VILNIAUS UNIVERSITETAS

KAUNO HUMANITARINIS FAKULTETAS

INFORMATIKOS KATEDRA

Verslo informatikos studijų programa

Kodas 62109P101

INGRIDA URMANAVIČIŪTĖ

MAGISTRO BAIGIAMASIS DARBAS

DUOMENŲ APSAUGOS PRIEMONIŲ KOMPIUTERIZUOTO PARINKIMO IR ĮVERTINIMO METODIKA

Kaunas 2010

VILNIAUS UNIVERSITETAS

KAUNO HUMANITARINIS FAKULTETAS

INFORMATIKOS KATEDRA

INGRIDA URMANAVIČIŪTĖ

MAGISTRO BAIGIAMASIS DARBAS

DUOMENŲ APSAUGOS PRIEMONIŲ KOMPIUTERIZUOTO PARINKIMO IR ĮVERTINIMO METODIKA

Leidžiama ginti _____

Magistrantas _____
(parašas)

Darbo vadovas _____
(parašas)

dr. doc. Vitolis Sekliuckis
(darbo vadovo mokslo laipsnis, mokslo pedagoginis vardas, vardas ir pavardė)

Darbo įteikimo data _____

Registracijos Nr._____

Kaunas 2010

TURINYS

SANTRUMPŲ SĄRAŠAS

„ActiveX“ – technologijų rinkinys, skirtas keistis duomenimis tarp įvairių programų

ACL (angl. Access Control Lists) - Prieigos kontrolės sąrašai

ALG (angl. Aplication Layer Gateway) - Sietuvai

ARP (angl. Address Resolution Protocol) – Adreso rezoliucijos protokolas

DAP – Duomenų apsaugos priemonė

DHCP (angl. Dynamic Host Configuration Protocol) - Dinaminis stočių konfigūravimo protokolas

DMZ (angl. Delimitarized Zone) delimitarizuota zona

ICMP (angl. Internet Control Message Protocol) – Internet tinklo valdymo pranešimų protokolas

IDS (angl. Intrusion detection system) – Įsibrovimų detektavimo sistema

IE (angl. Internet Explorer) – Interneto naršyklė

IEEE – Elektrotechnikos ir Elektronikos inžinierių institutas

IP (angl. Internet Protocol) – Interneto protokolas

IPS (angl. Intrusion detection system) - Įsilaužimo prevencijos sistema

IPsec (angl. IP Security) – tuneliavimo protokolas

IS – Informacinė sistema

IT – Informacinės technologijos

KO - kuriamas (projektuojamas) objektas

L2 – antras arba ryšio lygis pagal OSI modelį, aprašantis ryšį tarp gretimų tinklo komponentų.

L3 – trečias arba tinklo lygis pagal OSI modelį, aprašantis kaip duomenų sekos turi būti perduodamos visame tinkle.

L4 – ketvirtas arba taikymo lygmuo pagal OSI modelį, aukščiausias lygmuo, apibrėžiantis tinklo teikiamas paslaugas vartojo programoms.

MPLS (angl. Multi-Protocol Label Switching) – Paketų su žymėmis komutavimo technologija

NAT (angl. Network Adress Translation) - Tinklo adresų transliavimas

OS – Operacinė sistema

OSI (angl. Open Systems Interconnection Reference Model) modelis – abstraktus ryšio protokolų, naudojamų ryšio ir kompiuteriniuose tinkluose, aprašymas.

PAT (angl. Port Address Translation) – Prievadų adresų transliavimas

PĮ – Programinė įranga

PKI (angl. Public Key Infrastructure) - Viešojo rakto infrastruktūra

SPAN (angl. Switched Port Analyser) – komutuojamo priedo analizatorius

ST - struktūrinis tipas

TCP (angl. Transmission Control Protocol) – Transporto valdymo protokolas

TSE – tipinis struktūrinis elementas

TSEK – tipinių struktūrinių elementų katalogas

UPS (angl. Uninterrupted Power Supply) – Nepertraukiamos energijos tiekimo šaltinis

VLAN (angl. Virtual LAN) – Vietinio tinklo virtualūs potinkliai

VPN (angl. Virtual private Network) – Virtualus privatus tinklas

VRF (Virtual Routing and Forwarding) – Virtualus maršrutų parinkimas ir perdavimas

SUMMARY

Data protection systems in the functioning of the organization in a particular area, highlights the problems and challenges: of the large number of existing data protection types and their implementations to select appropriate; objectively evaluate the selected set of data protection measures to ensure the safety functions of quality; develop a set of data protection measures the relative evaluation method that is user friendly.

The main goal of the paper is to propose a methodology to ensure data security measures and evaluation of computerized prescribing.

The main tasks to reach this goal are: to know the ways how security of the computer system can be impinging and how to protect from it, to do analysis trying to know what methods of data security are usable at the moment, propose measures to safeguard the data selection and computer-based assessment methodology for the security measures compared to alternative.

While writing the paper, various methods, such as induction and deduction, data comparison method, generalization method were used.

During the period of implementation practical part of the work completed all main tasks. Proposed data protection computer selection and evaluation methodology to compare alternative security measures. The method of data protection measures to facilitate the selection and evaluation, in accordance with user-friendly criteria.

The length of this paper is 78 pages; there are 8 pictures and 34 tables in this paper.

PAVEIKSLŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

ĮVADAS

Duomenų apsaugos konkrečioje taikymo srityje įgyvendinimas – sudėtinga ir persipynusi saugos priemonių visuma. Tos priemonės priklauso viena nuo kitos. Priklausomai nuo įmonės darbo vietų skaičiaus, geografinio išsidėstymo ir tinklo darbo intensyvumo priklausys duomenų apsaugos užtikrinimo priemonių parametrai ir duomenų srautai. Duomenų apsaugos sistemas organizuojant konkrečioje funkcionavimo srityje, išryškėja šios problemos ir spręstini uždaviniai: iš didelio kiekio egzistuojančių duomenų apsaugos priemonių tipų bei jų realizacijų atrinkti tinkamas, objektyviai įvertinti pasirinkto duomenų apsaugos priemonių rinkinio užtikrinančių saugą funkcijų kokybę, sukurti duomenų apsaugos priemonių rinkinio kompiuterizuoto įvertinimo metodiką.

Taigi šio mokslinio tiriamojo darbo tikslas pasiūlyti duomenų apsaugos priemonių kompiuterizuoto parinkimo ir įvertinimo metodiką. Problemų sprendimui siūloma naudoti struktūrinio projektavimo principus, kurių dėka, gali būti išsprendžiama duomenų apsaugos priemonių pritaikomumo ir suderinamumo problema. Nustatysime organizacijos duomenų apsaugai užtikrinti reikalingų galimų sprendimų rinkinį. Pateiksime kiekybinius šio rinkinio elementų įvertinimo kriterijus.

Darbo objektas: duomenų apsaugos priemonės.

Darbo tikslas – pasiūlyti metodiką, užtikrinančią duomenų apsaugos priemonių kompiuterizuotą parinkimą ir įvertinimą.

Uždaviniai:

1. Ištirti ir suklasifikuoti grėsmes kylančias duomenų saugumui;
2. Išnagrinėti ir suklasifikuoti duomenų apsaugos technologijas ir priemones;
3. Apžvelgti duomenų apsaugos ir rizikos valdymo aspektus;
4. Pasiūlyti duomenų apsaugos priemonių kompiuterizuoto parinkimo ir įvertinimo metodiką, skirtą alternatyvioms apsaugos priemonėms palyginti ir įvertinti;
5. Parodyti šios metodikos realizavimo galimybes.

Darbą sudaro trys pagrindinės dalys: teorinė dalis, metodinė dalis bei eksperimentinis tyrimas. Pirmojoje darbo dalyje pateikta grėsmių kylančių duomenų saugumui klasifikacija, aprašytos išnagrinėtos ir suklasifikuotos duomenų apsaugos technologijos bei priemonės, apžvelgti metodai, kurių pagalba galima įvertinti kompiuterinės sistemos saugumą. Antroje darbo dalyje aprašyta kompiuterizuoto parinkimo ir įvertinimo metodikos kūrimo principai. Paskutinė darbo dalis – eksperimentinė, kurioje aprašytas pasiūlytos metodikos pritaikymas bandant parinkti ir įvertinti pasirinktą duomenų apsaugos priemonių rikinį.

Darbe naudota 2002 – 2010 metų literatūra: knygos, moksliniai straipsniai, internetiniai šaltiniai. Literatūros sąrašas yra sudarytas iš trijų kalbų šaltinių.

Darbe panaudoti metodai: dedukcijos metodas (naudotas temą suskaidant į smulkesnes dalis), palyginimo metodas (naudotas lyginant duomenų apsaugos priemones, duomenų saugumo įvertinimo metodus), apibendrinimo metodas (naudotas apdorojant pirminę informaciją), pilnosios indukcijos metodas (naudotas rašant darbo išvadas).

Darbą sudaro trys pagrindinės dalys, bei 4 priedai. Darbo apimtis 78 psl. Darbe panaudota: 11 formulių, 8 paveikslėliai, 34 lentelės.

1. DUOMENŲ APSAUGOS PRIEMONIŲ IR JŲ ĮVERTINIMO ASPEKTŲ ANALIZĖ

Duomenų apsaugos problema tampa vis aktualesnė kiekvienai įmonei ar organizacijai. Tai susiję su plačiu įvairių IT taikymu organizacijos veikloje bei rinkos globalizacija ir organizacijų bendradarbiavimo didėjimu. Duomenys, saugomi elektroninėje terpėje ir perduodami elektroninio ryšio kanalais, gali būti daug lengviau pasiekiami arba sugadinti, jei nėra tinkamai apsaugoti. Nustojus veikti IT sistemoms ar praradus jose saugomus duomenis, gali sutrikti organizacijos veikla. Labai svarbu imtis priemonių, kurios apsaugo įmonės informacinius resursus ir patį verslą nuo galimų grėsmių: konfidencialios informacijos vagysčių ar paviešinimo, duomenų sunaikinimo, darbo sutrikdymo.

Saugumui užtikrinti kompleksiškai turi būti nuolat naudojamos administracinės, technologinės (loginės) bei fizinės DAP. Šiandien taikomi įvairūs verslo saugumo sprendimų būdai – nauji produktai ir technologijos, naujos metodikos. Techniniai duomenų apsaugos sprendimai kainuoja nemažai pinigų. Specialistų ratas, kuris svarsto šią problemą – dažniausiai techninis personalas. Šiame lygmenyje problema suvokiama pakankamai gerai. Verslo struktūrose, generuojančiose pinigų srautus, šios grėsmės nėra taip aiškiai fiksuojamos, duomenų apsaugos supratimas čia miglotas. Todėl klausimas, kam reikalingos išlaidos sistemai, su kuria neuždirbami pinigai, kyla natūraliai. IT specialistai problemos sprendimą gvildena techniniam lygyje ir – savaime suprantama – techniniais terminais, įvardindami standartinių komponentų rinkinį: antivirusinę PĮ, užkardas, VPN ir t.t. Bet techninė kalba tolima nuo biznio kalbos, o aiškinimas techninėmis kategorijomis neperspektyvus, nes eiliniai IT vartotojai paprasčiausiai jų nesupras [25]. Kalbant apie duomenų apsaugą, iškyla būtinumas grėsmių identifikavimui, silpnųjų vietų nustatymui, rizikos vertinimui, galimų nuostolių paskaičiavimui ir tinkamų DAP pasirinkimui.

1.1. Grėsmių kylančių duomenų saugumui identifikavimas ir klasifikacija

Saugumo pažeidimai atsiranda iš tyčinės ir netyčinės veiklos, o jų padariniai yra tiesioginiai finansiniai nuostoliai, sumažėjęs darbo veiksmingumas arba reputacijos praradimas.

Grėsmė - tai potencialiai galimas įvykis, kuris gali nepageidautina linkme paveikti sistemą, jos elementus ar ryšius tarp sistemos elementų. Su tuo glaudžiai susijusi pažeidžiamumo sąvoka. Sistemos pažeidžiamumas - tai tam tikra nepageidaujama sistemos charakteristika, kuri savo buvimu leidžia atsirasti grėsmei. Dažniausiai, dėl sistemos pažeidžiamumo įvyksta nepageidaujami įvykiai. Atakos terminu apibrėžiamas sąmoningas veiksmas, nukreiptas siekiant pažeisti sistemos saugumo reikalavimus. Sistemos ataka – tai sąmoningi asmens arba jų grupės veiksmai, skirti

sistemos pažeidžiamumų paieškai ir jų panaudojimui savo, kitų interesams, įvairiems kenkėjiškiems tikslams.

Šiuo metu internetu plintančių grėsmių daugėja. FTB (Federalinis tyrimų biuras – JAV nusikaltimų tyrimo ir žvalgybos agentūra) vis daugiau dėmesio skiria tokiems nusikaltimams, nes virtualioje erdvėje vykstantys incidentai dažniausiai vykdomi siekiant materialinės naudos ir atneša vis daugiau nuostolių kompanijoms bei privatiems asmenims. Šiuos nusikaltimus sunku atskleisti, nes jiems reikia įvairių šalių teisėsaugos struktūrų bendradarbiavimo, dėl pastarųjų vykdymo tarptautiniu mastu. Lietuvoje kaip ir kai kuriose kitose šalyse baudžiamajame kodekse nėra punkto, apibrėžiančio sankcijas, taikomas vykdant virtualius nusikaltimus [3]. Todėl nusikaltėliai gali ir toliau veikti nebaudžiami.

Viena didžiausių grėsmių internete yra ***kenksminga programinė įranga***:

Kompiuterių virusai – specialiai parašytos, nedidelės programos, sukuriančios savo kopijas ir įrašančios jas į kitas kompiuterio programas, diskinių kaupiklių sektorius, tvarkykles ir pan.

„Kirminai“ (angl. worm) – savarankiškos programos, panašios į virusus, plintančios autonomiškai tinklu, dažniausiai elektroniniu paštu arba naudodamiesi programinės įrangos spragomis [3].

„Trojos arkliai“ (angl. Trojan horse) – programos, turinčios kenksmingų funkcijų. Jos dažnai sudaro vartotojui naudingos ar įdomios programinės įrangos įspūdį. „Trojos arkliai“ ne visada slepiasi, jie gali patekti į sistemą naudodamiesi interneto naršyklės spraga [3]. „Trojos arkliai“ į atakuojamą sistemą patenka socialinės inžinerijos būdu ir leidžia įsilaužėliui perimti sistemos kontrolę.

Šnipinėjimo programinė įranga (angl. spyware, adware), kuri stebi vartotojo kompiuterį ir kontroliuoja sistemą. Šnipinėjimo PĮ nesidaugina ir yra įdiegiama žinant vartotojui, pvz., kai lankomasi svetainėje naudojant naršyklę IE, gali būti siūloma įdiegti „ActiveX“ komponentą. Šiuo metu populiaresnis yra atskirų programų paketų platinimas kartu su šnipinėjimo PĮ [3].

Dažnai kenkėjiška PĮ veikia automatiniu būdu ir plinta pati. Vartotojas gali ir nežinoti kada jo kompiuteris yra „užkrėstas“. Dažnai tokios programos plinta pasinaudodamos įvairiomis spragomis, todėl reikia kuo dažniau atnaujinti programinę kompiuterio įrangą [3].

Įsilaužimai. Įsilaužimus per internetą galima išskirti į informacijos rinkimą ir patį įsilaužimą. Renkant informaciją siekiama sužinoti, kokios OS naudojamos, kokias atviras jungtis įmonės turi, kokia sisteminė ir taikomoji PĮ įdiegta, kaip ji sukonfigūruota. Pagal šiuos duomenis nustatomos pažeidžiamiausios sistemos vietos ir jų puolimo taktika. Informacijos vagystės dažnai atliekamos naudojantis kenksminga PĮ [3].

DoS ataka (angl. Denial of Service) — atsisakymas aptarnauti ir ***DDoS-ataka*** (angl. Distributed Denial of Service) — paskirstytas atsisakymas aptarnauti. Tai atakų prieš kompiuterines

sistemas rūšys. Jų tikslas yra sukurti tokias sąlygas, kad teisėtiems sistemos naudotojams jos ištekliai taptų neprieinami ar apsunkinamas jų gavimas. DDoS atakos gali būti naudojamos ir kaip priedanga kenksmingų šnipinėjančių programų įdiegimui, kuriomis gauta informacija perduodama konkurentams. Jos ypač skaudžiai atsiliepia, pavyzdžiui, kompanijoms, užsiimančioms telekomunikacijomis ir jos sau tiesiog negali leisti tapti piktavalių aukomis. Apsauga nuo DDoS atakų ypač svarbi internetinėms parduotuvėms, tinklaraščių tarnyboms, naujienų tarnyboms ir kitoms kompanijoms, kurių veiklai būtina, kad jų tinklalapiu nuolat galėtų naudotis klientai [2][8].

Socialinė inžinerija internetu. Socialinei inžinerijai internetu priskiriami duomenų vagystės būdai: slaptažodžio žvejyba (angl. Phishing), trumpųjų žinučių sukčiavimai (angl. Smishing), internetinės balso telefonijos sukčiavimai (angl. Vishing), apgaulingas laiškas (angl. Scam), nepageidaujami elektroniniai laiškai (angl. Spam) [3][5][21].

Nagrinėjant pavojus, į duomenų apsaugą reikia pažvelgti plačiau. Informacinės vertybės – tai materialieji ir nematerialieji ištekliai, kurie padeda individui arba įstaigai sėkmingai vykdyti veiklą. Kad informacinės vertybės liktų saugios, reikia atkreipti dėmesį į tris pagrindinius elementus, kurie užtikrina saugumą:

- Konfidencialumą – informacijos slaptumas, kreditinės kortelės numeriai, slaptažodžiai;
- Vientisumą – informacija nėra leistinai pakeičiama saugant arba persiunčiant;
- Pasiekiamumą – informacija pasiekiama įgaliotam vartotojui tada, kada jos reikia.

Grėsmes galima suskirstyti pagal jas sukeliančius gamtos, technologinius, infrastruktūrinius ir žmoniškuosius veiksnius. Nors gamtos, infrastruktūriniai ir technologiniai veiksniai yra svarbūs, didžiausią grėsmę duomenų saugumui kelia žmonės. Dažnai yra manoma, kad kompiuterių sistemose apdorojamiems duomenims didžiausią grėsmę kelia kompiuterių įsibrovėliai iš interneto. Statistiniai duomenys rodo, kad apie 80 procentų visų kompiuterinių įsibrovimų įvykdo patys įstaigos darbuotojai [38].

Pažeidžiamumas yra informacinės vertybės netinkama apsauga nuo konkrečios grėsmės. Kai grėsmės sukėlėjas išnaudoja informacinės vertybės pažeidžiamumą, informacinei vertybei yra padaroma žala. Žala gali būti tiek materiali (sugadintas turtas), tiek nemateriali (įvaizdžio, laiko praradimas). Pažeidžiamumus galima suskirstyti į grupes, pagal juos išnaudojančius sukėlėjus: gamtos, infrastruktūrinius, technologinius ir žmoniškuosius veiksnius.

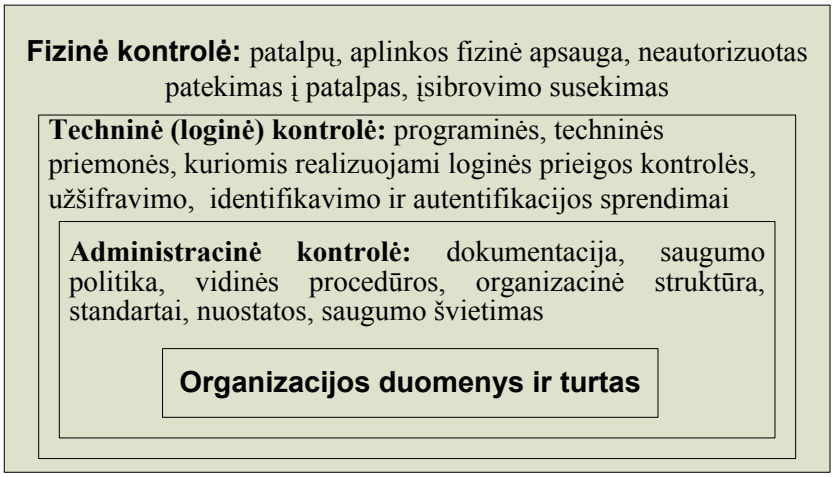
1.2. Duomenų apsaugos technologijos ir priemonės

Duomenų apsauga nuo aprašytų grėsmių pasiekiama taikant šias apsaugos priemonių rūšis:

- Administracines;

- Technologines (dar vadinamas loginėmis);
- Fizines [1] [2] [13] [26].

Šie trys kontrolės tipai formuoja pagrindą ant kurio kuriama nuodugnaus saugumo strategija. Tokiu būdu nuodugni apsauga gali būti suvokiama kaip trys skirtingi vienas ant kito sudėti sluoksniai:



Šaltinis: sukurta autorės pagal Harris S. (2005) CISSP, p. 55.

1 pav. Organizacijos duomenų ir turto administracinė, techninė ir fizinė apsauga

Administracinė kontrolė formuoja pagrindą parinkti ir įdiegti techninę (loginę) ir fizinę kontrolę. Techninė (loginė) ir fizinė kontrolės yra administracinės kontrolės pasireiškimas. Administracinė kontrolė yra laikoma pirmaeilės svarbos priemone. Techninė (loginė) kontrolė naudoja PĮ ir duomenis prieigai prie informacijos ir kompiuterinių sistemų kontroliuoti. Pavyzdžiui: slaptažodžiai, užkardos (angl. Firewall), IDS, ACL ir pasikėsinimas į duomenis yra techninės (loginės) kontrolės sritis [13].

Kartu su tradicinėmis DAP ypatingas dėmesys turi būti skiriamas IS ir ryšio tinklų saugos priemonėms parinkti ir valdyti. Šiuo aspektu duomenų apsaugą galima apibrėžti kaip elektroninių ryšių tinklo ar IS gebėjimu patikimai išsaugoti perduodamus elektroninius duomenis nuo pavojų, užtikrinti jų prieinamumą, tapatumą, vientisumą ir garantuoti jų slaptumą [1].

Duomenų apsaugos valdymas – tai nesibaigiantis sistemingas procesas, kuris turi būti nuolat kontroliuojamas, peržiūrimas ir atnaujinamas atsižvelgiant į rinką, įmonės tikslus ir strategiją, saugumo reikalavimus, IT kaitą [1].

Renkantis DAP reikėtų išskirti du duomenų apsaugos sprendimų būdus: tinklo ir kompiuterio apsaugos sprendimus. Kompiuterio apsaugos sprendimai priimami pasirenkant atitinkamas administracines, technologines (logines), fizines apsaugos priemones. O tinklo apsaugos sprendimai gali būti nagrinėjami kaip atskira apsaugos priemonių taikymo rūšis.

1.2.1. Technologijų užtikrinančių duomenų apsaugą tinkle klasifikavimas

Tinklo saugumui užtikrinti naudojamos įvairios priemonės ir technologijos. Tinklo protokolams ir technologijoms klasifikuoti gali būti naudojami įvairūs klasifikavimo metodai. Vienas iš jų – ***klasifikavimas pagal tinklo saugos funkcinius elementus***, kurie naudojami projektuojant tinklus. Šie funkciniai elementai atitinka pagrindines informacijos saugumo sąvokas: konfidencialumą, tapatybės patikrinimą, įgaliojimų ir teisių patikrinimą, atsakomybės pripažinimą, informacijos vientisumą.

1 lentelė

Tinklo saugumo funkciniai elementai pagal pagrindines informacijos saugumo sąvokas

Informacijos saugumo sąvoka	Duomenų apsaugos priemonės
Konfidencialumas	Šifravimo metodai ir protokolai
Tapatybės patikrinimas	Metodai ir protokolai
Įgaliojimų ir teisių patikrinimas	Autorizacijos metodai
Atsakomybės pripažinimas	Tinklo technologijos ir metodai
Informacijos vientisumas	Tinklo technologijos ir protokolai

Šaltinis: sudaryta autorės pagal Garla E., Dubovskaja V. (2008) Kompiuterinių tinklų projektavimas, p. 124.

Tinklo saugos technologijos pagal funkcinių elementų sudėtingumą gali būti padalintos į keturias grupes:

2 lentelė

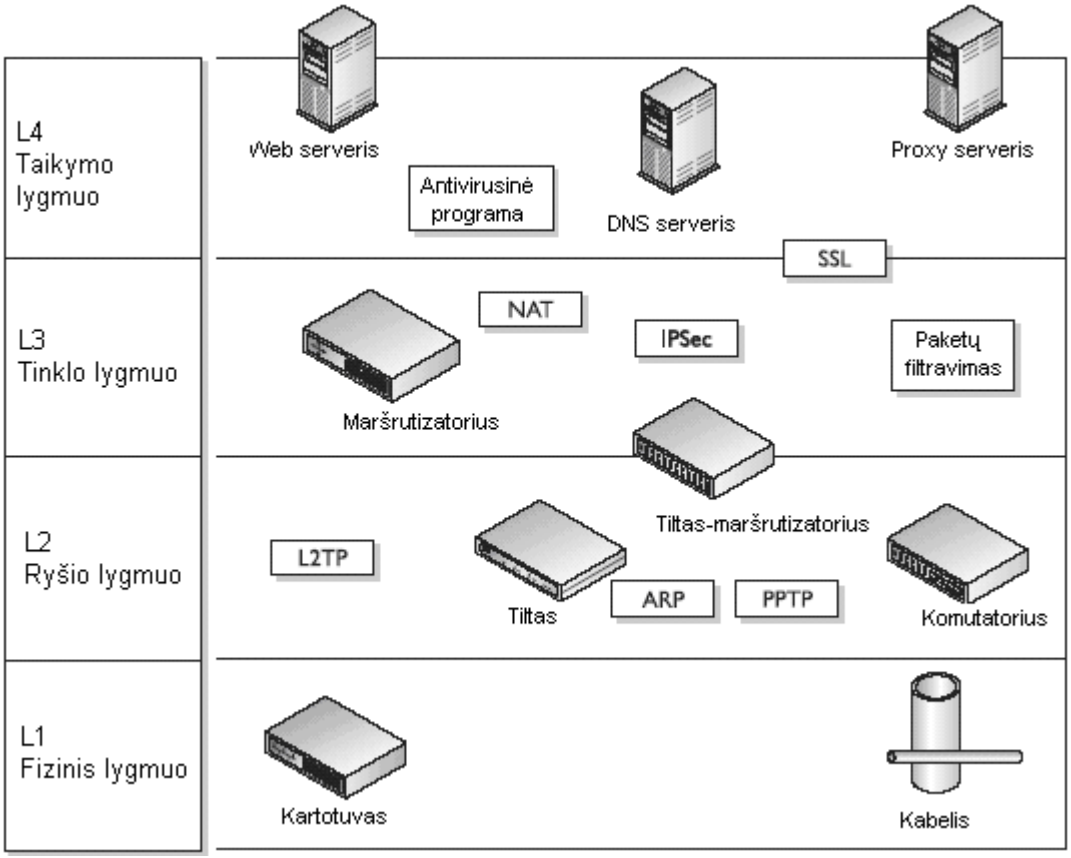
Tinklo saugos technologijų klasifikacija pagal funkcinių elementų sudėtingumą

Tinklo saugos technologijų grupė	Aprašymas	Technologijos pavyzdžiai
Bazinės	Skirtos vienai kokiai nors apsaugos funkcijai užtikrinti	L2 VPN, maršrutizatoriaus ACL
Patobulintos	Skirtos vienai funkcijai užtikrinti, dažnai besiremiančios kitomis bazinėmis technologijomis	Elektroninis parašas
Integruotos	Jungia kelias bazines ar patobulintas technologijas, skirtos veikti su keliais funkciniais elementais	IPsec VPN
Saugos architektūros	Tai bazinių, patobulintų ir integruotų technologijų sistemos, kurios atlieka kelias saugos funkcijas	PKI

Šaltinis: sudaryta autorės pagal Garla E., Dubovskaja V. (2008) Kompiuterinių tinklų projektavimas, p. 124.

Toks klasifikavimas gali lengviau padėti suprasti šias technologijas ir taikyti jas kuriant saugos sistemas. Tinklo saugumo technologijų yra daug, todėl apsiribosiu tik šiuo metu labiausiai paplitusių technologijų taikymo aprašu, kurių funkcijas gali realizuoti atitinkami tinklo įrenginiai (žr. 3 lentelę).

