KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ TINKLŲ KATEDRA

Vaida Ališauskaitė

Kompiuterių tinklų saugos modelių sudarymas

Magistro darbas

Darbo vadovas
prof. dr. R. Plėštys

Kaunas, 2008

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ TINKLŲ KATEDRA

Vaida Ališauskaitė

Kompiuterių tinklų saugos modelių sudarymas

Magistro darbas

Recenzentas
doc. dr. D. Rubliauskas
2008-01-14

Vadovas
prof. dr. R. Plėštys
2008-01-14

Atliko
IFM-2/4 gr. stud.
Vaida Ališauskaitė
2008-01-14

Kaunas, 2008

TURINYS

1. ĮVADAS 2
2. SAUGAUS INFORMACIJOS PERDAVIMO PROBLEMATIKA 4
   2.1 Kompiuterių tinklų saugos klausimų aktualumas 4
   2.2 Tyrimo sritis ir objektas 5
3. SAUGOS POLITIKOS FORMAVIMO YPATUMAI 6
   3.1 Saugos politiką charakterizuojantis CIA modelis 7
4. PRIEIGOS SAUGOS MODELIŲ ANALIZĖ 10
   4.1 Formalieji prieigos saugos modeliai 11
      4.1.1 Prieigos saugumo valdymo metodai: DAC, MAC ir RBAC 11
   4.2 Bell-LaPadula prieigos saugos modelis 15
   4.3 Biba prieigos saugos modelis 17
   4.4 Clark-Wilson prieigos saugos modelis 19
5. KONCEPCINIAI TINKLO SAUGOS MODELIAI 21
   5.1 Bendras (*generic*) tinklo saugos modelis 21
   5.2 Dviejų lygmenų tinklo saugos modelis 21
   5.3 Keturių lygmenų tinklo saugos modelis 22
   5.4 GRID saugos modelis 24
   5.5 „Gynybos į gylį“ tinklo saugos modelis 25
   5.6 Atakų medžio modelis 26
6. APIBENDRINTO KONCEPCINIO KOMPIUTERIŲ TINKLO SAUGOS MODELIO SUDARYMAS 28
   6.1 Apibendrinto modelio komponentai 28
   6.2 Saugos procesų valdymo modelis 29
      6.2.1 OSI modelio lygmenys 29
      6.2.2 Rizikos valdymo procesas 33
      6.2.3 Organizacijos veiklos saugos modelis 48
7. ĮTARTINŲ ĮVYKIŲ KOMPIUTERIŲ TINKLE APTIKIMO SISTEMOS KŪRIMAS 54
   7.1 Veiklos analizė 54
   7.2 Sistemos projektavimas, realizacija ir diegimas 57
8. ĮTARTINŲ ĮVYKIŲ APTIKIMO SISTEMOS REALIZACIJA 62
   8.1 saugos procesų valdymo kompiuterių tinkluose modelio pritaikymas 62
   8.2 Įtartinus įvykius aptinkančios sistemos eksperimentinis patikrinimas 63
IŠVADOS 65
LITERATŪRA 66
PRIEDAI 69
   I priedas. Straipsnis 69

1. ĮVADAS

Kompiuterių tinklų sauga yra vienas pagrindinių informacijos ir resursų saugumą užtikrinančių faktorių. Organizacijos elektroninėse duomenų bazėse saugomi svarbūs duomenys, serveriuose talpinamos informacinės sistemos, kompiuteriuose saugoma konfidenciali informacija. Nesankcionuoti neautorizuotų vartotojų veiksmai tinkle gali atskleisti slaptą informaciją, negrįžtamai ištrinti duomenis, sugadinti sistemos veikimą ir tokiu būdu sukompromituoti organizacijos veiklą.

Informacijos perdavimui kompiuterių tinklais naudojami įvairūs protokolai, apimantys visus OSI modelio lygmenis. Informacijos saugumas turi būti užtikrinamas kiekviename lygmenyje. Siekiant apsaugoti tinklo resursus (pavyzdžiui, serveriuose talpinamas informacines sistemas, duomenų bazes), turi būti naudojamos ir tarpusavyje derinamos įvairios saugumą didinančios priemonės, padedančios apsisaugoti nuo nepageidaujamų įvykių. Norint apsaugoti kompiuterių tinklą nuo neautorizuotų vartotojų nesankcionuotų veiksmų (įvairių tipų atakų), piktybinių programų (virusų, kirminų), saugumo spragų (programinėje įrangoje, operacinėse sistemose) ir kitų pažeidžiamumų, reikalingas esamų saugos modelių bei juose naudojamų saugumą užtikrinančių metodų tyrimas ir jų praktinis įgyvendinimas.

Siekiant užtikrinti kompiuterių tinklo saugumą, reikia išsiaiškinti kylančius pavojus, pasirinkti tinkamas saugos priemones, nustatyti taškus, kuriuose turi būti įgyvendinami saugos taisyklių reikalavimai ir tuose taškuose įdiegti pasirinktas saugos priemones.

Saugos modeliai padeda suprasti pagrindinius saugos užtikrinimo principus. Juose siūlomi metodai tinka įvairioms sistemoms, nes modeliuose vaizduojami apsaugos reikalaujantys objektai ir saugos strategija, nenurodant konkrečių saugos priemonių ar įrankių.

Magistrinio darbo *tyrimo sritis* – kompiuterių tinklai, o *tyrimo objektai* – įvairių tipų saugos modeliai. Kompiuterių tinklo saugos pagrindą sudaro saugos taisyklės, kurių formalizavimui naudojami modeliai. Nagrinėjant tinklo saugą svarbu atsižvelgti ne vien į techninius, bet ir į organizacinius saugos principus.

Magistrinio *darbo tikslas* – sudaryti apibendrintą kompiuterių tinklo saugos modelį, įvertinantį rizikos valdymą.

Iškeltiems tikslams pasiekti įgyvendinami šie *uždaviniai*:

- aktualių saugos tematikų nustatymas,
- esamų saugos modelių analizė,
- išanalizuotų modelių apibendrinimas,

- naujo modelio kūrimas atsižvelgiant į saugos politiką, kompiuterių tinklo saugos problemas kiekviename OSI lygmenyje, rizikos valdymą ir organizacijos saugos veiklą.
- įtartinų įvykių kompiuterių tinkle aptikimo sistemos, kuri informuotų tinklo administratorių apie kylančias grėsmes, sukūrimas. Informavimas apie potencialias grėsmes suteikia galimybę laiku reaguoti į incidentus. Tokiu būdu sumažinama informacijos saugos praradimo rizika.

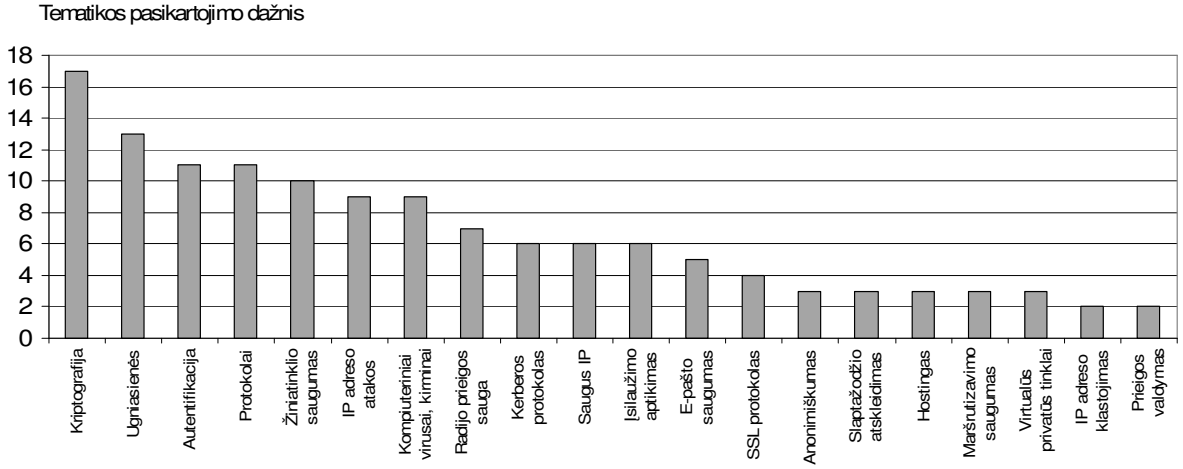
Magistrinio darbo tematika parašytas straipsnis ir perskaitytas pranešimas konferencijoje „Informacinės technologijos 2007“ [16].

2. SAUGAUS INFORMACIJOS PERDAVIMO PROBLEMATIKA

2.1 Kompiuterių tinklų saugos klausimų aktualumas

Kompiuterių tinklų saugos klausimai pastaruoju metu tampa vis aktualesni. Privačioms ir valstybinėms institucijoms, taip pat institucijoms, tiesiogiai susijusioms su saugumu, labai aktualus tinklo saugumo klausimas, nes duomenų vagystės kelia grėsmę jų pačių saugumui ar dėl to yra patiriami dideli finansiniai nuostoliai ir prarandamas verslas visiems laikams. Spartus kompiuterių tinklų vystymasis reikalauja vis daugiau dėmesio skirti duomenų perdavimo saugumui. Saugumo didinimui galima naudoti egzistuojančius tinklo saugos modelius bei kurti naujus.

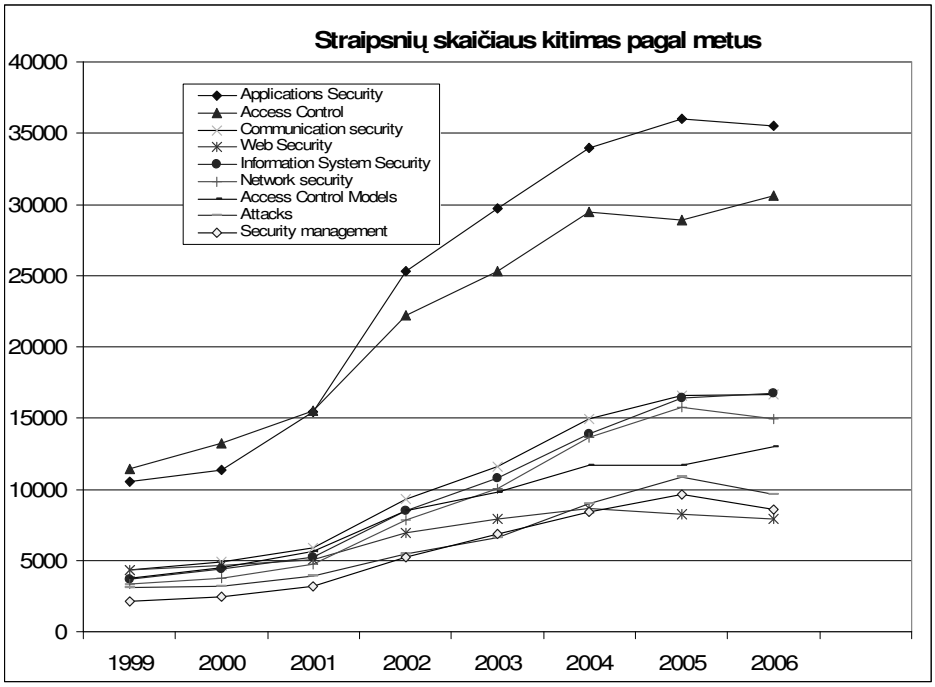
Aktualumui nustatyti ištirtos publikacijos, susijusios su tinklų sauga. Gautas nagrinėjamų tematikų pasiskirstymas pateiktas 1 pav. [16].



1 pav. temų pasiskirstymas

Gauti rezultatai parodo aktualiausias ir svarbiausias kompiuterių tinklų saugos tematikas. Jos gali būti naudojamos sudarant kompiuterių tinklo modelį.

Straipsnių apie tinklų saugą skaičius nuolat didėja. Vidutiniškai nuo 1999 iki 2006 metų metinis mokslinių publikacijų skaičius išaugo 19 kartų. Tačiau duomenys rodo, kad straipsnių apie tinklų saugą skaičius padidėjo daugiausiai – net 26 kartus. Didėjimo tendencija reiškia naujų tinklų saugos problemų atsiradimą ir jų nuolatinį sprendimą.



2 pav. Publikacijų apie tinklų saugą skaičiaus dinamika

Iš 2 pav. matyti, kad prieigos valdymo tematika yra viena aktualiausių saugos srityje ir jos aktualumas vis didėja. Šis klausimas taip pat labai svarbus sudarant saugos modelius.

2.2 Tyrimo sritis ir objektas

Magistrinio darbo sritis yra kompiuterių tinklas.

Darbo objektas – saugos modeliai, kurios galima pritaikyti kompiuterių tinkle saugumo didinimui.

Magistriniame darbe nagrinėjamas prieigos saugos valdymas, informacijos konfidencialumo, vientisumo ir pasiekiamumo užtikrinimas, kompiuterių tinklo saugos spragos ir taikytinos apsaugos priemonės, informacijos praradimo rizikos valdymas, organizacijos saugos veiklos procesai.

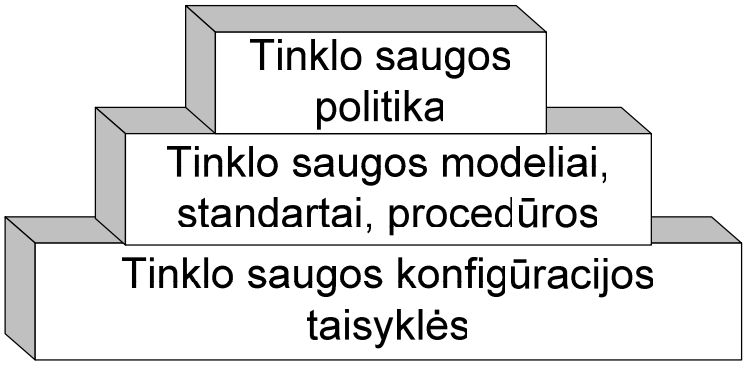
Magistrinio darbo metu siekiama sudaryti kompiuterių tinklo saugos modelį. Tuo tikslu analizuojami egzistuojantys įvairius saugos aspektus apimantys saugos modeliai. Išanalizuotų modelių pagrindu ir įvertinant aktualiausias problemas kuriamas koncepcinis apibendrintas kompiuterių tinklo saugos modelis.

3. SAUGOS POLITIKOS FORMAVIMO YPATUMAI

Saugos politika – tai taisyklių rinkinys, nurodantis, kaip turi būti valdoma, saugoma ar paskirstoma slapta informacija. Saugos politika išvardina tikslus, kurie turi būti pasiekti naudojant įvairias apsaugos priemones. Tokiu būdu saugos politika nurodo reikalaujamą saugos lygį.

Tinklo saugos politikoje taip pat gali būti nurodomi organizacijos poreikiai, tinklo saugumo užtikrinimo reikalavimai, kylančios problemos, įgyvendinti sprendimai, apibrėžiamos tinklo vartotojų teisės, pareigos, atsakomybės, sankcijos už pažeidimus.

Tinklo saugos politika yra abstrakti kategorija. Politikos įgyvendinimui reikalingi saugos modeliai, standartai, procedūros. Jų taikymui naudojamos tinklo įrangos konfigūravimo instrukcijos. Tinklo saugos politikos modelis pateikiamas 3 pav.



3 pav. Tinklo saugos politikos modelis

Tinklo saugos politikos sakinio pavyzdys: visi finansinių operacijų su verslo partneriais metu kompiuterių tinklu perduodami duomenys išliks konfidencialūs ir nebus pažeistas jų vientisumas.

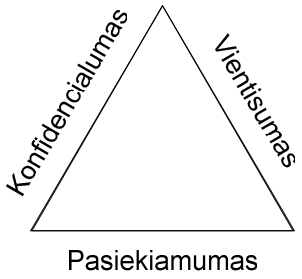
Tinklo saugos modelis, standartai ir procedūros nurodo būdus iškeltam tikslui pasiekti: konfidencialumo tarp tinklų užtikrinimui galima naudoti IPSec pagrindu veikiantį VPN tinklą, kuriame būtų naudojamas 256 bitų AES šifravimas [5].

Tinklo saugos konfigūracijos taisyklės aprašys, kaip turi būti diegiami IPSec, VPN, AES kompiuterių tinkle.

3.1 Saugos politiką charakterizuojantis CIA modelis

CIA modelis (4 pav.) vaizduojamas trikampiu, kurio briaunos arba viršūnės atspindi pagrindines informacijos saugos charakteristikas:

- konfidencialumą (C*onfidentiality*)
- vientisumą (*Integrity*)
- pasiekiamumą (*Availability*)



4 pav. Pagrindines informacijos saugos charakteristikas vaizduojantis. CIA modelis

Siekiant užtikrinti informacijos saugumą, turi būti atsižvelgiama į visas šias charakteristikas. Kiekviena organizacija, priklausomai nuo siekiamų tikslų ir saugumo įgyvendinimo galimybių, gali skirtingai interpretuoti CIA principus ir jų svarbą, tačiau galima suformuluoti bendrus saugumo charakteristikas atitinkančių terminų apibrėžimus [4]:

Konfidencialumas – tai principas, reiškiantis, kad objektai (pvz., bylos, jose saugomi slapti duomenys) nėra atskleisti neautorizuotiems subjektams (vartotojams, programoms, procesams). Konfidencialumas garantuoja, kad duomenys nebuvo sukompromituoti. Konfidencialumo išlaikymas reiškia, kad skaityti ar suprasti slaptą informaciją gali tik patikimi subjektai. Konfidencialumui grėsmę keliančių veiksnių ir apsaugos priemonių pavyzdžiai pateikiami 1 lentelėje.

1 lentelė. Konfidencialumui kylančios grėsmės ir apsaugos priemonės

Grėsmė	**Apsauga**
Tinklo stebėjimas ar šnipinėjimas	Siunčiamų ir saugomų duomenų šifravimas
Slaptažodžių vagystė	Vartotojų švietimas, slaptažodžių šifravimas
Socialinė inžinerija	Vartotojų švietimas, griežtų informacijos atskleidimo taisyklių įtvirtinimas
Viruso patekimas	Antivirusinės sistemos naudojimas
Duomenų vagystė	Tinkamas prieigos valdymas (autentifikacija ir autorizacija)
Informacijos nutekėjimas dėl netinkamai apdorojamų informacinės sistemos klaidų	Saugaus programavimo principų laikymasis

Vientisumas – tai principas, reiškiantis, kad objektai išlieka teisingi (neiškraipyti), o juos pakeisti gali tik autorizuoti subjektai. Siekiama uždrausti neautorizuotas modifikacijas ar

sunaikinti informaciją. Šios savybės išlaikymas užtikrina, kad subjektas A ir subjektas B iš tiesų yra tie, kuo prisistato, o subjekto A pateikti duomenys subjektą B pasiekia nepakitę. Vientisumas gali būti pažeidžiamas tyčia ar atsitiktinai iškraipius ar pakeitus subjekto A subjektui B perduodamą informaciją. Vientisumo užtikrinimui organizacijoje galima taikyti šiuos pagrindinius principus:

- „*Reikia žinoti*“ prieigos principą – vartotojui suteikiama prieiga tik prie tų bylų ar programų, kurių jam būtinai reikia pareigoms atlikti. Tai mažiausiai teisių turintis statusas.
- *Pareigų atskyrimą* – joks vartotojas negali vienas valdyti transakcijos nuo pradžios iki pabaigos. Už visą transakciją turėtų būti atsakingi du ar daugiau vartotojų.
- *Pareigų kaitaliojimą* – darbo atsakomybė turėtų būti periodiškai keičiama, tam kad vartotojui būtų sudėtinga visiškai perimti transakcijos valdymą ar panaudoti ją nesąžiningiems tikslams.

Vientisumui grėsmę keliančių veiksnių ir apsaugos priemonių pavyzdžiai pateikiami 2 lentelėje.

2 lentelė. Vientisumui kylančios grėsmės ir apsaugos priemonės

Grėsmė	**Apsauga**
Įsiterpusio žmogaus ataka (*man-in-the-middle*)	Duomenų šifravimas
IP, MAC adreso klastojimas	Virtualaus privataus tinklo sukūrimas
Neautorizuotas failo turinio modifikavimas	Tinkamas prieigos valdymas (autentifikacija ir autorizacija)
Viruso patekimas	Antivirusinės sistemos naudojimas
Duomenų perdavimo klaida	Patikimos tinklo įrangos naudojimas

Pasiekiamumas – tai principas, reiškiantis, jog autorizuotiems subjektams laiku suteikiama patikima prieiga prie objektų, o sąveikos sparta yra pakankama. Šios savybės išlaikymas vartotojams užtikrina kompiuterių tinklo veikimą ir galimybę pasiekti žiniatinklio resursus reikiamu momentu. Pasiekiamumui grėsmę keliančių veiksnių ir apsaugos priemonių pavyzdžiai pateikiami 3 lentelėje.

3 lentelė. Pasiekiamumui kylančios grėsmės ir apsaugos priemonės

Grėsmė	**Apsauga**
DoS ataka (*Denial of Service*)	Aptarnaujamų užklausų kiekio ir atsakymo laiko ribojimas serverio konfigūracijoje
Viruso patekimas	Antivirusinės sistemos naudojimas
Programinės įrangos klaida	Antrinio (papildomo) serverio naudojimas
Techninės įrangos gedimas	Patikimos tinklo įrangos naudojimas
Elektros dingimas	Energiją išlaikančių priemonių naudojimas
Stichinė nelaimė	Patikimos fizinės apsaugos įdiegimas
Įrangos vagystė	Vartotojų švietimas, fizinės apsaugos priemonių naudojimas (spyna, signalizacija)

Formaliai CIA modelio charakteristikas galima išreikšti tokiais teiginiais:

- Jei turime subjektų rinkinį X ir informaciją I, tai I išlaiko konfidencialumo savybę X atžvilgiu, jeigu nei vienas narys, nepriklausantis X negali gauti informacijos apie I.
- Jei turime subjektų rinkinį X ir informaciją arba resursą I, tai I išlaiko vientisumo savybę X atžvilgiu, jeigu visi X nariai pasitiki I.
- Jei turime subjektų rinkinį X ir resursą I, tai I išlaiko pasiekiamumo savybę X atžvilgiu, jeigu visi X nariai gali pasiekti I.

Saugos charakteristikas įtakoja įvairios grėsmės. Saugos politikos įgyvendinimui naudojamos priemonės pateiktos 4 lentelėje.

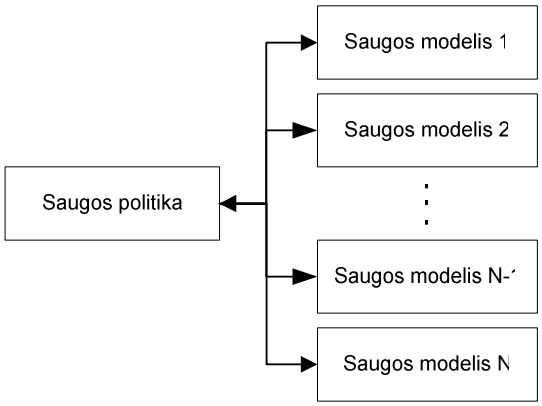
4 lentelė. Tos pačios apsaugos priemonės gali būti taikomos skirtingoms charakteristikoms

Apsaugos priemonė	**Konfidencialumas**	**Vientisumas**	**Pasiekiamumas**
Vartotojų švietimas	+		
Duomenų šifravimas	+	+	
Antivirusinė sistema	+	+	+
Prieigos valdymas	+	+	+
Patikima įranga		+	+

4. PRIEIGOS SAUGOS MODELIŲ ANALIZĖ

Saugos modelis yra skirtas saugos politikos formalizavimui. Modeliu siekiama aiškiai nurodyti kompiuteriams ir jų tinklams taikomas saugos normas arba požiūrį į saugą, kurio reikia laikytis įgyvendinant svarbiausius saugos principus, procesus ir metodikas, t.y. saugos politiką [2].

Saugos modeliai gali būti ne tik saugos politikos formalizavimo priemonė, bet ir saugos politikos kūrimo pagrindas (saugos politika formuojama pagal saugos modelius) (5 pav.).



5 pav. abipusis ryšys tarp saugos politikos ir saugos modelių

Egzistuoja daug saugos modelių, ir kiekvienas iš jų saugos problemą sprendžia vis kitu aspektu [9]. Saugos modelis išreiškia tam tikrus saugos kriterijus. Kompiuterių tinklų modeliuose apibūdinama prieiga prie informacijos ir informacijos srautai kompiuterių sistemoje [8].

Pradiniai saugos modeliai (pvz., Biba, Bell-LaPadula) buvo labiau taikomi atskiram kompiuteriui, bet ne kompiuterių tinklo sistemai. Tokį modelį adaptuojant tinklo sistemai būtina atsižvelgti į atsiradusį ryšį tarp kelių kompiuterių [8]. Kompiuterių tinklo sistemoms sukurti modeliai yra abstraktesni.

Saugos modeliai gali būti:

- formalūs – aprašomi būsenų mašinos veikimo principu
- koncepciniai – abstraktūs, komponentų tarpusavio ryšius parodantys modeliai

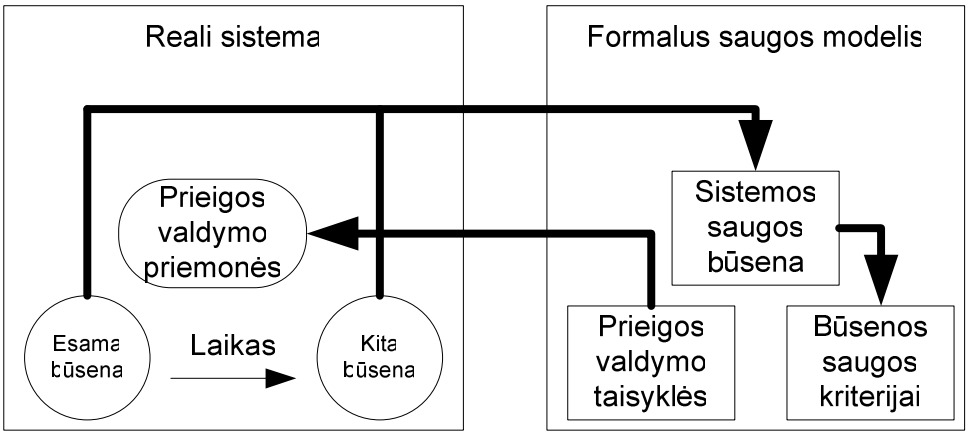
Magistriniame darbe išnagrinėtų saugos modelių klasifikacija pateikiama 5 lentelėje.

