ISSN 1392-0561. INFORMACIJOS MOKSLAI. 2007 42–43

Korporacinių įmonių informacinės saugos architektūrų modeliavimas

Mindaugas Mikučionis

Kauno technologijos universitetas
Kaunas University of Technology
Tel. (+370 37) 300 389
El. paštas: mindaugas.mikucionis@ktu.lt

Algimantas Venčkauskas

Kauno technologijos universiteto docentas
Kaunas University of Technology,
Assoc. Professor
Tel. (+370 37) 300 389
El. paštas: algimantas.venckauskas@ktu.lt

Eugenijus Toldinas

Kauno technologijos universiteto docentas
Kaunas University of Technology, Assoc. Professor
Tel. (+370 37) 300 389
El. paštas: eugenijus.toldinas@ktu.lt

Korporacinių įmonių kompiuterinių sistemų informacinės saugos užtikrinimas yra viena iš svarbiausių informacinių technologijų problemų. Augant ir plečiantis verslui iškyla nutolusių įmonės padalinių, partnerių, darbuotojų saugaus pasikeitimo duomenimis ir lokalių tinklų saugumo problema. Verslo ir valdymo procesuose informacinės technologijos tampa vis reikšmingesnės, didėja informacinių procesų sudėtingumas. Dėl šių priežasčių kompiuterinių sistemų informacinės saugos pažeidimų kaina nuolatos auga. Atsižvelgiant į informacinės saugos priemonių patikimumo ir našumo kriterijus, būtina šių sistemų veikimą ištirti prieš diegiant. Adekvačių sprendimų, užtikrinančių informacinę saugą už atitinkamą kainą, priėmimas tampa vis sudėtingesniu uždaviniu. Korporacinės įmonės informacinės saugos modeliai leidžia išspręsti šias problemas ir gali būti taikomi informacinės saugos sistemoms projektuoti, parametrams parinkti ir diegti. Šiame darbe sudaromi ir nagrinėjami korporacinių įmonių informacinės saugos sistemų modeliai, aprašantys įvairias saugaus duomenų pasikeitimo ir informacinės saugos grėsmių neutralizavimo priemonių architektūras. Informacinės saugos realizavimo priemonės įvertintos atitinkamais parametrais. Modeliai leidžia palyginti įvairias informacinės saugos realizavimo architektūras ir parinkti efektyviausią.

Korporacinę įmonę sudaro geografiškai nutolę padaliniai. Dažniausia padalinių lokalūs kompiuterių tinklai į bendrą korporacijos kompiuterių tinklą sujungiami internetinio ryšio priemonėmis. Kadangi internetas yra potencialiai pavojingas informacinės saugos požiūriu, iškyla šie pagrindiniai korporacinės įmonės lokalių kompiuterių tinklų sujungimo uždaviniai:

- saugus duomenų pasikeitimas tarp nutolusių padalinių lokalių tinklų kompiuterių;
- lokalių tinklų apsauga nuo galimų atakų ir įsilaužimų;
- antivirusinė apsauga.

Šie uždaviniai sprendžiami naudojant įvairias tinklines technologijas ir siekiant skirtingų tikslų. Mažoms įmonėms svarbu užtikrinti nebrangų ryšį, o didelėms įmonėms – sudėtingą,

įvairialypį, saugų tinklų sujungimą, užšifruojant informaciją ir kontroliuojant prieigą prie jos.