Tinklo saugos priemonių naudojamų saugumui nuo pažeidžiamumo skirtinguose OSI lygiuose pateiktas 2 paveiksle.



Šaltinis: sudaryta autorės pagal Harris S. (2005) CISSP, p. 26.

2 pav. Grafinis įrangos ir protokolų atvaizdavimas OSI modelyje

3 lentelė

Tinklo įrenginiai realizuojantys tinklo saugos sprendimų ir technologijų funkcijas

Tinklo saugos sprendimai ir technologijos	Komutatorius (Switch)	Maršrutizatorius (Router)	Užkarda (Firewall)	Integruotas saugumo įrenginys (Appliance)
Fizinis ir loginis tinklo segmentavimas	+	+	+	+
Filtravimas ir ACL		+	+	+
NAT		+	+	+
Tinklo prieigos kontrolė pagal 802.1x standartą	+			
DMZ		+	+	+
Užkarda		+	+	+
PKI technologijos		+	+	+
IPS			+	+
IPSEC ir MPLS VPN technologijos		+	+	+

Šaltinis: sudaryta autorės pagal Garla E., Dubovskaja V. (2008) Kompiuterinių tinklų projektavimas, p. 125.

Toliau išsamiau apibūdinsime tinklo saugos sprendimus ir technologijas, kurios buvo išvardintos 3 lentelėje.

Fizinis ir loginis tinklo segmentavimas. Vienas iš efektyviausių būdų užtikrinti vartotojų prieigos prie tinklo resursų kontrolę. Fizinio ir loginio tinklo segmentavimo ypatumų palyginimas pateiktas 4 lentelėje.

4 lentelė

Fizinio ir loginio segmentavimo palyginimas

Palyginimo aspektai	Fizinis segmentavimas	Loginis segmentavimas
Resursai	Reikalingi papildomi resursai	-
Tinklas	Tinkluose su dideliais saugumo reikalavimais	Mažuose arba vidutiniuose tinkluose segmentuojama L2. Dideliuose L2 ir L3, pvz. maršrutizatorius, L3 komutatorius, užkarda ir pan.
Paskirtis	Atskirti įmonės tinklą, bevielį tinklą, svečiams skirtą tinklą	Tinklo resursų ir vartotojų grupavimas į atskirus loginius segmentus: vidinio tinklo, bevielės prieigos taškų, L2 į VLAN

Šaltinis: sudaryta autorės pagal Garla E., Dubovskaja V. (2008) Kompiuterinių tinklų projektavimas, p. 126.

Filtravimas ir ACL. Maršrutizatorių ir užkardų vykdomoji funkcija ir gali būti atliekamas skirtinguose OSI lygmenyse. Filtravimas remiasi ACL ir nurodo, koks duomenų srauto tipas praleidžiamas į tinklo sąsają arba iš jos pagal tam tikras paketo charakteristikas, pvz., gavėjo adresai, protokolas, prievadas. Tai vienas efektyviausių būdų užtikrinti vartotojų prieigos prie tinklo resursų kontrolę.

NAT. Tai dar viena tinko technologija, leidžianti apsaugoti tinklo resursus nuo išorės veiksnių. Jei tinklas turi daug viešųjų adresų, labai dažnai jie priskiriami tarnybinėms ir darbo stotims be NAT. Dėl saugumo rekomenduojama visai įrangai vidiniame tinkle ir DMZ zonoje naudoti privačiuosius adresus ir transliuoti juos pagal poreikį į viešuosius IP adresus. Taikant NAT technologiją, galima daug paprasčiau ir lanksčiau kontroliuoti interneto srautus, ypač tada kai tinklo vartotojų yra daug.

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

DMZ. Tai prieigos kontrolės valdymo priemonė, leidžianti užtikrinti viešųjų serverių apsaugą. DMZ zonoje montuojami serveriai su viešomis paslaugomis arba vadinamieji tarpiniai (angl. proxy) serveriai, kurie atlieka tarpininko funkciją ir nustato dviejų žingsnių sujungimus tarp nutolusių vartotojų ir įmonės serverių, prie kurio jungiasi išoriniai vartotojai, ir taip pat padeda apsaugoti serverius nuo atakų iš išorės.

Užkarda. Pagrindinė prieigos valdymo priemonė. Apsaugo įmonės vidinį tinklą nuo įsibrovimų ir atakų. Tai programinė ir techninė įranga, kuri analizuoja ir valdo per ją einantį duomenų srautą ir yra skirta vidinio kompiuterių tinklo saugumui užtikrinti. Užkarda paremta paketų filtravimu, analizuojančiu paketų antraštę (angl. header) ir kontroliuojančią paketų judėjimą [27].

Tradicinė užkarda – įrenginys tarp vidinio ir išorinio tinklo, kuris atlieka ateinančių (kartais) išeinančių paketų filtravimą, remdamasis L3 (tinklo) ir L4 (taikomajame) pagal OSI informaciją paketų antraštėse (TCP, UDP, ICMP). Atsiradus naujoms saugumo grėsmėms, kurios naudoja kitas

technikas aukštesnio lygio protokolus (DNS, SMTP, POP3) šiuolaikinė užkarda gali atlikti žymiai daugiau funkcijų (žr.5 lentelę).

5 lentelė

Užkardos funkcijos

Privalomos funkcijos (verslo klasei)	Įprastos funkcijos	Papildomos funkcijos
Taikomojo lygmens filtravimas ALF (angl. Application Layer Filtering) apsaugai nuo: - Taikomojo lygmens atakų; - Virusų; - Nepageidaujamo pašto (angl. Spam);	Apsauga nuo DoS atakų	3DES šifruoti reikalinga licencija, turinio filtravimo funkcijai perkama „subscription“
Turinio filtravimas (angl. Content filtering) - blokuoja internetines svetaines pagal turinį, o ne IP adresus	NAT ir PAT transliavimas, vidiniam tinklui nuo išorinio paslėpti (trūkumas, kad ši technologija nemoka taisyklingai apdoroti protokolų, kurie saugo IP adresus paketo duomenų dalyje)	Svetainių įrašymas į atmintinę (angl. Web caching)
	VPN organizavimas	Centralizuotas valdymas ir ataskaitų formavimas
		Nepageidaujamo pašto filtravimas (angl. Spam filtering)
		Pasiekiamumo užtikrinimas (angl. High availability)
		URL filtravimas (angl. URL screening)
		Antivirusinės programos

Šaltinis: sudaryta autorės pagal Garla E., Dubovskaja V. (2008) Kompiuterinių tinklų projektavimas, p. 144.

Užkardų tipai:

Pagal paskirtį ir poveikio sritį užkardos skirstomos į:

- Personalines, kurios filtruoja įeinantį ir išeinantį duomenų srautą viename kompiuteryje.
- Tinklo, kurios filtruoja visą įeinantį ir išeinantį duomenų srautą tarp susijusių tinklų ir veikia dedikuotame tinklo įrenginyje ar kompiuteryje tarp dviejų ar daugiau tinklų ar delimitarizuotų zonų.

Pagal OSI modelio lygmenis užkardos skirstomos į:

- Tinklo lygmens (angl. Iptables);
- Taikomojo lygmens (angl. TCP Wrapper);
- Taikomosios arba operacinės sistemos.

Užkardų klasifikavimas pagal tipus, jų privalumai ir trūkumai pateikti 6 lentelėje.

6 lentelė

Užkardų klasifikavimas

Užkardos tipas	Tinklo lygmens	Taikymo lygmens	Charakteristikos	Privalumai / trūkumai
Ne visiškai taisyklingo jungimo (angl. Stateless)	+		Paketų filtravimas	Nedaro sudėtingų sprendimų, atsižvelgiant kuriame lygmenyje yra kompiuteriai. Šios užkardos funkcijas turi kiekvienas kompiuteris su OS (GNU/Linux, Solaris, BSD, MS Windows server) atliekantis paketų filtravimą ir maršrutizavimą.
Visiškai taisyklingo jungimo (angl. Statefull)	+		Sujungimų būsenos (pvz., nusistovėjusi, inicijuota, patvirtinta ar neįvykęs jungimas), laikinosios taisyklės	
Sietuvai ALG (angl. Aplication Layer Gateway)		+	Apsaugo klientų programas, nes veikia kaip tarpininkas tarp vidinio tinklo ir išorės	Labai saugios

Šaltinis: sudaryta autorės pagal Garla E., Dubovskaja V. (2008) Kompiuterinių tinklų projektavimas, p. 146. ir Harris S. (2005) CISSP, p. 492.

PKI technologijos. Naudojamos įmonėms, kurios turi geografiškai nutolusių padalinių, bevielio tinklo ar mobilių vartotojų. Tokiu būdu užtikrinami griežto identifikavimo sprendimai, kurie leidžia kontroliuoti prieigą prie įmonės vidaus tinklo per papildomas identifikavimo priemones. Prie tokių priemonių priskiriami šifravimo raktai ir sertifikatai. PKI plačiai naudojama elektroninėje komercijoje, bankininkystėje kaip ypatingai vertinama apsaugos priemonė, taip pat įmonės tinkluose kaip vartotojų tapatumo nustatymo mechanizmas.

IPS. Tinklo apsaugos įrenginys, kuris stebi tinklo ir/arba sistemos darbą piktavališkai ar nepageidaujamai veiklai ir gali reaguoti realiu laiku, užblokuodamas arba uždrausdamas šią veiklą [9]. IPS vaidmenį tinkle gali atlikti prieigos leidžiamumo ir taikomojo lygmens užkardos, tačiau tarp šių technologijų yra ryškių skirtumų. IPS rezultatai paprastai nėra IP adreso patvirtinimas apsaugotame tinkle, bet gali atsakyti visiems srautams įvairiais būdais. Nors IPS produktai turi galimybę įgyvendinti užkardos taisykles, tai dažnai tik patogumo ir nėra pagrindinė produktų funkcija. Be to, IPS technologija siūlo giliau pažvelgti į tinklo veiklą teikiant informaciją apie pernelyg aktyvius mazgus, blogus prisijungimus, netinkamo turinio ir daugelio kitų tinklo ir taikomojo sluoksnio funkcijų. Taikomosios užkardos atlieka tarpininko funkciją (angl. proxy) tinklo ir taikomojo lygmens srauto kreipčių valdymui apsaugoti. Taip pat kai kurios taikomojo lygmens užkardos turi integruotas IPS tipo paraiškas ir užtikrina srauto analizę ir blokavimą realiu laiku. Ne visos IPS atlieka pilnas tarpininko funkcijas (angl. full Proxy). Dėl to, taikomojo lygmens užkardos linkusios sutelkti dėmesį į užkardos pajėgumus, su papildoma IPS galimybe.

IPSEC ir MPLS VPN technologijos. Tai labiausiai šiuo metu paplitusios virtualių privačių tinklų technologijos. IPsec - tuneliavimo protokolas, kuris informacijos konfidencialumui, tapatumo

nustatymui ir vientisumui užtikrinti naudoja paketų inkapsuliacijos ir šifravimo metodus. Šis protokolas veikia tinklo lygmenyje ir skirtas tik IP srautui apsaugoti. MPLS – paketų su žymėmis komutavimo technologija ir protokolas, kurie plačiai naudojami interneto paslaugų tiekėjų ir didelio masto IP tinkluose. MPLS technologiją turi didelės spartos maršrutizatoriai [27].

Išvardinti tinklo saugumo sprendimai remiasi *ISO/IEC 27002* standarto rekomendacijomis. Dažniausiai keliami pagrindiniai tinklo saugumo politikos tikslai ir kryptys, kurių tikslams pasiekti tinkle naudojamos saugumą užtikrinančios priemonės ir technologijos:

7 lentelė

Tinklo saugumo projektavimo sprendimai ir technologijos pagal tinklo saugumo politiką

Tinklo saugumo politika	Tinklo saugumo priemonės
Užtikrinti apribojimus vartotojų arba įrangos naudojimąsi sistemų resursais pagal vartotojų arba įrangos poreikius ir funkcijas	Fizinis ir loginis tinklo segmentavimas; Paketų filtravimas ir ACL;
Apsaugoti tinklo resursus nuo nesankcionuotų vidinių ir išorinių vartotojų veiksmų ir DoS atakų	NAT, PAT; Tinklo prieigos kontrolė pagal 802.1x standartą; DMZ; Užkarda; IPS
Suteikti vartotojams galimybę saugiai naudotis sistemų resursais iš nutolusių darbo vietų	PKI technologijos
Susieti įmonės padalinius, prijungtus prie viešojo tinklo, į virtualųjį privatų tinklą, užtikrinus tokio tinklo saugumą ir perduodamų duomenų konfidencialumą ir vientisumą	IPsec/MPLS VPN įdiegimas

Šaltinis: sudaryta autorės

Lentelėje pateikti saugumo sprendimai ir technologijos, kurių įdiegimas padėtų pasiekti užsibrėžtus tinklo saugumo politikos tikslus. Pateikti tinklo saugumo sprendimai gali būti pritaikyti projektuojant naujus arba atnaujinant senus tinklus, o priemonių sąrašas gali keistis atsižvelgiant į tai, kokia tinklo architektūra ir informacijos saugos politika pasirinkta organizacijoje, taip pat keičiantis technologijoms ir atsirandant naujoms tinklo pažeidimo grėsmėms.

1.2.2. Papildomi technologiniai ir fiziniai apsaugos sprendimai

Kompiuterinis tinklas yra saugus kai visi jame esantys komponentai (kompiuteriai, serveriai, komutatoriai, maršrutizatoriai) yra tinkamai apsisaugoti. Reikalinga pasirinkti ir įdiegti apsaugos priemones kur kiekvienas tinklo elementas veikia kaip apsaugos taškas [27]. Kompiuterių apsaugą užtikrina techninės ir programinės apsaugos priemonės. Nuo įsibrovimo iš interneto apsaugo programinės užkardos, nuo virusų atakos – antivirusinė programinė įranga. Kompiuterių sistemose vartotojo tapatybė yra nustatoma pagal įvestą vartotojo vardą ir slaptažodį, o nustačius tapatybę, prieigą prie saugomos informacijos riboja skirtingos kiekvienam vartotojui suteiktos prieigos teisės. Elektroniniu paštu ar telefonu perduodamos duomenų saugumą užtikrina šifravimo priemonės [28].

Užšifruoti galima ir kompiuterio kietajame diske saugomus duomenis: kompiuterio vagystės atveju niekas negalės susipažinti su taip apsaugotos informacijos turiniu [26].

Apsaugos priemonės papildomai apsaugo nuo galimų grėsmių. Pavyzdžiui, nuo virusų ir įsilaužimo, kai naudojami paprasti komutatoriai, arba kai darbuotojas pats atneša duomenų laikmeną su užkrėstais failais. Atskiros apsaugos priemonės gali būti ir integruotos. Jos vadinamos kompleksinėmis programomis. Šios programos yra universalios ir gali apimti visą reikalingą apsaugos funkcijų rinkinį. Jei naudojamas vienas iš šių rinkinių, tai nereikės diegti papildomų apsaugos programų, tokių kaip apsaugos nuo šnipinėjimo programinės įrangos (angl. antispyware), užkardos, antivirusinės, apsaugos nuo nepageidaujamų elektroninių laiškų (angl. anti-spam), IDS ar kitų. Integravus tokią kompleksinę sistemą, kompiuteriai bei visa informacija bus apsaugoti nuo virusų ir įsilaužėlių žalingo poveikio, o tinklas bus apsaugotas ne tik perimetre (išėjimas į internetą), bet ir kiekviename sujungimo taške.

Tos pačios srities DAP panašios pagal atliekamas pagrindines funkcijas, tačiau skiriasi kokybinėmis ir kiekybinėmis charakteristikomis, papildomu funkcionalumu. Yra išskiriami pagrindiniai DAP pasirinkimo kriterijai. Pavyzdžiui, svarbūs užkardos pasirinkimo kriterijai:

- Srauto spartos parametras. Srauto sparta yra apibrėžiama kaip duomenų perduodamų per sekundę, kiekis. Užkardų pralaida gali keistis nuo 150Mbs iki 1Gbps ir daugiau;
- Aptarnaujamų vartotojų kiekis (dabar ir ateityje);
- VPN vartotojų kiekis (dabar ir ateityje);
- Svetainių įrašymas į atmintinę;
- Papildomų funkcijų vykdymas kituose serveriuose, pvz., „off box“ (nuimamas užkardos procesoriaus apkrovimas).

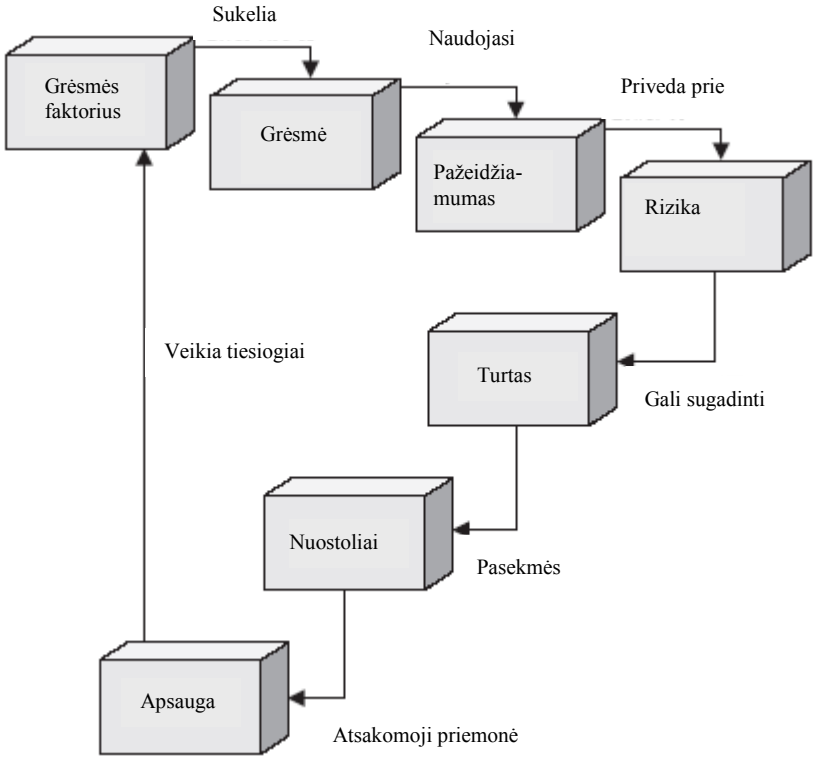
1.3. Duomenų apsaugos ir rizikos valdymo aspektai

Planuodama investicijas saugai organizacija turi atidžiai įvertinti savo IS pažeidžiamumą, grėsmes ir riziką, kylančią jos turimai informacijai ir kompiuterinėms sistemoms. Efektyviausią apsaugą užtikrina apgalvotas ir konkrečiai organizacijai pritaikytas techninių, programinių ir organizacinių priemonių rinkinys – sprendimų visuma, sudaranti saugumo sistemą. Pagrindinė jos funkcija yra užtikrinti IS ir jose saugomos informacijos vientisumą, konfidencialumą ir prieinamumą. Reikia priimti esminius sprendimus: kokie duomenys ir nuo ko turi būti saugomi, kokie yra prioritetai, koks priimtinas saugumo lygis.

Duomenų apsaugos valdymas – tai nesibaigiantis sistemingas procesas, kuris turi būti nuolat kontroliuojamas, peržiūrimas ir atnaujinamas atsižvelgiant į rinką, įmonės tikslus ir strategiją, saugumo reikalavimus, IT kaitą [1][7]. Saugios tinklo architektūros įvertinimas atliekamas

sistemingai atsižvelgiant į galimas kilti grėsmes organizacijos duomenims ir turtui. Grėsmės pasinaudodamos sistemos pažeidimais arba jų silpnosiomis vietomis priveda prie rizikos, jog gali sukelti organizacijos duomenų ar turto pažeidimus, kurių pasekmė – nuostoliai. Šiems galimiems nuostoliams išvengti naudojamos DAP, kurios tiesiogiai veikia grėsmės faktorius.

Norint geriau suvokti pavojus duomenims, reikėtų aptarti ryšius tarp informacinių vertybių, joms gresiančių grėsmių, jų sukėlėjų, pažeidžiamumų ir galimos žalos. Sekančiame paveiksle pateikti ryšiai tarp grėsmių, pažeidžiamumo, rizikos, ir apsaugos priemonių:



Šaltinis: sukurta autorės pagal Harris S. (2005) CISSP, p. 61.

3 pav. Ryšiai tarp skirtingų apsaugos komponentų

Remiantis šia metodika iškyla būtinumas grėsmių identifikavimui, silpnųjų vietų nustatymui, rizikos vertinimui, galimų nuostolių paskaičiavimui ir tinkamų apsaugos priemonių pasirinkimui.

1.3.1. Duomenų apsaugos įvertinimo kriterijai

Sukurti efektyvią informacijos valdymo sistemą ir pasirinkti tinkamas saugumo valdymo priemones padeda standartai, teikiantys rekomendacijas, kaip apsaugoti įmonių ir organizacijų informacinį turtą:

- *ISO/IEC 27000* standartų serija, kurią sudaro standartai, skirti saugumo reikalavimams, rizikos valdymui, saugos įgyvendinimo priemonėms aprašyti.

Standartas sudarytas iš įvadinio skyriaus, kuriame aprašomas rizikos vertinimas ir priežiūra, 11 saugumo valdymui skirtų poskyrių, kuriuose nurodomi 39 pagrindiniai saugumo valdymo tikslai ir daugybė saugumo rekomendacijų:

- saugumo politika;
- duomenų apsaugos organizavimas;
- turto valdymas;
- žmogiškųjų išteklių sauga;
- fizinė ir aplinkos sauga;
- ryšių ir operacijų valdymas;
- prieigos valdymas;
- IS komplektavimas;
- duomenų saugumo incidentų valdymas;
- veiklos tęstinumo valdymas;
- auditas ir atitiktis [1].

Kiekvienas proceso atributas yra detalizuojamas praktiškais rodikliais padedančiais įvertinti nagrinėjamą atributą. Kiekvienas proceso atributas yra vertinamas pagal keturių punktų vertinimo skalę (žr. 8 lentelę) [37].

8 lentelė

Proceso atributai pagal „ ISO/IEC 15504 “ standartą

Vertinimo kriterijus	Vertinimo skalė
Nepasiekta	0 - 15%
Iš dalies pasiekta	>15% - 50%
Didžiąja dalimi pasiekta	>50%- 85%
Pilnai pasiekta	>85% - 100%

Šaltinis: sudaryta autorės

Vertinimo rezultatai pagal ISO standartą yra pripažįstami globaliu mastu, todėl tai yra svarbus kriterijus vertinant skirtingas organizacijas [14]. ISO standartas kompiuterio saugumą vertina pagal jame vykstančius procesus, procesai savo ruoštu yra skirstomi į atributus, o atributai turi kelis įvertinimo lygmenis. Tokia kompiuterinio saugumo vertinimo metodika yra patikima ir ja remiantis organizacijos gali apibrėžti saugumo veiklas ir transformuoti jas į struktūras, koncentruotas į saugumą.

- JAV saugumo departamentas *TCSEC (Trusted Computer System Evaluation Criteria)* kompiuterines sistemas pagal saugumą skirsto į keturias kategorijas: A, B, C ir D (kur A - aukščiausio lygio, o D – žemiausio lygio kategorija) [9].

Metodo trūkumas: klasės išskiriamos tiktai keturios, o dažniausiai aptinkamos kompiuterinės sistemos pasiskirsto tarp dviejų klasių (B ir C), nėra išvengiama subjektyvaus vertinimo, nes saugumo klasėje nėra apibrėžti visi galimi kompiuterinės sistemos komponentai.

Apibendrinimas. Saugumo klasių klasifikacija pagal *TCSEC* pasižymi aiškumu ir apibrėžtumu, bet vertinant kompiuterinę sistemą neišvengiama subjektyvumo, nes perėjimas tarp klasių nėra išsamiai apibrėžtas.

Siekiant sukurti kokybišką teisinę duomenų apsaugą visų pirma reikia atrinkti tą informaciją, kuri turi būti gerai apsaugota ir prieinama tik griežtai ribotam žmonių kiekiui. Kiekviena įmonė disponuoja tam tikru kiekiu informacijos. Tik dalis jos yra svarbi komerciniu požiūriu ir todėl turi būti ypatingai saugoma. Didžiausia problema yra ta, jog daugelis tai suvokia tik kaip fizinę apsaugą ir neskiria reikiamo dėmesio verslo saugai kitu požiūriu – konfidencialios informacijos intelektualiai saugai. Tai, ar informacija konfidenciali, gali apibrėžti šie kriterijai [11]:

- jos saugai naudojamos išskirtinės apsaugos priemonės;
- įmonė gali patirti didelę žalą dėl tokios informacijos praradimo ar neteisėto paviešinimo;
- ja gali naudotis tik ribotas žmonių skaičius;
- numatyta atsakomybė už neteisėtą jos atskleidimą;
- komercinis interesas tokią informaciją laikyti paslaptyje.

1.3.2. Rizikos įvertinimas ir sprendimai jai sumažinti

Užtikrinti, kad organizacijoje saugoma informacija nebus neleistinai atskleista, pakeista ar sunaikinta, galima tik aiškiai žinant, kokia informacija organizacijoje yra svarbi, kas gali turėti įtakos, kokie yra teisiniai ar kiti išoriniai reikalavimai informacijos saugumui [1].

Rizikos analizė teikia tris rezultatus:

- identifikuotas grėsmes;
- įvertintą rizikos lygį;
- kontrolės bei saugiklių nustatymą.

Rizika yra identifikuotos grėsmės funkcija ir įtaka, kurią ši grėsmė turės veiklos procesams.

Rizikos analizės žingsniai:

1) Apibrėžti procesą, taikomąsias programas, sistemas arba kitas vertybes, kurios taps rizikos analizės aspektu. Identifikuoti vertybes ir veiklos procesus, kuriems bus daroma įtaka.

2) Apibrėžti grėsmes kaip nepageidaujamus įvykius, kurie gali daryti įtaką veiklos tikslams. Sudaryti įmanomų grėsmių sąrašą. Yra keli grėsmių sąrašo sudarymo metodai: kontrolinių sąrašų kūrimas (kurių naudojimas užtikrina, kad viskas yra padengta arba identifikuota), istorinių duomenų

rinkimas (kokie įvykiai buvo atsitikę ir koks jų dažnis), „smegenų šturmas“ (vienas tinkamiausių metodų identifikuoti grėsmes) [6][39].

3) Nustatyti grėsmės įvykio tikimybę. Potencialios grėsmės tikimybę, atsižvelgiant į jau suformuotą vertybių sąrašą.

4) Nustatyti grėsmės įvykio tikimybės įtaką organizacijai. Nustatant rizikos lygį (tikimybę ir įtaką) identifikuojama organizacijoje esanti saugumo kontrolės įtaka rezultatams. Dažniausiai per pradinę peržiūrą grėsmės yra vertinamos neatsižvelgiant į įdiegtas DAP. Tai suteikia rizikos valdymo komandai galimybę įvertinti kontrolės ir saugumo mechanizmus bei matuoti efektyvumą. Vertinant riziką įsivedami apibrėžimai [6][39]:

9 lentelė

Rizikos tikimybės įtakos matrica

Tikimybė	Įtaka		
	didelė	vidutinė	maža
Didelė	A	B	C
Vidutinė	B	B	C
Maža	B	C	D

Šaltinis: Vasilecas O. (2008) Informacinių sistemų sauga.

A: Būtini situacijos gerinimo veiksniai

B: Pageidaujami situacijos gerinimo veiksniai

C: Reikalinga kontrolė

D: Nereikalingi jokie veiksniai

Tikimybė: Grėsmės įvykio tikėtinumas:

Didelė tikimybė: grėsmė greičiausiai įvyks per ateinančius metus;

Vidutinė tikimybė: galima tikėtis, kad grėsmė įvyks per ateinančius metus;

Maža tikimybė: mažai tikėtina, kad grėsmė įvyks per ateinančius metus.

Įtaka: nuostolių arba žalos dydžio vertybėms matas:

Didelė įtaka: kritinio veiklos padalinio uždarymas, nuo kurio priklauso didelis veiklos praradimo mastas (įvaizdis, pelnas);

Vidutinė įtaka: trumpalaikis kritinių procesų arba sistemų sustabdymas, darantis įtaką ribotiems finansiniams praradimams viename veiklos padalinyje;

Maža įtaka: sustabdymas be didelių finansinių nuostolių.

Nustačius rizikos lygį po priskyrimo, identifikuojamos kontrolės arba apsaugos priemonės, kurios gali eliminuoti riziką arba sumažinti rizikos lygį iki priimtino.