5 lentelė. Saugos modelių klasifikacija

Formalus saugos modelis	**Skyrius**	**Koncepcinis saugos modelis**	**Skyrius**
Bell-LaPadula	4.2	CIA	3.1
Biba	4.3	Bendras (*generic*) tinklo saugos modelis	5.1
Clark-Wilson	4.4	Dviejų lygių tinklo saugos modelis	5.2
		Keturių lygių tinklo saugos modelis	5.3
		GRID saugos modelis	5.4
		„Gynybos į gylį“ saugos modelis	5.5
		Atakų medžio modelis	5.6

4.1 Formalieji prieigos saugos modeliai

Formalių saugos modelių tikslas yra apibrėžti autorizuotas ir neautorizuotas arba saugias ir nesaugias sistemos būsenas ir apriboti sistemos perėjimą į neautorizuotą būseną [9]. Ryšys tarp realios sistemos ir formalaus saugos modelio vaizduojamas 6 pav.



6 pav.: ryšys tarp realios sistemos ir formalaus saugos modelio

Formalieji modeliai pagrįsti MAC, DAC arba RBAC prieigos valdymo metodu. Be to, saugos modelis vaizduoja nuo programinės įrangos nepriklausančius su sauga susijusius elementus [9].

4.1.1 Prieigos saugumo valdymo metodai: DAC, MAC ir RBAC

Prieigos saugumo valdymui gali būti naudojami trys skirtingi metodai: DAC, MAC ir RBAC. Šiais metodais grindžiami formalieji saugos modeliai.

4.1.1.1 DAC – diskrecinis prieigos saugos valdymas

DAC (Discretionary Access Control) – diskrecinis prieigos valdymo modelis, kuriame subjekto savininkas nusprendžia, kas gali prieiti prie jo turimo subjekto. DAC dažniausiai įgyvendinamas naudojant ACL (Access Control List) – prieigos valdymo sąrašą. Prieiga ribojama atsižvelgiant į vartotojų teises, gautas autorizacijos metu [13].

4.1.1.2 MAC – imperatyvinis prieigos saugos valdymas

MAC (Mandatroy Access Control) – imperatyvinis prieigos valdymo modelis, kuriame vartotojams suteikiama mažai laisvės sprendžiant, kas gali prieiti prie jų turimų duomenų bylų. MAC modelyje apibrėžiamas nustatytas prieigos valdymo lygis. MAC pagrįstose sistemose prieigos sprendimai priimami atsižvelgiant į subjekto teises ir objekto įslaptinimo lygį. Įslaptinimo lygiams žymėti naudojamos specialios žymės. Objekto lygį gali pakeisti tik administratorius, bet ne objekto savininkas. Sistema pati sprendžia, kaip turi būti dalinamasi duomenimis. Tam tikras teises turintis subjektas galės prieiti prie tam tikro įslaptinimo lygmens objektų atsižvelgiant į „reikia-žinoti“ principą. MAC modelis draudžia rašyti į objektą aukštesnio įslaptinimo lygmens informaciją negu to objekto įslaptinimo lygmuo.
MAC laikomas saugesniu modeliu nei DAC, tačiau jį sudėtingiau konfigūruoti ir įgyvendinti [13].

4.1.1.3 RBAC – rolėmis pagrįstas prieigos saugos valdymas

RBAC (*Role Based Access Control*) – rolėmis pagrįstas autorizuotų vartotojų prieigos valdymo modelis, kuriame sprendimai priimami atsižvelgiant į subjektų roles [4].
RBAC modeli yra MAC ir DAC modelių alternatyva. Prieš jo sukūrimą DAC ir MAC buvo vieninteliai žinomi prieigos valdymo modeliai. Kiekviena prieigos valdymo strategija buvo priskiriama vienam iš šių modelių. Tyrimai parodė, kad RBAC modeliu vaizduojamas prieigos valdymo būdas nei MAC nei DAC. Dėl šios priežasties RBAC yra laikomas lygiaverčiu pirmtakams.

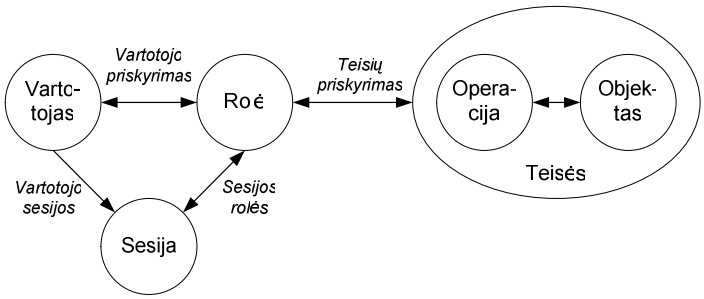
NITS (*National Institute of Standards and Technology*) RBAC modelį skirsto į keturis tipus:

- Pagrindinis RBAC (*core RBAC*)
- Hierarchinis RBAC (*hierarchical RBAC*)
- RBAC modelis su statiniu teisių atskyrimu (*Static Separation of Duty*)
- RBAC modelis su dinaminiu teisių atskyrimu (*Dynamic Separation of Duty*)

Žemiau pateikiami šių tipų apibūdinimai.

Pagrindinis RBAC modelis

7 pav. vaizduojamas RBAC pagrindas. Jį sudaro minimalus elementų ir ryšių rinkinys, galintis pilnai išreikšti rolėmis pagrįstą prieigos valdymą sistemoje.



7 pav. Pagrindinis RBAC saugos modelis

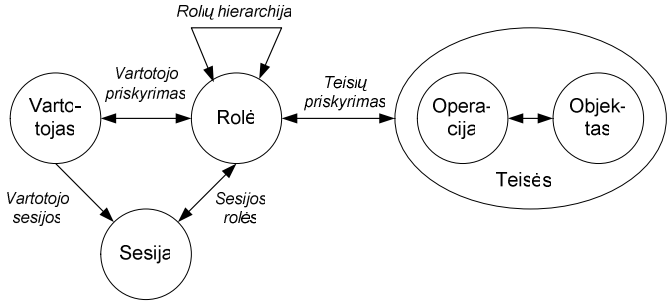
Pagrindinio RBAC modelio komponentai:

- *vartotojas* – žmogus, įrenginys, tinklas, autonominis agentas, kuris naudoja sistemą.
- *rolė* – organizacijoje atliekamo darbo funkcija. Vartotojo priskyrimas rolei reiškia tam tikrą (role apibrėžtą) vadovybės suteiktą atsakomybę darbuotojui.
- *teisė* – tai leidimas atlikti tam tikrą operaciją su vienu ar keliais RBAC modeliu apsaugotų objektų.
- *operacija* – tai vykdomasis programos atvaizdas, kurį iškvietus atliekamos tam tikros vartotojui reikalingos funkcijos.
- *objektas* – tai esybė, kuri turi arba gauna informaciją, pvz., operacinės sistemos failas, duomenų bazės lentelė, eilutė, stulpelis, naudojami sistemos resursai: spausdintuvas, vieta diske, CPU ciklai ir kt.
- RBAC valdomų operacijų ir objektų tipai priklauso nuo aplinkos. Pvz., failų sistemoje operacijos gali būti skaitymas, rašymas ir vykdymas, o duomenų bazių valdymo sistemoje galimos įterpimo, šalinimo, atnaujinimo ir kitos operacijos. Objektais laikomi elementai, kurių prieigai reikalingos role apibrėžtos teisės.
- Vartotojams priskiriamos rolės, o rolėms priskiriamos teisės. Tam naudojami *vartotojo priskyrimo* ir *teisių priskyrimo* ryšiai, kurių kardinalumas „daug su daug“. Tokiu būdu rolė leidžia susieti vartotojo ir teisės esybes vieną su kita ryšiu, kurio kardinalumas yra „daug su daug“. Toks sprendimas suteikia lankstumo ir skaidymo į gylį galimybę atliekant priskyrimus. Pavojus gali kilti dėl ribotos ryšių tarp vartotojui priskirtų rolių kontrolės. Administratorius turi nuspręsti, kokioms rolėms priskirti vartotoją, kad jam būtų suteiktos tik reikalingos teisės (mažiausių teisių principas).

- *Sesija* jungia vartotoją su aktyvuotų rolių rinkiniu. *Sesijos rolės* ryšys parodo sesijos metu aktyvuotas roles, o *vartotojo sesijų* ryšys parodo visas su vartotoju susietas sesijas. Vartotojui taikomos tos teisės, kurios priskirtos vartotojo sesijos metu aktyvuotai rolei.

Hierarchinis RBAC modelis

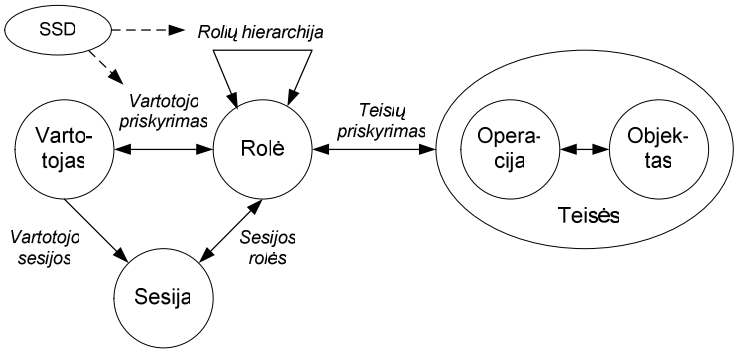
Hierarchinis RBAC modelio pavidalas gaunamas įtraukus rolių hierarchijos principą (8 pav.). Rolių hierarchija leidžia sudaryti organizacijos pavaldumo hierarchiją atitinkančias rolių struktūras. Galimi medžio, apversto medžio ir tinklelio rolių hierarchijos tipai.
Hierarchijos vaizdavimui modelyje naudojamas paveldėjimą reiškiantis ryšys. Paveldimumas apibūdinamas taip: rolė r_1 paveldi rolę r_2, jei visos r_2 teisės yra ir r_1 teisės. Įvairūs autoriai siūlo skirtingus paveldėjimo apibrėžimus ir interpretacijas.



8 pav. Hierarchinis RBAC saugos modelis

RBAC modelis su statiniu teisų atskyrimu

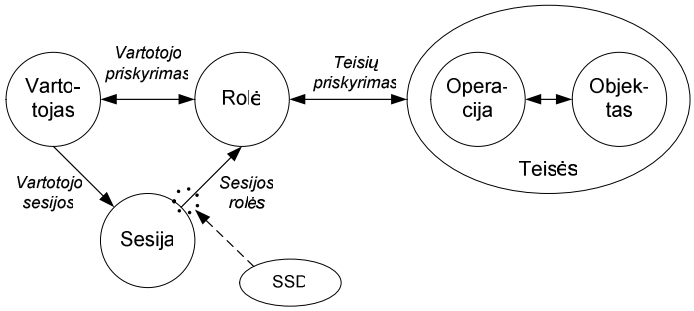
Autorizacijos metu vartotojui gavus konfliktinėms rolėms priskirtas teises RBAC sistemoje gali kilti interesų konfliktas. RBAC su statiniu teisių atskyrimu (SSD) sumažina teisių, kurios gali būti suteiktos vartotojui, skaičių. Tai pasiekiama pritaikius apribojimus vartotojams, kurie gali būti priskirti kelioms grupėms. Apribojimai nustatomi konkrečiam vartotojui, t.y. visoje vartotojo teisių erdvėje (9 pav.).



9 pav. RBAC modelis su statiniu teisių atskyrimu

RBAC modelis su dinaminiu teisų atskyrimu

RBAC su dinaminiu teisių atskyrimu (DSD), kaip ir su SSD, yra skirtas vartotojui priskiriamų teisių ribojimui. DSD nuo SSD skiriasi kontekstu, kuriame šie ribojimai įvesti. DSD atveju apribojimai nustatomi sesijos metu aktyvuojamoms rolėms (10 pav.). Kiekvienas vartotojas gali turėti skirtingo lygio teises atskirais laiko momentais, priklausomai nuo tuo momentu atliekamos rolės. Taip užtikrinama, kad turimos teisės naudojamos tik tuo metu, kai jos yra reikalingos darbui. Norėdamas įgyti kito lygio teises, vartotojas turi prisijungti prie kitos rolės, kuriai jis yra autorizuotas. Tokiu būdu išvengiama interesų konflikto [10].



10 pav. RBAC modelis su dinaminiu teisių atskyrimu

RBAC modelio apibendrinimas:

- RBAC modelis pateikia apibendrintą požiūrį į prieigos valdymą.
- RBAC prieigos modelis lengvai suderinamas su organizacijos struktūra, kadangi vartotojus galima grupuoti pagal pareigas ir valdyti grupių, bet ne atskirų vartotojų prieigą.
- Vartotojų priskyrimas teises apibrėžiančiai grupei yra žymiai paprastesnis negu tų pačių teisių priskyrimas kiekvienam vartotojui atskirai. Dėl šios priežasties RBAC modelis yra plačiai taikomas praktikoje.
- Administratorius turi nuspręsti, kokios operacijos leidžiamos kiekvienai grupei ir kokį RBAC tipą pasirinkti. Sprendimas turi būti gerai apgalvotas.
- RBAC modelis yra patogus didelio masto autorizacijos valdymui.
- RBAC modelis gali būti taikomas duomenų bazių valdyme, saugumo valdyme, tinklo įrenginių operacinėse sistemose.

4.2 Bell-LaPadula prieigos saugos modelis

Bell-LaPadula (BLP) modelis buvo sukurtas remiantis daugialygės saugos modeliu siekiant apsaugoti įslaptintą informaciją. Šis modelis naudojamas Jungtinių Amerikos Valstijų Gynybos ministerijoje (*DoD – Department of Defence*), kurioje informacija pagal slaptumą

klasifikuojama į keturis lygius (labai slaptą (LS), slaptą (S), Konfidencialų (K) ir neįslaptintą (N)).

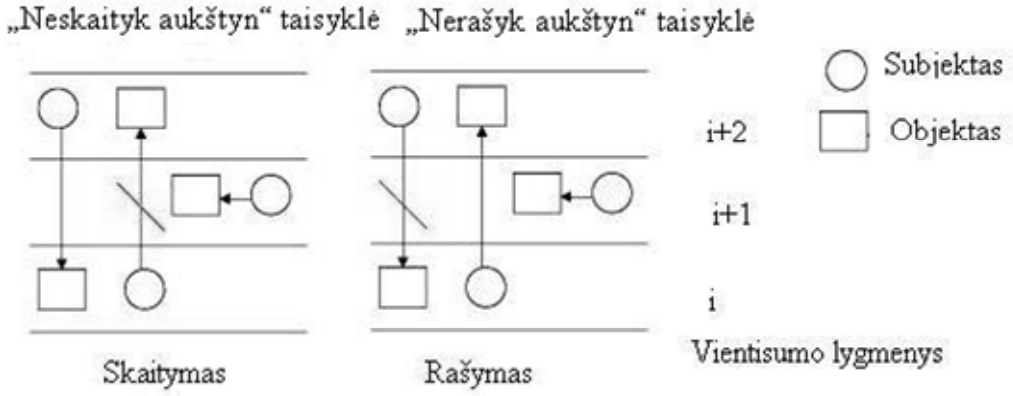
BLP yra sudarytas būsenų automato (state mashine) principu. Būsenų automatą sudaro tam tikras skaičius būsenų su aiškiai apibrėžtais perėjimais tarp bet kurių dviejų būsenų [safeguards].

BLP naudojami MAC, DAC ir tinklelio modeliai. Šiame modelyje dėmesys kreipiamas į konfidencialumą, neatsižvelgiant į kitus CIA modelio komponentus (vientisumą ir pasiekiamumą). Modelio tikslas yra apibrėžti minimalius reikalavimus konfidencialumui, kuriuos privalo patenkinti bet kuri MLS sistema.

BLP modelis pagrįstas dviem pagrindinėmis savybėmis:

1. Paprasta saugos savybė SS (*Simple Secuirty Property*) teigia, kad subjektas gali skaityti tik tame pačiame arba žemesniame slaptumo lygyje esantį objektą. Tai „neskaityk aukštyn“ taisyklė. Pavyzdžiui, prieigą prie konfidencialios informacijos turintis objektas negali perskaityti slaptos informacijos.
2. * (žvaigždutės) saugos savybė teigia, kad subjektas gali rašyti tik į tame pačiame arba aukštesniame slaptumo lygyje esantį objektą. Tai „nerašyk žemyn“ taisyklė. Ji apsaugo nuo galimybės įrašyti slaptą informaciją į konfidencialius dokumentus, kadangi tokiu atveju prieigą prie konfidencialios informacijos turintis subjektas galėtų perskaityti slaptą informaciją.

Šios dvi taisyklės apibrėžia būsenas į kurias gali pereiti sistema. Jokie kiti perėjimai negalimi, nes tik šiomis savybėmis apibrėžtos būsenos yra saugios [12]. BLP modelis grafiškai vaizduojamas 11 pav.:



11 pav.: Bell-LaPadula modelis

Matematiškai BLP modelį galima aprašyti taip:

SUB = {S1, S2, ..., Sm}, baigtinė subjektų aibė

OBJ = {O1, O2, ..., On}, baigtinė objektų aibė

$R \supseteq \{r, w\}$, a baigtinė teisių aibė

D – m×n diskrecinė prieigos matrica, kur $D[i,j] \subseteq R$

M – m×n einamoji prieigos matrica, kur $M[i,j] \subseteq \{r, w\}$

Konfidencialumo žymių tinklelis: $\Lambda = \{\lambda 1, \lambda 2, \ldots, \lambda p\}$

Statinis konfidencialumo žymių priskyrimas: $\lambda: SUB \cup OBJ \rightarrow \Lambda$

M – m×n einamoji matrica, kur:

$r \in M[i,j] \Rightarrow r \in D[i,j] \wedge \lambda(Si) \geq \lambda(Oj)$ - paprasta saugos savybė

$w \in M[i,j] \Rightarrow w \in D[i,j] \wedge \lambda(Si) \leq \lambda(Oj)$ - žvaigždutės savybė

4.3 Biba prieigos saugos modelis

Biba modelis yra analogiškas BLP modeliui, tik jame dėmesys kreipiamas į vientisumą. Jo tikslas yra išspręsti šias pagrindines vientisumo problemas:

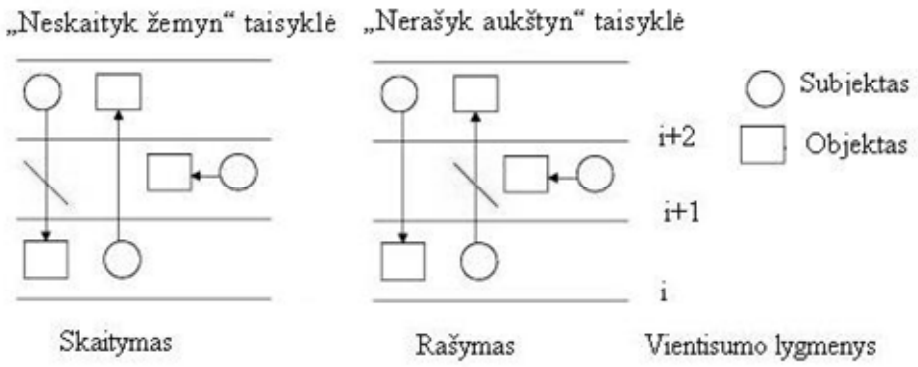
1. apsaugoti objektus nuo neautorizuotų subjektų atliekamų modifikacijų
2. apsaugoti neautorizuotus objektus nuo autorizuotų subjektų atliekamų modifikacijų
3. apsaugoti vidinę ir išorinę objektų nuoseklumą (consistency)

Biba modelis pagrįstas dviem aksiomomis:

1. Paprasto vientisumo aksioma SI (*Simple Integrity Axiom*) teigia, kad subjektas gali skaityti tik tame pačiame arba aukštesniame vientisumo lygyje esantį objektą. Tai „neskaityk žemyn“ taisyklė. Ji reiškia, kad negalima pasitikėti subjektu labiau nei jo perskaityta žemiausio lygio informacija. Subjektui draudžiama skaityti žemesnio vientisumo lygio objektą, kadangi jis subjektą gali suklaidinti.
2. * (žvaigždutės) vientisumo aksioma teigia, kad subjektas gali rašyti tik į tame pačiame arba žemesniame vientisumo lygyje esantį objektą. Tai „nerašyk aukštyn“ taisyklė [skaidrinis]. Ji reiškia, kad negalima pasitikėti subjekto įrašoma informacija labiau negu pačiu subjektu.

Jeigu galima pasitikėti objekto O1 vientisumu, bet negalima pasitikėti objekto O2 vientisumu, tai negalima pasitikėti iš O1 ir O2 sudaryto objekto O vientisumu. Subjektui perskaičius žemesnio vientisumo lygio objektą, sumažėja jo paties vientisumo lygis: jei objekto vientisumą pažymėsime I(O), o subjekto vientisumą I(S), tai subjektui S perskaičius

objektą O, gaunama I(S) = min (I(S), I(O)) [9]. Biba modelio grafinis vaizdavimas pateikiamas 12 pav.



12 pav.: Biba modelis

Matematiškai Biba modelį galima aprašyti taip:

Vientisumo žymių tinklelis: $\Omega = \{\omega 1, \omega 1, ..., \omega 1\}$

Vientisumo žymių priskyrimas: ω: SUB $\cup$ OBJ $\rightarrow \Omega$

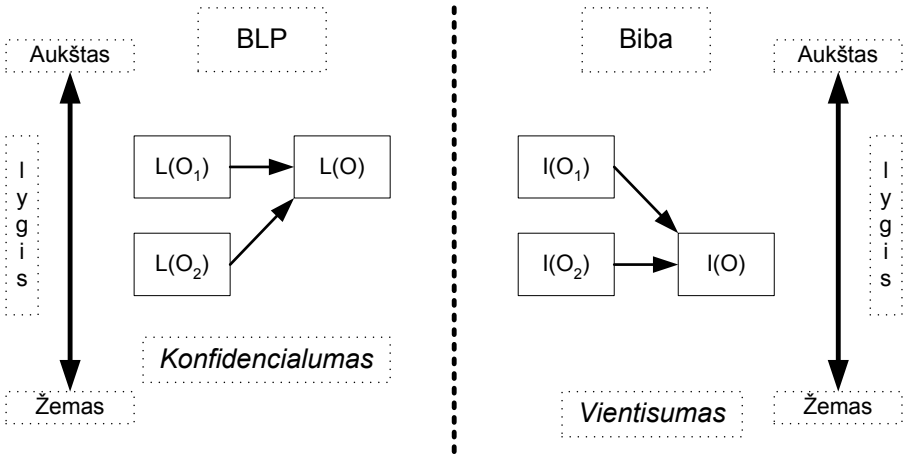
M – m×n einamoji prieigos matrica, kur

$r \in M[i,j] \Rightarrow r \in D[i,j] \wedge \omega(Si) \leq \omega(Oj)$ - paprasta saugos savybė

$w \in M[i,j] \Rightarrow w \in D[i,j] \wedge \omega(Si) \geq \omega(Oj)$ - vientisumo apribojimas

4.3.1.1 Bell-LaPadula ir Biba saugos modelių palyginimas

Bell-LaPadula ir Biba modelių palyginimas pateikiamas 13 pav. Pagrindinis skirtumas yra tas, kad BLP skirtas konfidencialumo, o Biba modelis – vientisumo užtikrinimui.



13 pav.: BLP ir Biba modelių palyginimas

Bell-LaPadula modelio privalumai:

- modelis yra primityvus, todėl gali būti naudojamas įrodymams, susijusiems su įvairių sistemų saugumu.
- efektyviai užtikrina CIA modelio komponentą – konfidencialumą

Bell-LaPadula modelio trūkumai:

- modelis yra per daug primityvus, todėl teikia mažai praktinės naudos
- nekreipiamas dėmesys į likusius du CIA modelio komponentus – vientisumą ir pasiekiamumą [12]

4.4 Clark-Wilson prieigos saugos modelis

Clark-Wilson modelyje, kaip ir Biba modelyje, dėmesys kreipiamas į vientisumo išsaugojimą, tačiau į problemą žvelgiama iš kitos perspektyvos. Vietoj tinklelio saugos naudojamas trijų dalių ryšys – subjektas-programa-objektas. Toks trilypis ryšys reiškia, kad subjektai neturi tiesioginės prieigos prie objektų. Objektai gali būti pasiekiami tik per programas.

Clark-Wilson modelyje vientisumo išsaugojimas pagrįstas dviem principais:

1. Tinkamai suformuotos transakcijos – tai programos, kurios subjektui suteikia prieigą prie objektų. Kitokio būdo objektams pasiekti nėra. Kiekviena programa turi specifinius apribojimus, nurodančius kokie veiksmai su objektu yra leidžiami, kokie draudžiami. Tokiu būdu apribojamos subjekto galimybės. Jeigu programos tinkamai suprojektuotos, tai trilypis ryšys leidžia veiksmingai apsaugoti vientisumą.
2. Pareigų atskyrimas – tai kritinių funkcijų padalijimas į dvi ar daugiau dalių. Toks būdas neleidžia autorizuotiems subjektams atlikti neautorizuotų modifikacijų objektams.

Kartu su jais reikalingas auditas, kuris leidžia sekti vietinių ar išorinių subjektų atliekamas modifikacijas ir prieigą prie objektų.