Saugus duomenų pasikeitimas tarp kompiuterių, esančių skirtinguose lokaliuose tinkluose, dažniausiai realizuojamas naudojant virtualius privačiuosius tinklus (VPN) (Mitchell, 2005). VPN yra tinklas, jungiantis korporacinės įmonės struktūrinius elementus per viešąjį interneto tinklą. Čia nenaudojamos saugios skirtinės linijos, todėl perduodami duomenys turi būti koduojami. Viešame interneto tinkle sukuriami koduoti duomenų perdavimo tuneliai tarp geografiškai išdėstytų taškų. VPN pranašumai yra saugus nutolusių kompiuterių sujungimas, maža kaina, nesudėtinga tinklo topologija. VPN trūkumai yra greitaveikos sumažėjimas dėl informacijos kodavimo, neužtikrinamas pastovus duomenų srauto perdavimo greitis. VPN gali būti realizuoti naudojant specialią aparatinę programinę įrangą (Juniper Networks Firewall, 2005), operacinių sistemų VPN priemones (Microsoft Internet Security and Acceleration (ISA) Server, 2005), interneto paslaugų teikėjų priemones (GPRS intranetas, Cisco VPN, 2005).

Lokalių tinklų apsaugai nuo galimų atakų ir įsilaužimų naudojamos ugniasienės ir tinklų atakų aptikimo priemonės (IDS). Ugniasienės yra pagrindiniai saugios korporacinės įmonės saugumo architektūros elementai (Slemp, 2001). Ugniasienės kontroliuoja duomenų srautą į tinklą ir iš jo. Tam, kad filtruotumėme paketus, reikia sudaryti aibę taisyklių, kurios nurodo protokolų tipus, kurie yra praleidžiami ir kurie nepraleidžiami atsižvelgiant į gavėjo ir siuntėjo adresus. Ugniasienės yra dviejų tipų: 1) filtravimo be atminties – kiekvieno paketo informacija lyginama su statiškai nustatytu taisyklių rinkiniu. Žiūrima tik į paketo antraščių informaciją (siuntėjo ir gavėjo IP, portus); 2) filtravimo su atmintimi, kai įvairiomis lentelėmis analizuojama paketų seka ir atitinkamos taisyklės taikomos atsižvelgiant į esamą susijungimo būseną. Ugniasienės kompiuterių tinklą skaido į skirtingo lygio saugumo zonas, tai labai padidina tinklo saugumą ir palengvina taikyti saugumo taisykles. Įsilaužimų aptikimo sistema (IDS) stebi duomenų srautą ir, aptikusi įsilaužimo požymį, generuoja pranešimus (Dobrucki, 2002). Ugniasienės saugo tinklą nuo įsilaužimų, o IDS parodo, ar tinklas atakuojamas. IDS yra dviejų tipų: tinklo ir lokalus. Abu turi savo pranašumų ir trūkumų. Lokalus IDS, esantis serveryje arba vartotojo darbo vietoje, renka lokalios sistemos generuojamą informaciją. Šio tipo IDS sudėtinga administruoti didelės įmonės tinkluose. Tinklinės IDS analizuoja duomenis, perduodamus kompiuterių tinklu. Kiekvienas paketas yra palyginamas su duomenų bazėje esančia informacija. Tinklines IDS yra lengviau paskirstyti ir administruoti. Tačiau yra ribotas maksimalus duomenų srautas, kurį gali apdoroti IDS.

Vieną didžiausių grėsmių informacijos saugumui kelia kompiuterių virusai. Virusams aptikti ir neutralizuoti naudojamos antivirusinės priemonės. Architektūra turi būti kelių saugos lygių. Vartotojų darbo vietose turi būti antivirusinės programos (AV). Tačiau vartotojo darbo vietos dažnai yra nepatikimos (antivirusas gali būti išjungiamas), todėl aukščiausiu lygiu duomenų srautas turi būti tikrinamas prieš patenkant į įmonės lokalų tinklą. Antivirusiniam duomenų srauto, ateinančio arba išeinančio iš lokalaus tinklo, skenavimui naudojamos programinės ir aparatinės priemonės. Pavyzdžiui, galima paminėti „Panda GateDefender“ įrenginį (Panda GateDefender, 2005). Jis blokuoja virusus, nepageidaujamą elektroninį paštą ir nepageidaujamą turinį prieš jiems patenkant į lokalų tinklą. „Panda GateDefender“ turi automatišką atsinaujinimo sistemą, kuri suteikia moderniausią apsaugą visam tinklui. „Panda GateDefender“ puikiausiai tinka mažoms, vidutinėms ir didelėms įmonėms. Tokie aparatiniai įrenginiai įterpiami tarp įmonės maršrutizatoriaus ir vidinio tinklo. Pagrindiniai parametrai yra maksimalus srauto tikrinimo greitis (5–30 Mbps). Kai srautas didelis, susidaro duomenų kamščiai ir tinklo funkcionavimas gali sutrikti. Esant kelioms tinklo saugumo zonoms tampa sudėtinga parinkti įrenginio darbo vietą, kad būtų patikrintas visas reikalingas srautas ir nebūtų tikrinamas nereikalingas.

