A priedas. Informacinės sistemos saugumo incidentai. Lentelės ir paveikslai

P1 lentelė. Populiariausi virusai
Table P1 Top viruses

Virusai	Įvykių skaičius	Viso, %	K	V	P	Lygis	m1	m2	m3	m4	m5
W32/Kryptik.AB!tr	25550	16,13	1	1	1	aukščiausias	1	1	0	0	0
JS/Iframe.W!tr	24729	15,61	0	1	0	žemiausias	1	1	0	0	0
JS/Blacole.L!tr.dldr	14218	8,97	1	1	0	vidutinis	1	1	0	0	0
W32/Zbot.ADN!tr	10827	6,83	1	1	1	aukščiausias	1	1	0	0	0
JS/Crypt.CAAD!tr	9402	5,93	1	1	1	aukščiausias	1	1	0	0	0
JS/JSRedir.AK!tr	9050	5,71	1	1	1	aukščiausias	1	1	0	0	0
W32/Dx.B2SS!tr	6287	3,97	1	1	1	aukščiausias	1	1	0	0	0
W32/Dapato.SMU!tr	4418	2,79	1	1	1	aukščiausias	1	1	0	0	0
W32/Zbot.YW!tr	3276	2,07	1	1	1	aukščiausias	1	1	0	0	0
JS/Obfuscus.AACA!tr	2947	1,86	1	1	1	aukščiausias	1	1	0	0	0
Others	47735	30,13	1	1	1		1	1	0	0	0
Total	158439	100									

P2 lentelė. Populiariausi *Spam* šaltiniai
Table P2 Top Spam sources

Siuntėjas	Įvykių skaičius	Viso, %
spam1@smap.spam	30478	1,73
spam2@smap.spam	18935	1,08
spam3@smap.spam	15912	0,9
spam4@smap.spam	15688	0,89
spam5@smap.spam	14937	0,85
spam6@smap.spam	12742	0,72
spam7@smap.spam	10763	0,61
spam8@smap.spam	10623	0,6
spam9@smap.spam	10023	0,57
spam10@smap.spam	9745	0,55
spam11@smap.spam	9534	0,54
spam12@smap.spam	8632	0,49
spam13@smap.spam	8593	0,49
spam14@smap.spam	8577	0,49
spam15@smap.spam	7823	0,44

P2 lentelės pabaiga

spam16@smap.spam	7458	0,42
spam17@smap.spam	7093	0,4
spam18@smap.spam	6286	0,36
spam19@smap.spam	6252	0,36
spam20@smap.spam	6011	0,34
spam21@smap.spam	5963	0,34
spam22@smap.spam	5941	0,34
spam23@smap.spam	5936	0,34
spam24@smap.spam	5250	0,3
spam25@smap.spam	4690	0,27
spam26@smap.spam	4584	0,26
spam27@smap.spam	4537	0,26
spam28@smap.spam	4505	0,26
spam29@smap.spam	4038	0,23
spam30@smap.spam	4037	0,23
Kiti	1483709	84,34
Viso	1759295	100

P3 lentelė. Populiariausios atsisakymo aptarnauti atakos
Table P3 Top denial of services atacks

Ataka	**Įvykių skaičius**	**Viso, %**	**K**	**V**	**P**	**Lygis**	m1	m2	m3	m4	m5
udp_flood	5611	5,91 %	0	0	1	aukščiausias	0	0	0	1	1
udp_dst_session	16004	16,86 %	0	0	1	aukščiausias	1	0	0	0	1
icmp_flood	8414	8,87 %	0	0	1	aukščiausias	0	0	0	1	1
tcp_syn_flood	5045	5,32 %	0	1	1	aukščiausias	1	0	0	0	1
udp_src_session	4446	4,69 %	0	0	1	aukščiausias	1	0	0	0	1
tcp_port_scan	4160	4,38 %	1	0	0	aukščiausias	0	0	0	0	1
icmp_sweep	3026	3,19 %	1	0	0	aukščiausias	0	0	0	0	1
tcp_src_session	2567	2,71 %	0	0	1	aukščiausias	1	0	0	0	1
icmp_src_session	2291	2,41 %	0	0	1	aukščiausias	0	0	0	0	1
tcp_dst_session	6359	6,70 %	0	0	1	aukščiausias	1	0	0	0	1
icmp_bad_checksum	4136	4,36 %	0	0	1	žemiausias	1	0	0	1	1
udp_scan	3525	3,71 %	1	0	0	aukščiausias	0	0	0	0	1
ICMP.Bad.Checksum	1792	1,89 %	0	0	1	žemiausias	1	0	0	1	1
TCP.Bad.Flags	1739	1,83 %	1	1	1	žemiausias	1	1	1	1	1
MS.Windows.WINS.Privilege.Elevation	808	0,85 %	1	1	0	vidutinis	1	1	1	0	0

