su srautų objektais. Tekstas ir grafiniai ne srautų objektai gali būti susieti su sekų objektais.	
Message flow: Pranešimo srautas yra naudojamas siųsti pranešimams tarp dviejų dalyvių. BPMN diagramoje du skirtingi baseinai, atstovaus du skirtingus dalyvius.	
Event: Įvykis yra tai kas kartais nutinka per veiklos procesą. Šie įvykiai įtakoja procesų srautus ir dažniausiai turi priežastį ar įtakojantį trigerį įvykiui įvykti. Įvykiai yra tuščiaviduriai rutuliukai leidžiantys vidiniams žymekliams atskirti skirtingus trigerius. Yra trys įvykių rūšys: pradžia, tarpinė ir galinė.	
Activity: veikla yra bendrinis terminas, apibūdinantis, kokį darbą įmonė atlieka. Veikla gali būti atominė ar neatominė. Veiklos, kurios yra proceso modelio dalis yra: procesas, subprocesas, ir užduotis.	
Gateway: vartai yra naudojami siekiant kontroliuoti skirtumus ir konvergenciją sekos srautuose. Tai bus nustatyta šakojimais, atsišakojimais, sujungimais ir takų sujungimais. Vidaus žymekliai parodys elgesio kontrolės rūšis.