MYKOLO ROMERIO UNIVERSITETO
VALSTYBINIO VALDYMO FAKULTETO
TEISINĖS INFORMATIKOS KATEDRA

VYTAUTAS PTAKAUSKAS
VIEŠO ADMINISTRAVIMO STUDIJŲ PROGRAMOS
ELEKTRONINĖS VALDŽIOS ADMINISTRAVIMO SPECIALIZACIJA

ELEKTRONINIŲ PASLAUGŲ INFORMACIJOS SAUGUMO POLITIKA VALSTYBINĖJE MOKESČIŲ INSPEKCIJOJE

Magistro baigiamasis darbas

Darbo vadovas
Prof. dr. Arūnas Augustinaitis

Vilnius, 2004

TURINYS

ĮVADAS

Europos Komisija 2002 m. gegužės 28 dieną patvirtino ir tų pačių metų liepos 21 – 22 d. d. Europos Tarybos posėdyje, vykusiame Sevilijoje (Ispanija), pristatė Veiksmų planą „e. Europa 2005: Informacinė visuomenė visiems" (*e Europe 2005: An information society for all*)[1]. Veiksmų plane Europos Sąjungos (ES) šalims iškeliamas tikslas - sukurti palankią aplinką ir sudaryti sąlygas privačioms investicijoms, kurti naujas darbo vietas, skatinti ir didinti darbo našumą, tobulinti viešąsias paslaugas ir suteikti galimybę kiekvienam dalyvauti globalioje informacinėje visuomenėje. Šį planą numatoma įgyvendinti, veikiant dviem kryptimis - **skatinant dialoginiu režimu teikiamas viešąsias paslaugas** (e. vyriausybė, e. mokymasis, e. sveikatos apsauga ir e. verslas) ir plėtojant plačiajuostę greitaeigę bei **saugią telekomunikacinę infrastruktūrą**.

Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. patvirtintoje Elektroninės valdžios koncepcijoje[2], akcentuojama labai svarbi nuostata - **saugus e. viešųjų paslaugų diegimas**. Koncepcijoje sakoma, kad atsižvelgiant „*į specifines Lietuvos Respublikos sąlygas ir Europos politinę iniciatyvą dėl e. valdžios*", būtina „*įdiegti e. valdžią, kad valstybės valdymas taptų atviresnis, demokratiškesnis, atskaitingesnis, efektyvesnis*, … *užtikrinti informacinių technologijų saugumą, kai viešosioms paslaugoms teikti naudojamos skaitmeninės technologijos*"[3].

Kalbant apie informacijos saugumą, labai dažnai apsiribojama technologinių, techninių ir programinių saugumo sprendimo būdų, jų privalumų ir trūkumų nagrinėjimu, o organizacinėms priemonėms – informacijos saugumo strategijai ir taktikai, koncepcijai ir politikai, informacinių resursų saugumo planams, skiriamas nepakankamas dėmesys[4]. Lietuvos integracija į ES reikalauja keisti valstybinių institucijų vadovų požiūrį į informacijos saugumą. Standartinių žodžių, kad informacija turi būti prieinama, kad turi būti užtikrintas jos vientisumas ir konfidencialumas, aiškiai nepakanka, kadangi pati informacijos sąvoka pakankami abstrakti, grėsmės jos saugumui turi tikimybinį charakterį, o techninės ir organizacinės priemonės brangiai kainuoja.

---

[1] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions eEurope 2005: An information society for all; http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf; prisijungimo laikas: 2004-11-12.

[2] Elektroninės valdžios koncepcija//Valstybės žinios. 2003. Nr.: 2-54

[3] Ten pat

[4] С. А. Петренко, С. В. Симонов, «Управление информационными рисками. Экономически оправданная безопасность». — М.: «Компания АйТи», «ДМИ Пресс», 2004 г.

Darbo tikslas – išnagrinėti viešųjų e. paslaugų informacijos saugumo prielaidas ir galimybes.

Siekiant šio tikslo, buvo keliami šie **uždaviniai**:

1. Apžvelgti ES ir Lietuvos Respublikos norminius aktus, reglamentuojančius informacijos saugumą ir teisines prielaidas viešųjų e. paslaugų teikimui VMI;
2. Pagrįsti vis didėjantį viešųjų e. paslaugų poreikį informacinėje visuomenėje ir pateikti technologinį viešųjų e. paslaugų modelį;
3. Apžvelgti pagrindinius informacijos saugumo modelius;
4. Supažindinanti su pagrindiniais saugumo sistemos elementais, pateikti jų ryšių modelį, saugumo koncepciją, principus bei valdymo tikslus.
5. Apžvelgti VMI informacinių sistemų audito išvadas, informacijos saugumo pažeidimų tyrimus Lietuvoje ir Jungtinėje Karalystėje.

Darbo objektas - Valstybinės mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos ir jai pavaldžių apskričių valstybinės mokesčių inspekcijos (toliau – VMI) viešųjų e. paslaugų saugumas. Pateikiamas požiūris, kokiais principais vadovaujantis turi būti nustatyti saugumo reikalavimai viešosioms e. paslaugoms.

Darbo hipotezė – informacijos pažeidimo pasekmių supratimas ir informacijos saugumo kultūros suformavimas - lemiami faktoriai, norint sėkmingai įdiegti informacijos saugumo sistemą, kuri užtikrintų saugias viešąsias e. paslaugas VMI.

Darbą struktūra. Darbą sudaro įžanga, trys skyriai su poskyriais, išvados, literatūros sąrašas, trumpa santrauka anglų kalba ir priedai.

Pirmame skyriuje apžvelgiami pagrindiniai ES ir Lietuvos Respublikos norminiai aktai, reglamentuojantys informacijos saugumą, pateikiama trumpa viešųjų e. paslaugų poreikio analizė ES ir Lietuvoje, analizuojamos teisinės prielaidas viešųjų e. paslaugų teikimui VMI, apžvelgiamas šių paslaugų teikimo galimybės bei poreikiai ir pateikiamas technologinis viešųjų e. paslaugų modelis.

Antrame skyriuje trumpai apžvelgiami pagrindiniai informacijos saugumo modeliai, pateikiamas saugumo sistemos įgyvendinimo procesas, apžvelgiami pagrindiniai informacijos saugumo sistemos elementai, pateikiamas jų ryšių modelis ir saugumo koncepcija, pagrindiniai informacijos saugumo principai bei viešųjų e. paslaugų saugumo valdymo tikslai, informacijos saugumo ypatumai ir informacijos saugumo tarnybos vieta VMI organizacinėje struktūroje.

Trečiame skyriuje apžvelgiamos VMI informacinių sistemų audito išvados, informacijos saugumo pažeidimų tyrimai Lietuvoje ir Jungtinėje Karalystėje (JK).

Literatūra. Darbe naudotasi ES ir Lietuvos norminiais aktais, reglamentuojančiais tinklo ir informacijos saugumą, tarptautiniais standartais ISO/IEC TR 13335 (Informacijos technologijų saugumo valdymo gairės) ir ISO/IEC 17799 (Praktiniai informacijos saugumo valdymo principai), Junginių Amerikos Valstijų Nacionalinio standartų ir technologijų instituto (*National Institute of Standards and Technology*) standartais ir rekomendacijomis, amerikiečių autorių T. R. Peltier‘o knyga „*Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*“ ir S. Barman‘o knyga „*Writing Information Security Policies*“, T. Braithwaite‘o internetiniu leidiniu „*Securing E-Business Systems: A Guide for Managers and Executives*“, Rusijos informacijos saugumo specialistų A. ir J. Rodičev‘ų, A. Lukackij ir kitų autorių straipsniais, kitais įvairias šaltiniais internete, ypač Jungtinių Amerikos Valstijų ir Jungtinės Karalystės vyriausybinėse svetainėse pateikiama medžiaga informacijos saugumo klausimais bei medžiaga VMI intranete. Literatūros sąrašas pateikiamas šia tvarka, pirmoje grupėje nurodomi naudoti Lietuvos Respublikos norminiai aktai, antroje – Europos Sąjungos norminiai aktai, trečioje tarptautiniai informacijos technologijų saugumo standartai ir ketvirtoje – naudotos literatūros sąrašas.

Iliustracijos. Įvairios nedidelės lentelės, grafikai ir schemos pateikiamos pačiame darbe, iš karto po teksto. Lentelių, grafikų ir schemų pavadinimai pateikiami jų apatinėje dalyje. Jie numeruojami, suteikiant skyriaus numerį ir lentelės, grafiko ar schemos eilės numerį šiame skyriuje. Didesnės apimties lentelės ir pilnas JK saugumo pažeidimų tyrimas ISBS 2004 pateikiamos darbo priede.

Citatos. Citatos iš norminių aktų ir naudotos literatūros pateikiamos kabutėse pasvirusiu šriftu, išnašose nurodomas cituojamas šaltinis.

1. VIEŠŲJŲ E. PASLAUGŲ SAUGUMO UŽTIKRINIMO POREIKIS

1.1. INFORMACIJOS SAUGUMAS EUROPOS SĄJUNGOJE

Europos Tarybos valstybės narės, atsižvelgdamos „*į didėjantį automatizuotai tvarkomų asmens duomenų srautą, kuris kerta sienas, drauge dar kartą patvirtindamos savo įsipareigojimą dėl informacijos laisvės, nepaisant sienų, pripažindamos, kad būtina derinti ir gerbti pagrindines asmens privataus gyvenimo vertybes ir laisvą informacijos srautą*“[5], 1981 m. sausio 28 d. Strasbūre priėmė vieną pirmųjų dokumentų, susijusių su informacijos saugumu ir reglamentuojančiu automatizuotai tvarkomus asmens duomenis - Europos Tarybos šalių narių Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)[6]. Šios Konvencijos tikslas – užtikrinti, „*kad, tvarkant asmens duomenis automatizuotai, visų šalių teritorijose bus gerbiamos kiekvieno asmens, nepaisant jo tautybės ir gyvenamosios vietos, teisės ir pagrindinės laisvės, o svarbiausia, jo teisė į privatų gyvenimą*.“[7] Konvenciją pasirašiusios šalys įsipareigojo dėl asmens duomenų rinkimo principų, jų kaupimo tikslingumo ir duomenų saugumo. Konvencijos septintame straipsnyje „Duomenų apsauga“ sakoma, kad „*Automatizuotai kaupiamiems asmens duomenims apsaugoti turi būti imtasi tinkamų apsaugos priemonių, kurios neleistų jų netyčia ar neteisėtai sunaikinti, netyčia prarasti, neleistinai palikti juos prieinamus, keisti ar platinti*”.[8] Europos Tarybos Ministrų komitetas 1999 m. birželio 15 d. priėmė šios Konvencijos pataisą, kurioje išskyrė kai kurias ypatingas Konvencijos taikymo sritis, kurioms priskiriamos ir viešosios institucijos.

Vėliau Europos Parlamentas ir Taryba priėmė keletą svarbių direktyvų - 95/46/EB, 2000/31/EB ir 2002/58/EB. **Direktyva 95/46/EB[9]** dėl asmenų apsaugos, tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Asmens duomenų apsaugos direktyva) buvo priimta 1995 m. spalio 24 d. Direktyvos 17 straipsnyje išdėstomi pagrindiniai reikalavimai asmens duomenų tvarkymo saugumui. Valstybės narės turi numatyti, „*kad duomenų valdytojas*

[5] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis//Valstybės Žinios, 2001, Nr. 32-1059.
[6] Convention for the protection of individuals with regard to automatic processing of personal data (ETS Np. 108), http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm; prisijungimo laikas: 2004-11-19.
[7] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis//Valstybės Žinios, 2001, Nr.: 32-1059.
[8] Ten pat.
[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23/11/1995.

privalo įgyvendinti tinkamas technines ir organizacines priemones, skirtas apsaugoti, kad asmens duomenys nebūtų netyčia ar neteisėtai sunaikinti ar netyčia prarasti, pakeisti, neleistinai atskleisti ar palikti prieinami, ypač, kai tvarkomus duomenis tenka perduoti tinklu, taip pat apsaugoti nuo bet kokių kitų neteisėtų tvarkymo būdų"[10].

Informacinės visuomenės paslaugų teikimas ir susijusi informacinės visuomenės paslaugų teikėjų veikla Europos Sąjungoje reglamentuojama kita svarbia 2000 m. birželio 8 d. Europos Parlamento ir Tarybos **direktyva 2000/31/EB**[11] dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektronines komercijos direktyva).

Direktyva Nr. 2002/58/EB[12] dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje buvo priimta 2002 m. liepos 12 d. Šios direktyvos ketvirtame straipsnyje „Saugumas" apibrėžiami du pagrindiniai reikalavimai informacijos saugumui. Tai, kad „*viešai prieinamų elektroninių ryšių paslaugų teikėjas turi imtis tinkamų techninių ir organizacinių priemonių, kad užtikrintų savo paslaugų saugumą, o tam tikrais atvejais tokių priemonių imasi kartu su viešųjų ryšių tinklo teikėju, kad užtikrintų ir paties tinklo saugumą. Atsižvelgiant į naujausius technikos laimėjimus bei jų įdiegimo kainą, šios priemonės užtikrina saugumo lygį, atitinkantį atsiradusiai rizikai"* ir, kad „*iškilus tam tikrai tinklo saugumo pažeidimo rizikai, viešai prieinamų elektroninių ryšių paslaugų teikėjas turi informuoti abonentus apie šią riziką, o tais atvejais, kai paslaugos teikėjo taikomos priemonės neapima šios rizikos – informuoti abonentus apie visas įmanomas teisės gynimo priemones, nurodant ir galimas jų kainas*"[13]. Ši direktyva pakeitė iki tol galiojusią **direktyvą Nr. 97/66/EB[14]** dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų sektoriuje.

---

[10] Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EC), Autentiškas vertimas, Europos komitetas prie LR Vyriausybės, Vertimo, dokumentacijos ir informacijos centras, http://www3.lrs.lt/c-bin/eu/preps2?Condition1=7879&Condition2=; prisijungimo laikas: 2004-11-19.

[11] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178/1, 08/06/2000.

[12] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37, 31/07/2002.

[13] Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), Autentiškas vertimas, Europos komitetas prie LR Vyriausybės, Vertimo, dokumentacijos ir informacijos centras, http://www3.lrs.lt/c-bin/eu/preps2?Condition1=36605&Condition2=; prisijungimo laikas: 2004-11-02.

[14] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24/1, 30/01/1998.

Europos Komisijos patvirtinto Veiksmų plano[15] 3.1.3. punkte „Saugi informacinė struktūra“ (*A secure information infrastructure*) numatomi trys pagrindiniai veiksmai:

1. sukurti kompiuterių saugumo greito reagavimo pajėgas (*Cyber security task force - CSTF*), kurios turėtų tapti kompetentingu informacijos saugumo centru;
2. iki 2005 m. pabaigos suprojektuoti ir įdiegti „saugumo kultūrą“ į informacijos ir komunikacijos gaminius, remti projektus ir dirbti, didinant visų vartotojų saugumo rizikų sąmoningumą;
3. iki 2003 m. pabaigos Komisija ir ES šalys turi išnagrinėti galimybę sukurti saugių ryšių aplinką keistis slapta vyriausybine informacija.

Europos Komisija, atsižvelgdama į tai, kad pastaruoju metu visi paslaugų tiekėjai ir užsakovai vis labiau atkreipia dėmesį į tai, kad transakcijų ir duomenų saugumas, teikiant e. paslaugas, įskaitant e. komerciją ir viešąsias e. paslaugas, tampa svarbiausia problema, pripažįsta saugumo svarbą bendrai, o tinklo ir informacijos saugumo ypatingai, ir suteikia šiai problemai spręsti aukščiausią prioritetą.

2003 m. lapkričio 17 d. Europos parlamentas ir Taryba pasirašė nutarimą Nr. 2256/2003/EB[16] dėl *eEurope* monitoringo, skleidžiant gerą praktiką ir gerinant tinklo ir informacijos saugumą. Šiame nutarime sakoma „*Interneto vartojimas per pastaruosius metus Europoje išaugo taip sparčiai, kad tampa aišku, jog tinklo ir informacijos saugumo užtikrinimas yra pagrindinis ekonomikos ir visuomenės plėtros veiksnys. Transakcijų ir duomenų saugumas užtikrinimas turi tapti būtina sąlyga, teikiant visas elektronines paslaugas, o tinklo prieinamumas yra ypatingai svarbus visai informacinių ir telekomunikacinių technologijų infrastruktūrai*“[17].

Šią MODINIS programą planuojama įgyvendinti 2003 – 2005 m. m. laikotarpyje ir jos įgyvendinimui planuojama skirti 25 mln. eurų. Pagal šią programą numatoma finansuoti specifinius tyrimus, studijas ir ekspertizes, siekiant sukaupti reikiamą patirtį tinklo ir informacijos saugumo srityje, pvz., saugumo mechanizmai ir jų operacinis suderinamumas, tinklo patikimumas ir apsauga, pažangi kriptografija, konfidencialumas, bevielio tinklo saugumas. Vienas centrinių programos elementų, sukurti ateityje Kompiuterių saugumo greito reagavimo pajėgas, kurios turėtų padėti šalims narėms spręsti tinklo ir informacijos saugumo

[15] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions „eEurope 2005: An information society for all“, COM(2002) 263 final, 28.5.2002.

[16] Decision No 2256/2003/EC of the European Parliament and of the Council of 17 November 2003 adopting a multi-annual programme (2003-2005) for the monitoring of the *e*Europe 2005 action plan, dissemination of good practices and the improvement of network and information security (MODINIS), OJ L 336, 23/12/2003.

problemas. Šalys kviečiamos šiuo klausimu pateikti Komisijai svarstyti savo pasiūlymus. Dėmesys veiksmams tinklo ir informacijos saugumo srityje bus fokusuojamas į šalių narių sąmoningumo lygio kėlimą, užtikrinant reikiamą tinklo ir informacijos saugumo lygį bei į informacijos apie saugumo rizikas kaupimą ir analizavimą.

Įgyvendinant Veiksmų planą, Europos Parlamento ir Tarybos 2004 m. kovo 10 d. nutarimu Nr. 460/2004[18] įkūrė Europos tinklo ir informacijos saugumo agentūrą ENISA (*European Network and Information Security Agency, http://www.enisa.eu.int*). Nutarime pažymima, kad „*komunikacijų tinklai ir informacinės sistemos tapo esminiu ekonomikos ir visuomenės plėtros faktoriumi, kad naudojimasis kompiuteriais ir komunikaciniais tinklais tapo visuotinai paplitęs, kaip elektros energijos ir vandens tiekimas. Komunikacinių tinklų ir informacinių sistemų saugumas, ypač savo prieinamumu, yra visuomenės padidinto susirūpinimo šaltinis, kadangi informacinių sistemų problemos, dėl jų sudėtingumo, avarijų, klaidų ir atakų, gali turėti skaudžius padarinius visai infrastruktūrai, kur paslaugų teikimas gali kelti grėsmę ES piliečių gerovei*"[19].

ENISA organizacijos tikslas - „*stiprinti Europos Sąjungos valstybių galią, užkertant kelią, atkreipiant dėmesį ir reaguojant į tinklo bei informacijos saugumo problemas*"[20]. Pagrindiniai uždaviniai - *„patarti ir pagelbėti Komisijai bei šalims narėms informacijos saugumo klausimais, dialogui su pramone, sprendžiant kompiuterinės ir programinės įrangos, skirtos saugumo užtikrinimui, kūrimo klausimus, kaupti ir analizuoti informaciją apie saugumo incidentus ir kylančias rizikas, skatinti rizikos įvertinimo ir jų valdymo metodų diegimą, didinant gebėjimą elgtis su informacijos saugumo grėsmėmis, bei kelti sąmoningumą ir bendradarbiavimą informacijos saugumo srityje*".[21]

Pažymima, kad didėjantis saugumo pažeidimų skaičius jau padarė žymius finansinius nuostolius, pakenkė vartotojų konfidencialumui ir buvo žalingas sėkmingai elektroninės komercijos plėtrai. Tačiau į tai pavieniai asmenys, viešosios administracijos ir verslas sureagavo pakankamai greitai, įdiegdamos į savo informacines sistemas reikiamas saugumo technologijas ir valdymo procedūras. ES šalys organizavo keletą informacinių kompanijų ir tyrimo projektų, siekdamos supažindinti visuomenę su tinklo ir informacijos saugumą grėsmėmis.

---

[17] Ten pat.
[18] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_077/l_07720040313en00010011.pdf; prisijungimo laikas: 2004-11-24.
[19] Ten pat.
[20] Ten pat.

1.2. PAGRINDINIAI LIETUVOS RESPUBLIKOS AKTAI, REGLAMENTUOJANTYS INFORMACIJOS SAUGUMĄ

2001 m. vasario 20 d. Lietuvos Respublika ratifikavo Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis[22].

1996 metais Lietuvoje priimamas asmens duomenų teisinės apsaugos įstatymas[23], o 2003 metais priimama nauja šio įstatymo redakcija[24]. Įstatymas suderintas su jau minėta Europos Sąjungos direktyva 95/46/EB, ir „*reglamentuoja santykius, kurie atsiranda tvarkant asmens duomenis automatiniu būdu, taip pat neautomatiniu būdu, tvarkant asmens duomenų susistemintas rinkmenas. ... Įstatymas nustato fizinių asmenų kaip duomenų subjektų teises, šių teisių apsaugos tvarką, juridinių ir fizinių asmenų teises, pareigas ir atsakomybę tvarkant asmens duomenis*“[25].

Lietuvos Respublikos elektroninių ryšių įstatymas[26] reglamentuoja *„visuomeninius santykius, susijusius su elektroninių ryšių paslaugomis, tinklais ir su jais susijusiomis priemonėmis bei paslaugomis, elektroninių ryšių išteklių naudojimu, taip pat visuomeninius santykius, susijusius su radijo įrenginiais, galiniais įrenginiais ir elektromagnetiniu suderinamumu*“[27].

Lietuvos Respublikos Vyriausybės nutarimu „Dėl duomenų saugos valstybės ir vietos savivaldos informacinėse sistemose“[28] buvo patvirtinti Bendrieji duomenų saugos reikalavimai, kurių pagrindinis tikslas „*sudaryti sąlygas saugiai tvarkyti automatizuotu būdu duomenis valstybės registruose ir kitose valstybės informacinėse sistemose*“[29]. Šiame nutarime rekomenduojama, diegiant informacijos saugumą valstybės institucijose, vadovautis tarptautiniais standartais ISO/IEC TR 13335, ISO 11442 ir ISO/IEC 17799:2002.

---

[21] Ten pat.
[22] Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis//Valstybės Žinios, 2001, Nr. 32-1059.
[23] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas//Valstybės Žinios, 1996, Nr. 63-1479.
[24] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas//Valstybės Žinios, 2003, Nr.: 15-597.
[25] Ten pat.
[26] Lietuvos Respublikos elektroninių ryšių įstatymas//Valstybės Žinios, 2004,Nr. 69-2382.
[27] Ten pat.
[28] Dėl duomenų saugos valstybės ir vietos savivaldos informacinėse sistemose//Valstybės Žinios, 1997, Nr. 83-2075; Valstybės Žinios, 2003, Nr. 2-45.
[29] Ten pat.

Kitame Lietuvos Respublikos Vyriausybės nutarime „Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo“[30] pateikiami pagrindiniai informacijos technologijų saugos valstybinės strategijos tikslai. Vienas iš tokių tikslų - plėtoti informacinių technologijų saugos teisinį reglamentavimą ir nustatyti e. verslo, kompiuterių tinklų, interneto tarnybinių stočių bei kitus saugumo reikalavimus.

2002 m. gruodžio 31 d. Lietuvos Respublikos Vyriausybė patvirtino Elektroninės valdžios koncepciją[31]. Koncepcijos skyriuje „Informacijos saugumas ir vartotojų tapatybės nustatymas” sakoma, kad „*e. valdžios projektai galės funkcionuoti, kai bus užtikrinta informacinių technologijų ir telekomunikacijų sauga, gyventojų interesų teisinė apsauga valstybės informacinėse sistemose”*[32]. Taip pat pabrėžiama, kad e. valdžios paslaugos turi būti teikiamos 24 valandas per parą ir 7 dienas per savaitę.

Ypač daug dėmesio informacijos saugumo problemoms skiriama pastaruoju metu. 2004 m. balandžio 19 d. Lietuvos Respublikos Vyriausybės priėmė nutarimą Nr. 451 „Dėl valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo"[33], kuriuo patvirtinamos valstybės informacinių sistemų steigimo ir įteisinimo taisyklės. Šių taisyklių 6 punktas nurodo, kad „*Informacinės sistemos steigėjas, teikdamas derinti informacinės sistemos nuostatų projektą Vidaus reikalų ministerijai, kartu turi pridėti informacinės sistemos duomenų saugos nuostatus, parengtus vadovaujantis Tipiniais duomenų saugos nuostatais*[34].“

2004 m. balandžio 28 d. vyriausybė patvirtino viešojo administravimo plėtros iki 2010 metų strategiją,[35] kurioje pažymima, kad „*viešąsias paslaugas būtų galima teikti internetu trečiuoju ir ketvirtuoju lygiu, reikia išspręsti fizinių ir juridinių asmenų identifikavimo valstybės informacinėse sistemose problemą, užtikrinti asmens duomenų teisinę apsaugą ir tai, kad administruojama viešoji paslauga būtų suteikiama tik tam asmeniui, kuriam ji skirta*“. Strategijoje pabrėžiama, kad viešosios paslaugos turi būti teikiamos naudojant tik saugias informacijos technologijas ir kad, viešųjų paslaugų teikimas naudojant informacijos technologijas ir šių technologijų sauga yra neatsiejami dalykai. Todėl, įgyvendinant informacijos technologijų saugos valstybinės strategijos įgyvendinimo planą, turi būti

[30] Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo//Valstybės Žinios, 2001, Nr. 110-4006.
[31] Elektroninės valdžios koncepcija//Valstybės žinios, 2003, Nr. 2-54.
[32] Ten pat.
[33] Dėl Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo//Valstybės Žinios, 2004, Nr. 58-2061.
[34] Dėl Tipinių duomenų saugos nuostatų patvirtinimo//Valstybės Žinios, 2003, Nr. 76 – 3511.
[35] Dėl Viešojo administravimo plėtros iki 2010 metų strategijos patvirtinimo//Valstybės Žinios, 2004, Nr. 69-2399.

tobulinamas informacijos technologijų saugos teisinis reglamentavimas, stiprinama svarbiausių valstybės informacinių sistemų sauga, ugdomi duomenų saugos įgaliotinių įgūdžiai ir užtikrinama IT saugos įgyvendinimo kontrolė.

Vidaus reikalų ministras savo įsakymais patvirtino visą eilę rekomendacijų ir nuostatų. Reikėtų paminėti Informacijos klasifikavimo pagal duomenų grupes rekomendaciją[36], Tipinius duomenų saugos nuostatus[37], Informacinių technologijų saugos atitikties vertinimo metodiką[38] ir Interneto tarnybinių stočių apsaugos rekomendacijas[39].

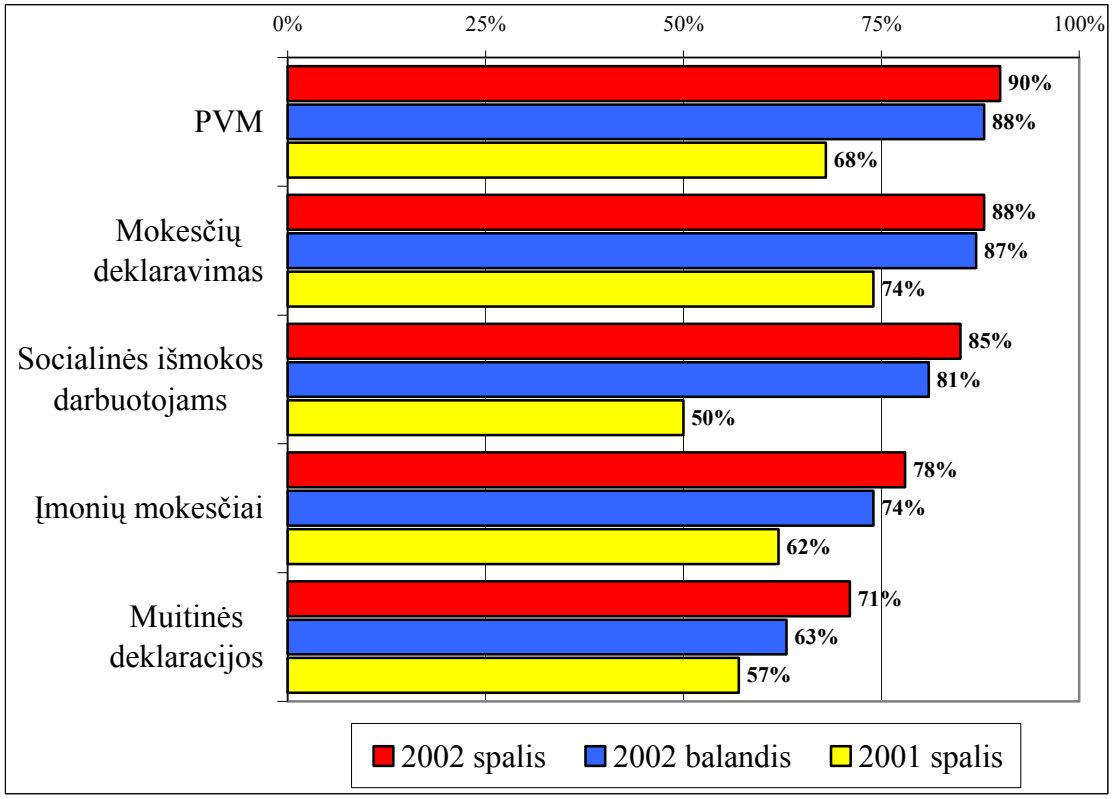
1.3. VIEŠŲJŲ E. PASLAUGŲ SAMPRATA

Įvertinus ES veiksmus, kuriais siekiama užtikrinti informacijos saugumą ir viešųjų paslaugų apibrėžimus, kuriuos pateikia Europos Parlamento ir Tarybos Elektroninės komercijos direktyva 2000/31/EB[40], Techninio reguliavimo ir standartų skaidrumo direktyva 98/48/EB[41], Lietuvos Respublikos viešojo administravimo įstatymas[42], Elektroninės valdžios koncepcija[43], Lietuvos Vyriausybės 2000 m. gruodžio 22 d. nutarimas Nr. 1482[44] suformuluojame e. viešosios paslaugos apibrėžimą - **tai paslauga, kuri suteikia asmeniui galimybę jo buvimo vietoje viešaisiais kompiuterių tinklais skaitmeniniu pavidalu atlikti jo poreikius tenkinančias įvairias procedūras ir gauti informaciją, užtikrinant apdorojamos informacijos konfidencialumą, vientisumą ir prieinamumą bei asmens ir verslo subjekto privatumą.**

Išskiriami trys pagrindiniai viešųjų e. paslaugų modeliai: vyriausybės paslaugos piliečiams (G2C), verslui (G2B) ir valdžios institucijoms(G2G). ES numatoma teikti dvylika viešųjų paslaugų gyventojams ir aštuonias viešąsias paslaugas verslui, kurios pagal savo pobūdį skirstomos į keturis klasteris: pajamų generavimo, registravimo, grįžtamumo ir licencijų –

[36] Dėl Informacijos klasifikavimo pagal duomenų grupes rekomendacijų patvirtinimo//Valstybės Žinios, 2003, Nr. 77-3541.
[37] Dėl Tipinių duomenų saugos nuostatų patvirtinimo//Valstybės Žinios, 2003, Nr. 76-3511.
[38] Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo//Valstybės Žinios, 2004, Nr. 80-2855.
[39] Dėl Interneto tarnybinių stočių apsaugos rekomendacijų patvirtinimo//Valstybės Žinios, 2004, Nr. 85-3095.
[40] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ, L 178, 17.7.2000.
[41] Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. OJ, L 217, 05.08.1998.
[42] Lietuvos Respublikos viešojo administravimo įstatymas//Valstybės Žinios, 1999, Nr. 60–1945.
[43] Elektroninės valdžios koncepcija//Valstybės žinios, 2003, Nr. 2-54.

leidimų. Kompanijos *Cap Gemini Ernst & Young* atliktas tyrimas[45] rodo, kad populiariausios ES, o kartu ir kiekvienai vyriausybei svarbiausios, yra pajamų generavimo klasteriui priskiriamos viešosios e. paslaugos, susijusios su piliečių (pajamų deklaravimas) ir verslo subjektų (įmonių mokesčiai, PVM, muitinės deklaracijos ir socialinės išmokos darbuotojams) mokesčių mokėjimu (1.1 pav.).



1.1 pav. Mokesčių generavimo klasterio paslaugų dinamika Europos šalyse.

Šio klasterio viešųjų e. paslaugų naudojimo vidurkis Europos šalyse siekia net 82 procentus. Trys iš šių paslaugų – pajamų deklaravimas, PVM ir įmonių mokesčiai, priskiriamos mokesčių inspekcijos veiklai. Kitų klasterių e. viešųjų paslaugų naudojimo vidurkis yra žymiai mažesnis: registravimo – 58 procentai, grįžtamumo – 53 procentai ir licencijų – leidimų 41 procentas.

Elektroniniu būdu teikiamos viešosios paslaugos gali būti ir skirtingo brandos lygio. Lietuvos elektroninės valdžios koncepcijoje viešosios e. paslaugos pagal jų brandą ir paslaugos

[44] Dėl Lietuvos Respublikos Vyriausybės 1999 m. gegužės 20 d. nutarimo Nr. 617 "Dėl keitimosi informacija apie standartus, techninius reglamentus ir atitikties įvertinimo procedūras" dalinio pakeitimo//Valstybės Žinios, 2000, Nr.: 111-3590.

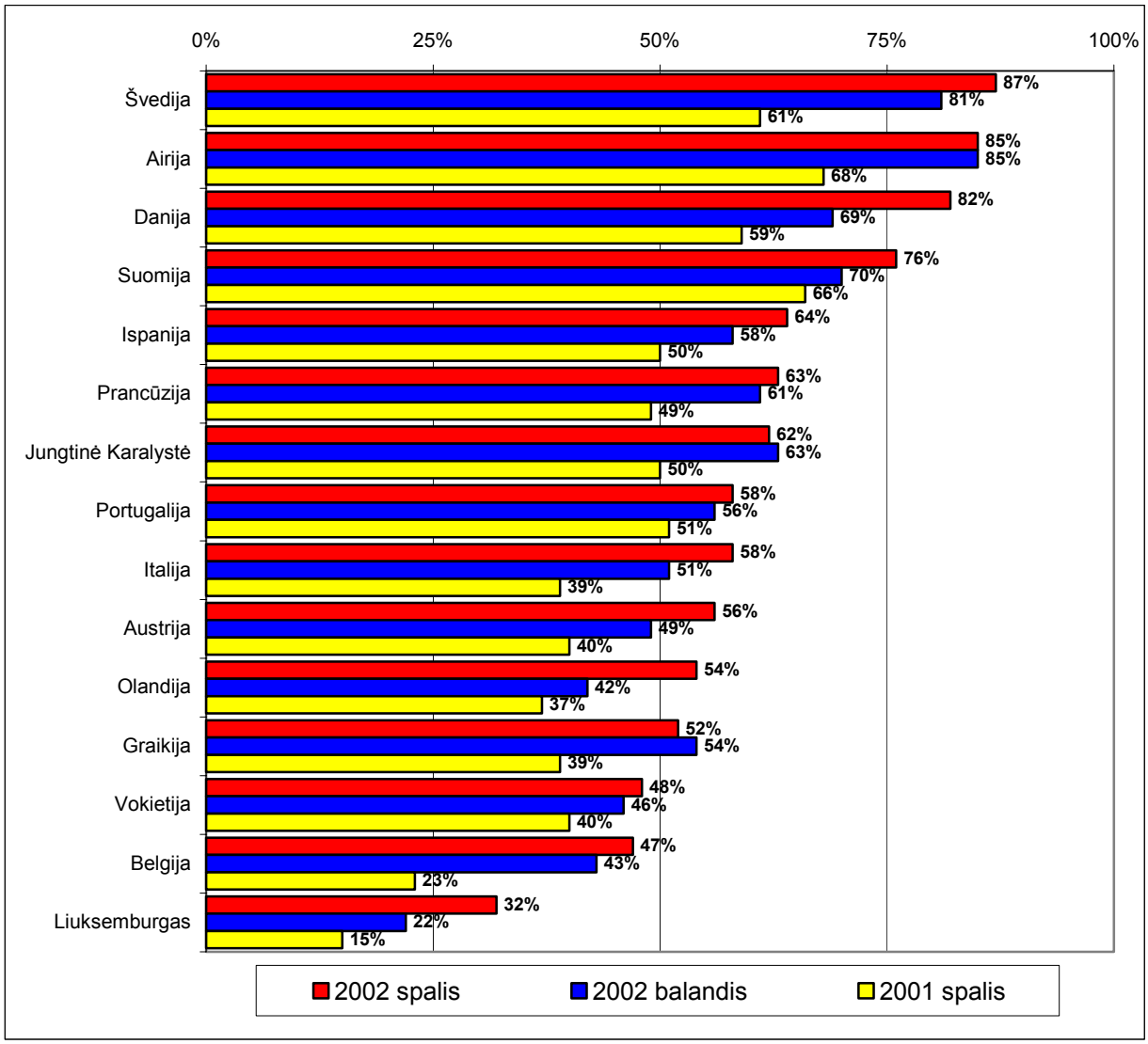
[45] Web-based Survey on Electronic Public Services: Results of the third measurement October 2002, Cap Gemini Ernst & Young, 2002; http://europa.eu.int/information_society/eeurope/2002/documents/CGEY-Report3rdMeasurement.pdf; prisijungimo laikas: 2004-12-14.

teikimo sudėtingumą, panašiai kaip ir Europos Sąjungos[46], skirstomos į keturis brandos lygius[47]. Viešųjų e. paslaugų modeliai turi būti rengiami nuosekliai, nuo žemesnio lygio ir laipsniškai, kūrimo eigoje, pereinant į aukštesnį lygį. Kiekvienas aukštesnis brandos lygis reikalauja ne tik sudėtingesnių informacinių sistemų naudojimo, bet ir kas ypač svarbu, didesnio šių paslaugų saugumo lygio, galinčio užtikrinanti pakankamą informacijos konfidencialumo, vientisumo ir prieinamumo lygį. Kiekviena valdžios institucija, atsižvelgdama į technologinių, organizacinių, finansinių prielaidų sukūrimo eigą, turi siekti gyventojams ir verslui teikti ketvirtojo lygio e. paslaugas. VMI teikiamoms e. paslaugoms, susijusioms su įvairių mokesčių mokėjimu ir turto deklaravimu, būtinas ketvirtasis brandos lygis.

1.4. VIEŠŲJŲ E. PASLAUGŲ POREIKIS

Europos Sąjungoje. Kompanijos *Cap Gemini Ernst & Young* atliktas viešųjų e. paslaugų trečiasis tyrimas[48] parodė, kad šių paslaugų teikimas gyventojams ir verslui aštuoniolikoje Europos valstybių 2002 metų pabaigoje vidutiniškai sudarė 60 procentus. Per vienerius metus (2001-2002) šių paslaugų teikimas vidutiniškai padidėjo 15 procentų. Lyginant trečiojo tyrimo rezultatus su antruoju, progresas stebimas 15 šalių. Kalbant apie kiekvieną Europos šalį atskirai, pats didžiausias viešųjų e. paslaugų teikimo lygis stebimas kaimyninėse Skandinavijos šalyse – Švedijoje (87%), Danijoje (82%) ir Suomijoje (76%). Šiose trijose šalyse ir Airijoje (85%) viešosios e. paslaugos sudaro daugiau kaip 75 procentus visų viešųjų paslaugų. 50 procentų ribą peržengė dar aštuonios valstybės, o tos kurios atsilieka, per metus padarė žymią pažangą - Liuksemburgas per vienerius metus sugebėjo viešųjų e. paslaugų sektorių padidinti daugiau negu dvigubai - nuo 15 iki 32 procentų, Belgija nuo 23 iki 47 procentų, Olandija nuo 37 iki 54 procentus ir tokiu savo šuoliu sugebėjo aplenkti Graikiją bei Vokietiją. Kiekvienos šalies padėtis viena kitos atžvilgiu nuolatos keičiasi. 2002 metų balandžio mėnesio lyderė Airija prarado turėtas pozicijas, per pusmetį šioje šalyje viešųjų e. paslaugų teikimas išliko nepakitęs, Graikijoje ir Jungtinėje Karalystėje e. viešųjų paslaugų teikimas keliais procentais sumažėjo (1.2 pav.).

[46] Web-based Survey on Electronic Public Services: Results of the third measurement October 2002, Cap Gemini Ernst & Young, 2002, http://europa.eu.int/information_society/eeurope/2002/documents/CGEY-Report3rdMeasurement.pdf; prisijungimo laikas: 2004-12-14.
[47] Elektroninės valdžios koncepcija//Valstybės žinios, 2003, Nr.: 2-54.
[48] Ten pat.

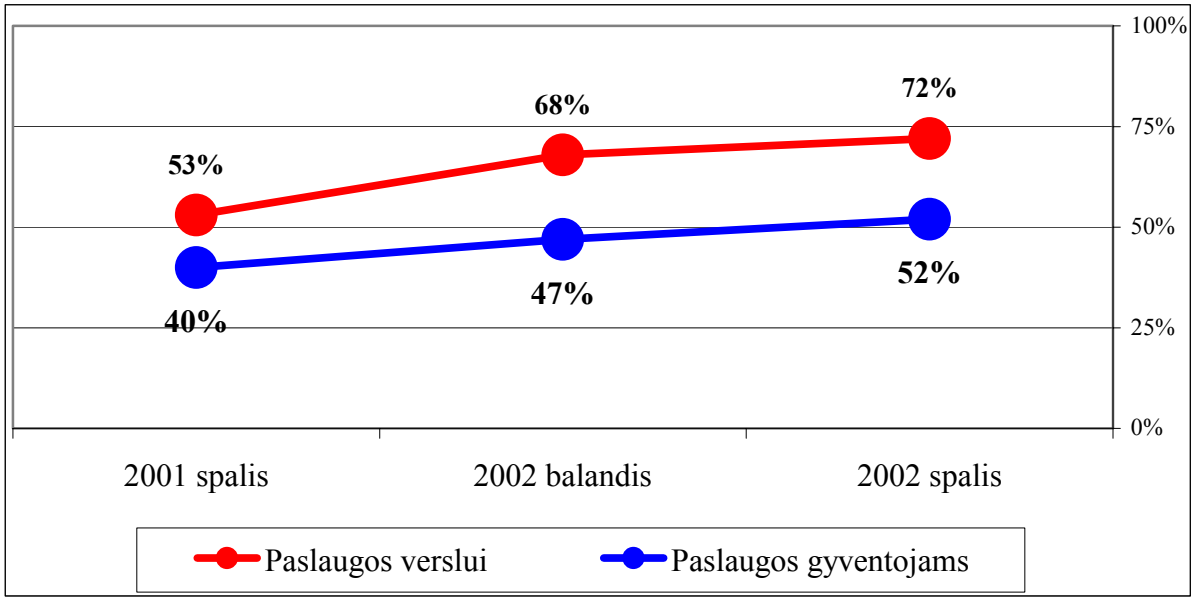


1.2 pav. Europos Sąjungos šalių išsidėstymas pagal e. viešųjų paslaugų teikimą.

Remiantis kompanijos *Cap Gemini Ernst & Young* tyrimo rezultatais galima konstatuoti, kad ES šalyse tarp viešųjų e. paslaugų gyventojams pačios populiariausios buvo pajamų deklaravimo ir laisvų darbo vietų paieškos paslaugos. Šias paslaugas 2002 m. pabaigoje pilnai teikė keturiolika ES šalių. Mažiau populiarios buvo leidinių paieškos bibliotekose, asmens duomenų, pranešimų policijai ir transporto priemonių registravimo paslaugos. Visiškai nepopuliarios buvo gydytojų konsultacijų paslaugos. Tik kelios valstybės (Ispanija, Portugalija ir Suomija) šios paslaugos pasiūla viršijo 20 procentų. Įdomu pastebėti, kad pranešimų policijai viešoji e. paslauga pilnai teikiama tik Jungtinėje Karalystėje, nors ši šalis, teikiant kitas e. paslaugas gyventojams, nepasižymi dideliu aktyvumu. Matomai, tai yra todėl, kad šioje šalyje (kaip ir Jungtinėse Valstijose) skiriamas labai didelis dėmesys gyventojų ir šalies

saugumo jausmui ugdyti. Tą patį būtų galima pasakyti ir apie šių šalių vyriausybių didelį dėmesį informacijos saugumui.

Kalbant apie viešąsias e. paslaugas verslui, to paties tyrimo duomenimis, pačios populiariausios buvo PVM, įmonių mokesčių ir socialinių išmokų darbuotojams viešosios e. paslaugos. Mažiausiai išvystytos buvo aplinkosauginių leidimų išdavimo paslaugos. Reikia pažymėti, kad viešosios e. paslaugos verslui populiaresnės negu gyventojams ir tas atotrūkis per vienerius metus dar labiau padidėjo (1.3 pav.).



1.3 pav. Viešųjų e. paslaugų verslui ir gyventojams pokytis.

Europos Komisijos prašymu kompanija *EOS Gallup Europe* 2002 m. gegužės – birželio mėn. penkiolikoje ES šalių atliko tyrimą *„Internet and the public at large"*[49]. Tyrimo tikslas - ištirti interneto naudojimo mastą visuomenėje. Telefoniniu būdu buvo apklausti 30 336 respondentai. Į vieną iš pateiktų klausimų respondentai turėjo atsakyti, kokiu tikslu naudodami internetą jie kreipiasi į viešąsias įstaigas. Apklausos rezultatai parodė, kad sparčiausiais tempais (+7%) per vienerius metus išaugo viešųjų e. paslaugų poreikis (1.4 pav.). Tokiomis paslaugomis naudojosi daugiau kaip ketvirtadalis (27 %) visų interneto vartotojų. Šiek tiek daugiau - 37 procentai interneto vartotojų kreipėsi į viešąsias įstaigas, norėdami surasti sau reikalingos informacijos. Beveik ketvirtadalis (23 %) vartotojų bendravimui su valdžios

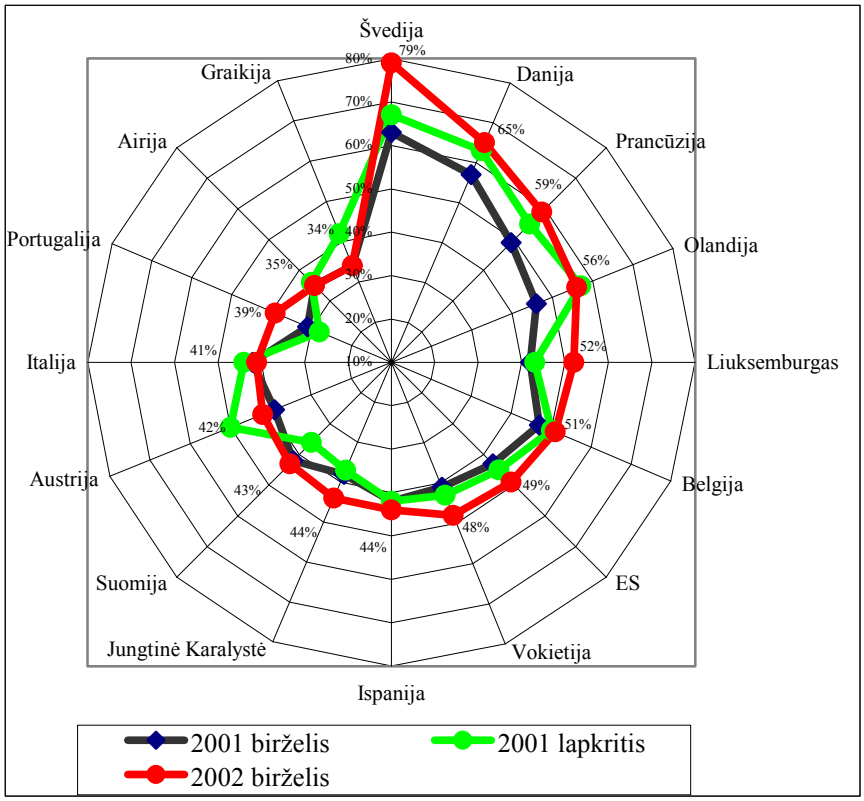
[49] Flash Eurobarometer 135: Internet and the Public at Large 6, EOS Gallup Europe, November 2002, http://europa.eu.int/information_society/eeurope/2002/benchmarking/list/source_data_pdf/report_eb125_en.pdf; prisijungimo laikas: 2004-12-14.

institucijomis naudojo elektroninį paštą. Tačiau beveik pusė (49 %) respondentų pareiškė, kad jie niekada nenaudoja interneto kreipimuisi į viešąsias įstaigas.