Įvertinti rekomendacijas dėl kontrolės priemonių ir alternatyvių sprendimų. Pavyzdžiui, kiek efektyvios yra rekomenduojamos kontrolės priemonės. Vienas iš būdų santykiniam efektyvumui

nustatyti - vertinant rizikos lygį, atsižvelgiant į planuojamas diegti kontrolės priemones. Jeigu rizikos lygis nėra sumažėjęs iki priimtino taško, reikės išanalizuoti kitą pasirinkimo galimybę [1].

Kontrolės išlaidas tikslinga subalansuoti su tikrąją galima neigiama įtaka organizacijai. Jei kontrolė kainuoja daugiau negu turtas, kurį ji turi apsaugoti, tokiu atveju investicijų grąža būtų labai žema. Naudinga identifikuoti kiekvieną kontrolės priemonę ir susieti ją su visomis grėsmėmis, kurių rizikos lygį ji gali sumažinti. Toks procesas parodo, kuri kontrolė yra efektyviausia kainos požiūriu. Rizikos analizės proceso išeiga yra kontrolės priemonės, kurios turi sumažinti grėsmės įvykio lygį [6].

Kadangi duomenų apsaugoje reikalaujama pakankamai daug organizacinių ir finansinių resursų, labai svarbu, kad organizacija identifikuotų savo saugumo reikalavimus ir pasirinktų tinkamą duomenų saugos lygmenį. Svarbu suderinti saugos lygmenį su reikalingomis jam užtikrinti investicijomis. Saugumo reikalavimai nustatomi įvertinant susijusią su informacijos praradimu saugos riziką, kuri skaičiuojama lyginant informacijos saugos valdymui skiriamas išlaidas su galimais veiklos nuostoliais praradus šią informaciją [1].

Organizacijai priėmus sprendimą nediegti tam tikrų būtinų saugumo reikalavimų, dėl didesnių investicijų į apsaugos priemones nei potencialaus praradimo vertė – rizika išlieka. Išliekamasis rizikos laipsnis skiriasi nuo visos rizikos vertės. Visa rizika ir išliekamoji rizika gali būti paskaičiuota pagal formules:

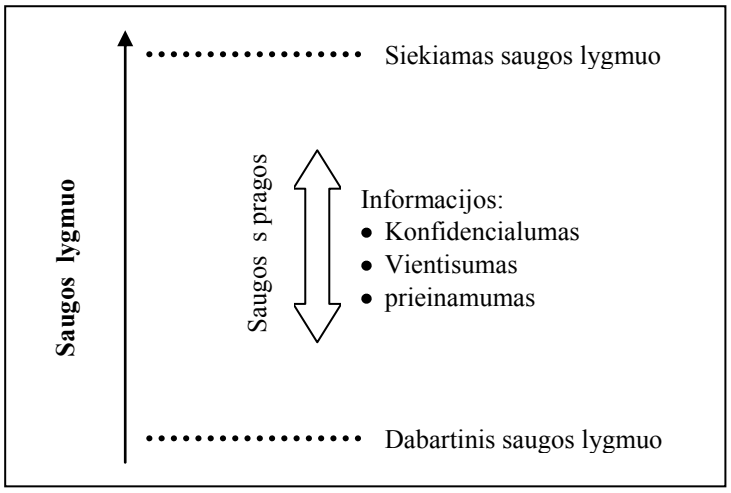
$$BR = G \times P \times TV, \quad (1)$$

$$IR = (G \times P \times TV) \times SK, \quad (2)$$

Čia *G* – grėsmės; *P* – pažeidžiamumas; *TV* – turto vertė, *BR* – bendra rizika; *SK* – spragos kontrolė; *IR* – išliekamoji rizika.

Apsaugos priemonių įgyvendinimas yra būdas sušvelninti galinčias iškilti grėsmes, tačiau nė viena organizacija negali išvengti visų galimų pavojų ir visada bus tam tikra išliekamoji rizika. Klausimas - kokį pavojaus lygmenį kompanija nori priimti [12].

Saugos reikalavimų ir rizikos vertinimas turėtų būti kartojamas periodiškai, atkreipiant dėmesį į bet kokį pasikeitimą, galintį turėti įtaką saugos rizikos vertinimo rezultatams. Pasikeitus sąlygoms nustatomos naujos saugos spragos ir įvertinamas atotrūkis tarp esamo ir norimo informacijos apsaugos lygmenų (žr. 4 paveikslą).



Šaltinis: Garla E., Dubovskaja V. (2008) Kompiuterinių tinklų projektavimas, p. 116.

4 pav. Dabartinis ir pageidaujamas įmonės duomenų saugos lygmuo

Nustačius saugos reikalavimus, parengiama įmonės saugos politika, parenkamos ir įdiegiamos tam tikros valdymo priemonės [1].

Saugumo politikai sudaryti galima remtis kompiuterio saugumo modeliais. Kurie yra saugumo politikos sudarymo ir vykdymo schema. Saugumo modelis gali būti apibūdinamas kaip formalus prieigos teisių modelis, skaičiavimų modelis, duomenų apdorojimo modelis, arba be ypatingo teorinio pagrindimo. Pagrindiniai yra žinomi šie saugumo modeliai: *Graham-Denning, Lattice-based access control, Brewer and Nash, Biba, Clark-Wilson, Role-based access control*, *Bell-LaPadula* ir kiti [2][6][15].

Kai kurie saugumo modeliai, tokie kaip *Bell-LaPadula* modelis, nurodo konfidencialumo apsaugos taisykles. Kiti modeliai, tokie kaip *Biba* modelis, nurodo taisykles vientisumo apsaugai. Šie oficialūs saugumo modeliai, tokie kaip *Bell-LaPadula model* ir *Biba*, naudojami aukšto lygmens saugumui užtikrinti. Neoficialūs modeliai, tokie kaip *Clark-Wilson*, naudojami daugiau kaip struktūra, saugumo politikai sudaryti ir vykdyti.

1.3.3. Duomenų apsaugos klasifikavimas

Ne visa informacija mums yra vienodai reikšminga, naudinga ir aktuali. Informaciją galima suskirstyti (klasifikuoti) pagal jos pasiekiamumo, vientisumo ir konfidencialumo kriterijus. Todėl informacijos vientisumo kriterijus nurodo, kokia yra informacijos pakeitimo svarba. Didžiosios dalies informacijos paviešinimas nesukelia problemų arba net yra pageidautinas, bet kai kurios informacijos, pavyzdžiui, asmens duomenų arba įslaptintos skelbimas didesniam negu norima gavėjų ratui gali turėti neigiamų pasekmių asmeniui, įstaigai arba valstybei. Svarbus informacijos apsaugos ir rizikos valdymo aspektas yra informacijos vertės pripažinimas ir atitinkamų procedūrų informacijos saugumo reikalavimų aprašymas. Ne visa informacija yra vienoda ir ne visai

informacijai reikia vienodo lygio apsaugos. Taigi reikalinga saugos klasifikacija. Kai kurie faktoriai darantys įtaką tam, kokia klasifikacija turi būti pasirinkta, priklauso nuo tos informacijos vertės organizacijai, kokio senumo ta informacija yra ir bet kuriuo atveju kai informacija yra pasenusi. Teisiniai ir kiti reguliavimo reikalavimai taip pat svarbūs klasifikuojant informaciją. Pagrindinės informacijos apsaugos klasifikavimo žymės naudojamos verslo sektoriuje yra: vieša, jautri, privati, konfidenciali, slapta, ypatingai slapta [13][14].

Duomenų jautrumui nustatyti gali būti panaudoti sekantys kriterijai:

- Duomenų naudingumas;
- Duomenų vertė;
- Duomenų amžius;
- Lygmuo žalos, kuri galėtų būti padaryta, jei duomenys buvo atskleisti;
- Lygmuo žalos, kuri galėtų būti padaryta, jei duomenys buvo pakeisti ar sugadinti;
- Ar už šių duomenų paviešinimą taikoma administracinė/baudžiamoji atsakomybė?;
- Ar duomenys reikalauja nacionalinio saugumo?;
- Kas gali turėti prieigą prie duomenų?;
- Kas turi tvarkyti duomenis?;
- Kur duomenys turi būti saugomi?;
- Kas galėtų atkurti duomenis?;
- Kokiems duomenims reikalingas etikečių ar ypatingas žymėjimas?;
- Ar duomenis reikalinga užšifruoti?[2].

Atsakymai į šiuos klausimus leis suklasifikuoti saugomus duomenis svarbos ir vertės atžvilgiu. Tačiau išlieka kiekybinio duomenų vertės nustatymo klausimas: ar ne per mažai investuojama į savo verslo saugumą ir išsaugojimą. Būtent šio atsakymo trūkumas neleidžia tiksliai atsakyti ar apsaugos sistema yra pakankamai patikima, ar tikslinga investuoti į ją daugiau.

1.3.4. Duomenų apsaugos priemonių pasirinkimo ir įvertinimo kriterijai

Duomenų apsaugos sistemų pasirinkimo ir efektyvumo įvertinimas galimas pagal daugelį metodų. Nesunkiai galime surasti konkretaus gamintojo antivirusinės programos ar užkardos aprašymą su bandymų rezultatais, duomenų kodavimo algoritmų imlumo kompiuteriniams resursams ir atsparumo atakoms duomenis ir kitus pavienių apsaugos priemonių panašių tyrimų rezultatus, ar siauros srities kompiuterinės sistemos saugumui keliamus reikalavimus. Toks įvertinimas taip pat gali būti naudingas kuriant kompiuterizuoto duomenų apsaugos sistemos parinkimo ir įvertinimo metodiką. Kaip pavyzdį galime pateikti literatūroje randamą antivirusinių programų palyginimą (žr. 10 lentelę).

10 lentelė

Antivirusinės PĮ ypatybių palyginimas

Ypatybė	BitDefender 8	AVG Anti-virus 7.1	ClamWin 0.88	AntiVir 6.35
Greitis	10	6	5	8
Darbo aplinka	9	7	7	9
Automatinis atnaujinimas	Yra	Yra	Yra	Yra
Automatinė apsauga	Nėra	Yra	Nėra	Yra
Automatinis patikrinimas	Yra	Yra	Yra	Yra

Šaltinis: LUČINSKIJ, M., POŽERSKIS, P., TUMĖNAS, P. (2007) Duomenų saugos pradmenys, p. 53.

Norint įsitikinti DAP efektyvumu reikia atlikti jų patikimumo testus. Galima pasinaudoti DAP efektyvumo testavimo organizacijų rezultatais. Pavyzdžiui, antivirusinių programų testavimo organizacijos testavime naudoja *ITW* (angl. In-the-Wild) virusų ir daugybės kitų kenkėjų, Trojos arklių, virusų ir kirminų pavyzdžius, kurie kenkia operacinėms kompiuterių sistemoms. Šiuo metu pagrindiniai antivirusų gamintojai testuojasi šiose laboratorijose: *Virus Bulletin („VB“)* – nepriklausoma testavimo organizacija, suteikia *VB100* sertifikatą, tikrina pagal *ITW* pavyzdžius; *AVTest.org* - tikrina pagal daug kriterijų; *AV Comparatives* - tikrina pagal daug kriterijų, *AV-Test Gmbh CheckVir* - tikrina pagal *ITW* pavyzdžius *ICSA labs* - suteikia savo sertifikatą, *West Coast Labs* - suteikia savo sertifikatą. Kuri iš šių laboratorijų testuoja objektyviausiai, vis dar aiškinasi antivirusų gamintojai. *„VB100“* saugumo testus atlieka *„Virus Bulletin“ („VB“)* – nepriklausoma testavimo organizacija, kurią sudaro profesionalūs antivirusinių programų ekspertai. Visi testai atliekami tiek vykdant failus, tiek skenuojant diską. Programai neatpažinus bent vieno viruso iš *„Wildlist“* sąrašo bet kuriame skenavimo režime arba pranešimus apie virusą, kurio iš tiesų nėra, ji nebegali gauti *„VB100“* apdovanojimo [29]. Rezultatų lentelės pavyzdys pateiktas 5 paveiksle:

On-demand tests	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets		RAP
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.	
Agnitum Outpost	0	100.00%	2	99.91%	442	88.58%	1685	80.78%	0	0	58.8%
AhnLab V3Net	0	100.00%	3	99.86%	246	98.92%	1945	75.38%	1	0	55.1%
Alwil avast!	0	100.00%	2	99.91%	13	99.22%	520	94.20%	0	0	71.4%
AVG Internet Security	0	100.00%	1	99.95%	21	98.96%	290	96.15%	0	0	80.6%
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	231	96.98%	1	1	88.5%

Šaltinis: HAWES, John (2009). VB100 on Windows 2003 Server x64

5 pav. Antivirusinių programų efektyvumo testų rezultatų lentelės pavyzdys

Dėl skirtingų kriterijų taikymo taip pat gali iškilti tam tikrų keblumų analizuojant ir vertinant duomenų apsaugos sistemas. Taikant skirtingus kriterijus vienos sistemos vertinimui, galima gauti skirtingus rezultatus.

2. DUOMENŲ APSAUGOS PRIEMONIŲ KOMPIUTERIZUOTO PARINKIMO IR ĮVERTINIMO METODIKA

DAP patikimumo įvertinimas - viena iš opiausių problemų su kuria susiduria IT specialistai. Jis galimas pagal daugelį metodų. Susiduriama su problema, kad skirtingais metodais įvertinta ta pati apsaugos priemonė yra vertinama skirtingai. Taip pat menkai kvalifikuoti specialistai pasirenka vieną ar kitą DAP neįvertinę ir nepalyginę galimų alternatyvių variantų. Duomenų apsaugos srityje trūksta bendro, visumą apimančio, požiūrio. Dažniausiai analizuojama ir testuojama viena konkreti apsaugos priemonė, atsižvelgiant į vieną ar keletą aspektų. Nesunkiai galime surasti konkretaus gamintojo antivirusinės programos ar užkardos aprašymą su bandymų rezultatais, duomenų kodavimo algoritmų imlumo kompiuteriniams resursams ir atsparumo atakoms duomenis ir kitus pavienių apsaugos priemonių panašių tyrimų rezultatus, ar siauros srities kompiuterinės sistemos saugumui keliamus reikalavimus. Toks įvertinimas taip pat gali būti naudingas kuriant DAP parinkimo ir įvertinimo metodiką. Tačiau trūksta bendro apsaugos sistemų analizavimo, testavimo ir vertinimo. Šiuo metu nėra universalios ir efektyvios kompiuterizuotos sistemos, kuria remiantis pakankamai gerai galima būtų įvertinti esamą kompiuterinę sistemą informacijos saugumo požiūriu, surūšiuoti DAP ir jų rinkinius pagal saugumo, patikimumo ir palankumo vartotojui lygius, kainą. Taip parenkant tinkamiausią DAP rinkinį konkrečiai kompiuterinei sistemai.

Taigi šio mokslinio tiriamojo darbo tikslas pasiūlyti DAP kompiuterizuoto parinkimo ir įvertinimo metodiką. Problemų sprendimui siūloma naudoti struktūrinio projektavimo principus, kurių dėka DAP pritaikomumo ir suderinamumo problema tampa nesunkiai išsprendžiama. Nustatysime organizacijos duomenų apsaugai užtikrinti reikalingų galimų sprendimų rinkinį. Pateiksime kiekybinius šio rinkinio elementų įvertinimo kriterijus. Kaip galimą taikymo sritį pasirenkame mažo ir vidutinio tipo organizacijas.

2.1. Duomenų apsaugos priemonių kompiuterizuoto parinkimo ir įvertinimo principai

Duomenų apsaugos organizavimo dabartinė padėtis, kurios pagrindinės ypatybės aprašytos 1 dalyje, rodo, kad yra tikslinga kurti metodikas, padedančias objektyviai įvertinti egzistuojančias duomenų apsaugos priemones (DAP) ir parinkti tinkamą jų rinkinį, efektyviai funkcionuojantį konkrečioje taikymo srityje. Pageidautina, kad tokį įvertinimą ir parinkimą galima būtų kompiuterizuoti. Šiems uždaviniams įgyvendinti galima remtis struktūrinio projektavimo metodika [4]. Jos pagrindas yra kuriamo (projektuojamo) objekto (KO) struktūros alternatyvių parinkimo principų taikymas. Kiekvienas KO paprastai turi keletą struktūrinių tipų (ST) kurie sudaryti iš tipinių struktūrinių elementų (TSE). Šiuo atveju projektavimo tikslas – parinkti efektyvią struktūrą

iš alternatyvių KO ST, naudojant alternatyvias TSE realizacijas. TSE – tai KO struktūriniai vienetai, kurie apibūdinami:

- Atliekamų funkcijų autonomiškumu ir baigtinumu;
- Išskirtos TSE aibės pakankamumu KO realizuoti.

Struktūrinio projektavimo principus tikslinga naudoti KO, kurie pasižymi šiomis savybėmis:

- Galima apibrėžti ir išskirti TSE, kurių kompozicija realizuojama KO;
- Egzistuoja žinomos standartinės kiekvieno TSE realizacijos;
- Yra daug KO alternatyvių realizacijų, o alternatyvumas apima tiek TSE, tiek juos realizuojančias priemones.

Tokias savybes turi konkrečias kompiuterinių duomenų saugos funkcijas (pvz., šifravimo, antivirusinę, užkardos ir kt.) realizuojančios DAP (išsamiau tai nagrinėsim kituose šios dalies skyriuose). Reikia pažymėti, kad apibrėžiant KO kiekvieną ST, dažnai tikslinga taikyti hierarchinį jo aprašymą. Šiuo atveju kiekvienas išskirtas TSE savo ruožtu gali būti sudarytas iš žemesnio lygio TSE, t.y. jų atžvilgiu yra ST.

Norint taikyti šią struktūrinio projektavimo metodiką kompiuterizuotai, turi būti sukurtas TSE katalogas (TSEK). Tokio katalogo pagrindiniai sudarymo principai yra šie:

1) katalogas dalinimas į pakatalogius, kurie atitinka apibrėžtiems TSE tipams;
2) TSEK struktūroje išskiriami du komponentai – vienas TSE charakteristikoms, kitas – TSE struktūrai ir funkcionavimui apibrėžti;
3) Kiekvienam TSE tipui apibrėžiami struktūriniai variantai, kurie skiriasi savo charakteristikomis. Charakteristikų vertinimo vienetai atitinka nustatytiems projektavimo kriterijams.

Tokio TSEK struktūra formaliai gali būti apibrėžta kaip aibė:

$$
\begin{aligned}
&A = \bigcup_i A_i = \bigcup_i (B_i, C_i),\ \boldsymbol{i}=1,2,\ldots,\boldsymbol{I};\\
&A_i = \{a_j^i\},\ B_i = \{b_j^i\},\ C_i = \{c_j^i\};\\
&a_j^i = \langle b_j^i, c_j^i \rangle,\ b_j^i = \langle q_1^i, q_2^i, \ldots, q_z^i, {}^j m_1^i, {}^j m_2^i, \ldots, {}^j m_p^i \rangle;\\
&{}^j m_s^i = \tau_s\left(n_1^i, {}^j n_2^i, \ldots, {}^j n_v^i\right),\ \boldsymbol{j}=1,2,\ldots,\boldsymbol{J^i};
\end{aligned}
\qquad (3)
$$

Čia $\boldsymbol{A_i}$ – aibė, kuri aprašo *i*-ąjį pakatalogį, atitinkantį *i*-jam TSE tipui; $\boldsymbol{B_i}$ – aibė aprašanti *i*-ojo pakatalogio TSE charakteristikas (pirmoji TSEK dalis); $\boldsymbol{C_i}$ – aibė aprašanti *i*-ojo pakatalogio TSE struktūrą ir funkcionavimą (antroji TSEK dalis); $\boldsymbol{a_j^i}$ - *i*-ojo TSE *j*-ojo struktūrinio varianto apibrėžimas kataloge; $\boldsymbol{b_j^i, c_j^i}$ - *i*-ojo TSE *j*-ojo struktūrinio varianto apibrėžimas pirmoje ir antroje

TSEK dalyse; q_z^i – parametras, kuris apibrėžia *i*-ojo pakatalogio elementų *z*-ąją savybę; ${}^j m_p^i$ – *j*-ojo struktūrinio varianto *p*-oji charakteristika, kuri įvertina šį variantą *p*-ojo projektavimo kriterijaus atžvilgiu; ${}^j n_v^i$ – *j*-ojo struktūrinio varianto parametras, apibrėžiantis *v*-ąją struktūrinę savybę; J_i – *i*-ojo TSE struktūrinių kiekis; I – TSE kiekis. TSEK visiems struktūriniams variantams yra sudarytos analitinės išraiškos ar algoritmai skaičiuoti charakteristikas ${}^j m_s^i = f_s(n_1^i, {}^j n_2^i, ..., {}^j n_v^i)$, kurios išreikštos apibrėžtais įvertinimo vienetais, atitinkančiais nustatytus projektavimo kriterijus.

Reikia pažymėti, kad mūsų nagrinėjamoje srityje KO pagrindiniai projektavimo kriterijai yra susieti su duomenų apsaugos lygiu (patikimumas, konfidencialumas, vientisumas) bei kaina (DAP realizacijų rinkinio ir jo eksploatavimo).

Pagal aprašytus principus sukurtam TSEK gali būti organizuotas jo kompiuterizuotas panaudojimas. Šiuo atveju yra sprendžiamas šis uždavinys: apibrėžtiems TSE, įvertinus apribojimus jų savybių q_z^i ir charakteristikų ${}^j m_s^i$ reikšmėms, yra generuojamos įvairios jų realizacijos. Kiekviena iš jų yra apibūdinama konkrečioms charakteristikų reikšmėmis ir detaliu struktūros ir funkcionavimo aprašymu, kuris gaunamas iš apibendrintų aprašymų c_j^i [4].

Aprašytam uždaviniui išspręsti reikalingi du etapai:

1) apibrėžti konkretaus KO TSE parametrų $q_1^i, ..., q_z^i$ reikšmėms;
2) skaičiuoti kiekvienai *i*-ojo TSE *j*-ojo ST realizacijai charakteristikų ${}^j m_s^i$ reikšmės.

Pirmasis etapas formaliai apibrėžiamas kaip paieška kelių σ_w nuo medžio $\sigma_w=(X,U)$ šaknies $X_0 \in X_1$, ir turinčių ilgį $l(\sigma_w)=Z$. (Čia Z – medžio G lygių skaičius). Medyje G kiekviena viršūnė $X_n^z \in X$ yra Z lygyje, kuris atitinka parametrui q_z^n , ir ši viršūnė atitinka z parametro reikšmes. Šaka $(X_m^{Z-1}, X_p^Z) \in U$ atitinka pasirinkimui: struktūrai su *Z-1* parametro reikšme *m* galimo varianto, charakterizuojamo *Z* parametro *p* reikšme. Skaičius šakų, išeinančių iš kiekvienos viršūnės X_n^z, yra lygus parametro q_z^n reikšmių skaičiui.

Antrajame etape, kai jau apibrėžtos visų q_z^i reikšmės, kiekvienam *i*-ojo TSE yra suformuojamas masyvas $E_i = \{\}$, kuriame yra duotus apribojimus charakteristikoms tenkinančios perspektyvios *i*-ojo tipo TSE realizacijos. Perspektyvumas suprantamas šia prasme: masyve E^i , bet kokia realizacijų pora bent viena charakteristikos reikšme geresnė už kitą.

Toliau, pritaikant aprašytus struktūrinio projektavimo principus, nustatyti apibrėžtai taikymo sričiai efektyvų DAP rinkinį, spręsime tokias užduotis:

a) pasirinkti KO, t.y. apibrėžti taikymo sritį ir nustatyti jos galimus ST;
b) apibrėžti TSE, t.y. reikalingas DAP ir jų rinkinius;
c) nustatyti KO (DAP rinkinio) įvertinimo (projektavimo) kriterijus ir vertinimo vienetus;
d) parodyti TSEK sukūrimo galimybes.

Šiuos katalogo principus, kurių dėka DAP pritaikomumo ir suderinamumo problema tampa nesunkiai išsprendžiama, taikysime ir mūsų kuriamoje metodikoje. Mūsų atveju kuriamo rinkinio TSE yra kompiuteris (stacionarus, nešiojamas), serveris (pagal paskirtį: duomenų bazių, failų, spausdinimo, bei tinklo servisų - Web, DNS, Proxy, el. Pašto). Kiekvienam iš šių TSE priskiriame po vieną DAP (komutatorių, maršrutizatorių, užkardų, antivirusinių programų, UPS ir t.t.) pakatalogį. Kiekvienas pakatalogis turi jame esančių DAP įvertinimų ir kitų parametrų katalogą (pvz., užkardos charakteristikos: programinė, valdymo sudėtingumas įvertintas 9 balais, įeinančio ir išeinančio srauto filtravimas, svetainių įrašymas į atmintinę, kaina litais), bei DAP pritaikymo ir suderinamumo struktūros atžvilgiu katalogą. Galiausiai kataloge yra ST pakatalogis (pvz., užkardos pritaikymas Windows operacinėms sistemoms, skirta vidutinio dydžio įmonėms, suderinama su įdiegta antivirusine programine įranga).

2.1.1. Duomenų apsaugos priemonių rinkinio išoriniai parametrai

Sudarant DAP rinkinį, išskirsim kompiuterinės sistemos išorinius parametrus, atitinkančius q_z^i (žr. 2.1. poskyrį):

- Tiesioginis atakuojamasis tinklo elementas: kompiuteris ar serveris;
- Naudojama OS;
- LAN, WAN, VPN.

Vienas iš daugelio aspektų, kurį reikia įvertinti parenkant tinkamas DAP, yra įmonės dydis. Lietuvoje didžiausią kompiuterinių tinklų dalį sudaro tinklai, kuriuose yra iki 200 darbo vietų. Firma „Cisco“ pagal tinklo vartotojų skaičių siūlo įmones skirstyti sekančiai:

- Maža įmonė, kurioje vartotojų skaičius iki 50;
- Vidutinė įmonė, kurioje vartotojų skaičius nuo 50 iki 100;
- Didelė įmonė, kurioje vartotojų skaičiuos nuo 100 iki 200 ir daugiau [1].

Šiuo metu didžiausią tinklinės įrangos pasirinkimą siūlo ši gamintoja, o jos gaminamos įrangos universalumą praplečia modulinė įrangos konstrukcija, kurią vis plačiau pradeda taikyti ir kitos firmos. Todėl šia tinklo architektūros variantų pagal tinklo vartotojų skaičių skirstymo metodika ir remsimės, sudarant tinkamą DAP tinklo architektūros rinkinį. Nors kai kurie autoriai mažais tinklais siūlo laikyti tinklus, kuriuose yra iki 100 vartotojų [5]. Ypatingos reikšmės įmonių skirstymas pagal vartotojų skaičių neturi, nes bet kokiu atveju tinklo sandara yra hierarchinė [1].

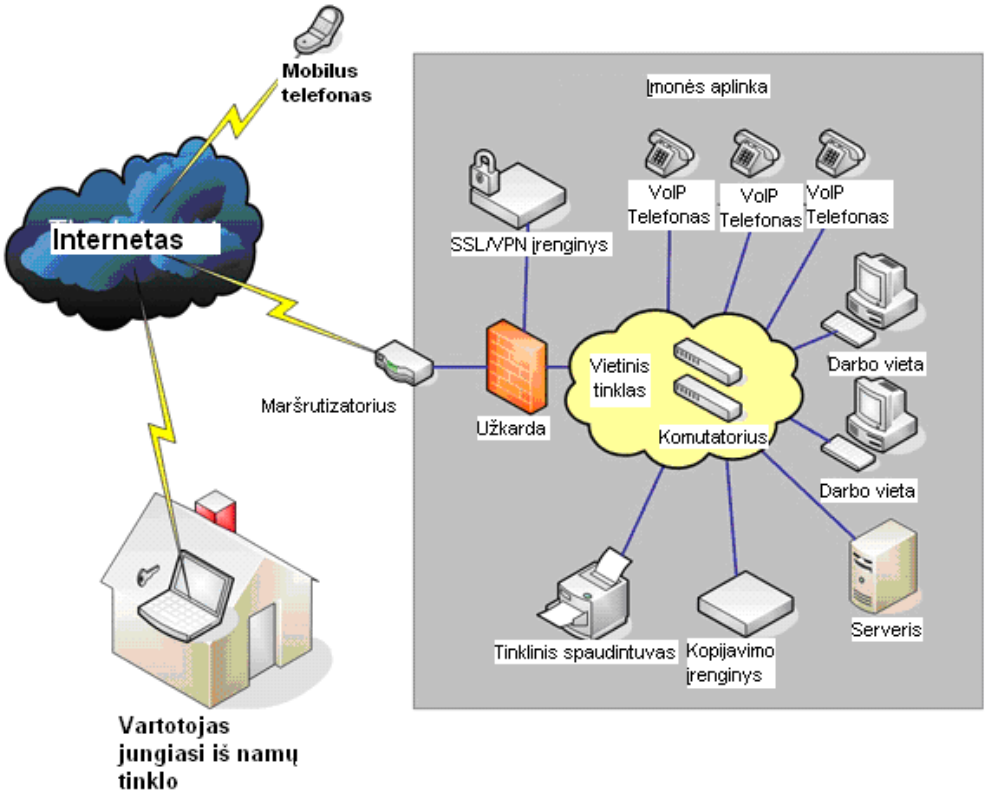
2.1.2. Pirmo lygio tipiniai struktūriniai elementai

Nagrinėsiu TSE pavyzdžius, atitinkančius a_j^i. Reikia pažymėti, kad TSE katalogas gali būti sudarytas iš kelių lygių. Pirmo lygio TSE priskiriame įmonės tinklo architektūras. Jas apsirašome pagal kompiuterizuotų darbo vietų skaičių įmonėje.