Įmonės saugumo infrastruktūros kūrimas yra sudėtingas procesas, todėl itin svarbu iš pradžių kuo tiksliau suprojektuoti visą sistemą, nes vėliau bus sugaišta daug laiko (ir išleista pinigų) sistemai modifikuoti. Todėl projektavimo etapu (tiek tinklo išdėstymo, tiek saugumo zonų pasiskirstymo, tiek papildomų saugumo priemonių) reikia sumodeliuoti kiek galima daugiau ir įvairesnių situacijų. Informacinė sauga – tai sudėtinga saugos priemonių sanpyna. Tos priemonės priklauso viena nuo kitos ir projektuojant reikia matyti bendrą vaizdą. Nuo darbo vietų skaičiaus, įmonės geografinio išsidėstymo ir tinklo darbo intensyvumo priklausys informacinės saugos užtikrinimo priemonių parametrai ir duomenų srautai. Šios priemonės savo ruožtu veikia duomenų srauto greitį. Šis apkrovimas taip pat priklausys nuo naudojamos tinklo architektūros ir saugos priemonių architektūros.

Modeliuodami įvertinsime šias charakteristikas: duomenų judėjimo tinkle greitį; tinklo architektūrą; įmonės struktūrą, t. y. geografinį išsidėstymą; VPN kodavimo, antivirusinių ir įsilaužimų aptikimo priemonių įtaką; protokolų pasiskirstymą duomenų sraute; įmonės paslaugas.

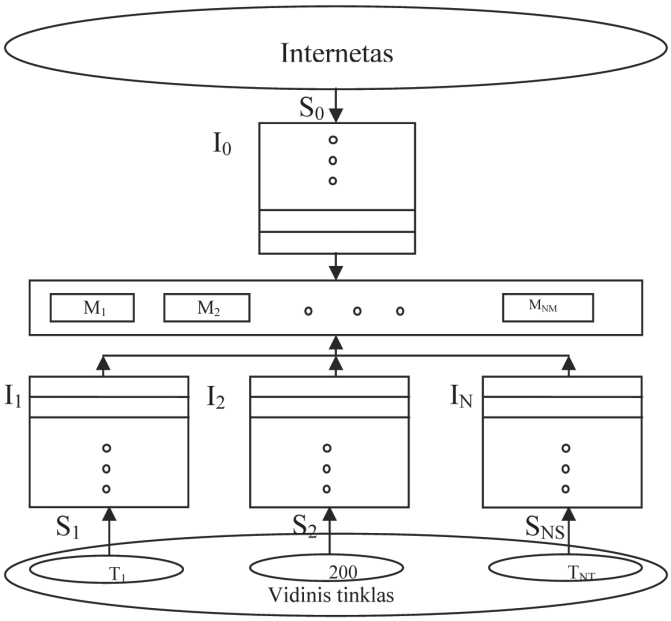
Panagrinėsime keletą informacinės saugos modeliavimo metodų ir apibrėšime jų pranašumus ir trūkumus: atakų grafo metodą, apibendrinto kriterijaus metodą ir imitacinį GPSS modelį.