Clark-Wilson modelis gali būti vadinamas ribotos sąsajos modeliu, nes jame naudojami įslaptinimu pagrįsti apribojimai tam, kad subjektui būtų suteikti tik jam reikalinga ar skirta autorizuota informacija bei funkcijos. Tam tikras subjektas tam tikrame įslaptinimo lygyje matys tam tikrą duomenų rinkinį ir turės prieigą prie tam tikrų funkcijų rinkinio, tuo tarpu kitas subjektas kitame įslaptinimo lygyje matys kitą duomenų rinkinį ir turės prieigą prie kitų funkcijų. [safeguards]

Clark-Wilson modelyje apibrėžti tokie elementai ir procedūros:

1. CDI (Constrained Data Item) – duomenų elementas, kurio vientisumą siekiama apsaugoti
2. UDI (Unconstrained Data Item) – bet koks duomenų elementas, kuris nepriklauso saugos modeliui. Bet koks įvedamas ir nevaliduotas arba išvedamas duomenų elementas laikomas UDI.
3. IVP (Integrity Verification Procedute) – duomenų elementus peržiūrinti ir jų vientisumą patvirtinanti procedūra.
4. TPs (Transformation procedures) – vienintelės procedūros, kurios gali modifikuoti CDI. Ribota prieiga prie CDI per TPs sudaro Clark-Wilson modelio pagrindą [12].

Formalių saugos modelių palyginimas pateikiamas 6 lentelėje:

6 lentelė. Formalių saugos modelių palyginimas

Lyginimo kriterijus	**Bell-LaPadula**	**Biba**	**Clark-Wilson**
Siekiama užtikrinti savybė	konfidencialumas	vientisumas	vientisumas
Saugumo lygmenys	Konfidencialumo	Vientisumo	-
Draudžiami veiksmai	skaitymas aukštyn rašymas žemyn	skaitymas žemyn rašymas aukštyn	nustatomi taisyklėmis
Saugumo būsenų savybės	SS*, stipri *, DS	SS, *	-
Pagrindinės sąvokos	subjektas, objektas, prieigos būdas, saugi būsena. DAC	subjektas, objektas, prieigos būdas, saugi būsena. MAC, DAC	apribotas (neapribotas) duomenų elementas {CDI, UDI}, vientisumą patikrinančios procedūra (IVP), transakcijų procedūra (TP)
Naudojamas MLS formalizavimui	taip	taip	taip
Naudojamas būsenų perėjimas	taip	taip	taip

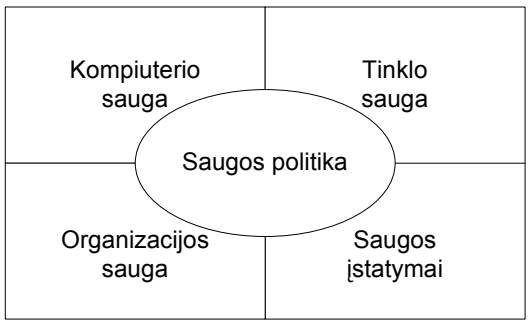
Išanalizuoti Bell-LaPadula, Biba ir Clark-Wilson modeliai yra skirti saugumo užtikrinimui, pagrįsti būsenų perėjimais ir daugiasluoksnėmis saugumo taisyklėmis. Modeliai skiriasi saugumo užtikrinimo metodais.

5. KONCEPCINIAI TINKLO SAUGOS MODELIAI

Koncepciniai tinklo modeliai vaizduoja pagrindinius kompiuterių tinklo saugos principus. Šiame skyriuje pateikiami šeši koncepcinių kompiuterių tinklo saugos modelių pavyzdžiai: bendras tinklo saugos modelis, dviejų ir keturių lygių tinklo saugos modeliai, GRID saugos modelis, „gynybos į gylį“ modelis ir atakų medžio modelis.

5.1 Bendras (*generic*) tinklo saugos modelis

Bendras (*generic*) saugos modelis (14 pav.) gali būti taikomas kompiuterių tinklui ir paskirstytoms sistemoms.



14 pav. Bendras tinklo saugos modelis

Saugos politika yra naudojama saugos tikslų apibrėžimui. Pavyzdžiui, išorinių vartotojų prieigos ribojimas tarpiniame serveryje. Tikslai formuluojami apibendrintai, nenurodant naudotinų priemonių. Jie įgyvendinami taikant įvairias tinklo ar kompiuterio apsaugos priemones. Pvz., kompiuteryje turi veikti saugi operacinė sistema, kad būtų apsaugoti nuo išorinių atakų jame esantys resursai. Informacijos mainai tarp kompiuterių turi būti atliekami naudojant saugius duomenų perdavimo kanalus. Kanalo saugumui didinti gali būti taikomos fizinės apsaugos priemonės, duomenų šifravimo metodai. Be to, turi būti apibrėžtos organizacinės saugos priemonės, kad techniniai saugos metodai būtų tinkamai naudojami. Jei neegzistuoja organizacinė sauga, vartotojai, siekdami efektyvumo, nepaiso saugos priemonių. Teisinės saugos priemonės turi užtikrinti, kad piktavališki kompiuterių tinklo vartotojai bus baudžiami įstatymų numatyta tvarka [13].

5.2 Dviejų lygmenų tinklo saugos modelis

Tinklo saugą galima nagrinėti atskirais lygiais [5]. Kuo įvairesniais aspektais analizuojama aplinka, tuo daugiau galima rasti pažeidžiamumų.

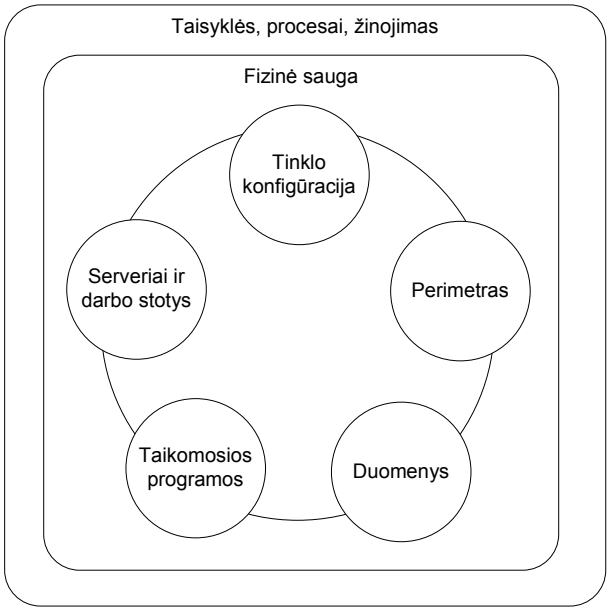
Pirmąjį tinklo saugos lygį sudaro taisyklės, procedūros ir žinojimas. Tinklo apsauga priklauso nuo organizacijos veiklos, vykdomų procesų, saugumui skiriamo dėmesio.
Pagrindiniai veiksniai įtakojantys tinklo saugą yra žmonės ir procesai ir technologijos. Tinklo sauga turi būti formuojama atsižvelgiant į juos visus.

Fizinė apsauga apima fizinę prieigą prie įrangos ir jos naudojimą. Fiziniam saugos lygiui priklauso fiziniai ir virtualūs prieigos būdai, susiję su

- perimetru,
- vidiniu tinklu,
- serveriais ir darbo kompiuteriais,
- taikomosiomis programomis,
- duomenimis.

Virtualūs priklauso prieigos būdai yra tokie, kuriais gali pasinaudoti organizacijos išorėje esantis tinklo vartotojas, pvz. prisijungimas prie žiniatinklio taikomosios programos. Fizinės prieigos pavyzdys – neužrakintos serverių patalpos durys.

Tinklo saugos modelis vaizduojamas 15 pav.

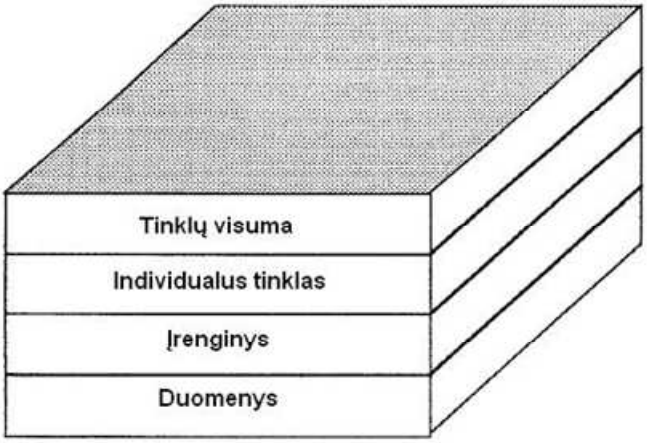


15 pav. Tinklo saugos modelis

5.3 Keturių lygmenų tinklo saugos modelis

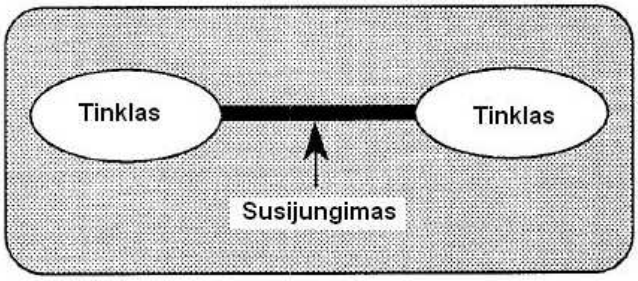
Tinklo elementai, kurie gali būti pasiekiami nesankcionuotu būdu, klasifikuojami hierarchine struktūra. (16 pav.) Kiekviename hierarchiniame lygmenyje kylančios problemos nagrinėjamos tik tame lygmenyje. Bet kokio dydžio tinklą galim traktuoti kaip individualių tinklų rinkinį. Kiekvienas individualus tinklas yra sudarytas iš komutavimo sistemos,

perdavimo sistemos, telekomunikacinių ir kitų sistemų. Nepriklausomai nuo naudojamų įrenginių tipų ir kiekio, kiekviename fiziniame įrenginyje yra talpinami tam tikri duomenys. Taigi, galima sudaryti vertikalų keturių sluoksnių modelį:



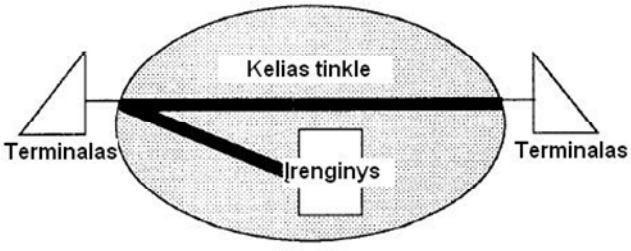
16 pav. Keturių lygmenų tinklo modelis

Tinklų visumos lygmuo. Šiame lygmenyje (17 pav.) nagrinėjamos problemos, susijusios su tarptinkline prieiga. Individualūs tinklai yra fiziškai arba logiškai nepriklausomi. Terminalų konfigūravimo problemos nepriskiriamos tarptinklinėms problemoms ir šiame lygmenyje nesprendžiamos. Tiriant tarptinklines problemas, terminalai laikomi tinklais ir nagrinėjamos tarp jų kylančios saugos grėsmės.



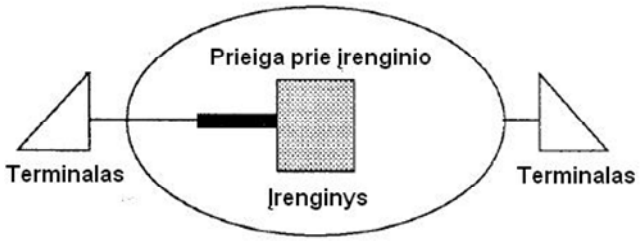
17pav. Tinklų visumos lygmuo

Individualaus tinklo lygmuo. Šiame lygmenyje (18 pav.) nagrinėjami saugos elementai, susiję su prieiga prie individualių tinklų. Didžiausias dėmesys skiriamas tinkle naudojamų kelių saugai.



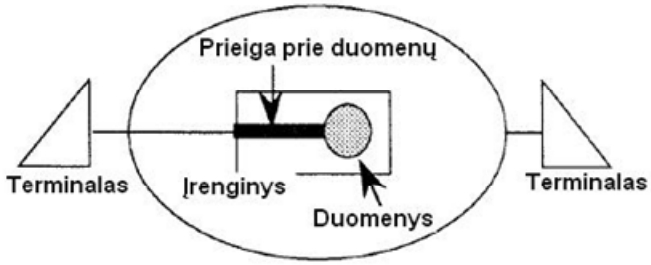
18pav. Individualaus tinklo lygmuo

Įrenginio lygmuo. Šiame lygmenyje (19 pav.) nagrinėjama prieiga prie individualius tinklus skiriančių telekomunikacinių įrenginių. Sprendžiamos prieigos valdymo ir įrenginio perpildymo problemos. Nagrinėjama tik tinklinė prieiga, neatsižvelgiant į galimybę fiziškai prieiti prie įrenginio.



19 pav. Įrenginio lygmuo

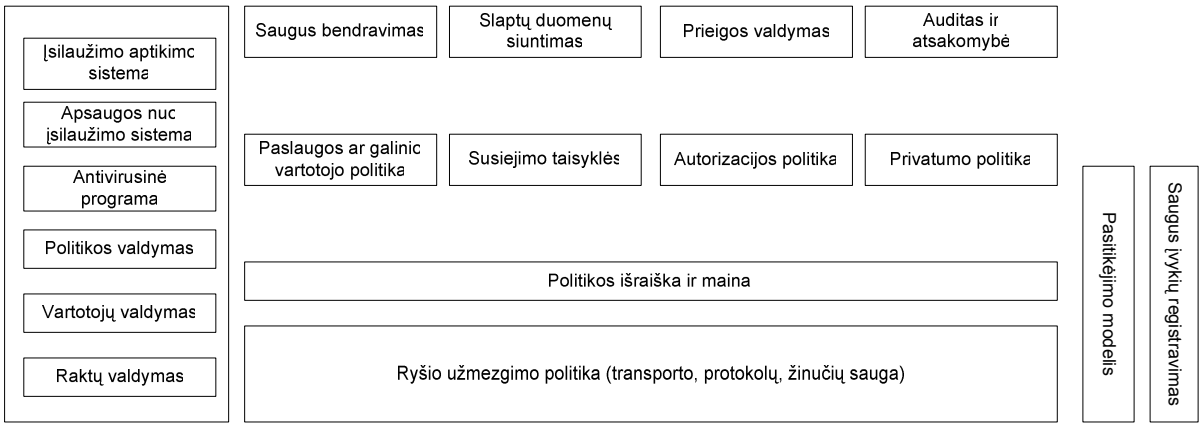
Duomenų lygmuo. Šiame lygmenyje (20 pav.) nagrinėjami saugos elementai, susiję su telekomunikaciniuose įrenginiuose laikomais duomenimis – programomis (pozityviais duomenimis) ir pastoviais (pasyviais) duomenimis. Siekiama uždrausti neteisėtą programų vykdymą, didelis dėmesys skiriamas klaidoms programose.



20 pav. Duomenų lygmuo

5.4 GRID saugos modelis

GRID – tai lokaliųjų skaičiavimų tinklų junginiai. GRID saugos modelis vaizduojamas 21 pav. Ryšio užmezgimo sauga priklauso nuo naudojamų protokolų saugos. Politikos išraiška ir mainai padeda paslaugos tiekėjui ir gavėjui pasirinkti optimalų, tarpusavyje suderinamą protokolą ryšio užmezgimui. Užmezgus ryšį, duomenų perdavimo saugą nulemia saugaus bendravimo politika. GRID aplinką gali sudaryti keletas skirtingų sričių su skirtingomis vartotojų bazėmis, paslaugomis, autorizacijos ir privatumo taisyklėmis. Tapatybės perdavimas užtikrina pasitikėjimą, suderinamumą ir autentikaciją tarp skirtingų GRID sričių. Saugus įvykių registravimas yra esminė GRID saugos modelio dalis, taikoma kitiems modelio komponentams ir yra pagrindas auditą užtikrinančioms paslaugoms [12].



21 pav. GRID saugos modelis

5.5 „Gynybos į gylį“ tinklo saugos modelis

„Gynybos į gylį“ saugos modelis (22 pav.) pagrįstas OSI modelio lygmenimis. „Gynybos į gylį“ esmė yra ta, kad tinklo sauga užtikrinama naudojant įvairias saugos priemonių įvairiuose lygmenyse . Projektuojant saugų tinklą, turi būti atsižvelgiama į kiekviename lygmenyje kylančius pavojus

22 pav. „Gynybos į gylį“ tinklo saugos modelis

Kiekviena organizacija gali detalizuoti ir išplėsti lygmens apibrėžimą priklausomai nuo siekiamų tikslų, poreikių, reikalavimų, prioritetų. Glausti apibūdinimai pateikiami žemiau:

1. **Duomenų saugos lygmuo**. Pažeidžiamumą išnaudojęs atakuotojas gali gauti prieigą prie konfigūracinių bylų, privačių duomenų, slaptos informacijos.
2. **Taikomųjų programų saugos lygmuo**. Pažeidžiamumą išnaudojęs atakuotojas gali gauti neautorizuotą prieigą prie taikomosios programos arba išnaudojęs laivai pasiekiamos taikomosios programos spragas gali prieiti prie tinklo resursų.

3. **Kompiuterio saugos lygmuo**. Atakuotojas gali pasinaudoti kompiuterio teikiamomis paslaugomis, atvirais prievadais, operacinės sistemos ar kitomis pačiame kompiuteryje esančiomis spragomis.
4. **Tinklo saugos lygmuo**. Dėmesys kreipiamas į saugų duomenų perdavimą tinklu organizacijos viduje.
5. **Saugos perimetre lygmuo**. Siekiama užtikrinti sąsajos tarp vidinio tinklo ir globalaus tinklo saugą.
6. **Fizinės saugos lygmuo**. Šiame lygyje atsižvelgiama į galimybę tiesiogiai prieiti prie kompiuterio ar įrenginio.
7. **Žmonės, taisyklės, procesas**. Norint efektyviai įgyvendinti saugos priemones, reikia į socialinius faktorius – žmonių apmokymą, taisyklių sudarymą ir laikymąsi, vykstančių procesų kontroliavimą [10].

Saugos sprendimus organizuojant pagal lygmenis, kylančios grėsmės gali būti eliminuojamos, sušvelninamos arba nukenksminamos. Lygmenų naudojimas ne lygiagrečiai, bet nuosekliai yra reikšmingas principas. Nuoseklus saugos apribojimų taikymas reiškia jų taikymą vienas paskui kitą linijine tvarka. Nuoseklios konfigūracijos dėka kiekviena ataka gali būti peržiūrėta, įvertinta ir sušvelninta. Tai turi atlikti kiekvienas saugos reguliatorius. Nesėkmingas vieno reguliatoriaus veikimas nelemia visos saugos sistemos neefektyvumo. Kai saugos reguliatoriai realizuojami lygiagrečiai, pavojus gali likti nepastebėtas tam tikrame viename kontrolės taške, kuris netraktuoja pavojingo veiksmo kaip piktybinės veiklos. Nuosekli konfigūracija yra labai siaura ir plato, o lygiagreti – labai plati, tačiau paviršutiniška. Naudojant lygmenis atsižvelgiama į tai, kad kompiuterių tinkle yra daug atskirų prieigos taškų ir prievadų. Juose gali būti įgyvendinti skirtingi saugos reguliatoriai bei egzistuoti skirtingi pažeidžiamumai. Norint, kad saugos sprendimas būtų veiksmingas, turi būti užtikrintas vienalaikis skirtingų, bet vienakrypčių priemonių veikimas tarp visų tinklo sistemų. Tokiu būdu sukuriamas viena saugos fronto linija. Atskirų saugos sistemų naudojimas sudaro lygmenimis pagrįstą saugos sprendimą [2].

5.6 Atakų medžio modelis

Atakų medis – tai grafinis medžio struktūros atakų modelis, naudojamas grėsmėms identifikuoti ir analizuoti. Medžio šaknyje nurodomas pagrindinis tikslas, o išsišakojimuose išvardijami tam tikslui pasiekti reikalingi veiksmai (23 pav.). Veiksmus galima jungti naudojant „IR“ bei „ARBA“ operatorius. „IR“ žymi būtinų veiksmų rinkinį atskiroms atakoms įvykdyti. „ARBA“ žymi reikalingų veiksmų alternatyvas. Kiekviename lygyje

veiksmai išskaidomi į mažesnius žingsnius (veiksmus). Į atakų medį galima įtraukti tam tikras žymes. Pvz., prie kiekvieno medžio elemento galima nurodyti, ar veiksmui atlikti reikia specialių įrankių, kokia apsaugos priemonės kaina, kokie galimi nuostoliai ir t. t. Tokiu atveju galima rasti kritinį kelią, kuris parodytų lengviausią būdą atakuoti, silpniausiai apsaugotą tinklo tašką, didžiausius nuostolius atakavus sėkmingai [1]. .

Atakų medį vaizduoti aprašyti grafiniu ir aprašomuoju būdu.

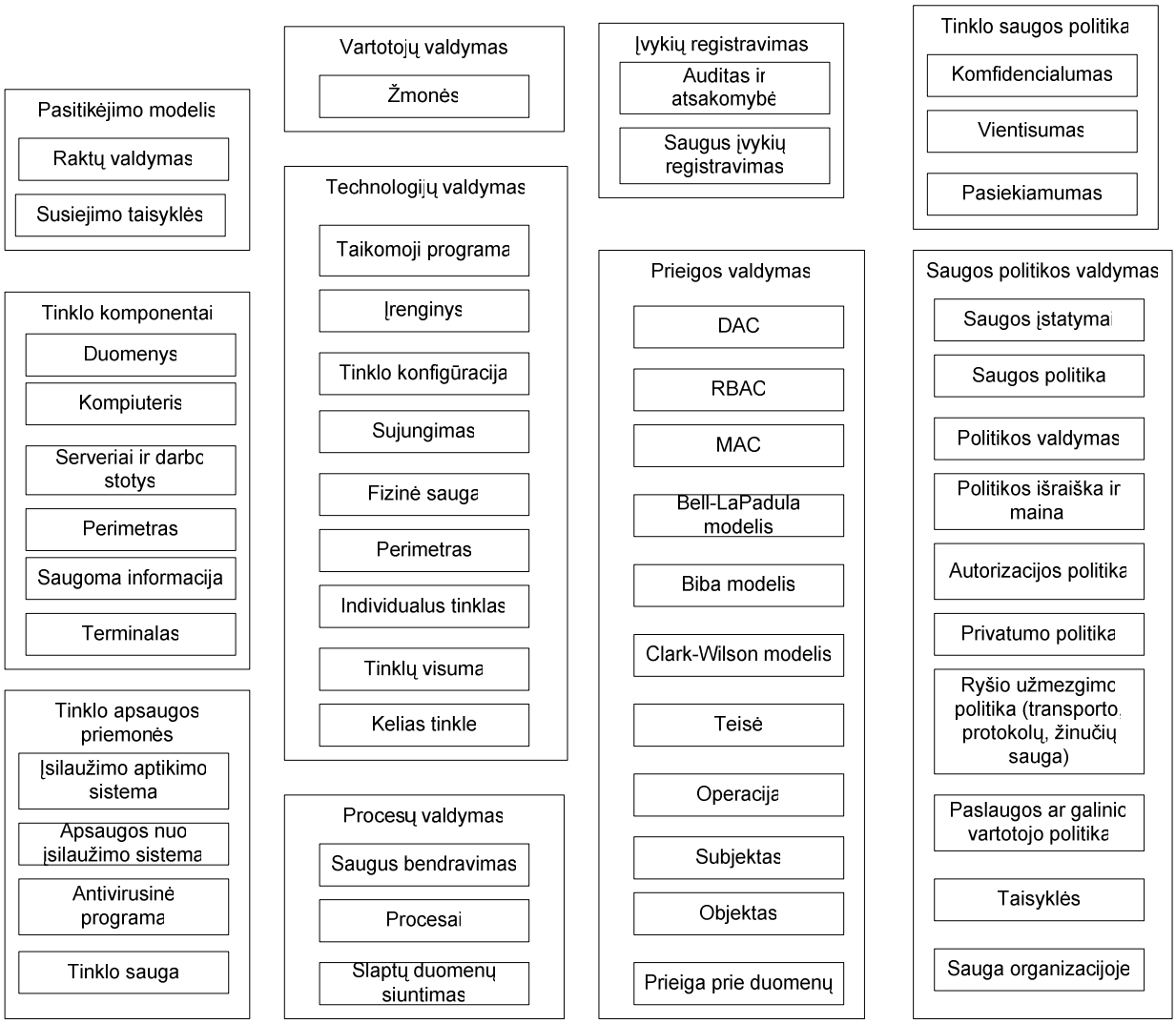
Atakų medžio rezultatas – hierarchinė galimų nepageidaujamų veiksmų struktūra su aktualiomis žymėmis. Atakų medį galima naudoti nustatant tinklo saugos spragų identifikavimą [7].

23 pav. Atakų medžio modelis

6. APIBENDRINTO KONCEPCINIO KOMPIUTERIŲ TINKLO SAUGOS MODELIO SUDARYMAS

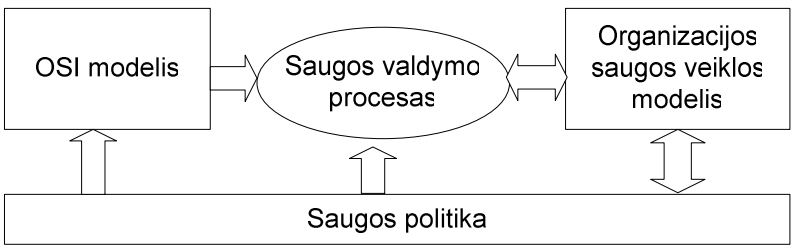
Atlikus įvairių saugos modelių analizę galima išskirti pagrindinius modelių komponentus (24 pav.) ir nustatyti jų tarpusavio ryšius.