Interneto pagalba kreipiuosi į viešąsias įstaigas, norėdamas…	2001 birželis	2001 lapkritis	2002 birželis
… surasti viešą informaciją	33%	35%	37%
… nusiųsti e. paštą	18%	20%	23%
… užpildyti formas ar atlikti e. paslaugas	20%	22%	27%
… kitos priežastys	1%	1%	2%
… niekada nesijungia prie viešųjų įstaigų	55%	54%	49%

1.4 pav. Kokiu tikslu interneto vartotojai kreipiasi į viešąsias įstaigas.

Pagal interneto naudojimą viešosioms paslaugos gauti pirmauja Skandinavijos šalys Švedija ir Danija. Didžiausias interneto naudojimo pokytis, kreipiantis į viešąsias įstaigas, stebimas Švedijoje (+12%), Portugalijoje (+11%), Olandijoje ir Liuksemburge (po +9%) (1.5 pav.). Švedija pirmauja visose srityse: ieškant viešosios informacijos (64%), naudojantis viešosiomis e. paslaugomis (53%) ir siunčiant elektroninį paštą (57%) (procentai nurodyti nuo apklaustų šalies gyventojų).



1.5 pav. Interneto naudojimas viešosioms paslaugoms gauti ES šalyse.

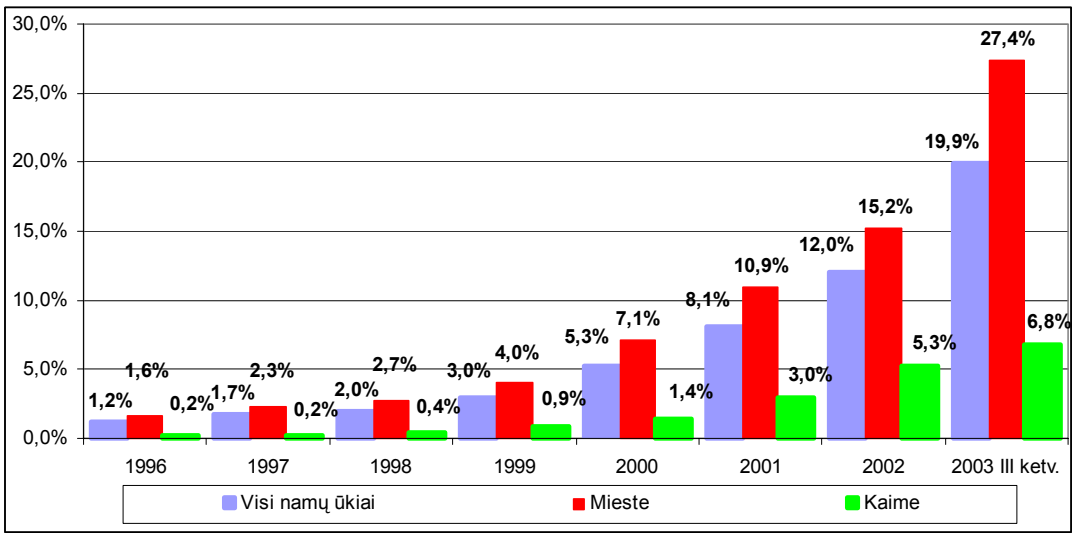
Šis tyrimas parodė, kad kai kuriose šalyse stebimas tam tikras sezoniškumas - kreipimasis per internetą į viešąsias įstaigas sumažėjo 2002 m. lapkričio mėnesį, pvz., Austrijoje ir

Graikijoje nukrito net 9%. Nors 2001 m. ir 2002 m. birželio mėnesį stebimi labai panašūs rezultatai: Austrijoje atitinkamai 39% ir 42% (padidėjimas 3% per metus), o Graikijoje išliko toks pats - 34%.

Lietuvoje. Lietuva viešųjų e. paslaugų srityje žengia pirmuosius žingsnius. Šių paslaugų teikimo tempas padidėjo 2004 metų, Lietuvai tapus ES nare. Nustatant e. viešųjų paslaugų poreikį Lietuvoje, reikia atsižvelgti ne tik į ES, bet ir įvertinti visą eilę svarbių faktorių, nusakančių visuomeninę naudą. Išskiriami tokie viešųjų e. paslaugų visuomeninės naudos matavimo rodikliai[50]:

1. segmento, kuris naudosis paslauga, dydis;
2. segmento, kuris turi galimybę gauti paslaugą elektroniniu būdu, dalis;
3. paslaugos naudojimosi dažnumas;
4. paslaugos teikimo ir gavimo kaštų pokytis, pradėjus ją teikti elektroniniu būdu;
5. valstybės politikos prioritetai;
6. valstybės prestižo prioritetai.

Statistikos departamento prie Lietuvos Respublikos Vyriausybės kartu su Danijos statistikos tarnyba 2004 m. pateikta ataskaita „Informacinės technologijos“[51] parodo, kad namų ūkio apsirūpinimas personaliniais kompiuteriais Lietuvoje ypač padidėjo per paskutiniuosius tris metus. Jeigu 1996 m. namuose kompiuterį turėjo tik vienas iš šimto namų ūkių, tai 2003 m. trečiąjį ketvirtį jau kas penktas – mieste virš 27 procentų, o kaime beveik 7 procentus (1.6 pav.).



[50] Lietuvos valstybės institucijų bei įmonių ir kitų įstaigų elektroninių viešųjų paslaugų, teikiamų viešaisiais kompiuterių tinklais svarbiausių paslaugų procedūrų tyrimas ir paslaugų teikimo galimybių analizė, IVPK, 2001. //http://www.ivpk.lt/dokumentai/el-paslaugos.pdf; prisijungimo laikas: 2004-11-14.

[51] Informacinės technologijos. Statistikos departamento prie Lietuvos Respublikos Vyriausybės, Vilnius, 2004.

1.6 pav. Namų ūkio aprūpinimas asmeniniais kompiuteriais.

Penkiuose didžiausiuose šalies miestuose vidutiniškai kompiuterius turėjo kas trečias namų ūkis. Internetu 2003 m. III ketvirtį naudojosi 7,7 procentai namų ūkių. Jeigu miestuose internetu naudojosi beveik kas aštuntas (didžiuosiuose miestuose kas šeštas) namų ūkis, tai kaimuose tik vienas iš šimto (0,8%). Beveik pusė (47%) namų ūkių nesinaudojančių internetu nurodė, kad internetas jiems nereikalingas. Kitos priežastys, dėl kurių namuose nenaudojamas internetas – brangi įranga, dideli paslaugų tarifai, galimybė naudotis internetu kitus, reikiamų žinių stoka.

Kompiuteriu naudojosi 39 procentai visų 15-74 metų amžiaus asmenų. Didelė dalis besinaudojančių - jauni žmonės, kurie sudaro 80 procentų 15-24 amžiaus asmenų. Tarp 65-74 metų amžiaus apklaustųjų kompiuteriu naudojosi tik 2 procentai. Daugiau kaip pusė (53%) visų apklaustųjų, besinaudojančių kompiuteriu, naudojosi juo kasdien ir daugiau kaip trečdalis (37%) naudojosi juo bent kartą per savaitę. Kasdien kompiuteriu naudojasi dirbantys, o kartą per savaitę besimokantys asmenys.

Internetu naudojosi 27 procentai visų 15-74 metų amžiaus asmenų. Populiariausias internetas mokinių ir studentų tarpe. Juo naudojosi 78 procentai visų šios grupės apklaustųjų. Šiek tiek mažesnis procentas jaunų žmonių, besinaudojančių internetu, buvo užfiksuota prieš keletą metų kompanijos SIC Rinkos Tyrimai (*Taylor Nelson Sofres Interactive*)[52] atliktų tyrimų metu. Tada 71 procentas jaunesnių kaip 34 m. respondentų naudojosi internetu.

Dauguma asmenų naudojosi internetu reguliariai, bent vieną kartą per savaitę. Dažniausiai internetas buvo naudojamas informacijos paieškai ir ryšiams. 2003 m. vis dažniau internete ieškoma informacijos apie prekes ir paslaugas, atliekamos bankinės operacijos. Pagrindinės priežastys kodėl Lietuvos gyventojai nesinaudojo e. prekybos paslaugomis buvo: nebuvo tam reikalo (76%), parduotuvėje, matant prekę, patogiau (33%), nepasitiki (14%), per brangus prekės pristatymas ir nesaugus apmokėjimas (reikia kreditinės kortelės duomenų) (po 7%).

Dažniausiai internetas naudojamas ryšiams ir informacijos paieškai (1.7 pav.). Elektroniniu paštu naudojosi daugiau kaip du trečdaliai (71%) respondentų, beveik tiek pat (73%) skaitė laikraščius ir žurnalus ir naudojosi paslaugomis susijusiomis su švietimu ir mokymu (64%). Beveik pusė respondentų žaidė arba siuntėsi žaidimus ir muzikos įrašus (49%) ir ieškojo informacijos apie paslaugas bei prekes (48%). Trečdalis respondentų (30%) interneto

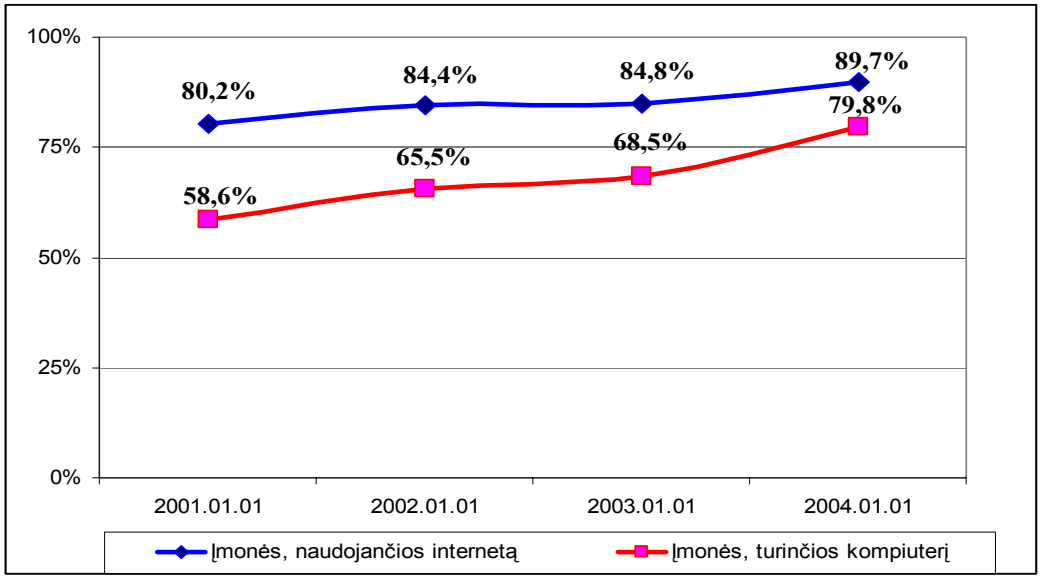
[52] Lietuvos valstybės institucijų bei įmonių ir kitų įstaigų elektroninių viešųjų paslaugų, teikiamų viešaisiais kompiuterių tinklais svarbiausių paslaugų procedūrų tyrimas ir paslaugų teikimo galimybių analizė, IVPK, 2001.//http://www.ivpk.lt/dokumentai/el-paslaugos.pdf; prisijungimo laikas: 2004-11-24.

vartotojų siuntėsi informaciją iš valstybės institucijų. Tai beveik tiek pat (37%) kiek buvo užfiksuota ir *EOS Gallup Europe* 2002 m. tyrimo *„Internet and the public at large"*[53] metu.

	Visi 15-74
Ryšiams	
siuntė/gavo elektroninius laiškus	71
skambino naudodamiesi internetu, vaizdo konferencijos	4
kita (pvz., pokalbių svetainės)	39
Informacijos paieškai ir tiesioginėms paslaugoms	
ieškojo informacijos apie prekes ir paslaugas	48
naudojosi paslaugomis, susijusiomis su kelionėmis ir apgyvendinimu	19
naudojosi paslaugomis, susijusiomis su švietimu ir mokymu	64
naudojosi paslaugomis, susijusiomis su sveikatos priežiūra	17
klausėsi radijo, žiūrėjo TV programas	29
žaidė, siuntėsi žaidimus ar muzikos įrašus	49
skaitė, siuntėsi laikraščius, žurnalus	73
Prekėms ir paslaugoms pirkti (užsakyti), banko operacijoms atlikti	
atliko bankines operacijas	20
atliko kitas finansines operacijas	3
pirko, užsakė prekes ar paslaugas	4
pardavė prekes ar paslaugas	2
Bendrauti su valstybės institucijomis	
siuntėsi informaciją iš valstybės institucijų svetainių	30
siuntėsi oficialius blankus	15
pildė, siuntė užpildytus blankus	14

1.7 pav. Interneto naudojimo tikslai 2003 m. III ketvirtį.

2004 m. pradžioje 89,7 procentai Lietuvos verslo įmonių naudojosi kompiuteriais, o 79,8 procento internetu (1.8 pav.).



1.8 pav. Kompiuterių ir interneto naudojimas įmonėse.

[53] Flash Eurobarometer 135: Internet and the Public at Large 6, EOS Gallup Europe, November 2002, http://europa.eu.int/information_society/eeurope/2002/benchmarking/list/source_data_pdf/report_eb125_en.pdf; prisijungimo laikas: 2004-11-10.

Daugiausia (99,7%) kompiuteriais naudoja didžiosios, turinčios virš 500 darbuotojų, įmonės, o mažiausia (51,9%) smulkiosios, turinčios iki 50 darbuotojų įmonės. Daugiau kaip pusė (51,9%) įmonių prie interneto jungėsi per skaitmenines (xDSL), trečdalis (30,3%) per komutuojamas ryšio linijas ir tik viena iš septynių (14,6%) naudojosi bevieliu ryšiu. Beveik visos (99,3%) stambiosios įmonės ir devynios iš dešimties (91,6%) vidutinio dydžio įmonių buvo prisijungusios prie interneto. Trys ketvirtadaliai smulkių įmonių taip pat naudojosi internetu.

38,6 procento apdirbamosios gamybos ir paslaugų įmonių turėjo savo interneto puslapius. Vien per 2003 m. interneto puslapius turinčių įmonių skaičius išaugo beveik 7 procentiniais punktais. Daugiau kaip du trečdaliai (69,2%) įmonių naudodamosi internetu atliko banko ir finansinius pavedimus ir tai net 27 procentais daugiau nei prieš metus. Dauguma įmonių internetu prekiavo su kitomis verslo įmonėmis (89,2%), kurių didžioji dauguma buvo Lietuvoje. Tačiau beveik trečdalis (30,5%) įmonių pardavė prekes internetu ES šalių pirkėjams, o ketvirtadalis (23,8%) jų – kitoms šalims.

Beveik du trečdaliai įmonių nurodė, kad naudoja internetą savo darbuotojų švietimui ir mokymui, daugiau kaip pusė – rinkos kontrolei (1.9 pav.). Aštuonios iš dešimties įmonių siekė gauti informacijos iš valstybės institucijų. Iš jų 78 procentai ieškojo informacijos, 75,3 procento parsisiuntė oficialias formas, kurias 2003 metais reikėjo pildyti. Daugiau kaip trečdalis (38,1%) įmonių užpildytas formas pateikia tiesiogiai internetu ir tik viena iš šešiolikos (5,9%) įmonių su valstybės institucijomis bendravo visiškai interaktyviame tinkle.

	Iš viso	Darbuotojų skaičius		
		0-49	50-249	250+
Švietimui ir mokymui	59,4	58,5	61,2	65,3
Rinkos kontrolei	51,6	50,7	52,6	61,1
Skaitmeniniams produktams gauti	23,5	20,1	30,0	49,8
Garantinėms paslaugoms	8,2	7,3	9,4	17,2
Kontaktams su valstybinėms institucijomis:	80,7	78,2	86,8	91,9
Informacijos gavimui	78,0	75,2	84,7	91,2
Formų parsisiuntimui	75,3	72,4	82,3	90,2
Formų grąžinimui	38,1	33,6	46,5	73,0
Bendravimui tiesiogiai internetu	5,9	5,0	8,0	10,9
Atliko mokėjimus tiesiogiai internetu	7,2	7,2	7,3	7,0
Pirko prekes ar paslaugas specializuotose interneto prekybos vietose	3,5	3,3	3,8	6,7

1.9 pav. Interneto naudojimo tikslai 2004 m. pradžioje.

2004 m. sausio 1 d. duomenimis valstybės ir savivaldybių valdymo įstaigose 100-ui darbuotojų teko 53,2 kompiuterio ir tai 7,5 kompiuterio daugiau negu prieš metus (1.10 pav.).

Kompiuterius savo darbe naudojo 67,5 procento visų valstybės ir savivaldybių valdymo įstaigų darbuotojų (2003 m. – 61,6%). 2004 m. pradžioje 88,4 procento valstybės ir savivaldybių valdymo įstaigų turėjo vietinius kompiuterių tinklus, 56,9 procento – interneto puslapius. 2004 m. pradžioje viešąsias e. paslaugas teikė 36,4 procento valstybės ir savivaldybių valdymo įstaigų arba 65,0 procento įstaigų, turinčių interneto svetaines. 49,2 procentai viešųjų paslaugų buvo teikiamos internetu ir viešosiomis e. paslaugomis naudojosi 11 procentų šalies gyventojų (2003 m. spalio mėn. – 6%).

	Institucijų, turinčių interneto svetaines, dalis		Institucijų, teikiančių paslaugas internetu, dalis	
	2003	2004	2003	2004
Iš viso	**53,7**	**56,9**	**33,5**	**37,0**
LR Prezidentūra	100,0	100,0	-	100,0
LR Seimas ir jam atskaitingos institucijos	100,0	93,3	78,6	60,0
LR Vyriausybė ir jam atskaitingos institucijos	77,8	94,4	66,7	66,7
Ministerijos ir joms atskaitingos institucijos	71,2	83,9	48,6	52,7
Apskričių administracijos	100,0	100,0	50,0	60,0
Miestų ir rajonų savivaldybės	82,4	91,7	45,0	53,3
Teismai	12,5	12,7	2,8	12,5
Policijos komisariatai	6,7	8,3	3,3	8,3
Muitinės	57,1	100,0	28,6	50,0
Įkalinimo įstaigos	-	18,2	-	-

1.10 pav. Interneto svetainių skaičius ir e. viešųjų paslaugų teikimas valstybės ir savivaldybių institucijose.

Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės (IVPK) užsakymu UAB „*Siemens*" 2004 m. pradžioje parengė studiją „E viešųjų paslaugų modelis“[54]. Vienoje iš ataskaitų „Viešųjų paslaugų teikimo esamos būklės analizė ir modelio aprašymas“, pagal nustatytą metodiką, įvertinus visų 20 viešųjų paslaugų pasiekiamumo vidurkį (procentais), buvo paskaičiuotas bendras viešųjų paslaugų, pasiekiamų internetu, rodiklis, kuris tam momentui sudarė **47,5 %**. Šio tyrimo organizatoriai padarė išvadą, kad iki 2004 m. interneto svetainėse daugiausia buvo galima parsisiųsti ar atsispausdinti pritaikytas formas, reikalingas pradėti paslaugos gavimo procedūrą. II brandos lygio paslaugos sudarė 40% visų e. viešųjų paslaugų. Pastebimas ir teigiamas poslinkis link trečio brandos lygio, kurios

[54] Viešųjų paslaugų teikimo esamos būklės analizė ir modelio aprašymas, IVPK, 2004 //http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_esamasV1.pdf; prisijungimo laikas: 2004-11-14.

sudaro 25 % visų viešųjų e. paslaugų. Verslui, kaip ir ES šalyse, skiriamas didesnis dėmesys. Viešųjų e. paslaugų piliečiams rodiklis - **45,83%**, o verslui - **50%**.

1.5. TEISINĖS PRIELAIDOS VIEŠŲJŲ E. PASLAUGŲ TEIKIMUI VMI

Nuo 2004 m. gegužės 1 d. įsigaliojęs naujos redakcijos Lietuvos Respublikos Mokesčių administravimo įstatymas[55] tiesiogiai nesudaro kliūčių elektroninių viešųjų paslaugų modelio diegimui. Šio įstatymo 57 straipsnis netgi sudaro teisines prielaidas deklaracijų pateikimui elektroniniu būdu: „*šio Įstatymo nurodytais atvejais, taip pat centrinio mokesčių administratoriaus nustatytais kitais atvejais ir tvarka, mokesčio deklaracija gali būti pateikta elektroniniu būdu*."

Įstatymo 75 straipsnio 2 ir 3 dalyse numatyta, kad „*šio Įstatymo nurodytais atvejais, taip pat centrinio mokesčių administratoriaus nustatytais kitais atvejais ir tvarka mokesčio deklaracija gali būti pateikta elektroniniu būdu*", bei „*mokesčių mokėtojas turi teisę pasirinkti mokesčio deklaracijos pateikimo būdą*". Taigi, įstatyme formuojamas funkcinis požiūris tiek į deklaracijos pateikimą, tiek ir į deklaruotojo asmens tapatybės patvirtinimą. Nėra apsiribojama kokia nors konkrečia technologija ar autentifikavimo / identifikavimo priemone.

1996 m. gegužės 16 d. Lietuvos Respublikos įstatymas dėl Lietuvos Respublikos gyventojų turto deklaravimo (Nr. I-1338)[56] nenumato turto ir pajamų deklaracijos pateikimo elektronine forma. Tačiau įgyvendinus visuotinį turto ir pajamų deklaravimą turėtų būti įdiegtos deklaracijų duomenų automatizuoto suvedimo bei apdorojimo technologijos - elektroninio dokumento ir elektroninio parašo naudojimo infrastruktūra.

Įgyvendinant Lietuvos Respublikos vienkartinio gyventojų turto deklaravimo įstatymą[57] VMI viršininko 2004 m. vasario 27 d. įsakymu VA-25[58] patvirtintos vienkartinės gyventojo (šeimos) turto deklaracijos formos ir jos užpildymo, teikimo ir tikslinimo taisykles. Šioje tvarkoje numatoma, kad įgyvendinus Lietuvos Respublikos elektroninio parašo įstatymo[59] nuostatas, deklaracijas bus galima pateikti nustatyta tvarka ir elektroniniu būdu, t.y. buvo nuspręsta, vienkartiniam deklaravimui naudoti aukščiausią autentiškumo ir patikimumo laipsnį.

---

[55] Lietuvos Respublikos mokesčių administravimo įstatymas//Valstybės Žinios, 2004, Nr. 63-2243.
[56] Lietuvos Respublikos gyventojų turto deklaravimo įstatymas//Valstybės Žinios, 1996, Nr. 50-1197, Valstybės Žinios, 2003, Nr. 123-5583.
[57] Lietuvos Respublikos vienkartinio gyventojų turto deklaravimo įstatymas//Valstybės Žinios, 2003, Nr. 123-5582.
[58] Dėl Vienkartinės gyventojo (šeimos) turto deklaracijos formos ir jos užpildymo, teikimo ir tikslinimo taisyklių patvirtinimo//Valstybės Žinios, 2004, Nr. 37-1214.
[59] Lietuvos Respublikos elektroninio parašo įstatymas//Valstybės Žinios, 2000, Nr. 61-1827.

Mokesčių mokėtojų registravimo taisyklių ir registro pildymo[60] ir pridėtinės vertės mokesčių mokėtojų registravimo[61] tvarkose nenumatomas registravimo paslaugos inicijavimas elektroniniu būdu, nes manoma, kad yra galimybė juridinio asmens registravimo duomenis gauti iš viešojo juridinių asmenų registro, o fizinio asmens – iš Lietuvos Respublikos Gyventojų registro, ir tokiu būdu turėtų būti sudaryta galimybė mokesčių mokėtojui užsiregistruoti ir elektroniniu būdu. Autentiškumo nustatymo metodo pavyzdžiu galėtų tapti tvarka, nustatyta VMI viršininko 2004 m. kovo 10 d. įsakymu Nr. VA-33[62], kuri siūlo, esant aukštesniam autentiškumo nustatymo patikimumo lygmens poreikiui, svarstyti II lygmens elektroninę paslaugą –registracijos formas atsiųsti elektroniniu būdu. Remiantis 2004 m. kovo 10 d. VMI viršininko įsakymu Nr. VA-33 elektroniniu būdu gali būti pateikiamos metinės gyventojų pajamų mokesčio ir metinės gyventojo (šeimos) turto deklaracijos bei prašymas pervesti iki 2 procentų pajamų mokesčio sumos Lietuvos vienetams, pagal Lietuvos Respublikos labdaros ir paramos įstatymą turintiems teisę gauti paramą. Šis įsakymas turi būti vertintinas itin palankiai, nes sukuria palankias prielaidas visiškam, t.y., ketvirtojo brandos lygio elektroninės paslaugos teikimui.

1.6. VIEŠŲJŲ E. PASLAUGŲ TEIKIMAS VMI

Remiantis IVPK parengto „Viešųjų paslaugų teikimo esamos būklės analizė ir modelio aprašymo"[63] medžiaga, Valstybinei mokesčių inspekcijai rekomenduojama imtis šių žemiau išvardintų jos kompetencijai priskiriamų viešųjų paslaugų:

E. viešosios paslaugos gyventojams	E. viešosios paslaugos verslui
Metinis pajamų mokesčio deklaravimas	Mokesčių mokėtojo registravimas
Asmens turto deklaravimas	Mokesčių deklaracijų pateikimas
Brangų turtą įsigijusių arba įsigyjančių Lietuvos Respublikos gyventojų pajamų deklaravimas	Pažymos apie atsiskaitymą su biudžetu pateikimas
	Duomenų mokesčių inspekcijai pateikimas
	Informacijos apie mokesčių mokėjimo balansą pateikimas
	PVM mokėtojo registravimas
	PVM deklaravimas

Kompanija „*SIC Rinkos Tyrimai*" atliktų tyrimų metu[64] paskaičiavo, kad jeigu Lietuvos piliečių, turinčių deklaruoti pajamas, būtų 2,7 mln., ir kiekvienai deklaracijai užpildyti bei

[60] Dėl Mokesčio mokėtojų registravimo taisyklių ir registro pildymo tvarkos patvirtinimo//Valstybės Žinios, 1996, Nr. 66-1591, Valstybės Žinios, 1996, Nr. 67.
[61] Dėl Pridėtinės vertės mokesčio mokėtojų registravimo//Valstybės Žinios, 2004, Nr. 29-946.
[62] Dėl Gyventojų deklaracijų ir prašymų formų teikimo elektroniniu būdu//Valstybės Žinios, 2004, Nr. 40-1319.
[63] Viešųjų paslaugų teikimo esamos būklės analizė ir modelio aprašymas, IVPK, 2004 //http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_esamasV1.pdf; prisijungimo laikas: 2004-11-24.

pateikti, įvairioms pažymoms surinkti vidutiniškai jie sugaištų 8 darbo valandas ir įvertinant tai, kad jie vidutiniškai per valandą sukuria 17,88 Lt vertės produktą, tai šie žmonės per šį laiką galėtų sukurti 386,2 mln. Lt vertės produktą, Tai pakankamai įspūdingas skaičius, kad elektroninis deklaravimas pasiteisintų.

IVPK parengto tyrimo „Viešųjų paslaugų teikimo esamos būklės analizė ir modelio aprašymas" duomenimis VMI 2004 m. pradžioje teikė dvi antro brandos lygio paslaugas verslo subjektams (Įmonių mokesčiai ir Pridėtinės vertės mokesčiai) ir vieną trečio lygio paslaugą gyventojams (Pajamų deklaravimas). Įgyvendinant Lietuvos Respublikos gyventojų turto deklaravimo įstatymą[65] nuo 2004 m. kovo mėn. pradėjo veikti VMI Elektroninio deklaravimo sistema (EDS). Pasinaudodami sistemos Gyventojų pajamų deklaravimo moduliu, gyventojai galėjo elektroniniu būdu pateikti VMI metines pajamų ir gyventojų (šeimos) turto deklaracijas. Pateikta deklaracija turi tokią pat juridinę galią, kaip to paties gyventojo pasirašyta ir įprasta tvarka pateikta deklaracija, t.y. gyventojas sėkmingai pateikęs deklaraciją elektroniniu būdu, neturi šios deklaracijos teikti popieriniame variante.

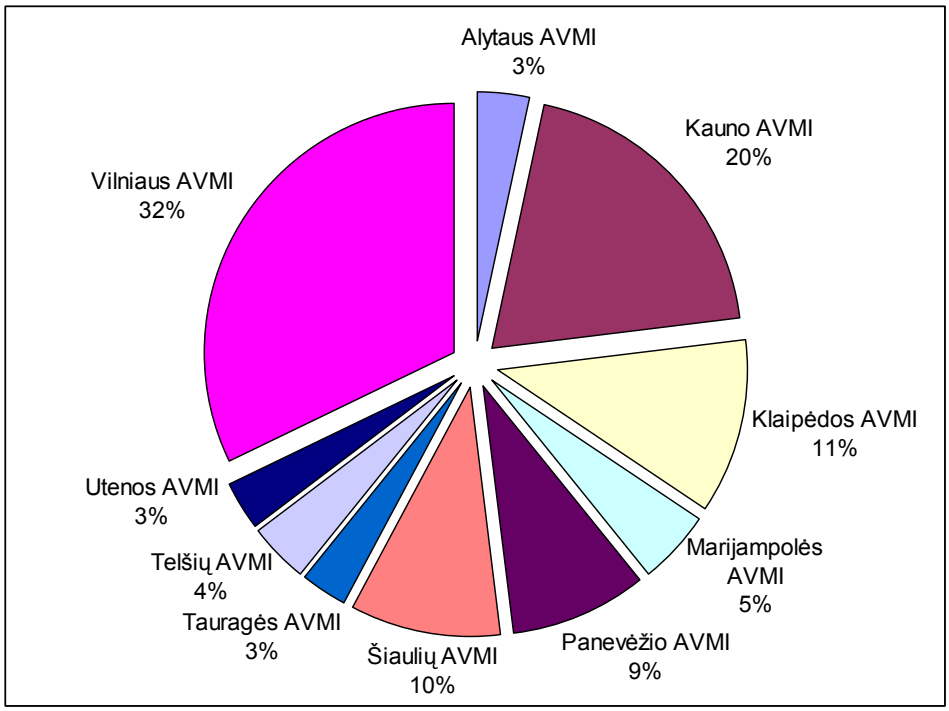
Kiekvienas asmuo, norėdamas pateikti deklaracijas elektroniniu būdu, turi sudaryti gyventojo deklaracijų ir prašymų formų teikimo elektroniniu būdu sutartį ir tapti EDS vartotoju. Ši sutartis gali būti sudaroma dviem būdais. Pirmasis būdas, kai asmuo pats atvyksta į VMI ir raštu sudaro sutartį, ir antrasis būdas, kai asmuo, būdamas interneto bankininkystės paslaugų vartotojas, gali sutartį pasirašyti elektroniniu būdu per komercinius bankus, su kuriais VMI yra pasirašiusi autentifikavimo duomenų teikimo sutartis. Tai reikalinga tam, kad asmuo pateikiantis deklaracijų būtų identifikuotas ir tokiu būdu būtų galima užtikrinti pateikiamos informacijos tikrumą, t.y. asmuo, teikdamas deklaraciją elektroniniu būdu, turi naudoti tik jam suteiktą EDS vartotojo vardą, prisijungimo ir darbo sesijos slaptažodžius arba asmens turimus pasirinkto komercinio banko interneto bankininkystės paslaugų vartotojo identifikacinius kodus, slaptažodžius ir pan.

Lietuvos piliečiai, kurie pasinaudojo šia paslauga turėjo pajusti jos privalumus – deklaraciją buvo galima pildyti ir pateikti bet kuriuo paros metu, nereikėjo vykti į apskrities VMI teritorinį skyrių, gaišti laiko, laukiant eilėje. Jeigu deklaruojantysis yra internetinės

[64] Lietuvos valstybės institucijų bei įmonių ir kitų įstaigų elektroninių viešųjų paslaugų, teikiamų viešaisiais kompiuterių tinklais svarbiausių paslaugų procedūrų tyrimas ir paslaugų teikimo galimybių analizė, IVPK, 2001.//http://www.ivpk.lt/dokumentai/el-paslaugos.pdf; prisijungimo laikas: 2004-11-22.
[65] Lietuvos Respublikos gyventojų turto deklaravimo įstatymą//Valstybės Žinios, 2003, Nr. 123-5583.

bankininkystės vartotojas, jam nereikėjo vykti į mokesčių inspekciją netgi vartotojo registracijai, sutartį su VMI galėjo sudaryti elektroniniu būdu.

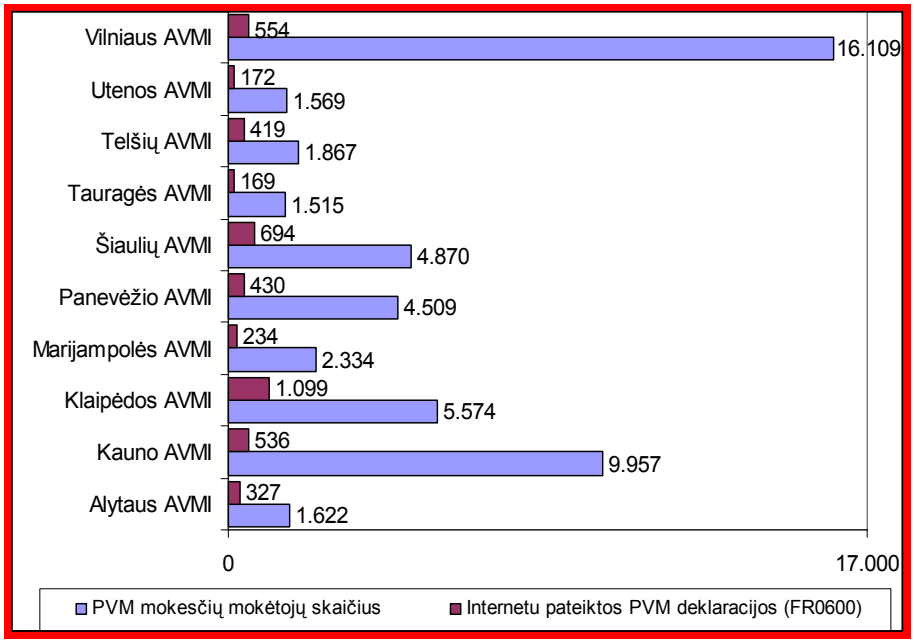
Tačiau elektroninis deklaravimas Lietuvoje dar nėra toks populiarus kaip Europos Sąjungos valstybėse. Pavyzdžiu, 2004 m. rugsėjo 1 d. Lietuvoje buvo užregistruota 49 926 PVM mokėtojai. Daugiausia PVM mokėtojų (32%) yra Vilniaus, o mažiausia Alytaus, Tauragės, Utenos (po 3%) ir Telšių (4%) apskrityse (1.11. pav.).



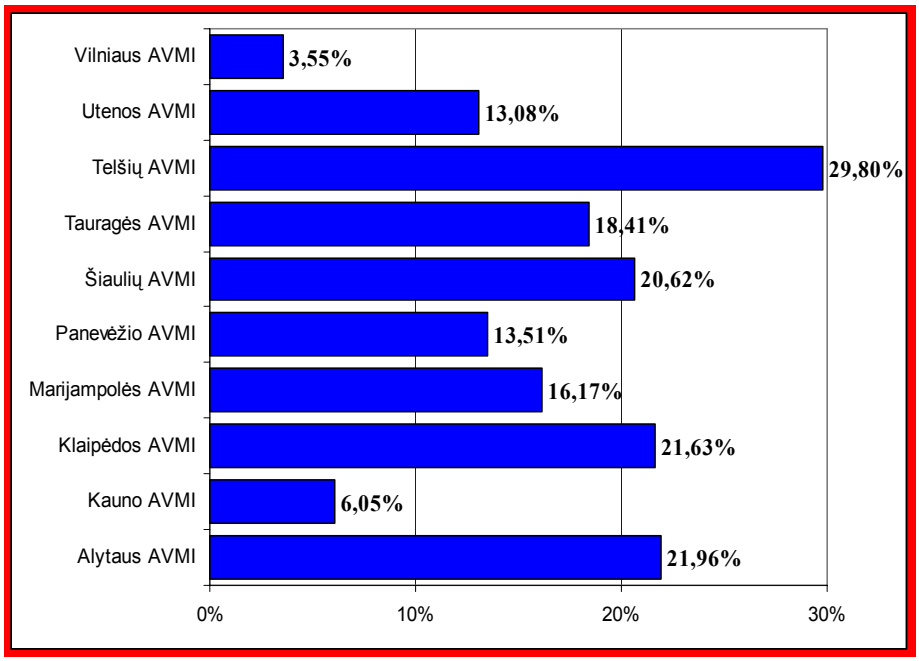
1.11 pav. PVM mokėtojų skaičius 2004 m. rugsėjo 1 d.

Tačiau tų pačių metų lapkričio 9 d. duomenimis elektroniniu būdu buvo pateikta tik 4 634 deklaracijos. Tai sudaro tik 10,86 procento nuo visų PVM mokėtojų. Įvertinus tai, kad net 79,8 procentai Lietuvos įmonių naudoja internetą[66] ir beveik visos jos yra PVM mokėtojai, toks e. deklaravimo rodiklis yra pakankamai žemas. Paradoksalu, tačiau apskrityse, kuriose yra mažiausia PVM deklaruotųjų (1.12 pav.), pastebimas didžiausias susidomėjimas PVM elektroniniu deklaravimu (1.13 pav.). Beveik trečdalis (29,8%) Telšių apskrities įmonių PVM deklaracijas teikia elektroniniu būdu. Šiek tiek mažiau atsilieka Alytaus (21,96%) ir Tauragės (18,41%) apskrityse registruoti PVM mokėtojai. Pačiose didžiausiose Vilniaus ir Kauno apskrityse, kurios sudaro daugiau kaip pusę (52%) PVM mokėtojų, PVM deklaracijas elektroniniu būdu 3,55 procentai Vilniaus ir 6,05 procentai Kauno apskričių PVM mokėtojų.

[66] Informacinės technologijos. Statistikos departamento prie Lietuvos Respublikos Vyriausybės, Vilnius, 2004



1.12 pav. PVM mokėtojų ir internetu pateiktų PVM deklaracijų skaičiaus 2004-09-01

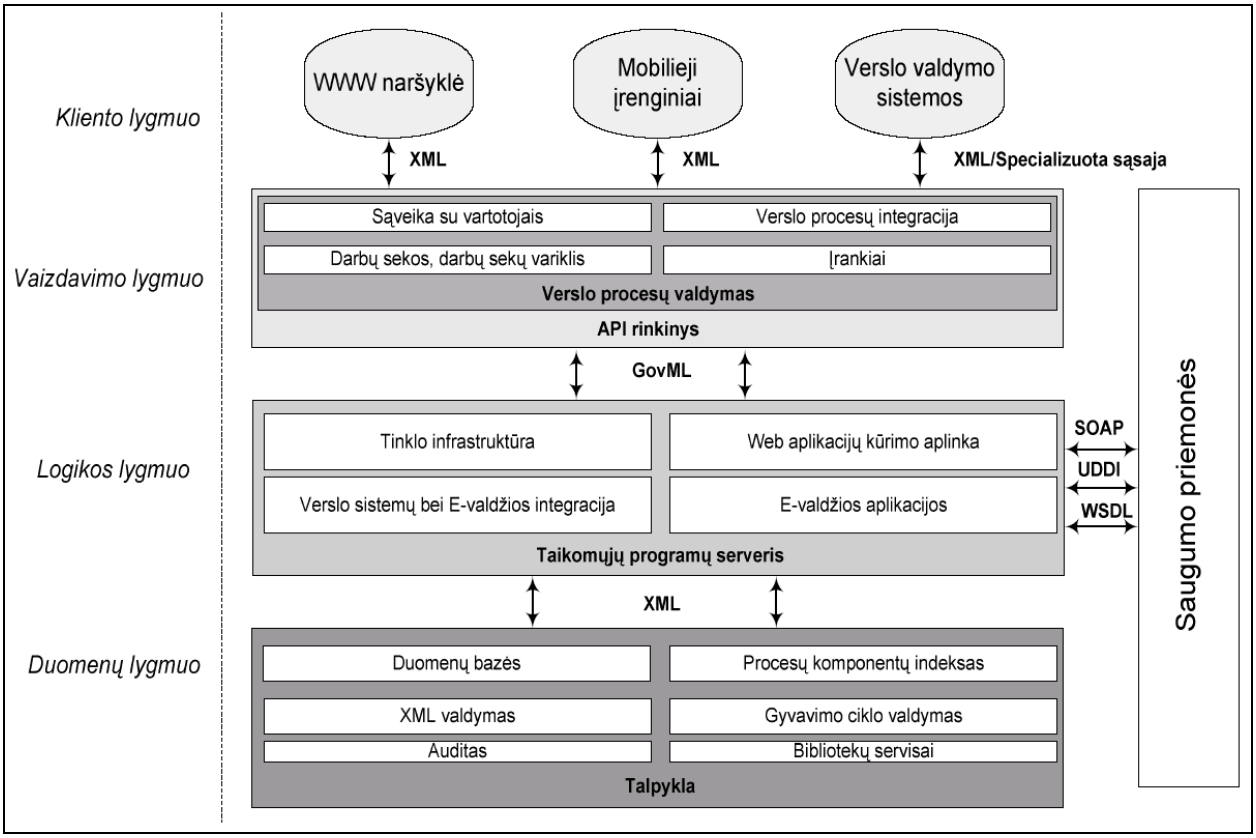


1.13 pav. Pateiktų PVM deklaracijų nuo PVM mokėtojų dalis 2004-09-01

Kadangi apskritys sudarytos iš rajonų, gali susidaryti įspūdis, kad šių didžiausių apskričių rodiklius žemina periferinių rajonų įmonės. Tačiau, kaip rodo analizė, patys žemiausi rodikliai užfiksuoti Vilniaus (3,27%) ir Kauno (3,27%) valstybinių mokesčių inspekcijų skyriuose. Iš didžiųjų apskričių VMI tik Klaipėdos ir Šiaulių apskričių VMI fiksuojamas pakankamai didelis PVM mokėtojų skaičius, atitinkamai 21,63 ir 20,62 procentai, teikiantis deklaracijas elektroniniu būdu.

1.7. TECHNOLOGINIS VIEŠŲJŲ E. PASLAUGŲ MODELIS

Elektroninės valdžios sistemos techninę architektūrą sudaro keturi lygiai[67]. Toks šios sistemos modelis leidžia sukurti lanksčią, greitai ir pigiai plečiamą sistemą, kurioje kiekvienas lygis gali būti realizuojamas skirtingomis techninėmis priemonėmis (1.14 pav.).



1.14 pav. Elektroninės valdžios sistemos techninė architektūra.

Kliento lygmuo sudarytas iš skirtingų prieigos prie sistemos kanalų, kurie atspindi skirtingus vartotojus, naudojamus įrenginius, perdavimo kelius ir skirtingas aplikacijas, naudojamas bendrauti su kitais sistemos moduliais. Galima išskirti tokius galutinius įrenginius, kaip WWW naršyklė, mobilieji įrenginiai ir verslo subjektų naudojamos valdymo sistemos.

Vaizdavimo lygmuo apibūdina informacijos atvaizdavimo formų, skirtų klientui, apdorojimą ir kliento bendravimą su specialiomis programomis. Vaizdavimo komponentas turėtų apimti visus standartus, kurie naudojami informacijos apsikeitimui su atitinkamais kliento lygio įrenginiais.

[67] Elektroninių viešųjų paslaugų siekiamo modelio aprašymas, http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_siekiamasV1.pdf; prisijungimo laikas: 2004-11-04.

Logikos lygmuo apima naujausius informacinių technologijų sprendimus, atsiradusius e. valdžios ir e. verslo srityje, ir daugeliu atveju turėtų sudaryti e. valdžios sprendimų pagrindą. Specifinius verslo sprendimus atliekantys aplikacijų moduliai yra sujungiami loginiame lygyje. Šiame lygmenyje duomenys yra priimami, apdorojami ir teikiami vaizdavimo lygmeniui, vykdomi pakeitimai duomenų bazėse. Čia, siekiant užtikrinti duomenų konfidencialumą, vientisumą ir prieinamumą, turi būti įdiegtos visos reikalingos saugumo priemonės.

Duomenų lygmuo turi užtikrinti duomenų saugojimą. Šis lygis apima operacinės sistemos funkcionalumą, duomenų bazių valdymo sistemas, dokumentų saugyklas, senas sistemas ir verslo valdymo sistemas.

Kiekviename išvardintame lygyje, visa sistema yra padalinta į atskirus modulius, atsakingus už konkrečių funkcijų vykdymą, kurie tarpusavyje bendrauja nustatytų sąsajų pagalba. Tokiu būdu, gaunama lankstesnė, lengvai kuriama, valdoma bei plečiama sistema. Bendravimas tarp modulių gali būti išorinis arba vidinis. Vidinis bendravimas vyksta tarp modulių, esančių vienoje aplikacijoje, o išorinis bendravimas vyksta tarp skirtingų aplikacijų ir yra apibrėžtas viešais protokolais. Sujungimai tarp šių sistemų įgyvendinami, naudojant įvairius protokolus, sukurtus XML pagrindu. Vieni protokolai (*WSDL - Web Services Description Language*) naudojami paslaugoms apibrėžti, kurie aprašo internetu tiekiamas paslaugas tokia forma, kokia jas gali panaudoti kitos kompiuterinės programos, nežinant jos įgyvendinimo smulkmenų ar papildomų specifikacijų, kiti (*UDDI - Universal Description, Discovery and Integration*) - skelbti, struktūrizuoti, kategorizuoti, valdyti ir pateikti naudotojams internetu teikiamas paslaugas, treti (*SOAP - Simple Object Access Protocol*) – siųsti užklausoms ir atsakymams tarp kompiuterinių programų, ketvirti (*GovML - Government Mark-up Language*) - aprašyti duomenims, apibūdinantiems paslaugas. Visi ryšio seansai, nepriklausomai nuo naudojamo protokolo tipo, turi būti koduojamas naudojant SSL (*Secure Socket Layer*) protokolą. Taip pat reikia paminėti ir protokolą S-HTTP (*Secure Hyper Text Transfer Protocol*), naudojamą interneto paslaugoms teikti, juo koduojamos užklausos interneto paslaugų serveriams bei šių serverių atsakymai. Šis protokolas suprojektuotas, siekiant užtikrinti saugų dokumentų apsikeitimą pasauliniame tinkle, jis palaiko kartotinio rakto valdymo mechanizmus ir kriptografinius algoritmus.