Atakų grafo metodas – kiekvienai sistemai galima aprašyti atakų grafų rinkinius (Jha ir kt., 2003; Sheyner, 2004). Grafo mazgas reiškia sistemos pažeidimą. Grafas parodo, kaip įsilaužėlis gali pakenkti įmonės kompiuterinėms sistemoms. Atakų grafas reprezentuoja visus galimus kelius, kuriais įmanoma pažeisti modeliuojamos sistemos saugumą. Didelių sistemų atakų medžių projektavimas yra ilgas ir sudėtingas procesas. Saugumo specialistai naudoja šiuos duomenis sistemos silpnybėms aptikti. Atakų grafo projektavimui reikia surinkti visus tinklo sistemos lokalius ir globalius pažeidžiamumus. Pažeidžiamumų duomenų bazės surinkimui naudojamos tinklo elementų, serverių saugumo tikrinimo priemonės. Sujungus ryšiais lokalius ir globalius pažeidimus gauname atakų grafą. Kiekvienas grafo lankas yra atitinkamą pažeidžiamumą išnaudojantis procesas, kuris perveda sistemą į nestabilią būseną. Atakų medžiai parodo: sėkmingas atakas, kurių neaptinka saugos priemonės; kur efektyviausiai išdėstyti saugos priemones; kaip parinkti efektyvias programines ir aparatines saugos priemonių realizacijas; kaip numatyti ateityje galimus incidentus; kaip įvertinti skirtingų tinko topologijų efektyvumą. Tačiau atakų grafų sudarymas yra labai sudėtingas darbas. Dabar kuriamas atakų medžių automatinio generavimo metodas. Šiuo metodu negalime įvertinti kiekybinių saugos priemonių parametrų (saugos priemonių greitaveikos ir t. t.). Apibrėžiami tik pažeidžiamumai ir negalima modeliuoti saugos priemonių darbo greitaveikos.

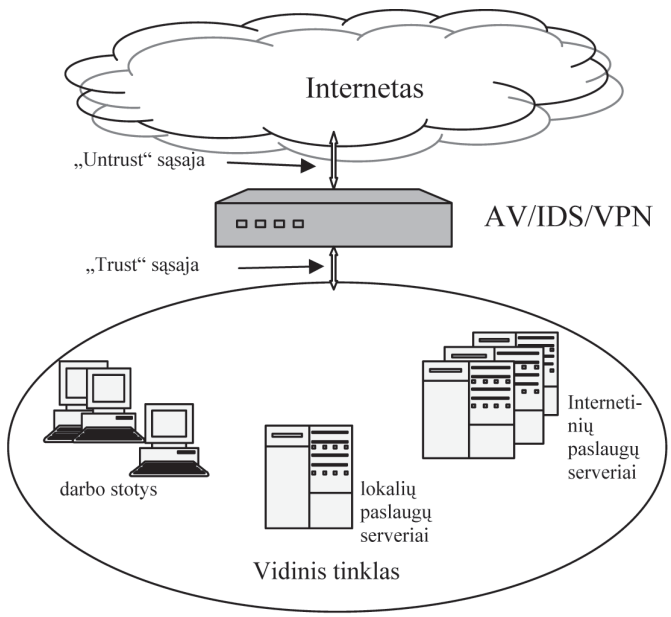
Įmonės informacinės saugos efektyvumą galima vertinti apibendrintu kriterijumi (Venčkauskas ir kt., 2003). Santykinė šio kriterijaus reikšmė leidžia palyginti keletą informacinės saugos realizavimo variantų ir pasirinkti geriausią. Šiuo metodu taip pat galima įvertinti įmonės informacinės saugos lygį pagal suformuluotus kriterijus ir vertinimo skalę, naudojant etaloninę informacinės saugos sistemą. Įmonės informacinės saugos efektyvumo vertinimo apibendrintu kriterijumi metodas yra informatyvus, nes sistemos sauga apibrėžiama vienu santykiniu dydžiu ir tai palengvina įvairių variantų analizę.