6.1 Apibendrinto modelio komponentai



24 pav. Saugos modelių komponentai

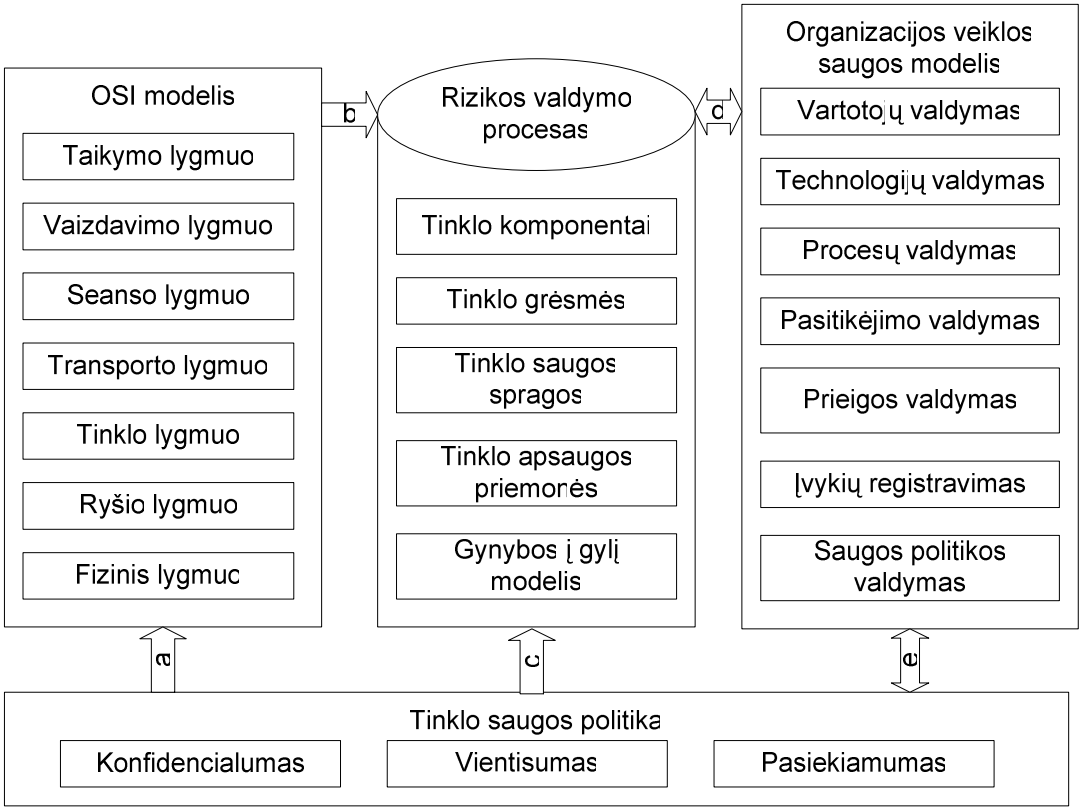
Įvairių modelių komponentus galima apjungti, sugrupuoti, papildyti. Tokiu būdu galima gauti naują saugos modelį. Koncepcinė sudaromo kompiuterių tinklų saugos modelio diagrama vaizduojama 25 pav.



25 pav. Kompiuterių tinklo saugos koncepcinis modelis

6.2 Saugos procesų valdymo modelis

Kompiuterių tinklo sauga valdoma organizacijoje vykstančių procesų metu. Pagal 25 pav. pateiktą koncepciją sudarytas konkretus kompiuterių tinklo saugos modelis informacijos saugos praradimo rizikos valdymo procesą vykdančiai organizacijai (26 pav.).



26 pav. Saugos procesų valdymo kompiuterių tinkluose modelis

6.2.1 OSI modelio lygmenys

OSI modelis – tai abstraktus septynių lygmenų kompiuterių tinklo protokolus aprašantis modelis. Pagal jį kuriami tinklo produktų standartai. OSI modelis aprašo informacijos mainų procesą funkciniame lygyje. Dėl šių priežasties tinklo sauga turi būti nagrinėjama atsižvelgiant į OSI modelį. x skyriuje pateikta tinklo saugos spragų ir apsaugos priemonių pavyzdžių bei nurodyti pagrindiniai protokolai kiekviename lygmenyje.

Kiekvienam OSI modelio lygmeniui būdingos tam tikros saugos problemos (spragos, grėsmės) ir taikytinos apsaugos priemonės. Žemiau pateikti jų pavyzdžiai:

7.2.1. *Fizinis lygmuo*

Problemos:

- Energijos tiekimo nutraukimas

- Techninės įrangos vagystė
- Fizinė žala, duomenų arba techninės įrangos sugadinimas
- Neautorizuoti pakeitimai funkcinėje aplinkoje (resurso pridėjimas arba pašalinimas)
- Fizinis duomenų perdavimo linijos nutraukimas
- Neaptinkamas duomenų perėmimas
- Klavišo paspaudimu ar kitu būdu įvedamų reikšmių registravimas

Apsaugos priemonės:

- Perimetro, patalpos užrakinimas
- Elektroniniai užrakto mechanizmai su įvykių registravimo ir autorizacijos galimybe
- Stebėjimas vaizdo ir garso aparatūra
- PIN kodu ir slaptažodžiais apsaugoti užraktai
- Biometrinės autentifikacijos sistema
- Duomenų saugyklų šifravimas
- Elektromagnetinė apsauga

7.2.2. *Ryšio lygmuo*

Problemos:

- MAC adreso suklastojimas
- Apgaulė naudojant VLAN
- Neautorizuotų subjektų prisijungimo prie bevielio tinklo galimybė
- Silpna autentifikacija ir šifravimas bevieliame tinkle suteikia klaidingą saugumo pojūtį.
- Galimybė sukonfigūruoti komutatorių taip, kad duomenų srautas būtų siunčiamas ne tik į reikiamus, bet į visus VLAN prievadus. Tai suteikia galimybę bet kuriam prie VLAN prijungtam įrenginiui perimti siunčiamus duomenis.

Apsaugos priemonės:

- MAC adresų, naudojamų prievadų filtravimas
- VLAN atsisakymas saugiame tinkle. Patikimi potinkliai turi būti fiziškai izoliuoti. Juose turi galioti griežtos taisyklės. Prieigos ribojimui tarp jų turi būti naudojamos ugniasienės.
- Turi būti įvertinta neautorizuotos prieigos prie bevielio tinklo taikomųjų programų galimybė. Saugumo didinimui turėtų būti naudojamas tinkamas šifravimas, autentifikacija ir MAC adresų filtravimas.

7.2.3. *Tinklo lygmuo*

Problemos:

- Maršruto suklastojimas – klaidingos tinklo topologijos platinimas
- IP adreso suklastojimas – klaidingas piktybinių paketų šaltinio adresas
- Tapatybės ir resurso identifikacijos numerio pažeidžiamumas – pasitikėjimas adresų paskirstymu identifikuojant resursą ir to paties lygio taškus (*peer*) gali būti pavojingas.

Apsaugos priemonės:

- Maršruto politikos valdymas – Naudoti statinį nuo suklastojimo apsaugantį filtrą ir maršrutų filtrą tinklų ribojimosi taškuose
- Piktnaudžiavimo protokolų veikimo savybėmis, pvz, transliavimo mažinimo priemonės

7.2.4. *Transporto lygmuo*

Problemos:

- Netinkamas neapibrėžtų, silpnai apibrėžtų arba neteisėtų sąlygų tvarkymas
- Operacinės sistemos identifikavimas (angl. *fingerprinting*) ar kitos informacijos apie kompiuterį nustatymas dėl skirtingo transporto protokolo panaudojimo
- Netinkamas srauto filtravimas dėl pakartotinio prievadų ar kitų transporto lygmens elementų panaudojimo skirtingoms funkcijoms
- Galimybė perimti srauto valdymą dėl nepakankamo siuntėjo tikrinimo

Apsaugos priemonės:

- Griežtos užkardos taisyklės, kuriose nurodomi ne tik protokolai (pvz. UDP, TCP, ICMP), bet ir jų atributų reikšmės (UDP, TCP prievado numeris, ICMP tipas).
- Būsenos ir paketo turinio (ne tik siuntėją ir gavėją nurodančios antraštės) stebėjimas ugniasienėje.

7.2.5. *Seanso lygmuo*

Problemos:

- silpni ar iš viso netaikomi autentifikacijos metodai
- vartotojo prisijungimo duomenų (pvz., vardo, slaptažodžio, seanso identifikatoriaus) perdavimas atviru tekstu.
- seanso identifikatoriaus suklastojimas arba pasisavinimas (vagystė).
- informacijos atskleidimas nesėkmingos autentifikacijos atveju

- dėl neribojamo nesėkmingų badymų užmegzti seansą skaičius gali būti vykdoma grubios jėgos (*brute force*) ataka prisijungimo duomenų gavimui.

Apsaugos priemonės

- slaptažodžių šifravimas. Duomenų bazėje saugomi ir kompiuterių tinklo perduodami slaptažodžiai turi būti užšifruoti.
- prisijungimo duomenų galiojimo laikotarpio nustatymas
- sesijos identifikatoriaus apsauga naudojant kriptografiją
- nesėkmingų bandymų užmegzti seansą skaičiaus ribojimas laiko atžvilgiu, neužblokuojant prieigos. Tokiu būdu galima išvengti grubios jėgos atakos.

7.2.6. *Vaizdavimo lygmuo*

Problemos:

- netinkamas klaidų apdorojimas
- buferio perpildymo ataka
- pašalinio kodo vykdymas aukos kompiuteryje
- šifravimo algoritmų klaidos

Apsaugos priemonės:

- įvesties reikšmių tikrinimas taikomosiose programose
- saugių šifravimo algoritmų naudojimas
- atsargus kompiuterio valdymą galinčių perimti programų naudojimas

7.2.7. *Taikymo lygmuo*

Problemos:

- atviros konstrukcijos problemos leidžia laisvai naudoti taikomųjų programų resursus nenumatytiems vartotojams.
- paslėptos durys (*backdoor*) ir taikomųjų programų kūrimo klaidos leidžia apeiti standartines apsaugos priemones.
- netinkamos saugos priemonės yra „viskas arba nieko“ pobūdžio, t.y. suteikia poreikius viršijančią arba nepakankamą prieigą.
- per daug sudėtingas taikomųjų programų apsaugos priemonių stengiamasi nediegti arba diegiamos neišsiaiškinus jų veikimo.

Apsaugos priemonės:

- Taikymo lygio prieigos valdymo priemonės, apibrėžiančios ir įgyvendinančios prieigos prie resursų kontrolę. Apsaugos priemonės turi būti detalizuotos ir lengvai

pritaikomos įvairioms taisyklėms, tačiau nesudėtingos. Per didelis sudėtingumas lemia saugos politikos ir įgyvendinimo trūkumus.

- standartų naudojimas, testavimas ir taikomosios programos kodo bei funkcionalumo peržiūrėjimas.
- IDS sistemos, kurios stebi sistemai siunčiamas užklausas ir sistemos veiklą.
- Kompiuterio (*host-based*) užkardos sistemos gali reguliuoti taikomųjų programų duomenų mainus. Tai apsaugo nuo neautorizuoto arba slapto (sunkiai pastebimo) tinklo naudojimo.

6.2.2 Rizikos valdymo procesas

Rizikos valymo procesas – tai organizacijoje atliekama speciali veikla, dėl kurios kinta tinklo saugos lygis. Procesas išreiškia veiklos, būsenos kitimą, todėl modelis tampa dinaminiu. Pavyzdžiui, į rizikos valdymo procesą įeina nuolatinis tinklo stebėjimą, saugos spragų nustatymas, apsaugos priemonių diegimas. Procesas valdo tinklo saugos lygį ir pasikeitimus.

Kompiuterių tinklų rizikos valdymas – tai procesas, kurio metu siekiama suprasti tinklo saugos problemas, sumažint riziką iki priimtino lygio ir valdyti organizacijos tinkle kylančius pavojus. Priimtinumo lygis nustatomas palyginus saugumo spragų išnaudojimo riziką ir apsaugos priemonės įdiegimo kainą. Saugoti turtą nuo labai mažai tikėtinų grėsmių, gali būti finansiškai nenaudinga.

Nors nėra vieningo ir griežtai apibrėžto rizikos valdymo modelio, tačiau galima išskirti pagrindines rizikos valdymo proceso dalis [1], [2]:

1) rizikos vertinimas (analizė ir įvertinimas),
2) rizikos tvarkymas,
3) rizikos kontroliavimas,
4) informavimas apie riziką.

Rizikos valdymo būdai

Rizikos valdymo proceso metu tinklui kylančius pavojus galima nagrinėti keturiais būdais [3]:

1) Proaktyvus (*proactive*) rizikos valdymo būdas. Atliekamas tinklo rizikos planavimas ir prognozavimas, kol dar neišnaudotos saugumo spragos, nekilo neigiamų padarinių. Naudojant proaktyvų valdymo būdą, nuolat atliekami rizikos valdymo proceso veiksmai, iš anksto pasirūpinama apsaugos priemonių, galinčių sumažinti riziką iki priimtino saugumo lygio, taikymu. Laikomasi nuomonės, kad kiekvienas žinomas

tinklo pavojus iš tikrųjų gresia organizacijos tinklui, todėl iš karto ieškoma sprendimo būdų. Taip iš anksto sumažinama saugumo spragų išnaudojimo, įsilaužimo į tinklą, piktybinių programų plitimo galimybė.

2) Interaktyvus (*interactive*) rizikos valdymo būdas. Rizikos problemos nagrinėjamos kiekviename sistemos gyvavimo ciklo etape (planavimo, projektavimo, diegimo, plėtros). Siekiama kiek įmanoma labiau sumažinti tinkle kylančių pavojų tikimybę. Šis būdas tinka tinklo taikomųjų programų rizikos valdymui.
3) Reaktyvus (*reactive*) rizikos valdymo būdas. Saugos problemos sprendžiamos tik pastebėjus neigiamus padarinius. Stengiamasi problemas išspręsti kuo greičiau, sukeliant kiek galima mažiau nepatogumų vartotojams. Rizikos valdymo procesui šis būdas nėra pats geriausias, nes iš anksto neužtikrina tinklo saugumo. Reaktyvus rizikos valdymas tinka tinklo incidentams, kurie jau įvyko, šalinti.
4) Neaktyvus (*inactive*) rizikos valdymo būdas. Neaktyviu rizikos valdymu laikomas visiškas rizikos valdymo proceso nebuvimas, kai iškilusioms tinklo saugos problemoms neskiriama jokio dėmesio.

Norint veiksmingai valdyti kompiuterių tinklo rizikos procesą, labiausiai tinka proaktyvus būdas.

Pagrindinės rizikos valdymo sąvokos

Turtas – tai materialinės ir nematerialinės vertybės, kurias reikia apsaugoti. Tai gali būti tinklo techninė, programinė įranga, sistema, paslauga, resursai, duomenys ir t. t. Turto vertė – tai turto piniginė vertė, priskirta atsižvelgiant į jo kainą ir kitas išlaidas. Į turto vertę įeina kūrimo, palaikymo, administravimo, taisymo ir kiti kaštai. Taip pat turi būti įvertinamos tokios savybės kaip konfidencialumas, produktyvumas ir pan.

Grėsmė – bet koks potencialus įvykis, kuris galėtų sukelti nepageidaujamas pasekmes organizacijai ar turtui. Grėsme laikomas bet koks veiksmas ar veiksmo neatlikimas, kuris gali padaryti žalos, paviešinti, pakeisti, sunaikinti turtą ar užblokuoti prieigą prie jo. Grėsmės ir jų padariniai gali būti įvairaus dydžio, tyčiniai ir netyčiniai. Galimi grėsmių šaltiniai yra žmonės, organizacijos, techninė įranga, tinklai, gamta.

Grėsmės agentas – tai asmuo, programa, techninė įranga ar sistema, kuri tyčia išnaudoja saugumo spragas. Grėsmingas įvykis (*threat event*) – tai atsitiktinis saugumo spragos išnaudojimas (pvz., gaisras, žemės drebėjimas, potvynis, sistemos gedimas (*failure*), žmogiška klaida (dėl žinių stokos ar ignoravimo), elektros tiekimo nutraukimas).

Grėsmės rodikliai – tai ženklai, įspėjantys apie realią grėsmę. Grėsmės rodiklių šaltiniai gali būti užkardos registracijos failai, įsilaužimo aptikimo ir apsaugos sistemos (IDS/IPS) ir kt.
Saugumo spraga – tai apsaugos priemonės ar kontrapriemonės nebuvimas ar jos silpnumas. Saugumo spraga yra klaida, apsirikimas, trūkumas, defektas, jautrumas ar silpnumas, kurį išnaudojus gali būti patiriami nuostoliai, padaroma žala.

Rizika – tai tikimybė, kad bus pasinaudota saugumo spraga ir bus padaryta žalos turtui. Nustatant riziką, turi būti įvertinama tikimybė, galimybė ir atsitiktinumas. Kuo labiau tikėtina grėsmės realizacija, tuo didesnė rizika. Galima užrašyti tokią formulę (1):

$$\text{Rizika} = \text{Turtas} * \text{Grėsmė} * \text{Pažeidžiamumas} \quad (1)$$

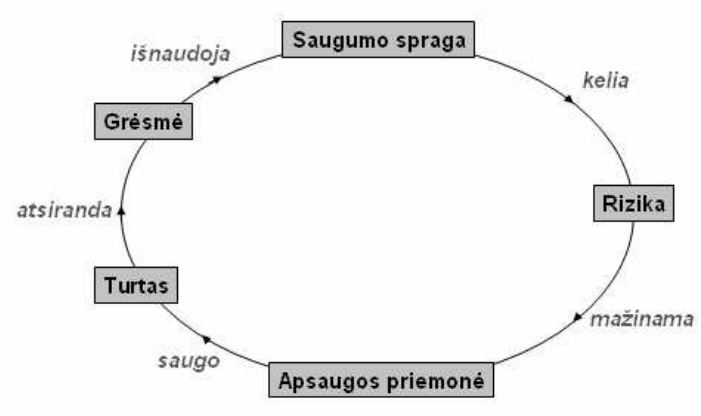
Vieno iš dėmenų sumažinimas lemia rizikos sumažėjimą. Rizikos realizacija reiškia, kad grėsmės agentas ar grėsmės atsitikimas pasinaudojo saugumo spraga ir padarė žalos turtui. Rizikos valdymo proceso tikslas yra neleisti susidaryti grėsmingai situacijai. To pasiekiama pašalinant saugumo spragas ir blokuojant grėsmės agento prieigą prie turto.

Apsaugos priemonė – tai bet koks elementas, kuris pašalina pažeidžiamumą arba apsaugo nuo grėsmės, pvz., programinės įrangos pataisos (*patches*), konfigūracijos pakeitimai, apsaugos darbuotojas ir t. t. Tai yra bet koks grėsmės arba saugumo spragos riziką sumažinantis arba panaikinantis veiksmas, produktas. Apsaugos priemonių naudojimas yra vienintelis rizikos sumažinimo būdas.

Ataka – tai bet koks iš anksto apgalvotas tyčinis bandymas išnaudoti saugumo spragą, siekiant padaryti žalos turtui; saugos taisyklių pažeidimas. Atakuoja grėsmės agentas [4].

Rizikos valdymo elementai ir jų tarpusavio sąsaja

Rizikos valdymo elementai yra turtas, grėsmė, saugumo spraga, rizika, apsaugos priemonė [4]. Organizacijos turtas turi tam tikrą vertę, todėl reikia užtikrinti jo saugą. Turtui gali kilti grėsmė iš įvairių šaltinių. Grėsmės agentas arba nelaimingas atsitikimas gali išnaudoti dėl techninių, programinių ar organizacinių klaidų atsiradusią saugumo spragą. Saugumo spragos išnaudojimo galimybė kelia riziką (pavojų patirti nuostolius). Riziką galima priimti, išvengti, perkelti arba sumažinti. Rizika mažinama apsaugos priemonėmis. Apsaugos priemonių diegimo tikslas yra organizacijos turto saugos užtikrinimas. Rizikos elementų sąsaja vaizduojama 27 pav.



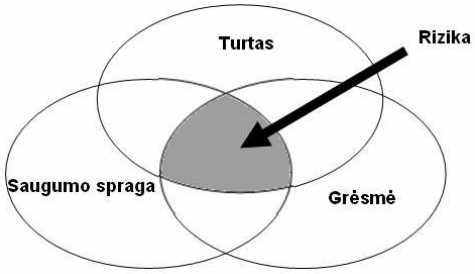
27 pav. Rizikos elementų sąsajos

Rizikos analizė

Rizikos analizei metu apibrėžiamos nagrinėjamos sistemos ribos, identifikuojamas turtas, grėsmės, saugos spragos.

Rizikos identifikavimas

Visus organizacijos aplinkos elementus galima suskirstyti į tris grupes: turtą, grėsmes, saugumo spragas. Kiekviena grupė sudaro baigtinę aibę. Rizika identifikuojama nustačius visų aibių susikirtimo sritį (28 pav.). Bendroji sritis vaizduoja tinklo turtą, kuriam gali būti padaroma žala, jeigu su tinklu susijusi grėsmė išnaudotų tinklo saugumo spragą. Tinklo turtas, tinklo grėsmė ir tinklo rizika – trys riziką aprašančios funkcijos kintamieji, kurie apibrėžiami rizikos identifikavimo metu [6].

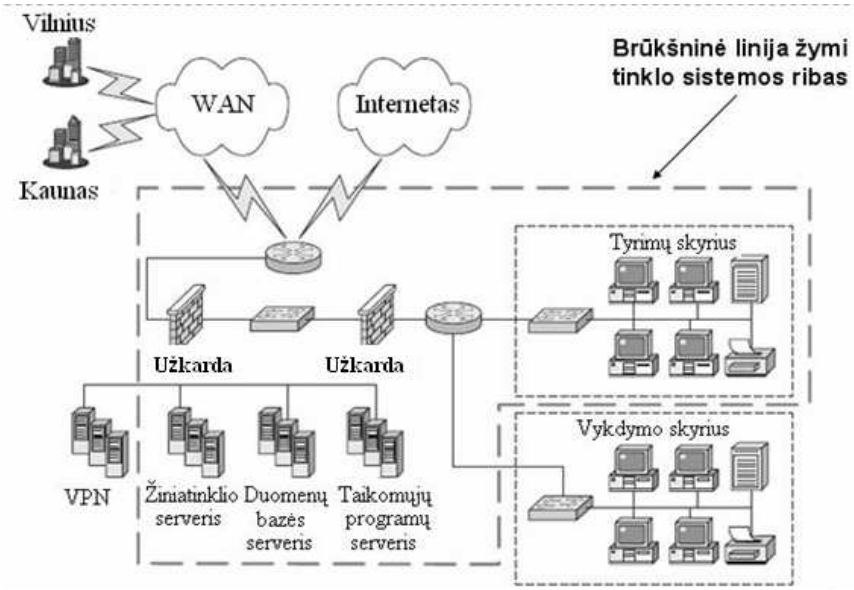


28 pav. Turto saugos modelis

Vertinamos sistemos apimties (ribų) apibrėžimas

Kompiuterių tinklo rizikos vertinimo proceso pradžioje turi būti nustatomos vertinamos sistemos ribos [2]. Tinklo sistemą sudaro procesai, ryšio kanalai, saugyklos ir kiti tinklo elementai, esantys toje pačioje aplinkoje ir priklausantys tam pačiam rizikos valdymo procesui. Ribos apibrėžiamos aiškiai išvardijant vertinimo sričiai priklausančius fizinius ir loginius tinklo elementus. Tai susiaurina vertinimo procesą iki dominančių komponentų, negaištant laiko kitų komponentų analizei ir vertinimui.

Fizinių ribojančių tinklo elementų (29 pav.) pavydžiai: darbo stotys (*workstations*), serveriai, tinklo įrenginiai, specialūs įrenginiai, kabeliai, patalpos. Loginiai ribojantys elementai – tai sistemos, kurios ribose bus atliekamas rizikos vertinimo procesas, funkcijos.



29 pav. Fizinių tinklo elementų ribos apibrėžimas

Tinklo duomenų rinkimas analizei

Duomenų rinkimo tikslas yra stebint (*observe*) ir nagrinėjant (*examine*) tinklo duomenis nustatyti tinklo grėsmes, saugumo spragas, atpažinti kylančius pavojus. Norint atlikti tikslią rizikos analizę, turi būti atsižvelgiama į dabartinius ir istorinius duomenis. Rizikos analizės ir vertinimo duomenys gali būti surenkami naudojant įrankius ir remiantis asmenine specialisto patirtimi. Šie abu būdai papildo vienas kitą ir leidžia gauti tikslesnius rezultatus.

Galimi duomenų apie tinklą rinkimo būdai: tinklo įrangos inventorizacija, tinklo auditas, tinklo skenavimas, įvykių registracijos žurnalų (*log files*) analizė, saugumo spragų įvertinimo įrankiai (*vulnerability assessment tools*), prasiskverbimo tikrinimo įrankiai (*penetration testing tools*), kitų organizacijų patirties ar rekomendacijų naudojimas.

Naudojant įvairius duomenų rinkimo būdus, gaunami tikslesni ir išsamesni rezultatai. Tačiau reikia vengti duomenų pertekliaus, nes gali kilti sunkumų juos sisteminant. Duomenų rinkimo tikslas yra gauti tuos duomenis, kurie yra reikalingi tinklo rizikai valdyti [2].

Saugomo turto analizė

Turto analizės tikslas yra sudaryti kritinio turto sąrašą ir nustatyti kiekvieno turto vertę. Kritinis turto lygis nustatomas pagal turto svarbą ir nuostolio dydį šį turtą praradus . Turtą

galima klasifikuoti pagal įvairius kriterijus, pvz., vietą, atliekamas funkcijas, tipą, jautrumą ir pan. Kiekvieno turto vertė nustatoma atsižvelgiant į šiuos veiksnius:

- duomenų svarbą,
- paskirties svarbą,
- pakeitimo ar atkūrimo sudėtingumą.

Pagrindinės tinklo turto kategorijos [7]:

- duomenys,
- įranga

Grėsmių analizė

Vienas iš rekomenduojamų grėsmių identifikavimo metodų yra jų grupavimas pagal šaltinius (pvz., žmogus: įsilaužėlis, nepatyręs administratorius; gamta: gaisras; technologija: elektros tiekimas, internetas). Sudarius tinklo grėsmių sąrašą, galima planuoti, kokias apsaugos priemones rinktis, pasirūpinti reikiamais finansais ir resursais.

Grėsmių analizei galima naudoti žemiau pateiktą STRIDE klasifikaciją ir x skyrelis aprašytą atakų medžio modelį.