MS.Windows.NAT.Helper.DNS.Query.DoS	448	0,47 %	0	0	1	aukščiausias	1	1	1	0	1
icmp_dst_session	1313	1,38 %	0	0	1	aukščiausias	1	0	0	1	1
TCP.Bad.Option.Length	5798	6,11 %	1	0	0	žemiausias	1	1	1	1	1
MS.SQL.Server.Empty.Password	3549	3,74 %	1	1	0	žemiausias	1	1	1	0	0
MSSQL.Empty.Password	3187	3,36 %	1	1	0	žemiausias	1	1	1	0	0
IKE.Exchange.DoS.Version	3071	3,24 %	0	0	1	žemiausias	1	1	1	0	0
MSSQL.Login.Brute.Force	2768	2,92 %	1	1	0	žemiausias	1	1	1	0	0
RealVNC.Server.Authentication.Bypass	1546	1,63 %	1	1	0	vidutinis	1	0	0	0	0
HTTP.URI.Overflow	1041	1,10 %	0	1	1	aukščiausias	1	1	1	0	0
HTTP.Request.Smuggling	798	0,84 %	1	1	0	aukščiausias	1	1	1	0	0
TCP.TTL.Evasion	339	0,36 %	0	1	0	žemiausias	1	0	0	1	1
MS.SQL.Server.XP.Command.Execution	210	0,22 %	1	1	0	žemiausias	1	1	1	0	0
SMTP.Auth.Buffer.Overflow	180	0,19 %	1	1	1	aukščiausias	1	0	0	1	1
MS.SQL.Server.Resolution.Service.Heap.Overflow	145	0,15 %	1	1	1	aukščiausias	1	1	1	0	0
CA.BrightStor.ARCserve.Backup.Agent.Buffer.Overflow	127	0,13 %	1	1	1	aukščiausias	1	0	0	0	0
Others	452	0,48 %	1	1	1		1	1	1	1	1
Total	**94894**	**100,00 %**									

P4 lentelė. Modeliuojamos realios informacinės sistemos charakteristikos
Table P4 Modelled real information system characteristics

	m														
	1			2			3			4			5		
$P_M(m)$	0,4			0,3			0,1			0,1			0,1		
Δt_d, h	0,5			0,5			2			4			4		
$w(m)$	0,3			0,2			0,1			0,2			0,2		
	$P_m(j)$														
j	K	V	P	K	V	P	K	V	P	K	V	P	K	V	P
3	0,021	0,062	0,021	0,021	0,062	0,014	0,011	0,006	0,004	0,005	0,001	0,008	0,005	0,001	0,008
2	0,027	0,027	0,010	0,024	0,024	0,010	0,001	0,034	0,033	0,000	0,000	0,000	0,000	0,000	0,000
1	0,054	0,059	0,115	0,054	0,055	0,055	0,000	0,001	0,001	0,000	0,000	0,028	0,040	0,005	0,095

P5 lentelė. Informacinės sistemos saugumo mechanizmai
Table P5 Information system security mechanismes

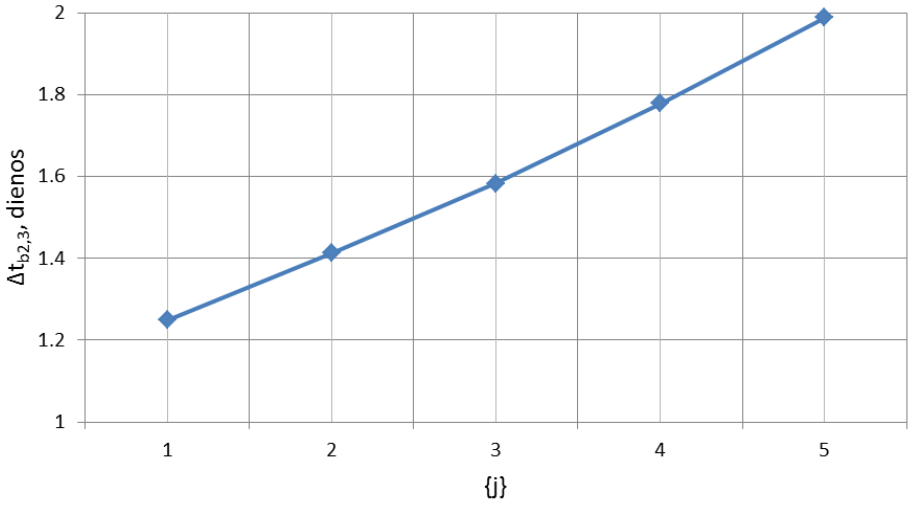
Saugumo mechanizmai	Saugumas			Informacinės sistemos moduliai				
	K	V	P	1	2	3	4	5
1.1.	1	1	1	1	1	1	1	1
1.2.	1	1	1	1	1	1	1	1
1.3.	1	1	1	1	1	1	1	1
1.4.	1	1	1	1	1	1	1	1
1.5.	1	1		1				
1.6.	1			1	1	1		
1.7.	1	1		1	1	1	1	1
1.8.	1	1	1	1	1	1	1	1
1.9.								
1.9.1.			1	1		1	1	1
1.9.2.	1	1	1	1	1	1		
1.9.3.	1	1	1	1	1	1	1	1
1.9.4.	1	1	1	1	1	1	1	1
1.9.5.	1	1	1	1	1	1	1	1
1.9.6.	1	1	1	1	1	1	1	1
1.9.7.	1	1	1	1	1	1	1	1
1.9.8.			1				1	1
1.9.9.								
1.9.10.			1	1	1	1	1	1
1.9.11.	1	1	1	1	1	1	1	1
2.1.	1	1	1	1	1	1	1	1
2.2.			1	1			1	1
2.3.	1	1			1	1		1
2.4.		1		1	1	1	1	1
2.5.	1	1	1	1	1	1	1	1
2.6.	1	1	1	1	1	1	1	1
2.7.			1	1	1	1	1	1
2.8.			1				1	1
2.9.								
2.10.	1		1	1	1	1	1	1
2.11.			1	1	1	1	1	1
2.12.	1			1	1	1	1	1
2.13.			1	1	1	1	1	1
2.14.			1	1	1	1	1	1
2.15.	1	1		1	1	1	1	1
2.16.	1	1		1	1	1	1	1
2.17.	1	1		1	1	1		
2.18.	1	1		1	1	1		
2.19.	1	1		1	1	1	1	1