Sudėtingoms techninėms sistemoms modeliuoti projektavimo etapu plačiai naudojami imitaciniai metodai. Įmonės informacinės saugos sistemų architektūroms modeliuoti panaudosime GPSS sistemą (GPSS World Reference Manual, 2001). Modeliuojant GPSS metodu, saugos sistema išskaidoma į blokus (procesus), kurie sujungiami ryšio kanalais. Blokai – tai saugos sistemos realizavimo komponentai: VPN kodavimo, antivirusinių ir įsilaužimų aptikimo priemonės ir moduliai, tinklo sąsajos, o ryšio kanalai – tai duomenų srautai tarp tinklo komponentų ir segmentų. Bendra informacinės saugos sistemos imitacinio modelio schema pateikiama 1paveiksle.

Modeliuodami vertinsime šiuos parametrus: paketų pasirodymo dažnius sąsajose IS_i, saugumo priemonių vėlinimus (paketų apdorojimo laikus) MD_i, eiles prie tinklo sąsajų IQ_i, eiles



1 pav. ***Bendra informacinės saugos sistemos imitacinio modelio schema: M_1, M_2..., M_{NM} – modeliuojamos informacinės saugos priemonės, NM – saugos priemonių kiekis sistemoje; I_0, I_2..., I_{NI} – tinklo sąsajos, NI – tinklo sąsajų kiekis sistemoje; S_1, S_2..., S_{NS} – tinklų sąsajų generuojami duomenų srautai; NS – duomenų srautų kiekis; T_1, T_2,..., T_{NT} – tinklo segmentai, NT – tinklo segmentų kiekis sistemoje.***



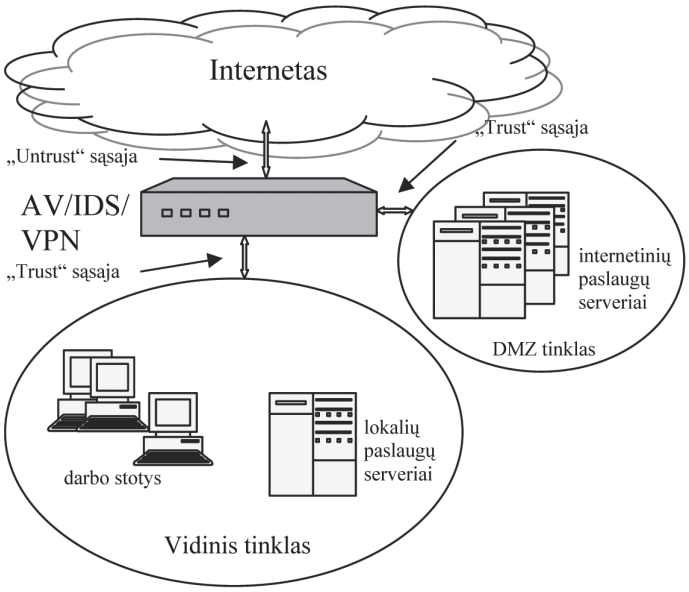
2 pav. ***„Trust-Untrust“ architektūra***

prie saugos modulių MQ_i. Tinklo sąsajų apkrovimas aprašomas paketo pasirodymo dažniu (ms). Tariama, kad kiekvienas modelio paketas yra 200 baitų dydžio. Jei norime aprašyti 2,5 Mbps srautą, paketų pasirodymo dažnis bus 0,64 ms.

Eilės susidaro prie tinklo sąsajų (kadangi reikalingas atitinkamas laiko tarpas duomenims siųsti ir gauti) ir prie saugos modulių (ribotas duomenų aptarnavimo kiekis ir laikas). Eilė prie sąsajų parodys tinklo pralaidumo išteklių nepakankamumą, o eilė prie saugos modulių – jų išteklių stygių (vadinasi, reikia kitaip dalinti duomenų srautus arba didinti modulių išteklius). Pagal masinio aptarnavimo teoriją paraiškos į sistemą ateina Puasono srautu (pasiskirsčiusios pagal eksponentinį dėsnį), kurio parametras – srauto intensyvumas – bus lygus IS_i.