STRIDE modelis

STRIDE modelis suskirsto kompiuterių tinklo grėsmes į šešias stambias klases [5]:

1) Suklastotos tapatybės (***S**poofing identity*). Šiai klasei priklauso atakos, susijusios su nelegalia prieiga prie duomenų ir jų panaudojimu apsimetant kitu subjektu. Tai konfidencialumo pažeidimo atakos. Pvz., slaptažodžių vagystės, IP adreso suklastojimas.
2) Duomenų pakeitimo (***T**ampering with data*). Šiai klasei priklauso atakos, susijusios su piktybiniu duomenų pakeitimu, pažeidžiančiu organizacijos duomenų vientisumą. Pvz., „įsiterpusio žmogaus“ (*man-in-the-middle*) ataka.
3) Neprisipažinimo (***R**epudiation*). Tokia grėsmė kyla tada, kai vartotojas atlieka prieš tinklo resursus nukreiptus piktybinius veiksmus ir vėliau savo veiksmus paneigia, o administratorius neturi nusikaltimui įrodyti reikalingų duomenų. Neprisipažinimas gali pažeisti bet kurį iš trijų CIA modelio principų (konfidencialumą, vientisumą, prieinamumą).
4) Informacijos paskelbimo/atskleidimo (***I**nformation disclosure*). Tai grėsmė, kuri atsiranda tada, kai informacija tampa prieinama asmenims, kurie neturi teisėms prie jos prieiti. Informacijos paskelbimo pavojus iškyla tada, kai tinkle netinkamai priskirtos prieigos teisės (*permission*). Tokiu atveju vartotojas gali perskaityti

konfidencialų failą, tinklo įsilaužėlis gali perskaityti tarp kompiuterių perduodamus duomenis. Šios grėsmės daro įtaką tinklo resursuose saugomų ir perduodamų organizacijos duomenų konfidencialumui.

5) Atkirtimo nuo paslaugos (***D**enial of Service*). DoS atakų tikslas yra sumažinti ar visai panaikinti teisėtiems vartotojams skirtos prieigos prie tinklo resursų galimybę. Šiai klasei priskiriamos ir paskirstytos DoS atakos (DDoS).
6) Teisių pakėlimo (***E**levation of privilege*). Tai atakos, kurių metu administratoriaus teisių neturintis vartotojas jas gauna. Dažniausiai šakninio lygio (*root-level*) prieiga prie visos sistemos gaunama pasinaudojus programinėje įrangoje paliktomis klaidomis. Administratoriaus teises turintis įsilaužėlis gali pakeisti ar visai sunaikinti tinklo resursuose saugomus duomenis.

Tinklo saugumo spragų analizė

Saugumo spragas nagrinėja specialios saugos organizacijos. Atliekant tinklo vertinimą, naudinga atsižvelgti į tų organizacijų pateikiamus duomenis, rekomendacijas.

Grėsminga situacija gali paveikti CIA modelio komponentus (konfidencialumą, vientisumą, prieinamumą). Saugumo spragos klasifikuojamos pagal jų pavojingumo lygį, įtakojamą CIA modelio principą, aptikimo vietą (administraciniame, techniniame, fiziniame lygmenyje).

Dažniausiai saugumo spragų atsiranda dėl šių priežasčių [7]:

- saugos reikalavimų neatitinkančių valdiklių (*controls*),
- prastos konfigūracijos, struktūrinių klaidų,
- naujinimų (*updates*) ir programinius taisinius (*patches-pataisa,* programinis taisinys) trūkumo,
- prasto administracinio valdymo.

Saugumo spragos gali būti techninės, programinės ir organizacinės.

Rekomenduojama pirmiausia pašalinti pavojingiausius saugumo spragas – tas, kurioms panaikinti reikia mažiausiai pastangų. Tai neišsprendžia visų problemų, tačiau sumažina bendrą riziką ir leidžia susikoncentruoti ties daugiau laiko reikalaujančiais sprendimais.

Tinklo saugumo spragų šaltiniai

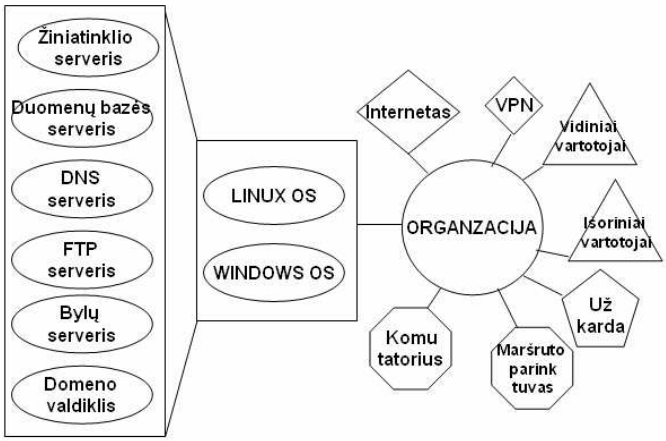
Tinklo saugumo spragų šaltiniai yra [8]:

1. Tinklo protokolai (pvz., TCP/IP, UDP, ICMP, SMTP; galimybė sužinoti TCP protokolo sekos numerį yra saugumo spraga, kuri gali būti išnaudojama siekiant suklastoti tapatybę).
2. Tinklo paslaugos (pvz., elektroninio pašto paslaugos saugumo spragos).

3. Prieigos valdymo stoka (pvz., neužrakintos serverių patalpos durys, neatsakingam tinklo vartotojui suteiktos administratoriaus prieigos teisės).
4. Socialinė inžinerija (pvz., atakuotojas gali sužinoti slaptažodį paskambinęs organizacijos darbuotojui, prisistatęs tinklo administratoriumi ir paaiškinęs, kad nori aktyvuoti naują paslaugą).

Taikinio modelis

Identifikavus saugotiną organizacijos turtą (vertybes) ir grėsmes (panaudojus atakų medį) galima sudaryti taikinio modelį (30 pav.), kuriame būtų sujungti skirtingų rūšių elementai [7]. Taikinio modelis vaizduoja organizaciją, pagrindines paslaugas ir su paslaugų naudojimu susijusius elementus. Į detalizuotą modelį įtraukiami tiek vidinio tinklo, tiek išorinio tinklo vartotojai, serveriuose įdiegtos operacinės sistemos, tinklo įrenginiai, apsaugos priemonės ir kiti su tinklo sauga susiję elementai.



30 pav. Taikinio modelis

Rizikos įvertinimas

Rizikos analizės metu nustatyti rizikos elementai naudojami rizikos įvertinimui. Rizikos įvertinimo rezultatas yra skaitinė išraiška, kuri parodo pavojaus dydį.

Turto įvertinimas

Kiekybinis turto įvertinimas pagrįstas skaitine pinigine turto verte, kurią sudaro:

- turto kaina rinkoje,
- turto pakeitimo kaštai,
- turto teikiamos pajamos.

Kokybiniam turto įvertinimui gali būti taikomi tokie metodai [2]:

- Binarinis turto įvertinimas. Galimi tik du atsakymai: taip arba ne. Tinka pagrindiniam saugotinam turtui identifikuoti (nustatoma, kuriam turtui reikia apsaugos priemonių, kuriam – nereikia).
- Klasifikacija pagrįstas turto įvertinimas. Turtas klasifikuojamas pagal svarbumo lygį, pvz., labai svarbus, vidutiniškai svarbus, mažai svarbus.
- Ranga pagrįstas turto įvertinimas. Kiekvienas turtas įvertinamas likusio turto atžvilgiu. Pvz., turint 20 identifikuoto tinklo turto, kiekvienas jų įvertinamas skaičiumi nuo 1 iki 20.
- Konsensusu pagrįstas įvertinimas. Turtui priskiriama daugumos nuomonę atitinkanti vertė (tinka *Delfi* metodas).

Kiekybinis rizikos įvertinimo metodas

Atliekant kiekybinę rizikos analizę, rizikos komponentams ir galimiems nuostoliams priskiriamos skaitinės vertės. Tai sudėtingas ir ilgas metodas, kuriam atlikti reikalingas vadovas ar koordinatorius.

Kiekybinės rizikos analizės metodo rezultatas – konkrečios procentais išreikštos tikimybės. Jis prasideda materialaus ir nematerialaus turto įvertinimu ir grėsmių identifikavimu. Tada skaičiuojama kiekvieno pavojaus (rizikos) galimybė ir dažnumas. Gauta informacija naudojama kaštų funkcijose, kuriomis įvertinamos apsaugos priemonės [4].

Kiekybinės rizikos analizės kaštų funkcijos:

1. Saugumo spragos veiksnys PV (*Exposure Factor EF*) – procentais išreikšti nuostoliai, kuriuos patirtų bendrovė, jeigu pasinaudojus grėsminga situacija (*realized risk*) būtų sugadintas tam tikras turtas. Dažniausiai tai nesibaigia visišku turto sunaikinimu. Lengvai pakeičiamo turto (pvz., techninės tinklo įrangos) PV reikšmė dažniausiai būna maža, o nepakeičiamo ar firminio turto (pvz., vartotojų duomenų bazės, organizacijos konfidencialios informacijos) gaunama didelė PV reikšmė.
2. Tikėtinas vienkartinis nuostolis TVN (*Single Loss Expectancy SLE*) – tai piniginė vertė, parodanti, kokius nuostolius patirtų organizacija, jeigu tam tikra grėsmė padarytų žalą tam tikram turtui. TVN apskaičiuoti naudojama formulė (2):

$$TVN = TV*PV \quad (2)$$

kur TV – turto vertė piniginiais vienetais. Pvz., jeigu maršruto parinktuvo TV yra 2000 Lt, o PV tam tikrai grėsmei įvertintas 75 %, tai TVN tai grėsmei bus lygus 1500 Lt.

3. Metinis dažnumo rodiklis MDR (*Annualized Rate of Occurance ARO*) – tai skaičius, kuris parodo, kiek kartų per metus gali būti pasinaudota tam tikra grėsminga situacija. MDR reikšmė gali būti lygi 0, jei žinoma, kad pavojinga situacija niekada nebus sėkmingai pasinaudota, arba labai didelė, kai tokiomis situacijomis pasinaudojama dažnai. Šis rodiklis gali būti nustatomas remiantis istoriniais, statistiniais duomenimis arba saugos specialisto spėjimu. Pvz., jeigu į serverių patalpą įsilaužiama kartą per ketverius metus, tai MDR bus lygus 0,25.
4. Tikėtinas metinis nuostolis TMN (*Annualized Loss Expectancy ALE*) – tai piniginė vertė, kuri parodo, kiek gali kainuoti tam tikros išnaudotos grėsmingos situacijos padaryta žala tam tikram turtui per metus. TMN skaičiuojamas pagal formulę (3):

$$TMN = TVN*MDR \quad (3)$$

Apsaugos priemonių kaštų/naudingumo analizė

Kiekvienai grėsmei turi būti priskiriama viena ar daugiau apsaugos priemonių remiantis kaštų/naudingumo įvertinimu [4]. Pirmiausia kiekvienai grėsmei sudaromas apsaugos priemonių sąrašas. Tada visoms apsaugos priemonėms apskaičiuojama turto vertė (TV), į kurią įeina: pirkimo, licencijos, realizacijos, pritaikymo, išlaikymo, administravimo, testavimo, tobulinimo, pokyčių aplinkai ir t. t. kainos.

Norint apskaičiuoti metinius apsaugos kaštus (MAK), reikia iš naujo apskaičiuoti TMN manant, kad apsaugos priemonė yra įdiegta. Tam reikalingos naujos PV ir MDR reikšmės, apskaičiuotos analizuojamai apsaugos priemonei. Metinės apsaugos priemonių išlaidos neturi viršyti tikėtinų metinių kaštų, patirtų dėl turto nuostolio (praradimo). Norint nustatyti, ar verta diegti pasirinktą apsaugos priemonę, naudojama apsaugos vertės AV (*Safeguard Value*) formulė (4):

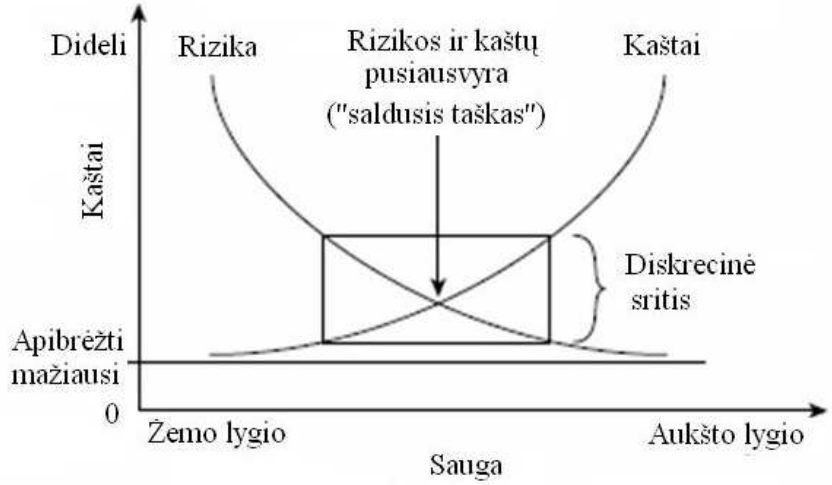
$$AV = (TMN_{prieš} - TMN_{po}) - MAK \quad (4)$$

$TMN_{prieš}$ ir TMN_{po} – TMN prieš apsaugos priemonės įgyvendinimą ir po jo. Jeigu gauta AV reikšmė yra neigiama, tai apsaugos priemonės diegimas finansiniu požiūriu yra nenaudingas. Jeigu AV reikšmė teigiama, tai ji parodo metines sutaupytas lėšas, kurių organizacija gali tikėtis įdiegus apsaugos priemonę.

Saugos ir kaštų balansas

Rizikos valdymo proceso metu svarbu sudaryti pusiausvyrą tarp išlaidų, kurios būtų patiriamos įvykus rizikingai situacijai, ir išlaidų, kurios yra skiriamos reikiamam priemonių, skirtų saugumo spragoms pašalinti, kiekiui įsigyti.

Saugos, kaštų ir rizikos santykis yra toks: didėjant saugos lygiui, didėja kaštų funkcija, o didėjant saugos lygiui ir kaštams, rizikos funkcija mažėja (31 pav.). Kaštų ir rizikos pusiausvyra pasiekiama kaštų ir rizikos funkcijų susikirtimo taške („saldžiajame taške“). Jis parodo optimalius apsaugos priemonėms skirtinus kaštus. Sritis aplink „saldųjį tašką“ vadinama diskrecine (*discretionary*) sritimi [10].



31 pav. Saugos ir kaštų balansas

Kokybinis rizikos įvertinimo metodas

Negalima atlikti visiškos kiekybinės rizikos analizės, nes ne visus elementus įmanoma įvertinti skaičiais. Kai kurie elementai yra kokybiniai, subjektyvūs, nematerialūs. Kokybinės rizikos analizės metodas pagrįstas ne matematiniais skaičiavimais, o subjektyviu vertinimu ir patirtimi. Rizika (tikimybė) išreiškiama žodžiais „maža“, „vidutinė“, „didelė“, arba skaitmenimis 1, 2, 3, kurių reikšmės iš anksto apibrėžtos. Kokybiniam rizikos įvertinimui naudojami įvairūs bendravimu pagrįsti metodai, pvz., proto šturmas, delfi metodas, apklausa ir t. t. Labai svarbu, kad kokybinės rizikos analizės komandą sudarytų tik kompetentingi asmenys [4].

Rizikos įvertinimo proceso metu nustatomas apskaičiuotos rizikos reikšmingumas ją įvertinant pagal tam tikrus kriterijus. Rizikos kriterijais gali būti kaštai, nauda, socialiniai-ekonominiai aspektai ir kiti veiksniai.

Kiekvienos rizikos tikimybė išreiškiama skaitine verte pagal iš anksto sudarytą rizikos klasifikaciją. Turi būti susitarta dėl naudojamų įvertinimo sąvokų. Rizikos klasifikavimo pavyzdys pateikiamas 7 lentelėje:

7 lentelė. Rizikos klasifikavimas

Žodinė reikšmė	Maža	Vidutinė	Didelė
Skaitinė vertė	1	2	3
Apibūdinimas	Poveikis tinklo turtui labai mažas	Patiriami dideli nuostoliai	Poveikis gali būti pražūtingas, padaryta žala nepataisoma

Kiekvienam tinklo turtui sudaroma lentelė 8, kurioje pirmame stulpelyje išvardijamos grėsmės ar saugumo spragos (veiksniai). Kiekvienam veiksniui lentelėje įrašomas rizikos tikimybės įvertinimas (kai netaikomos jokios apsaugos priemonės) ir žalos įvertinimas. Susumavus rezultatus kiekvienoje eilutėje, gaunamas bendras rizikos veiksnio įvertinimas. Šitaip nustatomi rizikos prioritetai.

8 lentelė. Rizikos įvertinimas

Turtas: maršrutizatorius			
Veiksnys	Rizika	Žala	Įvertinimas
Vagystė	1	3	4
Elektros dingimas	2	1	3
Atakuotojo įsilaužimas	2	2	4

Rizika vertinama priimant su rizikos valdymu susijusius sprendimus. Pvz., apsaugos priemonių lentelė gali būti sudaroma tik tiems veiksniams, kurių bendras įvertinimas yra didesnis už 4. Ne tokios pavojingos saugumo spragos ir grėsmės turi būti stebimos [1].

Rizikos tvarkymas

Rizikos tvarkymas – tai procesas, kurio metu pasirenkamos ir įdiegiamos rizikos pobūdį keičiančios priemonės. Atsižvelgiant į rizikos vertinimo proceso metu nustatytus pavojų (rizikos) prioritetus bei apskaičiuotas jų mažinimo išlaidas, numatomas rizikos valdymo procesas: pasirenkama rizikos valdymo strategija, priimami ir vykdomi tinklo saugos didinimo sprendimai.

Galima išskirti keturias rizikos valdymo strategijas [5]:

1. Sumažinimas (*mitigation*). Riziką galima sumažinti iki priimtino lygio naudojant apsaugos priemones, kurios mažina tinklo atakos tikimybę arba jos sukeltą žalą visiškai nepašalinant teikiamos paslaugos (taip daroma ir vengimo atveju). Rizika tinkle gali būti sumažinama taikant apsaugos ir rizikos mažinimo priemones

(*safeguards and conrtols*), pvz., serveriuose diegiant programinius patobulinimus, blokuojant nereikalingas paslaugas, diegiant užkardas.

2. Perkėlimas (*transference*). Riziką galima perkelti trečioms šalimas arba išorės partneriams, kurie turi tam tinkamas priemones ir yra kompetentingi. Sutartyje turi būti aiškiai apibrėžiami visi apsaugos reikalavimai, uždaviniai, priemonės. Pvz., galima apdrausti serverių patalpą nuo gaisro. Ištikus nelaimei bus kompensuojama gaisro padaryta žala. Perkėlimo strategija ne visada yra 100 % teisingas sprendimas, nes daugeliu atvejų atsakomybė už tinklo informacijos saugumą tenka pačiai organizacijai.
3. Vengimas (*avoidance*). Rizikos galima išvengti nustojus teikti rizikingos tinklo paslaugos teikimą. Pvz., norint apsisaugoti nuo virusų plitimo, galima uždrausti elektroninio pašto paslaugą. Daugeliu atvejų tai nėra tinkamas sprendimas. Tinklo saugos specialistas taikydamas saugos priemones turi stengtis užtikrinti teikiamų paslaugų saugumą, bet ne jas apriboti.
4. Priėmimas (*acceptance*). Panaudojus rizikos išvengimo, perkėlimo ir sumažinimo strategijas, vis tiek lieka tam tikrų pavojų, kurių negalima labiau sumažinti nedarant didelio poveikio organizacijos veiklai (pvz., norint apsisaugoti nuo virusų, negalima išjungti elektroninio pašto). Tokiu atveju vienintelis sprendimas yra rizikos priėmimas. Tinklo saugos specialistas turi nuspręsti, kada liekamoji rizika tinkle pasiekia priimtiną lygį.

Nėra vienos taisyklės pasirinkant rizikos valdymo strategiją.

Tinklo apsaugos priemonių klasifikacija

Apsaugos priemonė (*safeguard*) – tai turtui kylančią riziką mažinantis metodas, veikla ar technologija.

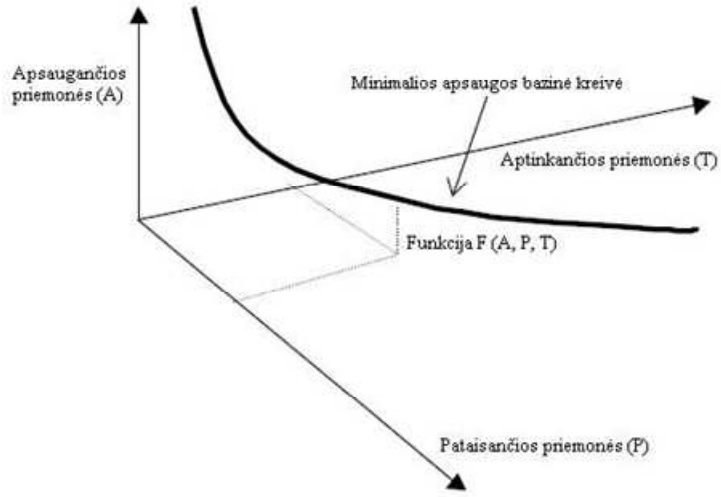
Apsaugos priemonės skirstomos į tris kategorijas [2]:

- apsaugančias (*preventive*) – skirtas nepageidaujamiems įvykiams blokuoti prieš jiems įvykstant. Pavyzdžiai: prieigos valdymo sąrašas, saugos mokymas;
- pataisančias (*corrective*) – skirtas nepageidaujamų įvykių padarytai žalai atitaisyti. Pavyzdžiai: apsaugos darbuotojai, bylų atstatymo priemonės (*file recovery*);
- aptinkančias (*detective*) – pagal tam tiktas sąlygas identifikuojančias jau įvykusius nepageidaujamus įvykius Pavyzdžiai: įvykių registracijos failai (*log files*), IDS.

Minimalios apsaugos bazinė kreivė

Visoms sudėtingoms sistemoms galima pritaikyti daug įvairių apsaugos, pataisymo ir aptikimo priemonių, kurios užtikrins tam tikrą saugos lygį. Kiekvienas minimalios apsaugos bazinės kreivės taškas vaizduoja saugos lygį, gautą naudojant skirtingas apsaugos, pataisymo ir aptikimo priemonių kombinacijas. Iš 32 pav. vaizduojamos minimalios apsaugos bazinės kreivės galima padaryti tokias išvadas:

- Bendra saugos kaina yra visų apsaugos, pataisymo ir aptikimo priemonių suma.
- Galima rasti kelis apsaugos, pataisymo ir aptikimo priemonių derinius, kurie duotų panašų rezultatą.
- Riboto dydžio biudžetas ir riboti resursai lemia apgalvotą apsaugos priemonių derinio pasirinkimą, o tai lemia saugos veiksmingumą [6].



32 pav. Minimalios apsaugos bazinė kreivė

Liekamoji rizika

Liekamoji rizika (*residual risk*) – tai rizika:

1) kuri išlieka įgyvendinus rekomenduojamas apsaugos priemones;
2) kurios nenorima sumažinti diegiant apsaugos priemones (pasirinkta priėmimo strategija).

Bendroji rizika (*total risk*) – tai rizika, su kuria įmonė susidurtų, jei nebūtų įgyvendintos jokios saugos priemonės. Bendrosios rizikos formulė yra tokia:

Bendroji_rizika=grėsmės*saugumo spragos*turto_vertė (5)

Skirtumas tarp bendrosios ir liekamosios rizikos vadinamas kontroliavimo skirtumu (*controls gap*). Kontroliavimo skirtumas išreiškia riziką, kuri buvo sumažinta įgyvendinant apsaugos priemones. Liekamoji rizika gali būti apskaičiuota taip [4]:

Liekamoji_rizika=bendroji_rizika-kontroliavimo_skirtumas (6)

Reikia pastebėti, kad negali būti 0 % liekamosios rizikos arba 100 % saugos.

Rizikos priežiūra

Rizikos priežiūros proceso metu atliekama [9]:

1. Apsaugos priemonių tikrinimas (testavimas). Apsaugos priemonės nustatomos rizikos tvarkymo proceso metu. Rizikos kontroliavimo etape patikrinamas jų veikimas ir veiksmingumas. Apsaugos priemonių testavimas atliekamas dažniau negu tinklo rizikos vertinimas.
2. Stebėjimas. Stebimas rizikos mažinimo sprendimų įgyvendinimo procesas ir įvertinamas progresas. Taip pat iš naujo renkami tinklo duomenys. Gali būti naudojami tie patys duomenų rinkimo būdai, kaip ir vertinimo proceso pradžioje. Pagal gautus rodiklius nustatomas naujų pavojų atsiradimo galimybė, buvusių pavojų sumažinimo tikimybė. Tinklo stebėjimas ir naujų duomenų peržiūra turi būti atliekami periodiškai.
3. Priežiūra. Apsaugos priemonių tikrinimo ir stebėjimo rezultatai lemia rizikos tvarkymo sprendimus dėl tolesnio planų vykdymo. Jeigu reikia, ankstesni planai gali būti keičiami, atsižvelgiant į iškilusius naujus poreikius. Priežiūra turi užtikrinti sėkmingą rizikos mažinimą.

Saugos pokyčio kreivė

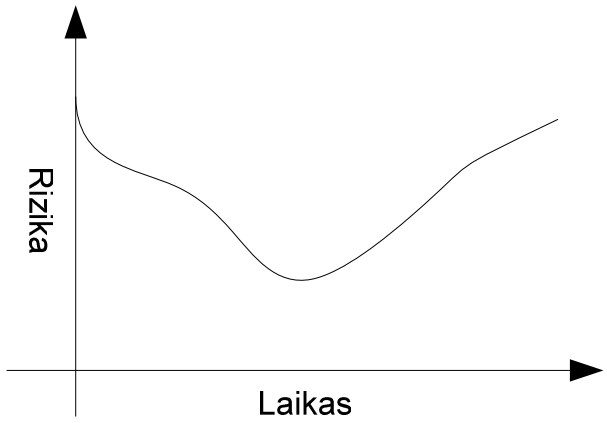
Saugos pokyčio kreivė vaizduoja rizikos pokytį laikui bėgant (33 pav.) [2]. Pradėjus taikyti apsaugos priemones, tinklo rizika sumažėja. Tačiau laikui bėgant keičiasi grėsmės ir aplinka, todėl atsiranda naujų pavojų ir kreivė kyla aukštyn.