Mažos įmonės, kurioje dirba mažiau nei 15 darbuotojų, tinklą gali sudaryti maršrutizatorius, prijungtas prie interneto paslaugų tiekėjo, taip pat iki dviejų serverių prijungtų eterneto linijomis prie maršrutizatoriaus. Kiti galimi mažos įmonės tinklo architektūros variantai:

- LAN, maršrutizatorius, komutatorius (-iai);
- WAN maršrutizatorius, komutatorius (-iai);
- VLAN, maršrutizatorius (teikiantis DHCP, užkardos, NAT funkcijas), komutatorius (-iai);
- Maršrutizatorius (turintis ir VPN funkcijas), komutatorius (-iai).

Galimas mažos įmonės tinklo schemos pavyzdys pateiktas 6 paveiksle.



Šaltinis: sudaryta autorės.

6 pav. Mažos įmonės tinklo schemos pavyzdys

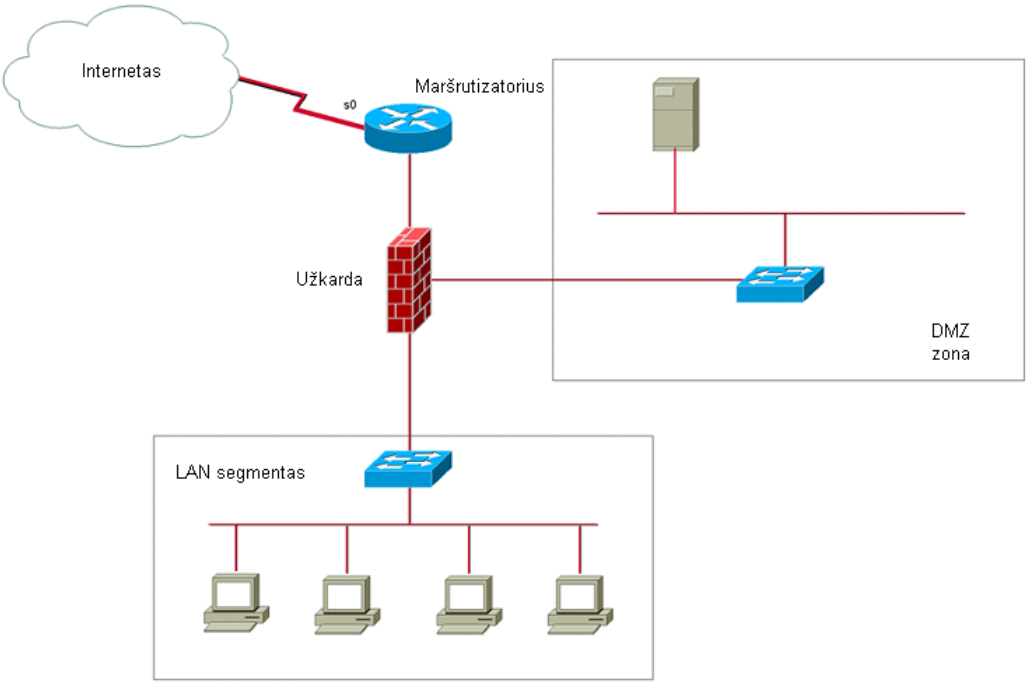
Vidutinio dydžio įmonės architektūros schema analogiška kaip ir mažos įmonės, tik pagrindinis skirtumas, jog naudojamas maršrutizatorius, turintis dvi integruotąsias 10/100/1000 sąsajas ir po vieną jungtį, skirtą paslaugų moduliui. Dažniausiai naudojami 24 prievadų komutatoriai, kurie jungiami į abi integruotąsias sąsajas. Viena sąsaja naudojama duomenų, o kita

balso perdavimo potinklių nustatytiems tinklų sietuvams (angl. default gateway) organizuoti. Prieigos tinklo patikimumui padidinti, vietoj paprastų komutatorių gali būti naudojami krūvą sudarantys (angl. Stackable) komutatoriai [1].

Didelės įmonės schema skiriasi nuo mažos ir vidutinės schemų tuo, kad čia naudojamas skirstomas tinklas, kurio įrangos ir tuo pačiu tinklo praleidžiamosios galios pasirinkimas priklauso nuo vartotojų skaičiaus, naudojamų taikomųjų programų ir serverių, jungiamų DMZ tinkle. Galima išskirti dvi didelės įmonės tinklo sudarymo schemas naudojant integruotąsias sąsajas arba integruotuosius paslaugų modulius [1].

Didelės organizacijos gali turėti keletą WAN sujungtų tarpusavyje.

Svarbu nurodyti kiek įmonėje yra kompiuterizuotų darbo vietų, komutatorių, maršrutizatorių, serverių. Išskirti, kurie įrenginiai talpinami saugioje zonoje DMZ.



Šaltinis: sudaryta autorės

7 pav. Vidinės kompiuterinės sistemos modelis

Paveiksle pateiktos vidinės kompiuterinės sistemos modelį galima laikyti pagrindiniu ir etaloniniu kompiuterinės sistemos struktūros pavyzdžiu (žr. 7 paveikslą). Jeigu įmonė turi geografiškai nutolusių padalinių, reikia įtraukti ir šiuos.

2.1.3. Antro lygio tipiniai struktūriniai elementai

Antro lygio TSE mūsų nagrinėjamoje srityje sudarytų DAP. Toliau apsibrėšime DAP, kurios galėtų būti jų kompiuterizuoto parinkimo ir įvertinimo sistemos objektais. Kaip buvo minėta 1.2.

poskyryje administracinė kontrolė formuoja pagrindą parinkti ir įdiegti techninę (loginę) bei fizinę kontrolę. Šios kontrolės yra administracinės kontrolės pasireiškimas. Administracinė kontrolė yra laikoma pirmaeilės svarbos priemone. Kadangi administracinės DAP priklauso nuo pačios organizacijos informacijos apsaugos politikos, tai į DAP kompiuterizuoto parinkimo ir įvertinimo sistemą įtrauksime tik technologines (logines) bei fizines DAP. Renkantis DAP išskirsime du informacijos apsaugos sprendimų būdus – tinklo apsaugos sprendimus ir atskirų jo elementų apsaugos sprendimus.

2.1.3.1. Tinklo apsaugos priemonės

Tinklo apsaugos priemonės yra technologinių (loginių) DAP dalis. Į DAP kompiuterizuoto parinkimo ir įvertinimo sistemą tikslinga įtraukti dažniausiai naudojamas tinklo apsaugos priemones:

1. Techninė užkarda (angl. Firewall). Šiuolaikiniuose tinkluose užkarda išlieka pagrindinis komponentas sprendžiant tinklo saugumą. Užkarda yra pagrindinis kiekvieno tinklo komponentas, užtikrinantis deramą vidinio įmonės tinklo apsaugą nuo išorinio tinklo (internetas, ekstranetas, nuotoliniai prisijungimai).
2. Komutatorius (angl. Switch) – tai daugelį skirtingų jungčių turintis koncentratorius, galintis paskirstyti duomenis reikiamiems tinklo segmentams. Gali būti prieigos tinklo komutatorius ir skirstomojo lygmens komutatorius. Prieigos tinko komutatorius yra antrojo lygmens 2L pagal OSI modelį pagrindinis paketų komutavimo prietaisas. Skirstomojo lygmens komutatoriai dažniausiai veikia tiek antrajame 2L, tiek ir trečiajame 3L pagal OSI modelio lygmenyse.
3. Maršrutizarorius (angl. Router) - tai įrenginys, kuris aprašo duomenų perdavimo srautų maršrutus, sujungia įvairių rūšių ir paskirčių tinklus į bendrą tinklą. Maršrutizatorius gali atlikti ir komutatoriaus funkcijas. Maršrutizatoriais sujungtas tinklas suvokiamas kaip daugelio mažų tinklų, vadinamų potinkliais (Subnet), visuma, vadinama intertinklu (angl. Internetworking arba Internet) [1].
4. Integruotas saugumo įrenginys (angl. Security Appliance) – įrenginys skirtas virtualių privačių tinklų organizavimui, turintis ir kitų saugos funkcijų.

Šios pasirinktos į DAP rinkinį įtrauktos tinklo saugos priemonės atlieka 1.2. poskyryje aprašytų tinklo apsaugos sprendimų funkcijas. Tai pagrindiniai tinklo elementai, kurie nėra tiesiogiai atakuojami. Dažniausiai atakų tikslas yra kompiuterinių sistemų resursai (kompiuteriai, Web servisai, taikomosios programos, duomenų bazės ir pan.). Tinklų apsaugos priemonės dažniausiai ribojamos tinklo įrangos technologinėmis galimybėmis, tačiau ne visada, netgi esant

reikalingai funkcijai, tinklas yra pakankamai saugus. Kompiuterinis tinklas yra saugus kai visi jame esantys komponentai (kompiuteriai, serveriai, komutatoriai, maršrutizatoriai) yra tinkamai apsisaugoti. Reikalinga pasirinkti ir įdiegti apsaugos priemones kur kiekvienas tinklo elementas veikia kaip apsaugos taškas. Integravus tokią kompleksinę sistemą, kompiuteriai bei visa informacija bus apsaugoti nuo virusų ir įsilaužėlių žalingo poveikio, o tinklas bus apsaugotas ne tik perimetre (išėjimas į internetą), bet ir kiekviename sujungimo taške.

2.1.3.2. Atskirų tinklo elementų apsaugos priemonės

Į formuojamą DAP rinkinį tikslinga įtraukti šias atskirų tinklo elementų saugumo lygį pakeliančias programines apsaugos priemones:

1. Antivirusinė programinė įranga - programa skirta aptikti virusą, jį sunaikinti ir atstatyti sugadintą informaciją.
2. Užkarda – programinė priemonė skirta apsaugoti kompiuterį nuo įsilaužėlių, iš išorės inicijuotų nepageidaujamų kreipimųsi i kompiuterį ar visą kompiuterių tinklą.
3. Kietojo disko šifravimas – programinė priemonė užtikrinanti kompiuterio kietajame diske esančių duomenų saugumą. Naudojama mobiliems kompiuteriams apsaugoti.
4. Įsiskverbimo aptikimo sistema (IDS) – programinė priemonė aptinkanti kompiuterinių įsilaužėlių veiksmus, juos sekanti ir blokuojanti [10].
5. Duomenų kopijavimas – duomenų atsarginių kopijų kūrimas ir jų panaudojimas, įvykus nenumatytam atvejui ir originaliems duomenims esant neprieinamiems ar nepataisomai sugadintiems.

Į DAP rinkinį taip pat tikslinga įtraukti šias atskirų tinklo elementų saugumo lygį pakeliančias fizines apsaugos priemones:

1. Nepertraukiamos srovės šaltinis (UPS) – techninė priemonė apsauganti nuo trikdžių sukeltų įtampos šuolių, ar tam tikrą laiko tarpą apsauganti nuo visiško elektros srovės dingimo.
2. Užraktas – fizinis užraktas (gali būti plieninis lynelis), neleidžiantis naudotis kompiuterine technika neturint rakto, tuo pačiu ir teisių. Dažniausiai naudojami nešiojamiems kompiuteriams pritvirtinti prie stalo arba kitokio masyvaus ar gerai įtvirtinto daikto.
3. Žaibolaidis – techninė priemonė apsauganti nuo elektros iškrovų (žaibų).
4. Ventiliacijos sistema – sistema apsauganti kompiuterinę įrangą nuo kenksmingo dulkių poveikio.

Toliau apžvelgsime pagrindines aprašytų DAP rinkinių savybes bei nustatysime svarbiausius atrinkimo kriterijus.

2.1.4. Apsaugos priemonių funkcijų charakteristikų aprašai

Nustatysime ir pateikime kiekvienai įtrauktai į DAP rinkinį priemonei ją įvertinančius pagrindinius parametrus ir charakteristikas.

DAP pasirinkimo kriterijai nustatyti remiantis informacijos apsaugos standartų rekomendacijomis, moksliniais straipsniais, mokomosiomis priemonėmis. Pirmiausiai išskiriamos pagrindinės DAP funkcijos, kurios būdingos visoms alternatyvioms tos grupės apsaugos priemonėms. Šios funkcijos yra privalomos, todėl DAP vertinimo kriterijui nėra reikšmingos. Dauguma apsaugos priemonių gali atlikti ir papildomų, tiesiogiai nesusijusių su jų paskirtimi, funkcijų. Papildomos funkcijos gali būti gali būti įtrauktos arba užsakytos atskirai. Kai kurios funkcijos įeina nemokamai į vienas DAP, bet turi būti mokamos kitose [1]. Pavyzdžiui, prie techninės užkardos papildomų funkcijų priskiriamos:

- Įsibrovimo susekimo sistema (IDS/IPS);
- Virtualaus privataus tinklo (VPN) organizavimas;
- Turinio filtravimas (angl. Content filtering);
- Centralizuotas valdymas ir ataskaitų formavimas;
- Pasiekiamumo užtikrinimas HA (angl. High availability);
- Internetinių svetainių rašymas į atmintinę (angl. Web caching);
- Antivirusinės programos funkcija;
- Nepageidaujamo pašto filtravimas (angl. Spam filtering) [1][22][32][33].

Pagrindinės (privalomosios) tinklo užkardos funkcijos:

- Įeinančio ir išeinanėio srauto filtravimas
- Tinklo adresų transliavimas NAT [1].

Renkantis DAP, svarbu atkreipti dėmesį į priemonės spartos ar pajėgumo charakteristikas. Pavyzdžiui, svarbus tinklo užkardos srauto spartos parametras. Srauto sparta yra apibrėžiama kaip duomenų, perduodamų per sekundę, kiekis. Užkardų pralaida gali keistis nuo 150 Mbps iki 1 Gbps ir daugiau. Gamintojų sąrašuose dažniausiai nurodoma dvikryptė užkardos pralaida. Tai nereiškia, kad tokia sparta bus internete, kuri ribojama internetinio ryšio kanalo pralaida. Kaip pasirinkti tinkamą užkardą pagal srauto spartos parametrą, pajėgumą ar kitus dydžio parametrus galima vadovautis rekomendacijomis pateiktomis lentelėje (žr. 11 lentelę). Lentelėje pateikti apibendrinti duomenys, kurie nustatyti žymiausių užkardų gamintojų:

11 lentelė

Užkardos pasirinkimo pagal dydį rekomendacijos

Vartotojų skaičius	Reikalavimai RAM (MB)	Procesoriaus pajėgumas (Mhz)	Nutolusių padalinių skaičius	Srauto sparta (Mbps)	Kainos ribos ($)
< 50	< 10	~ 66	1	< 10	< 500
51-1000	65	~ 200	2-299	< 100	~ 5000
1001-5000	128	~ 500	300	< 200	~ 10000
> 5000	256	~ 500 +	>300	> 200	~ 20000

Šaltinis: sudaryta autorės pagal TAYLOR, Laura. (2002) How to Choose the Right Enterprise Firewall

Jei planuojami vaizdo ar VPN srautai, tuomet užkardą reikėtų rinktis su didesniais pajėgumais, nei pateikta lentelėje. Taip pat reikia atsižvelgti ir į plėtimo galimybes, pavyzdžiui, jei planuojas didesnis vartotojų skaičius. Taip pat svarbios yra ir DAP palankumo vartotojui charakteristikos. Tokios kaip DAP valdymo sudėtingumas, efektyvumas, plėtimo galimybė, pagalba vartotojui ir pan. Šias charakteristikas gana sunku įvertinti. Todėl jų vertės nustatymui skaitine išraiška naudosimės internete nesunkiai surandamais DAP reitingais ar specialių organizacijų atliktais DAP efektyvumo testų rezultatais. Toliau 12-23 lentelėse pateikti svarbiausi atskirų DAP pasirinkimo kriterijai. Čia reikšmės DAP įvertinimui yra šios: *L* - loginė (1 ar 0), *B* - balinė (balai nuo 1 iki 10), *P* - piniginė, *K* - kiekis, - - neapibrėžta.

12 lentelė

Užkardos

Variantas	Kriterijai	Reikšmė įvertinimui	
a)	Tipas	Techninė (T)	Programinė (P)
b)	Srauto sparta (nuo 150Mbs iki 1Gbps)	B	-
c)	Valdymo sudėtingumas	B	B
d)	Įeinančio ir išeinančio srauto filtravimas	L	L
e)	Internetinių svetainių įrašymas į atmintinę	L	L
f)	Apsauga nuo šnipinėjančių programų (angl. spyware/adware)	L	-
g)	Iškylančiųjų langų (angl. pop-up) blokavimas	L	-
h)	El. pašto apsauga nuo virusų	L	-
i)	Įsiskverbimo prevencijos sistema	L	-
j)	VPN funkcija	L	-
k)	Kaina	P	P

Šaltinis: sudaryta autorės

13 lentelė

Integruoti saugumo įrenginiai

Variantas	Kriterijai	Reikšmė įvertinimui
a)	Palaiko IPSec protokolą	L
b)	VPN funkcija	L
c)	VLAN funkcija	L
d)	Integruota užkardos funkcija	L
e)	DMZ prievadas	L
f)	Įrangai teikia elektros energiją eterneto linijomis PoE pagal IEEE 802.3af standartą	L
g)	Kaina	P

Šaltinis: sudaryta autorės

14 lentelė

Komutatoriai

Variantas	Kriterijai	Reikšmė įvertinimui	
a)	Tipas	Prieigos lygmens (L2)	Skirstomojo lygmens (L3)
b)	Veikia dengiamojo medžio algoritmo protokolais STP pagal IEEE 802.1D standartą	L	L
c)	Veikia virtualiuose vietiniuose tinkluose VLAN pagal IEEE 802.1Q standartą	K	K
d)	Rūšiuoja paketus pagal aptarnavimo kokybės kriterijus QoS (Quality of service)	L	L
e)	Vykdo prieigos taškų tapatumo nustatymą, autorizaciją ir apskaitą AAA pagal IEEE 802.1x standartą	L	-
f)	Vykdyti antrojo lygmens saugumo funkcijas, pvz., dinaminė ARP inspekcija	L	-
g)	Veikia su prievadų analizatoriumi SPAN (Switched Port Analyser) ir su nuotoliniu SPAN (RSPAN)	L	-
h)	Įrangai teikia elektros energiją eterneto linijomis PoE pagal IEEE 802.3af standartą.	L	-
i)	Kaina	P	P
j)	TACACS+/RADIUS autentifikacija	-	L
k)	Palaiko SSH /SSL tinklo protokolus	-	L
l)	WEB pagrįstas autentiškumo nustatymas	-	L
m)	Autentifikavimas 802.1x MAC adresų pagrindu	-	L
n)	Palaiko DHCP protokolą	-	L
r)	ACLs	-	L
s)	Jungčių kiekis	-	K
t)	Plėtimo galimybė	-	K

Šaltinis: sudaryta autorės

15 lentelė

Maršrutizatoriai

Variantas	Kriterijai	Reikšmė įvertinimui	
a)	Jungčių kiekis	8 jungčių	4 jungčių
b)	Integruota užkarda	L	L
c)	VPN galimybė	L	L
d)	Maitinimo šaltinis	L	L
e)	Papildoma jungtis DMZ	L	-
f)	Maksimalus perduodamų duomenų greitis (apie 100 Mbps)	B	B
g)	Perkėlimo norma (angl. Transfer rate) (nuo 100 iki 800 MB/s)	B	B
h)	NAT, PAT funkcija	L	L
i)	Palaiko DHCP protokolą	L	L
j)	Kaina	P	P
k)	Maršrutų sudarymo „tam tikros politikos pagrindu“ galimybė	-	L
l)	Virtualaus maršrutų sudarymo ir perdavimo VRF (Virtual Routing and Forwarding) galimybė	-	L
m)	Pasiekiamumo užtikrinimo galimybė HA (angl. High availability)	-	L
n)	Plėtimo galimybė	-	L

Šaltinis: sudaryta autorės

16 lentelė

Antivirusinė programinė įranga

Variantas	Kriterijai	Reikšmė įvertinimui
a)	Operacinė sistema	Nurodomas OS tipas
b)	Atnaujinimo dažnumas (vid. valandų skaičius nuo pranešimo apie naują virusą)	K
c)	Valdymo sudėtingumas	B
d)	Įeinančio pašto srauto skanavimas	L
e)	Išeinančio pašto srauto skanavimas	L
f)	Pašto skanavimas	L
g)	Laikmenų skanavimas	L
h)	USB laikmenų skanavimas	L
i)	Euristinis virusų atpažinimas	L
j)	Apsauga tinkle	L
k)	Virusų veiklos blokavimas	L
l)	Automatinis failų valymas ir virusų šalinimas	L
m)	Apsauga nuo nepageidaujamų laiškų „Spam„	L
n)	Užkardos funkcija	L
o)	Licencijų kiekis	K
p)	Kaina	P

Šaltinis: sudaryta autorės

17 lentelė

Disko šifravimo programinė įranga

Variantas	Kriterijai	Reikšmė įvertinimui
a)	Keli šifravimo algoritmai	L
b)	Galimybė kurti paslėptus tomus	L
c)	Naudojimo sudėtingumas	B
d)	Pritaikymas dirbti riboto vartotojo teisėmis	L
e)	Kaina	P

Šaltinis: sudaryta autorės

18 lentelė

Duomenų kopijavimo įranga

Variantas	Kriterijai	Reikšmė įvertinimui
a)	Atsparumas trikdžiams	B
b)	Kopijos atsparumas fiziniam poveikiui	B
c)	Atstatymo iš kopijos greitis (KB/s)	K
d)	Kopijos sukūrimo trukmė (KB/s)	K
e)	Kaina	P

Šaltinis: sudaryta autorės

19 lentelė

UPS

Variantas	Kriterijai	Reikšmė įvertinimui
a)	Veikimo laikas (pilna apkrova) minutėmis	K
b)	Serverio išjungimo funkcijos palaikymas	L
c)	Galingumas (Maksimali apkrova) (VA)	K
d)	Kaina	P
e)	Tipas (išorinis – I, montuojamas - M)	Nurodomas UPS tipas

Šaltinis: sudaryta autorės

20 lentelė

IDS

Variantas	Kriterijai	Reikšmė įvertinimui
a)	Efektyvumas	B
e)	Kaina	P

Šaltinis: sudaryta autorės

21 lentelė

Užraktai

Variantas	Kriterijai	Reikšmė įvertinimui
a)	Pagal atsparumą mechaniniam poveikiui	B
b)	Naudingumas / efektyvumas (nuo vagystės, naudojimo, įjungimo, išjungimo)	B
e)	Kaina	P

Šaltinis: sudaryta autorės

22 lentelė

Žaibolaidžiai

Variantas	Kriterijai	Reikšmė įvertinimui
a)	Saugomas plotas (m^2)	K
b)	Pakartotinis panaudojamumas	B
e)	Kaina	P

Šaltinis: sudaryta autorės

23 lentelė

Ventiliacijos sistemos

Variantas	Kriterijai	Reikšmė įvertinimui
a)	Temperatūros palaikymas / reguliavimas	B
b)	Oro srauto valdymas	L
c)	Drėgmės reguliavimas	L
d)	Kaina	P

Šaltinis: sudaryta autorės

Atitinkamos DAP rinkinio įverčius skaičiuosime pagal 12-23 lentelėse pateiktus jos pasirinkimo kriterijus. Atskiroms kriterijų rūšims pritaikysime atitinkamus svorinius koeficientus (k_i), kurie turi įtakos bendram tos DAP rūšies patikimumui. Jose naudojamų koeficientų galimos reikšmės pateiktos 26 lentelėje, o funkcinių parametrų reikšmės 28-32 lentelėse. Toliau pateiksime šių skaičiavimų formules.

Programinės užkardos įvertį I_{UZKp} skaičiuosime pagal formulę:

$$I_{UZKp} = {}_{uzk} \cdot k_1 + {}_{uzk} + {}_{uzk} + {}_{uzk} + {}_{uzk} + {}_{uzk}, \quad (4)$$

Čia c_{uzk} – valdymo sudėtingumas, d_{uzk} – įeinančio ir išeinančio srauto filtravimas, e_{uzk} – svetainių įrašymas į atmintinę, f_{uzk} – apsauga nuo šnipinėjančių programų, g_{uzk} – iškylančių langų blokavimas, h_{uzk} – el. pašto apsauga nuo virusų.

Techninės užkardos įvertį I_{UZKt} skaičiuosime pagal formulę:

$$I_{UZKt} = b_{uzk} \cdot k_1 + l_{uzk} + d_{uzk} + e_{uzk} + g_{uzk} + h_{uzk} + i_{uzk} + j_{uzk}, \quad (5)$$

Čia b_{uzk} - srauto sparta, d_{uzk} – įeinančio ir išeinančio srauto filtravimas, e_{uzk} – svetainių įrašymas į atmintinę, f_{uzk} – apsauga nuo šnipinėjančių programų, g_{uzk} – iškylančių langų blokavimas, h_{uzk} – el. pašto apsauga nuo virusų, i_{uzk} - įsiskverbimo prevencijos sistema, j_{uzk} – VPN funkcija.

Prieigos lygmens komutatoriaus įvertį I_{KOMp} skaičiuosime pagal formulę:

$$I_{KOMp} = b_{kom} + c_{kom} \cdot k_1 + d_{kom} + e_{kom} + f_{kom} + g_{kom} + h_{kom}, \quad (6)$$

Čia b_{kom} – IEEE 802.1D, c_{kom} – IEEE 802.1Q, d_{kom} – QoS, e_{kom} - IEEE 802.1x, f_{kom} – ARP, g_{kom} – SPAN, h_{kom} - IEEE 802.3af.

Skirstomojo lygmens komutatoriaus įvertį I_{KOMs} skaičiuosime pagal formulę:

$$I_{KOMs} = b_{kom} + c_{kom} \cdot k_1 + d_{kom} + e_{kom} + f_{kom} + g_{kom} + n_{kom} + p_{kom} + r_{kom}, \quad (7)$$

Čia b_{kom} – IEEE 802.1D, c_{kom} – IEEE 802.1Q, d_{kom} – QoS, j_{kom} - TACACS+/RADIUS autentifikacija, k_{kom} - SSH /SSL, l_{kom} – Web grįsta autentifikacija, m_{kom} – MAC grįsta autentifikaciją, n_{kom} - DHCP, r_{kom} - ACLs.

Nepertraukiamos srovės šaltinio įvertį I_{UPS} skaičiuosime pagal formulę:

$$I_{UPS} = a_{ups} \cdot k_1 + b_{ups} + c_{ups} \cdot k_2, \quad (8)$$

Čia a_{ups} – veikimo laikas (pilna apkrova), b_{ups} – serverio išjungimo funkcijos palaikymas, c_{ups} – galingumas.

Asmeninės antivirusinės programinės įrangos įvertį I_{ANTa} skaičiuosime pagal formulę:

$$I_{ANTa} = b_{ant} \cdot k_1 + c_{ant} \cdot k_2 + l_{ant} + d_{ant} + e_{ant} + g_{ant} + i_{ant} + j_{ant} + k_{ant}, \quad (9)$$

Čia b_{ant} – atnaujinimo dažnumas, c_{ant} – valdymo sudėtingumas, d_{ant} – įeinančio pašto skanavimas, e_{ant} – išeinančio srauto skanavimas, g_{ant} – laikmenų skanavimas, i_{ant} – euristinis virusų atpažinimas, j_{ant} – apsauga tinkle, k_{ant} – virusų blokavimas, l_{ant} - automatinis failų valymas ir virusų šalinimas.