Eksperimentinius GPSS modelius realizuosime dviems skirtingoms korporacinės įmonės informacinės saugos architektūroms, pateiktoms 2 ir 3 paveiksluose.

„Trust-Untrust“ architektūra sudaryta panaudojant maršrutizatorių, kuris turi mažiausiai dvi sąsajas. Jis jungia išorinį (nesaugų, „Untrust“) ir vidinį (saugų, „Trust“) kompiuterių tinklus. Šiame maršrutizatoriuje yra integruoti antivirusinis, IDS ir VPN moduliai. Visi įmonės serveriai: vidinių duomenų bazių, WEB, pašto, FTP serveriai, išdėstyti vidiniame tinkle. Duomenų srautai tarp vidinio tinklo kompiuterių ir visų serverių, iš jų ir internetinių paslaugų WEB, pašto, FTP, perduodami be papildomo tikrinimo informacinės saugos priemonėmis.



3 pav. ***„Trust-Untrust-Dmz“ architektūra***

„Trust-Untrust-Dmz“ architektūroje realizuotas papildomas apsaugos sluoksnis – DMZ tinklas, kuris izoliuoja vidinį tinklą nuo interneto paslaugų serverių. DMZ zonoje įkeliamos Web, FTP ir pašto paslaugos, kurios yra labiausiai pažeidžiamos. Ši architektūra realizuojama naudojant maršrutizatorių su integruotais antivirusiniu, IDS ir VPN moduliais. Duomenų srautai tarp vidinio tinklo kompiuterių ir internetinių paslaugų WEB, pašto, FTP serverių perduodami papildomai tikrinant informacinės saugos priemonėmis. Tačiau jei įsilaužėlis patenka į DMZ zoną, šis sluoksnis užtikrina, kad nebus patekta į vidinį įmonės tinklą.

Atsižvelgiant į įmonės saugumo politiką ir pasirinktą sistemos architektūrą, apibrėžiama duomenų paketų judėjimo tarp sąsajų kryptys pagal protokolą, saugumo modulių tipas ir skaičius. Modeliuojamoje sistemoje parinkti trys saugumo moduliai: VPN kodavimo, antivirusinės ir įsilaužimų aptikimo priemonės, kurios realizuotos Jenifer NetScreen įrenginyje (Juniper Networks Firewall, 2005). Modeliuojamas VPN modulis duomenų paketą koduoja 0,16 ms, antivirusinis modulis – tikrina 0,6 ms, įsilaužimų aptikimo modulis – 0,19 ms. Modeliuojamų sistemų architektūrų charakteristikos pateikiamos 1 lentelėje.

1 lentelė. ***Modeliuojamų sistemų architektūrų charakteristikos***

	„Trust-Untrust“ architektūra		„Trust-Untrust-DMZ“ architektūra		
	„Untrust“ sąsaja	„Trust“ sąsaja	„Untrust“ sąsaja	„Trust“ sąsaja	„DMZ“ sąsaja
Saugumo modulių skaičius		3		3	3
Tinklo sąsajų kiekis	1	1	1	1	1
Leidžiami protokolai tarp sąsajų:					
Iš „Untrust“ sąsajos		HTTP, SMTP, SSH, FTP, IPSec (VPN)		IPSec (VPN)	HTTP, SMTP, IPSec (VPN)
Iš „Trust“ sąsajos	Visi		Visi		HTTP, POP3, SMTP, FTP, SSH
Iš „DMZ“ sąsajos			SMTP, DNS		