2. VIEŠŲJŲ E. PASLAUGŲ SAUGUMAS

2.1. SAUGUMO MODELIAI

Informacijos saugumo politikos įgyvendinimui naudojami įvairūs saugumo modeliai. 1971 m. slaptumui užtikrinti amerikietis *B. Lampson*[68] pirmasis sukūrė priėjimo kontrolės modelį (*Access control model for confidentiality*), kurį vėliau (1972 m.) ištobulino jo tėvynainiai *G. Graham* ir *P. Dening*[69]. Modelio struktūra paremta kompiuterio būsenos (*state machine*) principu, apibrėžiančia trilypę kompiuterio būseną (*S, O, M*), kur *S* – subjektų aibė, *O* – objektų aibė ir *M* – priėjimo matrica. Šios matricos eilutėse nurodyti subjektai, o stulpeliuose - objektai. Matricos elementas *M*[*c,o*] apibrėžia subjekto priėjimo teises (*Access rights*) prie objekto. Priėjimo teisės paimamos iš baigtinio priėjimo teisių *A* rinkinio. Būsena pasikeičia, atsiradus reikalavimui keisti priėjimo matricą *M*. Nepaisant savo paprastumo, šis modelis turėjo didelės įtakos *Harrison*, *Ruzzo* ir *Uleman*[70] bei *Bell* ir *Lapadula* saugumo modeliams.

Amerikiečių informacijos saugumo specialistai[71] išskiria tokius pagrindinius modelius:

- *State machine* modelis;
- *Bell-LaPadula* modelis;
- *Biba* modelis;
- *Clark-Wilson* modelis;
- *Information Flow* modelis;
- *Noninterference* modelis;
- *Take-Grant* modelis;
- *Access control matrix* modelis.

Kiekvienas iš šių modelių vienas su kitu turi tam tikrų panašumų ir aiškių skirtumų. Saugumo modeliai informacinių sistemų projektuotojams leidžia sudaryti algoritmų schemas, įvertinti abstrakčius saugumo politikos reikalavimus.

---

[68] B.Lampson. Protection. In 5th Princeton Symposium on Informatikon Sciences and System, March 1971. Reprinted in ACM Operating Systems Review, 8(1), 1974.

[69] G. Graham and P. Dening. Protection – principles and practice. In Proc. Spring Jodint Computer Conference. AFIPS Press, 1972.

[70] Harrison, M.H., Ruzzo, W.L and Uleman, J.D „Protection in Operating Systems.“ Comunications of ACM 19(8):461-471, 1976.

[71] CISSP: Certified Information Systems Security Professional. Study Guide. E.Tittel, M.Chapple, J.M.Stewart, Sybex, Inc, Alameda, CA, 2003.

Informacinėse sistemose, kuriose saugoma ir apdorojama kritiškai svarbi informacija, saugumo sistema turi remtis daugiapakope saugumo (*multi-level secure*) politika. 70-ųjų metų pabaigoje buvo pradėti kurti pirmieji daugiapakopiai priėjimo prie informacinių sistemų valdymo modeliai, labiausiai tinkami praktiniam naudojimui sudėtingose informacinėse sistemose. Daugiapakopė saugumo politikos sistema valdo daugelį informacijos srautų, skirstydama juos į leidžiamus ir neleidžiamus. Šiuolaikinėse saugumo sistemose tokia daugiapakopė saugumo politika realizuoja taip vadinamą mandatinę (*mandatory access control*) arba privalomąją priėjimo kontrolę, per kurią praeina kiekvienas subjekto kreipimasis į objektą, jeigu šį objektą saugo informacijos saugumo sistema[72]. Daugiapakopės saugumo politikos tikslas – užtikrinti informacijos slaptumą. Informacijos vientisumo klausimas, naudojant šią politiką, nesprendžiamas arba sprendžiamas kaip šalutinis informacijos slaptumo rezultatas.

Jungtinių Valstijų Gynybos ministerijoje (*U.S. Department of Defense*) buvo sukurtas vienas pirmųjų *Bell-LaPadula* modelis. Pirmą kartą jis buvo publikuotas 1976 metais, siekiant atkreipti įmonių dėmesį į slaptos informacijos saugojimą. Pagal šį modelį, tarp dviejų objektų X ir Y vyksta informacijos apsikeitimas, kur objektas X yra informacijos šaltinis, o Y - informacijos gavėjas. Išraiška c(Y)>c(X) reiškia, kad objektas Y yra vertingesnis už objektą X. *Bell-LaPadula* modelio politika nustato, kad informacijos srautas iš informacijos šaltinio X į informacijos gavėją Y leidžiamas tik tada ir tik tada, kai objektas Y yra slaptesnis už objektą X, t.y. c(Y)>c(X).

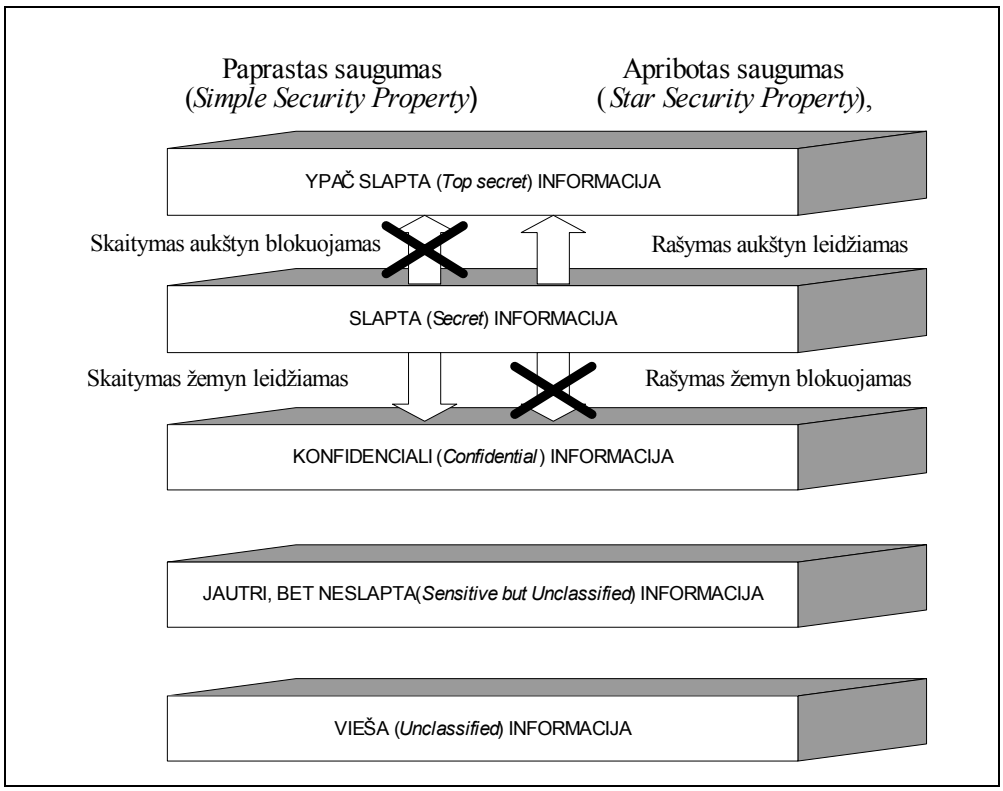
Gynybos ministerija klasifikuoja dokumentus į penkis lygius[73]:

1. Vieši (*Unclassified*);
2. Jautrūs, bet neslapti (*Sensitive but Unclassified*);
3. Konfidencialūs (*Confidential*);
4. Slapti (*Secret*);
5. Ypač slapti (*Top Secret*).

[72] Ran Atkinson, MLS Security Associations, http://www.netsys.com/ipsec/1995/msg00584.html; prisijungimo laikas: 2004-11-11.

[73] Bell D.E., L.J. LaPadula. 1976. Secure computer systems: unified exposition and multics inter-pretation. Report MTR-2997 Rev. 1. AD A023 588. Bedford, Mass.: The Mitre Corporation. http://csrc.nist.gov/publications/history/bell76.pdf; prisijungimo laikas: 2004-11-12.

Bet kuris asmuo, turintis priėjimo teisę prie slaptų dokumentų, taip pat gali prieiti ir prie viešų, jautrių, bet neslaptų ir konfidencialių dokumentų, bet neturi teisės prieiti prie ypač slaptų dokumentų (2.1 pav.).



2.1 pav. Bell-LaPadula modelis

Modelis turi dvi pagrindines ypatybes[74]:

1. paprasto saugumo ypatybė (*Simple Security Property*), kai subjektas gali tik skaityti objektą, jeigu subjekto priėjimo lygis dominuoja objekto priėjimo lygio atžvilgiu, t.y. toks subjektas negali skaityti informacijos, kurios jautrumo lygis yra aukštesnis (*no read up*), bet gali skaityti informaciją, kurios jautrumo lygis žemesnis:

$$X \xrightarrow{r} Y \Leftrightarrow c(X) \geq c(Y),$$

2. apriboto saugumo ypatybė ($^{\vee}$ *(star) Security Property*), kai subjektas gali tik rašyti į objektą, jeigu objekto priėjimo lygis dominuoja subjekto priėjimo lygio atžvilgiu, t.y. toks subjektas negali rašyti informacijos į objektą, kurio informacijos jautrumo lygis žemesnis (*no write down*), bet gali rašyti į objektą, kurio jautrumo lygis aukštesnis:

[74] Особенности применения криптографических средств в информационных системах с мандатной политикой управления доступом, Г. А. Черней, 2000, http://www.ase.md/~osa/publ/ru/pubru20.html; prisijungimo laikas: 2004-11-24.

$$X \xrightarrow{w} Y \Leftrightarrow c(X) \leq c(Y).$$

Biba modelis buvo sukurtas iš karto po *Bell-LaPadula* modelio. Tai labai analogiškas modelis, kuris skirtingai nuo anksčiau išnagrinėto, dėmesį kreipia ne į informacijos konfidencialumą, bet į jos vientisumą. Modelis turi dvi pagrindines aksiomas:

1. paprasto vientisumo aksioma (*Simple Integrity Axiom*), kai subjektas negali skaityti objekto su žemesniu vientisumo lygiu (*no read down*);
2. apriboto vientisumo aksioma ($^{\vee}$ *(star) Integrity Axiom*), kai subjektas negali modifikuoti objekto su aukštesniu vientisumo lygiu (*no write up*).

Svarbų vaidmenį informacijos saugumo teorijoje vaidina *Clark-Wilson* modelis[75], publikuotas 1987 m. (modifikuotas 1989 m.). Šis modelis skirtas verslo aplinkai, pagrįstas transakcijų naudojimu ir kruopščiu priėjimo teisių įforminimu ir suteikimu subjektams, leidžiančių jiems prieiti prie objektų. Šiame modelyje pirmą kartą išnagrinėtas trečiosios šalies saugumo problema – šalies, kuriai patikėtas saugumo sistemos priežiūra. Šį vaidmenį informacinėse sistemose dažniausiai atlieka tam tikra programa. Taip pat pirmą kartą šiame modelyje transakcijos buvo paremtos patikrinimo (*verification*) metodu, t.y. subjekto identifikavimas buvo atliekamas ne tik prieš jo komandos vykdymą, bet ir pakartotinai, po komandos įvykdymo. Tai leido išspręsti autoriaus pakeitimo problemą, tarp identifikavimo ir komandos vykdymo momento. *Clark-Wilson* modelis apibrėžia šiuos pagrindinius elementus ir procedūras:

1. suvaržyti duomenys (*constrained data item*), bet kokie duomenys, kurių vientisumą garantuoja saugumo modelis;
2. laisvi duomenys (*unconstrained data item*), bet kurie duomenys, nekontroliuojami saugumo modelio;
3. vientisumo patikrinimo procedūra (*integrity verification procedure*), skanuojanti duomenis ir patvirtinanti jų vientisumą;
4. transformacijos procedūra (*transformation procedures*), vienintelė procedūra, leidžianti modifikuoti suvaržytus duomenis.

[75] D.D. Clark and D.R.Wilson. A comparison of commercial and military computer security policies. In *IEEE Symphosium on Research in Security and Privacy*, April 1987.

Modelio pagrindas - apribotas priėjimas prie suvaržytų duomenų transformacijos procedūros pagalba. Šis modelis laikomas vienu iš labiausiai išbaigtų modelių, užtikrinančių informacinių sistemų vientisumą, garantuojantis duomenų saugumą nuo bet kurių vartotojų bet kokių neįgaliotų pakeitimų.

2.2. INFORMACIJOS SAUGUMO PASLAUGOS

Kategorijos. Jungtinių Valstijų Nacionalinis standartų ir technologijų institutas informacijos saugumo sistemos įgyvendinimą, įsivaizduoja kaip tam tikrų paslaugų teikimą. Šios paslaugos skirstomos į tris kategorijas: valdymo, operacinę ir techninę[76]. Valdymo paslaugos nukreiptos į organizacijos informacijos saugumo politiką ir rizikų valdymą, operacinės – į žmogaus diegiamas ir valdomas saugumo valdymo priemones, techninės – į kompiuterinių sistemų vykdomą saugumo valdymą (2.2 pav.).

Kategorija	Saugumo paslaugos
Valdymo (*Management*)	Saugumo programa (*Security Program*)
	Saugumo politika (*Security Policy*)
	Rizikos valdymas (*Risk Management*)
	Saugumo architektūra (*Security Architecture*)
	Sertifikavimas ir akreditavimas (*Serfification and Accreditation*)
	IT produktų saugumo analizė (*Security Evaluation of IT Products*)
Operacinė (*Operational*)	Nenumatytų situacijų planavimas (*Contingency Planning*)
	Incidentų valdymas (*Incident Handling*)
	Testavimas (*Testing*)
	Mokymas (*Training*)
Techninė (*Technical*)	Ugniasienės (*Firewalls*)
	Įsiveržimų aptikimas (*Intrusion Detection*)
	Viešieji infrastruktūras raktai (*Public Key Infrastructure*)

2.2 pav. Informacijos saugumo paslaugų kategorijos

Gyvavimo ciklas. Kiekviena informacijos saugumo sistemos paslauga, nepriklausomai nuo kategorijos, kuriai ji priskiriama, praeina šešias gyvavimo ciklo fazes, nuo saugumo proceso poreikio inicijavimo iki jo užbaigimo (2.3 pav.). Kad užtikrinti daugiapakopę saugumo sistemą, turi būti sukurta visapusiška informacijos saugumo programa, apimanti kiekvienos kategorijos saugumo paslaugas. Išskiriamos šios gyvavimo ciklo fazės[77]:

I fazė – inicijavimo (*Initiation*). Organizacija, norėdama pagerinti organizacijos saugumo sistemos efektyvumą, apibrėžia tam tikrų saugumo paslaugų poreikį.

[76] NIST Special Publication 800-35, Guide to Information Technology Security Services, October 2002, http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf; prisijungimo laikas: 2004-11-10.
[77] Ten pat.

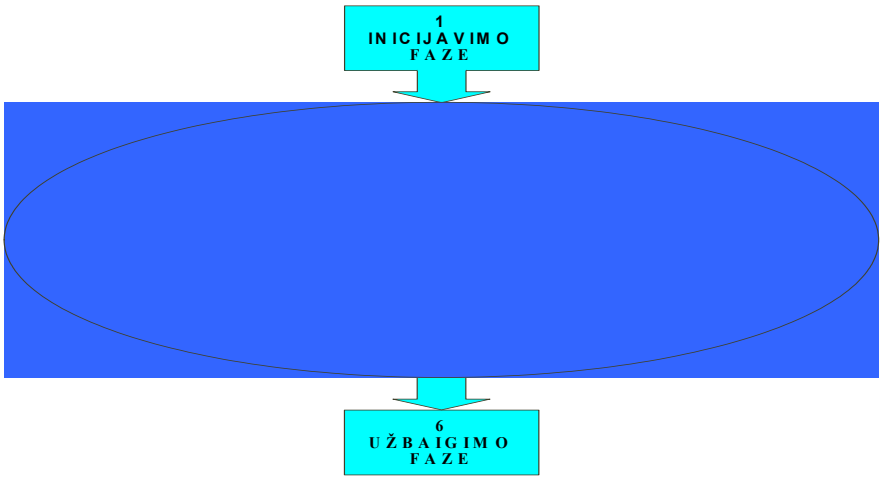
II fazė – įvertinimo (*Assessment*). Organizacija, atsižvelgdama į savo nustatytą saugumo politiką, įvertina savo turimas finansines, organizacines, technines, žmoniškųjų išteklių galimybes ir riziką naujojo saugumo sistemos paslaugų elemento įdiegimui. Padarytos išvados dokumentuojamos.

III fazė – sprendimo (*Solution*). Organizacijos vadovybė apsvarsto padarytas išvadas ir priima sprendimą įtraukti į organizacijos veiklos planą naujos saugumo paslaugos įdiegimą bei paveda formuoti šios paslaugos įgyvendinimo planą.

IV fazė – įgyvendinimo (*Implementation*). Organizacija, atsižvelgdama į savo poreikius, parengia naujos saugumo paslaugos techninę specifikaciją ir jos vykdymui parenka kvalifikuotą vykdytoją, pasirašo su juo sutartį, kuris įdiegia šią paslaugą.

V fazė – veikimo (*Operations*). Naujas saugumo sistemos elementas pradeda veikti. Organizacija privalo nuolatos stebėti kaip vykdoma ši paslauga, ar ji atitinka tuos reikalavimus, kurie buvo jai keliami. Iškylančius veikimo nesklandumus, paslaugos vykdytojas privalo juos šalinti.

VI fazė – užbaigimo (*Closeout*). Tuo atveju, kai teikiamos paslaugos organizacijai nereikia, arba kai ji atliekama netinkamai, atliekamas atitinkama šio saugumo sistemos elemento pašalinimo procedūra.



2.3 pav. Informacijos saugumo sistemos paslaugų gyvavimo ciklas.

Siekiant užtikrinti stabilų organizacijos saugumo sistemos veikimą, kiekvienas šios sistemos elementas nuo pat pradžių turi būti planuojamas, diegiamas ir šalinamas iš sistemos prisilaikant šios schemos. Informacijos saugumo vadovai turi ne tik nuspręsti, kuri saugumo paslauga turi būti įgyvendinama ar nutraukiama, bet ir įvertinti šių paslaugų poveikį kitoms saugumo sistemos paslaugoms.

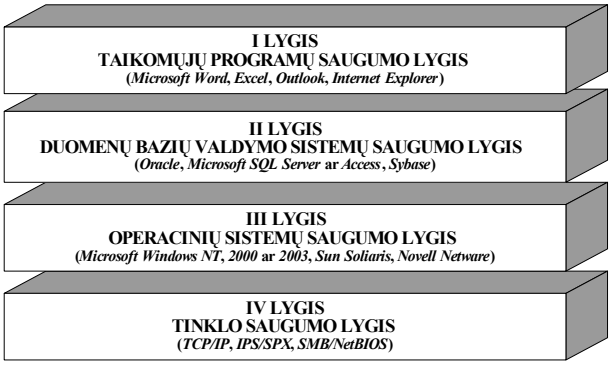
Saugumo lygiai. Paprastai naudojamas kompleksinis keturių lygių informacijos saugumas (2.4 pav.):

I. Taikomųjų programų *(Microsoft Word*, *Excel*, *Outlook*, *Internet Explorer* ir kt.), kurios bendrauja su vartotoju, lygis.

II. Duomenų bazių valdymo sistemų (*Oracle*, *Microsoft SQL Server* ar *Access*, *Sybase* ir kt.), saugančių ir apdorojančių informaciją informacinėse sistemose, lygis.

III. Operacinių sistemų (*Microsoft Windows NT*, *2000* ar *2003*, *Sun Soliaris*, *Novell Netware* ir kt.), aptarnaujančių duomenų bazių valdymo sistemas ir taikomąsias programas, lygis.

IV. Tinklo protokolų (*TCP/IP*, *IPS/SPX*, *SMB/NetBIOS*), užtikrinančių informacinės sistemos atskirų dalių sąveiką, lygis.



2.4 pav. Informacijos saugumo lygiai

Siekiant užtikrinti elektroninių paslaugų tinkamą saugumo lygį, saugumo sistema turi efektingai veikti visuose išvardintuose lygiuose. Kai nusikaltėliui sunku patekti į informacinę sistemą iš išorės, jis būtinai ieškos spragų viduje, tarp organizacijos darbuotojų. Jis gali pabandyti perskaityti duomenų bazėje saugomus duomenis iš *MS Query*, kuri leidžia prieiti prie daugelio duomenų bazių, naudojant, pavyzdžiui, *SQL* užklausų mechanizmą (pirmasis lygis), gali paimti duomenis iš pačios duomenų bazių valdymo sistemos, naudojant įvairias šios sistemos priemones (antrasis lygis), perskaityti elektronines duomenų bazių bylas tiesiogiai operacinės sistemos lygyje (trečiasis lygis) arba pasiųsti užklausas per tinklą, norint gauti reikalingą informaciją, ar perimti ryšio kanalais persiunčiamus duomenis (ketvirtasis lygis).

Šis paprastas pavyzdys patvirtina teiginį, kad turi būti įdiegiamos kompleksinės informacijos saugumo priemonės, nes kaip rodo praktika, labai dažnai apsiribojama tik operacinės sistemos (standartiniai saugumo nustatymai) ir tinklo (maršrutizatoriai) lygio saugumo priemonėmis. Šiuo atveju, jeigu nusikaltėliui, naudojant specialias programas, pavyko

gauti vartotojo identifikatorių ir slaptažodį, kuriuos jis naudoja elektroninėms paslaugos gauti, toliau įsiskverbti į sistemą jam turėtų sektis puikiai, nes jis į ją patenka naudodamasis autorizuoto asmens identifikatoriumi ir slaptažodžiu. Bet tai padaryti jam pavyko ne dėl šių sistemų trūkumo (tai tik toks jų veikimo mechanizmas), o dėl organizacijų darbuotojų, kurie privalo užtikrinti informacijos saugumą, klaidingo požiūrio. Tuo tikslu labai dažnai būtina naudoti papildomus saugumo mechanizmus - įsiveržimų aptikimo (*intrusion detection*), sukčiavimo aptikimo (*fraud detection*), saugumo įvertinimo sistemų (*security assessment systems*) ir saugumo skenerių (*security scanners*) mechanizmus, kurie gerai veikia vidiniame (nuo darbuotojų piktnaudžiavimo) ir išoriniame tinkle (nuo nesankcionuotų prisijungimų), apsaugo sistemą nuo aptarnavimo atmetimo (*denial of service*) incidentų ir analizuoja informacinių sistemų pažeidžiamumą. Kompanijos IDC duomenimis šių priemonių pardavimas išaugo nuo 58 mln. (1997 m.) iki 977,9 mln. dolerių (2003 m.)[78].

Taip pat gali kilti saugumo grėsmės ir dėl blogai sukonfigūruotos programinės ir techninės įrangos. Čia galima pateikti labai akivaizdų faktą ir e. prekybos praktikos, kai buvo visiškai paralyžuotas tokių populiarių svetainių, kaip *Yahoo*, eBay, *Amazon*, *Buy*, *CNN*, *ZDNet*, *Datek* ir *ETrade*, teikiančių e. prekybos paslaugas, interneto serverių darbas. Federalinio tyrimų biuro atliktas tyrimas parodė, kad serveriai sugedo dėl labai didelio užklausų kiekio, kuris buvo adresuotas į šiuos serverius. Pavyzdžiui, pranešimų srautas (*traffic*) į kompanijos *Buy* serverį viršijo vidutinį įprastą pranešimų srautą 24 kartus, o maksimaliai leistiną pranešimų srautą į serverį 8 kartus. Kompanija tik per tris prastovos valandas įvairiais vertinimais patyrė pusantro milijardo dolerių nuostolį!**[79]**

Kita potenciali grėsmė – duomenų perėmimas, priklausantis nuo tam tikrų versijų tinklo protokolų IP naudojimo. Kad to išvengti, reikia naudoti kriptografijos priemones arba protokolą IP6, garantuojantį duomenų perdavimo saugumą.

Problemos. Informacijos saugumo paslaugų diegimas ar jų derinimas gali būti pakankamai sunkus. Kiekviena saugumo paslauga turi savo kainą ir rizikos elementą. Priimant sprendimą, kuris paremtas vienos problemos sprendimu, galima turėti vienokių ar kitokių pasekmių kitose organizacijos srityse. Pvz., jeigu priimamas sprendimas, patikėti saugumo problemų sprendimą išoriniam vykdytojui, kuris tai gali atlikti efektyviau, iškyla klausimas, ką daryti su savo darbuotojais, kurie dirbo šioje srityje. Sprendimus priimantys vadovai visada balansuoja ant kainos/vertybės ribos, potencialių ilgalaikių rizikų, susijusių su darbuotojų moralės praradimu,

[78] Abner Germanow. Plugging the Holes in eCommerce: The Market for Intrusion Detection and Vulnerability Assessment Software, 1999-2003. International Data Corporation, August, 1999.

jų fiziniu išsekimu ar intelektualiuoju kapitalu. Jungtinių Valstijų Nacionalinis standartų ir technologijų institutas šiuos visus faktorius ir problemas sugrupuoja į šešias kategorijas[80]:

1. **strategines**, kai saugumas apskritai ir informacijos saugumas ypatingai turi garantuoti sėkmingą organizacijos veiklą. Kada organizacijos vadovai galvoja apie sprendimų priėmimo svarbą, jie privalo savęs paklausti, kas naudingiausia organizacijai strateginiu požiūriu, kas geriausia padeda jai siekti savo misijos.
2. **finansines**, nes bet kurio sprendimo priėmimo širdis dažniausiai yra finansavimas. Tačiau kaina dažnai yra tik viena iš daugelio problemų. Dėmesys turi būti sukoncentruotas į paslaugos vertę.
3. **technines**, nes kiekviena IT paslauga, net jeigu ji yra valdymo paslauga, visada turi techninę potekstę. Per paslaugos gyvavimo ciklą, informacijos saugumo vadovai privalo apsvarstyti, kokį techninį ir architektūrinį efektą organizacijai turės priimti sprendimas.
4. **organizacines**, nes šie klausimai yra susiję su neapčiuopiamais organizacijos elementais, tokiais kaip moralė ir reputacija.
5. **personalo** problemos siejasi su darbuotojais ir užsakovais. Vadovai privalo žinoti, kad jų priimti sprendimai ir saugumo paslaugų diegimo procesas, visada daro poveikį darbuotojams. Šių poveikių ir elgesio supratimas ankstyvoje stadijoje, turi garantuoti personalo, kaip svarbaus organizacijos resurso, išlaikymą.
6. **politikos**. Efektyvus informacijos saugumas prasideda nuo tvirtos politikos suformulavimo. Politika ir procesai privalo būti gerai apgalvoti, kad garantuotų sėkmingą įgyvendinimą.

Informacijos saugumo požiūriu, ketvirtasis - transakcijų stadijos lygis, yra pats pavojingiausias ir jam turi būti skiriamas ypatingas dėmesys. Pradiniame etape, kai daugelio organizacijų ir įmonių vadovams rūpi neatsilikti nuo sparčiais tempais vykstančios telekomunikacinių ir informacinių technologijų pažangos ir kuo greičiau pradėti teikti tokias e. paslaugas, stiprinančias organizacijos įvaizdį ir rodančias jos pajėgumą, informacijos saugumu per daug nesirūpinama. Toks požiūris vėliau gali turėti labai skaudžias pasekmes, kai vietoje gerų norų, įvykus informacijos pažeidimui, gali stipriai nukentėti pasitikėjimas ne tik valdžios institucijomis, bet ir jos teikiamų viešųjų e. paslaugų patikimumu ir kokybe. Verslo įmonėms tai gali grėsti ir bankrotu. Tik pavykus įsiveržti į organizacijos informacinius resursus

[79] Лукацкий А.В. Анатомия распределенной атаки. "PCWeek/RE", №5, 2000.
[80] NIST Special Publication 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004, http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf; prisijungimo laikas: 2004-10-24.

ir pažeisti duomenų bazėse esamą informaciją, jų vadovybė suvokia savo neatsakingo vadovavimo pasekmes. Paprastai kiekvienoje organizacijoje pagrindinis dėmesys skiriamas techniniams informacijos saugumo sprendimams, visiškai nekreipiant dėmesio į organizacines priemones, ypač ugdant darbuotojų sąmoningumą.

Kiekvienam viešųjų e. paslaugų vartotojui žinoti, ar organizacija elektroniniu būdu tvarkanti apie jį duomenis, tai atlieka tinkamai. Jam svarbu buti užtikrintam, kad nebus paviešinta jos ligos istorija, jeigu jis naudojasi e. sveikatos paslaugomis, ar darbdavys nesužinos, kad jis ieško naujo darbo, e. darbo paieškos sistemoje, ar apie jo ar jo įmonės mokamus mokesčius, deklaruojamas pajamas nesužinos konkurentai, ar atsiskaitydamas už paslaugas elektroniniu būdu, jis gali būti tikras, kad nebus paviešintos jo sąskaitoje saugomų pinigų sumos, ar jo naudojami prisijungimo slaptažodžiai ir kodai yra saugūs ir t.t.

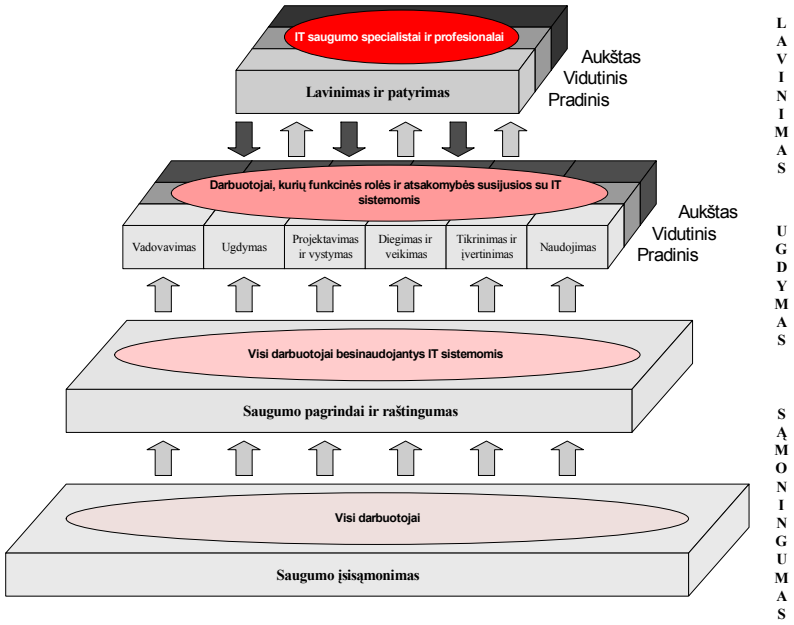
Organizacijai, teikiančiai elektronines paslaugas, svarbu neužmiršti apie visus informacijos saugumo aspektus. Galime apžvelgti vieną tipinį, bet pakankamai jautrų pavyzdį, kai vartotojas nori pasinaudoti apmokama paslauga ir nori už ją atsiskaityti per internetą. Vartotojas galvoja, kad pagrindinė saugumo problema yra tame, kad internetu perduodamas jo kreditinės kortelės numeris ir kiti duomenys, bei gaunama jo užsakyta informacija. Tačiau organizacijai teikiančiai e. paslaugas, jau pačioje pradžioje, kai tik vartotojas kreipiasi į ją su noru gauti paslaugą, kyla saugumo problemos, kurios ją lydi per visus transakcijos etapus.

Visų pirma, gali būti pakeista paslaugos suteikimo interneto svetainė, kai vartotojo užklausos paslaugai peradresuojamos į kitą serverį. Tai daroma, pakeičiant įrašus DNS serverių ar maršrutizatorių lentelėse. Tai ne tik pavojinga, kad paslauga nebus suteikta, ar bus suteikta apgaulingai, bet ypač pavojinga tuo atveju, kai vartotojas įves savo kreditinės kortelės duomenis ar kitą informaciją (asmens kodą, adresą ir pan.).

Sukurti melagingus užsakymus gali ir patys organizacijos darbuotojai savo pačių iniciatyva ar pašalinių žmonių, dažniausia potencialių sukčių, prašymu. Reikia atminti, kad pagal statistiką, daugiau kaip pusė visų incidentų susieti su darbuotojų vienokiais ar kitokiais veiksmais. Tą patvirtina ir paskutiniai bankų apiplėšimo atvejai Lietuvoje, kurie įvyko tiesiogiai ar netiesiogiai dalyvaujant pačių bankų, ar juos saugančių saugos tarnybų, darbuotojams. Kartais tokie žmonės gali įsiskverbti į duomenų bazes ir padaryti jiems reikalingus informacijos pakeitimus. Sužinoję kreditinių kortelių numerius ar pasiekę kitus savo tikslus nusikaltėliai užbaigia savo darbą, taip vadinamu aptarnavimo atmetimo (*denial of service*) incidentu. Kartais tokie incidentai gali būti įvykdomi, norint paprasčiausia iš keršto ar kitų paskatų sukompromituoti organizaciją ar įmonę ir sutrikdyti jos normalų darbą. To

pasėkoje, kompromituojama pati organizacija, nuostolius patyrę vartotojai, gali kreiptis į teismą dėl žalos atlyginimo, atskleidus slaptą informaciją. Po tokių incidentų reikia daug pastangų, siekiant vėl įtikinti vartotojus toliau naudotis teikiamomis paslaugomis.

Pasirengimas. Sėkmingam informacijos saugumo sistemos įgyvendinimui labai svarbų vaidmenį vaidina tinkamas visų darbuotojų parengimas saugumo sistemos įgyvendinimui. Jungtinių Valstijų Nacionalinis standartų ir technologijų institutas siūlo tokį organizacijos darbuotojų rengimo modelį[81] (2.5 pav.).



2.5 pav. Saugumo mokymo tęstinumo modelis

Modelis iliustruoja trimatį masyvą apimantį:

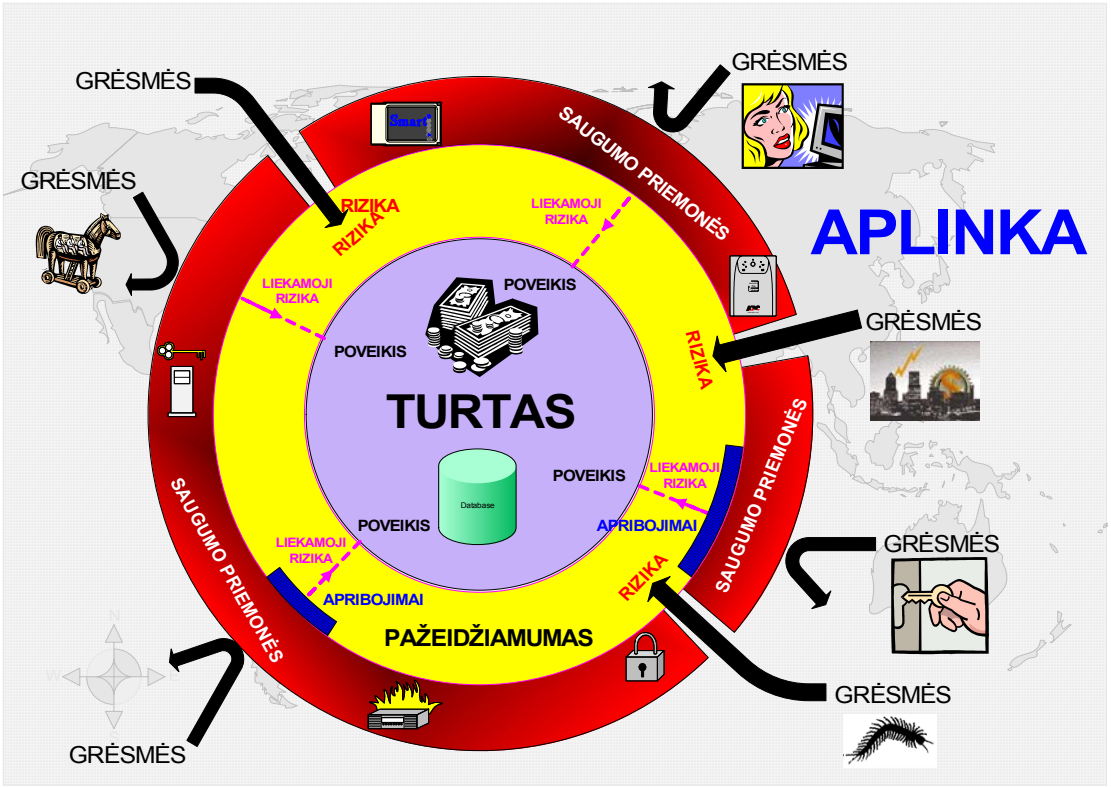
- tris pasirengimo lygius – sąmoningumo ugdymas, mokymas, lavinimas;
- šešis funkcinius saugumo vaidmenis – vadovavimas, ugdymas, projektavimas ir vystymas, diegimas ir veikimas, tikrinimas ir įvertinimas bei naudojimas;
- tris pasiruošimo lygius – pradinis, vidutinis ir aukštas.

Kiekvienas iš pasirengimo lygių skirtas skirtingoms darbuotojų grupėms, nuo eilinių sistemos vartotojų iki sistemos administratorių ir kitų aukščiausio lygio informacinių technologijų specialistų. Darbuotojų, kurių funkcinės rolės ir atsakomybės yra tiesiogiai susijusios su informacinėmis technologijomis ir informacinių technologijų specialistų pasirengimui ir įgūdžių ugdymui bei lavinimui turi būti skiriamas ypatingas dėmesys, atsižvelgiant į funkcinius saugumo vaidmenis.

[81] NIST Special Publication 800-35, Guide to Information Technology Security Services, October 2002, http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf; prisijungimo laikas: 2004-11-10.

2.3. SAUGUMO SISTEMOS ELEMENTAI IR JŲ RYŠIŲ MODELIS

Svarbiausias saugumo sistemos elementas, kuriam kuriama saugumo sistema, yra organizacijos **turtas** (2.6 pav.). Jį paprastai sudaro fizinis turtas (pastatai, komunikaciniai tinklai, kompiuterinė įranga ir pan.), žmonės (specialistai ir jų žinios), programinė įranga, informacija ir duomenys (dokumentai, duomenų bazės ir pan.), organizacijos gebėjimas sukurti tam tikrą produktą arba teikti paslaugas, tame tarpe ir elektronines, ir taip pat tokie neapčiuopiami dalykai, kaip organizacijos įvaizdis, gera valia ir panašiai.



2.6 pav. Saugumo sistemos elementų ryšių modelis

Šio organizacijos turto tinkamas valdymas yra visų organizacijos valdymo lygių svarbiausia pareiga ir veiklos sėkmės laidas. Turto įvertinimas turėtų būti atliktas aukščiausiame organizacijos valdymo lygmenyje ir paprastai tai nereikalauja smulkios, o tuo pačiu ir brangios analizės. Vertinant turtą reikia atsižvelgti į tokias jo savybes, kaip turto reikšmingumą, jo jautrumą ir taikytinas jam apsaugos priemones. Kadangi organizacija veikia tam tikroje aplinkoje ir kultūroje, šie aspektai gali daryti turto savybėms, tokioms kaip jo jautrumas, atitinkamą įtaką. Pavyzdžiui, jeigu kai kuriose kultūrose (pav., Vakarų Europos šalyse) asmeninės informacijos apsaugai skiriamas ypatingas dėmesys, tuo tarpu kitose (tame tarpe ir Lietuvoje), tam skiriama aiškiai nepakankamas dėmesys. Jeigu turtas nėra konkrečiai apibrėžtas, labai sunku užtikrinti tinkamą jo apsaugą.

Antrasis svarbus saugumo sistemos elementas – **grėsmės**. Bet koks turtas yra įvairios rūšies grėsmių taikinys. Grėsmė apibūdinama, kaip galimybė sukelti nepageidaujamą incidentą, kuris gali padaryti žalą organizacijos turtui. Žala gali įvykti dėl tiesioginės ar netiesioginės atakos, pažeidžiančios informacinėse sistemose esančią informaciją, ją sunaikinant, paviešinant, modifikuojant, padarant ją neprieinama ar visiškai prarandant. Grėsmės klasifikuojamos į keletą lygių. Pirmame lygyje grėsmės skirstomos pagal jų prigimtį - į *gamtines* ir į *dirbtines*. Prie gamtinių grėsmių priskiriamos įvairios stichinės nelaimės, avarijos, gedimai ir kitos grėsmės nepriklausiančios nuo žmogaus. Prie dirbtinių grėsmių priskiriamos žmogaus *netyčinės* ar *tyčinės* (atsitiktinės) veiklos sukeltos grėsmės. Prie netyčinių žmogaus veiklos sukeliamų grėsmių gali būti priskiriama nekvalifikuoti informacinių sistemų priežiūrą atliekančio personalo veiksmai, informacijos saugumo reikalavimų ir instrukcijų nesilaikymas ir panašiai. Tyčinės žmogaus veiklos grėsmės gali būti *išorinės*, sukeliamos pašalinių žmonių (kerštas, ekonominė nauda, „bloga žiniasklaida“ ir pan.) ir *vidinės*, sukeliamos pačių darbuotojų tyčinių veiksmų (sabotažas ir pan.). Išorinės pašalinių žmonių sukeliamos grėsmės gali būti vietinės, kai incidentai dėl pašalinių asmenų įvyksta organizacijos viduje ir nutolusios kilmės (“hakeriai”, nešiojamų kompiuterių vagystės ir pan.).

Trečiasis elementas – **pažeidžiamumas.** Pats savaime pažeidžiamumas jokios žalos padaryti negali, jis tik sudaro palankias sąlygas grėsmėms paveikti turtą. Pažeidžiamumas tai grėsmės galimybė padaryti žalą. Pažeidžiamumo analizė yra silpnų sistemos pusių nustatymas, kuriomis gali pasinaudoti dinamiškoje aplinkoje atsirandančios naujos ar pasikartojančios senos grėsmės. Rusijos saugumo specialistai *A.* ir *J. Radičev'ai* išskiria šešis pažeidžiamumo lygius[82]:

1. Fizinį, kurį apsprendžia kaip efektyviai veikia techninės įrangos (serverių, kompiuterių, komunikacinių ryšių ir t.t.) apsauga;
2. Technologinį, kurį apsprendžia kaip teisingai yra parinktos ir efektyviai vykdomos sisteminės, taikomosios ir duomenų bazių valdymo procedūros;
3. Loginį, kurį charakterizuoja adekvatus loginis informacijos saugojimo ir kodavimo mechanizmas;
4. žmoniškąjį, kurį atspindi personalo kvalifikacijos ir atsakomybė projektuojant ir prižiūrint informacines sistemas;
5. teisinį, kurį apsprendžia įstatyminiai ir teisiniai – normatyviniai aktai, reglamentuojantys subjektų santykius, keičiantis informacija;

6. organizacinį, kurį apsprendžia turimas organizacinių priemonių kompleksas, reglamentuojantis sistemų eksploatavimą.

Išsiaiškinus galimas grėsmes ir pažeidžiamumą, galima pereiti prie ketvirtojo elemento - **poveikio** (žalos) nustatymo. Poveikis turtui gali būti skirtingas - nuo kompiuterio gedimo, kai pažeidžiama tik viena darbo vieta, iki gaisro, kai ilgam laikui paralyžiuojama organizacijos veikla. Grėsmės gali ne tik sunaikinti materialųjį turtą, pažeisti informacijos slaptumą, vientisumą, prieinamumą, patikimumą, bet ir padaryti netiesioginius nuostolius – finansinius bei gero organizacijos įvaizdžio ir patikimumo. Todėl poveikio įvertinimas (pav., skalėje mažas-vidutinis-didelis) yra svarbus rizikos įvertinimo ir apsaugos priemonių parinkimo elementas. Grėsmės sukeliama žala gali būti laikina arba nuolatinė (turto sunaikinimo atveju).

Jungtinių Valstijų Nacionalinis standartų ir technologijų institutas išskiria tris poveikio lygius – žemą, vidutinį ir aukštą[83]:

1. Žemas poveikio lygis, kai konfidencialumo, vientisumo ir prieinamumo pažeidimas organizacijos veiklai, jos turtui ar personalui turi nežymią įtaką, t.y. kai organizacija gali vykdyti savo funkcijas, bet jų efektyvumas sumažėjęs, turtas yra nežymiai pažeistas, patirti nedideli finansiniai nuostoliai ar padaryta nežymi žala personalui.
2. Vidutinis poveikio lygis, kai konfidencialumo, vientisumo ir prieinamumo pažeidimas organizacijos veiklai, jos turtui ar personalui turi rimtus padarinius, t.y. organizacija dar gali vykdyti savo pirmines funkcijas, bet jų efektyvumas žymiai sumažėjęs, turtas pažeistas, patirti reikšmingi finansiniai nuostoliai ar padaryta žymi žala personalui.
3. Aukštas (arba katastrofinis) pažeidimo lygis, kai konfidencialumo, vientisumo ir prieinamumo pažeidimas organizacijos veiklai, jos turtui ar personalui turi katastrofinius padarinius, t.y. kai organizacija negali vykdyti vienos ar kelių savo pirminių funkcijų, sugadintas jos turtas, patirti milžiniški finansiniai nuostoliai, prarandamas personalas ar jo sveikatai padaryti grėsmingi sužalojimai.

Penktasis elementas - **rizikos** nustatymas. Tai tikimybė, kad pasinaudojus sistemos pažeidžiamumu, įvyks nepageidaujamas incidentas ir koks bus jo poveikis. Reikia įvertinti tą

---

[82] Вестник СамГУ _ Естественнонаучная серия. 2003. Второй спец. выпуск. 15 УДК 681.3 . Системная модель защиты информации информационных сист распределенного типа, 2003, А.Ю.Родичев, Ю.А.Родичев.

[83] NIST Special Publication 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004, http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf; prisijungimo laikas: 2004-11-10.

faktą, kad bet koks aukščiau išvardintų faktorių – turto, grėsmių, pažeidžiamumo ir saugumo priemonių pokytis, turės reikšmės rizikai.