P3 lentelės pabaiga

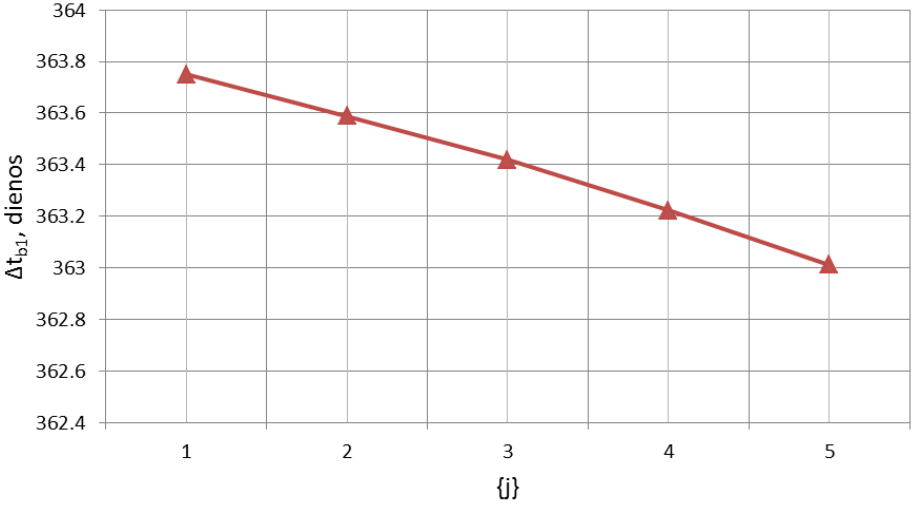
Saugumo mechanizmai	Saugumas			Informacinės sistemos moduliai				
	K	V	P	1	2	3	4	5
2.20.	1	1		1	1	1	1	1
2.21.	1	1		1	1	1	1	1

P6 lentelė. Informacinės sistemos modulių apsaugos charakteristikos
Table P6 Information system module security charakteristic

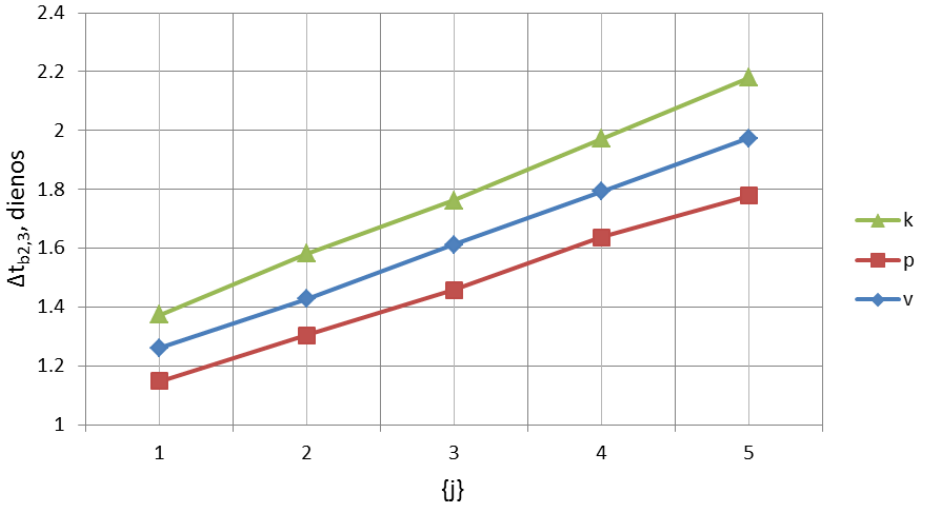
Inci-dento lygis	Modulis														
	1			2			3			4			5		
	K	V	P	K	V	P	K	V	P	K	V	P	K	V	P
3	0,04	0,04	0,08	0,04	0,04	0,16	0,04	0,04	0,12	0,21	0,19	0,04	0,18	0,15	0,04
2	0,05	0,05	0,10	0,05	0,05	0,21	0,05	0,05	0,16	0,28	0,25	0,05	0,23	0,20	0,05
1	0,06	0,06	0,13	0,06	0,06	0,26	0,06	0,06	0,19	0,35	0,31	0,06	0,29	0,25	0,06