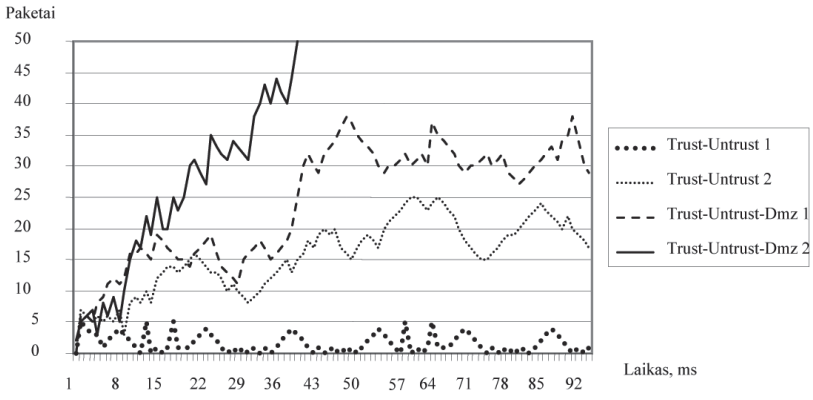
2 lentelė. ***Modeliuojami duomenų srautai ir jų pasiskirstymas pagal protokolus***

	„Trust-Untrust“ architektūra				„Trust-Untrust-DMZ“ architektūra					
	I variantas		II variantas		I variantas			II variantas		
	„Untrust“ sąsaja	„Trust“ sąsaja	„Untrust“ sąsaja	„Trust“ sąsaja	„Untrust“ sąsaja	„Trust“ sąsaja	„DMZ“ sąsaja	„Untrust“ sąsaja	„Trust“ sąsaja	„DMZ“ sąsaja
Duomenų srauto dydis, Mbps	2,50	1,10	5,00	2,50	2,50	3,50	0,10	5,00	2,50	1,00
Duomenų srautų pasiskirstymas pagal protokolus:										
HTTP	0,55	0,80	0,20	0,20	0,60	0,30		0,10	0,40	
FTP	0,05		0,05			0,30			0,40	
SMTP	0,30		0,55	0,50	0,30	0,15	0,99	0,85	0,05	0,99
IPsec (VPN)	0,10	0,05	0,20	0,15	0,10	0,05		0,05		
DNS							0,01			0,01
Kiti		0,05		0,15		0,10			0,15	

Duomenų srautų dydžiai, jų pasiskirstymas pagal protokolus priklauso nuo įmonės veiklos pobūdžio, naudojamų informacinių technologijų. Komercinėms įmonėms būdinga didesnis interneto paslaugų naudojimas, gamybinėms įmonėms – didesnis lokalių paslaugų naudojimas. Srautų charakteristikos gali būti nustatomos eksperimentiniais matavimais arba ekspertiniais vertinimais. Duomenų paketai į modeliuojamą sistemą ateina Puasono srautu (pasiskirstę pagal eksponentinį dėsnį). Modeliuojami duomenų srautai ir jų pasiskirstymas pagal protokolus pateikiami 2 lentelėje.

Modeliuodami gavome įvairius sistemos charakteristikų įvertinimus: saugos modulių darbo trukmes, jų apkrovimą, eilių prie saugumo modulių dydžius. Modeliuojamų architektūrų antivirusinio modulio gauti apkrovimai pateikiami 4 paveiksle.

Kaip matome iš gautų rezultatų, „Trust-Untrust-DMZ“ architektūroje, esant antrojo varianto duomenų srautams, antivirusinio modulio greitaveikos planuojamam apkrautumui nepakanka: reikia naudoti dar vieną antivirusinį modulį, perskirstyti duomenų srautus; pavyzdžiui, atskirti HTTP srautą ir jo netikrinti antivirusiniu moduliu.



4 pav. ***Antivirusinio modulio apkrovimas***

Išvados

Šiame darbe išanalizuota korporacinės įmonės informacinės saugos sistemos architektūrų modeliavimo svarba ir problemos. Apžvelgti architektūrų modeliavimo metodai: atakų grafai, apibendrinto kriterijaus metodas, imitacinis GPSS modelis, parodytos jų taikymo sritys ir sunkumai.