Siekiant apsisaugoti nuo grėsmių, apriboti nepageidaujamų incidentų poveikį, atskleisti nepageidaujamus incidentus ir palengvinti veiklos atstatymą po incidentų poveikio organizacija privalo naudoti įvairias **saugumo priemones** – šeštąjį saugumo sistemos elementą. Prie pagrindinių saugumo priemonių priskiriama antivirusinė programinė įranga, tinklo perimetro apsauga, informacijos šifravimas, skaitmeniniai parašai, prieigos kontrolės mechanizmas, tinklo stebėjimas ir analizė, rezervinis kopijavimas ir rezervinis elektros tiekimas. Efektyvus saugumas reikalauja derinti įvairias apsaugos priemones. Saugumo priemonių pagrindinės funkcijos yra įsisąmoninimas, stebėjimas, prevencija, apribojimas, aptikimas ir atkūrimas. Saugumo priemonės yra naudojamas valdymo, personalo, techninėje ir fizinėje aplinkose.

Dėl aplinkos dinamiškumo, beveik visada sunku parinkti tinkamas saugumo priemones, kurios galėtų garantuoti šimtaprocentinį turto saugumą. Todėl visada dėl nepakankamo darbuotojų sąmoningumo lygio, lėšų stokos ir kitų priežasčių išlieka, nors ir minimali, taip vadinama **liekamoji rizika**. Vadovybė, atsižvelgdama į savo organizacijos poreikius ir galimybes, visada turi tai įvertinti ir priimti tą riziką. Jeigu tokia rizika nėra priimtina, būtinai turi būti numatomas papildomų saugumo priemonių įdiegimas.

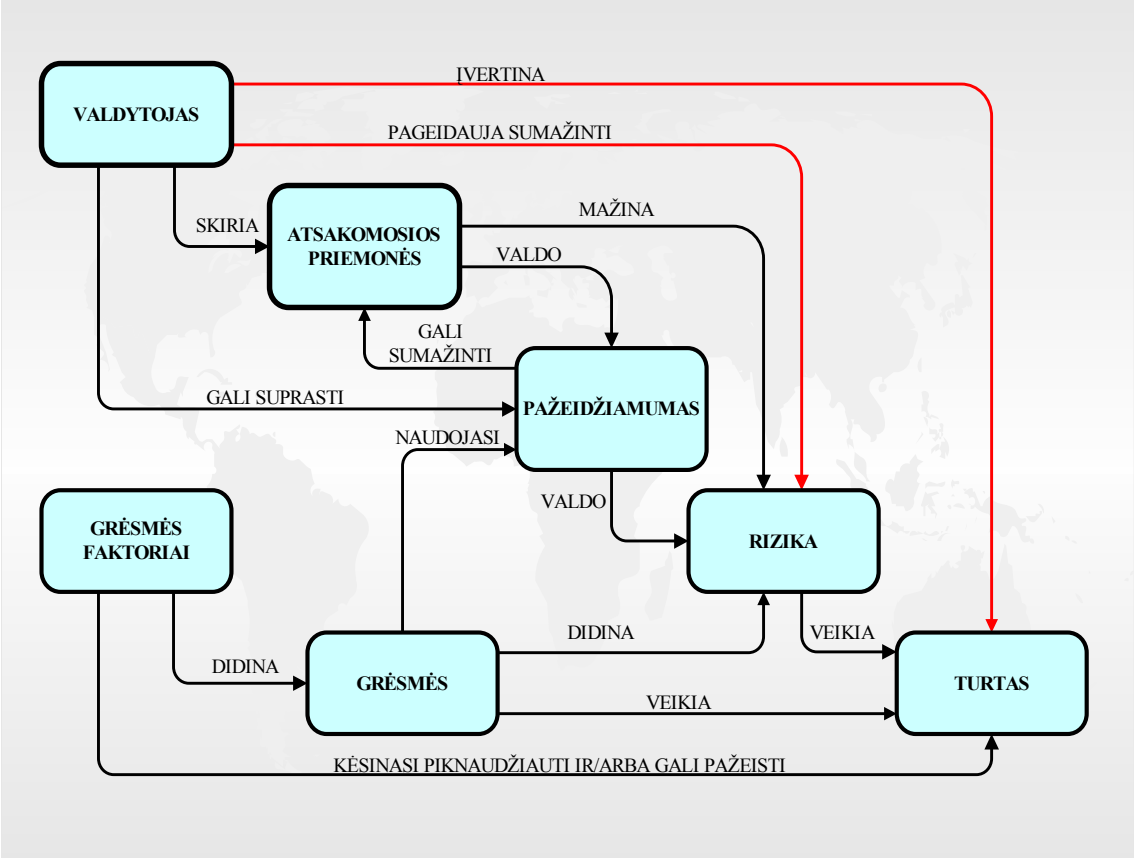
Paskutinysis aštuntasis elementas - **apribojimai**, kuriuos gali taikyti organizacijos vadovybė, jeigu apsaugos priemonės negali užtikrinti reikiamo saugumo lygio. Gali būti organizaciniai, finansiniai, aplinkos, personalo, laiko, teisiniai, techniniai, kultūriniai ir socialiniai apribojimai. Tai kraštutinės priemonės, varžančios tam tikras laisvės ir demokratijos nuostatas. Tačiau keičiantis aplinkoje ir kultūroje, kurioje veikia organizacija, apribojimai gali būti mažinami arba didinami.

2.4. INFORMACIJOS SAUGUMO KONCEPCIJA

Tarptautinis saugumo standartas ISO/IEC 15408-1:1999 nustato saugumo koncepciją ir ryšius tarp saugumo elementų[84] (2.7 pav.). Turto valdytojas yra atsakingas už turto, kuris jam yra vertybė, saugumą. Esamos ar numatomos grėsmės, taip pat šiam turtui daro įtaką ir nori jį panaudoti savo neteisėtoms reikmėms, nekreipdamas dėmesio į valdytojo teisėtus interesus. Valdytojas privalo įvertinti šias grėsmes jo valdomam turtui, kurios siekia sumažinti šio turto vertę.

---

84 International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) Date: 1998-12-18, ISO/IEC/15408-1: 1999(E), Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model.

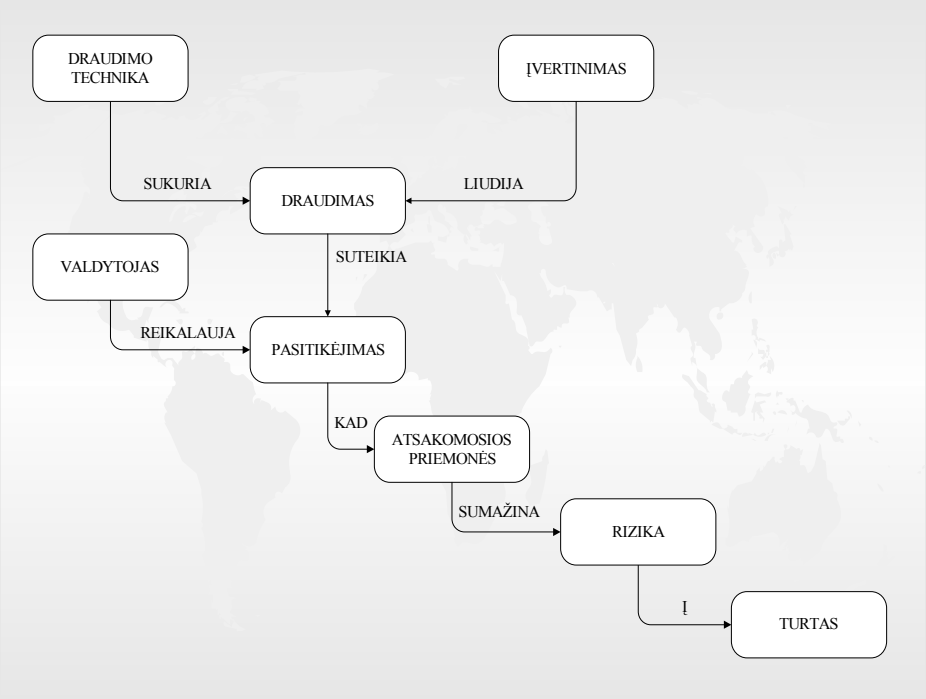


2.7 pav. Saugumo koncepcija ir ryšiai.

Informacijos saugumo pažeidimams priskiriama šie turto vertės nuostoliai: konfidencialumo praradimas, kai neįgalioti asmenys gali pasinaudoti šiuo turtu, vientisumo praradimas, kai neįgalioti asmenys gali modifikuoti šį turtą, ir prieinamumo praradimas, kai įgalioti vartotojai, negali pasinaudoti šiuo turtu. Valdytojas, turintis reikalingą kompetenciją ir suprantantis grėsmes jo valdomam turtui privalo labai atidžiai šias grėsmes išanalizuoti, kad būtų pajėgus kiek galima tiksliau įvertinti šių grėsmių sukeliamą riziką. Tiksli analizė gali pagelbėti, parenkant adekvačias atsakomąsias priemones, užkertančias kelius grėsmėms ir sumažinant jų sukeliamą riziką iki priimtino lygio.

Atsakomosios priemonės padeda kiek įmanoma labiau sumažinti riziką ir įgyvendinti turto valdytojų informacijos saugumo politiką. Nors ir turto apsaugai taikomos pačios tobuliausios atsakomosios priemonės, vis tiek išlieka tam tikra liekamoji rizika, kuria tam tikromis aplinkybėmis gali pasinaudoti grėsmės. Valdytojai stengsis kiek įmanoma sumažinti šią riziką ir reikalui esant, taikyti papildomus apribojimus. Valdytojai turi įsitikinti, kad jų taikomos atsakomosios priemonės užtikrins adekvačią turto apsaugą nuo išaiškintų grėsmių neigiamo poveikio. Patys turto valdytojai ne visada pajėgūs įvertinti visus taikomų atsakomųjų priemonių aspektus, todėl dažnai jie gali paprašyti ekspertų juos tinkamai įvertinti. Tokio

įvertinimo pasėkoje, ekspertai pateikia išvadą ar parinktos adekvačios atsakomosios priemonės ir ar galima jomis pasitikėti. Pasitikėjimas atsakomosiomis priemonėmis yra tokia charakteristika, kuri leidžia valdytojams būti tikriems, kad jų valdomas turtas yra tinkamai apsaugotas, įvertinant liekamąją riziką, kuri yra jiems priimtina. Įvertinimo koncepcija ir ryšiai su saugumo elementais pavaizduoti 2.8 paveiksle.



2.8 pav. Įvertinimo koncepcija ir ryšiai

Kadangi už turtą yra atsakingi jo valdytojai, jie privalo sugebėti apginti savo priimtą sprendimą dėl liekamosios rizikos jų valdomam turtui ir tinkamai šį sprendimą teisiškai įforminti, nes gali tekti kada nors pateikti tokį sprendimą kaip įrodymą.

Turtas šiuo atveju suprantamas kaip informacija, kuri informacinių technologijų pagalba yra apdorojama, perduodama ir saugoma tam, kad patenkintų tam tikrus valdytojo keliamus reikalavimus. Todėl informacijos valdytojas privalo reikalauti, kad bet koks šios informacijos platinimas ir modifikavimas būtų griežtai kontroliuojamas, naudojant įvairias kontrolės priemones, kad užkirstų kelią įvairioms grėsmėms, kurios kėsinasi į šios informacijos saugumą. Todėl visada, įsigyjant, įdiegiant ar kuriant naujas informacines sistemas ir technologijas, kurios naudojamos įvairioms organizacijos veikloms realizuoti, turi būti kreipiamas dėmesys į saugumo priemones, kurios gali ir turi būti realizuotos šiose sistemose ir šias saugumo priemones reikia tinkamai įvertinti. Pageidautina sudaryti tokių naujai pradėtų naudoti produktų saugumo aspektų katalogą, kad palengvintų darbą, įvertinant saugumo aspektus, kai šie produktai bus diegiami kitose informacinėse sistemose ar kai bus atliekamas jų auditas.

Darbuotojai, atliekantys informacinių sistemų ir technologijų auditą, turi turėti visus informacijos valdytojo įgaliojimus, kurie reikalingi pateikiant išvadas, ar naujai diegiamos sistemos ir technologijos atitinka reikalavimus, keliamus atsakomosioms saugumo priemonėms ir priimant sprendimą, ar saugumo priemonės tinkamai realizuotos ir šios sistemos bei technologijos gali būti eksploatuojamos.

2.5. PAGRINDINIAI INFORMACIJOS SAUGUMO PRINCIPAI

Vienas iš svarbiausių elementų, leidžiančių sėkmingai įveikti nuolat atsinaujinančias saugumo problemas - **organizacijos informacijos saugumo kultūros suformavimas**. Dėmesys, kuris skiriamas informacijos saugumo užtikrinimui, turi būti koncentruojamas jau nuo pat informacinių sistemų ir infrastruktūros projektavimo pradžios. Turi būti įgyvendintas visiškai naujas mąstymo ir veikimo modelis, kuris reiškia, kad informacijos saugumo problemų jokiais būdais nebegalima spręsti „atgaline data", kadangi visuomenės gyvenimas diena iš dienos vis labiau priklauso nuo informacinių technologijų, kurių pagalba gyventojams, verslo subjektams ir kitoms valstybės institucijoms teikiama vis daugiau ir daugiau įvairių elektroninių paslaugų. Informacijos teikimas tampa tokiu pat svarbiu produktu kaip ir elektros energijos, vandens, dujų ir kt. Informacijos saugumas turi būti užtikrintas tokiu lygiu, kad nebūtų pažeisti visų, informacijos mainuose dalyvaujančių pusių, interesai. Kiekvienas darbuotojas, nuo aukščiausiojo vadovo iki žemiausio rango darbuotojo, turi aiškiai suvokti grėsmes, kylančias organizacijos informacijos saugumui ir žinoti preventyvines apsaugos priemones. Kiekvienas jų privalo prisiimti atsakomybę ir imtis veiksmų, siekiant užtikrinti informacijos saugumą.

Siekiant stimuliuoti saugumo užtikrinimo kultūros formavimąsi ir tobulinimą, kiekvienos organizacijos vadovybė turi aiškiai suprasti ir skirti vis didesnį prioritetą saugumo užtikrinimo planavimui ir valdymui. Žemiau pateikiami devynis tarpusavyje glaudžiai susiję ir vienas kitą papildantys informacinių sistemų ir tinklo saugumo principai, išdėstyti Ekonominio bendradarbiavimo ir plėtros organizacijos (*Organization for Economic Co-operation and Development)* direktyvoje[85]. Jie skirti visų lygių informacinių sistemų naudotojams, nuo kiekvieno iš jų užimamų pareigų, priklausys jų vykdomos funkcijos ir vaidmenys, užtikrinant informacijos saugumą. Visi šio proceso dalyviai tik laimės, susipažinę su nauja papildoma informacija ir jie turės naudos, įgiję naujų žinių, kurios padės jiems giliau suprasti informacijos saugumo užtikrinimo problemas ir sėkmingai pritaikyti žinias praktinėje veikloje. Priemonės ir

[85] OECD Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security http://www.oecd.org/dataoecd/16/22/15582260.pdf; prisijungimo laikas: 2004-11-10.

pastangos, didinančios informacinių sistemų ir tinklų saugumą, neturi prieštarauti tokiems demokratinės visuomenės principams, kaip laisvas apsikeitimas duomenimis ir asmeninio gyvenimo privatumas.

Pirmas principas – sąmoningumas (*Awareness*). Proceso dalyviai turi įsisąmoninti informacinių sistemų ir tinklų saugumo užtikrinimo būtinumą ir suprasti, ką jie gali padaryti saugumo padidinimui. Rizikos faktorių ir egzistuojančių saugumo priemonių supratimas, tai kaip pirmoji „gynybos linija", užtikrinant informacinių sistemų ir tinklų saugumą. Informacines sistemas ir komunikacinius tinklus veikia tiek vidinės, tiek ir išorinės rizikos. Proceso dalyviai turi įsisąmoninti, kad saugumo sistemos sutrikimas, gali padaryti žymią žalą visai sistemai ir tinklams, kurią jie kontroliuoja. Žala gali būti padaryta ir kitoms informacinėms sistemų ir tinklų vartotojams, kadangi dauguma informacinių sistemų dirba glaudžioje sąveikoje. Proceso dalyviai turi žinoti savo sistemos konfigūraciją, kur yra sistemos atnaujinimai, jų valdomos sistemos vietą tinkle ir atitinkamus veiksmus, kurie privalo būti naudojami, siekiant užtikrinti informacijos saugumą, o taip pat kitų proceso dalyvių poreikius ir reikalavimus.

Antrasis principas – atsakomybė (*Responsibility)*. Už informacinių sistemų ir tinklų saugumą atsako visi šio proceso dalyviai. Tarpusavyje sąveikaujančios lokalios ir globalios informacinės sistemos ir tinklai vaidina svarbų vaidmenį užtikrinant visų dalyvių normalų darbą ir šie dalyviai turi suprasti savo atsakomybę už informacinių sistemų ir tinklų saugumo užtikrinimą. Jie turi atsakyti už savo veiksmus pagal jiems priskirtas funkcijas ir vaidmenis. Proceso dalyviai privalo reguliariai analizuoti savo pačių politiką, praktiką, priemones ir procedūras ir įvertinti, kiek jos atitinka tos dienos situacijai. Tie, kurie projektuoja, diegia programinę įrangą ir atlieką informacinių sistemų bei tinklų priežiūrą, savo darbe turi skirti dėmesį informacinių sistemų ir tinklų saugumo užtikrinimo klausimams ir laiku pateikti atitinkamą informaciją, įskaitant atnaujinimus, tam, kad vartotojai galėtų geriau suprasti naujos programinės įrangos ar jos versijų ir teikiamų paslaugų privalumus ir galimybes, įtakojančias saugumo užtikrinimą, o taip pat ir savo įsipareigojimus saugumo užtikrinimui.

Trečiasis principas - reagavimas (*Response*). Proceso dalyviai, bendradarbiaudami su kitais proceso dalyviais, privalo nedelsdami imtis būtinų priemonių, užkertant kelią, išsiaiškinant ir reaguojant į incidentus, galinčius pažeisti informacinių sistemų ir tinklų saugumą. Įvertinant tą faktą, kad informacinės sistemos ir tinklai vieni su kitais sujungti ir vienas nuo kito priklauso, ir potencialią galimybę, kad šioms sistemoms, per labai trumpą laiką gali būti padaryti milžiniški pažeidimai, proceso dalyviai privalo savalaikiai, rodydami geranoriškumą tarpusavyje glaudžiai bendradarbiauti, reaguojant į incidentus, pažeidžiančius jų

saugumą. Jie privalo vienas su kitu dalintis žiniomis apie grėsmes ir pažeidžiamas vietas, o taip pat vadovautis procedūromis, leidžiančiomis greitai ir veiksmingai suderinti veiksmus, užkertant kelius ir išsiaiškinant incidentus, pažeidžiančius saugumą ir efektyviai į juos reaguoti. Tais atvejais, kai tik yra įmanoma, būtina pasinaudoti tarptautiniu bendradarbiavimu ir informacija.

Ketvirtasis principas – etika (*Ethics*).Visi proceso dalyviai privalo įvertinti kitų asmenų ir organizacijų teisėtus interesus. Tai, kad informacinės sistemos ir tinklai mūsų visuomenėje yra labai paplitę, proceso dalyviai turi įsisąmoninti, kad jų veikimas ar neveikimas gali atnešti žalą kitiems asmenims ir organizacijoms. Todėl labai svarbu etiškas elgesys ir proceso dalyviai privalo siekti atidirbti ir įdiegti optimaliausius darbo metodus ir stimuliuoti tokį elgesį, kuriuo įsisąmoninama būtinybė siekti saugumo ir gerbti teisėtus kitų interesus.

Penktasis principas – demokratija (*Democracy*). Užtikrinant informacinių sistemų ir tinklų saugumą neturi būti prieštaravimų su demokratinės visuomenės pagrindinėmis taisyklėmis. Saugumas turi būti įgyvendintas tokiu būdu, kad derintųsi su demokratinės visuomenės vertybėmis, tokiomis kaip privatumas, laisvas pasikeitimas nuomonėmis ir idėjomis, laisvas pasikeitimas informacija, informacijos ir ryšių konfidencialumas, reikiama asmeninės informacijos apsauga, atvirumas ir informacinis skaidrumas.

Šeštasis principas - rizikos įvertinimas (*Risk Assessment*). Proceso dalyviai privalo nuolatos įvertinti riziką. Rizikos įvertinimo proceso eigoje išaiškinamos grėsmės ir labiausiai pažeidžiamos vietos. Toks įvertinimas privalo būti kiek įmanoma visapusiškas, kad būtų galima įvertinti vidinius ir išorinius faktorius, įtakojančias saugumą. Rizikos įvertinimas leidžia nustatyti priimtinausią rizikos lygį ir padėti parinkti atitinkamas situacijų, kai kyla grėsmė informacinių sistemų ir tinklų saugumui, valdymo priemones ir metodus, tuo pačiu įvertinti saugomos informacijos charakterį ir svarbumą. Nuolat augant informacinių sistemų ir tinklų tarpusavio ryšiui ir priklausomumui, rizikos įvertinimo metu reikia įtraukti ir potencialios žalos analizę, kuri gali kilti iš kitų asmenų ir organizacijų, arba kokia žala gali būti padaryta jiems.

Septintas principas – Saugumo projektavimas ir diegimas (*Security design and implementation)*. Proceso dalyviai privalo į saugumą žiūrėti kaip į vieną svarbiausių informacinės sistemos ir tinklų elementų. Siekiant užtikrinti reikiamą saugumo lygį reikia atitinkamai suprojektuoti, įgyvendinti ir koordinuoti sistemas, tinklus ir politikas. Svarbiausia, bet ne vienintelė tokios veiklos kryptis - reikiamų saugumo priemonių ir sprendimų sukūrimas ir įdiegimas, leidžiančių pašalinti arba apriboti potencialią žalą, kurią padarytų nustatytos grėsmės ir silpnosios vietos. Tam tikslui reikalingos saugumo priemonės ir tiek techniniai, tiek

ir ne techniniai sprendimai. Šios priemonės ir sprendimai turi atitikti organizacijos informacinėje sistemoje saugomos informacijos vertei. Saugumo užtikrinimas turi būti viena iš pagrindinių sudedamųjų dalių visų informacinių sistemų ir tinklų produktų ir paslaugų, lygiai taip pat, kaip ir neatskiriama sistemos projektų ir architektūros dalis. Paprastai galutiniam vartotojui projektavimo ir įdiegimo saugumo faktorius reiškia informacinių produktų ir paslaugų reikiamas parinkimas ir sukonfigūravimas.

Aštuntasis principas - saugumo valdymas (*Security management*). Proceso dalyviai privalo kompleksiškai prieiti prie saugumo valdymo. Saugumo valdymas turi remtis rizikos įvertinimu. Jis turi būti dinamiškas, apimantis visus proceso dalyvių veiklos lygius ir jų darbo aspektus. Jis turi apimti įspėjantį reagavimą į atsirandančias grėsmes, numatyti atitinkamas priemones, nukreiptas užkirsti kelią ir išaiškinti incidentus, bei į juos tinkamai sureaguoti. O taip pat parengti priemones, kurios reikalingos atstatyti sistemas po sutrikimų, atlikti nuolatinę techninę priežiūrą, analizę ir auditą. Informacinių sistemų ir tinklų saugumo užtikrinimo politika, praktika, priemonės ir procedūros privalo būti sukoordinuotos ir integruotos, kad sudarytų logiškai nuoseklią saugumo valdymo sistemą. Reikalavimai saugumo valdymui priklauso nuo proceso dalyvių dalyvavimo lygio, vaidmenų ir funkcijų, egzistuojamos rizikos ir reikalavimų sistemai.

Devintasis principas - pakartotinis įvertinimas (*Reassessment*). Proceso dalyviai privalo analizuoti ir atlikti pakartotiną informacinių sistemų ir tinklų saugumo įvertinimą, o taip pat padaryti atitinkamus politikos, praktikos, priemonių ir procedūrų pakeitimus saugumo srityje. Nuolatos atrandami nauji, besikeičiantys grėsmių faktoriai ir labiausiai pažeidžiamos vietos. Proceso dalyviai privalo nuolatos analizuoti, pakartotinai įvertinti, daryti pakeitimus visame saugumo užtikrinimo priemonių komplekse, kad atsilaikytų prieš nuolatos besikeičiančius rizikos faktorius.

Labai svarbu, kad šiuos informacijos saugumo principus ir kylančias grėsmes informacijos saugumui labai gerai suvoktų Lietuvos Respublikos aukščiausiųjų valdžios institucijų vadovai, kaip tai suvokia Jungtinių Amerikos Valstijų, Kanados, D. Britanijos ir kitų šalių vyriausybės. Labai svarbu, kad informacijos saugumo užtikrinimo kultūra būtų formuojama valstybiniu lygiu. Be šių principų įsisąmoninimo, neįmanoma kalbėti apie sėkmingą informacijos saugumo sistemos įgyvendinimą valstybės valdymo institucijose.

2.6. VIEŠŲJŲ E. PASLAUGŲ SAUGUMO VALDYMO TIKSLAI

Teikiant e. viešąsias paslaugas vienas iš svarbiausių saugumo valdymo tikslų yra

tinkama kreipties kontrolės politika. Kreipties kontrolei taikomi reikalavimai turi būti aiškiai apibrėžti ir dokumentuoti. Kiekvieno vartotojo kreipties taisyklės ir teisės turi būti aiškiai išdėstytos kreipties politikoje. Galima nustatyti tokius pagrindinius e. viešųjų paslaugų saugumo reikalavimus:

1. **Kreipties kontrolė.** Kreiptis vartotojui prie e. viešųjų paslaugų aplikacijų ir turto leidžiama tik tiek, kiek reikalingas jam gauti kokybiškas paslaugas. Kreipties kontrole siekiama įsitikinti, kad vartotojas vieną kartą save identifikavęs ir patvirtinęs tapatybę, gali prieiti tik prie tų sistemos dalių ir turto, kurie yra būtini atlikti sankcionuotai užduočiai.

2. **Vartotojo kreipties valdymas.** Valdytojas vykdo pilną kontrolę per kreipties teisių suteikimą, reikalingą e. viešųjų paslaugų atlikimui. Kreipties valdymu siekiama įvesti arba pašalinti vartotoją kai tik būtina, be vartotojo žinios. Techniškai tai siejasi su reikalavimu panaikinti kreiptį apibrėžtai paslaugai. Ši procedūra turi apimti visas vartotojo kreipties raidos ciklo stadijas nuo pradinio naujų vartotojų įregistravimo iki galutinio tų vartotojų, kuriems daugiau nebereikia kreiptis į informacines sistemas ir e. viešąsias paslaugas.

3. **Vartotojų identifikavimas ir autentiškumo patvirtinimas.** Atskaitingos e. viešosios paslaugos turi būti prieinamos tik įgaliotiems vartotojams ar sistemoms. Keliami reikalavimai techninėms priemonėms, siekiant užtikrinti, kad atlikti e. viešąsias paslaugas galima tik teisingai įvedus kreipties kredencialus. Kiekvienas vartotojas privalo turėti unikalų vartotojo identifikatorių. Vartotojo autentiškumui patvirtinti naudojamos įvairios procedūros - vartotojo slaptažodžiais, šifravimo priemonės, atminties atpažinimo ženklai, intelektualiosios kortelės, biometrinės technologijos, autentiškumo patvirtinimo protokolai ir pan.

4. **Vartotojų registravimas.** Leidimas kreiptis dėl e. viešosios paslaugos atlikimo, suteikiamas tik tiems, kurių sąžiningumas tinkamai pripažintas. Reikalavimas techninėms ir procedūrinėms priemonėms, siekiant užtikrinti, kad vartotojas tinkamai identifikuotas ir patvirtintas jo autentiškumas.

5. **Pripažinimas.** Sutarties šalys turi turėti galimybę aiškiai atsekti transakcijų eigą. Užkertamas kelias mėginimams paneigti nesąžiningo naudojimo e. viešąja paslauga atsakomybę. Taip pat vartotojai turi būti garantuoti, kad paslaugų tiekėjas negali nepripažinti savo įsipareigojimų, taip kaip ir paslaugų tiekėjai turi būti garantuoti, kad vyriausybė negali nepripažinti savų įsipareigojimų.

6. **Gavimo įrodymas.** Gavėjai aiškiai atseka transakcijų eigą. E. viešųjų paslaugų

vartotojai ir teikėjus privalo turėti galimybę įsitikinti, kad transakcija pilnai priimta ir įvykdyta, ir ji negali būti traktuojama kaip klaidinga, kurią reikia sugrąžinti ar atmesti.

7. Įsipareigojimas patikimai atlikti paslaugą. Valdžios institucija įsipareigoja apsaugoti e. viešąją paslaugą nuo galimų vagysčių ar apgavysčių. Autorizuotas klientas, besinaudojantis e. viešąja paslauga privalo būti įsitikinęs, kad jo atliekami mokėjimai bus prideramai kontroliuojami ir nebus pažeidžiami nesąžiningiems mokėjimams atlikti. Vartotojo kredencialai ir kita asmeninė informacija bus tinkamai apsaugota.

8. Privatumas ir konfidencialumas. Asmeninė ar kita informacija, kuri pateikiama paslaugos vykdymui, negali būti be vartotojo leidimo skelbiamas ar rodoma. Vartotojo pateikti duomenys e. viešosios paslaugos atlikimui privalo būti tinkamai apsaugoti, kaip yra numatyta duomenų apsaugos įstatymuose. Paslaugos teikėjas privalo saugoti šią informaciją patikimai saugiai.

9. Vientisumas. Informacija gauta tiesiai ar priimta per e. viešąsias paslaugas yra nepakeista ar kitaip pažeista. Vartotojas turi būti įsitikinęs informacijos ir gautų konsultacijų tikslumu, užbaigtumu ir kompetencija, taip tuo, kad išsiųsta informacija buvo teisingai priimta. Tai liečia ir klaidingą informaciją ir informaciją, kuri saugojimo, apdorojimo ar pernešimo metu buvo netyčia ar tyčia pakeista.

10. Paslaugų prieinamumas. Turi būti užtikrintas nepertraukiamas priėjimas prie e. viešųjų paslaugų. E. viešųjų paslaugų vartotojai privalo turėti galimybę nepertraukiamai naudotis paslaugomis ir tikėti valdžios įsipareigojimais užtikrinti tokias paslaugas.

11. Informacijos prieinamumas. Turi būti užtikrintas nepertraukiamas priėjimas prie duomenų, naudojamų e. viešosioms paslaugoms atlikti. Visi e. viešųjų paslaugų duomenys yra svarbūs ir privalo būti išsaugoti incidentų, nerūpestingo elgesio, tyčinių veiksmų ar įrangos gedimo metu.

12. Paslaugų apsauga. E. paslaugos ir bendras turtas privalo būti apsaugotas nuo išorės trukdžių ir įsiskverbimų, o taip pat privalo būti atitinkamai apsaugotos nuo išorės atakų, nukreiptų prieš šių paslaugų taikomąsias programas ar komunikacinių tinklų infrastruktūrą.

13. Efektyvus auditas ir apskaita. Turi būti saugojami viešųjų e. paslaugų svarbių transakcijų įrašai. Visuotinis reikalavimas saugoti tikrus svarbių įvykių įrašus, kurie audito metu galėtų būti peržiūrimi. Iš dalies jie gali būti naudojami ir vartotojų apskaitai. Tai turi apimti būdingus įrašus, siekiant įrodyti, kad yra atliekama privatumo ir konfidencialumo

prižiūra.

2.7. VIEŠŲJŲ E. PASLAUGŲ SAUGUMAS VMI

IVPK užsakymu UAB „Siemens“ parengtame „Elektroninių viešųjų paslaugų modelyje“[86] aprašomas VMI pavyzdys, kaip teikiant e. viešąsias paslaugas - užpildant ir siunčiant deklaracijas elektroniniu būdu, nėra būtinas elektroninio parašo sertifikavimo centras. VMI pasiremdama komercinių bankų e. bankininkystės patirtimi, pripažino jose naudojamą e. parašą, ir tuo pačiu sudarė galimybę fiziniams asmenims pajamų ir turto deklaracijas teikti elektroniniu būdu. VMI viršininko 2004 m. kovo 10 d. įsakymu Nr. VA-33[87] patvirtintoje tvarkoje patvirtinama, kad elektroniniu būdu asmens sudaryta sutartis, panaudojant asmens turimas banko interneto bankininkystės paslaugų vartotojo identifikavimo priemones (identifikavimo kodus, slaptažodžius ir pan.), turi tokią pat juridinę galią, kaip ir asmens pasirašyta sutartis. Taip pat nurodoma, kad „*asmens elektroniniu būdu pateikta Deklaracija turi tokią pat juridinę galią, kaip Asmens pasirašyta ir įprasta tvarka pateikta deklaracija*“[88] (12 punktas). Tačiau išlieka esminis klausimas, kas atsako už duomenų praradimą ar iškraipymą.

To paties įsakymo VI skyriuje „Šalių atsakomybė“ sakoma, kad VMI neatsako už tai „*kad dėl telekomunikacijų tinklų gedimų Asmuo negalės prisijungti prie EDS arba dėl tokių gedimų bus prarasti ar iškraipyti elektroniniu būdu teikiamų deklaracijų duomenys“* ir „*už Deklaracijų duomenų pakeitimą, įvykusį jų pateikimo metu“*[89]. Taigi šiuo atveju pačiai VMI, kaip e. viešosios paslaugos teikėjai, dėl duomenų pakeitimo, dingimo ar iškraipymo elektroninės deklaracijos siuntimo metu tiesiogiai jokių neigiamų pasekmių nekyla. Vienintelė svarbesnė neigiama pasekmė yra nevisiškai tikslios informacijos sukaupimas statistikos tikslais.

Direktyva 2002/58/EB[90] numato, kad „*viešai prieinamų elektroninių ryšių paslaugų teikėjas turi imtis tinkamų techninių ir organizacinių priemonių, kad užtikrintų savo paslaugų saugumą, o tam tikrais atvejais tokių priemonių imasi kartu su viešųjų ryšių tinklo teikėju, kad užtikrintų ir paties tinklo saugumą”*. Toje pačioje Direktyvoje taip sakoma, kad „*iškilus tam tikrai tinklo saugumo pažeidimo rizikai, viešai prieinamų elektroninių ryšių paslaugų teikėjas*

[86] Elektroninių viešųjų paslaugų siekiamo modelio aprašymas, http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_siekiamasV1.pdf; prisijungimo laikas: 2004-10-10.
[87] Dėl Gyventojų deklaracijų ir prašymų formų teikimo elektroniniu būdu tvarkos patvirtinimo//Valstybės Žinios, 2004, Nr. 40-1319.
[88] Ten pat.
[89] Ten pat.
[90] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37, 31/07/2002.

turi informuoti abonentus apie šią riziką, o tais atvejais, kai paslaugos teikėjo taikomos priemonės neapima šios rizikos – informuoti abonentus apie visas įmanomas teisės gynimo priemones, nurodant ir galimas jų kainas".

Taigi vadovaujantis šios direktyvos nuostatomis riziką ir nuostolius dėl elektroninių duomenų praradimo, įvykusio jų siuntimo metu dėl telekomunikacinių tinklų gedimo, turėtų prisiimti telekomunikacinių tinklų operatorius, o e. viešųjų paslaugų teikėjas – VMI nuo šios rizikos apsaugotų paslaugų vartotoją, nukreipdamas reikalavimą į telekomunikacinių tinklų operatorių. Be to, tokia VMI nuostata dėl atsakomybės už duomenų pakeitimą ir iškraipymą, iš esmės diskriminuoja privačiuosius ūkio subjektus, tame tarpe ir komercinius bankus, teikiančius e. komercijos paslaugas, kur jie priversti prisiimti visą su duomenų dingimu susijusią riziką. Juk nepriklausomai nuo to ar tai valstybinės institucija, ar verslo įmonė, jų pareiga profesinėje veikloje elgtis apdairiai ir rūpestingai, garantuoti šios veiklos patikimumą, efektyvumą ir saugumą. Pagal dabartinę nuostatą VMI už duomenų pakeitimą dėl ryšio gedimų neatsako visais atvejais, todėl ji ir nėra suinteresuota apie tokius atvejus informuoti vartotojų, kuriems tenka visa tokia rizika.

Minėtame „Elektroninių viešųjų paslaugų modelyje" sakoma, kad būtų protinga, jeigu VMI susietų savo, kaip atsakingo e. viešosios paslaugos teikėjo (tai svarbu, stiprinant gyventojų pasitikėjimą valdžios institucijų teikiamoms e. paslaugoms) atsakomybę su paties mokesčių mokėtojo pareiga aktyviai domėtis tuo, kaip jo elektroniniu būdu pateikti duomenys yra atspindėti VMI duomenų bazėje. Mokesčių mokėtojas turi turėti galimybę, VMI duomenų bazėje pasitikrinti savo deklaracijos duomenis. Tam jam turi būti duotas nustatytas terminas. Jeigu asmuo per šį nustatytą terminą neįspėja VMI apie tai, kad jo deklaracijos duomenys VMI duomenų bazėje atspindėti neteisingai, praėjus šiam terminui laikoma, kad VMI duomenų bazėje įregistruoti deklaracijos duomenys atitinka duomenis, elektroniniu būdu pateiktoje deklaracijoje. Taip pat, VMI vadovaudamasi principu, kad už duomenų iškraipymą, įvykusį dėl telekomunikacinių tinklų gedimų, riziką prisiima tų tinklų valdytojas – ryšio operatorius, tai VMI, kaip e. paslaugos teikėjas, nuo tokios rizikos apsaugotų šios paslaugų gavėją, įgydama reikalavimo teisę į tinklo valdytoją, turėtų:

1. *užtikrinti visų rūšių ir formų informacijos apsaugą jos įregistravimo, perdavimo ryšių linijomis, saugojimo, apdorojimo ir naudojimo metu;*
2. *užkirsti kelią slaptos ir neskelbtinos (konfidencialios) informacijos atskleidimui;*
3. *užtikrinti saugomos informacijos tikslumą (t. y. atitikti duomenims, kuriu pagrindu ši informacija įrašyta i VMI duomenų bankus);*

4. užtikrinti asmens duomenų apsaugą nuo bet kokio neteisėto tvarkymo. [91]

Remiantis Lietuvos Respublikos elektroninių ryšių įstatymo 62 straipsniu[92], „*Viešųjų elektroninių ryšių paslaugų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų paslaugų saugumui užtikrinti, o prireikus - kartu su viešųjų ryšių tinklų teikėjais imtis tokių pat priemonių viešųjų ryšių tinklų saugumui užtikrinti. Šios priemonės turi užtikrinti iškilusią grėsmę atitinkantį saugumo lygį“* ir „*Iškilus ypatingai elektroninių ryšių tinklo ar jo dalies saugumo pažeidimo grėsmei, viešųjų elektroninių ryšių paslaugų teikėjas privalo informuoti abonentus apie tokią grėsmę ir tais atvejais, kai paslaugų teikėjo taikomos priemonės nepanaikina grėsmės kilmės priežasčių, taip pat informuoti abonentus apie visas įmanomas gelbėjimo priemones ir nurodyti tikėtinas jų kainas“*.

2.8. INFORMACIJOS SAUGUMO TARNYBA

Mažose organizacijose informacijos saugumu tuo paprastai gali pasirūpinti vienas žmogus, taip vadinamas duomenų saugos įgaliotinis[93], o didelėse gali būti įkuriami atskiri skyriai. Šiuo metu vyrauja kelios šios organizacinės problemos sprendimo kryptys:

- informacijos saugumo problemas sprendžia organizacijos IT skyriaus darbuotojai;
- informacijos saugumo problemas sprendžia organizacijos tarnybos, kurios atsakingos už bendrą - fizinį ir informacijos, saugumą;
- informacijos saugumo problemas sprendžiamos aukščiausiu vadovybės lygiu. Įvedamos dvi labai svarbios specialistų pozicijos - informacijos saugumo direktorius (*Chief Information Security Officer - CISO*), atsakingas už organizacijos informacijos saugumo politikos, atitinkančios organizacijos tikslus ir uždavinius, sukūrimą ir įgyvendinimą ir informacijos saugumo tarnybos vadovas (*Business Information Security Officer - BISO*), atsakingas už informacijos saugumo politikos praktinį įgyvendinimą padalinių lygyje.

Kaip rodo užsienio kompanijų patirtis[94] efektingiausiai informacijos saugumo užtikrinimo funkcijas organizacijoje atlieka tam tikslui sukurti padaliniai, turintys reikiamus įgaliojimus ir

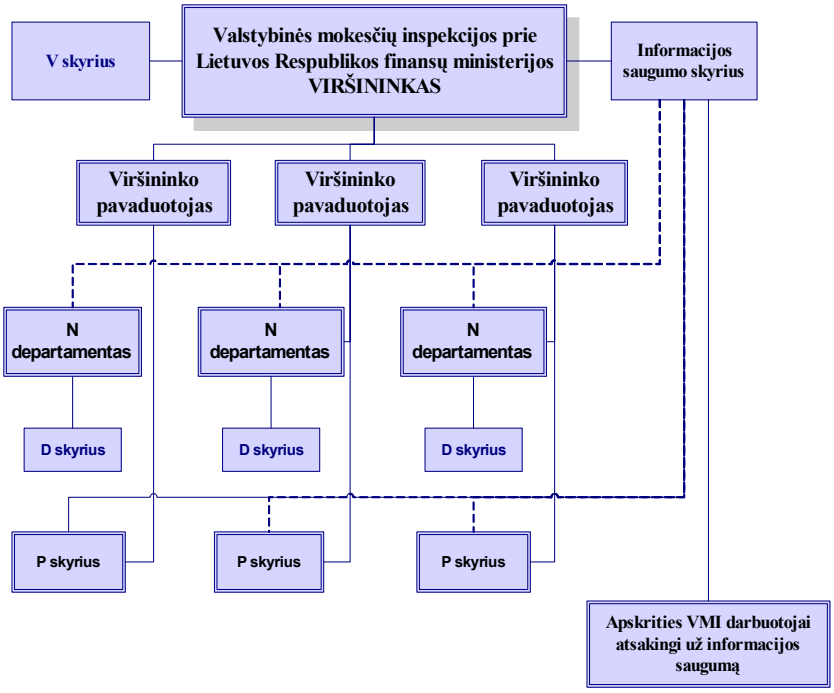
[91] Siekiamas elektroninių viešųjų paslaugų modelis. http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_siekiamasV1.pdf; prisijungimo laikas: 2004-11-19.

[92] Lietuvos Respublikos elektroninių ryšių įstatymas//Valstybės Žinios, 2004, Nr. 69-2382.

[93] Dėl Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo//Valstybės Žinios, 2001, Nr. 110-4006.

[94] Global Information Security Survey, KPMG, 2002 http://www.kpmg.com/microsite/informationsecurity/isssurvey.html; prisijungimo laikas: 2004-11-17.

vadovybės palaikymą. 2.9 paveiksle pateikiama rekomendacija, kokią vietą VMI organizacinėje struktūroje galėtų užimti Informacijos saugumo skyrius.



2.9 pav. Informacijos saugumo skyriaus vieta organizacijos struktūroje.

Pagrindinis informacijos saugumo direktoriaus uždavinys – technologinių, informacinių ir organizacijos veiklos rizikų įvertinimas ir jų valdymas. Jis turi sugebėti įvertinti organizacijos informacinių aktyvų (turto) dydį ir vertę, identifikuoti ir valdyti rizikas, atsižvelgdamas į organizacijos tikslus ir uždavinius. Pagrindinės jo funkcijos galėtų būti tos, kurias apibrėžia Rusijos informacijos saugumo specialistai *S. A. Petrenko* ir *S.B. Simonov'as*[95]:

- organizacijos informacijos saugumo koncepcijos ir politikos kūrimas, įskaitant reglamentus, standartus, metodikas ir instrukcijas;
- organizacijos informacijos aktyvų klasifikavimo principų sukūrimas ir jų saugumo įvertinimas;
- organizacijos informacijos rizikų įvertinimas ir jų valdymas;
- organizacijos darbuotojų informacijos saugumo mokymų organizavimas, instruktavimas ir žinių tikrinimas, įgyvendinant informacijos saugumo politiką;
- padalinių vadovų konsultavimas informacijos rizikų valdymo klausimais;

[95] С. А. Петренко, С. В. Симонов, «Управление информационными рисками. Экономически оправданная безопасность». — М.: «Компания АйТи», «ДМИ Пресс», 2004

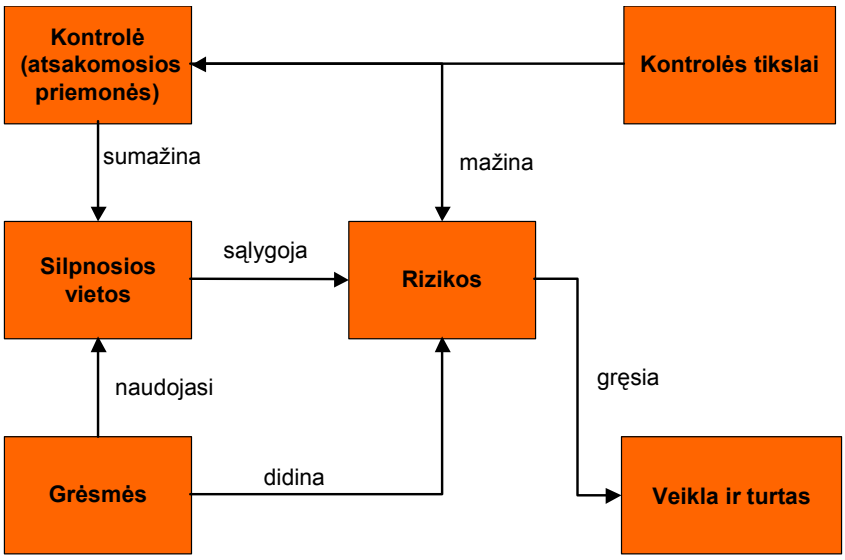
- atskirų organizacijos padalinių politikų ir reglamentų derinimas;
- dalyvavimas ekspertų tarybose, įvertinant organizacijos veiklos rizikas;
- informacinių technologijų padalinių kontroliavimas, ataskaitų ir kitų dokumentų tvirtinimas;
- bendradarbiavimas su fizinio saugumo ir personalo tarnybomis, sprendžiant įvairius informacijos fizinio saugumo ir personalo priėmimo klausimus;

Informacijos saugumo direktorius turėtų priklausyti organizacijos vadovų lygiui, kad sugebėtų tinkamai įvertinti veiklos poreikius ir informacijos saugumo reikalavimus, įvertinti IT vystimąsi, informacinių nusikaltėlių aktyvumą ir naudojamus įsilaužimo metodus, įstatymų kaitą, vykdytojų galimybes. Reikia atminti, kad dažnai organizacijos veikla gali prieštarauti ir kirstis su informacijos saugumo reikalavimais, todėl informacijos saugumo direktorius turi sugebėti organizacijos vadovybei išaiškinti techninius informacijos saugumo klausimus ir problemas. Neužtenka turėti vien specialias technines, ekonomines ar vadybines žinias, jis turi turėti tam tikras asmenines ypatybes - sugebėti analitiškai mąstyti, turėti strateginio vadovavimo sugebėjimus, būti lojalus organizacijai.