2
1.8
1.6
1.4
1.2
1
$\Delta t_{b2,3}$, dienos
1
2
3
4
5
{j}

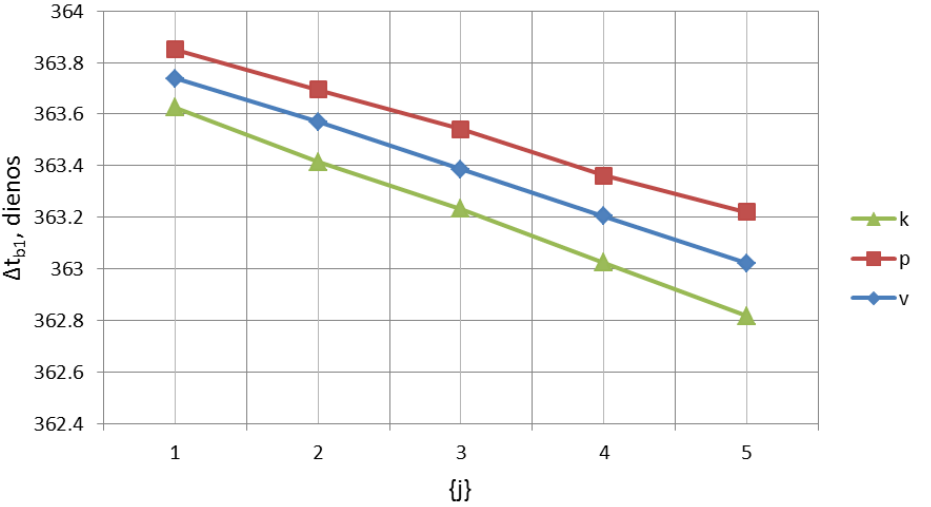
a)


364
363.8
363.6
363.4
363.2
363
362.8
362.6
362.4
Δt_{b1}, dienos
1
2
3
4
5
{j}

b)



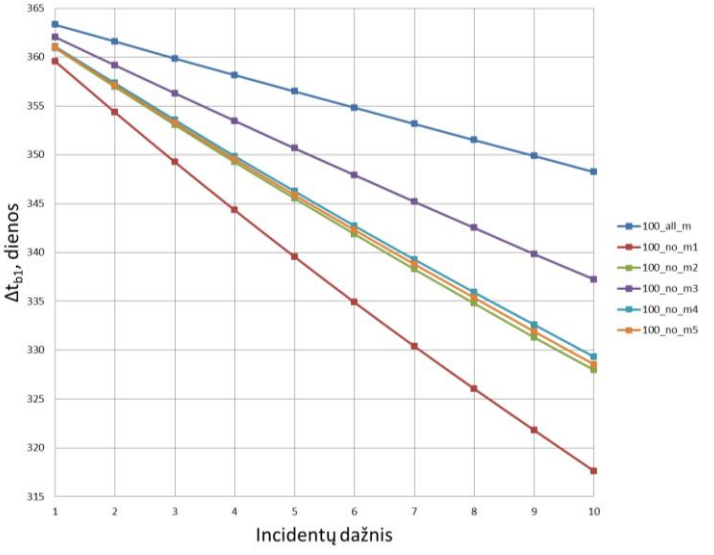
c)



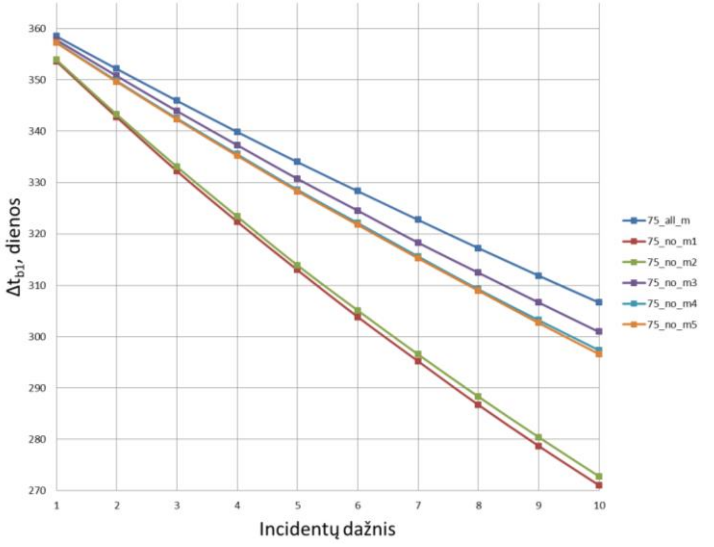
d)

P1 pav. Incidentų sunkumo įtaka sistemos būsenai: a) b_2 ir b_3 b) b_1; c) b_2 ir b_3 d) b_1 priklausomai nuo grėsmės (3.2 lentelė)

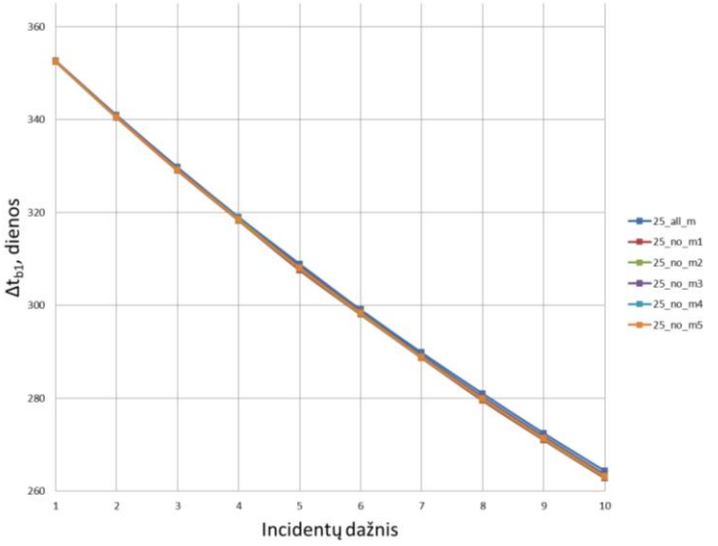
Fig. P1 Incident Severity Influence on System States: a) b_2 and b_3 b) b_1; c) b_2 and b_3 d) b_1 according to the threat (Table 3.2.)