Antivirusinės programinės įrangos skirtos įmonei įvertį I_{ANT} skaičiuosime pagal formulę:

$$I_{ANTi} = b_{ant} \cdot k_1 + c_{ant} \cdot k_2 + d_{ant} + e_{ant} + g_{ant} + i_{ant} + k_{ant} + n_{ant} + p_{ant}, \quad (10)$$

Čia b_{ant} – atnaujinimo dažnumas, c_{ant} – valdymo sudėtingumas, f_{ant} – pašto skanavimas, h_{ant} – USB laikmenų skanavimas, i_{ant} – euristinis virusų atpažinimas, k_{ant} – virusų blokavimas, l_{ant} - automatinis failų valymas ir virusų šalinimas, m_{ant} – apsauga nuo nepageidaujamų laiškų, n_{ant} – užkardos funkcija.

2.1.5. Trečio lygio tipiniai struktūriniai elementai

Trečio lygio TSE mūsų nagrinėjamoje srityje sudarytų tinklo struktūriniai elementai. Nes kompiuterinis tinklas yra saugus kai visi jame esantys komponentai (kompiuteriai, serveriai, komutatoriai, maršrutizatoriai) yra tinkamai apsisaugoti. Reikalinga pasirinkti ir įdiegti apsaugos priemones kur kiekvienas tinklo elementas veikia kaip apsaugos taškas. Išskyrėme tokius tinklo struktūrinius elementus:

- Kompiuteris (stacionarus, nešiojamas),
- Serveris (pagal paskirtį: duomenų bazių, failų, spausdinimo, bei tinklo servisų - Web, DNS, Proxy, el. pašto) [34],
- Šliuzas - tinklų sąsaja (Gateway),
- Mobilieji įrenginiai (Smartphone, PDA).

Tam tikros DAP užtikrina apsaugą atitinkamiems tinklo struktūriniams elementams. Yra ir tokių DAP, kurios skirtos kelių skirtingų tinklo struktūrinių elementų apsaugai užtikrinti. Pavyzdžiui, nešiojamų kompiuterių diskai šifruojami tik šiai struktūrinio elemento grupei skirtomis apsaugos priemonėmis. Patartina daryti serveryje, stacionariame ar nešiojamajame kompiuteryje bei mobiliajame telefone saugomų svarbių duomenų atsargines kopijas ir jas laikyti saugioje vietoje. Mobiliųjų įrenginių elektros maitinimą užtikrina baterijos. Joms išsikrovus, įrenginys nebeveiks ir jame saugomi duomenys taps neprieinami. Todėl vykstant į ilgesnes keliones vertėtų pasirūpinti atsarginėmis baterijomis. Jei nešiojamasis kompiuteris yra naudojamas biure, reikėtų užtikrinti, kad juo nepasinaudotų arba nepavogtų įstaigos interesantai arba piktavaliai kolegos. Nešiojamąjį kompiuterį galima specialiu metaliniu lynu pritvirtinti prie stalo arba kitokio masyvaus ar gerai įtvirtinto daikto. Nešiojamieji kompiuteriai, taip pat kaip ir staliniai kompiuteriai, gali tapti virusų ir kitokios kenksmingos programinės įrangos taikiniu. Todėl reikėtų naudoti ir periodiškai atnaujinti antivirusinę programą, įdiegti naudojamas programinės įrangos pataisų paketus. Tai gali būti padaryta automatiškai, prijungiant nešiojamąjį kompiuterį prie įmonės kompiuterių tinklo ar interneto arba pernešant duomenų laikmenomis [35][36]. Pasirenkant DAP reikia atsižvelgti į tokius išorinius parametrus, kaip struktūrinių elementų kiekis, OS, pajėgumas, resursai ir pan.

2.2. Duomenų svarbos ir saugumo nustatymo taikymas

Organizacijoje esamos informacijos reikšmingumo lygmeniui nustatyti pasinaudosim dalimi kriterijų aprašytų 1.3.2. skyrelyje, padėsiančių nustatyti duomenų svarbumą. Kiekvienam iš kriterijų skirsime atitinkamą balų skaičių intervale nuo 1 iki 2 (1-netinkamas; 1,5-tinkamas; 2- labai tinkamas), arba atitinkamą balų skaičių (0-netinkamas arba 1-tinkamas).

24 lentelė

Duomenų svarbos nustatymas

Duomenų jautrumo kriterijus	Balai
Naudingumas duomenų	intervale nuo 1 (nenaudingi) iki 2 (labai naudingi)
Vertė duomenų	intervale nuo1 (nevertingi) iki 2 (labai vertingi)
Lygmuo žalos, kuri galėjo būti padaryta, jei duomenys buvo atskleisti	intervale nuo1 (mažas) iki 2 (labai didelis)
Lygmuo žalos, kuri galėjo būti padaryta, jei duomenys buvo pakeisti ar sugadinti	intervale nuo1 (mažas) iki 2 (labai didelis)
Ar už šių duomenų paviešinimą taikoma administracinė/baudžiamoji atsakomybė?	1
Ar reikalingas duomenų šifravimas?	1
VISO:	**10**

Šaltinis: sudaryta autorės

Bendras duomenų svarbumas bus vertinamas dešimties balų sistemoje (nuo 1 iki 10). Kuo svarbesni yra duomenys tuo daugiau dėmesio ir lėšų reikia skirti jų apsaugai, tačiau nenaudinga ir netikslinga už apsaugą mokėti daugiau negu yra verti patys duomenys. Atsakymai į šiuos klausimus ir padeda rasti tinkamą apsaugos ir jos kainos pasirinkimo variantą. Tokiu būdu organizacija gali identifikuoti savo saugumo reikalavimus ir palengvinti tinkamo duomenų apsaugos lygmens užtikrinimo pasirinkimą. Svarbu suderinti saugos lygmenį su reikalingomis jam užtikrinti investicijomis (žr. 1.3.2. skyrelį). Saugumo reikalavimai nustatomi įvertinant susijusią su informacijos praradimu saugos riziką, kuri skaičiuojama lyginant informacijos saugos valdymui skiriamas išlaidas su galimais veiklos nuostoliais praradus šią informaciją (žr. 1 ir 2 formules, 1.3.2. skyrelyje). Šis rizikos ir išliekamosios rizikos nustatymo būdas gana paprastas, lengvai suprantamas, todėl juo ir remsimės nustatant organizacijos saugios tinklo architektūros laipsnį prieš duomenų apsaugos priemonių parinkimą ir po parinkimo, o taip pat galėsime įvertinti ir išliekamąją riziką po atitinkamo saugos priemonių rinkinio parinkimo.

2.3. Duomenų apsaugos priemonių rinkinio įvertinimas

Esamą bei pasirinktą DAP rinkinį vertinsime pagal kainos ir patikimumo lygį. Pasirinktas DAP rinkinys laikomas priimtinesniu jei kainos ir patikimumo lygio atžvilgiu yra geresnis.

Atsirinkę kompiuterinės sistemos struktūrą bei nurodę išorinius apribojimus, keliamus DAP, (tokius kaip: veikimo terpė – operacinė sistema, kaina) ir turėdami atskirų DAP įverčius, galėsime paskaičiuoti bendrą DAP rinkinio kainą ir bendrą DAP rinkinio patikimumo koeficientą.

Pažymėkime *i*-tąjį DAP rinkinį R_i, o *i*-tojo rinkinio įvertį I_{Ri}, visų galimų DAP skaičių – *n*, kompiuterinėje sistemoje esančių skirtingų tipų struktūros elementų (kompiuteris, serveris ir pan.) skaičius *m*, tuomet:

$$I_{Ri} = k_1 \cdot \left(\sum_{j=1}^{n_1} c_j \cdot I_j \right) + k_2 \cdot \left(\sum_{j=1}^{n_2} c_j \cdot I_j \right) + \ldots + k_m \cdot \left(\sum_{j=1}^{n} c_j \cdot I_j \right), \quad (11)$$

kur $c_j = 0, \forall \ AP_j \notin \ _i$,kur $j = \overline{,n}$ ir I_j, kur $j = \overline{,n}$, atitinkamai yra lygus I_{UZKp}, I_{UZKt}, I_{KOMp}, I_{KOMs}, I_{UPS}, I_{ANTa}, I_{ANTi}. Čia c_j, j – tosios DAP svorinis koeficientas, k_l, $l = \overline{,m}$, l – tojo kompiuterinės sistemos struktūros elemento svorinis koeficientas.

Turėdami pasirinktų DAP rinkinius, skaičiuojame kiekvieno sudaryto rinkinio kainą, bei patikimumo koeficientus. Pasirenkame tą DAP rinkinį, kurio kaina yra mažesnė arba lygi naudotam priemonių rinkiniui, o rinkinio patikimumo koeficientas yra didesnis arba lygus esamam priemonių rinkiniui, jei šis buvo nurodytas. Renkantis naują DAP rinkinį, pasirenkamas labiausiai vartotojo poreikius atitinkantis DAP rinkinys.

Kad DAP rinkinio įvertinimas būtų lengvai suvokiamas nuspręsta gautus rezultatus grupuoti į kategorijas, atspindinčias duomenų saugumo lygį. Panašus grupavimas yra atliekamas saugumą vertinant pagal *ISO 15504* standartą grupuojant proceso atributus (žr. 8 lentelę). Gautus rezultatus sugrupuosim į penkis lygmenis, kur pirmas lygmuo yra aukščiausiais balais vertinama informacijos saugumo sistema, o penktasis lygmuo apibūdina kritinio patikimumo informacijos apsaugą (žr. 25 lentelę).

25 lentelė

Duomenų apsaugos priemonių įvertinimas

Patikimumo lygmenys	Įvertinimas	Procentinis įvertinimas (iš 100% galimų)
Pirmas	DAP patikimumas yra labai aukšto lygio	80,5-100%
Antras	DAP patikimumas yra aukšto lygio	60,5-80%
Trečias	DAP patikimumas yra patenkinamo lygio	40,5-60%
Ketvirtas	DAP patikimumas yra žemo lygio	20,5-40%
Penktas	DAP patikimumas yra kritinio lygio	0-20%

Šaltinis: sudaryta autorės

Turėdami tinkamų DAP katalogą, bei apsibrėžę visas galimas jų naudojimo struktūras atliekame pilną visų galimų DAP derinių perrinkimą. Šio perrinkimo metu skaičiuojame kiekvieno sudaryto rinkinio kainą, saugumo bei palankumo vartotojui lygių įverčius. Jei rinkinio parametrai

tenkina apribojimus tuomet jį priimame kaip vieną iš alternatyvių rinkinių, kuriuos galima naudoti konkrečioje kompiuterinėje sistemoje. Galiausiai turime pasirinkti vieną iš kelių ar keliolikos gautų alternatyvių DAP rinkinių.

3. DUOMENŲ APSAUGOS PRIEMONIŲ RINKINIO SUDARYMO IR ĮVERTINIMO METODIKOS EKSPERIMENTINIS TYRIMAS

Eksperimentinio tyrimo dalyje aprašyta pasiūlytos metodikos tinkamumui pagrįsti ir patikrinti pasirinktas DAP rinkinys, atlikti eksperimentai.

3.1. Duomenų rinkimas apie galimų realizacijos DAP

DAP rinkiniams sudaryti duomenys rinkti iš įvairių kompiuterine įranga prekiaujančių firmų kainoraščių ir tinklalapių, kuriuose pateikta informacija apie DAP funkcines savybes ir kainą. Kainos pateiktos litais už vienetą. Eksperimentui atlikti pasirinktos tokios DAP: užkardos, antivirusinės programos, komutatoriai, UPS. Užkardų parametrų reikšmės pateiktos 28 lentelėje, komutatorių – 29 lentelėje, UPS - 30 lentelėje, o antivirusinių programų tinkančių personaliniam kompiuteriui bei namų ofisui 31 lentelėje, bei antivirusinių programų tinkančių mažo bei vidutinio dydžio įmonėms 32 lentelėje. DAP parametrų reikšmių lentelėse pateikti jau paskaičiuoti pagal įverčio formules DAP patikimumo koeficientai ir išreikšti procentais. Taip bus lengviau vertinti DAP pagal vertinimo lentelę (žr. 25 lentelė). Prieš vertinant DAP, pirmiausiai siūloma jas suklasifikuoti išorinių parametrų atžvilgiu. Pavyzdžiui, prieš vertinant technines užkardas tikslinga suskirstyti jas pagal vartotojų skaičių (žr. 11 lentelę). Komutatorius tikslinga skirstyti pagal rūšis, UPS – pagal įmonės dydį, antivirusines - pagal atnaujinimo dažnumą. Svoriniai koeficientai (k_1, k_2) naudojami formulėse skaičiuojant atitinkamų DAP įverčių reikšmes (žr. 2.1.4. skyrelį). Toliau pateiksiu svorinių koeficientų lentelę, taikomą sugrupuotoms DAP pagal išorinius parametrus:

26 lentelė

DAP svoriniai koeficientai

DAP	**DAP klasifikavimo parametras**	**Parametro reikšmė**	**Svorinis koeficientas (k_1)**	**Svorinis koeficientas (k_2)**
Tinklo užkarda	Vartotojų skaičius	< 50	0,3	-
Tinklo užkarda	Vartotojų skaičius	51-1000	0,03	-
Tinklo užkarda	Vartotojų skaičius	1001-5000	0,015	-
Tinklo užkarda	Vartotojų skaičius	> 5000	0,0001	-
Komutatorius	Prieigos lygmens	-	0,0001	0,0015
Komutatorius	Skirstomojo lygmens	-	0,0005	0,0015
UPS	Įmonės dydis	Namų / Maža	0,0015	0,014
UPS	Įmonės dydis	Maža / Vidutinė	0,03	0,003
UPS	Įmonės dydis	Didelė	0,03	0,0015
Antivirusinė	Atnaujinimo dažnumas	Kas minutę	0,4	0,2
Antivirusinė	Atnaujinimo dažnumas	Kas valandą	0,3	0,2
Antivirusinė	Atnaujinimo dažnumas	Kasdien	0,2	0,2
Antivirusinė	Atnaujinimo dažnumas	Kas savaitę	0,1	0,2

Šaltinis: sudaryta autorės

Pateiksime atskirų DAP patikimumo koeficiento įverčio skaičiavimo pavyzdį pagal 4-10 formules. Techninės užkardos patikimumo koeficiento įverčio skaičiavimas pagal 5 formulę. Gautą reikšmę išreiškiame procentais.

$$I_{UZKt} = 30000 \cdot 0{,}0001 + \; + \; + \; + \; + \; + \; + \; = 3 * 100 = 80(\%)$$

Čia į formulę įstatytos reikšmės (b_{uzk}, d_{uzk}, e_{uzk}, f_{uzk}, g_{uzk}, h_{uzk}, i_{uzk}, j_{uzk}) paimtos iš 28 lentelės, kurios santrauka dėl patogumo pateikta 27 lentelėje.

27 lentelė

Užkardos Juniper NetScreen-5400 parametrų reikšmės

Pavadinimas	Duotos reikšmės		Įvestos reikšmės								Rezultatų reikšmės
	Srauto sparta (Mbps)	Kaina (Lt)	Tipas	Įeinančio ir išeinančio srauto filtr.	Svetainių rašymas į atmintinę	Apsauga nuo šnipinėjančios PĮ	Iškylančių langų blokavimas	E-pašto apsauga (nuo virusų)	IPS	VPN	Patikimumas paskaičiuotas pagal (5) formulę
Juniper NetScreen-5400	30000	95600	T	1	1	0	0	1	1	1	80%

O svorinis koeficientas (k_i) paimtas iš 26 lentelės. Šis svorinis koeficientas taikomas tinklo užkardai, kai numatomas įmonėje vartotojų skaičius >5000. O iš 11 lentelės matyti, jog tinklo užkardos, kurių srauto sparta >200 Mbps, tinka įmonėms, kuriose numatomas vartotojų skaičius >5000.

28 lentelė

Užkardų parametrų reikšmės

Pavadinimas	Duotos reikšmės				Įvestos reikšmės								Rezultatų reikšmės
	Valdymo sudėtingumas	Operacinė sistema	Srauto sparta (Mbps)	Kaina (Lt)	Tipas	Įeinančio ir išeinančio srauto filtr.	Svetainių rašymas į atmintinę	Apsauga nuo šnipinėjančios PĮ	Iškylančių langų blokavimas	E-pašto apsauga (nuo virusų)	IPS	VPN	Patikimumas paskaičiuotas pagal (5) formulę
ZoneAlarm Pro	10	Windows 7/Vista/XP	-	72	P	1	1	1	1	1	-	-	-
Agnitum Outpost Firewall	10	Windows XP/Server 2003/2000/98/ME	-	138	P	1	1	1	1	1	-	-	-
Norman Personal Firewall	9	Windows XP/2000/98/95/NT/ME	-	135	P	0	1	1	0	0	-	-	-
eConseal Pro	10	Windows XP/2000/98/95/NT/ME	-	84	P	1	1	0	1	0	-	-	-
Webroot Desktop Firewall	8	Windows Vista/XP	-	48	P	1	1	0	0	1	-	-	-
Injoy Firewall	8	Windows XP/Server 2003/2000/98/95/ME	-	72	P	1	1	0	0	1	-	-	-
Cisco ASA5580-40	-	-	10000	186125	T	1	1	0	0	0	0	1	40%
Cisco ASA5505 Base	-	-	150	173	T	1	1	0	0	0	1	1	60,25%
Juniper NetScreen-5400	-	-	30000	95600	T	1	1	0	0	1	1	1	80%
Juniper NetScreen-5200	-	-	10000	28680	T	1	1	0	0	1	1	1	60%

Šaltinis: sudaryta autorės pagal [16]

29 lentelė

Komutatorių parametrų reikšmės

Pavadinimas	Duotos reikšmės					Įvestos reikšmės													Rezultatų reikšmės
	IEEE 802.1Q	Kaina (Lt)	Valdymo sudėtingumas	Jungčių kiekis	Plėtimo galimybė	Tipas	Įmonės dydis	IEEE 802.1D	QoS	IEEE 802.1x	ARP	SPAN	IEEE 802.3af	TACACS+ /RADIUS Autentifik.	SSH /SSL	Web autenti-fikavimas	MAC autenti-fikavimas	DHCP	ACLs	Patikimumas paskaičiuotas pagal (6, 7) formules
Procurve Switch 2510-24	64	1224	3	24	0	L2	M	1	1	1	0	0	0	1	1	1	1	0	0	70%
Procurve Switch 2510-24G	64	1739	3	20	0	L2	M	1	1	1	0	0	0	1	1	1	1	0	0	70%
ProCurve Switch 2510G-48	64	3553	3	44	0	L2	M	1	1	1	0	0	0	1	1	1	1	0	0	70%
ProCurve Switch 2510-48	64	1913	3	48	0	L2	M	1	1	1	0	0	0	1	1	1	1	0	0	70%
ProCurve Switch 2524	30	1545	2,5	24	0	L2	M	1	1	1	0	0	0	1	1	0	0	0	0	50%
ProCurve Switch 6600-24XG	2048	40454	5	21	0	L3	D	1	1	1	1	0	0	1	1	1	1	1	1	100%
ProCurve Switch 5304xl	256	5216	5	0	4	L3	M/V	1	1	1	1	0	1	1	1	1	1	1	1	100%
ProCurve Switch 5308xl	256	7896	5	0	8	L3	M/V	1	1	1	1	0	1	1	1	1	1	1	1	100%
Procurve Switch 5406zl 48G	2048	19764	5	48	6	L3	M/V	1	1	1	1	0	1	1	1	1	1	1	1	100%
Procurve Switch 5406zl	2048	6410	5	0	6	L3	M/V	1	1	1	1	0	1	1	1	1	1	1	1	100%
Procurve Switch 5412zl 96G	2048	45359	5	96	12	L3	M/V	1	1	1	1	0	1	1	1	1	1	1	1	100%
Procurve Switch 5412zl	2048	13967	5	0	12	L3	M/V	1	1	1	1	0	1	1	1	1	1	1	1	100%
Procurve Switch 8212zl	2048	58170	5	0	12	L3	D	1	1	1	1	0	1	1	1	1	1	1	1	100%
Procurve Switch 4208vl	256	5968	5	0	8	L3	D	1	1	1	0	0	0	1	1	1	1	1	0	70%
Procurve Switch 4208vl-72GS	256	10618	4	72	8	L3	D	1	1	1	0	0	0	1	1	1	1	1	0	70%
Procurve Switch 4208vl-96	256	12458	4	96	8	L3	D	1	1	1	0	0	0	1	1	1	1	1	0	70%
Procurve Switch 4204vl	256	3899	4	0	4	L3	D	1	1	1	0	0	0	1	1	1	1	1	0	70%
Procurve Switch 4204vl-48GS	256	7801	4	48	4	L3	D	1	1	1	0	0	0	1	1	1	1	1	0	70%
Procurve Switch 4202vl-72	256	9606	4	0	2	L3	D	1	1	1	0	0	0	1	1	1	1	1	0	70%

Šaltinis: sudaryta autorės

30 lentelė

UPS parametrų reikšmės

Pavadinimas	Duotos reikšmės			Įvestos reikšmės		Rezultatų reikšmės
	Galingumas	Veikimo laikas (min)	Kaina (Lt)	Tipas	Serverio išjungimas	Patikimumas paskaičiuotas pagal (8) formulę
APC Back-UPS CS 350	350	4,7	277	I	0	49%
APC Back-UPS ES 550	550	3,2	310	I	0	77%
APC Back-UPS CS 500	500	2,4	330	I	0	70%
APC Back-UPS CS 650	650	2,4	600	I	0	91%
HP UPS T1000 G3	1000	5	930	I	1	41,5%
HP UPS T1500 G3	1400	6	1126	I	1	53,8%
HP UPS T1000 G2	1000	4	1400	I	1	41,2%
HP UPS T1500 XR	1500	6,5	1438	I	1	56,95%
ORV UPS 1500VA SIN/RT2U/(X)IEC320	1500	5	1600	M	1	56,5%
HP UPS R1500 G2	1500	5	1870	M	1	56,5%
ORV UPS ORVALDI 2000RT SINUSOIDA 2U	2000	5	2065	M	1	71,5%
HP UPS R/T3000	3000	4	3482	M	0	91,2%
HP UPS R5500	6000	5	10.800	M	1	100%

Šaltinis: sudaryta autorės

31 lentelė

Antivirusinės programinės įrangos skirtos kompiuteriui parametrų reikšmės

Pavadinimas	Duotos reikšmės			Įvestos reikšmės							
	OS	Atnaujinimo dažnumas	Valdymo sudėtingumas	Įeinančio pašto srauto skanavim.	Išeinančio pašto srauto skanavim.	Laikmenų skanavimas	Euristinis virusų atpažinimas	Apsauga tinkle	Virusų blokavimas	Automatinis failų valymas ir virusų šalinimas	Kaina (Lt)
BitDefender Antivirus	Windows 7/Vista/XP	Kas valandą	10	1	1	1	1	0	1	1	60
Kaspersky Anti-Virus	Windows 7/Vista/XP	Kas valandą	10	1	1	1	1	1	1	1	143
Webroot AntiVirus with SpySweeper	Windows 7/Vista/XP	Kas valandą	10	1	1	1	1	1	1	1	72
Norton AntiVirus	Windows 7/Vista/XP	Kas 5-15 min.	10	1	1	1	1	1	1	1	96
ESET Nod32 Antivirus	Windows 7/Vista/XP/2000	Prireikus	10	1	1	1	1	1	1	1	84
AVG Anti-Virus	Windows 7/Vista/XP/2000	Kas valandą	10	1	1	1	1	0	1	1	96
F-Secure Anti-Virus	Windows 7/Vista/XP	Kas 2 val	10	1	1	1	1	1	1	1	60
G DATA AntiVirus	Windows 7/Vista/XP	Kas valandą	10	1	1	1	1	1	1	1	60
Avira AntiVir	Windows Vista/XP/2000	Kas valandą	9	1	1	1	1	0	1	1	64
Trend Micro	Windows 7/Vista/XP	Kas valandą	10	1	1	1	0	0	1	1	95
AVAST! Antivirus with Anti-Spyware	Windows Vista/XP/2000	Kasdien	9	1	1	1	1	0	1	1	95
McAfee VirusScan	Windows 7/Vista/XP/2000	Kas 4 val.	9	1	0	0	1	0	1	1	72
ZoneAlarm Antivirus	Windows 7/Vista/XP	Prireikus	9	0	1	1	1	0	1	1	48
CA Antivirus	Windows 7/Vista/XP/2000	Kas valandą	10	1	1	0	1	0	1	1	119
Panda Antivirus	Windows 7/Vista/XP	Kasdien	9	1	1	1	1	0	1	1	119
Vipe Antivirus + Antispyware	Windows 7/Vista/XP	Kas valandą	10	1	1	1	1	1	1	1	72
CyberDefender Early Detection Center	Windows Vista/XP	Kasdien	9	1	0	0	0	1	1	1	72
PeretoLogic Anti-Virus PLUS	Windows Vista/XP/2000	Kasdien	9	0	0	1	0	0	1	1	95
Norman Antivirus & Antispyware	Windows 7/Vista/XP/2000	Kasdien	5	1	1	0	1	0	1	1	119
PC Tools AntiVirus	Windows Vista/XP/2000	Kas valandą	6	1	1	1	1	0	1	1	72
ViRobot Desktop	Windows 7/Vista/XP/2000	Kas 4 val.	7	1	1	1	0	0	1	1	79
F-Prot	Windows 7/Vista/XP/2000	Kasdien	6	0	1	1	1	0	1	1	69

Šaltinis: sudaryta autorės pagal [17]

32 lentelė

Antivirusinės programinės įrangos skirtos įmonei parametrų reikšmės

Pavadinimas	Duotos reikšmės					Įvestos reikšmės							Rezultatų reikšmės
	OS	Atnaujinimo dažnumas	Valdymo sudėtingumas	Licencijų kiekis (vnt)	Kaina (Lt)	Pašto skanavimas	Apsauga nuo „Spam“	Užkarda	USB laikmenų skan.	Euristinis virusų	Virusų blokavimas	Automatinis failų valymas	Patikimumas paskaičiuotas pagal (10) formulę
Kaspersky Business Space Security	Windows Vista/XP/2000/ Server/2000/ 2003/2008/ Linux/ Novell Netware /Samba	Kas valandą	10	10-150	932	1	1	1	1	1	1	0	83%
BitDefender Small Office Security	Windows Vista/XP/2000/ Server 2000/2003/2008/ Linux/ Samba	Kas valandą	10	5+	1074	1	1	1	1	1	1	1	93%
ESET NOD32 Antivirus	Windows Vista/XP/2000/ Server 2000/ 2003/2008 / Linux	Kai reikia	8	5-10000	1027	1	1	1	1	1	1	1	90%
G Data AntiVirus Business	Windows Vista/XP/2000/ Server 2003/2008	Kas minutę	9	1-1 mln.	537	1	1	0	0	1	1	1	72%
Avast! Standart Suite	Windows Vista/XP/2000/ Server 2000/2003	Kas dvi savaites	9	10-199	1002	1	0	0	0	1	1	0	49%
Panda Security for Business	Windows Vista/XP/2000/ Server 2000/ 2003/2008 Linux / Novell Netware	Kasdien	9	5-2000	2134	1	1	1	1	1	1	1	90%
Symantec Endpoint Protection	Windows Vista/XP/2000/ Server 2000/ 2003/2008/ Linux / Novell Netware	Kasdien	8	5-1000	1294	1	0	1	0	1	1	1	68%
CA Threat Manager	Windows Vista/XP/2000/ Server 2000/2003/2008	Kasdien	8	1-2499	1649	1	1	1	0	1	0	0	58%
AVG Antivirus	Windows Vista/XP/2000/ Server 2000/ 2003/2008 / Linux	Kasdien	8	2-200	716	0	1	1	0	0	1	0	48%
F-Secure Small Business Suite	Windows Vista/XP/2000/ Server 2000/ 2003/2008/ Linux	Kasdien	9	5-4999	1806	1	0	1	1	1	1	0	70%
Sophos AntiVirus	Windows Vista/XP/2000/ Server 2000/2003	Kas valandą	8	3-100	901	0	0	0	1	1	1	0	49%
Avira AntiVir Network Bundle	Windows Vista/XP/2000/ Server 2000/ 2003/2008 / Linux	Kasdien	7	1-100	1068	1	0	0	0	1	1	1	56%
McAfee VirusScan	Windows Vista/XP/2000/ Server 2000/ 2003	Kasdien	8	1-100	1229	1	0	1	0	1	1	0	58%

Šaltinis: sudaryta autorės pagal [18]

Sudaryti DAP rinkiniai orientuoti daugiau į mažas ir vidutinio tipo įmones. Taip pat dalis rinkiniuose esančių DAP tinka ir pavieniams kompiuteriams, bei stambioms organizacijoms. Į DAP rinkinį įtraukus didesnį apsaugos priemonių spektrą, galima būtų atlikti išsamesnį apsaugos vertinimą. Tačiau mūsų tikslas nėra išsami DAP vertinimo sistema. Todėl vertinsime tik apsibrėžtą DAP rinkinį. Pradžioje apsirašysime organizacijoje naudojamas DAP ir kompiuterizuotos sistemos pagalba išrinksime jas iš sudarytų rinkinių. Taip galėsime palyginti ir įvertinti esamo rinkinio apsaugos lygį su alternatyviais variantais.