Riziką mažinančios saugumo priemonės gali būti:

- vartotojų mokymas;
- saugos taisyklių kūrimas ir įgyvendinimas;
- techninės ir programinės tinklo įrangos stiprinimas (*hardening*) saugos aspektu;
- saugos pataisų (*patches*) diegimas;
- antivirusinis naujinimas;
- incidentų valdymas.

Riziką didinantys ir aplinkos bei grėsmių pasikeitimą lemiantys veiksniai gali būti:

- naujos saugumo spragas išnaudojančios programos;
- naujos tinklo funkcijos;
- nauja tvarka (*regulations*);
- naujas personalas.



33 pav. Saugos pokyčio kreivė

6.2.3 Organizacijos veiklos saugos modelis

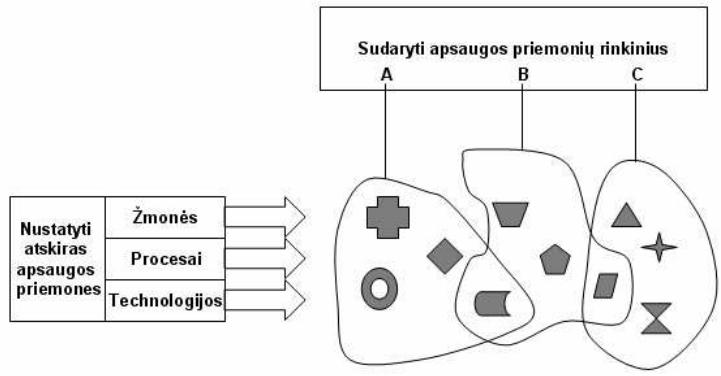
Organizacijos saugos veiklos modelis, susijęs su organizacijos tikslais ir darbo principais, kurie turi įtakos informacijos mainų saugumui. Organizacijos veiklos saugos modelis vaizduoja organizacijos veiklos sritis, kurios turi įtakos informacijos saugumui. Informacijos perdavimo saugumas priklauso ne tik nuo techninių, bet ir nuo organizacinių aplinkybių. Šioje modelio dalyje įvertinamas žmonių, technologijų ir procesų valdymas, bendravimas su išoriniais partneriais, prieigos prie saugomų objektų valdymas, įvykių registravimas ir taisyklių (politikos) kūrimas bei tobulinimas. Kiekvienas komponentas plačiau aptariamas žemiau pateiktuose poskyriuose.

Vartotojų, technologijų ir procesų valdymas

Tinklui reikalingos apsaugos priemonės gali būti skirstomos į tris rūšis:

1. Susijusias su žmonėmis, pvz., patikimi vartotojai, kvalifikuoti administratoriai.
2. Susijusias su procesais, pvz., apmokymų organizavimas, reguliarus tinklo auditas.
3. Susijusias su technologijomis, pvz., dvigubą (*two factor*) autentifikacija, prieigos valdymo sąrašai (ACL), įvairių rūšių užkardos, įsilaužimo aptikimo ir apsaugos sistemos, VPN, duomenų šifravimas ir t. t.

Kiekvienai grėsmei nustačius veiksmingas apsaugos priemones galima sudaryti apsaugos priemonių rinkinius. Sprendimų rinkinį turi sudaryti viena kitą papildančios ir tarpusavyje suderinamos priemonės, kuriomis būtų galima sumažinti tinklo riziką iki priimtino lygio. Atsižvelgiant į kaštus, veiksmingumą ir rizikos priimtinumą, iš sprendimų rinkinių pasirenkamos optimalios priemonės (34 pav.) [2].



34 pav. Tinklo apsaugos priemonių rinkiniai

Vartotojų informavimas ir mokymo būdai

Norint sėkmingai įgyvendinti su sauga susijusius sprendimus, būtini vartotojų elgesio pokyčiai. Vartotojų veiksmai turi keistis taip, kad būtų tenkinami saugos standartai, principai, saugos taisyklėse nurodytos procedūros. Tam reikia mokyti vartotojus. Galima išskirti tris mokymo lygius [4]:

1. Įsisąmoninimas. Tikslas – kad vartotojai pripažintų saugos taisykles ir jų laikytųsi. Įsisąmoninti padeda skelbimai, straipsniai, pranešimai, bendravimas. Šis lygis turėtų būti privalomas visiems tinklo vartotojams. Vartotojų sąmoningumo didinimo procesas turėtų būti nenutrūkstamas.

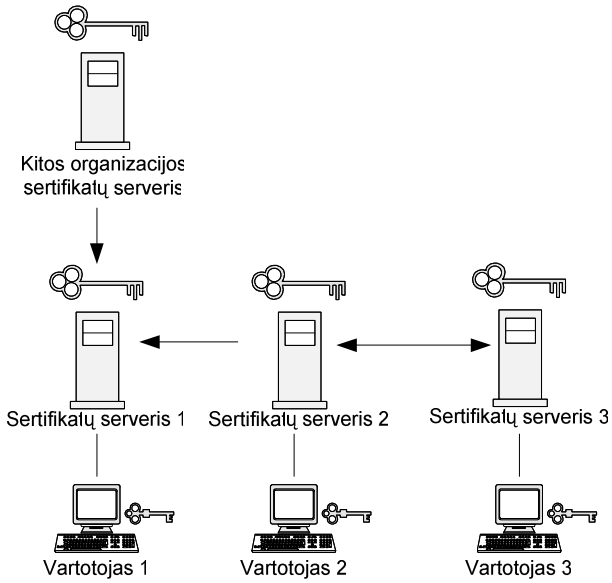
2. Kursai, treniravimas. Tai darbuotojų mokymas atlikti savo pareigas taip, kad nepažeistų saugos reikalavimų. Pvz., naujam vartotojui prieiga prie tinklo resursų turėtų būti suteikiama tik specialiai apmokius. Kursai turėtų būti organizuojami periodiškai.

3. Ugdymas. Tai nuodugnesnis ir daugiau pastangų reikalaujantis mokymas. Dažniausiai tai apima daugiau nei reikia pareigoms atlikti. Ugdymas taikomas saugos sertifikatų siekiantiems specialistams.

Pasitikėjimo valdymas

Organizacijoje galima nustatyti pasitikėjimo ryšius tarp skyrių, serverių, vartotojų, tinklų 35 pav. vaizduojamas vartotojų autentifikavimo pasitikėjimo modelis naudojant sertifikatus.

Kiekvienas organizacijos skyrius turi savo sertifikatų tarnybą. Kiekvieno skyriaus vartotojų prieigai prie kito skyriaus resursų naudojami sertifikatai. Tarp skyrių sertifikatų serverių galimas vienpusis arba dvipusis ryšys. Pagal x pav. vartotojas 2 ir 3 gali naudotis vienas kito skyrių resursais. Vartotojas 1 negali naudotis kitų skyrių resursais, tačiau jo skyriaus resursais gali naudotis Vartotojas 2 bei kitos organizacijos vartotojai.

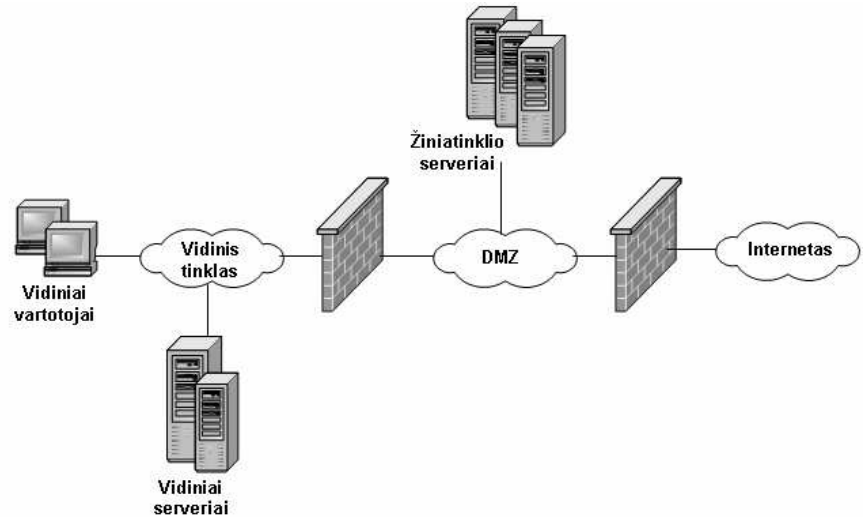


35 pav. pasitikėjimo ryšių nustatymas

Prieigos saugos valdymas

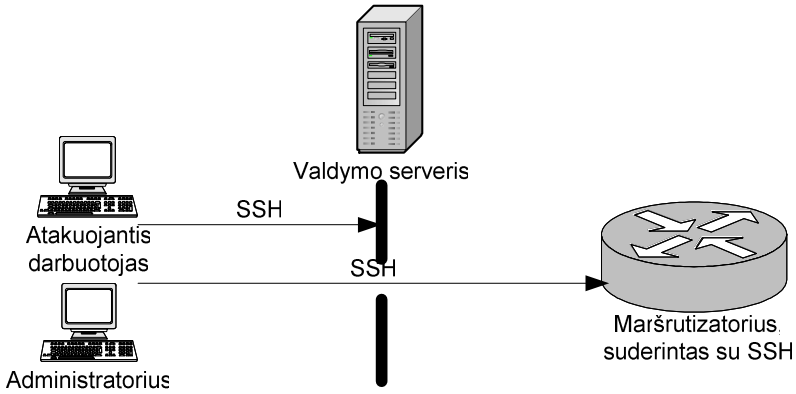
Prieigos saugos valdymas yra vienas iš pagrindinių saugos modelio tikslų. Kompiuterių tinkle vartotojų prieigos saugos valdymui naudojamos ugniasienės (36 pav.), autentifikacija (37 pav.) ir autorizacija.

Norint apsaugoti serverius nuo atakų, rekomenduojama juos izoliuoti atskiruose tinkluose. Naudojant ugniasienes, sukuriama demilitarizuotoji zona (DMZ). Viena ugniasienė įdiegiama prieš internetą, kita – prieš vidinį tinklą. Tokiu būdu suformuojama neutrali sritis, atskirianti grėsmes (atakas) nuo saugomo turto (duomenų, darbo stočių, tik organizacijos viduje naudojamų serverių). Tarp šių dviejų ugniasienių diegiami žiniatinklio, elektroninio pašto bei kiti internetu pasiekiami serveriai. Ugniasienėmis sukurtos demilitarizuotos zonos tikslas yra riboti prieigą prie internetu pasiekiamų serverių ir teikti papildomą apsaugą vidiniam tinklui, tuo atveju, jeigu būtų sukompromituoti internetu pasiekiami serveriai. Demilitarizuotoji zona vaizduojama 36 pav.



36 pav. Demilitarizuotoji zona gaunama naudojant ugniasienes

Prieigos saugumo didinimui gali būti naudojama prieigos valdymo serveris ir dviejų lygių autentifikacija. 37 pav. vaizduojamas neautorizuoto darbuotojo ir administratoriaus SSH prisijungimų prie maršrutizatoriaus bandymai. Valdymo serveris apsaugo maršrutizatorių nuo tiesioginės neautorizuotų vartotojų prieigos. Dviejų lygių autentifikacija apsaugo nuo netesėto prisijungimo net ir tuo atveju, jeigu paviešintas administratoriaus slaptažodis. Atakuojančio darbuotojo prisijungimas prie maršrutizatoriaus būtų neįmanomas be viešo rakto, kuris saugomas administratoriaus kompiuteryje.



37 pav. Autentifikacijos valdymas

Autorizacijos metu autentifikuotiems vartotojams priskiriamos teisės. Trys pagrindiniai prieigos saugos valdymo būdai x skyriuje išanalizuoti MAC, DAC ir RBAC. Šie metodai gali būti derinami tarpusavyje.

Įvykių registravimas

Sėkmingam tinklo administravimui ir saugos didinimui reikalingas tinklo įvykių registravimas. Vartotojų prieigos prie paslaugų ir atliekamų veiksmų fiksavimas, įrenginių ir procesų gedimo ir veikimo fiksavimas yra naudingas atliekant auditą, reaguojant į atakas, taisant tinklo saugos spragas. Organizacija turi nuspręsti, kokius įvykius registruoti ir kiek

laiko saugoti sukauptą informaciją. Įvykių registravimas gali būti taikomas visiems saugos modelio komponentams.

Saugos politikos valdymas

Saugos politika abstrakčiai apibrėžia saugos taisykles. pvz. užtikrinti konfidencialumą tinkle. Saugos modelis turi vaizduoti kokiais būdais tai galima pasiekti. Modelio komponentų specifikacija šiuos būdus detalizuoja.

Saugos politika – tai aukšto lygio dokumentas, apibūdinantis organizacijos tikslus, darbo principus, aplinką. Laiku bėgant saugos politika gali keistis. Politikos tobulinimas turi taip pat turi būti valdomas. Pagal saugos politikos pokyčius gali keistis organizacijos procesai, naudojami standartai.

Modelio komponentų sąsaja

Koncepciniai modelio komponentai vienas su kitu susiję vienpusiu arba dvipusiu ryšiu. OSI modelis nagrinėjamas atsižvelgiant į saugos politiką. Pagal OSI modelį identifikuojami į saugos valdymo procesą įeinantys elementai. Saugos valdymui taip pat reikalingi duomenys apie organizacijos veiklą. Proceso eigoje gali būti atliekami organizacijos veiklos pakeitimai, pvz., apribojamas patikimų vartotojų diapazonas. Poreikis keisti organizacijos veiklą gali lemti saugos politikos pasikeitimą. Komponentų tarpusavio sąsaja pateikta žemiau esančioje 9 lentelėje.

4.3	4.3	4.1	4	3.7	3.6	3.5	3.4	3.3	3.2	3.1	3	2.6	2.5	2.4	2.3	2.2	2.1	2	1.7	1.6	1.5	1.4	1.3	1.2	1.1	1	ID	Komponentas
			+								+							+								*	1	OSI modelis
+	+	+		+	+	+	+	+	+	+		+	+		+	+	+							+	*		1.1	Taikymo lygmuo
+	+	+		+		+			+			+	+		+	+							+	*	+		1.2	Vaizdavimo lygmuo
+	+	+		+	+	+	+		+	+		+	+		+	+						+	*	+			1.3	Seanso lygmuo
+	+	+		+	+	+						+	+		+	+					+	*	+				1.4	Transporto lygmuo
+	+	+		+	+	+						+	+		+	+	+			+	*	+					1.5	Tinklo lygmuo
+	+	+		+	+	+						+	+		+	+	+		+	*	+						1.6	Ryšio lygmuo
+	+	+		+		+	+	+	+	+		+	+		+	+	+		*	+							1.7	Fizinis lygmuo
			+								+							*								+	2	Tinklo rizikos valdymas
+	+	+		+	+	+	+	+	+	+		+	+	+	+	+	*		+	+	+				+		2.1	Tinklo komponentai
+	+	+		+	+	+		+	+	+		+	+	+	+	*	+		+	+	+	+	+	+	+		2.2	Tinklo grėsmės
+	+	+		+	+	+							+	+	*	+	+		+	+	+	+	+	+	+		2.3	Tinklo saugos spragos
+	+	+		+									+	*	+	+	+										2.4	Tinklo rizikos įvertis
+	+	+		+	+	+	+	+	+	+		+	*	+	+	+	+		+	+	+	+	+	+	+		2.5	Tinklo apsaugos priemonės
+	+	+		+	+	+	+	+	+	+		*	+			+	+		+	+	+	+	+	+	+		2.6	Gynybos į gylį modelis
+	+	+	+								*							+								+	3	Organizacijos veiklos
+	+	+		+	+	+	+	+	+	*		+	+			+	+		+				+		+		3.1	Vartotojų valdymas
+	+	+		+				+	*	+		+	+			+	+		+				+	+	+		3.2	Technologijų valdymas
+	+	+		+	+	+	+	*	+	+		+	+			+	+		+						+		3.3	Procesų valdymas
+	+	+		+		+	*	+		+		+	+				+		+				+		+		3.4	Pasitikėjimo valdymas
+	+	+		+	+	*	+	+		+		+	+		+	+	+		+	+	+	+	+	+	+		3.5	Prieigos valdymas
+	+	+		+	*	+		+		+		+	+		+	+	+			+	+	+	+		+		3.6	Įvykių registravimas
+	+	+		*	+	+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+	+		3.7	Saugos politikos valdymas
			*								+							+							+	+	4	Saugos politika
		*		+	+	+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+	+		4.1	Konfidencialumas
	*			+	+	+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+	+		4.2	Vientisumas
*				+	+	+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+	+		4.3	Pasiekiamumas

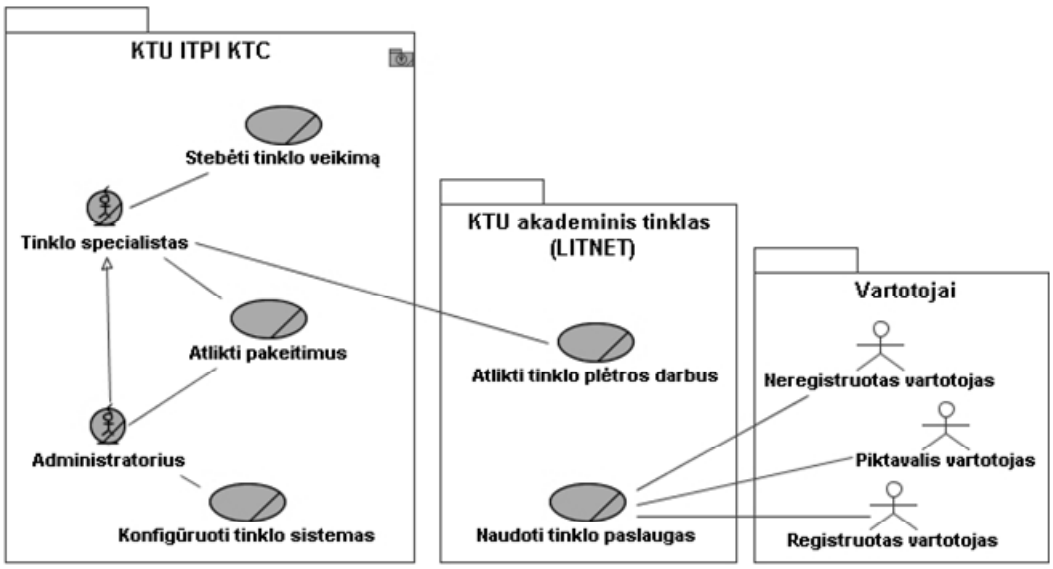
7. ĮTARTINŲ ĮVYKIŲ KOMPIUTERIŲ TINKLE APTIKIMO SISTEMOS KŪRIMAS

Veiksmingam kompiuterių tinklo saugumo užtikrinimui reikalingas tinklo stebėjimas ir reagavimas į incidentus.

Informacijos sistemos kūrimo tikslas yra išplėsti KTU kompiuterių tinklo stebėjimą, integruojant papildomas programas į esamą tinklo stebėjimo sistemą. Sukurta sistema bus naudojama KTU ITPI Kompiuterių tinklų centre (KTC).

7.1 Veiklos analizė

Organizacijos veiklos sąveikų modelyje (38 pav.) vaizduojami pagrnidiniai veiklos principai, susiję su kuriama informacijos sistema.



38 pav.: Veiklos sąveikų modelis

KTU ITPI KTC tinklo specialistas yra atsakingas už tinklo plėtrą ir jo saugumą. Administratorius yra tinklo specialistas, kuris atsakingas už tinklo sistemų konfigūravimą ir tinklo veikimą. KTC teikia paslaugas KTU akademiniam tinklui, kuris yra Lietuvos mokslo ir studijų tinklo (LITNET) dalis. Paslaugas naudojančius vartotojus galima skirstyti į tris kategorijas:

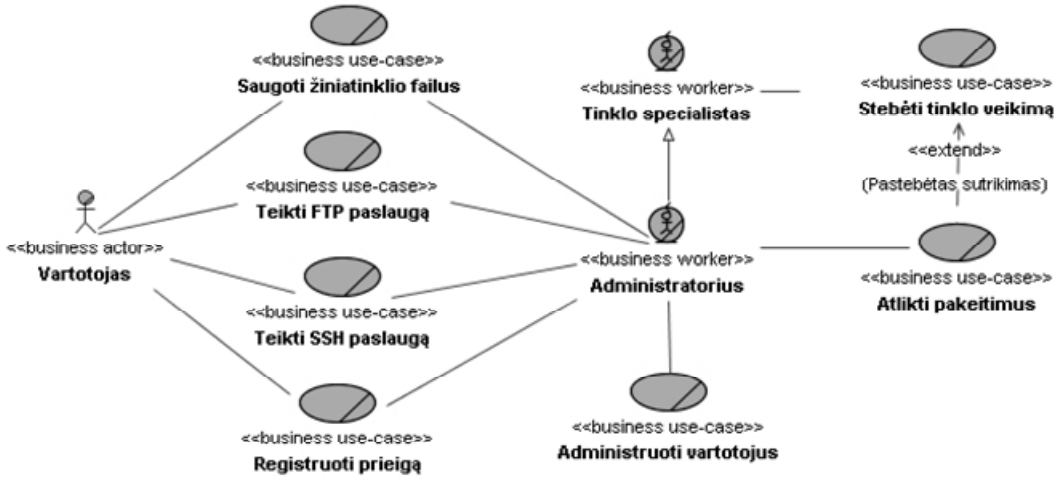
- KTU duomenų bazėje neregistruotus vartotojus, kurie neturi teisės naudotis tinklo paslaugomis. Pasitaiko prisijungimo bandymų iš kitų tinklų, pvz. užsienio šalių. Neregistruotų vartotojų bandymas prisijungti prie KTU tinklo laikomas grėsme.
- piktybiniai vartotojai, kurie stengiasi gauti prieigą išnaudodami sistemoje esančias saugos spragas.

- KTU duomenų bazėje registruoti vartotojai, kurie turi teisę naudotis tinklo paslaugomis ir nepažeidžia prieigos taisyklių.

Administratorius tinklo vartotojams gali suteikti arba panaikinti prieigos prie paslaugų teises, registruoti naujus bei šalinti netinkamus tinklo vartotojus. Registruotų ir neregistruotų vartotojų prieiga prie tinklo paslaugų yra registruojama nepriklausomai nuo prisijungimo rezultato (pavyko ar nepavyko). Tai suteikia galimybę stebėti tinklo vartotojų veiksmus, tinklo naudojimą.

Žiniatinklio failų talpinimas serveryje kelia grėsmę tinklo saugumui. Taikomųjų žiniatinklio programų kode esančios klaidos sudaro saugos spragą, kuria gali pasinaudoti piktavalis vartotojas ir sukompromituoti sistemą ar jos dalį. Programinės įrangos gamintojų produktuose aptiktos klaidos yra viešai skelbiamos, kad sistemų administratoriai galėtų jas ištaisyti įdiegtose programose. Paskelbta informacija gali pasinaudoti ne tik administratorius, bet ir piktavalis vartotojas.

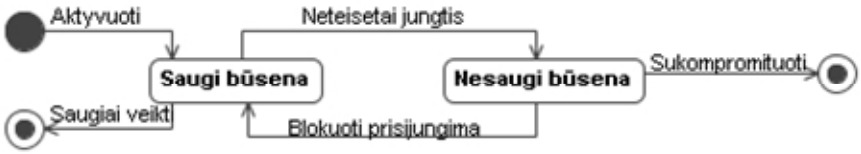
Tinklo specialistas gali stebėti tinklo veikimą. Tam naudojama speciali programinė įranga, kuri informuoja tinklo specialistą apie veikimo sutrikimus, pvz., įrenginių gedimus, paslaugų sutrikimus, vietos diske trūkumą ir pan. Sužinojęs apie sutrikimą tinklo specialistas turi imtis reikiamų veiksmų sutrikimui pašalinti. Tuo tikslu gali būti reikalingi konfigūracijos, programinės ar techninės įrangos pakeitimai.



39 pav. Detalizuotas veiklos sąveikos modelis

Kompiuterių tinklas laikomas saugiu jei keičiantis tinklo sistemos būsenai išlaikomas būsenos saugumas, t.y. jei pradinė būsena yra saugi, tai ir kita būsena, į kurią pereina sistema po bet kokio įvykio, taip pat turi būti saugi. 40 pav. vaizduojama būsenų diagrama parodo, kad neteisėtas bandymas pasinaudoti tinklo resursais ar paslaugomis bei saugos spragų

išnaudojimas pakeičia tinklo būseną iš saugios į nesaugią. Norint grąžinti ar užtikrinti būsenos saugumą turi būti blokuojami neleistini bandymai jungtis bei panaikintos saugos spragos.