365
360
355
350
345
340
335
330
325
320
315
1
2
3
4
5
6
7
8
9
10
Δt_b1, dienos
Incidentų dažnis
100_all_m
100_no_m1
100_no_m2
100_no_m3
100_no_m4
100_no_m5

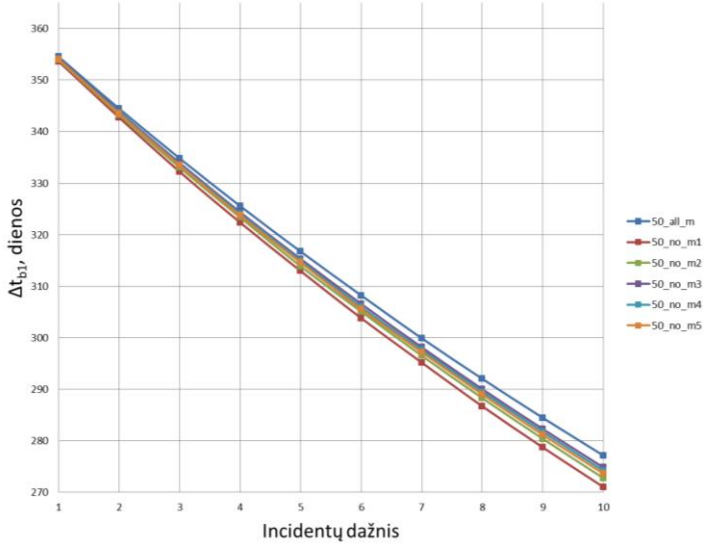
a)


360
350
340
330
320
310
300
290
280
270
1
2
3
4
5
6
7
8
9
10
Δt_b1, dienos
Incidentų dažnis
75_all_m
75_no_m1
75_no_m2
75_no_m3
75_no_m4
75_no_m5

b)



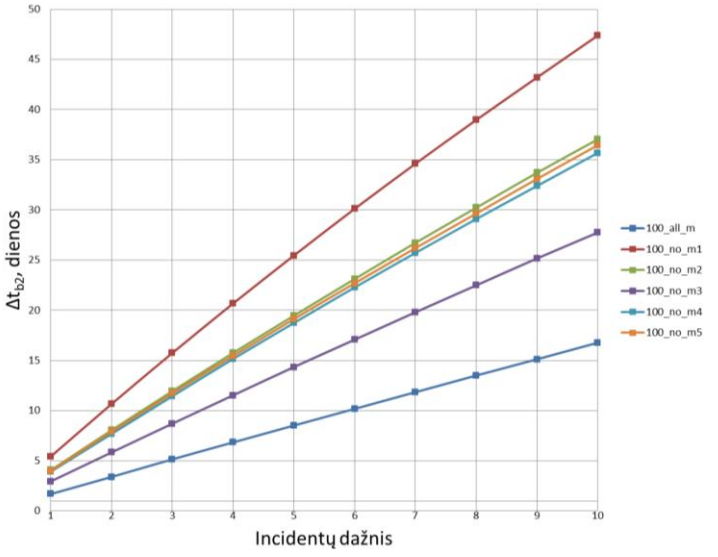
c)



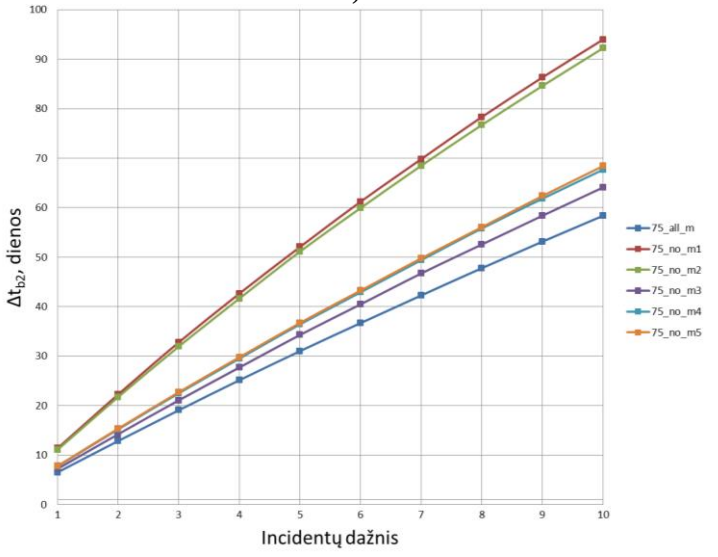
d)

P2 pav. Sistemos normalios būsenos priklausomybė nuo incidentų dažnio eliminuojant tam tikrus modulius a) 100 %, b) 75 %, c) 50 % ir d) 25 % įdiegtų mechanizmų kiekis