3. INFORMACIJOS SAUGUMO TYRIMAS

3.1. INFORMACINIŲ SISTEMŲ AUDITAS VMI

Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos (VMI) 2001 – 2004 metų strateginiame plane teigiama, kad be dabartinių informacijos technologijų neįmanoma užtikrinti tinkamo veiklos efektyvumo ir tinkamai pasirengti mokesčių informacijos mainams su Europos Sąjungos informacinėmis sistemomis (VIES, SEED ir kt.). Tuo metu buvusi Integruotos mokesčių informacinės sistemos (IMIS) informacinė architektūra bei infrastruktūros greitaveika neleido patenkinti integravimo į ES informacines sistemas reikalavimų. Todėl VMI vadovybė, siekdama objektyviai įvertinti VMI naudojamų informacinių sistemų padėtį, 2001 m. lapkričio - 2002 m. sausio mėnesiais, su UAB „*Arthur Andersen*" pagalba, atliko VMI informacinių sistemų auditą. Pagrindinis šio audito tikslas - įvertinti informacinių technologijų valdymo atitikimą tarptautiniams standartams ir geriausiai patirčiai keturiose srityse: organizavimo ir planavimo, įsigijimo ir diegimo, palaikymo ir priežiūros ir stebėjimo (monitoringo). VMI informacinių sistemų auditas atliktas pagal Informacinių sistemų audito ir kontrolės asociacijos ISACA (*Information Systems Audit and Control Association & Foundation*) sukurtą Informacijos ir susijusių technologijų kontrolės tikslų metodologiją COBIT (*Control Objectives for Information and Related Technologies*) (2 priedas). Auditoriai naudojo rizikos įvertinimo modelį, kurio elementai ir jų tarpusavio ryšiai analogiški saugumo modelio elementams, kurie buvo pateikti šio darbo II skyriuje (3.1 pav.).



3.1 pav. Rizikos įvertinimo modelis

Kiekviena VMI informacinių technologijų veikla buvo įvertinta pagal jos svarbos (didelė, vidurinė, maža), brandos lygio (0-5) ir rizikos (didelė, vidurinė, maža) kriterijus (3.2 pav.).

Lygis	Paaiškinimas	Svarba		
		Didelė	Vidutinė	Žema
0	**Neegzistuoja**. Visiškai nėra jokių atpažįstamų procesų. Organizacijoje nėra suvokimo, kad egzistuoja svarstytina problema	Didelė rizika	Didelė rizika	Vidutinė rizika
1	**Pradinis/atsitiktinis**. Yra požymių, kad organizacija suvokia, esant svarstytinas problemas, tačiau standartinių procesų nėra, pasitenkinama atsitiktiniais sprendimais, taikomais kiekvienu atskiru atveju. Vadovybės požiūris yra nesistemingas.	Didelė rizika	Vidutinė rizika	Vidutinė rizika
2	**Kartotinis intuityvusis**. Procesai yra išvystyti tiek, kad skirtingi darbuotojai atlieka tas pačias užduotis pagal panašias procedūras. Nėra formalaus standartinių procedūrų mokymo ir komunikavimo, atsakomybė priskiriama atskiriems darbuotojams ir pasikliaujama šių darbuotojų žiniomis, todėl galimos klaidos.	Vidutinė rizika	Vidutinė rizika	Maža rizika
3	**Nustatytas procesas**. Procedūros yra standartizuotos ir dokumentuotos, apie jas mokymų metu informuojami visi darbuotojai. Vadovavimasis procedūromis paliekamas darbuotojų atsakomybei, o nukrypimai nėra pastebimi. Pačios procedūros yra nesudėtingos ir formaliai aprašo egzistuojančią darbo tvarką.	Vidutinė rizika	Maža rizika	Maža rizika
4	**Valdomas procesas**. Yra įmanoma stebėti ir išmatuoti veiklos atitikimo nustatytoms procedūroms lygį ir įmanoma imtis veiksmų, jei kuris nors procesas vyksta neefektyviai. Procesai pastoviai tobulinami ir kartais atitinka geriausias praktikas. Kai kur yra naudojamos automatizuotos stebėjimo priemonės.	Maža rizika	Maža rizika	Maža rizika
5	**Optimizuotas procesas**. Procesai išgryninti iki geriausių praktikų lygio, pastoviai tobulinant veiklą ir lyginant su kitomis organizacijomis savo veiklos modelio brandą. IT integruotos į veiklos procesus ir teikia galimybę organizacijai pagerinti veiklos kokybę ir efektyvumą, leidžia greitai prisitaikyti prie kintančių aplinkos reikalavimų.	Maža rizika	Maža rizika	Maža rizika

3.2 pav. Rizikos įvertinimo matrica.

Audito metu buvo apklausta virš 40 VMI darbuotojų, peržiūrėta daugiau kaip 40 vidaus dokumentų. VMI savo informacinę sistemą plečia, užsakydama informacinių sistemų kūrimo darbus pas išorinius tiekėjus, kurie atlieka ir dalį informacinių technologijų infrastruktūros ir informacinių sistemų priežiūros darbų. VMI informacinių technologijų skyriai patys kuria tik mažesnės apimties taikomąsias programas, skirtas skubių veiklos poreikių patenkinimui, bei atlieka informacinių sistemų projektų valdymo, eksploatacijos bei vartotojų palaikymo darbus. VMI būdinga didelė veiklos automatizavimo poreikių apimtis, dažnas šių poreikių kitimas bei

nepakankamas teminių skyrių specialistų dalyvavimas informacinių sistemų projektuose. Dėl šių priežasčių didėja rizika nespėti laiku paruošti informacinių sistemų tiekėjams kokybiškus funkcinius reikalavimus naujai kuriamoms sistemoms bei atlikti suplanuotus smulkesnių automatizuotų priemonių kūrimo darbus. Audito metu buvo nustatytos tokios VMI informacinių technologijų sričių ir procesų rizikos (3.3 pav.):

Planavimas ir organizavimas	Svarba	Brandos lygis	Rizika
Strateginio IT plano nustatymas	Didelė	2	Vidutinė
Informacinės architektūros nustatymas	Didelė	1	Didelė
Technologijų plėtros krypčių nustatymas	Vidutinė	2	Vidutinė
IT organizacijos ir jos ryšių nustatymas	Didelė	1 - 2	Didelė
IT investicijų valdymas	Vidutinė	1 - 2	Vidutinė
Vadovybės tikslų ir krypčių komunikavimas	Vidutinė	1 - 2	Vidutinė
IT personalo valdymas	Didelė	1 - 2	Didelė
Atitikimo išoriniams reikalavimams užtikrinimas	Vidutinė	0 –1	Vidutinė
Rizikos įvertinimas	Vidutinė	0 –1	Didelė
Projektų valdymas	Didelė	1 - 2	Didelė
Kokybės valdymas	Didelė	1	Didelė
Įsigijimas ir diegimas			
IT sprendimų identifikavimas	Didelė	1 - 2	Didelė
IS įsigijimas ir palaikymas	Didelė	1 - 2	Didelė
IT infrastruktūros įsigijimas ir palaikymas	Vidutinė	2	Vidutinė
IT procedūrų sukūrimas ir palaikymas	Vidutinė	1	Vidutinė
Sistemų įdiegimas ir priėmimas	Didelė	2	Vidutinė
Pakeitimų valdymas	Didelė	1 - 2	Didelė
Aptarnavimas ir palaikymas			
Aptarnavimo lygio nustatymas ir valdymas	Vidutinė	0	Didelė
Aptarnaujančių organizacijų teikiamų paslaugų valdymas	Vidutinė	2	Vidutinė
Sistemos funkcionavimo ir pajėgumų valdymas	Vidutinė	2	Vidutinė
Veiklos tęstinumo užtikrinimas	Didelė	1	Didelė
Sistemos saugumo valdymas	Didelė	1	Didelė
Kaštų apskaita ir valdymas	Vidutinė	1	Vidutinė
Vartotojų apmokymas	Vidutinė	2	Vidutinė
Pagalba ir patarimai vartotojams	Vidutinė	1 - 2	Vidutinė
Duomenų valdymas	Didelė	1 - 2	Vidutinė
Patalpų ir įrengimų valdymas	Maža	3	Maža
IT operacijų valdymas	Vidutinė	1	Vidutinė
Stebėjimas			
IT procesų stebėjimas	Vidutinė	0 - 1	Didelė
Vidinės kontrolės tinkamumo įvertinimas	Maža	1	Vidutinė
Nepriklausomo IT veiklos tinkamumo užtikrinimo gavimas	Maža	0	Vidutinė
Nepriklausomo audito atlikimas	Maža	1	Vidutinė

3.3 pav. Informacinių technologijų sričių ir procesų rizikos įvertinimo rezultatai.

Audito ataskaitoje pateiktos pagrindinės šių procesų išvados bei rekomendacijos 3 priede. Daug dėmesio buvo skiriama informacijos saugumui. Parengtas atskiras „Sistemos saugumo

valdymo“ skyrius, kuriame pabrėžiama, kad VMI sistemos saugumo valdymo procesas turi būti skirtas tenkinti organizacijos veiklos reikalavimą apsaugoti informaciją nuo neleistino panaudojimo, paviešinimo, modifikavimo, sugadinimo ar sunaikinimo. Auditoriai pateikė išvadą, kad „*IS saugumo kontrolės sistema VMI veikia nepakankamai. IS saugumo politika nėra apibrėžta. Informacijos saugumo lygiai neapibrėžti ir nesusieti su Duomenų modeliu. Veiklos padaliniai nėra apibrėžę reikalavimų informacijos saugumui, todėl šie reikalavimai nėra įgyvendinti kuriant IS, ko pasėkoje nesukurtas pagrindas informacijos saugumo užtikrinimui. IS saugumo auditas ir monitoringas nėra atliekami. Nėra paskirtas už IT ir IS saugumą atsakingas darbuotojas*“.

Atsižvelgiant į šias išvadas rekomenduojama VMI priskirti funkciją IT specialistams, kurie „*būtų atsakingi už IS saugumo sistemos (politikos) sukūrimą, įgyvendinimą ir kontrolę. Sukurti ir įgyvendinti saugumo politiką bei ją realizuojančias procedūras. Į IS kūrimo specifikacijas privaloma įtraukti informacijos saugumo reikalavimus. Ši veikla turi būti suderinta su IS ir jų duomenų savininkų priskyrimo iniciatyva*“.

Auditoriai savo ataskaitoje sistemos saugumo valdymui suteikė patį aukščiausią saugumo svarbos ir rizikos laipsnį. Tačiau tuo metu buvusį brandumo lygį įvertino kaip **pradinį arba atsitiktinį**. Tai reiškia, kad organizacija suvokia problemas, tačiau standartizuotų procesų nėra, pasitenkinama tik atsitiktiniais sprendimais, kurie taikomi kiekvienu atskiru atveju. Vadovybės požiūris yra nesistemingas.

Ataskaitos dalyje, skirtoje sistemos saugumo valdymui, buvo pažymėta, kad nepavyko surasti dokumentų, įrodančių, kad VMI turi patvirtintą informacijos (duomenų) klasifikavimo schemą, kurios pagrindu skyrių darbuotojams būtų priskiriamos priėjimo prie atitinkamų duomenų ir funkcijų informacinėje sistemoje teisės. Nors pagal VMI patvirtintą tvarką nauji vartotojai sistemoje registruojami remiantis skyrių vedėjų tarnybiniais raštais, kuriuose yra nurodomos vartotojui reikalingos aplikacijos, tačiau nėra aišku, kokiomis taisyklėmis vadovaujasi skyrių vedėjai, prašydamas darbuotojui suteikti atitinkamas teises į informacines sistemas. Informacinėje sistemoje naudojama vaidmenų (rolių) sistema nėra plačiai pristatyta VMI darbuotojams. Taip pat neaišku kokiomis taisyklėmis remiantis, anuliuojamos teises į tam tikras aplikacijas darbuotojams, pervedamiems dirbti į kitas pareigas ar kitą skyrių. Neaišku, kas yra atsakingas už tokios vartotojų teisių informacinėje sistemoje korekcijos inicijavimą ir įvykdymo kontrolę.

Auditoriai atkreipė dėmesį, kad pagrindinė VMI informacinė sistema yra suprojektuota, įvertinant saugumo reikalavimus: vartotojų autentifikavimą, priėjimo prie sistemos lygio suteikimą, vartotojų veiksmų registravimą. Sistemoje įdiegta speciali „Saugumo" aplikacija, kuria naudodamiesi šios informacinės sistemos administratoriai gali registruoti naujus vartotojus, priskirti juos vartotojų grupėms, suteikti atitinkamas roles ir teises darbui su reikalingomis aplikacijomis bei jų duomenimis. Sistemos vartotojo vardas privalomai susiejamas su VMI darbuotoju, nurodant jo vardą, pavardę, skyrių ir pareigas.

Tačiau administratoriai nenaudoja šios aplikacijos informacinės sistemos vartotojų paskyroms kurti, nes jų požiūriu ši „Saugumo" aplikacija neveikia taip, kaip turėtų. Todėl vietoje šios aplikacijos yra sukurta nuosava programa, kuri registruoja pagrindinės informacinės sistemos vartotojus. Kadangi auditoriams nebuvo pateikta informacija, patvirtinanti, kad ši posistemė yra praėjusi pilną akreditavimo procedūrą, taikomą VMI funkcionuojančioms sistemoms, jie pagrįstai tvirtina, kad tokių skirtingų teisių į IS vartotojams suteikimo posistemių naudojimas VMI, didina realią saugumo reikalavimų pažeidimo riziką.

Dalis VMI specialistų sukurtų pagrindinės informacinės sistemos informaciją naudojančių programų reikalauja vartotojų autentifikavimosi ir prie duomenų prieina vartotojo vardu. Tik bendro pobūdžio intranetinės aplikacijos jungiasi prie informacinės sistemos duomenų bazės pasinaudodamos anoniminio informacinės sistemos vartotojo identifikatoriumi. Šioms vietinių AVMI programuotojų sukurtoms aplikacijoms nėra sukuriama visa privaloma dokumentacija, nėra dokumentuojami prisijungimai prie informacinės sistemos, niekas neperžiūri šių aplikacijų saugumo konfigūracijos. Todėl iškyla grėsmė informacinės sistemos saugumui. Programuotojai gali palikti nereglamentuotus prisijungimus prie duomenų bazės ar nustatyti didesnes teises, nei priklausytų anoniminei jungčiai. Anoniminės jungtys neregistruojamos „Saugumo" aplikacijoje, todėl negali būti užtikrinama tinkama jų kontrolė.

Nors buvo aiškinama, kad tinklo vartotojus registruoja tinklo administratoriai pagal tarnybinį skyriaus vedėjo raštą, tačiau auditoriams VMI tinklo vartotojo vardas buvo sukurtas be jokio rašto. VMI administratoriai naudojasi tinklo operacinės sistemos teikiamomis galimybėmis (slaptažodžių politika, vartotojų grupės ir pan.), tačiau neturi formaliai patvirtintų vartotojų identifikatorių kūrimo standartų ir slaptažodžių keitimo tvarkos.

Auditoriai pastebėjo ir kitų informacijos saugumo pažeidimų, kai darbuotojai dažnai palieka savo darbo vietas neišsiregistravę, ekrano užsklandos nereikalauja slaptažodžio įvedimo. Personalinių kompiuterių operacinė sistema yra nepakankamai sukonfigūruota

saugumo požiūriu. Vartotojai nėra įsisąmoninę informacijos apsaugos būtinybės, o tai padidina neautorizuoto priėjimo prie VMI informacinių resursų ir informacijos nutekėjimo grėsmę.

VMI nėra nustatytos tvarkos, pagal kurias yra naikinamos VMI kompiuterinio tinklo ir informacinės sistemos vartotojų teisės. Kartais sistemų administratoriai sužino apie darbuotojo atleidimą iš personalo skyriaus, o kartais darbuotojui atėjus grąžinti jam patikėtą kompiuterinę įrangą. Kai kurie administratoriai nereguliariai peržiūri registruotų vartotojų sąrašus ir ištrina ilgą laiką nebenaudojamas registracijas. Nereglamentuota ir nekontroliuojama teisių panaikinimo tvarka kelia informacijos nutekėjimo grėsmę, kurią potencialiai kelia neautorizuoti vartotojai vis dar galintys pasiekti informacines sistemas.

Audito ataskaitoje pateiktos pagrindinės rekomendacijas sistemos saugumo valdymui. Joje nurodoma, kad VMI turėtų pasitvirtinti informacinės sistemos modelį ir duomenų klasifikavimo schemą, nustatyti informacijos slaptumo lygius ir sudaryti matricą, pagal kurią būtų nustatoma, kokią informaciją ir kokiomis priėjimo teisėmis gali pasiekti kiekvieno suinteresuoto skyriaus atitinkamos pareigybės darbuotojas. Teisių suteikimo ir panaikinimo procesą siūloma kontroliuoti saugumo administratoriui, kuri turi būti pavaldus VMI viršininkui ar jo pavaduotojui, kuruojančiam informacines technologijas. Saugumo administratorius turėtų nustatyti informacinių sistemų saugumo taisykles, kontroliuoti jų laikymąsi, identifikuoti su informacinėmis sistemomis saugumu susijusias rizikas bei inicijuoti atitinkamas saugumo priemones. Taip pat jis turėtų įvertinti ir formaliai patvirtinti tiek VMI programuotojų, tiek išorinių tiekėjų kuriamas ir diegiamas sistemas saugumo ir atitikimo išoriniams reikalavimams prasme.

Rekomenduoja uždrausti pagrindinės informacinės sistemos tiekėjo darbuotojams jungtis prie VMI tinklo, kol nebus įvertintos visos su tokiu jungimusi susijusios rizikos, įgyvendinta saugumo kontrolė ir tvarkos, reglamentuojančios jungimąsi prie VMI tinklo resursų. Taip pat siūloma bendradarbiauti su Personalo skyriumi, nustatant tvarką, nurodančią kokiu būdu IT skyrius informuojamas apie priimamus, perkeliamus ar atleidžiamus darbuotojus. Tai leistų laiku suteikti darbuotojui priėjimą prie darbui reikalingų informacinių sistemų arba nedelsiant apriboti priėjimą prie sistemų. Ypatingas dėmesys turėtų būti skiriamas tvarkai, pagal kurią yra atleidžiami informacinių sistemų administratoriai ar ypatingieji vartotojai. Sistemų saugumo žurnalų peržiūra turėtų būti vienu iš kasdieninių sistemų administratorių atliekamų darbų. Įtartini įvykiai turėtų būti nedelsiant registruojami ir analizuojami, apie tyrimo rezultatus informuojant saugumo administratorių ir IT vadovybę.

Atkreipiamas dėmesys į visų informacinių sistemų vartotojų reguliarų švietimą informacijos saugumo temomis - jie turi būti supažindinami su priimtino naudojimosi internetu ir elektroniniu paštu taisyklėmis, informacinių sistemų saugumo ir informacijos apsaugos taisyklėmis, tinkamo darbo su personaliniu kompiuteriu tvarka. Šios tvarkos ir taisyklės turėtų būti reguliariai peržiūrėtos bei atnaujinamos. Reguliarus vartotojų informavimas apie vadovybės poziciją informacinių sistemų saugumo klausimais yra viena iš prevencinių priemonių, leidžiančių sumažinti pažeidimų, įvykdytų dėl nežinojimo ar piktnaudžiavimo suteiktomis teisėmis, grėsmę.

3.2. INFORMACIJOS SAUGUMO PAŽEIDIMŲ TYRIMAS LIETUVOJE

Lietuvos statistikos departamento ir Danijos statistikos tarnybos parengtame leidinyje „Informacinės technologijos"[96] nemažai dėmesio skiriama informacijos saugumo pažeidimams. Tyrime pateikiama informacija apie interneto naudojimo problemas, su kuriomis susiduria privatūs interneto vartotojai, įmonės ir valstybės institucijos.

Privatūs interneto vartotojai. Vartotojų, kurie nesusidūrė su jokiais saugumo incidentais respondentų buvo beveik dvigubai, negu tų, kurie patyrė vienokių ar kitokių saugumo problemų (3.4 pav.).

Visi asmenys, kurie naudojosi internetu namų valdoje 100, procentais	Visi 15-74 metų	Iš jų:	
		Dirbantys	Mokiniai, studentai
Neprašyti e. laiškai	26	27	24
Kompiuterių virusai	34	37	32
Nesąžiningas kreditinės kortelės naudojimas	0	0	0
Nelegalus, žalingas tinklapių turinys	10	12	8
Niekada nesusidūrė su sunkumais	46	43	54

3.4 pav. Asmenų, patyrusių sunkumus naudojantis internetu 2003 m. III ketv. dalis

Tačiau toks tyrimo rezultatas reiškia ne tai, kad tokių informacijos saugumo incidentų buvo mažai, bet tai, kad jie paprasčiausia nebuvo užfiksuoti dėl antivirusinių programų neturėjimo ar nesuvokimo, kas yra neprašyti e. laiškai (*spam*) ar žalingas interneto turinys. Toks menkas saugumo pažeidimų suvokimas yra moksleivių ir studentų tarpe. Didelė tikimybė, kad kompiuterio nenormalus darbas buvo traktuojamas kaip kompiuterio gedimas ar programinės įrangos klaidos. Kalbant apie saugumo incidentų tipus, dominuoja pažeidimai, susiję su kompiuterių virusais. Tokio tipo incidentai padarė žalą beveik trečdaliui interneto vartotojų, kai tuo tarpu su incidentais, kuriuos iššaukė neprašyti e. laiškai, susidūrė ketvirtadalis respondentų. Labiausia galima patikėti tuo tyrimo rezultatu, kad nei vienas iš respondentų

[96] Informacinės technologijos. Statistikos departamento prie Lietuvos Respublikos Vyriausybės, Vilnius, 2004.

nesusidūrė su nesąžiningu kreditinės kortelės naudojimo atveju, nes tokį sukčiavimą galima lengvai pastebėti. Tai tikrai geras rezultatas, nežiūrint to, kad Lietuvoje e. bankininkystės vartotojų tarp gyventojų nėra pakankamai daug.

Įmonės. Pagrindinę dalį Lietuvoje tarp stambiųjų įmonių sudaro finansinio tarpininkavimo (78%), elektros, dujų ir vandens tiekimo (42,6%) ir poilsio organizavimo, kultūrinės ir sportinės veiklos (39,3%) įmonės. Vidutiniame ir smulkiajame sektoriuje didžiąją dalį užima įmonės besiverčiančios kompiuteriais ir su jais susijusia veikla (atitinkamai 91,4% ir 87,6%), finansiniu tarpininkavimu (68,5% ir 84,6%) ir pašto bei telekomunikacijų paslaugomis (59,2% ir 63,8%). Tyrimo organizatoriai užfiksavo, kad beveik kiekviena Lietuvos įmonė nepriklausomai nuo jų dydžio turėjo informacijos saugumo incidentus (3.5 pav.).

Procentais nuo turinčių internetą įmonių	Iš viso	Darbuotojų skaičius		
		0-49	50-249	250+
Turėjo elektroninio saugumo problemų, iš jų:	41,7	38,4	49,1	60,4
Kompiuterinių virusų padariniai	97,3	96,7	98,1	100
Neautorizuotas priėjimas prie įmonės sistemos ar duomenų	5,3	4,8	7,6	1,2
Šantažas ar grėsmė duomenims, sistemai	3,5	3,8	3,2	2,3

3.5 pav. Įmonių elektroninio saugumo problemos 2004 m. pradžioje.

Saugumo pažeidimų situaciją įmonėse tyrimas atspindi žymiai tikroviškiau. Įmonėms dažniausia teko susidurti su kompiuterinių virusų padariniais. Rezultatai smulkiose (96,7%) ir stambiose (100%) beveik vienodi ir panašūs į užfiksuotus Jungtinės Karalystės informacijų saugumo pažeidimo tyrimo ISBS 2004 metu. Jeigu kompiuterinių virusų grėsmės vienodai atakuoja visus interneto vartotojus, tai neautorizuotas priėjimas prie įmonės sistemos ar duomenų labiau būdingas vidutinėms įmonėms (7,6%), negu smulkioms (4,8%) ir beveik nebūdingas stambioms (1,2%). Logiškai mąstant, tokį mažą tokio tipo pažeidimų procentą stambiose turėtų lemti griežtų priėjimo kontrolės mechanizmų įdiegimas. Smulkios įmonės labiau tikėtina, tokių mechanizmų neturėjo įdiegusios. Stambiosios įmonės mažiau negu vidutinės ir smulkiosios susiduria su tokiais pažeidimais, kaip šantažas ar grėsmė duomenims ir sistemai. Tai, kad įmonės fiksuoja tokį didelį kompiuterinių virusų padarinių dalį, įrodo tai, kad dauguma jų naudoja antivirusines programas (3.6 pav.).

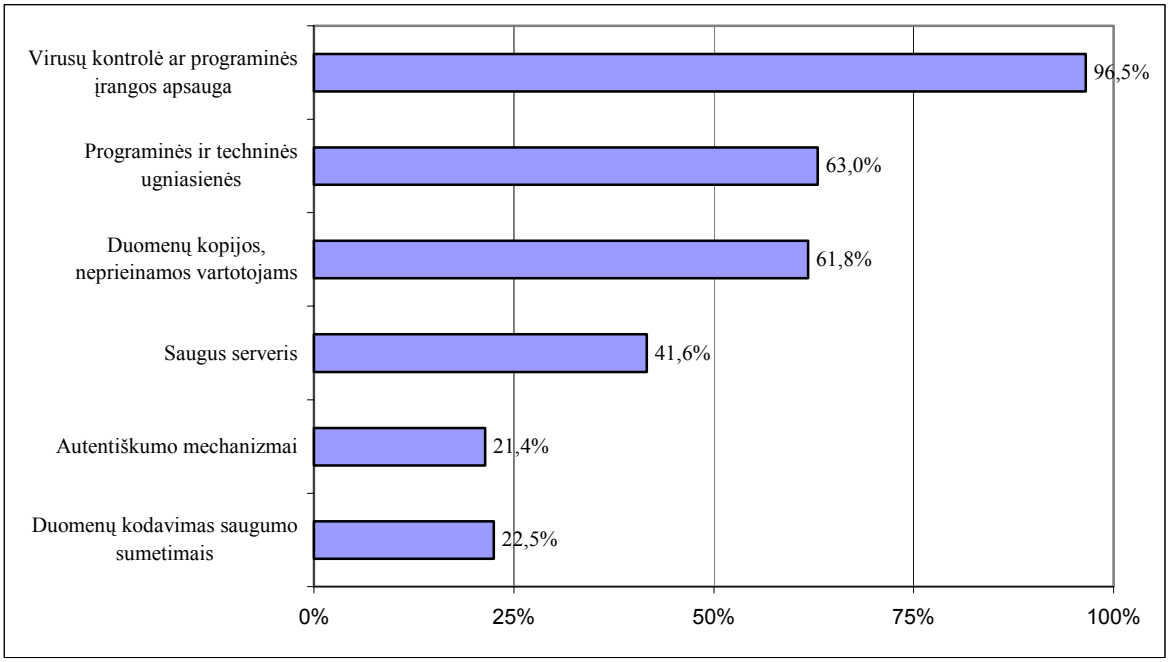
Procentais nuo turinčių internetą įmonių	Iš viso	Darbuotojų skaičius		
		0-49	50-249	250+
Naudoja elektronines saugos priemones, iš jų	93,6	92,6	95,8	99,6
Antivirusinės programos	86,6	84,6	91,1	96,5
Ugniasienės	25,1	19,5	35,0	73,0
Saugus serveris	29,0	25,0	36,2	62,5

Duomenų kopijos	39,0	34,0	49,1	77,2
Autentiškumo mechanizmai	29,5	26,8	35,3	44,6
Duomenų kodavimas	11,1	9,6	12,9	29,5

3.6 pav. Įmonių, kurios naudojo elektronines saugos priemones 2004 m. pradžioje, dalis.

Vidutiniškai daugiau kaip aštuonios iš dešimties įmonių turėjo įsidiegusios tokias programas. Tačiau kitos informacijos saugumo priemones – duomenų kopijavimas (39,0%), autentiškumo mechanizmai (29,5%), saugus serveris (29,0%), ugniasienės (25,1%) ir duomenų kodavimas (11,1%), nebuvo tokios populiarios, nekalbant apie stambiąsias įmones. Šio tipo įmonės labai plačiai naudojo duomenų kopijavimą (77,2%) ir ugniasienes (73,0%).

Valstybinės institucijos. Labai panaši situacija Lietuvos valstybės bei savivaldybių institucijose (3.7 pav.). Tačiau įvairių informacijos saugumo priemonių jos naudoja šiek tiek mažiau negu stambiosios įmonės.



3.7 pav. Valstybės ir savivaldybių valdymo įstaigų naudojamos elektroninio saugumo priemonės 2004 m. pradžioje

2003 metais 61,3 procentų valstybės ir savivaldybių valdymo įstaigų susidūrė su elektroninio saugumo problemomis (3.8 pav.). Ypač tai pajautė Lietuvos Respublikos Prezidentūra (100%), apskričių administracijos (90%) ir muitinės (83,3%), nepaisant to, kad jos buvo labiausiai linkusios atnaujinti saugumo priemones. Mažiausiai (33,3%) su saugumo problemomis susidūrė labiausiai kompiuterizuota Lietuvos institucija - Lietuvos Respublikos Seimas.

	Atnaujino saugumo priemones per 3 mėn.	Susidūrė su saugumo problemomis
Iš viso	**85,5**	**61,3**
Lietuvos Respublikos Prezidentūra	100	100
Lietuvos Respublikos Seimas ir jam atskaitingos institucijos	93,3	33,3
Lietuvos Respublikos Vyriausybė ir jam atskaitingos institucijos	94,4	50,0
Ministerijos ir joms atskaitingos institucijos	89,2	73,1
Apskričių administracijos	90,0	90,0
Miestų ir rajonų savivaldybės	95,0	76,7
Teismai	68,1	34,7
Policijos komisariatai	90,0	65,0
Muitinės	100	83,3
Įkalinimo įstaigos	54,5	45,5

3.8 pav. Elektroninė sauga valstybės ir savivaldybių valdymo institucijose 2003 m., procentais.

Net 60,7 procentų valstybės ir savivaldybių valdymo įstaigų 2003 metais dėl kompiuterinių virusų prarado savo informaciją ar sugaišo laiką tokių incidentų pasekmėms šalinti (3.9 pav.).

	Prarasta informacija ar laikas dėl virusų	Neautorizuotas priėjimas prie sistemos ar duomenų	Šantažas ar grėsmė duomenims ar programinei įrangai
Iš viso	**60,7**	**5,2**	**1,4**
Lietuvos Respublikos Prezidentūra	100	-	-
Lietuvos Respublikos Seimas ir jam atskaitingos institucijos	33,3	6,7	-
Lietuvos Respublikos Vyriausybė ir jam atskaitingos institucijos	50,0	-	-
Ministerijos ir joms atskaitingos institucijos	72,0	2,2	3,2
Apskričių administracijos	90,0	-	-
Miestų ir rajonų savivaldybės	76,7	6,7	-
Teismai	33,3	-	2,8
Policijos komisariatai	65,0	1,7	-
Muitinės	83,3	83,3	-
Įkalinimo įstaigos	45,5	45,5	-

3.9 pav. Elektroninio saugumo grėsmės valstybės ir savivaldybių valdymo institucijose 2003 m.

Lyderiai su tais pačiais rodikliais ir vėl tie patys - Lietuvos Respublikos Prezidentūra, apskričių administracijos ir muitinės. Tai reiškia, kad kiekvienas saugumo incidentas pasibaigė informacijos ar laiko praradimu. Muitinei ir įkalinimo įstaigoms kiekvienas neautorizuotas priėjimas prie sistemos ar duomenų pasibaigdavo informacijos ar laiko praradimu. Kitoms įstaigoms neautorizuotas priėjimas ir šantažas neturėjo lemiamos įtakos informacijos praradimui.

Europos Komisijos tris metus Europos Sąjungos šalyse kandidatėse vykdė tyrimą „*2001-2003 eEurope+ Final Progress Report*“ [97], kurio vienas pagrindinių tikslų buvo nustatyti, koks progresas šiose šalyse padarytas įgyvendinant Veiksmų planą *eEurope+*. Tyrimas parodė, kad 2003 m. birželio mėn. duomenimis Lietuvoje milijonui gyventojų tenka tik 14 saugių interneto serverių. Tai vienas žemiausių rodiklių tarp šalių kandidačių. Lietuva lenkia tik tas šalis, kurios 2004 m. gegužės 1 d. nebuvo pakviestos į Europos Sąjungą - Bulgariją, Rumuniją ir Turkiją. Toks Lietuvos rodiklis yra beveik 3 kartus žemesnis už bendrą visų šalių kandidačių vidurkį - 48 saugūs interneto serveriai milijonui gyventojų. Pagal saugumo problemų skaičių, naudojant internetą, Lietuva pirmauja. Per paskutiniuosius tyrimo 12 mėnesių mūsų šalyje užfiksuota, kad 68 procentai respondentų, kurie naudojosi internetu, turėjo saugumo problemų. Tai beveik 2 kartus daugiau negu vidutiniškai 15 šalių kandidačių (36%). Mus šiek tiek lenkia tik Latvija – 73 procentai. Pagal incidentų, susijusių su kompiuterių virusais, skaičių Lietuva pirmauja (90%), tačiau nelabai daug atsilieka nuo kitų šalių ir bendro šių šalių vidurkio – 86 procentai. Pagal naudojamų saugumo priemonių skaičių, Lietuva ir vėl lentelės pabaigoje. Tik 14 procentų Lietuvos respondentų naudoja kokias nors saugumo priemones. Estija mus lenkia beveik trigubai (45%), o nuo apklaustų šalių vidurkio atsiliekame beveik du kartus (26%).

Pagal turimus rezultatus galima daryti aiškią išvadą, kad Lietuva į Europos Sąjungą įstojo turėdama labai rimtų problemų. Norint ištaisyti šią situaciją, matomos labai didelės spragos Lietuvos vyriausybės darbe, šviečiant visuomenę informacijos saugumo klausimais, skiriant reikiamą dėmesį valstybinių institucijų saugumo problemoms spręsti. Labai tinkamas pavyzdys, sprendžiant informacijos saugumo problemas, Lietuvos Respublikai turėtų Jungtinės Karalystės vyriausybės požiūris. Šiame darbe pateikiamas vienas iš šios šalies vyriausybės sprendimo būdų – kas dveji metai atliekami saugumo pažeidimų tyrimai.

[97] 2001-2003 eEurope+ Final Progress Report, February 2004, http://www.emcis2004.hu/dokk/binary/30/17/3/eEurope__Final_Progress_Report.pdf; prisijungimo laikas: 2004-11-09.

3.3. INFORMACIJOS SAUGUMO PAŽEIDIMŲ TYRIMAS JUNGTINĖJE KARALYSTĖJE

Jungtinės Karalystės Prekybos ir pramonės ministerija (*Department of Trade and Industry, www.dti.gov.uk*), siekdama padėti savo šalies įmonėms ir organizacijoms geriau suprasti informacijos saugumo rizikas, nuo 1991 metų remia informacijos saugumo pažeidimų tyrimus. Informacijos saugumo pažeidimų tyrimas ISBS 2004 (*Information Security Breaches Survey*) tai jau septintasis tokio pobūdžio tyrimas šioje šalyje. Šiam tyrimui, kaip ir ankstesniems, vadovavo kompanija *PricewaterhouseCoopers* (*www.pwc.com*) kartu su kitais rėmėjais - *Computer Associates* (*www.ca.com*), *Entrust* (*www.entrust.com*) bei *Microsoft* (*www.microsoft.com*). Šio tyrimo rezultatus vertino nepriklausomi ekspertai - Informacijos patikimumo konsultacinė taryba (*The Information Assurance Advisory Council, www.iaac.org.uk*), Nacionalis aukštų technologijų nusikaltimų padalinys (*The National Hi-Tech Crime Unit, www.nhtcu.org)* ir Londono universiteto *Royal Holloway* kolegija (www.isg.rhul.ac.uk). Visa tyrimo ISBS 2004 medžiaga kartu su grafikais pateikiama šio darbo 4 priede.

Septintoje apklausoje ISBS 2004, vykusioje 2003 m. spalio 2 d. - 2004 m. sausio 30 d. buvo apklausta įvairaus dydžio 1 209 organizacijų. Tyrimo ISBS 2004 pagrindiniu elementu buvo pasirinktas kiekybinis tyrimas, naudojant struktūrinį anketinį apklausimą. Įmonės buvo atsitiktinai parenkamos iš šalies įmonių registro. Tyrimo organizatoriai kiekvienu atveju susisiekdavo su organizacijų ir įmonių darbuotojais, atsakingais už informacijos saugumą. Stambiose kompanijose paprastai tai buvo IT vadovai, smulkiosiose – komercijos vadovai. Respondentai buvo apklausiami telefoniniu interviu, kuris trukdavo apie 30 minučių. Organizatoriai pastebėjo, kad skirtingo dydžio įmonės skirtingai supranta informacijos saugumą. Kadangi Jungtinėje Karalystėje vyrauja smulkaus ir vidutinio verslo gamybinių ir prekybinių įmonių modelis, tyrimo organizatoriai, norėdami turėti prasmingas išvadas stambiosioms įmonėms, padidino šios grupės apklausą. Kur stambiųjų įmonių apklausos rezultatai žymiai skyrėsi nuo bendrųjų rezultatų, tyrimo organizatoriai juos parodydavo atskirai. Įmonės pagal jų veiklos sritis buvo suskirstyto į dešimt grupių. Valstybinės institucijos buvo išskirtos į atskirą grupę ir sudarė apie 7% nuo visų apklausoje dalyvavusių organizacijų.

Reikia pažymėti, kad organizatoriai papildydami telefoninį tyrimą, atliko papildomą nuodugnų interviu „akis į akį“ su įmonių informacijos saugumo darbuotojais. Kai kurie iš jų,

buvo dalyvavę ir telefoninėje apklausoje. Tokie susitikimai reikalingi tam, kad būtų patvirtintas telefoninių duomenų pagrįstumas ir, kad organizatoriai turėtų papildomą kokybišką informaciją. Taip pat buvo naudojama tiesioginės (*on-line*) interneto apklausos rezultatai, kad įmonės, nepatekusios į atrinktųjų iš įmonių registro sąrašą, telefoniniams ar „akis į akį“ interviu, galėtų prisidėti prie šio tyrimo. Nors internetinės apklausos rezultatai nepateko į pagrindinę statistiką, jie buvo paminėti organizatorių komentaruose. Kaip ir visų internetinių apklausų rezultatai nėra privalomi ir į juos reikia žiūrėti atsargiai. Reikia paminėti, kad pusė internetinėje apklausoje dalyvavusių respondentų atstovavo stambiosioms įmonėms, o trečdalis smulkiosioms. Tokių savanoriškų internetinių apklausų pati prigimtis reiškia, kad respondentai patys domisi ir geriau žino nagrinėjamas problemas, šiuo atveju informacijos saugumo, nei vidutinis respondentas. Į tai reikia atsižvelgti ir aiškinant apklausos rezultatus.

Tyrimas patvirtino faktą, kad internetas yra įprastas dalykas beveik kiekvienoje įmonėje - 93 procentai įmonių naudoja elektroninį paštą, 89 procentai suteikia galimybę darbuotojams jungtis prie interneto, 85 procentai turi nuosavas interneto svetaines. Šis tyrimas atskleidė keletą naujų tendencijų, kaip pasikeitė veiklos aplinka per paskutiniuosius du metus. Pirma tendencija, kad beveik šešis kartus padidėjo įmonių, sudarančių sutartis tiesiogiai internete. Jeigu 2002 m. tokių įmonių buvo tik 13 procentų, tai 2004 m. jų jau buvo 73 procentai. Antroji tendencija – įmonės vis labiau naudoja bevielio ryšio technologijas. Įmonių, naudojančių šias ryšio technologijas, padidėjo net 17 kartų. Tačiau toks didelis šuolis nereiškia, kad bevielis tinklas įmonėse yra labai populiarus. Jis naudojamas tik trečdalyje apklaustų įmonių. Ir trečioji tendencija – beveik dvigubai padidėjo įmonių, naudojančių priėjimą prie įmonės informacinių resursų, per nuotolį. Ypač ši tendencija stebima stambiosiose įmonėse. Beveik devynios įmonės iš dešimties leidžia jungtis darbuotojams prie įmonės informacinių sistemų per nuotolį.

Įmonių skaičius, kurios tvirtina, kad informacinėse sistemose saugoma labai svarbi informacija, per pastaruosius dvejus padidėjo tik 7 procentais (nuo 51% iki 58%), tačiau net 77 procentai stambiųjų įmonių patvirtino, kad savo sistemose saugo labai svarbią informaciją. Beveik pusė (52%) apklaustų įmonių pareiškė, kad informacijos pažeidimas labai smarkiai paveiktų įmonės veiklą ir šiek tiek mažiau kaip pusė (44%) įmonių tvirtino, kad informacijos neprieinamumas, rimtai sutrikdytų įmonės darbą.

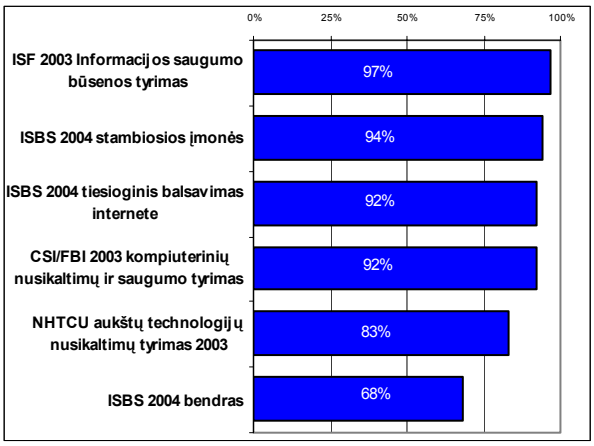
Tyrimo ISBS 2004 metu buvo bandoma įsiaiškinti, kiek lėšų įmonės investuoja į informacijos saugumą. Nustatyta, kad informacijos saugumui vidutiniškai išleidžiama apie 3 procentus nuo bendro IT biudžeto, o stambiosios įmonės 4 procentus. Tyrimo organizatoriai,

pasiremdami kitų šalių patirtimi, galvoja, kad išlaidos informacijos saugumui vidutiniškai turėtų sudaryti 3-5 procentus nuo viso IT biudžeto, o aukštos rizikos sektoriuose, tokiuose kaip finansinės paslaugos, turėtų siekti 10 procentų. Beveik ketvirtadalis įmonių į saugumą investuoja daugiau nustatyto efektyvaus lygio, o tarp stambiųjų, beveik pusė jų, investuoja daugiau nustatyto lygio. Tačiau dar yra nemažai įmonių, kurios informacijos saugumui skiria mažiau negu 1 procentas arba neskiria visiškai. Vienas iš faktorių, trukdančių pakankamai investuoti į informacijos saugumą yra tas, kad įmonės į išlaidas saugumui dažnai žiūri ne kaip į investiciją, o kaip į pridėtines išlaidas.

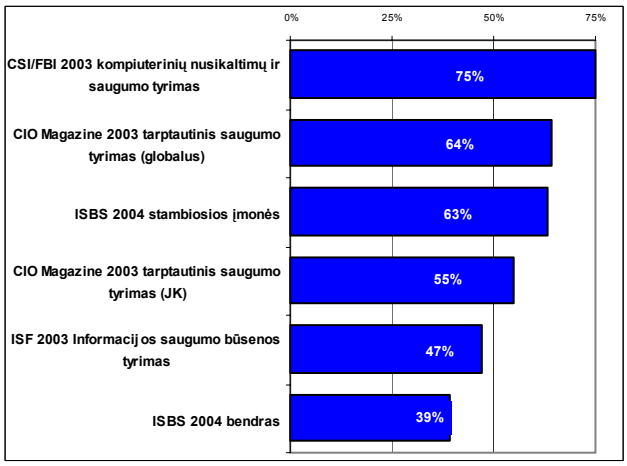
Kaip rodė ankstesnių metų patirtis, daugiausia saugumo incidentų linkę sukelti „savi žmonės". Tačiau dar 2002 m. tyrimas identifikavo esminį šios padėties pasikeitimą - beveik du trečdalius incidentų mažose įmonėse sudarė išoriniai incidentai, o stambiose - vidiniai ir išoriniai incidentai pasidalijo beveik po lygiai. 2004 m. tyrime, respondentai pirmą kartą galėjo identifikuoti mišrų incidentą, kurį iššaukė vidinių ir išorinių veiksnių kombinacija. Buvo pateikiami tokie pavyzdžiai: viruso paplitimas dėl netinkamų įmonės darbuotojo veiksmų, sistemos sutrikimas dėl išorinių veiksnių (tokių kaip įtampos sutrikimas) ir nelegalus personalo bendravimas su pašaliniais. Respondentų pranešimuose virusai ir tyčiniai kodai, be jokių abejonių, priskiriami prie dažniausiai pasitaikančių saugumo incidentų ir sudaro du trečdalius pačių rimčiausių incidentų. Beveik trys ketvirtadaliai įmonių pranešė, kad elektroniniu paštu gautos bylos buvo užkrėstos virusais arba Trojos arkliais. Stambiąsias įmones virusai paveikė labiau negu smulkiąsias. Per pastaruosius dvejus metus žymiai išaugo incidentai dėl personalo netinkamo informacinių sistemų naudojimo. Beveik ketvirtadalis (22%) įmonių pranešė apie incidentus, įvykusius dėl personalo klaidų naudojant informacines sistemas. Tai lygiai dvigubai daugiau, negu tokių pažeidimų buvo 2002 m. Tokį padidėjimą sąlygojo išaugęs interneto vartojimas. Piktnaudžiavimas elektroniniu paštu ir interneto naršymas sudarė didžiąją dalį netinkamo naudojimo incidentų, atitinkamai 35 ir 51% procentas.

Tyrimas ISBS 2004 yra vienas iš didžiausių informacijos saugumo tyrimų visame pasaulyje, todėl jis pakankamai tiksliai duoda informacijos saugumo būsenos vaizdą Jungtinėje Karalystėje. Palyginimas su kitais panašiais tyrimais atliktais kitose šalyse visada yra naudingas gautų rezultatų patikrinimui ir skirtingų tyrimų traktavimo skirtumų supratimui. Visi kiti tyrimai naudoja mažesnes atrankas ir todėl turi didesnes paklaidas. Taip pat jie gali būti tendencingi stambesnių ir saugumą suprantančių įmonių atžvilgiu. Ir galiausiai, gali skirtis saugumo incidento nustatymas būdas, kuris buvo naudojamas tyrime ISBS 2004. Aukštų

technologijų nusikaltimų tyrimas NHTCU 2003 buvo atliekamas tuo pačiu laiku. Jo metu buvo apklausta 201 įmonė. Pusė jų turėjo virš 1 000 darbuotojų. 83 procentai šio tyrimo respondentų turėjo aukštų technologijų nusikaltimų incidentus. Šis skaičius labai artimas bendram ISBS2004 tyrimo vidurkiui ir stambiųjų įmonių tyčinių incidentų rezultatui (3.10 pav.).



3.10 pav. Saugumo incidentų lygis



3.11 pav. Rimtų saugumo incidentų lygis.