Sudarytus DAP rinkinius, nuolat atnaujinant, papildant naujais duomenimis, būtų galima panaudoti kitų įmonių DAP parinkimui ir įvertinimui.

Eksperimento, kiekybinių tyrimų patikimumą garantuotų pakankamai didelė ir pagrįstai sudaryta tyrimo imtis (įvairiarūšių DAP rinkiniai), kurie atspindėtų visus tiriamų DAP sluoksnius. Kokybinių tyrimų pakankamumą garantuoja išsamus, įvairiapusiškas DAP rinkinio aprašymas, kelių DAP rinkinių palyginimas.

Tyrimui atlikti pasirinkau realią organizaciją. Šioje įmonėje dirbu ketverius metus, todėl išvados remiasi geresniu įmonės veiklos konteksto bei tinklo architektūros apsaugos priemonių pažinimu. Renkant duomenis laikytasi konfidencialios informacijos nutekėjimo pasižadėjimo taisyklių.

3.2. Duomenų apdorojimas ir analizė

Sudarytai DAP kompiuterizuoto parinkimo ir įvertinimo metodikai patikrinti atliktas eksperimentinis tyrimas, panaudojant skirtingus analizės įrankius. Pirmiausiai eksperimentinį tyrimą buvo bandyta atlikti sukuriant ekspertinę sistemą. Buvo atsižvelgta į tai, jog šiuo metu vis daugiau dėmesio skiriama į žiniomis grindžiamas IS, kitaip ekspertines sistemas. Šios sistemos vadinamos kompiuterinėmis programomis, darančiomis išvadas arba sprendžiančios tam tikros dalykinės srities uždavinius. Ekspertinė sistema naudojasi žiniomis ir analizės taisyklėmis, apibrėžtomis tos srities ekspertų. Taip pat analizuoja duomenis ir pateikia išvadas [19]. Ekspertinei sistemai sukurti buvo pasirinkta „*Expertise2go – Web-Enabled Expert Systems*“ programinė įranga. Su *eXpertise2Go* ekspertinės sistemos kūrimui naudojami du įrankiai: *E2gRuleEngine* ekspertinės sistemos kūrimo įrankis arba „*Shell*“ ir *e2gRuleWriter* sprendimo lentelė. Ši programinė įranga yra nemokama, dėl to ją galima panaudoti realių problemų sprendimui. Taip pat yra pateiktas išsamus ekspertinės sistemos kūrimo aprašymas bei galimybė parsisiųsti pavyzdžius (sukurtas mini ekspertines sistemas), su kuriais galima eksperimentuoti ir sėkmingai išmokti su *eXpertise2Go* įrankiais kurti ekspertines sistemas.

e2gRuleWriter sprendimo lentelė (angl. decision table) skirta atributų įvedimui ir taisyklių sukūrimui. Sprendimų lentelė – stačiakampė matrica susidedanti iš eilučių, kuriose aprašoma sąlygos ir veiksmai, bei stulpelių, kuriuose sudaromos taisyklės. Gale matricos pasirenkamas rekomenduojamas sprendimas. Atributai – kintamieji, aprašantys reikšmes, kurios gali būti trijų tipų: skaičiai, tekstas, ar loginės reikšmės (true/false). Atributai sudaro faktines žinias žinių bazėje. *Certainy Factor* (CF) – patikimumo priskyrimas atributo vertei nustatyti. Išreiškiamas procentais (nuo 0 iki 100%). 100% arba 1,0 reiškia, kad atributo reikšmė (vertė) yra žinoma. Tikslas (angl. Goal) – priskirtas atributas, nustatyti vieną arba daugiau reikšmių, atsižvelgiant į taisyklių išvadas (žr. 1 priedą).

Žinių bazės sudarymo matricinės lentelės pagalba privalumai:

- Sprendimai pateikiami lentelėje lengviau supaprastinami, nes yra skaidrūs ir nedviprasmiški. Kiekviena taisyklė (atskiras stulpelis) gali būti aiškinamas (pavadinamas) individualiai, santrumpomis: jei sąlygos yra įvykdytos, turi būti atlikti nurodyti veiksmai taisyklėje.
- Sprendimų lentelę galima papildyti tos srities ekspertų žiniomis.
- Lengva žinių bazės priežiūra, išvengiant klaidų. Sistema nebepasileidžia jeigu pasitaiko klaida atlikus žinių bazės redagavimą, išmetamas klaidos pranešimas su kodu, pagal kurį, klaidų kodų lentelėje galima pasižiūrėti kokia klaida įvyko.

Žinių bazės sudarymo matricinės lentelės pagalba trūkumai:

- Norint realizuoti, pateikti žinių bazėje sukauptą informaciją reikia išmokti dirbti su kita programine aplinka – ekspertinės sistemos apvalkalu.
- Yra galimybė sprendimų lentelę konvertuoti į žinių bazę, tačiau nėra galimybės iš žinių bazės konvertuoti į sprendimų lentelę.

Problema sprendžiama naudojant taisyklių „Jei... tai...“ logiką. Tokiu būdu randamas „geriausio“ sprendimo variantas iš daugybės kitų galimų sprendimų. Ekspertinės sistemos išvadų darymo mechanizmas paremtas *Forward chaining* (tiesioginio išvedimo) principu.

Reikalavimai *e2gRuleWriter* paleisti: turi būti įdiegta ne žemesnė nei *1.6.x Java Runtime Engine (JRE)* aplinka. *e2gRuleWriter yra Java* programinė įranga, ne apletas, kuri pasileidžiama per internet naršyklę. Žinių bazė paleidžiama su *E2gRuleEngine*, naudojant *web* tinklapį (.htm), kuriame įterptos atitinkamos *Java Applet* komandos.

Ekspertinė sistema, buvo kuriama keturioms pasirinktoms DAP rūšims: užkardoms, komutatoriams, antivirusinėms programoms, UPS. Ekspertinė sistema sudaryta iš 147 taisyklių, kurios paremtos *IF/THEN* pagrindu. Kadangi ekspertinėje sistemoje realizuoti 72 klausimai, todėl buvo sukurti 72 statiniai kintamieji, kurių dėka buvo sudaryti sistemos klausimai. Taip pat buvo panaudoti 102 ”*confidence*” kintamieji, kurių pagalba buvo realizuoti sistemos išėjimai (atsakymai -

patarimai). Ekspertinės sistemos sudėtį papildžius dar vienu statiniu kintamuoju, kuris atitiktų atitinkamą parametrą pasirenkant papildomai įvestą tikrinį kintamąjį, buvo viršytas programos pajėgumas. Padaryta išvada, jog *eXpertise2Go* programinis įrankis yra netinkamas mūsų eksperimentiniam tyrimui atlikti.

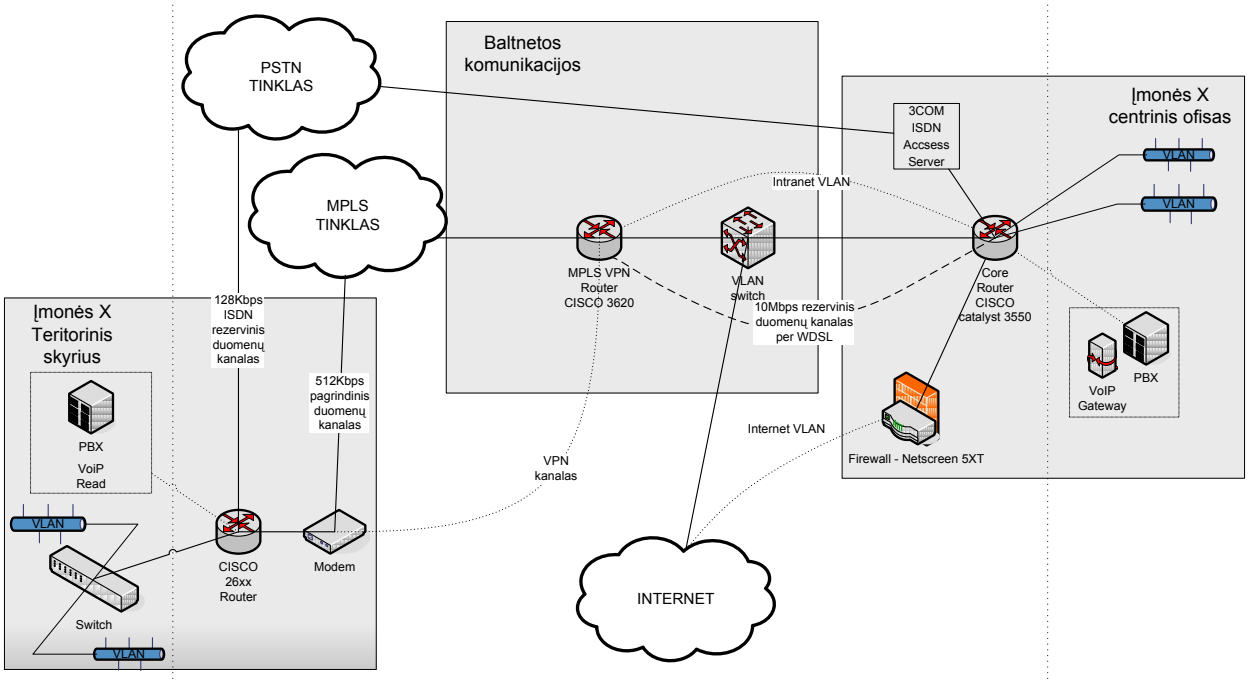
Todėl pasirinkome kitą „Exsys *CORVID Knowledge Automation Expert System Software*“ programinę įrangą. Tai viena sėkmingiausių ekspertinų sistemų įrankių. EXSYS programinė įranga paverčia žinių verslo ekspertus į interaktyvias sistemas, kurias galima tiekti per Interneto svetaines. EXSYS produktai yra panaudoti daugiau kaip 50% sėkmingiausių kompanijų, daugelyje vyriausybinių ir karinių agentūrų, ir tūkstančiuose firmų ir organizacijų [40]. Duomenys į ekspertinę sistemą įvesti iš pateiktų 28-32 lentelėse, sudarant taisyklių rinkinį. Programos sudarytas taisyklių medis pateiktas 4 priede, o langų pavyzdžiai 2 priede.

DAP kompiuterizuoto parinkimo ir įvertinimo metodikai patikrinti pasirinkta reali įmonė X, turinti 50 nutolusių padalinių. Padalinys Vilniuje yra pagrindinis, ten dirba dauguma įmonės darbuotojų, naudoja daugiausiai kompiuterinių resursų. Kituose padaliniuose darbuotojai iš kompiuterizuotų darbo vietų turi priėjimą prie interneto ir vidinių bendrų resursų.

X įmonėje suinstaliuotas neekranuotas tinklas (6 kategorijos UTP kabeliai 4x2x0.5 gyslos su PVC izoliacija, 6 kategorijos RJ45 tipo lizdai, 19“ 6 kategorijos 24 prievadų komutacinės panelės, 6 kategorijos komutaciniai kabeliai). Tinklo komutacijai ir aktyvinei tinklo įrangai sumontuoti įrengta komutacinė spinta. Tinklo kabeliai iš komutacinės spintos pakloti instaliaciniuose PVC loveliuose iki darbo vietos rozetės – po du Cat.6 UTP kabelius. Visi įmonėje esantys kompiuteriai ir serveriai turi tinklo adapterius užtikrinančius TCP/IP protokolo veikimą ir galinčius duomenis persiųsti 1 Gbps sparta.

Tinklo prieigos kontrolės architektūra naudoja įvairių aplikacijų teikiamas paslaugas: DHCP, IAS (RADIUS), DNS, AD infrastruktūrą. Visas šias paslaugas teikia vietiniai vartotojų autentifikavimo serveriai. Autentifikavimas vyksta naudojant PEAP protokolą.

Įmonės intranetinio tinklo ir interneto ryšio realizacijos schema pavaizduota 8 paveiksle.



Šaltinis: sudaryta autorės

8 Pav. X įmonės intranetinio tinklo ir interneto ryšio realizacijos schema

X įmonės tinklas su paslaugų tiekėjo tinklu sujungtas optika. Internetinių paslaugų tiekėjas teikia nutolusių padalinių sujungimo vieną pažangiausių MPLS technologija grindžiamą paslaugą.

Kad užtikrintų duomenų ir viešųjų paslaugų teikimo saugumą įstaiga naudoja sekančias apsaugos priemones:

Programinės saugumo užtikrinimo priemonės:

- Naudojama įsibrovimo susekimo programa IDS.
- Centralizuotai įdiegta antivirusinė ir užkardos programinė įranga.
- Centralizuotai diegiami kompiuterizuotų darbo vietų OS atnaujinimai.
- IS naudotojai autentifikuojami kompiuteriniame tinkle.
- Kiekvienas sistemos naudotojas IS unikaliai atpažįstamas – IS naudotojas turi patvirtinti savo tapatybę slaptažodžiu.
- Slaptažodžiai kuriami, naudojamas ekrano užsklandos slaptažodžio įsijungimas ir kiti saugumo parametrai nustatomi, vadovaujantis įmonės AD (angl. Active Directory) sistemos saugumo politikos nuostatomis.
- Institucijos duomenų centrui taikomas trijų lygių tinklo saugumas: išorė/duomenų bazės, kiekvieną iš lygių atskiriant užkardomis (angl. Firewall).
- Institucijos administravimo įstaigų vietiniai kompiuterių tinklai organizuojami pagal tarptautinių standartų reikalavimus, atsižvelgiant į tinkle esančius resursus, sistemų naudotojų

grupes bei duomenų saugumui keliamus reikalavimus. Vietiniuose tinkluose naudojami valdomi aktyvinai tinklo elementai, kurių būklė pastoviai stebima.

- Internet ar kitame tinkle esantys duomenys ar resursai, taip pat duomenys ir resursai institucijos kompiuteriniame tinkle iš internet ar kitų tinklų, gali būti pasiekiama tik per institucijos lokaliame tinkle esančius „vartus“, kurie yra griežtai kontroliuojami.
- Nešiojamų kompiuterių diskai šifruojami.
- IS darbo stebėjimui ir analizei, siekiant užtikrinti duomenų apsaugą, naudojamos saugumo ir pažeidžiamumų valdymo sistemos.
- Naudojamos specializuotos sistemos, perspėjančios administratorius, kai IS techninėje įrangoje sumažėja iki nustatytos ribos laisvos atminties ar vietos diske, ilgą laiką apkraunama kompiuterių tinklo sąsaja, naudotojo darbą imituojančios procedūros vyksta per lėtai ir pan..
- Bendri (mainų) prieigos katalogai nenaudojami kompiuterizuotose darbo vietose, o reikalui esant suteikiama autorizuota prieiga.

Fizinės patikimumo užtikrinimo priemonės:

- Serveriams naudojami - nepertraukiamo maitinimo šaltinis, dubliuoti maitinimo šaltiniai, tinklo adapteriai, ventiliatoriai, priemonės, apsaugančios nuo diskinių įrenginių gedimų.
- Nešiojamiems kompiuteriams – plieniniai lyneliai.

IS tvarkomos elektroninės informacijos klasifikavimas, jos priskyrimas kategorijai valstybinės institucijos IT sistemų kritiškumo vertinimo tvarkos aprašas, kuriame sudaryta IT saugumo atitikties vertinimo metodika. Pagal šią metodiką periodiškai atliekamas IS saugumo vertinimas. Metodika parengta remiantis bendraisiais duomenų saugos reikalavimais, Lietuvos standartu *LST ISO/IEC 17799:2000*, Lietuvos ir tarptautiniais grupės „Informacijos technologija“. Saugumo technika“ standartais, reglamentuojančiais saugų duomenų tvarkymą. IT saugos atitikties įstaigos IS vertinimas atliekamas vertinant atskirai kiekvieną objektą. Objektas vertinamas pagal penkių balų skalę, kurioje žemiausia reikšmė yra vienetas, o aukščiausia – penketas:

- vienetas – nėra vertinamo objekto;
- dvejetas – parengtas vertinamo objekto projektas;
- trejetas – vertinamas objektas patvirtintas, tačiau netaikomas (nesivadovaujama parengtomis priemonėmis ar procedūromis, vartotojai nesupažindinti su jomis, nepaskirtas atsakingas vykdytojas ir pan.);
- ketvertas – vertinamas objektas taikomas, tačiau rasta nežymių trūkumų, kurie nurodomi pastabose;
- penketas – vertinamas objektas taikomas.

Parengiama IS saugos atitikties vertinimo ataskaita, pagal kurią organizuojamas trūkumų šalinimo priemonių planas.

Išskiriame eksperimentiniam tyrimui organizacijoje naudojamas šias DAP:

- Užkarda - *Juniper NetScreen-5200*;
- Komutatoriai - *Procurve Switch 2524* (2 vnt), *Procurve Switch 5304xl* (5 vnt), *Procurve Switch 5308* (3 vnt), *Procurve Switch 5406zl* (53 vnt);
- UPS - HP T1500XR (80 vnt) ir HP UPS R/T 3000 (60);
- Antivirusinė - *Symantec Endpoint Protection* (apie 4000 licencijų).

Pagal naudojamo DAP rinkinio charakteristikas pasinaudodami sukurta ekspertine sistema atrenkame siūlomas DAP (žr. 3 priedas). Naudojamą DAP rinkinį susivedame į lentelę (žr. 33 lentelę), priemonių rinkinio kainos ir patikimumo koeficientų su gautu alternatyviu rinkiniu palyginimui.

33 lentelė

Įmonės X naudojamas DAP rinkinys

Priemonė	Pavadinimas	Vieneto kaina (Lt)	Kiekis	Kaina (Lt)	Patikimumas
Užkarda	Juniper NetScreen-5400	95600	1	**95600**	**80%**
Komutatorius	Procurve Switch 2524	1545	2	3090	50%
Komutatorius	Procurve Switch 5304xl	5216	5	26080	100%
Komutatorius	Procurve Switch 5308xl	7896	3	23688	100%
Komutatorius	Procurve Switch 5406zl	6410	53	339730	100%
			VISO:	**388411**	**87,5%**
UPS	HP T1500XR	1438	80	115040	56,95%
UPS	HP UPS R/T3000	3482	60	208920	91,2%
			VISO:	**323960**	**74, 08%**
Antivirusinė	Symantec Endpoint Protection	1295	4	**5179**	**68%**
			IŠ VISO:	**1992243**	**77,27%**

Šaltinis: sudaryta autorės

Pasinaudodami gautais ekspertinės sistemos rezultatais sudarome antrąjį DAP rinkinį, pateiktą 34 lentelėje.

34 lentelė

Alternatyvus DAP rinkinys sudarytas ekspertinės sistemos pagalba

Priemonė	Pavadinimas	Vieneto kaina (Lt)	Kiekis	Kaina (Lt)	Patikimumas
Užkarda	Juniper NetScreen-5200	28680	1	**28680**	**60%**
Komutatorius	Procurve Switch 2524	1545	2	3090	50%
Komutatorius	Procurve Switch 4204vl	3899	5	19495	70%
Komutatorius	Procurve Switch 4208vl	5968	3	17904	70%
Komutatorius	Procurve Switch 5406zl	6410	53	339730	100%
			VISO:	**380219**	**72,5%**
UPS	HP UPS T1500 XR	1438	80	115040	56,95%
UPS	HP UPS R/T3000	3482	60	208920	91,2%
			VISO:	**323960**	**74,08%**
Antivirusinė	Symantec Endpoint Protection	1294	4	**5176**	**68%**
			IŠ VISO:	**184509**	**68.65%**

Šaltinis: sudaryta autorės

Iš lentelės matyti, jog procentaliai sumažėjo rinkinio patikimumo koeficientas, tačiau kaip ir pirmojo rinkinio atveju, patenka į apsibrėžtą diapozoną (60,5-80%), rodantį, jog DAP patikimumas yra aukšto lygio (žr. 25 lentelę).

3.3. Rezultatų analizė, interpretavimas ir apibendrinimas

Pagal siūlomą metodiką įvertinus X įmonės naudojamą DAP rinkinį sudarytą iš užkardų, komutatorių, UPS, antivirusinių programų, ir parinkus alternatyvų, bei palyginus juos galima daryti išvadą, jog vertinant DAP pagal panašias savybes galime sutaupyti investicijas skirtas saugumui. Žinoma čia atliktas vertinimas preliminarus, geresnių rezultatų galima pasiekti įtraukiant didesnės apimties DAP į sudarytus rinkinius, tuomet ir patikimumo rodiklis išliktų toks pats, o gal ir didesnis. Pagal gautus rezultatus matome, kad pasirinkę alternatyvų DAP rinkinį, galime sutaupyti pinigine prasme ir nedaug ką prarasti saugos priemonių patikimumo atžvilgiu.

Vienas sunkiausių uždavinių yra kompiuterizuotai realizuoti visumą apibendrinančio DAP parinkimo ir įvertinimo aspektu. Tikslaus DAP įvertinimo nėra. Jį galima tik artinti prie užsibrėžto ir objektyviau įvertinti analizuojamas DAP. Eksperimentui iš esmės pagal siūlomą DAP kompiuterizuoto parinkimo ir įvertinimo metodiką analizavau, kaip parinkti ir įvertinti įmonės tinklo saugos priemones. Išskyriau įvairių lygių TSE ir nustačiau juos charakterizuojančius parametrus. Pabandžiau pažvelgti į TSE keliais lygiais. Išnagrinėtus ir suklasifikuotus DAP rinkinius įvedžiau į sukurtą ekspertinę sistemą, taip supaprastindama DAP pasirikimą pagal vartotojui palankius kriterijus.

IŠVADOS

1. Darbe apibendrinti DAP analizės ir įvertinimo rezultatai, kuriais remiantis išspręsti DAP kompiuterizuoto parinkimo ir įvertinimo metodikai sudaryti reikalingi aspektai: grėsmių kylančių duomenų saugumui, duomenų saugos technologijų ir priemonių klasifikacija; duomenų apsaugos ir rizikos valdymo aspektų apžvalga, reikalinga duomenų apsaugos įvertinimo kriterijų ir apsaugos būdų parinkimui.
2. Parodyta, kad egzistuoja sunkumai: kaip iš DAP įvairovės atrinkti tinkamas, kaip kokybines saugos funkcijų charakteristikas vertinti formalizuotai; trūksta universalios ir efektyvios kompiuterizuotos sistemos, kuria remiantis pakankamai objektyviai galima būtų įvertinti esamą kompiuterinę sistemą informacijos saugumo požiūriu, surūšiuoti DAP ir jų rinkinius pagal saugumo, patikimumo ir palankumo vartotojui lygius, kainą.
3. Pasiūlyta DAP kompiuterizuoto parinkimo ir įvertinimo metodika. Metodika grindžiama struktūrinio projektavimo principais. Jos pagrindas yra formalizuotas alternatyvių variantų katalogas.
4. Pateiktas metodikos etapas, kuriame nustatomos iš DAP rinkinio išorinių parametrų reikšmės, realizuotas ekspertinės sistemos pavidalu.
5. Pagal siūlomą DAP kompiuterizuoto parinkimo ir įvertinimo metodiką analizuota, kaip parinkti ir įvertinti įmonės tinklo saugos priemones. Buvo išskirti įvairių lygių TSE ir nustatyti juos charakterizuojantys parametrai.
6. Ateityje pasiūlytą metodiką galima būtų praktiškai taikyti sukūrus ir realizavus nagrinėjamos (atitinkamos) srities DAP rinkinio kompiuterizuotą katalogą.