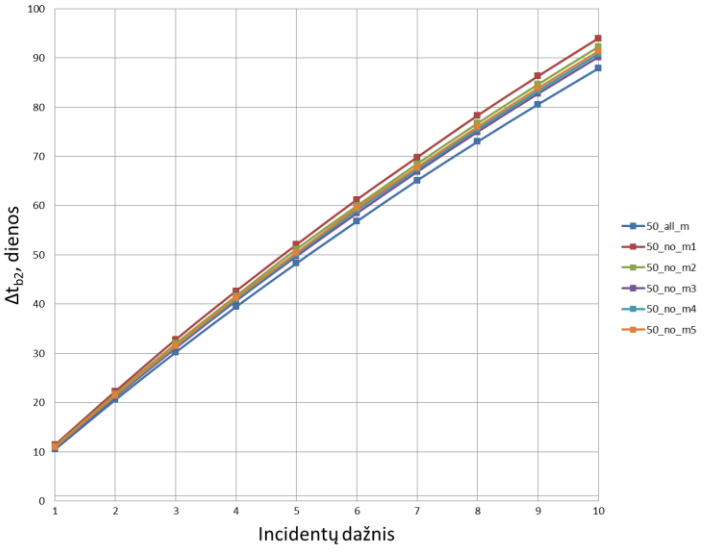
Fig. P2 Normal system state dependency charakteristic according to incident frequency and module existence a) 100%, b) 75%, c) 50% and d) 25% implemented security mechanisms


50
45
40
35
30
25
20
15
10
5
0
1
2
3
4
5
6
7
8
9
10
Δt_b2, dienos
Incidentų dažnis
100_all_m
100_no_m1
100_no_m2
100_no_m3
100_no_m4
100_no_m5

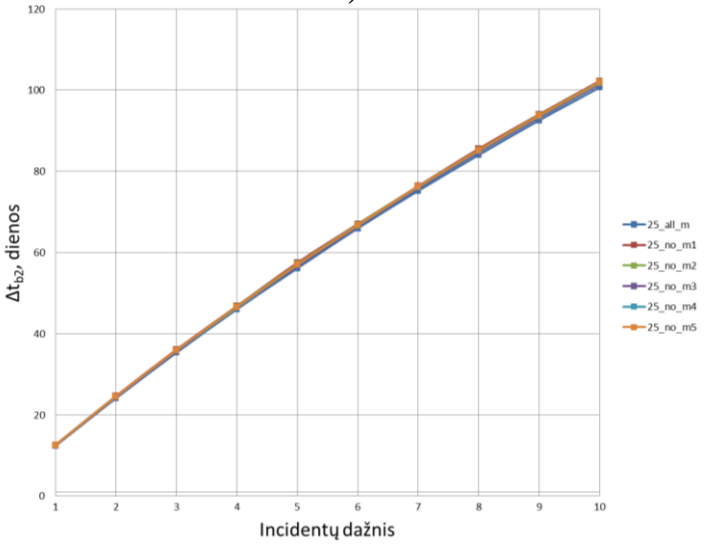
a)


100
90
80
70
60
50
40
30
20
10
0
1
2
3
4
5
6
7
8
9
10
Δt_b2, dienos
Incidentų dažnis
75_all_m
75_no_m1
75_no_m2
75_no_m3
75_no_m4
75_no_m5

b)

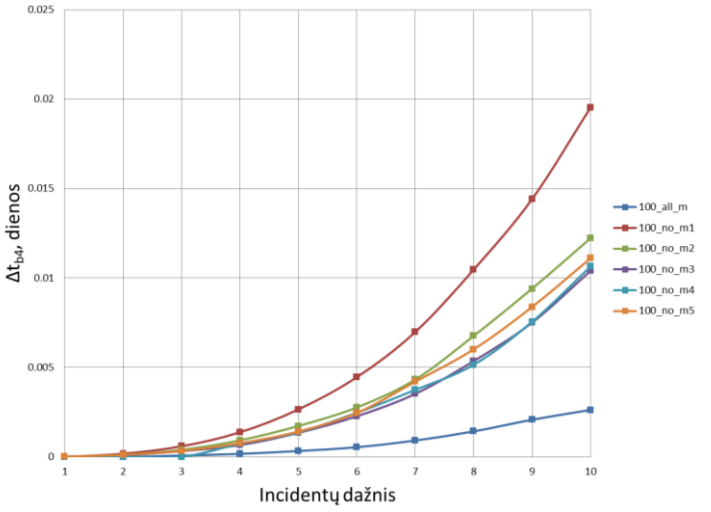


c)

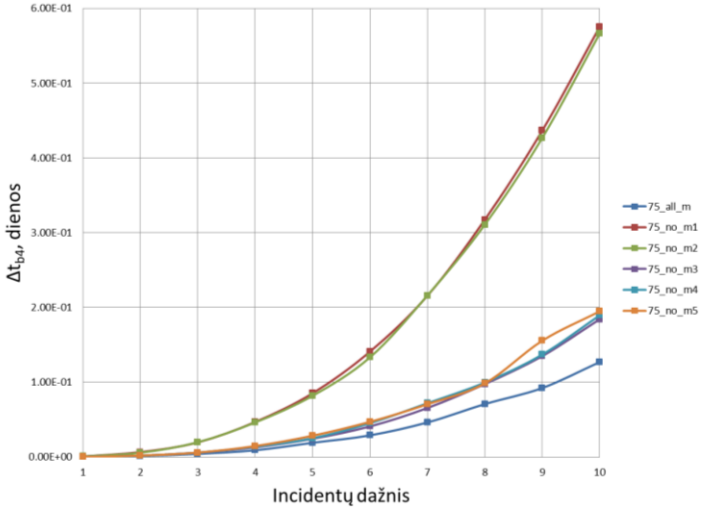


d)