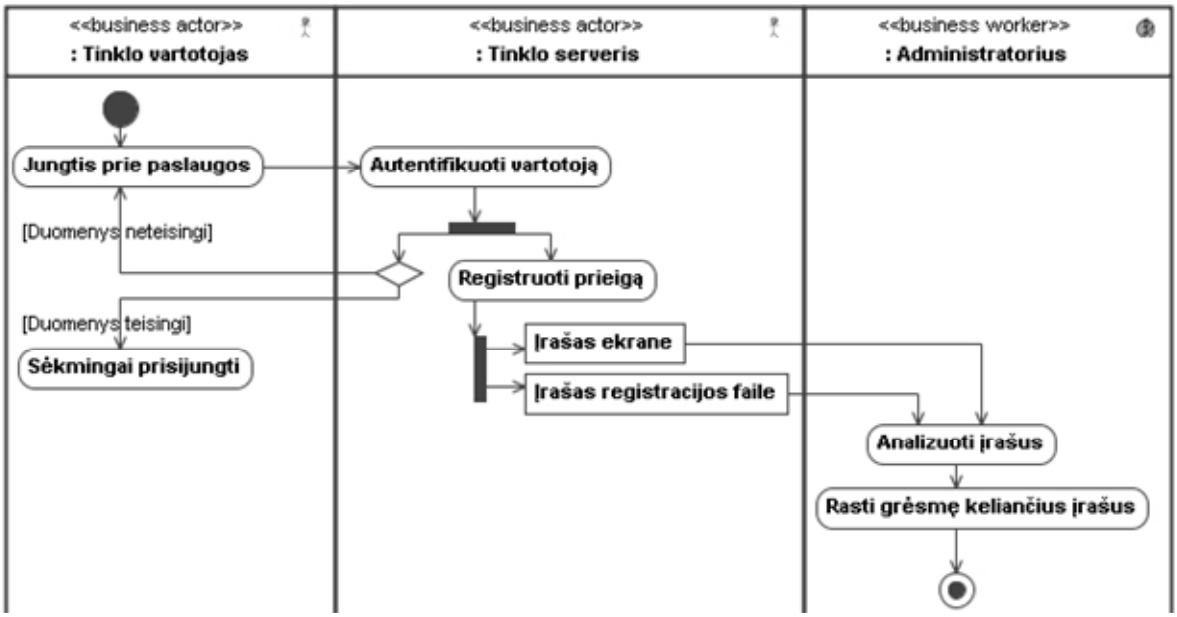
40 pav. Būsenų diagrama

41 pav. vaizduojamas tinklo vartotojų prisijungimų analizės procesas. Šio proceso tikslas yra nustatyti grėsmę keliančius prisijungimų bandymus. Pagal gautus analizės rezultatus galima papildyti prieigos valdymo taisykles tinklo užkardoje ar paslaugos teikimo konfigūracijoje.

Tinklo vartotojui bandant jungiantis prie serverio teikiamos paslaugos, pirmiausia atliekama autentifikacija. Jeigu vartotojo pateikti prisijungimo duomenys yra teisingi (sutampa su duomenų bazėje saugomais duomenimis apie vartotoją), vartotojas prisijungia sėkmingai. Kitu atveju pateikta užklausa atmetama ir pasiūlomas pakartotinis prisijungimo bandymas. Abiem atvejais (sėkmingu ir nesėkmingu) prieigos bandymas yra fiksuojamas. Administratorius prisijungimo bandymus gali matyti dviem būdais:

- skaitydamas serverio įvykių registracijos faile užfiksuotą istorinę informaciją
- realiu laiku stebėdamas serveryje per komandinę eilutę iškviestos programos pateikiamus rezultatus.

Abu prieigos analizės būdai yra neefektyvūs dėl duomenų gausumo ir laiko sąnaudų.



41 pav. Tinklo vartotojų prisijungimų analizės procesas

Administratoriui ir tinklo specialistui aktualu gauti informaciją apie tam tikrus įvykius tinkle, pvz., tinklo įrenginių gedimus, neleistinus vartotojų veiksmus, esančias saugos spragas ir kitas problemas.

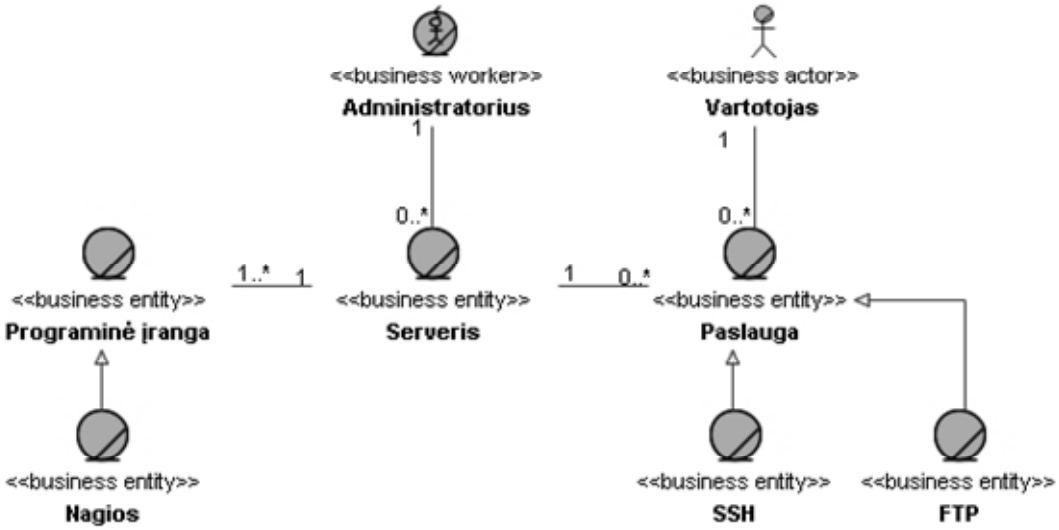
Tinklo stebėjimui galima naudoti taikomąsias programas, kurios stebi tinklo įvykius ir informuoja administratorių apie pastebėtus sutrikimus. Tokios sistemos pavyzdys yra plačiai naudojama atviro kodo programinė įranga Nagios. Pagrindiniai Nagios privalumai:

- tinklo įrenginių (maršrutizatorių, serverių, darbo kompiuterių) stebėjimas,
- centralizuotas valdymas (stebimi nutolę įrenginiai, stebėjimo periodiškumas nurodomi konfigūracijoje),
- informavimas apie įrenginių veikimo sutrikimus (garsu, vaizdu, pranešimais),
- lankstumas (galimybė išplėsti funkcionalumą integruojant vartotojo programas).

Nagios leidžia stebėti:

- tinklo įrenginių pasiekiamumą (aptinka tinklo sutrikimus)
- paslaugos pasiekiamumą (aptinka paslaugų sutrikimus)
- resursų trūkumą (vietos diske arba operatyviosios atminties trūkumą)

Organizacijos veiklos objektų modelis pateikiamas 42 pav.



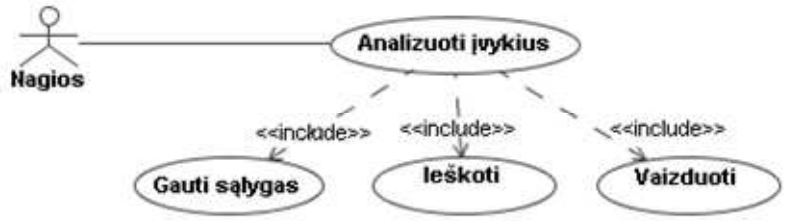
42 pav. Organizacijos veiklos objektų modelis pateikiamas

7.2 Sistemos projektavimas, realizacija ir diegimas

Atlikus veiklos analizę nustatyta, kad reikalinga įtartinus įvykius aptinkanti sistema, kuri palengvintų įtartinų prisijungimų nustatymą.

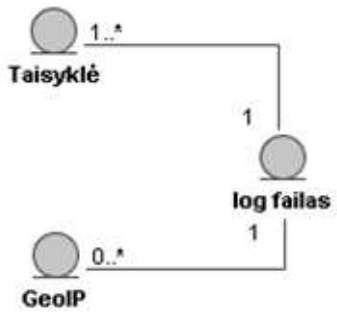
Nauja sistema turi būti integruota į egzistuojančią tinklo įrenginių stebėjimo sistemą Nagios. Tokiu būdu siekiama išlaikyti centralizuotą stebėjimą sistemą. Įtartinus įvykius aptinkanti sistema turi būti patikima, lanksti, lengvai diegiama ir saugi.

Išskirti kompiuterizuojami panaudojimo atvejai vaizduojami 43 pav.



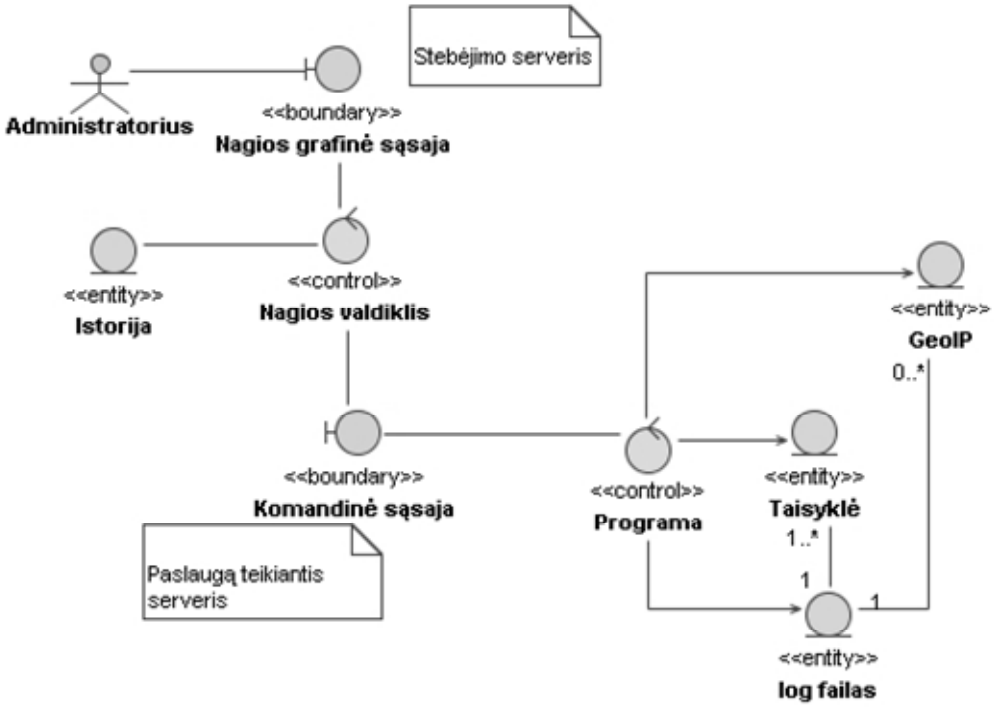
43 pav. Kompiuterizuojami panaudojimo atvejai

Įtartinų įvykiu stebėjimo sistemos objektų klasių modelis pateikiamas 44pav.



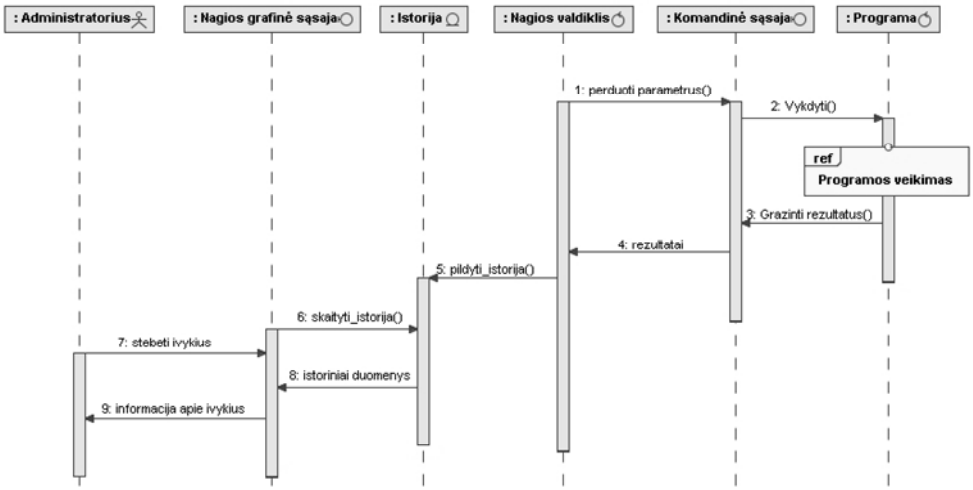
44 pav. objektų klasių modelis

Analizės klasių modelis vaizduojamas 45 pav.



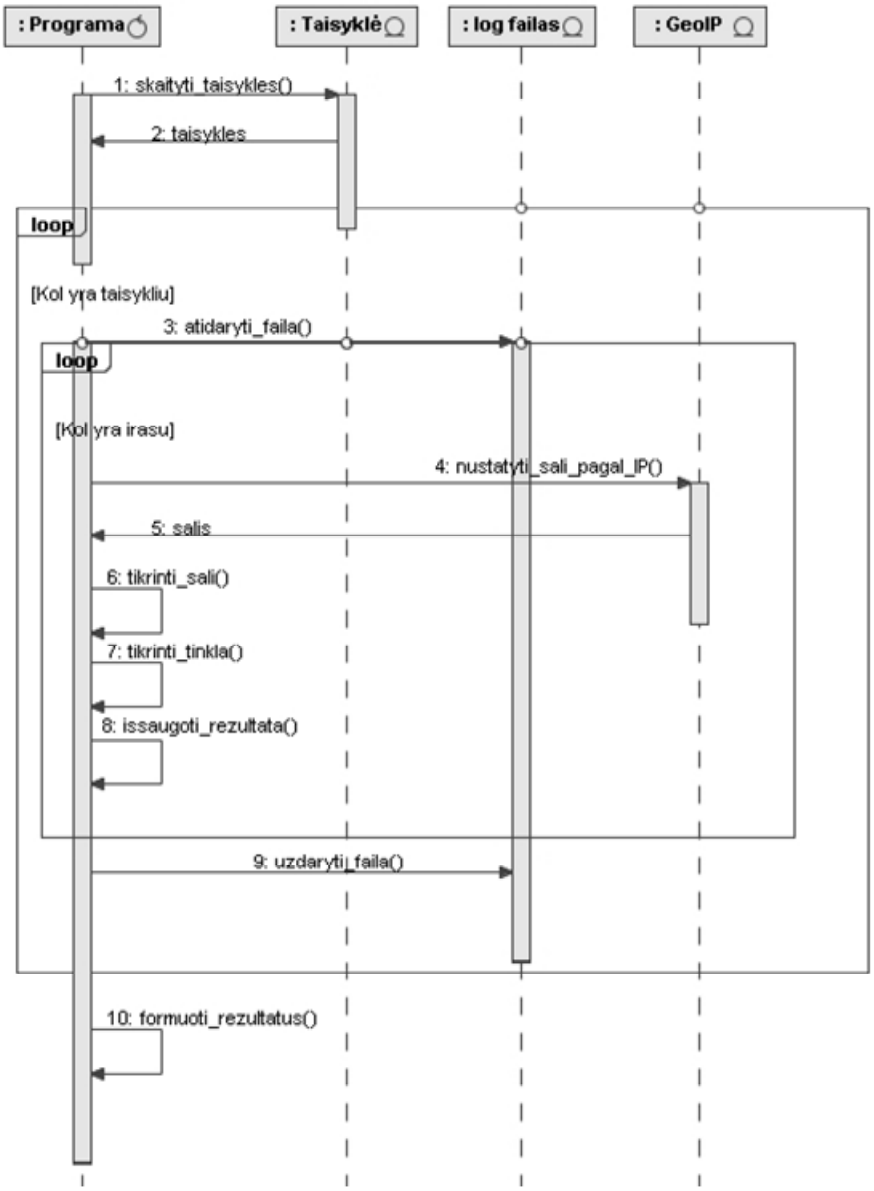
45 pav. Analizės klasių modelis

Administratoriaus ir tinklo stebėjimo programinės įrangos sąveikos diagrama vaizduojama 46 pav.



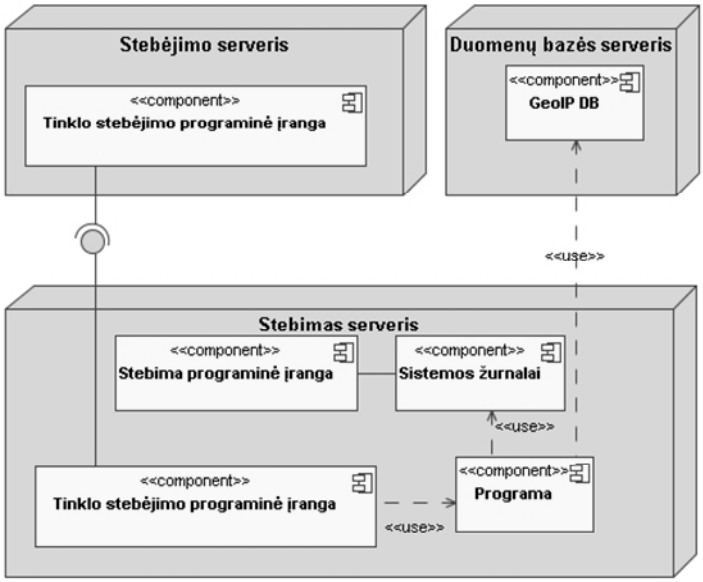
46 pav. Administratoriaus ir tinklo stebėjimo programinės įrangos sąveikos diagrama

Programos veikimo sekų diagrama vaizduojamas 47 pav.



47 pav. Programos veikimo sekų diagrama

Sukurta sistema yra didesnės sistemos dalis. Stebėjimo serveryje esanti Nagios programinė įranga gali stebėti nutolusius tinklo įrenginius. Stebimame serveryje turi būti įdiegta papildoma programinė įranga, leidžianti vykdyti programas nutolusiame serveryje. Viena iš tokių programų yra įtartinų įvykių aptikimo sistema. Ji naudoja stebimo serverio sisteminius žurnalus, kuriuose fiksuojama prieiga prie tinklo paslaugų, klaidos bei kita aktuali informacija. Sisteminių žurnalų užfiksuoti prisijungimo IP adresai lyginami su GeoIP duomenų bazėje saugomais IP adresais. Sistemos išdėstymo diagrama vaizduojama 48 pav.

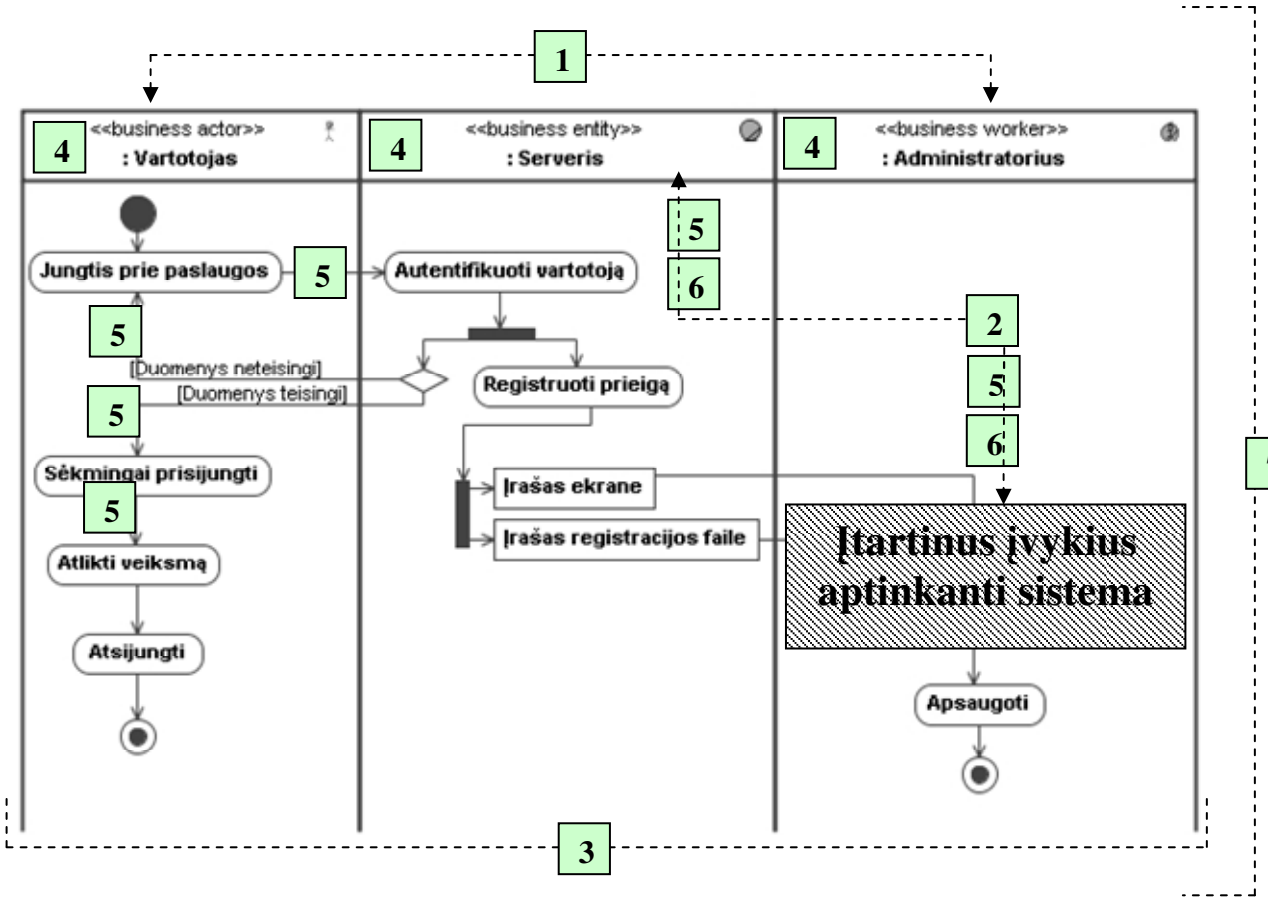


48 pav. Įtartinus įvykius aptinkančios sistemos išdėstymo diagrama

8. ĮTARTINŲ ĮVYKIŲ APTIKIMO SISTEMOS REALIZACIJA

8.1 saugos procesų valdymo kompiuterių tinkluose modelio pritaikymas

Sukurtas saugos procesų valdymo kompiuterių tinkluose modelio pritaikymas organizacijoje vaizduojamas 49 pav.



49 pav. saugos procesų valdymo kompiuterių tinkluose modelio komponentų vieta

1 – vartotojų valdymas
2 – technologijų valdymas
3 – procesų valdymas
4 – pasitikėjimo valdymas
5 – prieigos valdymas
6 – Įvykių registravimas
7 – saugos politicos valdymas

1 – Vartotojų valdymas apima vartotojo ir administratoriaus teisių valdymą.

2 – technologijų valdymas apima serverio ir programinės įrangos valdymą.

3 – proceso valdymas apima visą proceso eigą.

4 – pasitikėjimo valdymas gali būti taikomas vartotojui, serveriui ir arministratoriui.

5 – prieigai valdyti naudojama ugniasienė, autentifikacija, autorizacijos metu priskirti komandų vykdymo apribojimai.

6 – įvykių registravimas atliekamas jungiantis prie serverio ir informacinės sistemos.

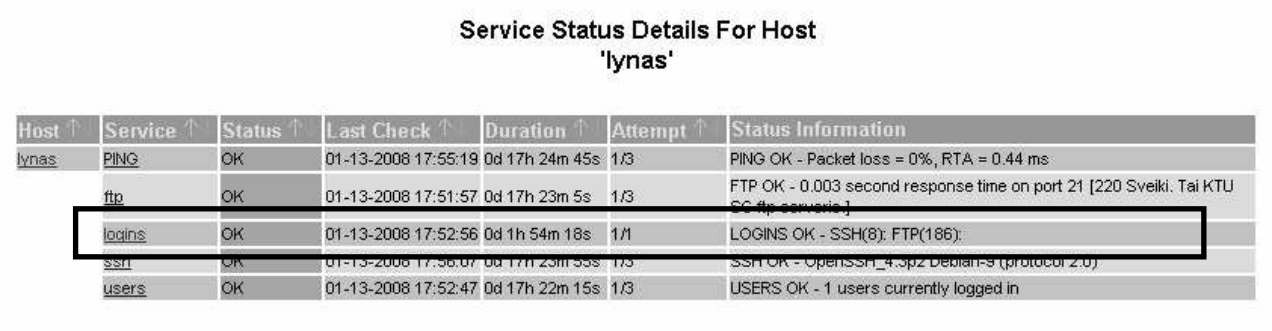
7 – saugos politikos valdymas apima visas proceso metu naudojamas saugos taisykles ir metodus.

8.2 Įtartinus įvykius aptinkančios sistemos eksperimentinis patikrinimas

Sukurta įtartinus įvykius aptinkanti sistema yra integruota į tinklo įrenginių stebėjimo sistemą Nagios. Toliau pateiktuose paveikslėliuose ji vaizduojama kaip „logins“ paslauga. Stebimame serveryje įdiegta programa stebi įvykius. Aptikus įtartinus prisijungimus, siunčiamas pranešimas administratoriui.

Įtartinumo kriterijus yra vartotojo IP adresas. Organizacija paslaugas teikia tik Lietuvos akademinių organizacijų vartotojams, todėl prisijungimas iš užsienio yra įtartinas ir turėtų būti patikrinamas. Šalis, iš kurios jungiasi vartotojas, nustatoma pagal duomenų bazėje saugomus IP adresus. Yra žinomos kiekvienos šalies IP adresų sritys.

50 pav. parodytas atvejis, kai nėra įtartinų prisijungimų. Tokiu atveju serverio būsenos reikšmė „OK“ ir vaizduojama žaliai.

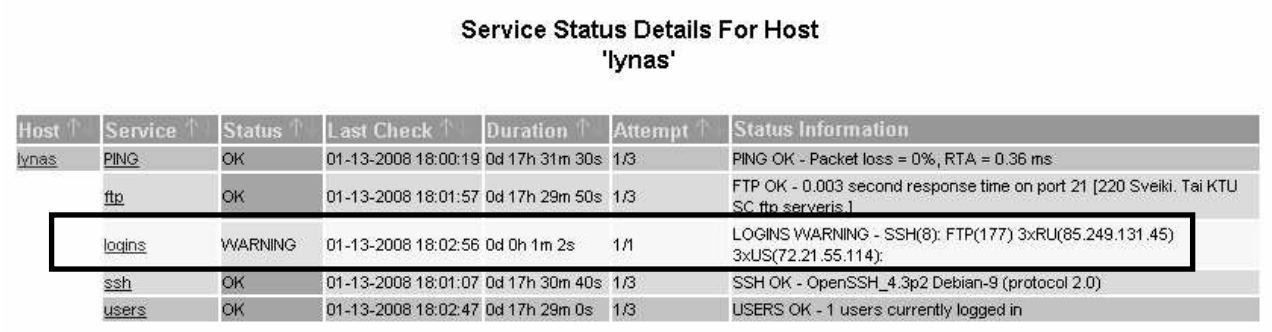


Service Status Details For Host 'lynas'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
lynas	PING	OK	01-13-2008 17:55:19	0d 17h 24m 45s	1/3	PING OK - Packet loss = 0%, RTA = 0.44 ms
	ftp	OK	01-13-2008 17:51:57	0d 17h 23m 5s	1/3	FTP OK - 0.003 second response time on port 21 [220 Sveiki. Tai KTU SC ftp serveris.]
	logins	OK	01-13-2008 17:52:56	0d 1h 54m 18s	1/1	LOGINS OK - SSH(8): FTP(186):
	ssh	OK	01-13-2008 17:56:07	0d 17h 23m 53s	1/3	SSH OK - OpenSSH_4.3p2 Debian-9 (protocol 2.0)
	users	OK	01-13-2008 17:52:47	0d 17h 22m 15s	1/3	USERS OK - 1 users currently logged in

50 pav. Serverio “lynas” būsena “OK”, kai nėra įtartinų prisijungimų

51 pav. rodomas perspėjimas, kad prie sistemos buvo sėkmingai prisijungta ne iš Lietuvos kompiuterių tinklo. Tokiu atveju serverio būsenos reikšmė „WARNING“ ir vaizduojama geltona spalva.