LITERATŪRA

1. GARLA, E., DUBOVSKAJA, V. (2008) Kompiuterinių tinklų projektavimas Vilnius: UAB CIKLONAS, 240 p.
2. HARRIS, Shon. (2005) CISSP: All-in-one exam guide New York [N.Y.] [etc.]: McGraw-Hill/Osborne. 1001 p.
3. LUČINSKIJ, M., POŽERSKIS, P., TUMĖNAS, P. (2007) Duomenų saugos pradmenys Kaunas: "Smaltijos" leidykla.160 p.
4. SEKLIUCKIS V., ADOMAVIČIUS J., GARŠVA G. Informacinių technologijų įvaldymas struktūrinio projektavimo požiūriu // Informacijos mokslai, 2003, t. 24. p. 68-73. ISSN 1392-0561.
5. Сергеев, А. П. Офисные локальные сети. Самоучитель. – М.: Издательский дом „Вильяме“, 2003. 320 с. ISBN 5-8459-0504-4.
6. VASILECAS, Olegas. (2008) Informacinių sistemų sauga. Vilnius: Technika. 273 p.
7. ARUST, Ainas. (2009) Informacijos saugumas – Lietuvos įmonių „pamiršta zona“ gegužės 27d. *elektronika.lt*, [interaktyvus]. Prieiga per internetą: <http://www.elektronika.lt/articles/ computers/17315/>
8. CRITICAL SECURITY. (2008) DDos atakų anatomija [interaktyvus]. *elektronika.lt*, rugpjūčio 8d. [žiūrėta 2009 m. kovo 20 d.]. Prieiga per internetą: <http://www.elektronika.lt/articles/computers/12566/>
9. DANIELIUS, Tadas. (2005) Kompiuterinių sistemų klasifikacija [interaktyvus]. *elektronika.lt*, kovo 20d. [žiūrėta 2009 m. spalio 25 d.]. Prieiga per internetą: <http://www.elektronika.lt/theory/theme/160/792/>
10. Kompiuterių tinklų saugumo terminų aiškinamasis žodynas. (2009) Intrusion Prevention System [interaktyvus]. *tinklusaugumas.lt,* vasario 19d. [žiūrėta 2009 m. kovo 20 d.]. Prieiga per internetą: <http://www.tinklusaugumas.lt/cgi-bin/moin.py/Intrusion%20Prevention%20System>
11. MATELIS, Stasys. (2004) Intelektualios informacijos apsauga įmonėse [interaktyvus]. *esecurity.lt,* [žiūrėta 2009 balandžio 15d.]. Prieiga per internetą: <http://www.esecurity.lt/article.php?id=1322>
12. RAMAŠAUSKAS, Olegas. (2009) Kompiuterių tinklai [interaktyvus]. Elektroninė mokomoji knyga: Klaipėdos universitetas, [žiūrėta 2009 balandžio 14d.] Prieiga per internetą: <http://ik.ku.lt/lessons/konspekt/tinklai/index.htm>
13. WIKIPEDIA. (2009) Informacijos apsauga [interaktyvus]. *wikipedija.lt*, sausio 7d. [žiūrėta 2009 m. spalio 25 d.]. Prieiga per internetą: <http://www.e-bcg.com/uploads/IS_Wikipedija.pdf>

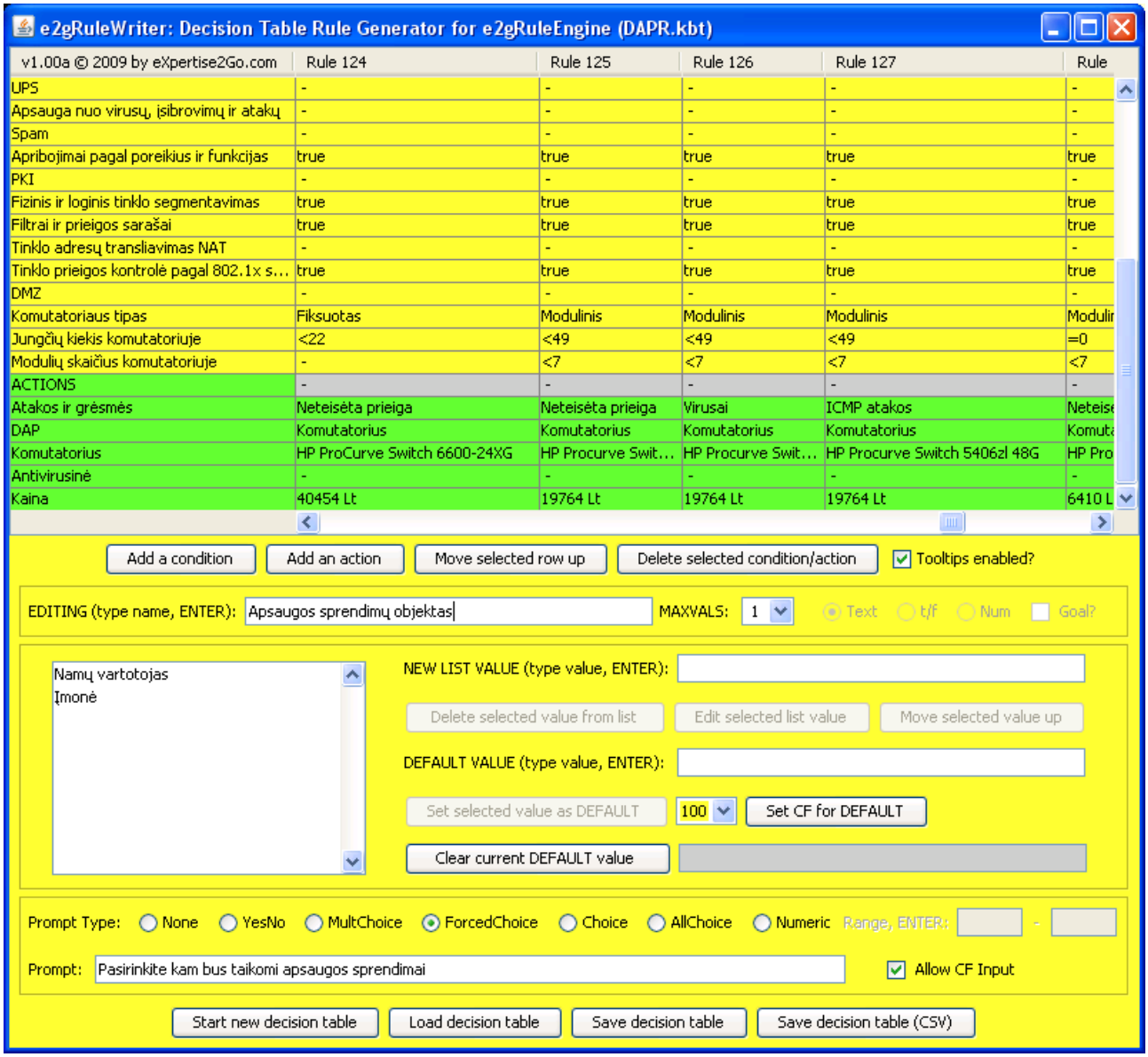
14. WIKIPEDIA. (2009) ISO 15504 [interaktyvus]. *wikipedia.org*, birželio 15d. [žiūrėta 2009 m. birželio 20 d.]. Prieiga per internetą: <http://en.wikipedia.org/wiki/ISO_15504>
15. WISWIKI. Computer security model [interaktyvus]. *viswiki.com*, [žiūrėta 2009 balandžio 15d.]. Prieiga per internetą: <http://www.viswiki.com/en/Computer_security_model>
16. TopTenREVIEWS. (2003-2009) Personal Firewall Software Review 2010 [interaktyvus]. *TopTenREVIEWS*.com, [žiūrėta 2009 gruodžio 30d.]. Prieiga per internetą: <http://personal-firewall-software-review.toptenreviews.com/>
17. TopTenREVIEWS. (2003-2009) AntiVirus Software Review 2010 [interaktyvus]. *TopTenREVIEWS*.com, [žiūrėta 2009 gruodžio 30d.]. Prieiga per internetą: <http://anti-virus-software-review.toptenreviews.com/index.html>
18. TopTenREVIEWS. (2003-2009) Small Bussiness AntiVirus Review 2010 [interaktyvus]. *TopTenREVIEWS*.com, [žiūrėta 2009 gruodžio 30d.]. Prieiga per internetą: <http://anti-virus-software-review.toptenreviews.com/small-business-antivirus>
19. WIKIPEDIA. (2009) Laisvoji enciklopedija [interaktyvus]. Ekspertinė sistema [žiūrėta 2009 spalio 9d.]. Prieiga per internetą: <http://lt.wikipedia.org/wiki/Ekspertin%C4%97_sistema>
20. WIKIPEDIA. (2010) Laisvoji enciklopedija [interaktyvus]. Duomenų bazė [žiūrėta 2010 sausio 9d.]. Prieiga per internetą: <http://lt.wikipedia.org/wiki/Duomen%C5%B3_baz%C4%97>
21. ŠTITILIS, Darius.; LAURINAITIS, Marius. (2009) Tapatybė ir identifikavimas: grėsmės elektroninėje erdvėje [interaktyvus], *balsas.lt*, spalio 30 d. [žiūrėta 2010 m. balandžio 2 d.]. Prieiga per internetą: <http://www.balsas.lt/naujiena/325671/ tapatybe-ir-identifikavimas-gresmes-elektronineje-erdveje/>
22. TAYLOR, Laura. (2002) How to Chooise the Right Enterprise Firewall [interaktyvus]. *Datamation.com*, [žiūrėta 2010 kovo 13d.]. Prieiga per internetą: <http://itmanagement.earthweb.com/secu/article.php/974501>
23. JAMES, Jeff. (2008) Enterprises Firewall Apliances [interaktyvus]. *WindowsITPro*, [žiūrėta 2010 kovo 13d.]. Prieiga per internetą: <http://www.windowsitpro.com/article/firewalls3/enterprise-firewall-appliances.aspx>
24. APNET UAB. (2005-2009) Kompiuterinio tinklo saugumas [interaktyvus]. [žiūrėta 2010 kovo 14d.]. Prieiga per internetą: <http://www.apnet.lt/Paslaugos/ Kompiuterinio-tinklo-saugumas>

25. VAIČYS, Audrius. (2003) Informacijos apsauga ir verslo interesai. [interaktyvus]. *Verslobanga.lt*, sausio 8 d. [žiūrėta 2010 kovo 20d.]. Prieiga per internetą: <http://www.verslobanga.lt/lt/patark.full/3e19ff3ac9123.1>
26. Informacijos apsaugos sritys. (2010). [interaktyvus]. [žiūrėta 2010 kovo 21d.]. Prieiga per internetą: <http://web.esaugumas.lt/VRM/kursas/37169.html>
27. STOUFFER, K., FALCO, J., SCARFONE, K. (2008). Guide to Industrial Control Systems (ICS) Security [interaktyvus]. [žiūrėta 2010 kovo 21d.]. Prieiga per internetą: <http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf>
28. Valstybinė duomenų apsaugos inspekcija (2008). Saugus duomenų perdavimas elektroniniu paštu [interaktyvus]. *Ada.lt,* Spalio 28 d. [žiūrėta 2010 kovo 21d.]. Prieiga per internetą: <http://www.ada.lt/index.php?action=page&lng=lt&id=594>
29. MATRIX UAB (2008). Kaip testuojamos antivirusų programos (antivirusai)? [interaktyvus]. [žiūrėta 2010 kovo 21d.]. Prieiga per internetą: <http://www.matrix.lt/products/antivirus-review-ltu-kaip-testuojami-antivirusai.htm>
30. HAWES, John (2009). VB100 on Windows 2003 Server x64 [interaktyvus]. *virusbtn.com,* Balandžio 1 d. [žiūrėta 2010 kovo 21d.]. Prieiga per internetą: <http://www.virusbtn.com/virusbulletin/archive/2009/06/vb200906-comparative>
31. BENDORAITYTĖ, Dijana (2007). Interneto grėsmės 2007-aisiais [interaktyvus]. *Alfa.lt*, kovo 28 d. [žiūrėta 2010 m. balandžio 2 d.]. Prieiga per internetą: <http://www.alfa.lt/straipsnis/132094>
32. SCARFONE, K., HOFFMAN, P. (2009). Guidelines on Firewalls and Firewall Policy [interaktyvus]. [žiūrėta 2010 balandžio 2d.]. Prieiga per internetą: <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf>
33. SHINDER, Deb (2004). Choosing a Firewall [interaktyvus]. *windowsnetworking.com*, liepos 19 d. [žiūrėta 2010 m. balandžio 2 d.]. Prieiga per internetą: <http://www.windowsnetworking.com/articles_tutorials/Choosing_a_Firewall.html>
34. SCARFONE, K., JANSEN, W., TRACY, M. (2008). Guide to General Server Security [interaktyvus]. [žiūrėta 2010 balandžio 2d.]. Prieiga per internetą: <http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf>
35. LabMice (2003). Laptop Security Gudelines [interaktyvus]. *LabMice.net*, gruodžio 10 d. [žiūrėta 2010 m. balandžio 2 d.]. Prieiga per internetą: <http://labmice.techtarget.com/articles/laptopsecurity.htm>

36. JANSEN, W., SCARFONE, K. (2008). Guidelines on Cell Phone and PDA Security [interaktyvus]. [žiūrėta 2010 balandžio 2d.]. Prieiga per internetą: <http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>
37. DORLING, Alec. (2008). ISO SPICE [interaktyvus]. [žiūrėta 2010 m. balandžio 2 d.]. Prieiga per internetą <http://www.isospice.com/authors/1/Alec-Dorling>
38. Vidaus reikalų ministerija (2005). Informacijos sauga valstybės institucijų ir įstaigų darbuotojams [interaktyvus]. [žiūrėta 2010 balandžio 2d.]. Prieiga per internetą: <http://web.esaugumas.lt/VRM/pdf/2_skyrius.pdf>
39. VAGERIS, Robertas (2005). Rizikos analizės vadovas [interaktyvus]. [žiūrėta 2009 m. birželio 20 d.]. Prieiga per internetą: <http://www.vrm.lt/fileadmin/Padaliniu_failai/Informacines_politikos_dep/IT_sauga/Rizikos_analize.pdf>
40. EXSYS Inc. (2000-2010). EXSYS Knowledge Automation Expert System [interaktyvus]. [žiūrėta 2010 balandžio 2d.]. Prieiga per internetą: <http://www.exsys.com/>

1 PRIEDAS

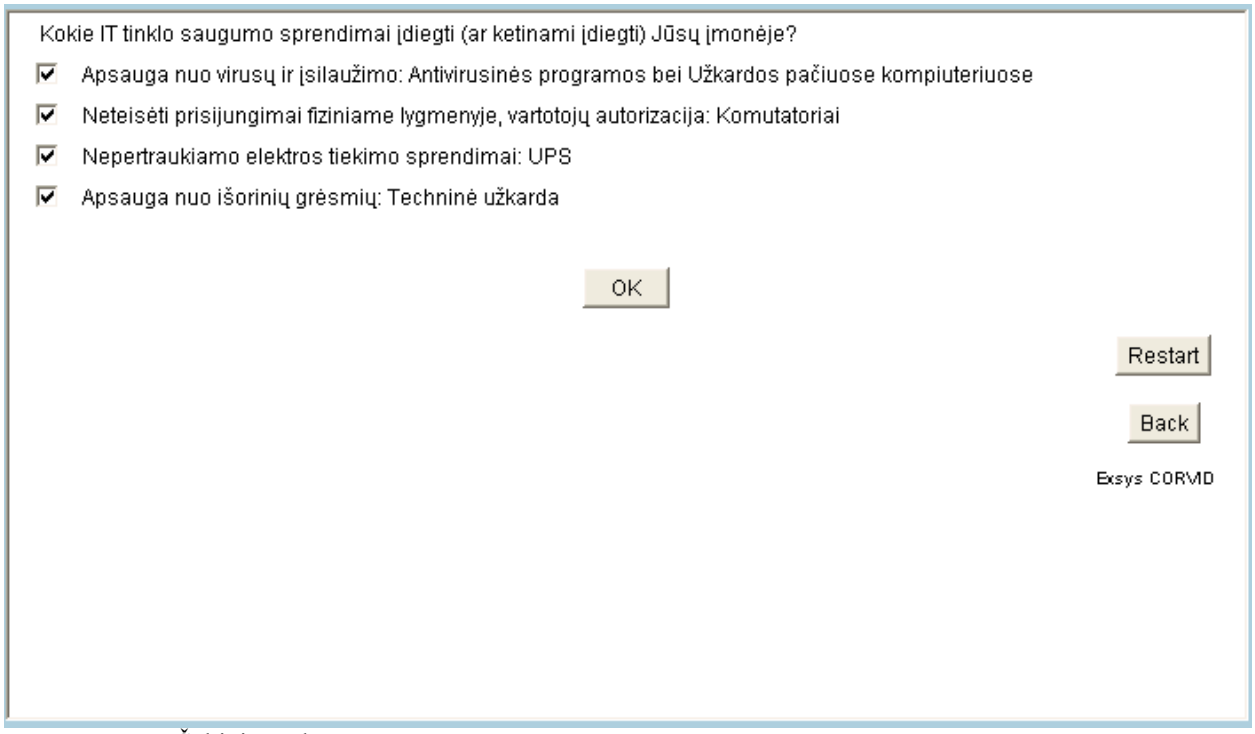
e2gRuleWriter SPRENDIMO LENTELĖ



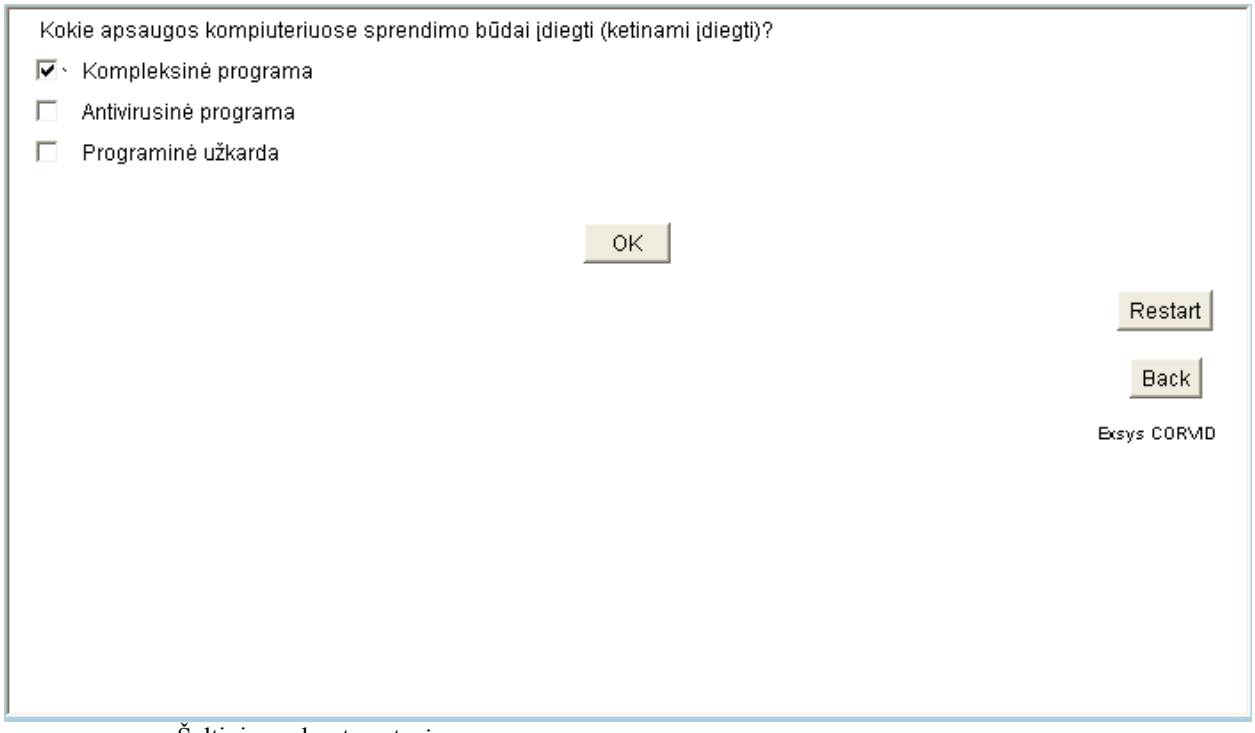
Šaltinis: sudaryta autorės

2 PRIEDAS

EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID LANGŲ PAVYZDŽIAI

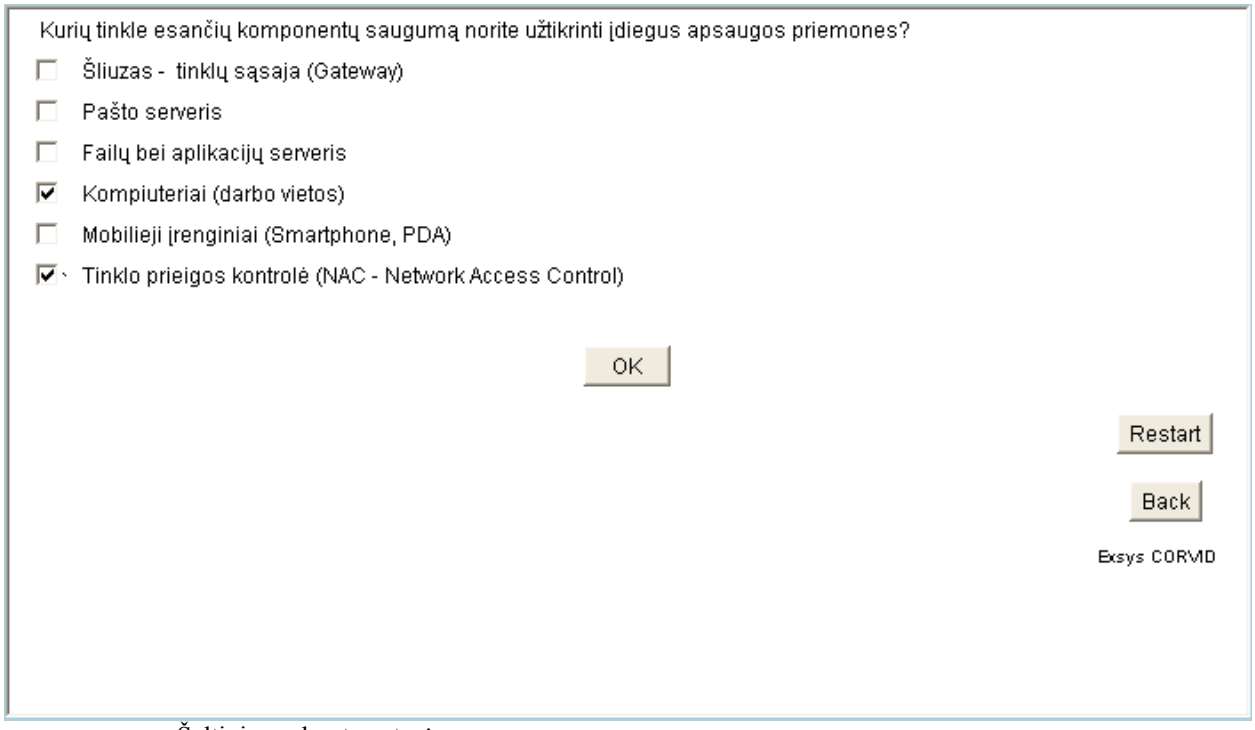


Šaltinis: sudaryta autorės

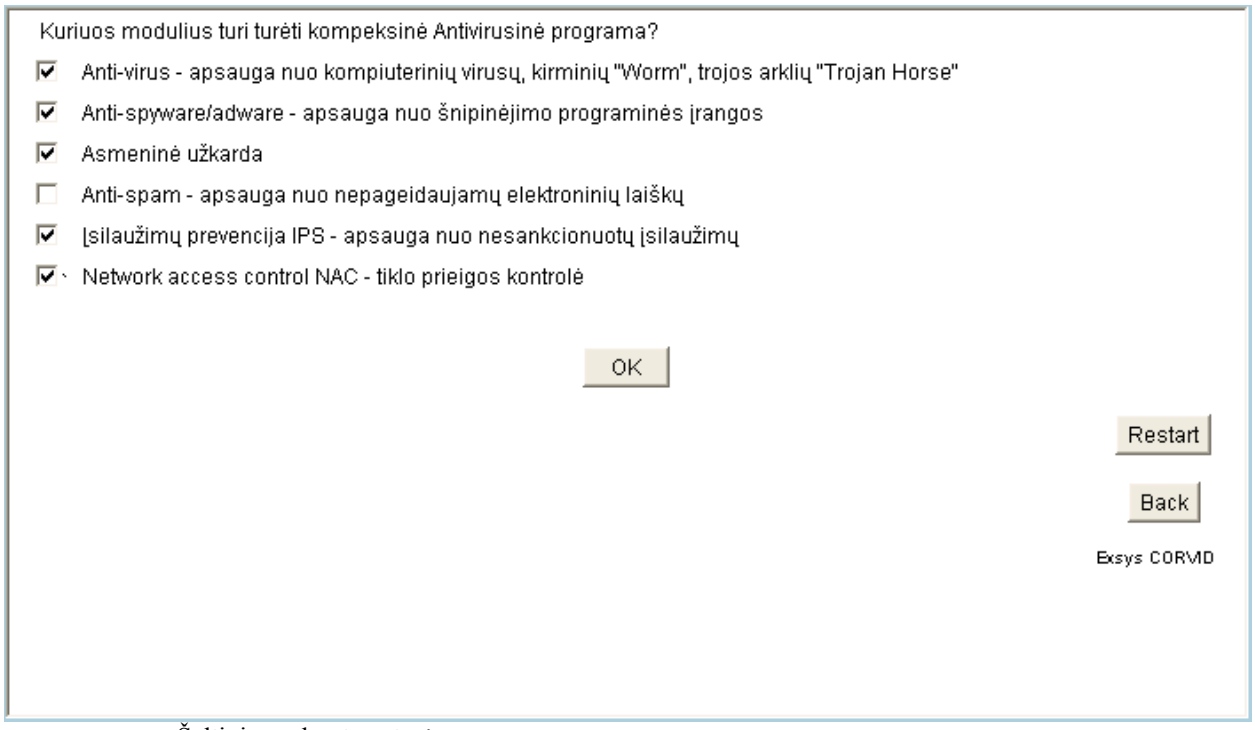


Šaltinis: sudaryta autorės

EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID LANGAI



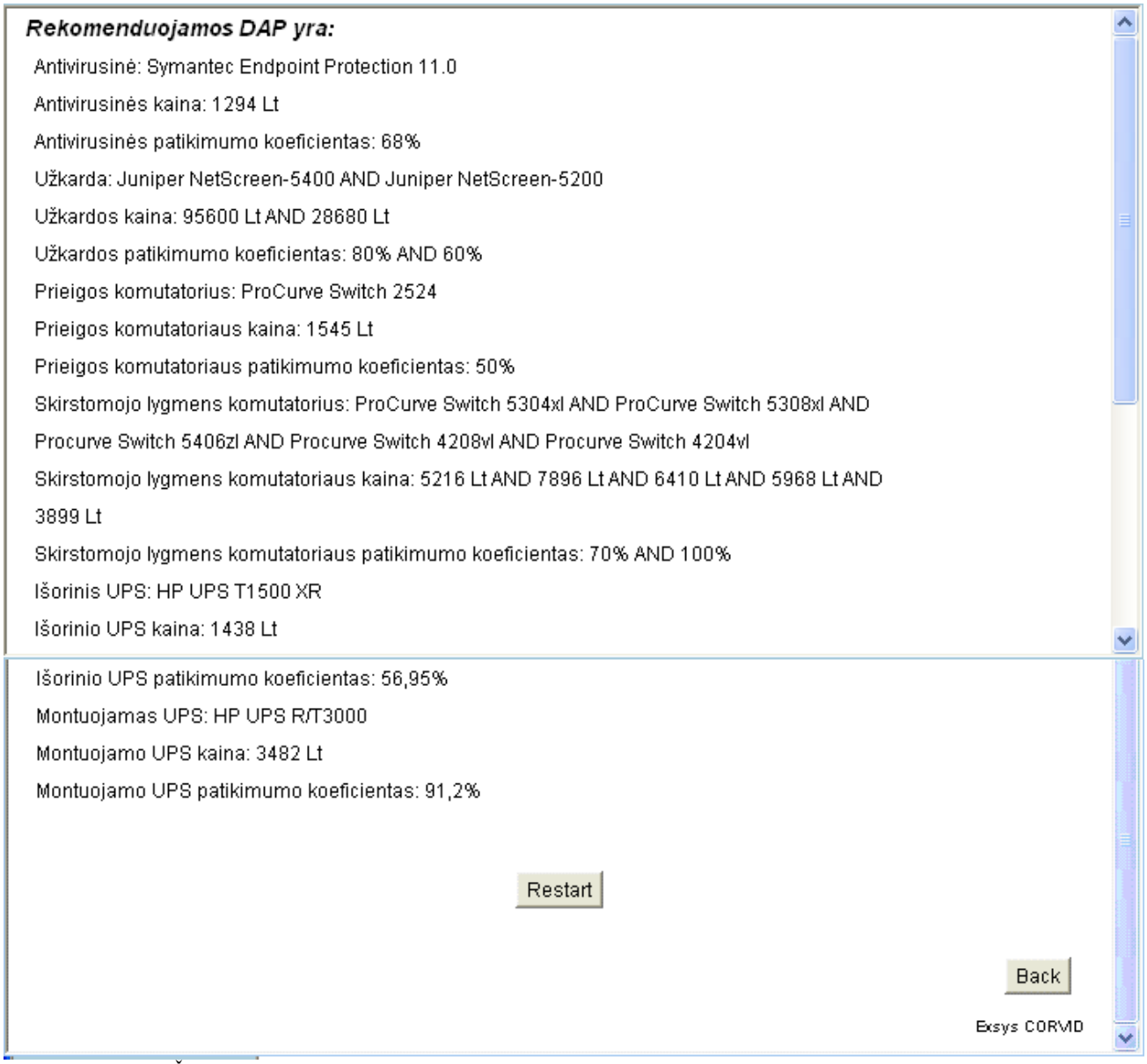
Šaltinis: sudaryta autorės



Šaltinis: sudaryta autorės

3 PRIEDAS

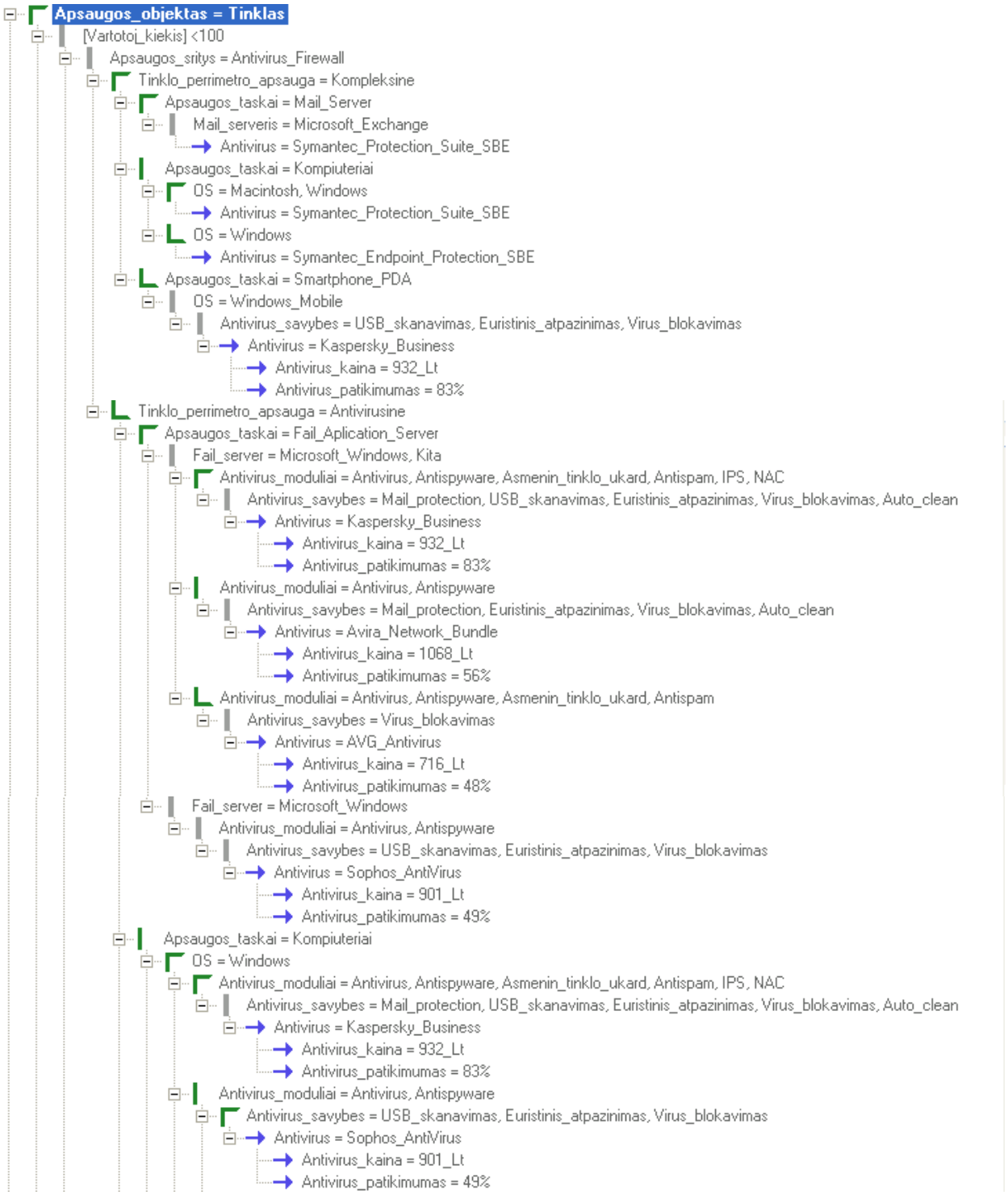
EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID REZULTATŲ LANGAS