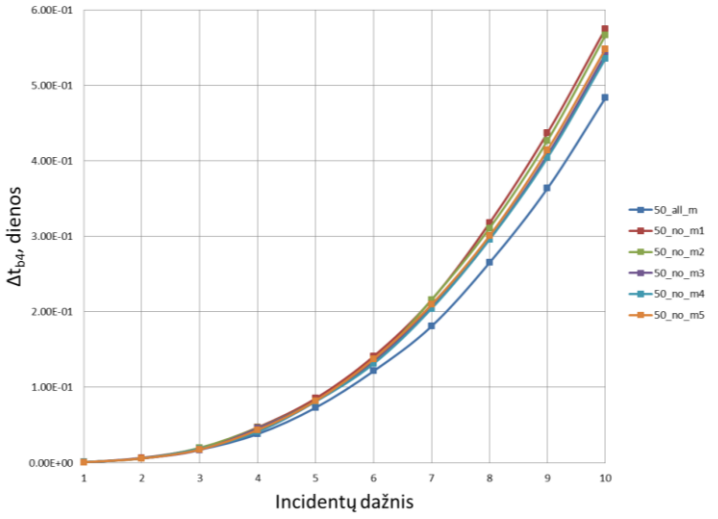
P3 pav. Sistemos b_2 būsenos priklausomybė nuo incidentų dažnio eliminuojant tam tikrus modulius a) 100 %, b) 75 %, c) 50 % ir d) 25 % įdiegtų mechanizmų kiekis
Fig. P3 System b_2 state dependency charakteristic according to incident frequency and module existence a) 100%, b) 75%, c) 50% and d) 25% implemented security mechanisms


0.025
0.02
0.015
0.01
0.005
0
1
2
3
4
5
6
7
8
9
10
Δtb4, dienos
Incidentų dažnis
100_all_m
100_no_m1
100_no_m2
100_no_m3
100_no_m4
100_no_m5

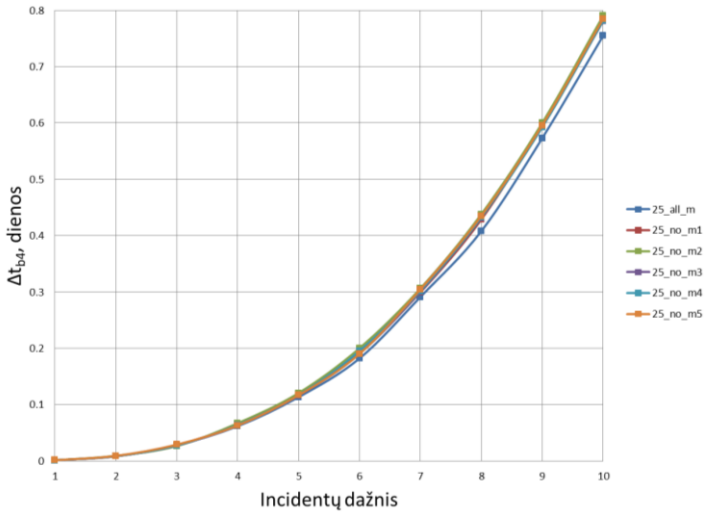
a)


6.00E-01
5.00E-01
4.00E-01
3.00E-01
2.00E-01
1.00E-01
0.00E+00
1
2
3
4
5
6
7
8
9
10
Δtb4, dienos
Incidentų dažnis
75_all_m
75_no_m1
75_no_m2
75_no_m3
75_no_m4
75_no_m5

b)



c)



d)

P4 pav. Sistemos b_4 būsenos priklausomybė nuo incidentų dažnio eliminuojant tam tikrus modulius a) 100 %, b) 75 %, c) 50 % ir d) 25 % įdiegtų mechanizmų kiekis
Fig. P4 System b_4 state dependency charakteristic according to incident frequency and module existence a) 100%, b) 75%, c) 50% and d) 25% implemented security mechanisms

B priedas. Informacinės sistemos saugumo reikalavimai

Informacinės sistemos reikalavimai paimti iš valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techninių saugos reikalavimų aprašo (Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai, 2008).

1. Bendrieji informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai:

1.1. turi būti periodiškai atliekamas informacinės sistemos informacinių technologijų saugos atitikties vertinimas (toliau – atitikties vertinimas);

1.2. informacinė sistema turi registruoti bent vieną paskutinį informacinės sistemos elektroninės informacijos pakeitimą atlikusį informacinės sistemos naudotoją ir pakeitimo laiką;

1.3. informacinės sistemos priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus identifikatorių, kuriuo naudojantis nebūtų galima atlikti informacinės sistemos naudotojo funkcijų;

1.4. kiekvienas informacinės sistemos naudotojas turi būti informacinėje sistemoje unikaliai identifikuojamas – informacinės sistemos naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kita autentiškumo patvirtinimo priemone;

1.5. informacinės sistemos naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai informacinės sistemos naudotojas atostogauja, vykdomas informacinės sistemos naudotojo veiklos tyrimas ir pan.; pasibaigus tarnybos (darbo) santykiams, informacinės sistemos naudotojo teisė naudotis informacine sistema turi būti panaikinta;

1.6. baigus darbą turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą ir pan.;

1.7. informacinės sistemos naudotojui neatliekant jokių veiksmų, informacinė sistema turi užsirakinti, kad toliau naudotis informacine sistema galima būtų tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