Service Status Details For Host 'lynas'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
lynas	PING	OK	01-13-2008 18:00:19	0d 17h 31m 30s	1/3	PING OK - Packet loss = 0%, RTA = 0.36 ms
	ftp	OK	01-13-2008 18:01:57	0d 17h 29m 50s	1/3	FTP OK - 0.003 second response time on port 21 [220 Sveiki. Tai KTU SC ftp serveris.]
	logins	WARNING	01-13-2008 18:02:56	0d 0h 1m 2s	1/1	LOGINS WARNING - SSH(8): FTP(177) 3xRU(85.249.131.45) 3xUS(72.21.55.114):
	ssh	OK	01-13-2008 18:01:07	0d 17h 30m 40s	1/3	SSH OK - OpenSSH_4.3p2 Debian-9 (protocol 2.0)
	users	OK	01-13-2008 18:02:47	0d 17h 29m 0s	1/3	USERS OK - 1 users currently logged in

51 pav. Serverio “lynas” būsena “WARNING”, kai yra įtartinų prisijungimų

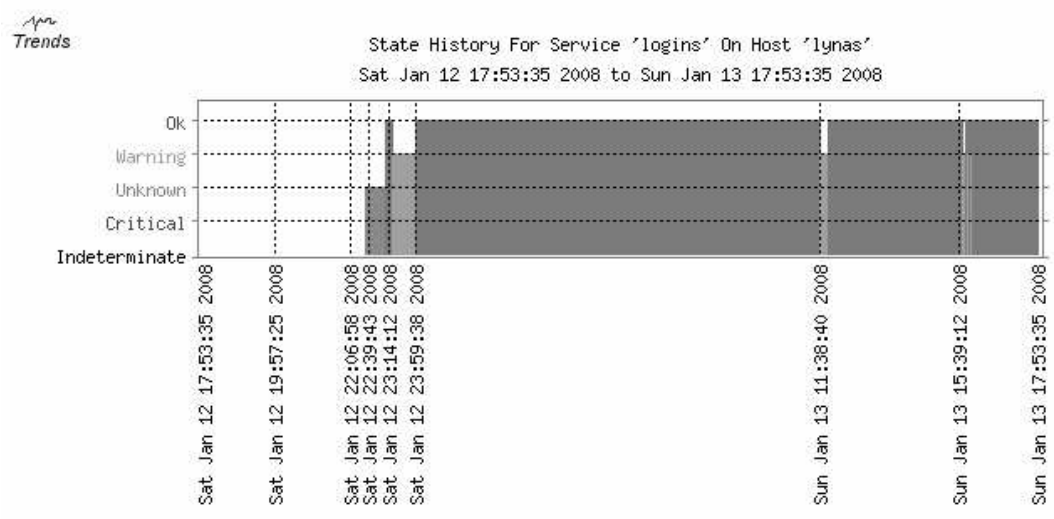
Aptikus įtartiną prisijungimą tinklo administratoriui išsiunčiamas elektroninis laiškas su išsamesne (registracijos faile užfiksuota) infromacija:

```
FTP IP: 85.249.131.45, Country: RU
Jan 12 11:46:52 lynas proftpd[21807] lynas.litnet.lt
(85.249.131.45.addr.datapoint.ru[85.249.131.45]): USER kunig: Login
successful.
```

```
FTP IP: 85.249.131.45, Country: RU
Jan 12 11:46:54 lynas proftpd[21808] lynas.litnet.lt
(85.249.131.45.addr.datapoint.ru[85.249.131.45]): USER panem: Login
successful.

FTP IP: 72.21.55.114, Country: US
Jan 12 17:52:31 lynas proftpd[12286] lynas.litnet.lt
(72.21.55.114[72.21.55.114]): USER nalma: Login successful.
```

Tinklo stebėjimo sistema veda sukurtos integruotos sistemos užfiksuotų įvykių istoriją. 52 pav. matyti, kad buvo aptikta įtartinų prisijungimų. Grafike jų reikšmė yra „Warning“. Reikšmė „OK“ rodo, kad įtartinų prisijungimų nurodytame laiko intervale nebuvo.



52 pav. Sistemos įvykių istorija

Įtartinų įvykių aptikimas ir pateikimas administratoriui padeda stebėti tinklo prieigą. Pastovus prieigos stebėjimas yra reikalingas greitam reagavimui į incidentus.

IŠVADOS

1. Kompiuterių tinklo saugos pagrindą sudaro organizacijos tinklo saugos politika. Tinklo saugos modeliai yra skirti saugos politikos formalizavimui, tačiau jie gali būti naudojami ir saugos politikos sudarymui.
2. Saugos modelių analizės metu nustatyta, kad saugos modeliai gali būti dviejų tipų: formalūs ir koncepciniai. Koncepciniai modeliai įvertina daugiau tinklo saugos problemų, tačiau nėra tokie tikslūs ir konkretūs kaip formalieji.
3. Sukurtas koncepcinis saugos procesų kompiuterių tinkluose modelis apibendrina išanalizuotus saugos modelius ir įvertina informacijos saugos praradimo riziką.
4. Sukurta įtartinus tinklo įvykius aptinkanti sistema informuoja administratorių apie grėsmę keliančius vartotojų prisijungimus. Įtartinais laikomi tokie prisijungimai, kai vietinėje duomenų bazėje registruoti vartotojai sėkmingai prisijungia iš užsienio tinklo.
5. Sukurta sistema yra skirta Lietuvos akademinei organizacijai, kuri neaptarnauja užsienio vartotojų. Dėl šios priežasties minėti prisijungimai iš užsienio prie Lietuvos akademinio tinklo resursų turi būti stebimi ir tikrinami. Nuolatinis kompiuterių tinklo stebėjimas yra vienas iš pagrindinių saugos didinimui reikalingų veiksmų.

LITERATŪRA

1. Lietuvos Respublikos Vidaus reikalų ministerija. Rizikos analizės vadovas. Vaga, 2005, p. 160
2. D. J. Landoll. The Security Risk Assessment Handbook a Complete Guide for Performing Security Risk Assessments. CRC Press, 2006, p. 473
3. By Giampiero E. G. Beroggi, William A. Wallace. Computer Supported Risk Management, Springer 1995, p. 384
4. J. M. Stewart, E. Tittel, M. Chapple. CISSP: Certified Information Systems Security Professional Study Guide 2nd Edition, Sybex, 2005, p. 800
5. S. Snedaker. Syngress IT Security Project Management Handbook, Syngress, 2006, p. 612
6. T. Bass, R. Robichaux. Defense-In-Depth Revisited: Qualitative Risk Analysis Methodology for Complex NetworkCentric Operations, publikacija, 2002, p. 10
7. M. Horton, C. Mugge. HackNotes Network Security Portable Reference, McGraw-Hill Professional, 2003, p. 288
8. Cisco Systems Inc. Designing Network Security, Cisco Press Publications, 2001, p. 406
9. C. Alberts, A. Dorofee. Managing Information Security Risks: The OCTAVESM Approach, Addison Wesley, 2002, p. 512
10. H. F Tipton, M. Krause. nformation Security Management Handbook, Sixth Edition, Auerbach Publications, 2007, p. 3231
11. C. Riggs. Network Perimeter Security: Building Defense In-Depth, Auerbach Publications, 2004, p. 424
12. Nataraj Nagaratnam. The Security Architecture for Open Grid Services, July 17, 2002, Version 1.
13. M. Stamp. Information Security: Principles and Practice, John Wiley & Sons, 2006, p. 390
14. M. Horton, C. Mugge. HackNotes Network Security Portable Reference, McGraw-Hill Professional, 2003, p. 288
15. D. Mackey. Web Security for Network and System Administrators, Thomson Course Technology, 2003, p. 440
16. V. Ališauskaitė, D. Rimkus. Kompiuterių tinklų saugos sistemų problematikos analizė. Straipsnis. Informacinių sistemų konferencija, 2007.

Design of Computer Network Security Models

Summary

Computer network security is one of the most important things in an organization. Confidential user data is stored in databases and transmitted over the network. Information leakage, data theft, network sniffing, spoofing attacks are some of network security issues. They can cause undesired consequences to organization's business.

Understanding and using computer network security models can help to avoid damage of attacks that exploit security wholes and vulnerabilities in computer network components.

For this reason a wide security model analysis was done.

The goal of this work is to create a computer network security model, which would evaluate not only the technical details of network management security, but also the organizational security activity.

The result of this work is a newly designed computer network security model which comprises of OSI model layers, risk management process and organizational security activities such as policy management, user management, access controls, trust management. To influence risk management process an integrated network monitoring system whish detects suspicious user logons for unauthorized services was designed. It helps network administrator to learn about undesirable usage of services and to prevent the network from accessing network services for unregistered users.

TERMINŲ IR SANTRUMPŲ ŽODYNAS

OSI (*Open System Interconnection Reference Model*) modelis – koncepcinis kompiuterių tinklo protokolų modelis.

ACL (*Access Control list*) – prieigos valdymo sąrašas, kurį sudaro prieigą apribojančios taisyklės.

DAC (*Discretionary Access Control*) - diskrecinis prieigos valdymo modelis, kuriame subjekto savininkas nusprendžia, kas gali prieiti prie jo turimo subjekto.

MAC (*Mandatory Access Control*) - imperatyvinis prieigos valdymo modelis, kuriame vartotojams suteikiama mažai laisvės sprendžiant, kas gali prieiti prie jų turimų duomenų bylų.

RBAC (*Role Based Access Control*) – rolėmis pagrįstas autorizuotų vartotojų prieigos valdymo modelis, kuriame sprendimai priimami atsižvelgiant į subjektų roles.

MLS (*Multilevel Security*) – daugialygis saugumas.

CIA (*Confidentiality, Integrity, Availability*) – informacijos patikimumo modelis, įvardinantis tris pagrindines informacijos saugos savybes (konfidencialumą, vientisumą, pasiekiamumą).

VLAN (*Virtual Local Aria Network*) – virtualus vietinis tinklas.

IP (*Internet Protocol*) – interneto protokolas.

TCP (*Transport Control Protocol*) – transporto valdymo protokolas

UDP (*User Datagram Protocol*) – duomenų perdavimo protokolas

ICMP (*Internet Control Message Protocol*) – interneto kontrolės žinučių protokolas.

IDS (*Intrusion Detection System*) – įsilaužimo aptikimo sistema.

IPS (*Intrusion Prevention System*) – apsaugos nuo įsilaužimo sistema.

PRIEDAI

I priedas. Straipsnis

Kompiuterių tinklų saugos sistemų problematikos analizė

Vaida Ališauskaitė, Dangis Rimkus

Kauno Technologijos Universitetas, Kompiuterių tinklų katedra, Studentų g. 50

Pateikiama kompiuterių tinklų saugos tematikos mokymo moduliuose nagrinėjamų temų statistika, kuri yra panaudota sudarant aktualių mokymo modulių turinius. Tematikos klasifikacija atlikta panaudojus paieškas pagal raktinius žodžius arba jų junginius

1. Temos aktualumas

Kompiuterių tinklų saugos klausimai pastaruoju metu tampa vis aktualesni. Todėl įvairių šalių universitetuose pradėti dėstyti moduliai, nagrinėjantys tinklų saugos problemas. Iki šiol Lietuvos universitetuose yra dėstomi keli moduliai, kurie tik netiesiogiai apima kelis kompiuterių tinklų saugos aspektus: pirma (tinklų moduliuose) - kaip teisingai sukonfigūruoti, sujungti, panaudoti tipinius protokolus, kad būtų kuo didesnis tinklo patikimumas ir pateikiamumas ir tokiu būdu užtikrinant informacijos perdavimą apskritai; antra (kriptografijos arba informacijos saugos moduliuose) - kokius taikyti šifravimo mechanizmus, kaip užšifruoti informaciją, kad ji nebūtų panaudota piktavališkiems tikslams, taip pat aiškinama kaip ir kam taikomos specialios programinės ir techninės priemonės informacijos saugai padidinti. Didžioji dalis kitų tinklų saugos temų nėra įtraukta į mokymų programas.

Lietuvos universitetinės studijų programos jau keletą metų yra sparčiai modernizuojamos. Visuomenėje atsiradęs poreikis surasti tokius būdus, kad būtų galima užtikrinti šalies konkurencingumą visose ūkio šakose. Privačioms ir valstybinėms institucijoms, taip pat institucijoms, tiesioginiai susijusioms su saugumu, labai aktualus tinklo saugumo klausimas, nes duomenų vagystės kelia grėsmę jų pačių saugumui ar dėl to yra patiriami dideli finansiniai nuostoliai ir prarandamas verslas visiems laikams. Ypač spartus per pastarąjį dešimtmetį kompiuterių tinklų vystymasis reikalauja vis daugiau specialistų, kurie galėtų tinkamai prižiūrėti ir kurti šią struktūrą. Atsiranda naujų mokymo programų, atsiliepiančių į šiuolaikinio mokslo tendencijas ir ekonomikos poreikį.

2. Problematikos statistikos surinkimo metodika

Kompiuterių tinklų saugos sistemų problematika gali būti atskleista pagal informacijos šaltinius, pasiekiamus žiniatinklyje. Galima analizuoti trijų tipų informacijos šaltinius: mokslines konferencijas, mokslines publikacijas ir mokymo programas. Atliekant paieška pagal mokslinių konferencijų tematiką nustatomos perspektyvios tinklų saugos mokslo vystymo kryptys. Atliekant paieška pagal mokslines publikacijas galima surasti aktualiausias šios dienos problemas ir jų sprendimo metodus. Šių dviejų paieškų rezultatai gali būti gerai pritaikomi sudarant doktorantūros modulių tematiką. Ruošiant naujas magistrantūros mokymo programas tikslingiau analizuoti mokymo programose pateikiamus modulių turinius.

Šiame darbe pagrindinis dėmesys skirtas nustatyti pagrindines tematikas, kurių įsisavinimas būtų privalomas visiems tinklų krypties magistrantūros studijų studentams. Tyrime panaudotos dvidešimties skirtingų universitetų mokymo modulių medžiaga. Išanalizavus programų modulių turinius atrinkta dvidešimt aktualiausių raktinių žodžių arba jų junginių: Anonymity; Authentication; Computer virus, worm; Cryptographic; E-mail security; Firewall; Host Issues; IP Spoofing; Kerberos protocol; Password cracking; Protocols; Routing security; Spoofing attacks; SSL protocol; VPN Security; Web Security; Wireless Security; IPsec, Intrusion detection; Access control. Tam, kad padidinti problemų analizės patikimumą kiekvienam raktiniam žodžiui arba jų junginiui nustatėme jo prasmės semantiką:

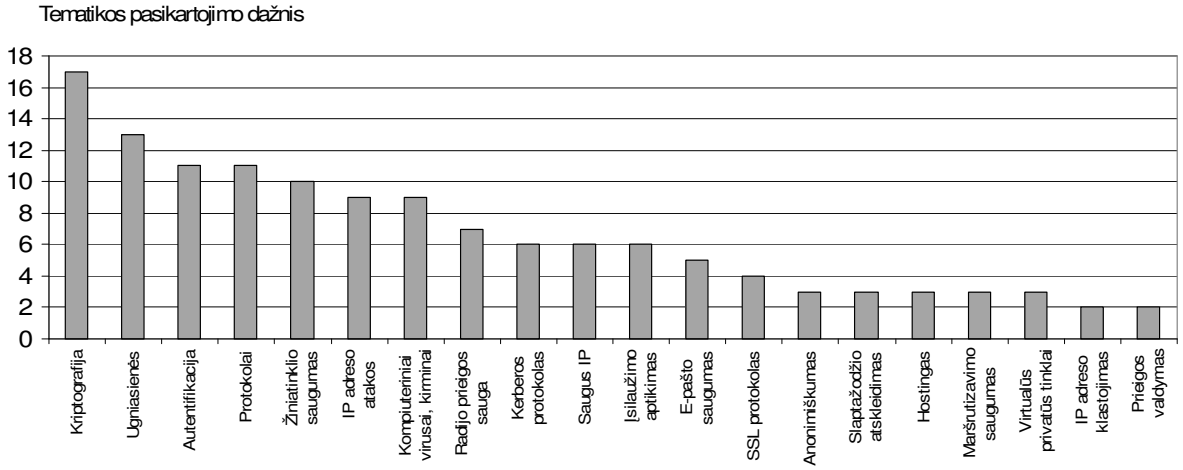
- Kriptografija (Cryptography) – tai informacijos teorijos mokslo kryptis, nagrinėjanti pranešimo perdavimo slaptumą; informacijos teorijos šaka, matematiškai nagrinėjanti informaciją ir jos perdavimą iš vienos vietos į kitą;
- Ugniasienė (Firewall) – tai informacijos technologijų saugos įrenginys, sukonfigūruotas leisti, drausti arba praleisti susijungimus įvertinant organizacijos saugos politiką;
- Įsilaužimo aptikimas (Intrusion detection) - tai galinčių sukompromituoti resurso konfidencialumą, vientisumą ir pasiekiamumą veiksmų aptikimas;
- IP adreso klastojimas (IP Spoofing) - tai neautorizuotas prisijungimas prie kompiuterio siunčiant pranešimus su suklastotu IP adresu, atitinkančiu tikrojo kompiuterio IP adresą;

- Virtualus privatus tinklas (VPN) - tai privatus kompanijos arba kelių kompanijų komunikacijų tinklas, skirtas jų konfidencialios informacijos perdavimui per bendrąjį kompiuterių tinklą;
- Saugus IP (IPsec) saugiam IP protokolo perdavimui skirtas protokolų rinkinys, atliekantis kiekvieno IP paketo autentifikacija arba šifravimą;
- Prieigos valdymas (Access control) –gebėjimas kažkam leisti arba drausti prieigą prie kažko;
- Slaptažodžio atskleidimas (Password cracking) – saugomuose arba kompiuterių tinklais perduodamose duomenyse esančio slaptažodžio atskleidimas;
- Kompiuterinis virusas (Virus) – tai programinėse bylose paslėpta kompiuterinė programa, skirta keisti kompiuterio veikimą be vartotojo sutikimo ar žinios;
- Komputerinis kirminas (Computer worm) – tai savaime besidauginanti kompiuterinė programa, naudojama siusti kitiems kompiuteriams savo pačios kopijas nedalyvaujant vartotojui;
- Kerberos protokolas (Kerberos)– tai kompiuterių tinklo autentifikacijos protokolas, leidžiantis vartotojams per nesaugų tinklą saugiai patvirtinti savo tapatumą;
- Suklastojimo ataka (Spoofing attack) – tai situacija, kurios metu asmuo arba programa apsimeta kitu asmeniu ar programa falsifikuodamas duomenis ir tuo būdu įgydamas neteisėtą pranašumą;
- SSL (Secure Sockets Layer) – tai kriptografinis protokolas, skirtas internetu sklindančios informacijos apsaugojimui šifruojant;
- Autentifikacija (Authentication) – tai norinčio prisijungti per komunikacijų tinklą skaitmeninių duomenų patikrinimo procesas;
- Anonimiškumas (Anonymity) – savybė tokio elemento, kuris negali būti identifikuotas.

3. Problematikos statistikos analizė

Išnagrinėjus literatūros šaltinius pastebėta, kad tinklų saugos tematika kiekvieną mėnesį vyksta 5-6 tarptautinės konferencijos. Tačiau konferencijų tematika yra pateikiama gana abstrakčiai. Pirminė analizė parodė, kad nėra aiškaus ryšio tarp studijų modulių medžiagas dėstančių autorių ir mokslinių straipsnių autorių.

Detaliau analizuoti magistrantūros modulių turiniai. Modulių turiniuose aptikta virš 200 skirtingų kompiuterių tinklų saugos srities temų. Pagal pagrindinius aukščiau pateiktus raktinius žodžius gautas nagrinėjamų tematikų pasiskirstymas pateiktas 1 pav. Analizė parodė, kad didžioji dalis kompiuterių tinklų saugos programų yra JAV universitetuose. Skirtinguose universitetuose nagrinėjama tematika yra labai įvairi. Tai tikriausiai priklauso nuo mokslinių tyrimų tematikos skirtinguose universitetuose. Didžiausias dėmesys skiriamas kriptografijos pagrindams. Toliau seka tokios tematikos: ugniasienės, autentifikacija, saugos protokolai, žiniatinklio saugumas, IP adreso atakos, kompiuteriniai virusai ir kirminai. Rečiausiai nagrinėjamas tinklo prieigos valdymas ir IP adreso klastojimas. Palyginti mažai dėmesio skirta VPN saugai, maršrutizavimo saugai, hostingui, slaptažodžių atskleidimui, anonimiškumui. Įvertinant tai, kad Europa didelį dėmesį skiria mobiliosioms ir bevielėms komunikacijoms, tinklų saugos moduliuose turėtų būti padidintas dėmesys kompiuterių tinklų prieigos valdymui.



1 pav. Aukštųjų mokyklų mokymo moduliuose pateikiamų temų pasiskirstymas

4. Išvados

Sukurta problematikos statistikos surinkimo metodika pritaikyta atrinkti tiek doktorantūros, tiek ir magistrantūros aktualias mokymo modulių tematikas. Atlikta mokymo moduliuose pateikiamų turinių analizė parodė, kad didžioji dalis kompiuterių tinklų saugos programų yra JAV universitetuose. Daugiau negu puse magistrantūros programų nagrinėjami kriptografijos pagrindai, ugniasienės, autentifikacija, saugos protokolai,

žiniatinklio saugumas, IP adreso atakos, kompiuteriniai virusai ir kirminai. Rečiausiai nagrinėjamas tinklo prieigos valdymas ir IP adreso klastojimas. Palyginti mažai dėmesio skirta VPN saugai, maršrutizavimo saugai, hostingui, slaptažodžių atskleidimui, anonimiškumui. Tolimesniuose problematikos tyrimuose tikslinga susieti mokymo moduliuose pateiktą tematiką su publikacijų tematikomis.

Literatūros sąrašas

[1] D. Gollmann. Network Security.Hamburg-Harburg University of Technology. http://www.sva.tu-harburg.de/html/modules.php?op=modload&name=PagEd&file=index&page_id=1

[2] S. Vitaly. Network Security and Privacy. The University of Texas at Austrin. http://www.cs.utexas.edu/~shmat/courses/cs378_spring06/cs378_home.html

[3] H. Taylor. Network Technology and Security. School of Mathematical and Computer Sciences (MACS). http://www.macs.hw.ac.uk/cs/online/4nu2/

[4] P. Reiher. Advanced Topics in Network Security. Laboratory for Advanced Systems Research. http://www.lasr.cs.ucla.edu/classes/239_3.spring06/Class_plan.xls

[5] C. Gamage. Computer and Network Security. Vrije Universiteit, Amsterdam. http://www.cs.vu.nl/~chandag

[6] P. McDaniel. Computer and Network Security. New York University, Stern School of Business. http://www.patrickmcdaniel.org/courses/nyu/b20-3157-sum05/

[7] P. McDaniel.. Computer Security. Pennsylvania State University, College of Engineering. http://www.cse.psu.edu/~cg543/

[8] S. Zdancewic. Computer and Network Security. University of Pennsylvania. http://www.cis.upenn.edu/~cis551/#topics#topics

[9] [9] I. Petre. Cryptography and Network Security. Abo Akademi University. http://www.abo.fi/~ipetre/crypto/

[10] M. Wright. Internet Security. The University of Texas at Arlington. http://ranger.uta.edu/~mwright/inetsec/syllabus.html

[11] S. Goldwasser. Network and Computer Security. Massachusetts Institute of Technology. http://theory.csail.mit.edu/classes/6.857/lecture.html

[12] A. Arora. Network Security. Ohio State University. http://www.cse.ohio-state.edu/~anish/694K.html

[13] D. Frincke. Network Security. University of Idaho. http://www.csds.uidaho.edu/deb/

[14] E. S. Al-Shaer. Network Security I. Multimedia Networking Research Laboratory (MNLAB). http://www.mnlab.cs.depaul.edu/~ehab/Courses/TDC572/

[15] J. Xu. Network Security. College of Computing Georgia Institute of Technology. http://www.cc.gatech.edu/classes/AY2003/cs6262_spring/

[16] J. Leiwo. Network Security. Vrije Universiteit, Amsterdam. http://www.cs.vu.nl/~nb/

[17] K. Kim. Network Security. Information and Communications University. http://eng.icu.ac.kr/curriculum/curri21_l.asp?year=2003

[18] M. Wright. Network Security. The University of Texas at Arlington. http://ranger.uta.edu/~mwright/netsec/syllabus.html

[19] W. Lee. Network Security. Georgia College of Computing. http://www3.cc.gatech.edu/classes/AY2006/cs6262_spring/

[20] [20] P. Mateti. Internet Security. Wright State University. http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/Top/index.html

Analysis of problematic of computer networks system security

A lot of lectures topics of security computers network are analyzed and frequencies of topics are counted. Themes are used to do a table of contents of lectures of security computers network. Classification by that has been made, using search by keywords or their combinations.