Šaltinis: sudaryta autorės

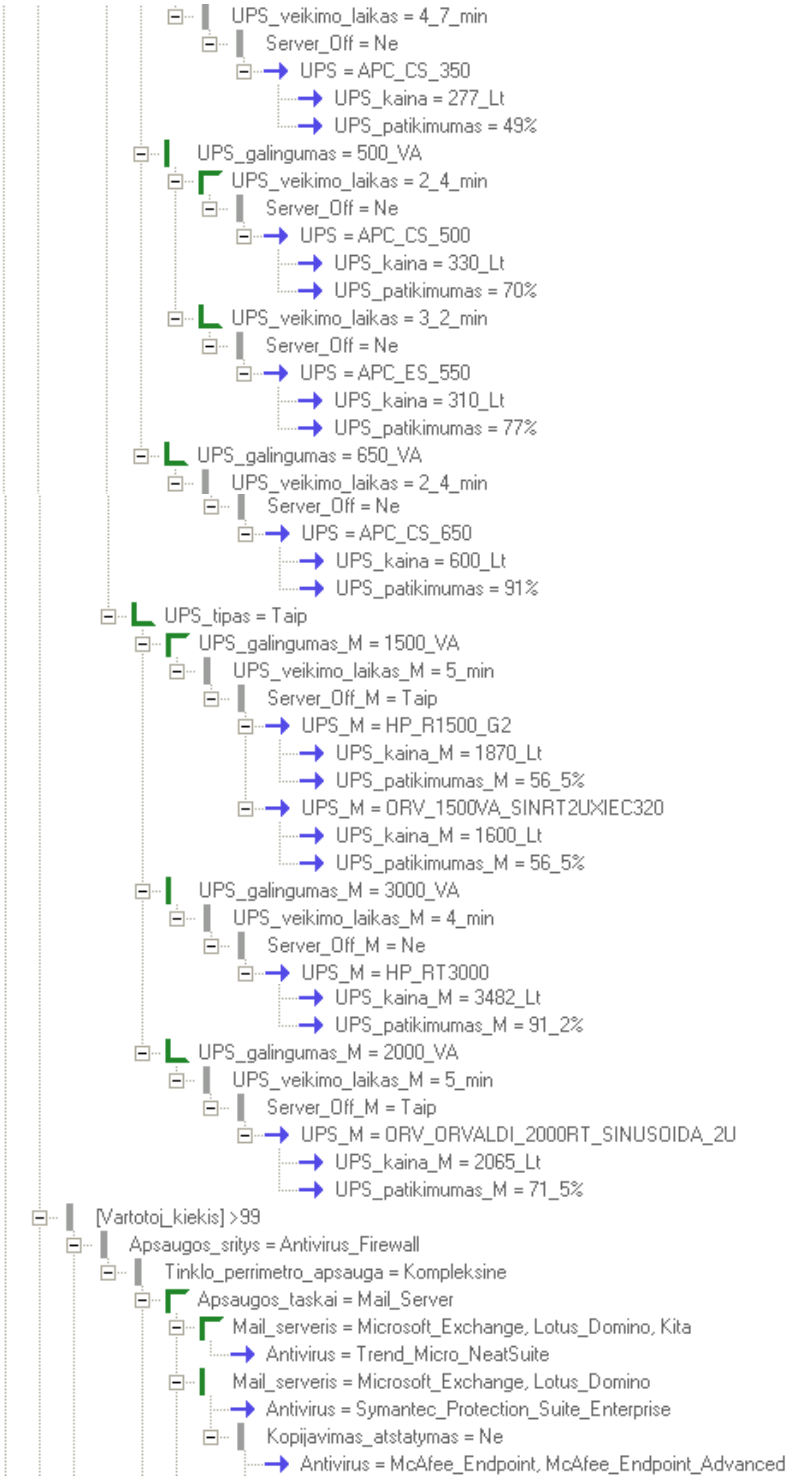
4 PRIEDAS

EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID TAISYKLIŲ MEDIS

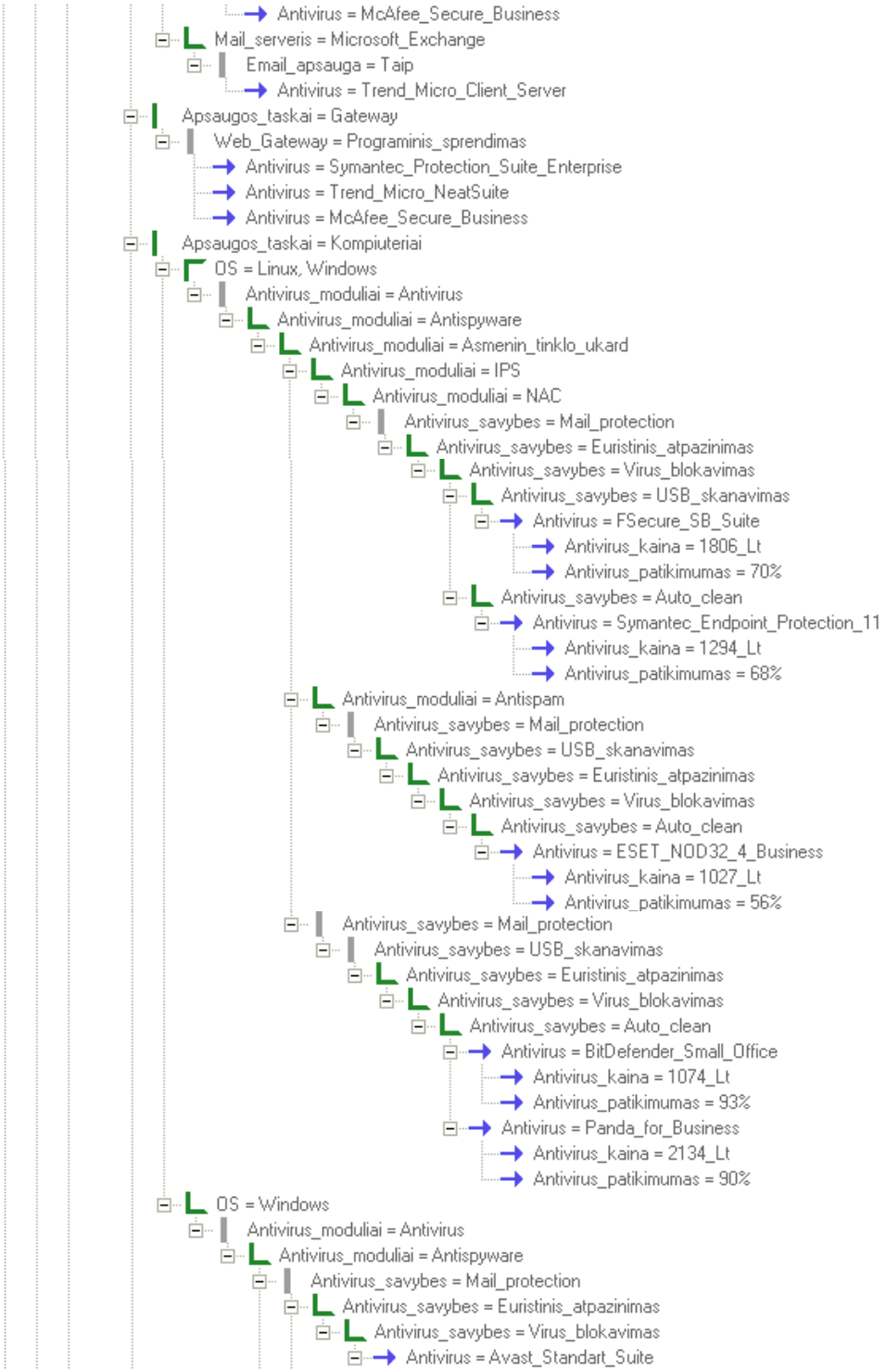


EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID TAISYKLIŲ MEDIS

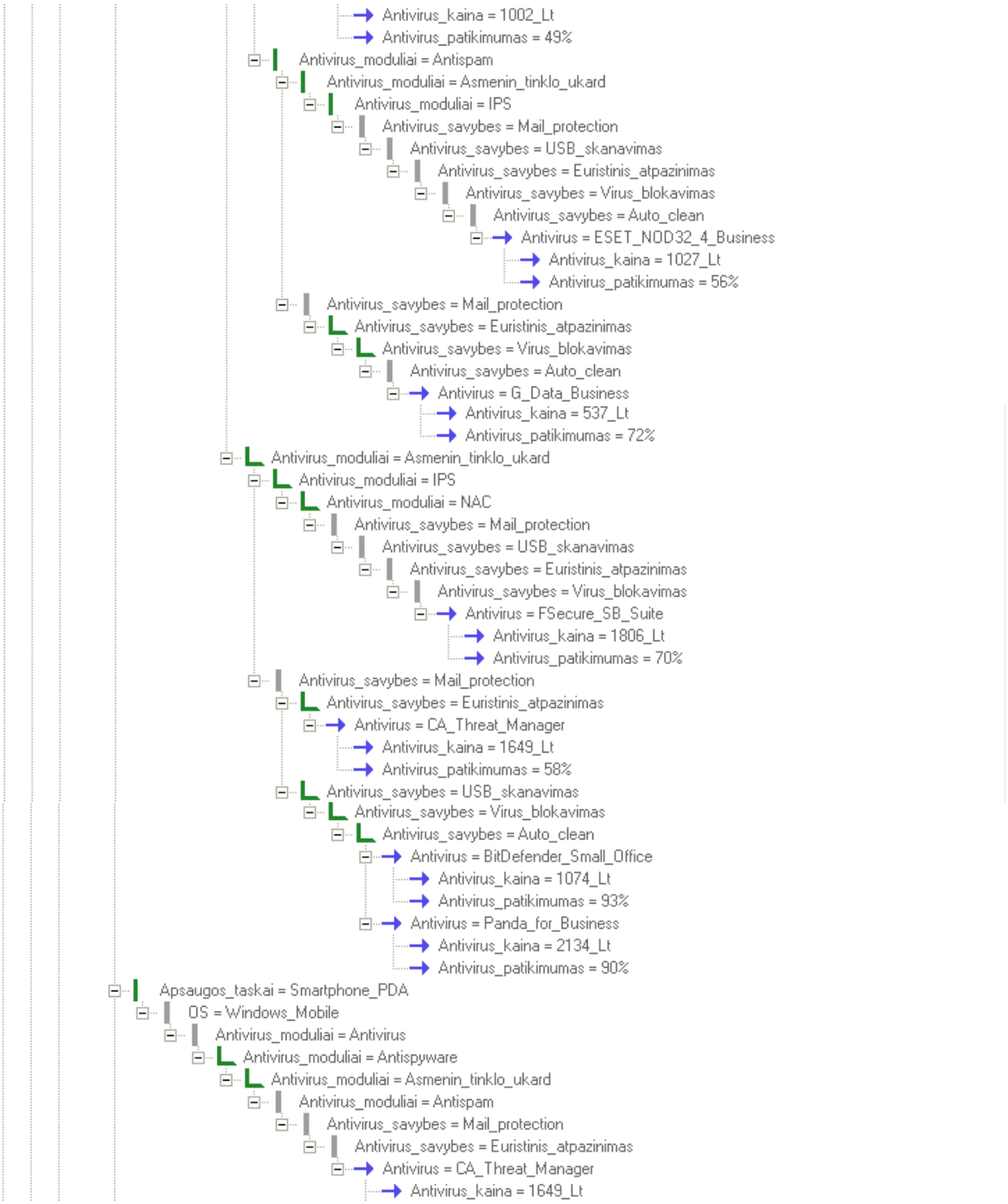
EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID TAISYKLIŲ MEDIS



EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID TAISYKLIŲ MEDIS

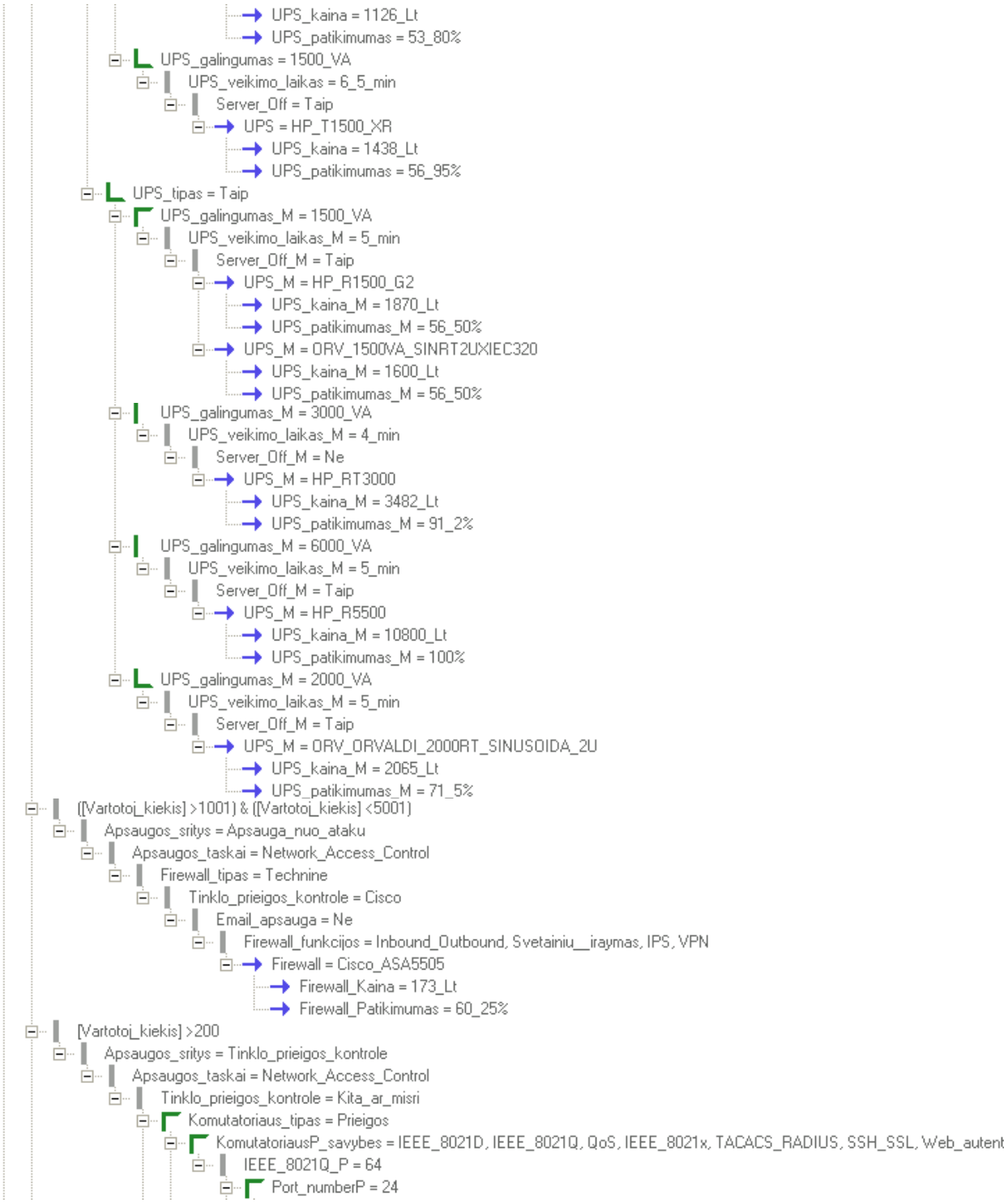


EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID TAISYKLIŲ MEDIS

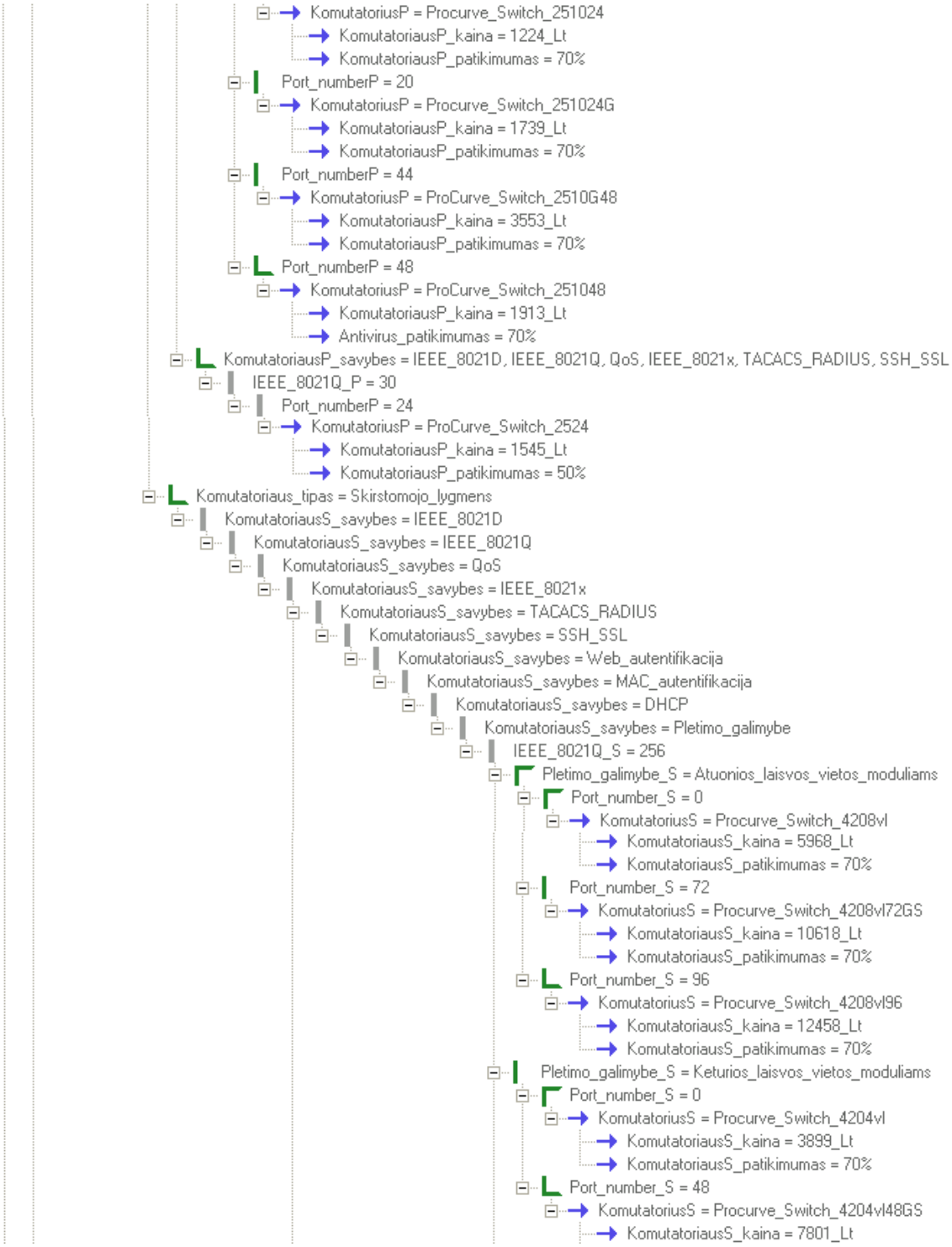


EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID TAISYKLIŲ MEDIS

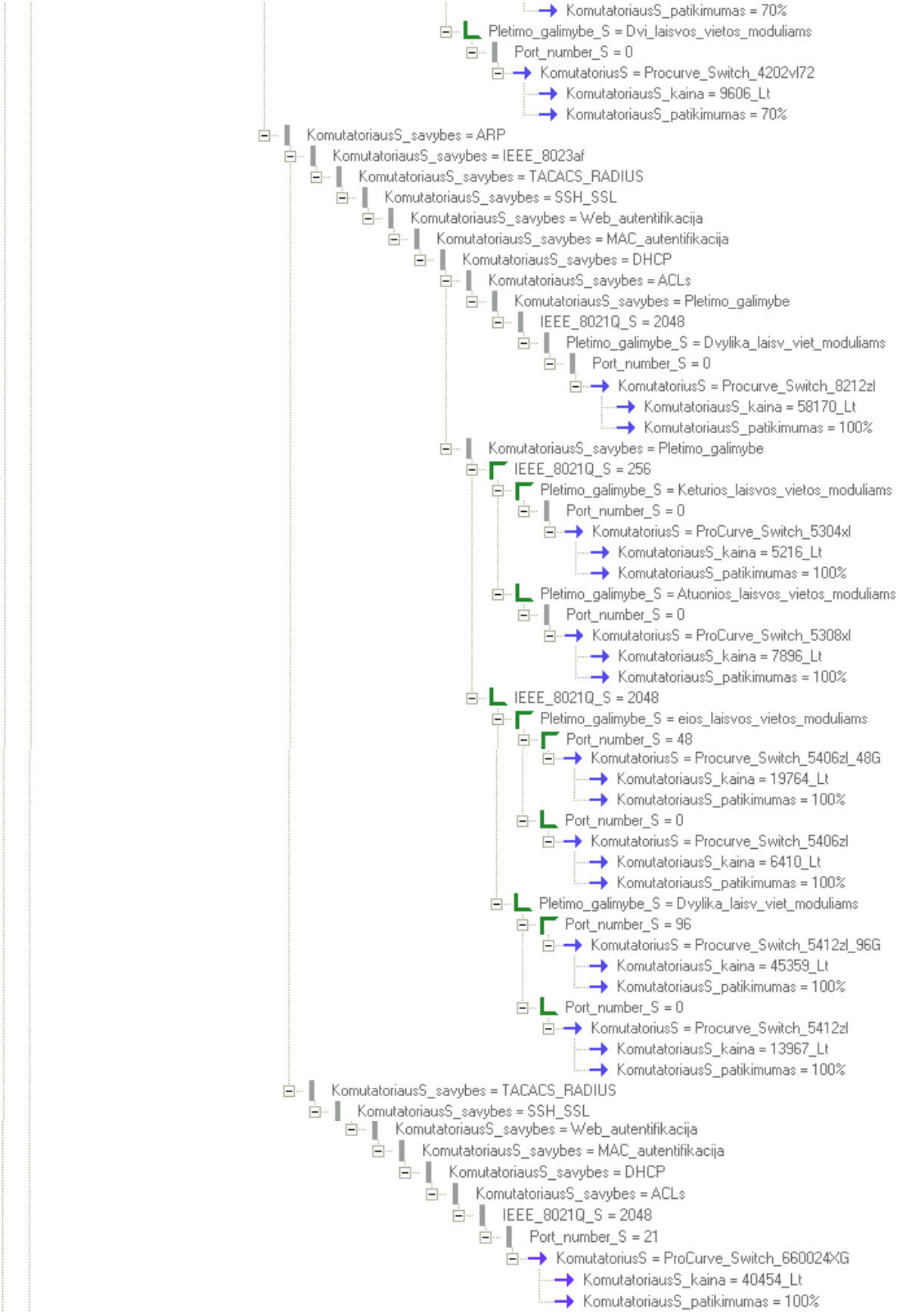
EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID TAISYKLIŲ MEDIS



EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID TAISYKLIŲ MEDIS

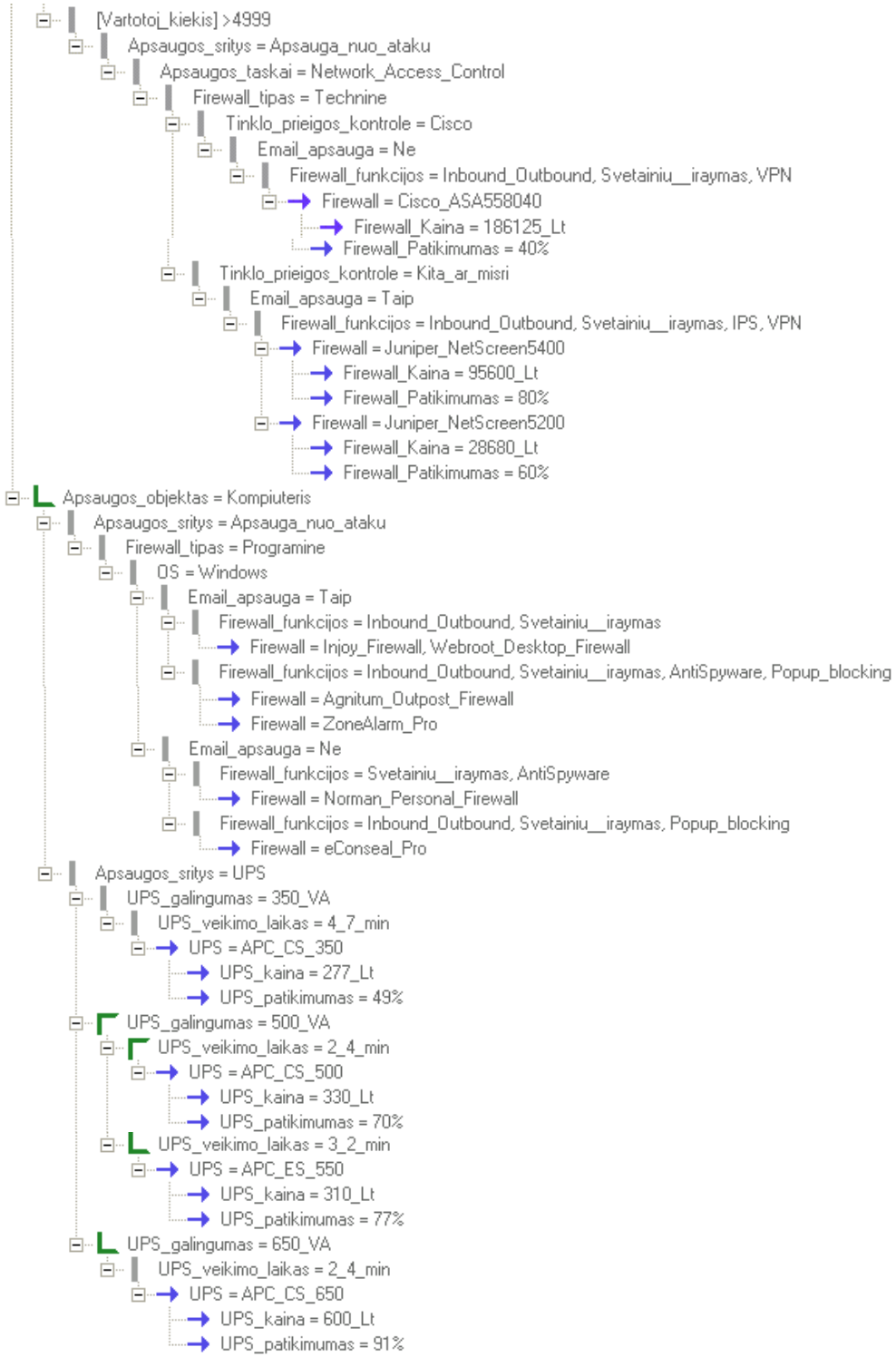


EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID TAISYKLIŲ MEDIS



14 PRIEDAS (TĘSINYS)

EKSPERTINĖS SISTEMOS REALIZUOTOS SU Exsys CORVID TAISYKLIŲ MEDIS



Šaltinis: sudaryta autorės