Informacijos saugumo forumas (ISF) tai organizacija, galinti surinkti pakankamai duomenų apie informacijos saugumo incidentus iš savo narių, dominuojančių stambiajame versle. Jie savo 2003 m. Informacijos saugumo būsenos tyrime ISF 2003 apklausė 189 respondentus. 97% jų patyrė mažiausiai kaip vieną saugumo incidentą. Tai irgi labai panašu su ISBS2004 tyrimo rezultatu stambiosioms įmonėms (94%). ISF 2003 tyrimas taip pat parodė, kad 47% įmonių patyrė mažiausiai kaip vieną rimtą incidentą. Tai irgi atitinka ISBS 2004 tyrimo rezultatams, pagal kuriuos 39% stambiųjų įmonių turėjo patyrusios ypač rimtus incidentus ir 63% įmonių turėjo patyrusios rimtus incidentus (3.11 pav.).

Jungtinės Karalystės Prekybos ir pramonės ministerijos specialioje interneto svetainėje http://www.ukonlineforbusiness.gov.uk/healthcheck/survey.do pateikiamas informacijos saugumo testas *Health Check*. Bet kurios organizacijos darbuotojai, tame tarpe ir Lietuvos, atsakę į 126 klausimus, gali pasitikrinti savo organizacijos informacijos saugumo būseną. Ši anketa visiškai anoniminė. Testas paremtas standartu BS7799 ir duoda tikrus, praktiškus patarimus palankiam informacijos saugumo tikslo siekimui. Toks Jungtinės Karalystės vyriausybės požiūris informacijos saugumo problemoms, teikia organizacijoms didelę naudą sprendžiant informacijos saugumo klausimus.

Klausimai į sugrupuoti į dešimt skyrių, kurių kiekvienas turi pagrindinį aukštesnio lygio klausimą ir keletą detalesnių žemesnio lygio klausimų:

1. Saugumo politika (1 pagrindinis/5 papildomi klausimai);
2. Saugumo organizavimas (3/9);
3. Turto klasifikavimas ir valdymas (2/8);
4. Personalo saugumas (3/9);
5. Fizinis ir aplinkos saugumas (3/11);
6. Komunikacijų ir operacijų valdymas (6/19);
7. Kreipties kontrolė (6/24);
8. Sistemų plėtra ir priežiūra (2/10);
9. Veiklos tęstinumo valdymas (1/3);
10. Atitiktis (3/8).

Kiekvienas skyrius atitinka standarto ISO 17799 (BS7799) atitinkamą skyrių. Į kiekvieną klausimą galimi trys atsakymai: „taip“, „dalinai“ arba „ne“. Į šiuos klausimus reikia atsakyti tik tada, kai į skyriaus pagrindinius klausimus, kurių iš visi yra 20, atsakoma teigiamai („taip“). Tuo atveju, kai į pagrindinius klausimus atsakoma neigiamai („ne“), kiti papildomi klausimai blokuojami.

Panašų testą galima rasti ir Rusijos mokslinės inžinierinės įmonės „*ИНФОРМЗАЩИТА*" svetainėje http://www-old.infosec.ru/uslugi/security_quiz.php. Skirtingai negu Jungtinės Karalystės testo atveju, šioje svetainėje pateikiami šeši vienas nuo kito nepriklausomi labai trumpi testai: saugumo politika; organizacinis palaikymas, fizinis saugumas, veiklos tęstinumo užtikrinimo analizė, veiklos atstatymas, įvykus avarinei situacijai, techninės saugumo priemonės, telekomunikacijų saugumas.

3. IŠVADOS

Atsižvelgiant į darbo hipotezė, lemiamas faktorius viešųjų e. paslaugų informacijos saugumui - informacijos pažeidimo pasekmių supratimas ir informacijos saugumo kultūros suformavimas. Formuojant organizacijos saugumo politiką ir diegiant informacijos saugumo sistemą, būtina:

1. Gerai žinoti Europos Sąjungos norminius aktus, kurie reglamentuoja informacijos saugumą ir įvertinti tą faktorių, kad analogiškų norminių aktų leidyba Lietuvos Respublikoje šiuo metu yra pradinėje stadijoje;

2. Išanalizuoti geriausią tarptautinę patirtį informacijos saugumo srityje. Taikyti pažangiausią ir labai turtingą JAV, Jungtinės Karalystės ir kitų Europos Sąjungos šalių patirtį informacijos saugumo srityje;

3. Tinkamai suprasti ir įvertinti informacinius resursus - informacines sistemas ir informacijos apdorojimo technologijas, kurių pagrindu teikiamos viešosios e. paslaugos mokesčių mokėtojams, bei savo specialistų - informacinių technologijų ir mokesčių administratorių, žinias;

4. Suvokti įvairaus pobūdžio ir nuolat besikeičiančias grėsmes informaciniams resursams, mokėti įvertinti riziką ir pažeidimo poveikį (finansinius nuostolius, gero organizacijos įvaizdžio ir patikimumo praradimą ir pan.) organizacijai, kuris galėtų būti padarytas, įvykus nepageidaujamam informacijos saugumo pažeidimo incidentui;

5. Formuoti organizacijos informacijos saugumo kultūrą, kai visi organizacijos informacinių sistemų vartotojai įsisąmonins ir supras saugumo užtikrinimo būtinumą, supras savo atsakomybę, laiku ir tinkamai sureaguos į saugumo pažeidimo incidentus, sugebės įvertinti mokesčių mokėtojų ir kitų organizacijų teisėtus interesus, užtikrindami informacijos saugumą, vadovausis pagrindinėmis demokratinės visuomenės taisyklėmis;

6. Aiškiai suformuluoti vieną iš svarbiausių saugumo valdymo tikslų – tinkamą kreipties kontrolės politiką, leidžiančią tiksliai identifikuoti vartotojus ir patvirtinti jų autentiškumą, užtikrinti jų privatumą ir konfidencialumą;

7. Sugebėti parinkti optimaliausias saugumo priemones, leidžiančias apsaugoti organizacijos informacinius resursus nuo grėsmių, apribojant nepageidaujamų incidentų poveikį, atskleidžiant nepageidaujamus incidentus ir palengvinant organizacijos veiklos atstatymą po įvykusių incidentų.

8. Vykdyti efektyvų auditą ir apskaitą, leidžiančius saugoti svarbiausių transakcijų įrašus, siekiant įrodyti, kad yra atliekama privatumo ir konfidencialumo priežiūra.

Šis darbas atskleidė ir eilę naujų problemų.

1. Dažnai net ir labai gerai parengta organizacijos informacijos saugumo politika neveikia taip, kaip turėtų veikti. Todėl galima iškelti naują hipotezę - sėkmingas informacijos saugumo politikos diegimas organizacijoje galimas tik tada, jeigu čia jau yra įdiegtas kokybės ar informacinių technologijų valdymas (pagal ISO 9000, ITIL, ITSM ir pan. reikalavimus). Reikalavimai informacijos saugumui turi būti keliami jau informacinių sistemų projektavimo stadijoje.

2. Lietuvoje turi būti institucija, kurioje dirbtų kvalifikuoti informacijos saugumo specialistai, sugebantys teikti konsultacijas ir rengti įvairius mokymus informacijos saugos klausimais, padedantys spręsti iškylančias saugumo problemas

LITERATŪROS SĄRAŠAS

LIETUVOS RESPUBLIKOS NORMINIAI AKTAI

1. Lietuvos Respublikos elektroninių ryšių įstatymas//Valstybės Žinios, 2004, Nr. 69-2382.
2. Lietuvos Respublikos elektroninio parašo įstatymas//Valstybės Žinios, 2000, Nr. 61-1827.
3. Lietuvos Respublikos viešojo administravimo įstatymas//Valstybės Žinios, 1999, Nr. 60–1945.
4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas//Valstybės Žinios, 1996, Nr. 63-1479, 2003, Nr.: 15-597.
5. Lietuvos Respublikos gyventojų turto deklaravimo įstatymas//Valstybės Žinios, 1996, Nr. 50-1197, Valstybės Žinios, 2003, Nr. 123-5583.
6. Lietuvos Respublikos mokesčių administravimo įstatymas//Valstybės Žinios, 2004, Nr. 63-2243.
7. Lietuvos Respublikos vienkartinio gyventojų turto deklaravimo įstatymas//Valstybės Žinios, 2003, Nr. 123-5582.
8. Elektroninės valdžios koncepcija//Valstybės žinios, 2003, Nr.: 2-54.
9. Dėl Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo//Valstybės Žinios, 2001, Nr. 110-4006.
10. Dėl Tipinių duomenų saugos nuostatų patvirtinimo//Valstybės Žinios, 2003, Nr. 76-3511.
11. Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo//Valstybės Žinios, 2004, Nr. 80-2855.
12. Dėl Interneto tarnybinių stočių apsaugos rekomendacijų patvirtinimo//Valstybės Žinios, 2004, Nr. 85-3095.
13. Dėl Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo//Valstybės Žinios, 2004, Nr. 58-2061.
14. Dėl duomenų saugos valstybės ir vietos savivaldos informacinėse sistemose//Valstybės Žinios, 1997, Nr. 83-2075; Valstybės Žinios, 2003, Nr. 2-45.
15. Dėl Lietuvos Respublikos Vyriausybės 1999 m. gegužės 20 d. nutarimo Nr. 617 "Dėl keitimosi informacija apie standartus, techninius reglamentus ir atitikties įvertinimo procedūras" dalinio pakeitimo//Valstybės Žinios, 2000, Nr.: 111-3590.
16. Dėl Informacijos klasifikavimo pagal duomenų grupes rekomendacijų patvirtinimo//Valstybės Žinios, 2003, Nr. 77-3541.
17. Dėl Gyventojų deklaracijų ir prašymų formų teikimo elektroniniu būdu tvarkos patvirtinimo//Valstybės Žinios, 2004, Nr. 40-1319.
18. Dėl Pridėtinės vertės mokesčio mokėtojų registravimo//Valstybės Žinios, 2004, Nr. 29-946.
19. Dėl Mokesčio mokėtojų registravimo taisyklių ir registro pildymo tvarkos patvirtinimo//Valstybės Žinios, 1996, Nr. 66-1591, Valstybės Žinios, 1996, Nr. 67.
20. Dėl Vienkartinės gyventojo (šeimos) turto deklaracijos formos ir jos užpildymo, teikimo ir tikslinimo taisyklių patvirtinimo//Valstybės Žinios, 2004, Nr. 37-1214.
21. Dėl Viešojo administravimo plėtros iki 2010 metų strategijos patvirtinimo//Valstybės Žinios, 2004, Nr. 69-2399.

EUROPOS SĄJUNGOS NORMINIAI AKTAI

1. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis//Valstybės Žinios, 2001, Nr. 32-1059.
2. Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EC), Autentiškas vertimas, Europos komitetas prie LR Vyriausybės, Vertimo, dokumentacijos ir informacijos centras, http://www3.lrs.lt/c-bin/eu/preps2?Condition1=7879&Condition2=.
3. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), Autentiškas vertimas, Europos komitetas prie LR Vyriausybės, Vertimo, dokumentacijos ir informacijos centras, http://www3.lrs.lt/c-bin/eu/preps2?Condition1=36605&Condition2=.
4. Convention for the protection of individuals with regard to automatic processing of personal data (ETS Nr. 108), http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm.
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23/11/1995.
6. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24/1, 30/01/1998.
7. Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. OJ, L 217, 05.08.1998.
8. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178/1, 08/06/2000.
9. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37, 31/07/2002.
10. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions „eEurope 2005: An information society for all“, COM(2002) 263 final, 28.5.2002.
11. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_077/l_07720040313en00010011.pdf.
12. Decision No 2256/2003/EC of the European Parliament and of the Council of 17 November 2003 adopting a multi-annual programme (2003-2005) for the monitoring of the *e*Europe 2005 action plan, dissemination of good practices and the improvement of network and information security (MODINIS), OJ L 336, 23/12/2003.
13. http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope 2005/ eeurope2005_en.pdf.

TARPTAUTINIAI INFORMACIJOS TECHNOLOGIJŲ STANDARTAI

1. LST ISO/IEC 15408-1:2002. Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai. 1 dalis. Įvadas ir bendrasis modelis.
2. LST ISO/IEC 15408-2:2002. Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai. 2 dalis. Funkciniai saugumo reikalavimai.
3. LST ISO/IEC 15408-3:2002. Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai. 3 dalis. Saugumo užtikrinimo reikalavimai.
4. LST ISO/IEC 17799:2002. Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai.
5. LST ISO/IEC TR 13335-1:2000. Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 1 dalis. Informacijos technologijų saugumo sąvokos ir modeliai.
6. LST ISO/IEC TR 13335-2:2000. Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 2 dalis. Informacijos technologijų saugumo valdymas ir planavimas.
7. LST ISO/IEC TR 13335-3:2000. Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 3 dalis. Informacijos technologijų saugumo valdymo metodai.
8. LST ISO/IEC TR 13335-4:2002. Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 4 dalis. Apsaugos priemonių parinkimas.
9. LST ISO/IEC TR 13335-5:2002. Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 5 dalis. Tinklo saugumo valdymo patarimai.

NAUDOTA LITERATŪRA

1. Atkinson R., MLS Security Associations, http://www.netsys.com/ipsec/1995/msg00584.html.
2. Bell D. E., LaPadula L. J. Secure computer systems: unified exposition and multics inter-pretation. Report MTR-2997 Rev. 1. AD A023 588. Bedford, Mass.: The Mitre Corporation. 1976. http://csrc.nist.gov/publications/history/bell76.pdf.
3. Barman S. Writing Information Security Policies. New Riders Publishing, 2002.
4. Clark D.D., Wilson D.R. A comparison of commercial and military computer security policies. In IEEE Symphosium on Research in Security and Privacy, April 1987.
5. Germanow A. Plugging the Holes in eCommerce: The Market for Intrusion Detection and Vulnerability Assessment Software, 1999-2003. International Data Corporation, August, 1999.
6. Graham G. and Dening P. Protection – principles and practice. In Proc. Spring Jodint Computer Conference. AFIPS Press, 1972.
7. Harrison M.H., Ruzzo W.L and Uleman, J.D „Protection in Operating Systems“. Comunications of ACM, 1976.
8. Lampson B. Protection. In 5th Princeton Symposium on Informatikon Sciences and System, March 1971. Reprinted in ACM Operating Systems Review, 8(1), 1974.
9. Peltier T.R. Information Security Policies, Procedures and Standards. Guidelines for Effective Information Security Management. Auerbach Publications, 2002.
10. Tittel E., Chapple M., Stewart J.M. CISSP: Certified Information Systems Security Professional. Study Guide. Sybex, Inc, Alameda, CA, 2003.
11. Черней Г. А. Особенности применения криптографических средств в информационных системах с мандатной политикой управления доступом, 2000, http://www.ase.md/~osa/publ/ru/pubru20.html.
12. Лукацкий А.В. Анатомия распределенной атаки. "PCWeek/RE", №5, 2000.
13. Родичев А.Ю., Родичев Ю.А. Вестник СамГУ _ Естественнонаучная серия. 2003. Второй спец. выпуск. 15 УДК 681.3. Системная модель защиты информации информационных сист распределенного типа, 2003.
14. Петренко С. А., Симонов С. В., «Управление информационными рисками. Экономически оправданная безопасность». — М.: «Компания АйТи», «ДМИ Пресс», 2004.
15. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) Date: 1998-12-18, ISO/IEC/15408-1: 1999(E), Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model.
16. NIST Special Publication 800-35, Guide to Information Technology Security Services, October 2002, http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf.
17. NIST Special Publication 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004, http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf.
18. OECD Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security http://www.oecd.org/dataoecd/16/22/15582260.pdf.
19. Flash Eurobarometer 135: Internet and the Public at Large 6, EOS Gallup Europe, 2002, http://europa.eu.int/information_society/eeurope/2002/benchmarking/list/source_data_pdf/report_eb125_en.pdf.
20. Global Information Security Survey, KPMG, 2002 http://www.kpmg.com/microsite/informationsecurity/isssurvey.html.

21. 2001-2003 eEurope+ Final Progress Report, February 2004, http://www.emcis2004.hu/dokk/binary/30/17/3/eEurope__Final_Progress_Report.pdf.
22. Web-based Survey on Electronic Public Services: Results of the third measurement October 2002, Cap Gemini Ernst & Young, 2002, http://europa.eu.int/information_society/eeurope/2002/documents/CGEY-Report3rdMeasurement.pdf.
23. Informacinės technologijos. Statistikos departamento prie Lietuvos Respublikos Vyriausybės, Vilnius, 2004.
24. Siekiamas elektroninių viešųjų paslaugų modelis. http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_ siekiamasV1.pdf.
25. Lietuvos valstybės institucijų bei įmonių ir kitų įstaigų elektroninių viešųjų paslaugų, teikiamų viešaisiais kompiuterių tinklais svarbiausių paslaugų procedūrų tyrimas ir paslaugų teikimo galimybių analizė, IVPK, 2001.//http://www.ivpk.lt/dokumentai/el-paslaugos.pdf.
26. Viešųjų paslaugų teikimo esamos būklės analizė ir modelio aprašymas, IVPK, 2004 //http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_esamasV1.pdf.

SANTRAUKA

Europos Komisijos pristatytame Veiksmų plane „*e Europe 2005: An information society for all“,* Europos Sąjungos šalims iškeliami tikslai - skatinti dialoginiame režime teikiamas viešąsias paslaugas (e. vyriausybė, e. mokymasis, e. sveikatos apsauga ir e. verslas) ir vystyti saugią telekomunikacinę infrastruktūrą. Saugus e. viešųjų paslaugų diegimas akcentuojamas ir Lietuvos Respublikos Vyriausybės patvirtintoje Elektroninės valdžios koncepcijoje.

Labai dažnai, kalbant apie informacijos saugumą, apsiribojama technologinių, techninių ir programinių saugumo sprendimo būdų, jų privalumų ir trūkumų nagrinėjimu, o organizacinėms priemonėms – informacijos saugumo strategijai ir taktikai, koncepcijai ir politikai, informacinių resursų saugumo planams, skiriamas nepakankamas dėmesys. Pagrindinis šio darbo tikslas - nustatyti pagrindinius reikalavimus, kurių būtina laikytis, norint VMI sėkmingai įdiegti informacijos saugumo sistemą, užtikrinančią saugių viešųjų e. paslaugų teikimą mokesčių mokėtojams, nustatyti šios sistemos valdymo principus ir tikslus, leidžiančius garantuoti reikiamą informacijos konfidencialumo, vientisumo ir prieinamumo lygį.

Darbo pradžioje suformuluota hipotezė pasitvirtino – lemiami faktoriai, norint sėkmingam įdiegti informacijos saugumo sistemą, kuri užtikrintų saugias viešąsias e. paslaugas, Valstybinėje mokesčių inspekcijoje - informacijos pažeidimo pasekmių supratimas ir informacijos saugumo kultūros suformavimas šioje organizacijoje. Išanalizavus geriausią tarptautinę patirtį informacijos saugumo srityje ir atsižvelgus į Europos Sąjungos bei Lietuvos norminius aktus galima pateikti išvadas, į kurias reikia atsižvelgti, diegiant informacijos saugumo sistemą. VMI vadovybė, formuodama savo informacijos saugumo politiką, privalo tinkamai suprasti ir įvertinti savo informacinius resursus, suvokti įvairaus pobūdžio grėsmes šiems resursams, nustatyti galimą informacijos pažeidžiamumo mastą, sugebėti įvertinti saugumo pažeidimo poveikį ir riziką, sugebėti parinkti optimaliausias saugumo priemones, formuoti organizacijos informacijos saugumo kultūrą, savo veikloje taikyti pažangiausią JAV, Jungtinės Karalystės ir Europos Sąjungos patirtį informacijos saugumo srityje.

Šis darbas atskleidė ir eilę naujų problemų - sėkmingas informacijos saugumo politikos diegimas organizacijoje galimas tik tuo atveju, jeigu organizacijoje jau yra įdiegtas kokybės ar informacinių technologijų valdymo standartai (ISO 9000, ITIL ir pan.).

SUMMARY

The European Committee introduced Action project „e Europe 2005: an information society for all" settled a cause for EU countries to encourage on-line public service (e. government, e. health security and e. business) and to develop secure telecommunication facility. Secure e. public service implementation is a keystone and for Lithuania Government which has confirmed an e-Government Conception.

Then we talk about information security we often talk only about technological, technical and with programs security their advantages and disadvantages related problems. Actually that is one of the reasons why it is not given enough attention to organization implements such us policy of information security, its conception and tactic of development or security of information resources and etc. The main goal of this work is to define the basic requirements which are necessary to follow if we want in our organization to encourage the development of information security system which would guarantee secure e. public services for taxpayers. The determination of principals and purposes of this system will let us guarantee information confidentiality, entity and accessibility.

A hypothesis at the end was certified - the crucial factors such us understanding the subsequences of information destruction or creation of information security culture, will let State Tax Inspectorate (STI) to achieve the successful system of information security and save e. public services. According to international experience related with information security – we came to conclusion, which we need developing the system of information security. STI need to understand and estimate information importance also to assess a real danger to their information resources and realize subsequences if the information would be disturb in ever level. Modelling the policy of information security in State Tax Inspectorate, it should be identified the effect of information breaches, must be selected optimal security tools to avoid information breaches and formed the model of information security culture. The experience related with information security system in such countries as USA, UK or in EU countries should be analyzed and profit for State Tax Inspectorate also.

This work disclose and some new problems. The basic of them is that it is hard to say, how successfully must be improved information security policy in this organization, but it is obvious that the development of this policy will be started if STI would improve quality of information or information technological managerial standards such as ISO 9000, ITIL and etc.

PRIEDAI

1 priedas

PAGRINDINIAI IT SAUGUMO TECHNIKOS STANDARTAI

ISO/IEC FCD 7064 Information technology -- Security techniques -- Data processing Check character systems

ISO 8372:1987 Information processing -- Modes of operation for a 64-bit block cipher algorithm.

ISO/IEC FCD 9796-1 Information technology -- Security techniques -- Digital signature scheme giving message recovery -- Part 1: Mechanisms using redundancy.

ISO/IEC 9796-2:1997 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Mechanisms using a hash-function.

ISO/IEC 9796-3:2000 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms.

ISO/IEC 9797:1994 Information technology -- Security techniques -- Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.

ISO/IEC 9797-1:1999 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher.

ISO/IEC 9797-2 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function.

ISO/IEC 9798-1:1997 Information technology -- Security techniques -- Entity authentication -- Part 1: General.

ISO/IEC 9798-2:1999 Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms.

ISO/IEC 9798-3:1998 Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques.

ISO/IEC 9798-4:1999 Information technology -- Security techniques -- Entity authentication -- Part 4: Mechanisms using a cryptographic check function.

ISO/IEC 9798-5:1999 Information technology -- Security techniques -- Entity authentication -- Part 5: Mechanisms using zero knowledge techniques.

ISO/IEC 9979:1999 Information technology -- Security techniques -- Procedures for the registration of cryptographic algorithms.

ISO/IEC 10116:1997 Information technology -- Security techniques -- Modes of operation for an n-bit block cipher.

ISO/IEC 10118-1:2000 Information technology -- Security techniques -- Hash-functions -- Part 1: General.

ISO/IEC 10118-2:2000 Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher.

ISO/IEC 10118-3:1998 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions.

ISO/IEC 10118-4:1998 Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic.

ISO/IEC AWI 10118-4 Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic.

ISO/IEC 11770-1:1996 Information technology -- Security techniques -- Key management -- Part 1: Framework.

ISO/IEC 11770-2:1996 Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques.

ISO/IEC 11770-3:1999 Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques.

ISO/IEC TR 13335-1:1996 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security.

ISO/IEC TR 13335-2:1997 Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security.

ISO/IEC TR 13335-3:1998 Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security.

ISO/IEC TR 13335-4:2000 Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards.

ISO/IEC CD TR 13335-5 Information technology -- Security techniques -- Guidelines for the management of IT Security -- Part 5: Management guidance of network security.

ISO/IEC 13888-1:1997 Information technology -- Security techniques -- Non-repudiation -- Part 1: General.

ISO/IEC 13888-2:1998 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques.

ISO/IEC 13888-3:1997 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques.

ISO/IEC CD TR 14516 Information technology -- Guidelines on the use and management of Trusted Third Party (TTP) services.

ISO/IEC 14888-1:1998 Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General.

ISO/IEC 14888-2:1999 Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Identity-based mechanisms.

ISO/IEC 14888-3:1998 Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Certificate-based mechanisms.

ISO/IEC FCD 15292 Information technology - Security techniques - Protection Profile registration procedures.

ISO/IEC 15408-1:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.

ISO/IEC 15408-2:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements.

ISO/IEC 15408-3:1999 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements.

ISO/IEC WD 15443 Information technology - Security techniques - A framework for IT security assurance.

ISO/IEC WD 15446 Information technology - Security techniques - Guide on the production of Protection profiles and Security Targets.

ISO/IEC 15816 Information technology -- Security techniques -- Security information objects for access control.

ISO/IEC 15945 Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures.

ISO/IEC FCD 15946-1 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General.

ISO/IEC FCD 15946-2 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 2: Digital signatures.

ISO/IEC FCD 15946-3 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 3: Key establishment.

ISO/IEC CD 15946-4 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 4: Digital signatures giving message recovery.

ISO/IEC CD 15947 Information technology - Security techniques - IT intrusion detection framework.

ISO/IEC 17799:2000 Information technology -- Code of practice for information security management.

ISO/IEC AWI 18029 Information technology -- Specification for the management and interoperation of public key infrastructure components.

ISO/IEC AWI 18030 Information technology -- Suppliers declaration of conformity for IT security products.

ISO/IEC AWI 18031 Information technology -- Random number generation.

ISO/IEC AWI 18032 Information technology -- Prime number generation.

ISO/IEC AWI 18033 Information technology -- Encryption algorithms.

ISO/IEC DIS 21827 Information technology -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM).

2 priedas

AUDITO PLANAS PAGAL *COBIT* METODOLOGIJĄ

Planavimas ir organizacija
Strateginio IT plano nustatymas
Ar egzistuoja organizacijos IT strategija ir veiklos planas? Ar jie apima veiklos tikslų palaikymą, procesų automatizaciją, esamos situacijos įvertinimą, sistemų architektūrą, techninę architektūrą, IT iniciatyvas, kainos/naudos įvertinimą, kt. ?
Ar IT strategija ir veiklos planas suderinti su visos organizacijos strategija ir veiksmų planu, organizacijos veiklos tikslais?
Informacinės architektūros nustatymas
Ar organizacija turi sukūrusi duomenų klasifikatorių ir identifikavusi informacijos srautus tarp padalinių ir sistemų? Ar jie reguliariai peržiūrimi ir atnaujinami?
Ar egzistuoja abipusis ryšys tarp strateginio planavimo ir informacinio modelio?
Technologijų plėtros krypčių nustatymas
Ar egzistuoja organizacijos technologinės infrastruktūros ir jos plėtros planai? Ar jie atsispindi IT strategijoje ir veiklos plane?
Ar egzistuoja organizacijos technologiniai standartai?
IT organizacijos ir jos ryšių nustatymas
Ar įsteigtas IT strateginio planavimo komitetas?
Ar yra atskirtos nesuderinamos IT darbuotojų funkcijos?
Ar egzistuoja sistemų bei duomenų savininkai ir prižiūrėtojai? Ar visoms sistemoms ar jų dalims?
Ar pagal nustatytą tvarką dokumentuojami kontaktai su vartotojais, tiekėjais, vykdytojais? Ar tai suderinama su bendra organizacijos tvarka?
Ar yra galimybė greitai išplėsti IT funkcijų ar IT išteklių kiekį, esant veiklos poreikiui?
IT investicijų valdymas
Ar investicijų į IT procesas suderinamas su bendra organizacijos pirkimų tvarka?
Ar egzistuoja metinis IT biudžeto sudarymo procesas, kuris yra suderintas tiek su IT strategija, tiek su organizacijos strategija ir veiksmų planais?
Ar yra apskaičiuojama investicijų grąža?
Ar planuotas biudžetas lyginamas su realiomis išlaidomis? Ar numatytos ir atskirtos kapitalinės išlaidos ir pastovios operacinės išlaidos (*Cost of Ownership*)?
Vadovybės tikslų ir krypčių komunikavimas
Ar su organizacijos suformuluota IT vizija ir strategija yra supažindinami vartotojai?
Ar egzistuoja tinkamo elgesio su IS, saugumo, kokybės tvarka?
Ar šios tvarkos ir taisyklės yra skelbiamos vartotojams? Ar jos reguliariai peržiūrimos, kad atsižvelgti į technologinius, veiklos, kt. pokyčius organizacijoje?
IT personalo valdymas
Ar IT vadovybė reguliariai įvertina, ar IT funkcijas atlieka pakankamai kvalifikuoti darbuotojai? Ar atliekamas darbas atitinka kvalifikaciją? Kokie yra pagrindiniai vertinimo kriterijai?
Ar yra skiriamas dėmesys IT darbuotojų apmokymui kad jie efektyviai atliktų jiems pavestą darbą? Ar skatinamas kvalifikacijos kėlimas, gretutinių funkcijų įsisavinimas?
Ar darbuotojų priėmimo, paaukštinimo procese dalyvauja tiek Personalo skyrius, tiek IT vadovybė? Ar priėmimo tvarka yra nešališka?
Kokia IT biudžeto dalis skiriama personalo mokymui, skatinimui?
Atitikimo išoriniams reikalavimams užtikrinimas
Kokie yra pagrindiniai išoriniai reikalavimai?
Ar yra organizacijoje tvarka ir procedūra, užtikrinant atitikimą išoriniams reikalavimams (teisiniams, kontraktiniams)?
Ar įvertinami asmens privatumo, intelektualinės nuosavybės, slaptumo reikalavimai?

Rizikos įvertinimas
Ar yra tvarka ir procedūros identifikuoti, įvertinti, suteikti prioritetai ir apsisaugoti nuo su IT susijusių rizikų (sistemos, technologija, žmonės, reikalavimai)?
Projektų valdymas
Ar veiklos padalinių atsakingi darbuotojai (vartotojai) yra tie asmenys, kurie "stumia" IS diegimo procesą (yra sistemų savininkai)?
Ar organizacija turi ir vadovaujasi Projektų valdymo metodologiją? Ar ši metodologiją dengia pilną IS diegimo ciklą pradedant planavimu ir baigiant podiegimine priežiūra?
Ar funkciniai padaliniai yra įtraukti į IT projektus ir dalyvių rolės aiškiai nustatytos?
Ar kartu su projekto valdymu vyksta ir projekto kokybės valdymas?
Kokybės valdymas
Ar yra įkurta Kokybės užtikrinimo funkcija, nustatytos jos pareigos? Ar yra nustatyta ir laikomasi IS projektų ir IT veiklos kokybės užtikrinimo tvarkos?
Ar vykdomos testavimo ir priėmimo procedūros IS diegimo projektams ir didesniems pakeitimams? Ar rezultatai dokumentuojami ir vadovybės analizuojami?
Ar nustatyti kokybiniai IT veiklos rodikliai, kad įvertinti veiksmingumą ir naudingumą?
Įsigijimas ir diegimas
IT sprendimų identifikavimas
Ar funkcinių padalinių reikalavimai yra aiškiai nustatyti ir raštiškai patvirtinti atsakingo vartotojo prieš pradedant sistemos parinkimo ir diegimo projektą? Ar šių reikalavimų laikomasi?
Ar įvertinti visi įmanomi sprendimai kaštų ir funkcionalumo prasme? Ar įvertintos alternatyvos kurti IS patiems arba įsigyti gatavą?
Ar įvertintos visos pasirinkto sprendimo pusės (funkcionalumas, kainos/naudingumo santykis, saugumas, našumas, palaikymas)?
IS įsigijimas ir palaikymas
Ar vartotojai yra įtraukiami į sprendimo įgyvendinimo procesą?
Ar organizacijos sistemų kūrimo procesas apima visas IS naudojimo sritis (įvedimas, apdorojimas, išvestis, registravimas, apsauga, pagalba, sąsajos...)?
Ar visų IS kūrimo etapų darbo rezultatai yra dokumentuoti, patikrinti ir patvirtinti atsakingo vartotojo?
Ar Pagalbos tarnyba yra pasirengusi padėti naudotis sistema?
IT infrastruktūros įsigijimas ir palaikymas
Ar naujai įsigyjama aparatinė ir sisteminės programinė įranga yra vertinama atitikimo organizacijos strategijai, našumo, atitikimo organizacijos standartams ir integracijos į egzistuojančias sistemas požiūriu?
Ar organizacija turi ir laikosi preventyvinės aparatinės ir sisteminės programinės įrangos priežiūros procedūrų?
Ar aparatūra ir sisteminė PĮ diegiama ir prižiūrima, saugumo parametrai nustatomi pagal tiekėjo rekomendacijas?
IT procedūrų sukūrimas ir palaikymas
Ar organizacija turi nustatytą priimtiną IT veiklos lygį?
Ar vartotojų tvarkos darbui su PK ir sistemine PĮ yra parašytos, periodiškai peržiūrimos ir atnaujinamos?
Ar administratorių tvarkos darbui su Serveriais, sistemine PĮ ir tinklo įranga yra parašytos, periodiškai peržiūrimos ir atnaujinamos?
Ar yra prieinama mokymo medžiaga vartotojams ir administratoriams? Ar ji periodiškai atnaujinama?
Sistemų įdiegimas ir priėmimas
Ar organizacija turi ir vadovaujasi standartizuotą PĮ diegimo planą, kuris įtraukia bent jau: testavimą, vartotojų mokymą, sistemų integraciją, duomenų perkėlimą, saugumo nustatymą, įvedimą į gamybą, podiegiminę peržiūrą?
Ar testavimo planas apima visą IS funkcionalumą?
Ar atliekami IS pakeitimų testavimai, lygiagretus arba pilotinis testavimas rezultatų patikrinimui, galutinis priimtinumo testavimas, apsaugos nustatymų ir sąsajų su kitomis IS testavimas, testavimas realiu darbu?
Pakeitimų valdymas
Ar organizacija turi pakeitimų į IS inicijavimo, registravimo, patvirtinimo, diegimo tvarką? Ar ši formali tvarka taikoma vartotojams, IT ir tiekėjui?
Ar valdomas pakeitimų į IS procesas? Ar visi pakeitimai registruojami ir žinomas jų statusas?

Aptarnavimas ir palaikymas
Aptarnavimo lygio nustatymas ir valdymas
Ar organizacijoje yra praktika nustatyti ir susitarti dėl priimtino IT paslaugų teikimo lygio organizacijos viduje ir su išoriniais tiekėjais?
Ar yra nustatyti ir matuojami pagrindiniai IT veiklos rodikliai? Ar atsiskaitoma vadovybei?
Ar vartotojai žino ir supranta reikalautiną IT paslaugų lygį?
Aptarnaujančių organizacijų teikiamų paslaugų valdymas
Ar organizacija turi ir laikosi santykių su kitomis įmonėmis valdymo tvarkos, tame tarpe - derybos dėl sutarčių, paslaugų teikimo lygio nustatymo, pareigų ir atsakomybių nustatymo, sutarties pakeitimų istorijos, sąskaitų pateikimo istorijos, stebėjimo ir audito?
Ar tiekėjo parinkimo procesas yra skaidrus ir nepriklausomas?
Ar yra gaunami garantijos dėl tiekėjo veiklos tęstinumo, ar atliekami kitokie prevenciniai (apsidraudimo) žingsniai?
Ar reguliariai atliekamas įvertinimas dėl tiekėjo teikiamų paslaugų reikalingumo?
Sistemos funkcionavimo ir pajėgumų valdymas
Ar organizacija turi IS prieinamumo, pajėgumo, apkrovos ir išteklių planus? Ar jie reguliariai peržiūrimi, kad atitiktų vartotojų poreikius, našumo reikalavimus, technologinių naujovių įtaką?
Veiklos tęstinumo užtikrinimas
Ar organizacija turi veiklos atstatymo po kritinių situacijų (veiklos tęstinumo esant kritinei situacijai) planą? Ar jis peržiūrimas ir patikrinamas? Ar paskirtai ir apmokyti atsakingi darbuotojai?
Ar visos IT&T sistemos įtrauktos į planą?
Ar organizacija turi nustatytą rankinio informacijos apdorojimo tvarką?
Sistemos saugumo valdymas
Ar organizacija turi tvarką ir taisykles nustatant informacijos apsaugos lygius ir priėjimo teises visoms IS? Ar prašymai suteikti priėjimo teises yra tinkamai apiforminti ir patvirtinti?
Ar organizacija skiria pakankamai dėmesio apsaugant infrastruktūrą nuo nesankcionuoto išorinio įsiskverbimo?
Ar su internetu susiję projektai yra įvertinti saugumo, autorizacijos, privatumo, asmens tapatumo požiūriu?
Ar organizacija turi planus ir veda visų priėjimo prie IS taškų inventorizaciją? Ar visi šie taškai yra apsaugoti ir stebimi?
Ar organizacija turi tvarką atimti priėjimo prie IS teises iš vartotojų ir ypatingų vartotojų?
Kaštų apskaita ir valdymas
Ar IT vadovybė turi nustačiusi veiklas ir išteklius, kurie gali būti įvertinti kaštų prasme?
Ar IT biudžetas yra sudaromas įvertinant IT išteklių panaudojimo istoriją?
Ar IT veiklos kaštai yra paskirstomi funkciniams padaliniams pagal nustatytą tvarką?
Vartotojų apmokymas
Ar organizacija turi procedūrą nustatant būtinybę ir planuojant vartotojų apmokymus darbui su IS?
Ar vartotojai apmokomi informacijos ir IS apsaugos principų?
Pagalba ir patarimai vartotojams
Ar yra įkurta Pagalbos tarnyba?
Ar Pagalbos tarnyba naudoja incidentų registravimo ir eskalacijos sistemą, kad sekti savo veiklą?
Ar šios sistemos ataskaitos naudojamos planuojant mokymus, išteklių, funkcionalumo poreikį?
Sistemos konfigūracijos valdymas
Ar organizacija turi nusistačiusi sistemų bazinę konfigūraciją, kad vėliau nustatyti priimtiną sistemų veikimo lygį?
Ar organizacija turi pilną aparatinės, programinės ir telekomunikacijos įrangos inventorizacinį sąrašą (planus)? Ar inventoriaus valdymas yra automatizuotas?
Ar yra standartizuota aparatinė ir programinė įranga kad sumažinti pastangas keičiant sistemų konfigūraciją?
Problemų ir incidentų valdymas
Ar yra naudojama incidentų registravimo ir valdymo sistema?

Duomenų valdymas
Ar organizacijos tvarka yra pakankama įvedant pradinius duomenis (dokumentus), tikrinant ir taisant, tam kad į IS įvesti visą reikalingą informaciją?
Ar yra registruojamas duomenų įvedimo ir pakeitimo veiksmai?
Ar atliekamas periodinis duomenų rezervinis kopijavimas?
Ar organizacija turi tvarką informacijos išvedimui, ataskaitų spausdinimui ir platinimui, archyvavimui?
Patalpų ir įrengimų valdymas
Ar organizacija turi įsivedusi pakankamas fizinės apsaugos priemones aparatinei, sisteminei programinei įrangai ir informaciniams ištekliams?
Ar organizacija skiria dėmesį darbuotojų darbo apsaugai?
IT operacijų valdymas
Ar IT padalinys turi pagrindines kasdienines, savaitines, mėnesines ir išimtines veiklos kontrolinius sąrašus ir instrukcijas?
Ar IT padalinys turi darbo grafikus?
Ar įmanoma nutolusiu būdu valdyti IS sistemas?
Stebėjimas (monitoringas)
IT procesų stebėjimas
Ar organizacija turi nustačiusi pagrindinius veiklos rodiklius, kad įvertinti IT procesus? Ar informacija rodiklių paskaičiavimui pastoviai renkama?
Ar vykdoma vartotojų apklausa, grįžtamajam ryšiui gauti ?
Ar vadovybė reikalauja periodinės atskaitomybės iš IT padalinio, kad įsitikinti, jog jis veikia pagal organizacijos strategiją ir veiklos tikslus?
Vidinės kontrolės tinkamumo įvertinimas
Ar visoje IT veikloje projektuojamos atitinkamos vidinės kontrolės? Ar IT vadovybė pasirengusi stebėti vidines IT kontroles, vertinti jas ir atsiskaityti už jas vadovybei?
Nepriklausomas IT veiklos tinkamumo užtikrinimas
Ar organizacija reikalauja nepriklausomo įvertinimo (sertifikavimo) naujai įsigyjamoms IT paslaugoms ar sistemoms?
Nepriklausomo audito atlikimas
Ar organizacija atlieka nepriklausomą savo IT auditą?
Ar vidinis organizacijos audito skyrius pasirengęs atlikti IT auditą?

3 priedas

PAGRINDINĖS PROCESŲ IŠVADOS BEI REKOMENDACIJOS

Procesas	Išvados	Rekomendacijos
Informacinių sistemų architektūros valdymas	Sistemų architektūra ir projektiniai sprendimai nėra tinkamai dokumentuoti. VMI nedisponuoja formaliu IS architektūros modeliu bei duomenų žodynu. Tik keli IT specialistai išmano koncepcinę VMI IS architektūrą ir detaliau žino IS funkcionavimo principus.	Paskirti IT specialistus, atsakingus už visuminės IS ir IT architektūros specifikavimą, palaikymą ir pakeitimų kontrolę. Dokumentuoti (įsigyti) ir palaikyti duomenų modelio aprašymą. Reguliariai peržiūrėti IS architektūros atitikimą VMI poreikiams.
IS investicijų efektyvumas	Nėra įdiegta veiklos efektyvumo ir kokybės matavimo sistema, detalizuota iki veiklos funkcijų. Todėl sudėtinga nustatyti, ar įdiegtos IS pasiekia joms keliamus veiklos kokybės efektyvumo gerinimo tikslus	IS projektų inicijavimo metu veiklos padaliniai privalo nustatyti IS įdiegimo vertinimo kriterijus ir jais paremti projekto tikslus. Veiklos padaliniai turi tapti IS projektų iniciatoriais ir savininkais (valdytojais).
IS savininkų nustatymas	IS nėra priskirtos veiklos padaliniams ir jie nesijaučia atsakingi už IS projektų biudžetus, specifikacijų ar joms sudaryti reikiamos informacijos pateikimą, vengia prisiimti IS ir jų duomenis savo atsakomybėn.	Sukurti IS savininkų ir prižiūrėtojų funkcijas apibrėžiančias politikas ir procedūras, pavesti jiems IS projektų biudžeto valdymą, reikalavimų nustatymą, IS priėmimą eksploatavimui ir aptarnavimo lygio nustatymą bei valdymą. Toks IS kūrimo veiklos įvedimas turėtų būti vykdomas kaip atskiras projektas. Šis projektas turėtų būtinai apimti veiklos padalinių apmokymą ir naujų veiklų pilotinių IS projektų vykdymą sutinkamai su šia iniciatyva.
Aptarnavimo lygio nustatymas	Veiklos padaliniai nėra nustatę reikalavimų priimtinam IT teikiamų paslaugų lygiui. Dėl to sudėtinga matuoti ir įvertinti IT paslaugų efektyvumą ir kokybę, atskirti pagrindines IT padalinių funkcijas (atsakomybę) nuo funkcijų, kurios atliekamos esant laisviems resursams.	Nustatyti IT padalinių teises ir atsakomybę, siejant juos su kitų veiklos padalinių funkcijomis. Įdiegti Aptarnavimo lygio susitarimus tarp IT ir veiklos padalinių, kaip pagrindinį IT paslaugų teikimo ir paslaugų kokybės matavimo mechanizmą.
IS kūrimo procesas	IS kūrimo proceso kontrolė neužtikrina pakankamo IS valdymo - nekuriami formalūs reikalavimai IS, neanalizuojamas ir netvirtinamas koncepcinis IS projektas, nekuriami testų scenarijai ir neatliekamas formalus testavimas ir t.t.	Nustatyti IS kūrimo ciklo reikalavimus (ciklo etapus, žingsnius, kuriamą ir naudojamą dokumentaciją, jos šablonus ir priimtinumo kriterijus) ir suderinti reikalavimų atitikimą visuotinai priimtiems standartams.

IS saugumo sistema	IS saugumo kontrolės sistema veikia nepakankamai. Nėra apibrėžta IS saugumo politika. Informacijos saugumo lygiai neapibrėžti ir nesusieti su Duomenų modeliu. Veiklos padaliniai nėra apibrėžę reikalavimų informacijos saugumui, todėl šie reikalavimai nėra įgyvendinti kuriant IS, ko pasėkoje nesukurtas pagrindas informacijos saugumo užtikrinimui. IS saugumo auditas ir monitoringas nėra atliekami. Nėra paskirtas už IT ir IS saugumą atsakingas darbuotojas.	Paskirti IT specialistus, atsakingus už IS saugumo sistemos politikos sukūrimą, įgyvendinimą ir kontrolę. Sukurti ir įgyvendinti saugumo politiką bei ją realizuojančias procedūras. Į IS kūrimo specifikacijas privaloma įtraukti informacijos saugumo reikalavimus. Ši veikla turi būti suderinta su IS ir jų duomenų savininkų priskyrimo iniciatyva.
IT organizacijos galimybės ir jų vystymas	IT padalinių atliekamų funkcijų organizavimas, apimtis, kokybė, veiklos ir dabartinės šių padalinių galimybės netenkina VMI poreikių. IT padaliniuose trūksta aukštos kvalifikacijos specialistų. Pokyčių IT padaliniuose poreikį stipriai įtakoja ir IS plėtros planai, pagal kuriuos numatomas ženklus IS kūrimo ir diegimo apimčių padidėjimas 2002 – 2004 metais	Paskirti VMI viršininko pavaduotoją (*CIO* - IT direktoriaus atitikmuo), atsakingą už IS ir IT. Paskirti dedikuotus specialistus, atsakingus už IS saugumą, kokybę ir IS architektūros vystymą. Rasti būdų motyvuoti svarbiausius IT specialistus, perduoti išoriniams vykdytojams dalį vidinių IT funkcijų, sudaryti prielaidas IT potencialo ir jo panaudojimo vystymui.
Priėjimo prie operatyvių duomenų apribojimas	IS sistemos tiekėjų turimi priėjimai prie operatyvių VMI duomenų nėra sąlygoti IS kūrimo poreikių ir gali sukelti nepakankamai kontroliuojamus pakeitimus duomenų struktūrose ir duomenyse.	Sukurti griežtą atsakomybės ir teisių padalijimo tvarką. Išoriniai IS tiekėjai turi prieiti tik prie testavimo aplinkos ir joje laikomų duomenų. Priėjimas prie operatyvių duomenų ar kitų sistemų gali būti suteiktas tik išskirtiniais atvejais, vykdant tiksliai patvirtintas procedūras.
Veiklos tęstinumas	Nėra patvirtinto ir ištestuoto veiklos tęstinumo plano.	Sukurti IT infrastruktūrą, kuri tenkintų veiklos padalinių reikalavimus, apsprendžiančius priimtiną IS veikimo lygį. Sukurti, išbandyti ir paskelbti VMI darbuotojams nenumatytų situacijų valdymo ir veiklos atstatymo planus.