1.8. institucija turi išsiaiškinti, kiek ji ilgiausiai gali tęsti savo funkcijų įgyvendinimą neveikiant informacinei sistemai ar jos daliai; institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi užtikrinti informacinės sistemos veiklos atkūrimą per šį laikotarpį; turi būti parengtas veiksmų planas, užtikrinantis informacinės sistemos veiklos atnaujinimą ketvirtosios kategorijos informacinėms sistemoms per 16 val., trečiosios kategorijos informacinėms sistemoms – per 8 val., antrosios kategorijos

informacinėms sistemoms – per 1 val., pirmosios kategorijos informacinėms sistemoms – per 15 min.;

1.9. reikalavimai informacinės sistemos įrangai ir patalpoms:

1.9.1. pagrindinė informacinės sistemos kompiuterinė įranga turi turėti įtampos filtrą arba (ir) rezervinį maitinimo šaltinį;

1.9.2. turi būti naudojamos kenksmingosios informacinės sistemos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos;

1.9.3. turi būti operatyviai įdiegiami informacinės sistemos operacinės sistemos ir naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

1.9.4. informacinėje sistemoje turi būti naudojama tik legali programinė įranga;

1.9.5. įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

1.9.6. įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai;

1.9.7. turi būti apribota fizinė prieiga prie informacinės sistemos tarnybinių stočių (atskiros rakinamos patalpos arba rakinama spinta);

1.9.8. patalpose, kuriose yra informacinės sistemos tarnybinės stotys, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

1.9.9. turi būti užtikrintas informacinės sistemos prieinamumas ketvirtosios kategorijos informacinėms sistemoms ne mažiau kaip 70 % laiko darbo metu darbo dienomis, trečiosios kategorijos informacinėms sistemoms – ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis, antrosios kategorijos informacinėms sistemoms – ne mažiau kaip 96 %. laiko visą parą, pirmosios kategorijos informacinėms sistemoms – ne mažiau kaip 99 % laiko visą parą;

1.9.10. turi būti daromos atsarginės elektroninės informacijos kopijos (toliau – kopijos), kurios turi būti laikomos atskiroje patalpoje;

1.9.11. informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacinių tinklų naudojant užkardą ar kitas priemones.

2. Trečiosios kategorijos informacinių sistemų elektroninės informacijos papildomi techniniai saugos reikalavimai:

2.1. atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per dvejus metus, jei teisės aktuose nenustatyta kitaip;

2.2. informacinė sistema turi perspėti administratorių, kai pagrindinėje informacinės sistemos kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

2.3. viešaisiais telekomunikaciniais tinklais perduodamos informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas,

naudojant šifravimą, virtualų privatų tinklą (angl. *Virtual Private Network*), skirtines linijas, saugų valstybinį duomenų perdavimo tinklą ar kitas priemones;

2.4. informacinė sistema turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones;

2.5. informacinėje sistemoje turi būti registruojami ir nustatytą laiką saugomi duomenys apie informacinės sistemos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinėje sistemoje, kitus saugai svarbius įvykius, nurodant informacinės sistemos naudotojo identifikatorių ir įvykio laiką; ši informacija turi būti reguliariai analizuojama;

2.6. patekimas į informacinės sistemos tarnybinių stočių patalpas turi būti kontroliuojamas;

2.7. rezervinis maitinimo šaltinis turi užtikrinti informacinės sistemos pagrindinės kompiuterinės įrangos veikimą ne mažiau nei 10 min.;

2.8. jei informacinės sistemos tarnybinių stočių patalpose esančios įrangos bendras galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga;

2.9. institucija turi numatyti atsargines patalpas, į kurias galėtų laikinai perkelti informacinės sistemos įrangą, nesant galimybių tęsti veiklą pagrindinėse patalpose; institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi užtikrinti informacinės sistemos veiklos atnaujinimą atsarginėse patalpose per tokį laikotarpį, kad nebūtų nusižengta institucijos įsipareigojimams, susijusiems su informacinės sistemos veikla;

2.10. kopijų darymas turi būti fiksuojamas žurnale;

2.11. kopijos turi būti saugomos užrakintoje nedegioje spintoje;

2.12. elektroninė informacija kopijose turi būti užšifruota arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų neteisėtam elektroninės informacijos atkūrimui;

2.13. periodiškai turi būti atliekami elektroninės informacijos atkūrimo iš kopijų bandymai;

2.14. atsarginės laikmenos su programine įranga turi būti laikomos nedegioje spintoje;

2.15. slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius;

2.16. slaptažodį turi sudaryti ne mažiau kaip 6 simboliai;

2.17. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;

2.18. keičiant slaptažodį informacinė sistema neturi leisti nustatyti slaptažodžio iš buvusių 3 paskutinių slaptažodžių;

2.19. slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija;

2.20. pirmojo prisijungimo prie informacinės sistemos metu iš informacinės sistemos naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį;

2.21. turi būti draudžiama slaptažodžius atskleisti tretiesiems asmenims.

Pagal pateiktus saugumo reikalavimus buvo nustatytas visų informacinės sistemos modulių atsparumas konfidencialumo, vientisumo ir pasiekiamumo atakoms. Saugumo mechanizmai buvo priskirti informacinės sistemos moduliams. Rezultatai pateikiami 4.7 lentelėje (A priedas).