Sudarėme imitacinius GPSS modelius keliems informacinės saugos sistemos architektūrų variantams. Modeliavimas parodė, kad imitacinius modelius naudinga taikyti parenkant saugos sistemos realizavimo priemones, jų charakteristikas ir išdėstymą, duomenų srautų paskirstymą sistemoje. Atlikti tyrimai ir modeliavimo rezultatai parodė, kad siekiant visapusiškai įvertinti saugos sistemos architektūrą reikia naudoti keletą metodų: galimiems pažeidžiamumams aptikti, saugumo zonų topologijai projektuoti – atakų grafus, kiekinėms charakteristikoms apibrėžti, duomenų srautams paskirstyti – imitacinį GPSS modelį.

Atlikę tolesnius tyrimus, parengsime kelių informacinės saugos sistemos architektūros modeliavimo būdų kompleksinio taikymo metodikas.

LITERATŪRA

DOBRUCKI, M. (2002). Priorities in The Deployment of Network Intrusion Detection Systems. Prieiga per internetą: www.tml.hut.fi/~tpv/opiskelijat/dobrucki.pdf [žiūrėta 2005-05-19].

GPRS intranetas, Cisco VPN (2005). Prieiga per internetą: http://www.omnitel.lt/?m3_lt$206052_212539_212578_212932 [žiūrėta 2005-05-19].

GPSS World Reference Manual (2001) Prieiga per internetą: http://www.minutemansoftware.com/reference/rpreface.htm. [žiūrėta 2005-05-19].

JHA, S.; SHEYNER, O.; WING, J. (2003). The Formal Analyses of Attack graphs. Prieiga per internetą: http://www.cs.wisc.edu/~jha/jha-papers/security/CSFW_2002_1.pdf [žiūrėta 2005-05-19].

Juniper Networks Firewall / IPSec VPN (2005). Prieiga per internetą: http://www.juniper.net/products/integrated. [žiūrėta 2005-05-19].

Microsoft Internet Security and Acceleration (ISA) Server (2005). Prieiga per internetą: http://www.microsoft.com/isaserver/evaluation/overview/default.mspx [žiūrėta 2005-05-19].

MITCHELL, B. (2005) An introduction to VPN software, VPN hardware and protocol solutions. Prieiga per internetą: http://compnetworking.about.com/od/vpn/l/aa010701a.htm [žiūrėta 2005-05-19].

Panda GateDefender (2005). Prieiga per internetą: http://enterprises.pandasoftware.com/products/gatedefender/. [žiūrėta 2005-05-19].

SHEYNER, O. (2004). Scenario Graphs and Attack Graphs. Prieiga per internetą: http://reports-archive.adm.cs.cmu.edu/anon/2004/CMU-CS-04-122.pdf [žiūrėta 2005-05-19].

SLEMP, R. (2001) Firewall Architecture. Prieiga per internetą: www.nextep.com.au/upload/Firewall_Architecture.pdf [žiūrėta 2005-05-19].

VENČKAUSKAS, A.; MIKUCKIENĖ, I.; MIKUCKAS, A. (2003). Įmonės informacinės saugos efektyvumo vertinimas. *Informacijos mokslai,* T. 26, p. 90–93.

MODELLING OF ARCHITECTURES OF INFORMATION SYSTEM SECURITY OF COMPANIES'

Mindaugas Mikučionis, Eugenijus Toldinas, Algimantas Venčkauskas

Summary

The purpose of this work is to create and analyze the information security models of large corporations. It's difficult and hard to deploy efficiently safe systems due to complex network environment and enterprise computer systems. It's important to analyze security system parameters before design process. The enterprise information security system modelling helps us to solve these problems. Information security models with complex information security elements and safe data transferring between remote locations are designed. The models will help designers to compare different systems and to find the most secure and effective. This work generalizes the information security modelling process and describes the factors influencing it.