4 priedas

JUNGTINĖS KARALYSTĖS INFORMACIJOS SAUGUMO PAŽEIDIMŲ TYRIMAS

Nuo 1991 metų Jungtinės Karalystės (*United Kingdom*) prekybos ir pramonės ministerija (*Department of Trade and Industry, www.dti.gov.uk/industries/information security*) remia informacijos saugumo pažeidimo tyrimus, kurie padėtų šios šalies įmonėms ir organizacijoms geriau suprasti informacijos saugumo rizikas, su kuriomis jie gali susidurti. Septintajam Informacijos saugumo pažeidimų tyrimui ISBS 2004 (*Information Security Breaches Survey*), kaip ir ankstesniems tyrimams, vadovavo kompanija *PricewaterhouseCoopers* (*www.pwc.com/security*). Kiti šio tyrimo rėmėjai gerai visame pasaulyje žinomos kompanijos, dirbančios informacijos saugumo srityje, - *Computer Associates* (*www.ca.com/uk*), *Entrust* (*www.entrust.com*) bei *Microsoft* (*www.microsoft.com/security*). Šio tyrimo rezultatams vertinti buvo pakviesti nepriklausomi ekspertai: Informacijos patikimumo konsultacinė taryba (*The Information Assurance Advisory Council, www.iaac.org.uk*), Nacionalinis aukštų technologijų nusikaltimų padalinys (*The National Hi-Tech Crime Unit, www.nhtcu.org)* ir Londono universiteto *Royal Holloway* kolegija (www.isg.rhul.ac.uk).

Tyrimo ISBS 2004 rezultatai parodė, kad Jungtinės Karalystės (JK) visos organizacijos ir įmonės, nepriklausomai nuo veiklos jų pobūdžio ir dydžio, visapusiškai naudojasi Internetu ir pilnai gyvena informaciniame amžiuje. Tas iš esmės pakeičia organizacijų veiklos esmę, gerinant klientų aptarnavimą ir efektyvumą,. Tačiau iš kitos pusės, šios padidėjusios veiklos galimybės iššaukia šalutinį efektą, susijusį su informacijos saugumu. Šis tyrimas parodė, kad saugumo problemos dabar tapo neatsiejama visų organizacijų veiklos dalimi. Nors organizacijos ir bando visomis savo pajėgomis kovoti su šiomis grėsmėmis, informacijos saugumo incidentų skaičius ir toliau didėja. Informacijos saugumas tampa aukščiausiu prioritetu valdymo lygmenyje. Daugelis kompanijų supranta standarto BS7799 naudą ir vadovaudamos juo pas save įdiegia saugumo politiką. Jungtinės Karalystės vyriausybė šiai problemai spręsti skiria labai daug dėmesio. Įžanginiame šio tyrimo žodyje Valstybės energetikos, e-komercijos ir pašto tarnybos ministras *Stephan Timms* pažymėjo "… mūšis, kaip atsilaikyti prieš informacijos saugumo grėsmes bus ilgas, ir iki pergalės dar toli. Tačiau tai nebus mūšis, kuriame Jungtinės Karalystės verslas gali leisti sau pralaimėti".

Tyrimas ISBS 2004 į pagrindinį planą iškelia grėsmes kylančias informacijos saugumui. Nors įmonės ir organizacijos saugumui skiria daug dėmesio, tačiau jų atstovai supranta, kad jų apsidraudimas neadekvatus. Beveik kiekviena įmonė ar organizacija turi įdiegusios antivirusines programas, tačiau praėjusiais metais beveik pusėje jų sistemos buvo užkrėstos kompiuteriniais virusais. Nors kiekvienas jų daro rezervines kopijas, bet tik vienam iš dešimties pavyko atstatyti duomenis. Labai dažnai trūksta naujausių žinių ir patirties, kadangi naujos grėsmės pasirodo nuolatos.

Nenuostabu, kad dauguma respondentų informacijos saugumo perspektyvos atžvilgiu buvo nusiteikę pesimistiškai. Tačiau pasyvus laukimas nėra išeitis, ir burtininko su stebuklinga lazdele neverta laukti. Yra keletas paprastų žingsnių, padedančių sumažinti būsimų incidentų tikimybę ir poveikį. Tyrimas parodė, kad pakankamai daug organizacijų nesiėmė jokio kontrpriemonių, o paprasčiausia laukė, kol incidentas paveikė juos.

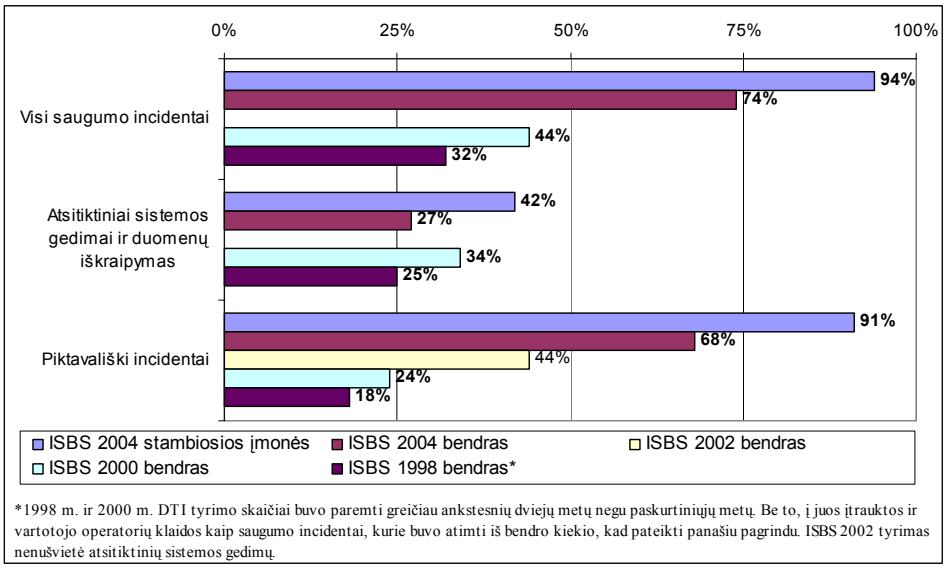
1. TRUMPA SITUACIJOS APŽVALGA.

Trumpai susipažinkime su situacija Jungtinėje Karalystėje, kurioje vyko tyrimas ISBS 2004. Kokios gi pagrindinės laikraščių antraštės? Pagrindinis pastebėjimas, kad verslo ir veiklos aplinka toliau keičiasi vis labiau naudojamas internetas. Beveik devynios iš dešimties organizacijų ar įmonių naudojasi elektroniniu paštu, naršo internete ir turi savo svetaines. Daugelyje svetainių klientams sudarytos galimybės pradėti sudaryti sutartis tiesiogiai internete. Organizacijos pradėjo masiškai naudoti belaidį tinklą. Dvigubai išaugo galimybės darbuotojams

jungtis prie sistemos, naudojant internetą ar telefoninį ryšį. Įmonių ir organizacijų priklausomumas nuo elektroninės informacijos ir sistemų nuolat didėja – 87 procentai apklaustų įmonių ir organizacijų patvirtino, kad jos tapo labiau priklausomos, palyginus su 76 procentais, kurie buvo fiksuoti prieš dvejus metus vykusiame tyrime.

Toks didelis interneto naudojimas žymiai padidino organizacijų ir įmonių neapsaugomumą nuo įvairaus pobūdžio elektroninių grėsmių. Šios grėsmės ir toliau plečiasi, su naujais virusais ir pažeidimais, identifikuojamais kiekvieną savaitę. Vidutiniškai kiekviena apklausta organizacija ar įmonė per metus gauna apie dvidešimt virusų, jų svetainės skanuojamos arba tiriamos daugelį kartų. Reikia pabrėžti, kad stambiosios įmonės atakuojamos žymiai dažniau, vidutiniškai kas savaitę gauna po virusą. Tai verčia organizacijų ir įmonių vadovybes informacijos saugumui skirti pakankamai aukštą prioritetą. Trys ketvirtadaliai organizacijų patvirtino, kad jų vykdomosios vadovybės ar direktorių tarybos informacijos saugumui skyrą aukštą arba aukščiausiu prioritetu.

Jeigu prieš dvejus metus tik kas antra įmonė patvirtino turėjusios tyčinį ar piktavališką incidentą, tai šių metų tyrimas parodė, kad jau du trečdaliai organizacijų ir įmonių turėjo tokius incidentus. Ketvirtadalis jų turėjo žymų incidentą, kurie iššaukė atsitiktines sistemos klaidas ar duomenų iškraipymus(1 pav.). Daugelio incidentų pagrindinės priežastys - virusinės infekcijos ir netinkamas darbuotojų sistemos naudojimas. Sparčiai didėjant nepageidaujamų elektroninių laiškų („Spam”) srautui, jie tampa labai rimta problema trečdaliui įmonių.



1 pav. Koks įvykusių incidentų santykis?

Labai svarbu įvertinti incidentų kainą. Tyrimo metu buvo nustatyta, kad organizacijoms rimto incidento pasekmės vidutiniškai kainuoja apie 10 000 svarų sterlingų, o stambioms siekia net iki 120 000 svarų sterlingų (2 pav.). Didžiausia šios kainos sudedamoji dalis, be jokios abejonės, yra poveikis kompanijos egzistencijai. Kai kurių organizacijų patirti nuostoliai buvo labai žymūs, sustabdė jų veiklą ilgiau kaip mėnesį laiko. Daugelis apklausos dalyvių informacijos saugumo pažeidžiamumo klausimu buvo nusiteikę žymiai pesimistiškiau, negu prieš dvejus metus.

Per dvejus metus, praėjusius nuo paskutinio analogiško tyrimo, organizacijose ir įmonėse buvo padaryta tam tikra pažanga įdiegiant saugumo kontrolės priemones. Tyrimo metu buvo nustatyta, kad trečdalis visų organizacijų ir įmonių bei du trečdaliai stambiųjų šiuo metu turi suformavusios informacijos saugumo politiką. Faktiškai visos įmonės yra įdiegusios antivirusines programas ir daugelis iš jų nedelsdamos atnaujina jas, kai tik sužino apie naujų virusų atsiradimą. Daugelyje įmonių, kurios pagal sutartis samdo trečiąsias šalis, atlikti tam tikrus IT priežiūros darbus, sutartyse aiškiai išdėstomi informacijos saugumo reikalavimai.

	Bendrai	Stambiosios įmonės
Veiklos sustabdymas	5 000 – 10 000 daugiau kaip 1 - 2 dienos	50 000 – 150 000 daugiau kaip 1 - 3 dienos
Sunaudotas laikas, sureaguoti į incidentą	500 – 1 000 2 - 4 žmogaus dienos	3 000 – 6 000 10-20 žmogaus dienų
Sunaudotos tiesioginės grynosios lėšos, sureaguoti į incidentą	1 000 – 2 000	5 000 – 10 000
Tiesioginiai finansiniai nuostoliai (turto nuostoliai, baudos ir pan.)	200 - 300	2 000 – 4 000
Reputacijos diskreditacija	100 - 300	5 000 – 20 000
Bendra vidutinė blogiausio incidento kaina	**7 000 – 14 000**	**65 000 – 190 000**

2 pav. Kiek organizacijoms vidutiniškai kainavo jų blogiausi incidentai?

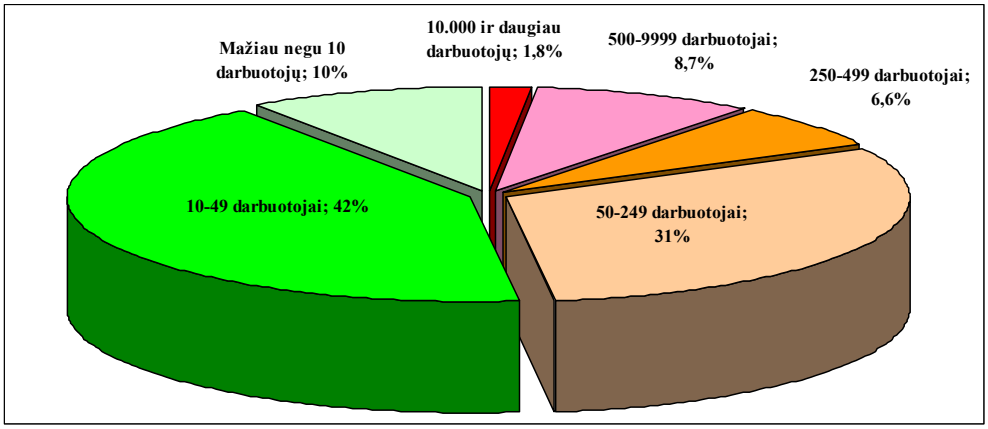
Tačiau virusai vis labiau apeina tradicines antivirusines programas ir bando pažeisti kompiuterių operacines sistemas, bet įmonės dar pakankamai aiškiai nesuvokia, kaip svarbu atnaujinti antivirusinę programinę įrangą naujausiomis versijomis. Įmonės linkusios išimtinai pasitikėti savo ugniasienėmis, kad apsaugotų nuo atakų savo interneto vartus ir svetaines. Vartotojo tapatumas ir slaptažodis vis dar dominuojantis mechanizmas patvirtinantis vartotojo tapatumą. Tačiau jau trečdalis stambiųjų įmonių perėjo prie dviejų faktorių tapatumo patvirtinimo, kad sumažintų nesankcionuotas kreiptis. Vis dar labai mažai kontroliuojamas elektroninis paštas, jungimasis per nuotolį, bevieliai tinklai. Tik kas antra įmonė savo bevieliuose tinkluose yra įdiegusios saugumo kontrolės priemones. Mažiau kaip viena iš dešimties įmonių (ir tik ketvirtadalis stambiųjų) patikrino tikrovėje savo veiklos atstatymo po incidento planus.

Viena svarbiausių priežasčių, kodėl daugelis organizacijų neskiria pakankamo dėmesio informacijos saugumui yra ta, kad joms aiškiai trūksta kompetencijos, imtis šios komplikuotos ir nuolat kintančios srities. Be to, trys ketvirtadaliai įmonių įsitikinusios, kad jų įdiegti techniniai saugumo procesai yra pakankamai sėkmingi, kad užkirstų ar aptiktų visas saugumo spragas. Įvertinus šias kontrolės priemonių silpnybes, atrodo, kad daugelis nepilnai įvertina rizikas, kurias jie valdo. Per paskutiniuosius dvejus metus nepadidėjo įmonių skaičius, kurios įdiegė standartą BS 7799. Tačiau organizacijos, įdiegusios šį standartą, suprato realią jo naudą savo veiklai. Kita priežastis dėl kurios išlaidos informacijos saugumui nors ir didėja, bet vis dar yra santykinai mažos, yra ta, kad į šias lėšas žiūrima ne kaip į investicijas, o kaip į išlaidas.

Tyrimas parodė, kad kompanijos šiuo metu informacijos saugumui vidutiniškai išleidžia 3 procentus nuo jų IT biudžeto, palyginus su 2 procentus, kurie buvo išleidžiami prieš dvejus metus. Stambiosios kompanijos tam skiria apie 4 procentus. Taigi investicijų lygis informacijos saugumui yra 5-10 procentais žemesnis už etaloninį lygį. Mažiau kaip pusė visų įmonių įvertina investicijų sugrįžimą, kurios buvo padarytos saugumui užtikrinti.

2. TYRIMO METODOLOGIJA

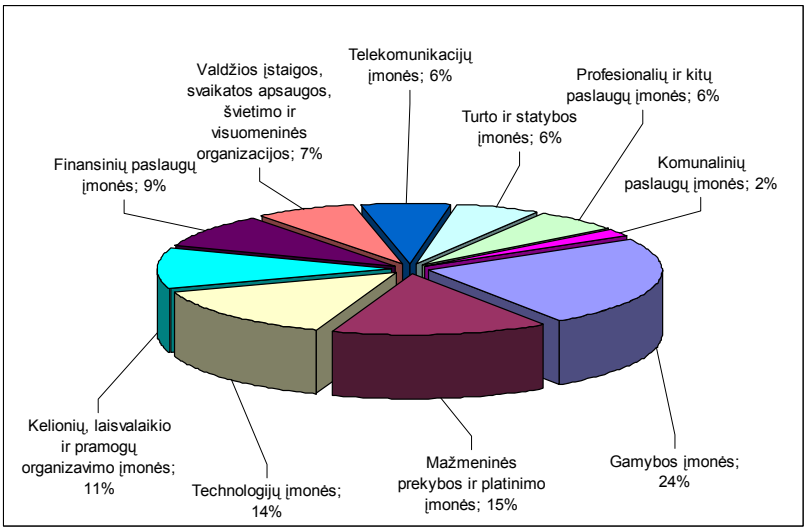
Tyrimo ISBS 2004 pagrindiniu elementu buvo pasirinktas kiekybinis tyrimas, panaudojant struktūrinį anketinį apklausimą. Įmonės buvo atsitiktinai parinktos iš Jungtinės Karalystės įmonių registro. Organizatoriai kiekvienu atveju susisiekdavo organizacijos ar įmonės darbuotoju atsakingu už informacijos saugumą. Stambiose kompanijose paprastai tai buvo IT vadovas, smulkiose – komercijos vadovai. Su kiekvienu respondentu buvo daromas 30 minučių telefoninis interviu. Apklausa vyko nuo 2003 spalio 2 d. iki 2004 sausio 30 d. 3 paveiksle pateiktas įmonių pasiskirstymas pagal darbuotojų skaičių ir jų dalis bendrame įmonių kontekste.



	Įmonių skaičius
10.000 ir daugiau darbuotojų	1
500-9999 darbuotojai	4
250-499 darbuotojai	4
50-249 darbuotojai	30
10-49 darbuotojai	176
Mažiau negu 10 darbuotojų	994
Viso:	**1209**

3 pav. Tyrime dalyvavusių įmonių pasiskirstymas pagal darbuotojų skaičių

Jungtinėje Karalystėje vyrauja smulkaus ir vidutinio verslo gamybinių ir prekybinių įmonių modelis. Tyrimo metu buvo pastebėta tendencija, kad skirtingo dydžio įmonės rodo skirtingus informacijos saugumo supratimo lygius. Todėl turimo organizatoriai, norėdami turėti prasmingas išvadas stambiosioms kompanijoms, padidino šių grupių apklausą. Įmonių pasiskirstymas pagal jų veiklos sritis pateiktas 4 pav. Ten, kur stambiųjų įmonių apklausos rezultatai žymiai skyrėsi nuo bendrųjų rezultatų, tyrimo organizatoriai juos parodė atskirai.



4 pav. Tyrime dalyvavusių įmonių pasiskirstymas pagal veiklos sritis.

Pasiremdami šiuo tyrimo bendruoju modeliu, tyrimo organizatoriai 95 procentais įsitikinę, kad paklaidos ribos atrankos procedūroms ir jų rezultatams neviršija +/- 3 procentų. Normaliai tokiems tyrimams, paklaidos ribos kinta su individualia statistika:

- esant ribiniams rezultatams (artėjant link 0 arba 100 procentų), paklaidų ribos mažėja. Pvz., buvo įvertinta, kad 93+/-1 procentas įmonių turi antivirusinę programinę įrangą.
- analizuojant rezultatus modelių dalims, paklaidų ribos didėja. Pvz., stambiųjų įmonių statistinių duomenų paklaidų ribos ne didesnės kaip +/- 8 procentai.

Taip pat reikia įvertinti, kad tam tikros klaidos, kaip ir kituose tyrimuose, galėjo atsirasti ir dėl atrankos klaidų, klausimų formulavimų, jų supratimo ir kitų praktinių sunkumų. Kaip ir bet kurio kito tyrimo trukmė, slaptumas bei greitaeigiškumas buvo pakankamai žemas. Palyginti su prieš dvejus metus vykusiu tyrimu, mažiau įmonių norėjo dalyvauti šiame tyrime. Iš dalies gal būt pasireiškė tyrimų nuovargis, dalis nenoro (padrąsinimas) atėjo iš padidėjusios rizikos supratimo, susijusios su konfidencialios informacijos pateikimo telefonu. Kai tyrimo greitaeigiškumas žemas, yra rizika, kad tyrimo modelis gali būti tendencingas. Organizatoriai tai minimizavo, garantuodami, kad modelis bus atstovaujamas atitinkamo svorio veiklos sričių ir regionų.

Reikia pažymėti, kad organizatoriai papildydami telefoninį tyrimą, atliko papildomą nuodugnų interviu „akis į akį“ su įmonių informacijos saugumo darbuotojais. Kai kurie iš jų, buvo dalyvavę ir telefoninėje apklausoje. Tokie susitikimai buvo naudojami tam, kad būtų patvirtintas telefoninių duomenų pagrįstumas ir, kad organizatoriai turėtų papildomą kokybišką informaciją.

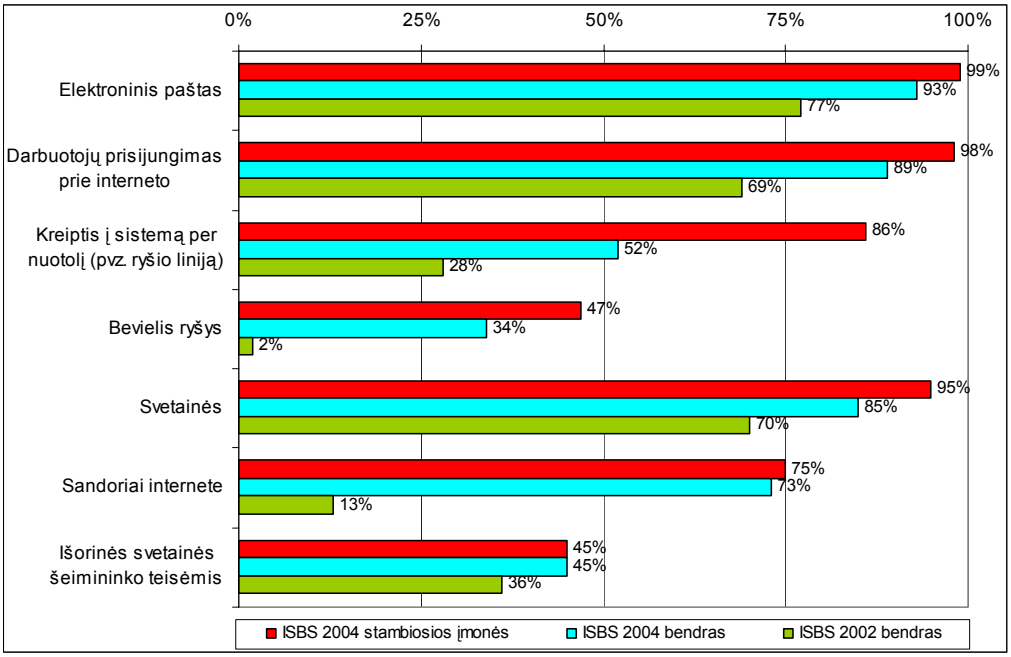
Taip pat buvo naudojama tiesioginės interneto apklausos rezultatai, kad įmonės, nepatekusios į atrinktųjų iš įmonių registro sąrašą, telefoniniams ar „akis į akį“ interviu, galėtų prisidėti prie šio tyrimo. Nors internetinės apklausos rezultatai nepateko į pagrindinę statistiką, jie buvo paminėti organizatorių komentaruose. Kaip ir visų internetinių apklausų rezultatai nėra privalomi ir į juos reikia žiūrėti atsargiai. Reikia paminėti, kad pusė internetinėje apklausoje dalyvavusių respondentų atstovavo stambiosioms įmonėms, o trečdalis smulkiosioms. Tokių savanoriškų internetinių apklausų pati prigimtis reiškia, kad respondentai patys domisi ir geriau žino nagrinėjamas problemas, nei vidutinis respondentas. Į tai reikia atsižvelgti ir aiškinant apklausos rezultatus.

3. BESIKEIČIANTI APLINKA

2002 m. tyrimo metu fiksuotas Interneto naudojimo bumas, tęsiasi iki šių dienų (5 pav.). Smulkus ir vidutinis verslas vis labiau suvokia naudą, kurią gali atnešti internetas. Pasaulinis tinklas ir elektroninis paštas - kasdieninis dalykas įvairaus dydžio įmonėse. Technologijų ir telekomunikacijų srityse veikiančios įmonės užima pirmaujančias pozicijas. Devynios iš dešimties įmonių suteikia galimybę savo darbuotojams jungtis prie interneto. Labai gaila, bet visa tai lydi šalutinis efektas – virusų infekcijos, netinkamas interneto ir elektroninio pašto naudojamas, nepageidaujami elektroniniai laiškai.

Daugelis įmonių turi savo nuosavas interneto svetaines. Prekybos, kelionių ir paslaugų įmonės šioje srityje užima pirmaujančias pozicijas. Tuo tarpu energetikos, sveikatos apsaugos ir švietimo įmonės atsilieka. Žymiai išaugo įmonių skaičius, teikiančių e. paslaugas. Smulkios ir vidutinės įmonės klientams suteikia galimybę per internetą naudotis savo išoriniais sandėliais arba leidžia elektroniniu paštu daryti užsakymus. Tuo tarpu stambiųjų įmonių svetainės pilnai integruotos į pagrindinį verslą. Per internetą sudaromų sandorių apimtys auga. Tuo pačiu tempu didėja ir potenciali saugumo incidentų įtaka, tokia kaip mėginimai įsilaužti į duomenų bazes, paslaugų atsisakymas ir t.t.

Prieš dvejus metus buvo pastebėta tendencija - leisti darbuotojams jungtis iš išorės prie įmonės informacinės sistemos. Per paskutiniuosius pora metų kreiptis per nuotolį išaugo beveik dvigubai. Beveik pusė visų įmonių tai daryti savo darbuotojams leidžia. Stambiosios įmonės šioje srityje tęsia naujos mados tendencijas. Technologijų, telekomunikacijų ir energetikos įmonės čia yra pradininkai, o žemės ūkio ir turto įmonės tokia galimybe naudojasi mažiausiai. Tuo pačiu metu kreiptis per nuotolį, leidžianti pasiekti įmonei didžiausią lankstumą, gali tapti labai rimta spraga saugumo perimetre.



5 pav. Veiklos aplinkos pokytis per 2002-2004 metų laikotarpį.

Jeigu 2002 m. bevielis tinklas buvo ankstyvoje stadijoje, tai visiškai nenuostabu, kad dabar bendras naudojimas šiuo tinklo padidėjo nuo 2 iki 34 procentų. Beveik kas antra įmonė turi bevielį tinklą. Technologijų ir telekomunikacijų įmonės ir čia yra lyderiai. Tačiau bevielio tinklo raida santykinai atsilieka dėl nepakankamai subrendusios technologijos. Čia dar lieka daug neišspręstų vartojimo, saugumo ir kainų problemų. Kadangi šios ypač greitos bevielės paslaugos buvo pradėtos teikti visiškai neseniai, stebima tendencija, kad jos yra labai priklausomos nuo abonentinio ir minutės mokesčio. Todėl jos šiuo kaip verslo instrumentas dar negali būti plačiai naudojamos.

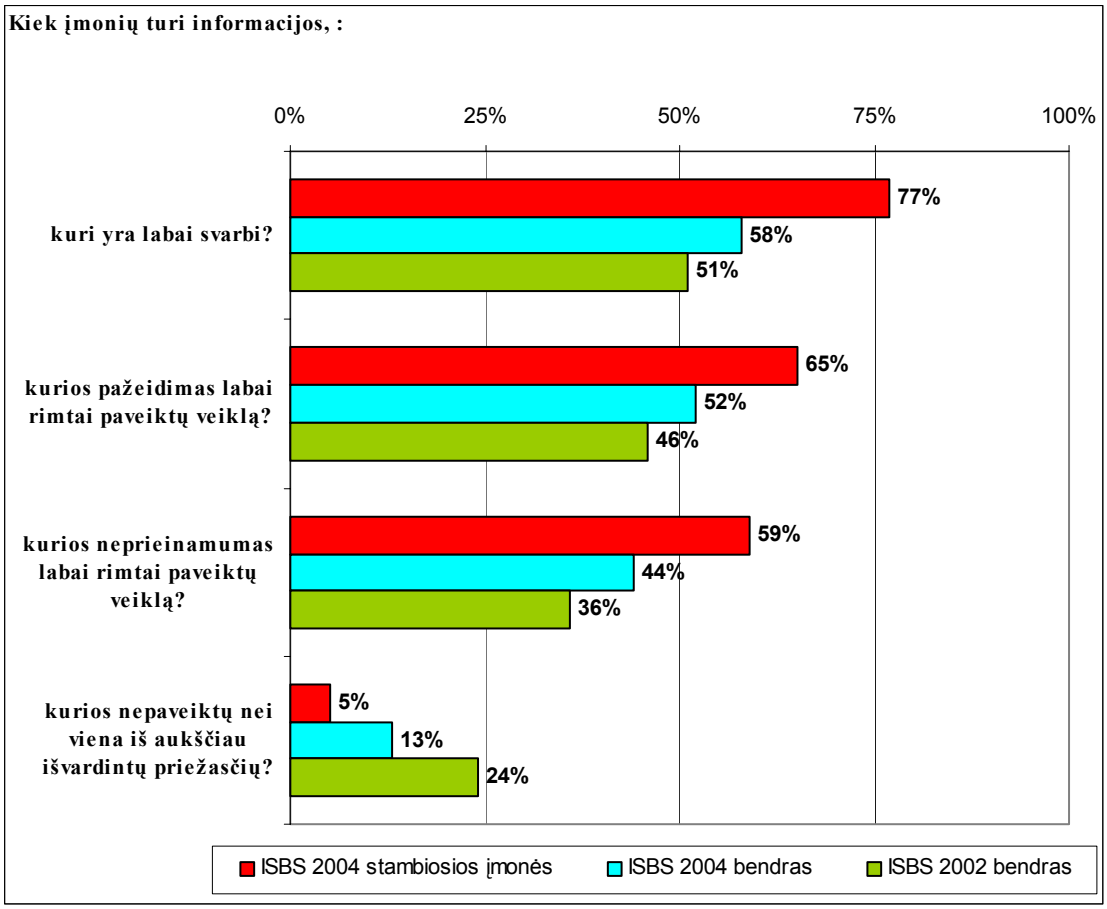
Apie pusė visų įmonių dabar naudojasi trečiųjų šalių paslaugomis, kuriant taikomąją programinę įrangą, atliekant jos priežiūrą, administruojant informacines sistemas, teikiant svetainių šeimininkų ar pagalbos tarnybos paslaugas. To pasėkoje, daugelis įmonių dabar priklauso ir nuo jų trečiųjų šalių informacijos saugumo lygio. Daugelis stambiųjų įmonių perduoda įvairių sistemų eksploatavimą į žemesnės kainos šalis, tokias kaip Indija ar Kinija. Toks „nutolęs“, nepatenkantis į valstybės reguliavimo sferą, sistemų eksploatavimas daro saugumo kontroliavimą ar darbuotojų sąmoningumo ugdymą žymiai sunkesniu.

Taip nyksta tradicinės ribos tarp organizacijų. Pokyčių tempas ir toliau didėja. Norint būti šių pokyčių viršūnėje, iš bet kurio veiklos reikalaujama daug laiko, jau nekalbant apie patikimus pakeitimus daromus saugumo ir patikimumo srityje.

4. POŽIŪRIS Į INFORMACIJOS SAUGUMĄ

Šiuolaikiniame pasaulyje informacija vertinama kaip gyvybinės jėgos šaltinis įvairiai veiklai. Šis tyrimas parodė, kad Jungtinės Karalystės įmonės vis labiau supranta duomenų konfidencialumo, vientisumo ir prieinamumo svarbą. Tiems, kuriems kompiuterio naudojimas yra antraeilis dalykas, nuo 2002 m. sumažėjo perpus. Tyrimas parodė svarbių duomenų informacinėse sistemose saugoja žymiai daugiau įmonių negu prieš dvejus metus. Daugiau kaip pusė įmonių slaptus savo duomenis laiko kompiuteriuose. Valdžios institucijos, sveikatos apsaugos ir finansinių paslaugų sektoriai kompiuteriuose saugoja ypač svarbius duomenis. Gamybininkai ir žemės ūkio įmonės tokių duomenų turi mažiausia. Daugiau nei pusė visų tyrime dalyvavusių įmonių pripažino, kad informacijos praradimas jų veiklai turėtų žymų neigiamą poveikį (6 pav.). Labai didelė tikimybė, kad stambiąsias įmones (telekomunikacijų,

technologijų ir gamybos) informacijos praradimas paveiktų labai skaudžiai. Mažesnį neigiamą poveikį patirtų žemės ūkio, turto ir statybos įmonės.

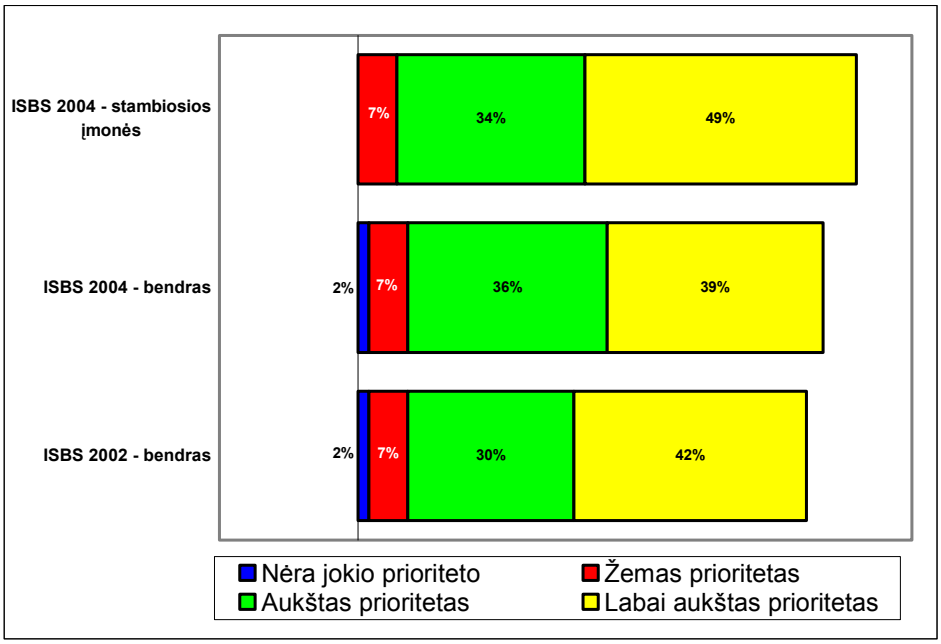


6 pav. Informacijos svarbumas.

Beveik pusė visų įmonių, kad būtų užtikrinta normali jų veikla, dabar labai priklauso nuo informacinių sistemų tinkamo veikimo. Duomenų vientisumas šiuo metu yra svarbus kaip niekada ir yra nuolatinis galvos skausmas visuose be išimties sektoriuose. Tačiau stambiosios įmonės ir vėl labiausiai yra priklausomos nuo informacinių sistemų darbo.

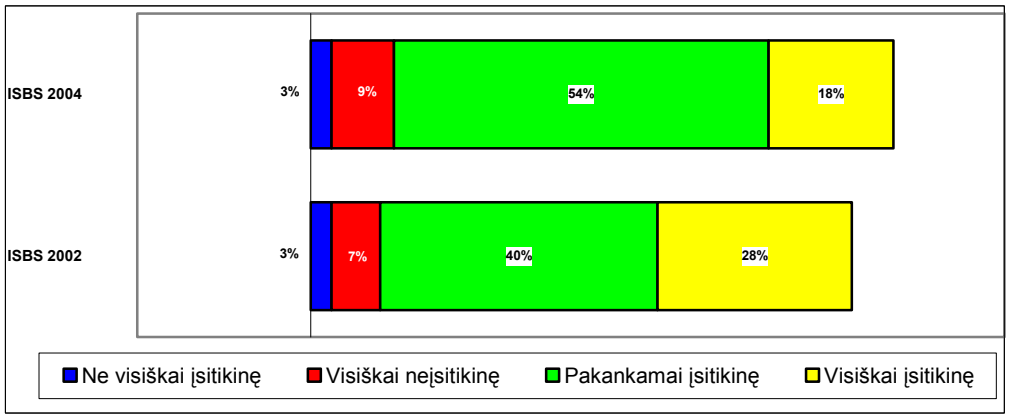
Po rugsėjo 11 dienos įvykių Jungtinėse Valstijose, jau 2002 m. tyrimas parodė įmonių vadovybių padidėjusį dėmesys informacijos saugumui. Dveji metai saugumo klausimai kiekvienos įmonės vadovybės dienotvarkėje užima pakankamai svarbią vietą (7 pav.). Trys ketvirtadaliai įmonių saugumui skiria aukštą arba labai aukštą prioritetą. Aukščiausias prioritetas saugumui yra skiriamas stambiosiose įmonėse, kur penkios iš šešių į tai žiūri rimtai. Kiekvienas finansinių paslaugų respondentas jautė, kad saugumas - tai labai svarbu. Žemės ūkio ir mažmeninės prekybos įmonės nors ir mažiausiai buvo susirūpinusios saugumu, bet net 60 procentų jų saugumui skyrė aukštą prioritetą.

Vienos telekomunikacinių paslaugų įmonės saugumo vadovas kiekvieną mėnesį valdybai teikia ataskaitą apie informacijos saugumo problemas. Ataskaitoje pateikiamas virusų incidentų skaičius, informacija apie išorinius skanavimus ir interneto tyrimus. Valdybos direktoriai atsisakė tikėti jo teikiama statistika ir kitame biudžeto sudarymo cikle jie nusprendė žymiai padidinti biudžetą, skirtą saugumo stebėjimo įrankiams įsigyti.



7 pav. Kokį prioritetą informacijos saugumui suteikia įmonių vadovybės ar direktorių tarybos?

2002 m. tyrimas kaip vieną iš svarbiausių susirūpinimų iškėlė pernelyg didelį darbuotojų, atsakingų už informacijos saugumą, pasitikėjimą. Per paskutiniuosius dvejus metus pasitikėjimo lygis išlieka toks pat aukštas. Beveik trys ketvirtadaliai įmonių tiki jų saugumo kontrolės priemonėmis, kad jos užkirs kelią arba suras visas žymesnes saugumo spragas (8 pav.) . Nors įmonių skaičius, kurios labai pasitiki šiomis priemonėmis, sumažėjo 10 procentų. Įvertinus supančią aplinką ir nuolat didėjantį įvairių incidentų skaičių tai neturėtų būti keista.



8 pav. Kaip atsakingi už informacijos saugumą darbuotojai įsitikinę, kad jiems pavyko sugauti visus jų įmonėje įvykusius žymius saugumo pažeidimus?

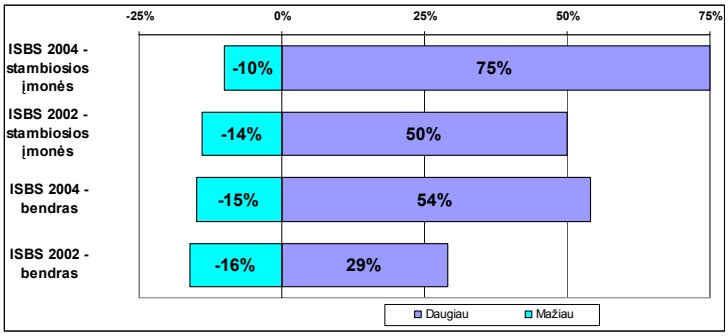
Pasitikėjimas saugumo priemonėmis pats aukščiausias finansinių paslaugų sferoje. Tai atspindi direktorių valdybų sprendimai informacijos saugumui suteikti aukštus prioritetus. Pasitikėjimas yra žemesnis profesionalių paslaugų ir energetikos įmonėse. Abiejuose šiuose sektoriuose yra daug darbuotojų, turinčių priėjimą prie slaptos įmonės informacijos per internetą arba ryšio linijas. Pats žemiausias pasitikėjimas žemės ūkio įmonėse, kur informacijos saugumui neskiriama daug dėmesio.

Tiesioginės internetinės apklausos respondentai parodė ypatingą supratimą saugumo klausimais. 76 procentai respondentų nurodė, jog jų įmonė naudojasi labai slapta informacija ir

78 procentai respondentų buvo susirūpinę galimu duomenų praradimu. 5 procentų respondentų jautė, kad jų įmonės vadovybė suteikia informacijos saugumui per žemą prioritetą. Įdomu pažymėti tą faktą, kad jie buvo mažiau užtikrinti saugumo kontrolės priemonėmis, nei respondentai, dalyvavę telefoninėje apklausoje. Nežiūrint į turimas patikimas saugumo kontrolės priemones, dvigubai tiek pat nebuvo užtikrinti jų gebėjimu surasti visas saugumo spragas. Susidaro įspūdis, kad kuo daugiau respondentai žino, tuo mažiau jie užtikrinti.

5. ŽVILGSNIS Į ATEITĮ

Jeigu 2002 m. atliktame tyrime Jungtinės Karalystės įmonės buvo pesimistiškai nusiteikę informacijos saugumo ateities perspektyvos atžvilgiu, tai po dvejų metų jų pesimizmas dar labiau padidėjo. Nežiūrint į didelį tikėjimą esamomis kontrolės priemonėmis, daugiau kaip pusė visų įmonių įsitikinusios, kad ateityje informacijos saugumo incidentų tik didės (9 pav.). Tik 15 procentų respondentų galvoja, kad jų turėtų mažėti. Labiau susirūpinusios yra stambiosios įmonės, ypač tos kurios teikia finansines paslaugas. Profesionalių paslaugų ir žemės ūkio įmonės susirūpinusios mažiausiai, bet ir čia pesimistiškai nusiteikusių yra dvigubai daugiau negu optimistiškai.

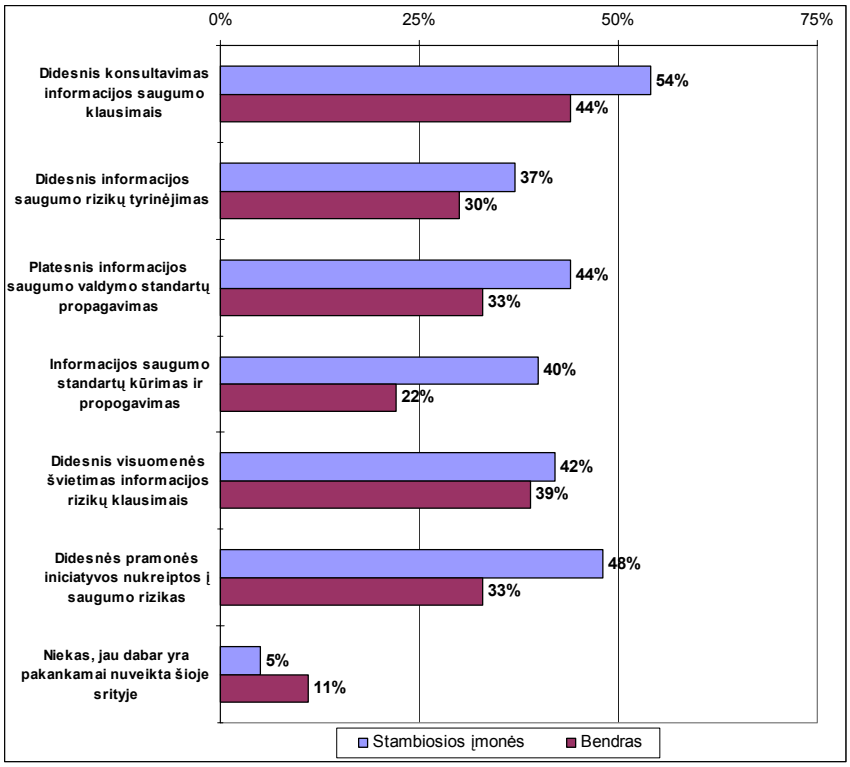


9 pav. Kiek incidentų daugiau tikimasi ateinančiais metais, lyginant su praėjusiais metais?

Labai panašiai respondentai atsakė į klausimą „Ar ateityje bus lengviau/sunkiau aptikti saugumo pažeidimus“ (10 pav.). Daugiau kaip 2,5 karto respondentai atsakė, kad ateityje saugumo spragas bus vis sunkiau aptikti, negu tų kurie galvojo, kad tai padaryti bus lengviau. Tai irgi pesimistiškesnis vertinimas, negu buvo prieš dvejus metus. Iš visų sektorių tik telekomunikacinių paslaugų tiekėjai buvo nusiteikę nežymiai optimistiškiau.

Tyrimo organizatoriai atsižvelgę į tokį neigiamą perspektyvos vertinimą, respondentų paklausė, kas padėtų jiems valdyti informacijos saugumo rizikas. Apie pusę jų mano, kad labai naudingos būtų trečiosios šalies konsultacijos informacijos saugumo klausimais, tame tarpe ir šalies Vyriausybės. Įdomu pažymėti, kad stambiosios įmonės, kurios yra labiausia pažengusios informacijos saugumo valdymo srityje, labiausia ir jaučia tokių konsultavimų poreikį. Žemės ūkio sektoriaus įmonės, kuriose saugumas turi patį žemiausią prioritetą, iš tokių konsultavimų matė pačią mažiausią naudą.

Pakankamai didelis procentas respondentų mano, kad labai naudingas būtų visuomenės švietimas informacijos saugumo klausimais. Santykinai mažas prioritetas duodamas tam, kad įmonės daugiau dėmesio skirtų savo darbuotojų švietimui. Vienas nedidelis bankas pripažino, kad nepakankamas vartotojų mokymas, gali būti didžiausioji grėsmė jų internetinėms banko operacijoms. Jų bankas neseniai patyrė palyginti naujo būdo sukčiavimą – vadinamą „žvejyba“ (*phishing*), kai nusikaltėliai bankų klientams išsiuntinėjo elektroninius laiškus su prašymu patvirtinti informaciją apie savo sąskaitas. Klientas buvo siūloma užpildyti specialią formą (tame tarpe įvesti slaptažodžius), patalpintą suklastotame banko interneto tinklapyje. Suprantama, iš išorės šis tinklapis buvo praktiškai identiškas tikrajam banko tinklapiui. Todėl jeigu nesikeis visuomenės elgesys, internetinė bankininkystė masinei rinkai ateityje gali būti pasmerkta.



10 pav. Kas labiausiai galėtų padėti įmonėms valdyti informacijos saugumo rizikas?

Vienas trečdalis respondentų mano, kad būtų naudingas platesnis informacijos saugumo valdymo standartų, tokių kaip BS 7799, propagavimas. To labiausiai norėjo telekomunikacinių paslaugų tiekėjai ir vyriausybės institucijos, o mažiausiai finansinių paslaugų, sveikatos apsaugos ir švietimo įstaigos. Daugelis įmonių, buvo labai suinteresuotos gauti papildomos informacijos, pritaikytos jų reikmėms

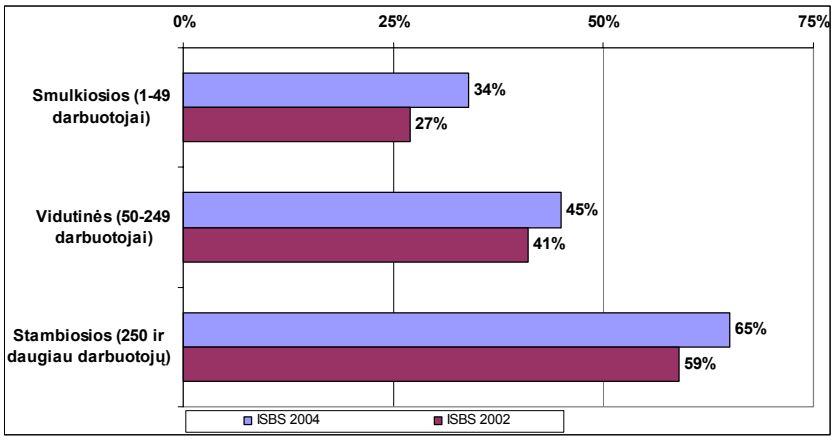
Analogiškas respondentų skaičius norėtų, kad daugiau iniciatyvos, kaip valdyti saugumo rizikas, rodytų pramonė. Tą ypač akcentavo mažmeninės prekybos ir leidybos įmonės. Stambiosios įmonės norėjo šioje srityje dirbti kartu su pramonės įmonėmis. Tik viena iš dešimties įmonių teigė, kad jau buvo pakankamai nuveikusios informacijos saugumo srityje. Įvertinus tokį įmonių ateities rizikų supratimą, galima teigti, kad daugelis įmonių tikrai nori didesnės pagalbos.

6. SAUGUMO SUPRATIMAS

Pirminė daugumos saugumo spragų priežastis – žmogaus, bet ne technologinės klaidos. Daugeliui įmonių labai svarbu sukurti sąmoningą saugumo kultūrą, padedančią darbuotojams išsiugdyti atsakomybės jausmą, veikti protingai ir saugiai. Kaip parodė šis tyrimas, šioje srityje progresuojama labai lėtai, daugelis įmonių atrodo nenori ar negali investuoti į personalo sąmoningumo ugdymą.

Bendrai paėmus trečdalis įmonių turi įsidiegusios informacijos saugumo politiką. Tai nežymus padidėjimas palyginus su 2002 m. tyrimu. Atrodytų, toks žemas rezultatas prieštarauja tam, kad trys ketvirtadaliai įmonių informacijos saugumui teikia aukštą prioritetą. Patį geriausią rezultatą rodo finansinių paslaugų įmonės - net trys ketvirtadaliai jų turėjo įsidiegusios saugumo politiką. Gerą supratimą taip pat parodė ir tiesioginės internetinės apklausos respondentai – 71 procentų jų turėjo įsidiegę saugumo politiką. Priešingai, tokią politiką turėjo įsidiegusios tik viena iš penkių prekybos ir žemės ūkio įmonių. Be aiškios ir suprantamos politikos, gali būti sunku imtis drausminančių priemonių prieš personalą, neteisingai

naudojančių informacines sistemas. Labai dažnai, įmonėje įdiegta saugumo politika pradeda išvengti skaudžių incidentų.

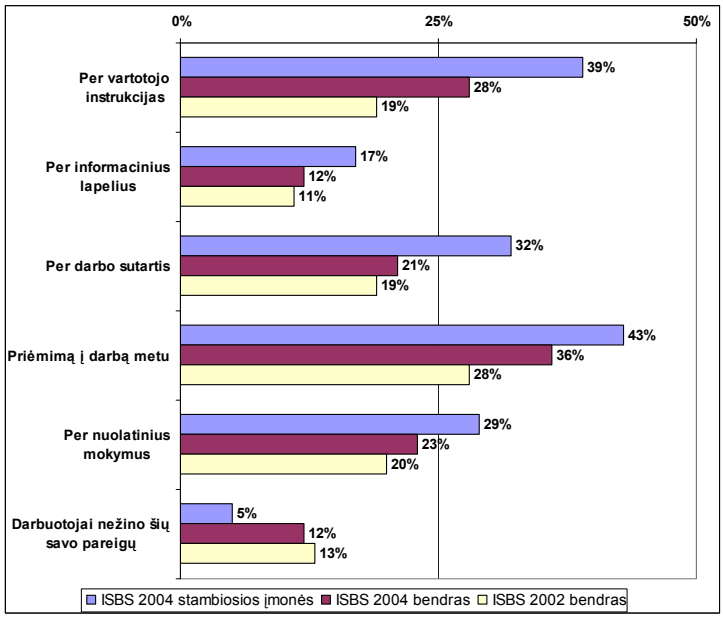


11 pav. Kiek įmonių turi formaliai apibrėžtą ir patvirtintą informacijos saugumo politiką?

Nedidelė draudimo kompanija turėjo tam tikrų sunkumų po to, kai atleido vieną savo darbuotoją, kuris darbo metu lankydavosi pornografijos svetainėse. Atleistasis darbuotojas teisme teigė, kad jo atleidimas iš darbo buvo neteisėtas, nes jis nepažeidė jokių įstatymų ar kompanijoje nustatytos tvarkos. Savo ruožtu ši kompanija tuo klausimu tikrai neturėjo nustatytos aiškios politikos, ir buvo priversta gražiuoju tarti su buvusiu savo darbuotoju.

Tačiau šiandien vien turėti saugumo politikos aiškiai nepakanka. Kadangi įmonių veiklos aplinka kartu su saugumo rizikomis nuolatos keičiasi. Politika būtinai turi atitikti šiandieninius reikalavimus. O ir pačios įmonės organizacinė struktūra retai kada yra statiška, atsirandančios naujos sistemos ir technologijas, įtakoja saugumą. Labai dažnai yra taip, kad įmonėse įdiegta saugumo politika neina koja kojon su įmonės veiklos prioritetais.

Labai svarbus faktorius yra bendravimas. Geriausia pasaulyje politika bus bevertė, jeigu apie ją niekas nežinos (12 pav.). Įmonės darbuotojai su politikos pasikeitimais turi būti supažindinami veiksmingais metodais, o naujieji darbuotojai su ja turi būti supažindinti iš karto, kaip tik pradeda dirbti.

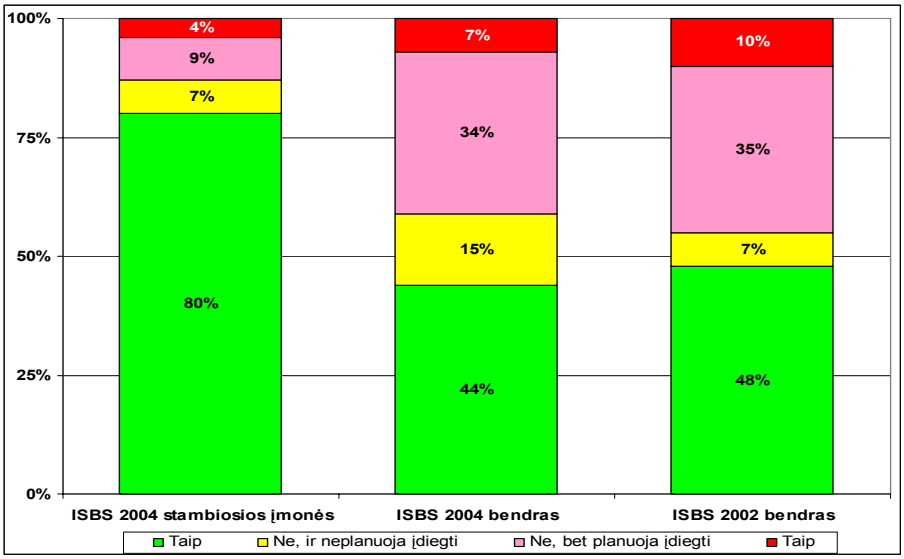


12 pav. Kaip darbuotojai sužino apie savo pareigas informacijos saugumui?

Jau prieš dvejus metus atliktame tyrime buvo matyti, kad daugelis įmonių buvo įtraukusios supažindinimą su įmonės saugumo politika į personalo rengimo programą. Nuolat didėja ir bendravimas saugumo klausimais su naujai priimamais darbuotojais. Kiti galimi supažindinimo mechanizmai - informaciniai lapeliai ir nuolatinis mokymas, kaip nebūtų gaila, per pastaruosius metus nelabai pasistūmėjo į priekį. Viena iš aštuonių įmonių vis dar negali personalui išaiškinti, kad jis suprastų savo pareigas. Šis rodiklis per pastaruosius du metus beveik nepasikeitė.

Darbuotojų kvalifikacijos tikrinimas personalo verbavimo metu, taip pat yra svarbus veiksnys, norint turėti stiprią informacijos saugumo kultūrą. Tai darančių įmonių skaičius išlieka stabilus – 43 procentai įmonių nuolatos seka informaciją, atlieka pasitikėjimo kontrolę ar imasi kitų panašių veiksmų, 14 procentų apsiriboja patikrinimais, o 9 procentų patikrinimus atlieka tik retkarčiais. Labai gaila, bet trečdalis įmonių, priimdamos į darbą darbuotojus, elgiasi labai avantiūriškai, netikrina būsimų darbuotojų tapatybės ir kvalifikacijos. Panašiai elgiasi ne tik smulkiosios, bet net ir stambiosios įmonės.

Tyrimo organizatoriai mėgino išsiaiškinti, kaip Jungtinės Karalystės įmonės laikosi Duomenų apsaugos įstatymo (lietuviškas atitikmuo - Asmens duomenų teisinės apsaugos įstatymas), kuris šioje šalyje galioja šešerius metus. Tik 44 procentai įmonių turėjo dokumentuotas procedūras, kurių reikalavo šis įstatymas, 15 procentų jų planavo jas įdiegti. Palyginus su ISBS 2002 tyrimu pastebimas nežymus įmonių skaičiaus sumažėjimas, kurios tvirtino, kad tokias procedūras yra įdiegusios (13 pav.).



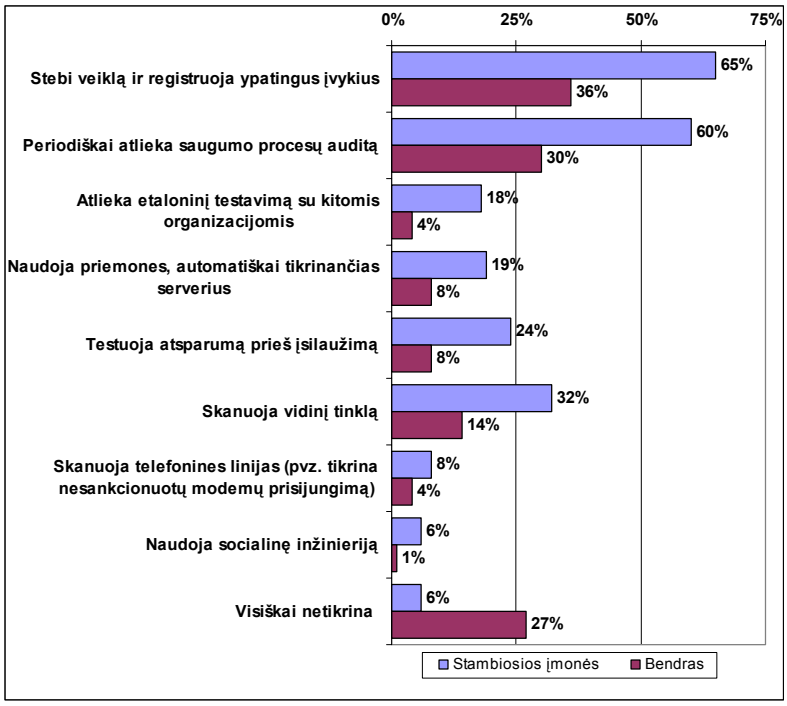
13 pav. Ar įmonės turi įteisintas procedūras, patvirtinančias, kad ji atitinka 1998 m. Duomenų apsaugos įstatymo reikalavimus?

Net trečdalis kompanijų neplanavo įdiegti tokių procedūrų. Nors tai beveik atitinka 2002 m. tyrimo parodymus. Bet tai kelia nerimą, nes beveik kiekviena įmonė informacinėje sistemoje saugo slaptą informaciją apie piniginius išmokėjimus savo darbuotojams, o šio įstatymo 7 principas reikalauja saugoti savo darbuotojų asmeninius duomenis. Tačiau kai kurios įmonės arba nieko nežino apie tokių duomenų saugojimo įsipareigojimus arba tam skiria labai žemą prioritetu savo veikloje. Todėl jeigu įmonėse neįdiegta saugumo politika, labai sunku patikrinti, ar šie duomenys yra saugūs. Žymiai geresnė padėtis yra stambiosiose ir finansinių paslaugų įmonėse, o blogiausia prekybos ir gamybos įmonės.

Apklausos metu, kai kurie finansinių paslaugų sektoriaus respondentai komentavo įvairių įstatymų ir taisyklių turinį. Jie nurodė keletą įstatymų reikalavimų, prieštaraujančių vienas kitam. Taigi duomenų apsauga visoje šalyje pakankamai komplikuota.

Darbuotojų informacijos saugumo sąmoningumo kultūra turi atitikti organizacijos saugumo politikai ir labai svarbu turėti kontrolės mechanizmą, kaip darbuotojai laikosi saugumo

politikos reikalavimų. Daugiau kaip pusė finansinių paslaugų įmonių kontroliavo veiklą ar registravo ypatingus įvykius (14 pav.). Tuo tarpu tai darė tik 8 procentai žemės ūkio įmonių. Trečdalis įmonių periodiškai atliko tikrinimus ar įmonės veikla atitinka saugumo politikos reikalavimus. Čia geriausius rezultatus parodė energetikos įmonės, o prasčiausius telekomunikacinių paslaugų tiekėjai.



14 pav. Kaip įmonės tikrina ar laikomasi patvirtintos saugumo politikos reikalavimų?

Vis plačiau sistemų pažeidžiamumui tikrinti įmonės naudoja automatizuotus instrumentus. Trečdalis stambiųjų įmonių skanuoja savo vidinį tinklą, šiek tiek mažiau atlieka testavimą prieš įsilaužimą ir tikrina nesankcionuotų modemų prisijungimą. Šešis kartus padidėjo socialinės inžinerijos naudojimas. Tokie akli testavimai pateikia naujausią požiūrį ir realybės patikrinimą tikram saugumo lygiui. Plačiausiai automatizuotas priemones naudoja finansinių paslaugų ir vyriausybinis sektorius, tuo tarpu, kaip nebūtų keista, technologijų įmonės yra tarp tų sektorių, kurie tai daro mažiausiai.

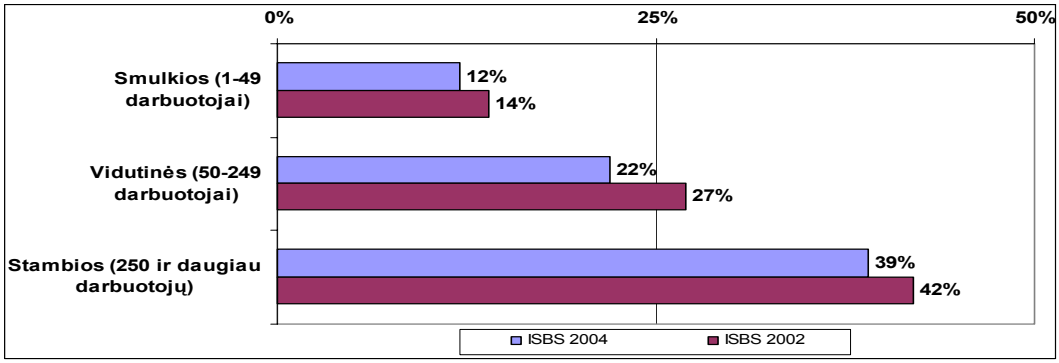
Šiame tyrime paminėtas vienas įdomus atvejis, kai viena įmonė įgaliojo kitą įmonę atlikti socialinius techninius bandymus. Rezultatai buvo neįtikėtini, parodę kaip lengva prieiti prie to, ką įmonė laikė saugiausia pastato dalimi. Jų mėgstamiausias triukas - apgauti ginkluotą apsaugą, sugalvojus dingstį įteikti gimtadienio tortą nuo tariamų partnerių ar jų bendradarbio žmonos. Įmonės vadovybė buvo priversta suprasti, kiek dar daug reikia dirbti gerinant saugumą.

7. STANDARTO BS7799 ĮDIEGIMAS

Britanijos informacijos saugumo valdymo standartas BS7799 plačiai pripažintas kaip svarbi informacijos saugumo sistema. 2000 m. gruodžio mėn. šio standarto Pirmosios dalies pagrindu buvo priimtas tarptautinis standartas ISO/EC 17799, kurį įvairių šalių įmonės vis labiau ir labiau naudoja, formuodamos savo saugumo procesus. Standarto BS 7799 Antroji dalis apibrėžia identifikuotų saugumo reikalavimų valdymo sistemą ir naudoja geriausią valdymo praktiką, apibrėžtą standarte ISO/EC 17799. Standartas nuosekliai, žingsnis po žingsnio, apibrėžia procesą, kuris gali būti naudojamas projektuojant, diegiant ir prižiūrint efektyvią informacijos saugumo valdymo sistemą. Standartas BS7799 padeda organizacijoms

įvertinti tiek jų pačių, tiek ir jų verslo partnerių informacijos saugumo procedūras, nustato praktinius principus ir pateikia rekomendacijas.

2002 m. tyrimas parodė, kad standarto BS 7799 supratimo lygis buvo nuviliančiai mažas. Po dviejų metų šis paveiksliukas ne tik kad nepasikeitė, bet šio standarto supratimo lygis net sumažėjo. Tik 12% specialistų atsakingų už informacijos saugumą prisipažino, kad jie žino šio standarto turinį. Stambiose įmonėse šis lygis siekė iki 39% (15 pav.), bet ir tai labai žemas lygis.



15 pav. Kokia dalis įmonių yra susipažinusi su standartu BS7799?

Daugiausia susipažinusių su šio standarto turiniu buvo telekomunikacinių paslaugų įmonėse ir valstybės institucijose, mažiausiai, tik 4 procentai - turto ir statybos įmonėse. 73 procentai tiesioginės internetinės apklausos respondentų prisipažino, kad yra susipažinę su šiuo standartu.

Kodėl šis standartas nėra taip plačiai pripažintas ir naudojamas šalies įmonėse? Paprastai įvardijama aukšta standarto BS 7799 kopijos įsigijimo kaina. Dabartiniame informacinių technologijų pasaulyje labai užimti profesionalai, naudodami internetines paieškos sistemas, tikisi iš karto rasti reikiamą informaciją. Daugelis įmonių tikisi įsigyti standartą nemokamai ir elektroninėje formoje.

Kita priežastis yra ta, kad daugelis smulkių įmonių nors ir supranta standarto BS 7799 svarbą, bet linkusios naudoti stambiųjų įmonių parengtus modelius. Jos galvoja, kad įdiegti šiam standartui reikalinga didelė ekspertizė, daug laiko ir tai brangiai kainuoja.

Tos organizacijos, kurios susipažįsta su šiuo standartu, vis labiau jį priima. Daugiau kaip pusė iš jų šiuo metu dalinai ar visiškai pritaria jo reikalavimams, palyginus su 38 procentais užfiksuotais 2002 m. Tai pakankamai dėsningas pavyzdys pramonės įmonėms. Efektyvumo ir našumo siekimas, veda į šio standarto įgyvendinimą. Įmonių skaičius, kurių atitikimą šiam standartui peržiūri ar pripažįsta nepriklausomos trečiosios šalys, išliko visiškai nepakitęs.

Vienas bankas standarto BS 7799 priėmimui pritaikė 80:20 principą - vienintelį tikrą efektyviai dirbančių žmonių ir organizacijų dėsnį, kai 80 procentai rezultatų lemia tik 20 procentų priežasčių, ir pasiekė tam tikrų greitų pergalių. Jo, kaip Britanijos Standarto vardas, padėjo lengvai įtikinti banko vadovybę. Nors šio banko prioritetu ir nebuvo šiandien tapti visuotinai pripažintu, bet jis tokiu siekė tapti ateityje. Jam reikėjo labai nedaug ką pakeisti, pradedant nuo įdiegimo.

Pirmą kartą šių metų tyrimo metu organizatoriai apklausė įmones, kaip standartas BS 7799 pakeitė jų požiūrį ir elgesį į pačią saugumo politiką, saugumo organizavimą, sistemų kūrimą, priežiūrą ir į daugelį kitų reiškinių. Nuo 30 iki 50 procentų respondentų pareiškė, kad susipažinus su šio standartu, jų požiūris ir elgesys pasikeitė nežymiai, o nuo 20 iki 30 procentų respondentų pažymėjo, kad jų požiūris ir elgesys pasikeitė žymiai. Be to, daugelis įmonių buvo priverstos pripažinti spragas egzistuojančiuose procesuose ir pakeisti naudojamus saugumo metodus daugelyje sričių.

Daugelis sutiko, kad standarto BS 7799 Antrosios dalies įdiegimas suteikė įmonėms naudą – 87 procentai jautė, kad tai pagerino jų verslo tęstinumą, 85 procentai tikėjo sumažinti jų kompanijos pažeidžiamumą įvykus saugumo incidentams, 53 procentai komentavo, kad padidėjo investicijų grąža ir veiklos galimybes. Šie rezultatai teikia vilčių, kad įmonių investicijos į saugumo valdymą susilauks realaus atpildo.

8. SAUGUMO PATIRTIS IR KOMPETENCIJA

2002 m. tyrimas atskleidė aiškias žmonių, atsakingų už informacijos saugumą, žinojimo spragas. Po dviejų metų ši spraga pasirodė gili kaip niekada. Tai nieko neturėtų stebinti, dėl spartaus technologijų ir saugumo grėsmių pokyčių tempo. Kaip ir ankstesniais metais jaučiamas IT personalo, turinčio kompetenciją informacijos saugumo srityje, trūkumas.

Trys ketvirtadaliai įmonių įsitikinusios, kad jų turimos techninės saugumo priemonės pajėgios aptikti visas reikšmingas saugumo spragas. Tačiau, kai kurios saugumo kontrolės priemonės, atrodo, turi pakankamai silpnų vietų, o kai kurios ir daug saugumo spragų. Respondentai, atrodo, pilnai neįvertino rizikų, kurios jiems gali iškilti. Jų toks perdėtas pasitikėjimas gali būti dėl atitinkamos patirties ir kompetencijos trūkumo. Tyrimas parodė, kad beveik 90 procentai žmonių, dirbančių komandoje atsakingoje už informacijos saugumą, neturi formalios saugumo kvalifikacijos, o apie 60 procentų formalios IT kvalifikacijos. Dauguma darbuotojų dirbančių šioje komandoje turi verslo išsilavinimą.

Informacijos saugumo patirties šie žmonės įgauna įvairiausiais būdais ir jų kompetenciją, šioje greitai besikeičiančioje srityje, paprasčiausia gali būti sunku išmatuoti. Suprasti aktualius saugumo standartus tai tik vienas matavimo vienetas. Kaip jau buvo paminėta anksčiau, nedidelėse įmonėse tik 12 procentų įmonių yra susipažinę su standartu BS7799.

Formali darbuotojo kvalifikacija - kitas svarbus kompetencijos indikatorius. Per šiuos paskutinius dvejus metus keletas darbuotojų įgijo reikalingą kvalifikaciją informacijos saugumo srityje. Tokioms kvalifikacijoms priskiriama specialistai, turintys tiksliųjų mokslų magistro (*MSc - Master of Science*) laipsnį, ir saugumo profesionalų kvalifikaciją – sertifikuoto informacinių sistemų saugumo profesionalo (*CISSP - Certified Information Systems Security Professional*) bei sertifikuoto informacijos saugumo vadovo (*CISM - Certified Information Security Manager*).

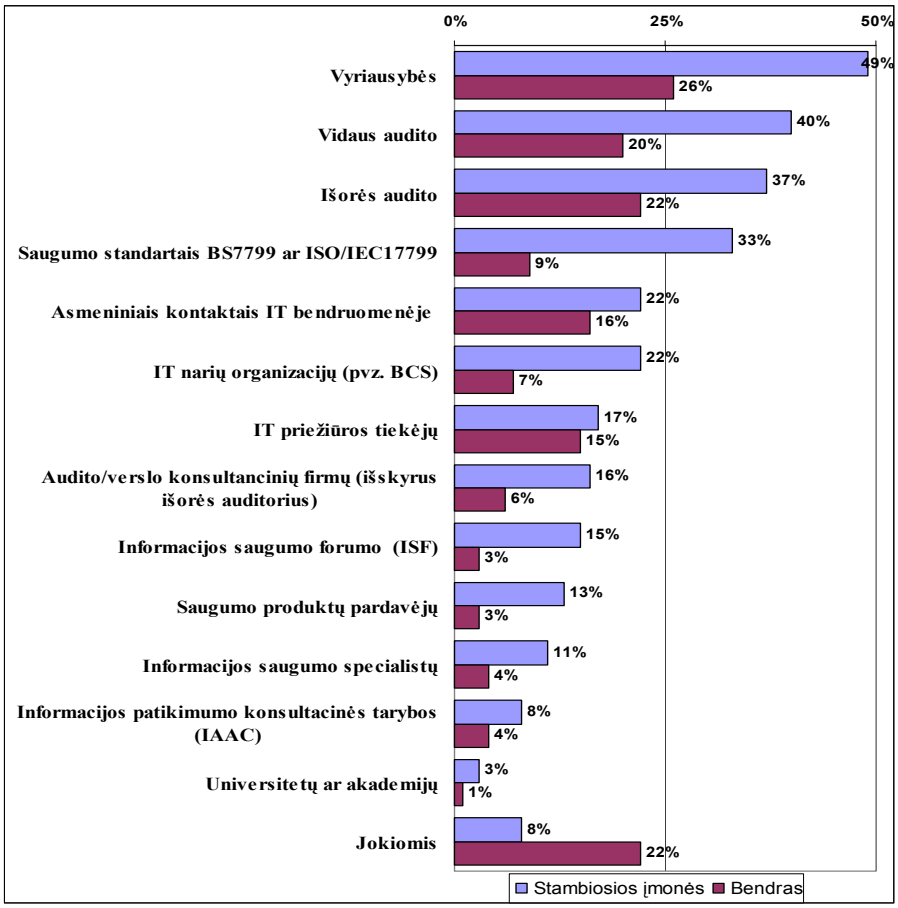
Tačiau tai nieko nuostabaus, nes tokios kvalifikacijos specialistai tik pradedami ruošti, ir poreikis vis didėja. Tik apie 11 procentų įmonių turi specialistus su informacijos saugumo kvalifikacija. Smulkiose įmonėse suprasti saugumo rizikas padeda universalus IT darbuotojas. Stambiosioms įmonėms labiau finansiškai apsimoka turėti parengtus informacijos saugumo darbuotojus, nes čia jų atsipirkimas yra greitesnis. Todėl tokiose įmonėse kvalifikuotų informacijos saugumo specialistų yra dvigubai daugiau. Tokių darbuotojų skaičius įmonėse priklauso nuo veiklos sferos, telekomunikacinių paslaugų įmonėse jie sudaro trečdalį, o turto ir statybų įmonėse vienas iš dvidešimties turi informacijos saugumo kvalifikaciją. Saugumo kvalifikaciją turintys specialistai paprastai dažnai buvo sutinkami tiesioginėje internetinėje apklausoje. Beveik pusė jų dirbo organizacijose, turinčiose kvalifikuotą personalą.

Stambiose įmonėse už informacijos saugumą atsakingas darbuotojas, paprastai turėdavo IT kvalifikaciją, o smulkiose – verslo magistro ar apskaitininko kvalifikaciją. Tai atitinka ir respondentų profilį. Stambiose įmonėse labiausia buvo tikėtina, kad jie save pristatys kaip IT vadovus, o smulkiosiose- kaip verslo vadovus.

Tik apie 40% įmonių savo saugumo komandoje turėjo darbuotojus su IT kvalifikacija. Efektyvi reakcija į saugumo pažeidimus dažnai reikalauja gero technologijų panaudojimo supratimo. Smulkiose įmonėse, tai nelabai įmanoma. Todėl informacijos saugumo produktų pardavėjai, norėdami savo sprendimus parduoti smulkioms įmonėms, privalo padaryti savo produktus paprastus ir efektyvius.

Vienas stambus prekybininkas, turintis didelę IT komandą ir priėjimą prie visų naujausių priemonių ir informacijos šaltinių, paminėjo, kad jų įmonės IT vadovas iš paskutiniųjų bando neatsilikti nuo naujausių technologijų ir saugumo pasikeitimų. Jis sako, kad jeigu dirbtų mažoje įmonėje, kokie nors grėsmių pasikeitimai labai greitai nugramzdintų jį.

Daugelis tyrime dalyvavusių įmonių per daug mažos, kad galėtų turėti savo saugumo specialistus. Todėl beveik trys ketvirtadaliai įmonių patarimus informacijos saugumo klausimais gauna iš išorės (16 pav.). Įdomu, kad net stambiosios įmonės, galinčios turėti nuosavus saugumo ekspertus, pakankamai dažnai naudojasi išorės konsultantų paslaugomis. Tokie sektoriai, kaip energetika, telekomunikacijų ir finansinių paslaugų, konsultuojasi daugiausia, o žemės ūkio ir turto įmonės mažiausiai. Atrodo, kad kuo daugiau žinai apie saugumą, tuo labiau supranti, kad nežinai nieko. Taip pat labai svarbu žinoti, kur galima surasti trūkstamą informaciją.



16 pav. Kokiomis išorinėmis saugumo konsultacijomis praėjusiais metais naudojosi įmonės?

Kad pagelbėtų savo šalies įmonėms, Jungtinės Karalystės vyriausybė per praėjusius dvejus metus išleido daugelį naudingų vadovų informacijos saugumo klausimais. Kaip labai vykusį pavyzdį galima paminėti jau minėtos Prekybos ir pramonės ministerijos svetainę, kurioje kiekviena įmonė gali testo pagalba atlikti taip vadinamą Informacijos saugumo sveikatos patikrinimą (*http://www.ukonlineforbusiness.gov.uk/healthcheck/index.jsp*) bei Nacionalinio aukštų technologijų nusikaltimų skyriaus (NHTCU) svetainę http://www.nhtcu.org/. Tai įgauna išties platų naudojimą šalies verslo bendruomenėje. Jie atstovauja didžiausius išorinius šaltinius, konsultuojančius šalies įmones. Ketvirtadalis visų įmonių ir pusė stambiųjų, šiais išoriniais šaltiniais pasinaudojo praėjusiais metais.

Kitu plačiai naudojamu išorinių konsultacijų resursu buvo vidaus ir išorės auditoriai. Viena iš penkių įmonių sakė, kad auditoriai juos aprūpindavo tam tikrais vadovais ir ekspertizių formomis informacijų saugumo klausimais. Daugelis mažesnių įmonių neatlieka įstatymu numatytų auditų, kad nustatytų savo finansinę būklę. Stambiosios įmonės du kartus daugiau konsultuojasi su savo auditoriais nei smulkiosios. Daugelis įmonių informacijos saugumo klausimais yra linkusios konsultuotis su savo verslo patarėjais, kuriais jos pasitiki. Todėl labai dažnai iškilus saugumo klausimams auditoriai yra pirmas taškas, kuriems įmonės skambinama. Tačiau, atrodo, kad auditorių nepriklausomumas nėra pagrindinis rodiklis saugumo patarimo klausimais ir įmonės tris kartus daugiau linkusios saugumo klausimais tartis su savo išoriniais auditoriais, nei naudotis audito ar verslo konsultacinių kompanijų paslaugomis.

Trečdalis stambiųjų įmonių, susipažinusių su standartu BS7799, naudoja jį saugumo rizikų valdymui. Didelė dalis išorinių konsultacijų tenka asmeniniam bendravimui IT bendruomenėje. Tokiomis pažintimis naudojosi viena iš šešių įmonių. Žmonės dažnai buvo linkę kalbėti su tais, kuriais pasitikėjo ir kurie dirbo toje pačioje srityje. Informacijos saugumas tarp specialistų kol kas nėra matoma kaip konkurencinės kovos arena, ir daugiau naudojama nuomonių pasikeitimui. Kol daugelis įmonių drovisi viešai komentuoti saugumo dalykus, todėl privačios diskusijos yra daug įprastesnės. Be to dėl kompetencijos stokos daugelis informacijos saugumo tarnautojų sunkiai įsitraukia į informacijos saugumo bendruomenę, ir labiau linkę neakivaizdžiai konsultuotis su Britanijos Kompiuterių Draugijos ar kitų IT organizacijų nariais.

Nors IT tiekėjai ir saugumo pardavėjai linkę teikti daug vertingų konsultacijų, bet tik 15 procentų įmonių šiomis konsultacijomis pasikliauna. Viena iš priežasčių gali būti informacijos nepriklausomumas, nes pardavėjai dažnai yra šališki tam tikriems produktams ir paslaugoms.

Vienas IT saugumo koordinatorius, duodamas interviu tyrimo organizatoriams, patvirtino, kad dažnai apie saugumo grėsmes ieško informacijos internete. Beveik visada ta informacija yra pernelyg techninė, kuria gal būt nelabai ir reikia pasitikėti. Jis pageidavo turėti vieną pasitikėjimo vertą informacijos šaltinį, kuriame informacija būtų pateikta kasdienine suprantama kalba.

Šio skyriaus pabaigoje verta paminėti keletą informacijos šaltinių, pritaikytų galutiniam vartotojui. Didelėms įmonėms labai vertingą etaloninę informaciją jos nariams teikia Informacijos saugumo forumas (*Information Security Forum* - http://www.securityforum.org). Panašiai į kolektyvinius valdymo aspektus dėmesį fokusuoja ir Informacijos patikimumo konsultacinė taryba (*Information Assurance Advisory Council* http://www.iaac.org.uk). Griežtus informacijos saugumo reikalavimus yra nustatęs *Royal Holloway* koledžas prie Londono universiteto.

9. INVESTICIJOS Į SAUGUMĄ

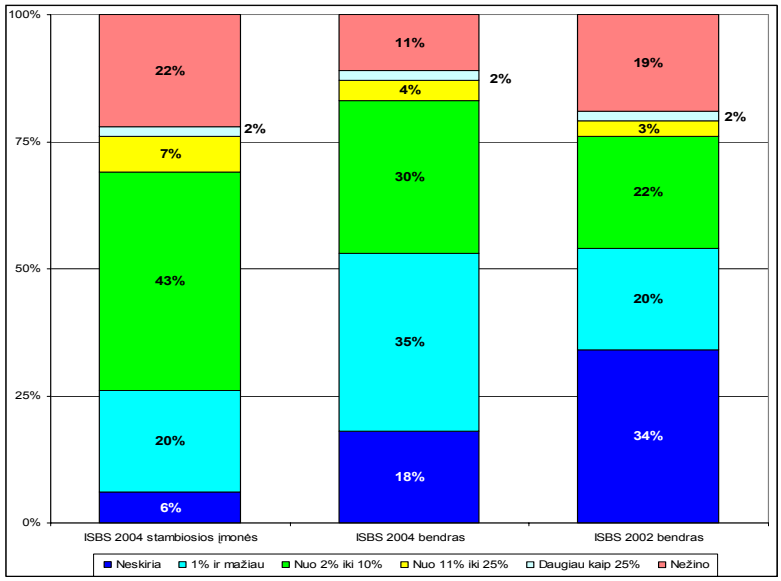
Prieš dvejus metus įvykusio tyrimo viena iš išvadų, siekiant mažinti saugumo incidentų skaičių, buvo nepakankamos įmonių investicijos į informacijos saugumą. Šių metų tyrimo rezultatai parodė, kad Jungtinės Karalystės įmonės į informacijos saugumą investuoja daugiau.

Tik viena iš dvidešimties įmonių pranešė, kad praėjusiais metais investavo mažiau. Be to, per paskutiniuosius dvejus metus į IT buvo investuojama mažiau, bet didelis informacijos saugumo prioritetas įmonių vadovybių lygyje, atrodo, kad išsaugojo išlaidas saugumui.

Šiuo metu įmonės informacijos saugumui vidutiniškai išleidžia 3 procentus nuo savo IT biudžeto, kaip tuo tarpu praėjusio tyrimo duomenimis išleido 2 procentus. Stambiosios įmonės nurodė, kad išleidžia dar daugiau, apie 4 procentus (17 pav.).

Tyrimo organizatoriai, pasiremdami kitų šalių patirtimi, galvoja, kad išlaidos informacijos saugumui vidutiniškai turėtų 3-5 procentus nuo viso IT biudžeto. Aukštos rizikos sektoriuose, tokiuose kaip finansinės paslaugos, galėtų siekti vidutiniškai 10 procentų.

Tyrimo organizatoriai daro išvadą, kad investicijų lygis kaip tik ir artėja prie šių ribų. Beveik ketvirtadalis įmonių į saugumą investuoja daugiau nustatyto efektyvaus lygio, o stambiosios įmonės sudaro beveik pusę, kurių investicijos viršija. Tačiau vis dar yra nemažai įmonių, kurios informacijos saugumui skiria mažiau kaip 1 procentą nuo bendro IT biudžeto.

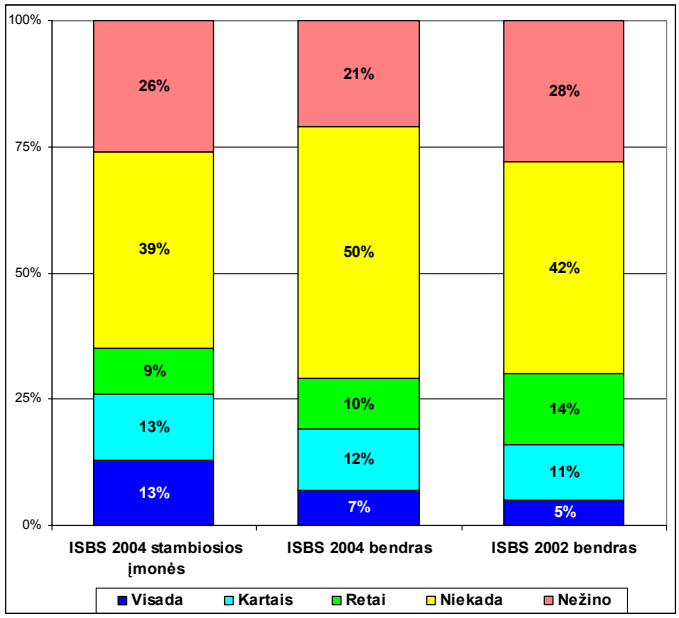


17 pav. Kokį procentą nuo IT biudžeto informacijos saugumui skiria įmonės

Šitame vertinime gali būti tam tikro netikslumo, nes daugelis įmonių išlaidas skirtas informacijos saugumui įtraukia į bendrą IT biudžetą, t.y. jų neišskiria. Tai nebūdinga stambiosioms įmonėms, kur informacijos saugumo komanda dirba atskirai nuo IT komandos. Tačiau joms sunkiau atsakyti, kokia dalis lėšų, išleistų informacijos saugumui, sudaro nuo IT biudžeto.

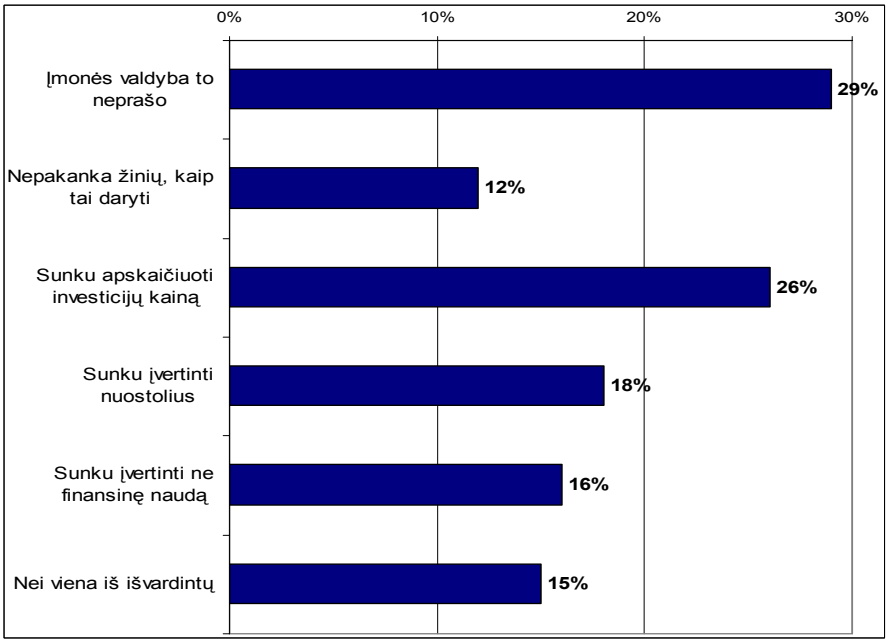
Bet reikia atminti, kad skirtingas investicijų informacijos saugumui naudojimas priklauso nuo veiklos pobūdžio. Tą atspindi ir tyrimo rezultatai. Sektoriai, kurių veikla priklauso nuo technologijų ar informacijos slaptumo, linkusios leisti daugiau, tuo tarpu atviresni sektoriai linkę leisti mažiau. Beveik kiekviename sektoriuje, mažiausiai trečdalis įmonių informacijos saugumui skyrė mažiau nei 1 procentą nuo savo IT biudžeto.

Vienas iš faktorių trukdančių pakankamai investuoti į informacijos saugumą yra tai, kad įmonės į išlaidas saugumui dažnai žiūri kaip pridėtines išlaidas, o ne kaip į investiciją. Mažiau kaip pusė visų įmonių įvertina įplaukas iš investicijų, kurios buvo išleistos saugumui stiprinti. Per dvejus metus įvyko tik labai nežymus pasikeitimas (18 pav.). Čia stambiosios įmonės yra tik truputį geresnės nei mažosios.



18 pav. Kaip dažnai įmonės įvertina įplaukas iš investicijų į saugumą?

Neturint ir neįvertinant šios informacijos, gali būti sunku nustatyti teisingą prioritetą investicijoms į saugumą, lyginant su kitais projektais. Įmonių vadovybės saugumui užtikrinti reikalingas išlaidas gali priskirti prie priverstinių, o ne prie išlaidų, kurios gali atnešti teigiamą naudą verslui. Keista, bet pagrindinė priežastis, kodėl įmonės neįvertina investicijų grįžimo yra tai, kad niekas to neprašo jų daryti (19 pav.). Šią priežastį nurodė beveik trečdalis įmonių.



19 pav. Pagrindinės kliūtys, trukdančios įvertinti saugumui išleistų investicijų grįžimą?

Ketvirtadalis respondentų nurodė, kad išlaidų reikalingumą sunku išreikšti skaičiais. Tai aišku netikėtas rezultatas. Tiesioginę kainą apskaičiuoti neturėtų būti sunku. Žymiai sunkiau yra įvertinti neapčiuopiamą naudą gautą iš investicijų arba praradimų, neinvestavus į informacijos saugumą. Vienas iš tokių rodiklių galėtų būti reputacijos potencialas, tokiuose jautriuose sektoriuose, kaip finansinės paslaugos ar telekomunikacija! Apklausos metu vienas didelis bankas pareiškė, kad neskaičiuoja į saugumą investuotų lėšų susigrąžinimo, kadangi banko reputacija yra pirmaeilis dalykas. Saugumo spragos gali pakirsti reputaciją ir to pasėkoje

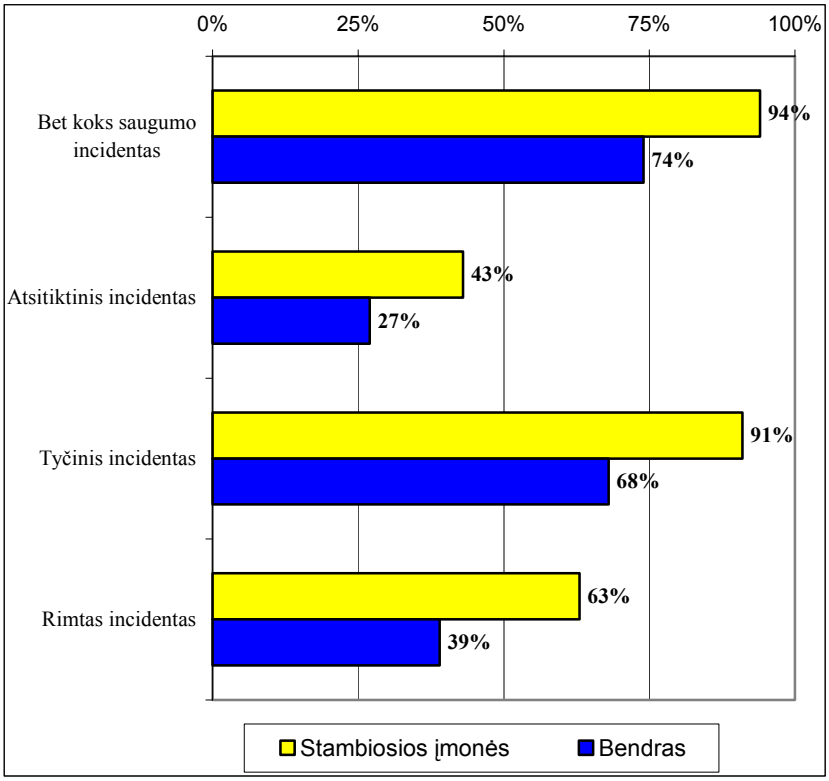
bankas gali patirti neproporcingus nuostolius. Saugumo kontrolė šiame banke yra svarbiausios, ir kaina tik antraeilis dalykas.

Savo ruožtu informacijos saugumo priemonių tiekėjai, jeigu tuo galima tikėti, teigia, kad jie yra pasiruošę konsultuoti įmones ir tiekti joms priemones, padedančias įvertinti investicijų grįžtamumą. Įmonių vadovai galvoja, kad jiems paskaičiuoti investicijų naudingumą, tokioms saugumo priemonėms kaip antivirusinių programų ir rezervinio kopijavimo įsigijimui yra pakankamai nesunku, o tokioms informacijos saugumo sritims, kaip duomenų saugumas, šifravimas, serverių saugumas, saugumo politika ir standartai, įsitikinimas yra mažesnis. Bet net ir čia, daugelis pradeda suprasti, kad tai padaryti gali būti lengva.

Iš to, kas šiame skyriuje pasakyta, galima padaryti išvadą, kad įvertinti investicijas informacijos saugumui yra sąlyginai lengva, todėl belieka atsakyti į klausimą: kodėl daugelis įmonių taip sunkiai investuoja į saugumą?

10. SAUGUMO PAŽEIDIMŲ PAPLITIMAS

Tyrimas ISBS 2004 konstatavo, kad ir toliau didėja Jungtinės Karalystės įmonių skaičius, kurios kenčia nuo saugumo pažeidimų. Trys ketvirtadaliai įmonių ir beveik visos stambiosios įmonės praėjusiais metais patyrė mažiausiai po vieną incidentą. Trečdalis įmonių ir du trečdaliai stambiųjų įmonių patyrė rimtus saugumo pažeidimus.



20 pav. Kiek įmonių praėjusiais metais turėjo informacijos saugumo incidentus?

Labai padidėjo tyčinių incidentų, tokių kaip kompiuteriniai virusai, nesankcionuotas priėjimas prie informacinių sistemų, netinkamas sistemos vartojimas, sukčiavimai ir vagystės, skaičius. Pastaraisiais metais du trečdaliai įmonių turėjo tyčinius saugumo incidentus ir palyginus su ankstesnio tyrimo ISBS 2002 rezultatais tokių incidentų padidėjo beveik 50 procentų ir šis augimas metai iš metų didėja. Virš ketvirtadalio įmonių patyrė rimtus incidentus, kurių priežastys buvo atsitiktinis sistemų gedimas ar duomenų praradimas. Kadangi 2002 m. tyrimas analizavo tik tyčinius incidentus, taigi kitų incidentų santykį galime lyginti tik su 2000 m. tyrimo duomenimis. Dabartinis atsitiktinių incidentų lygis panašus į tą, kuris buvo

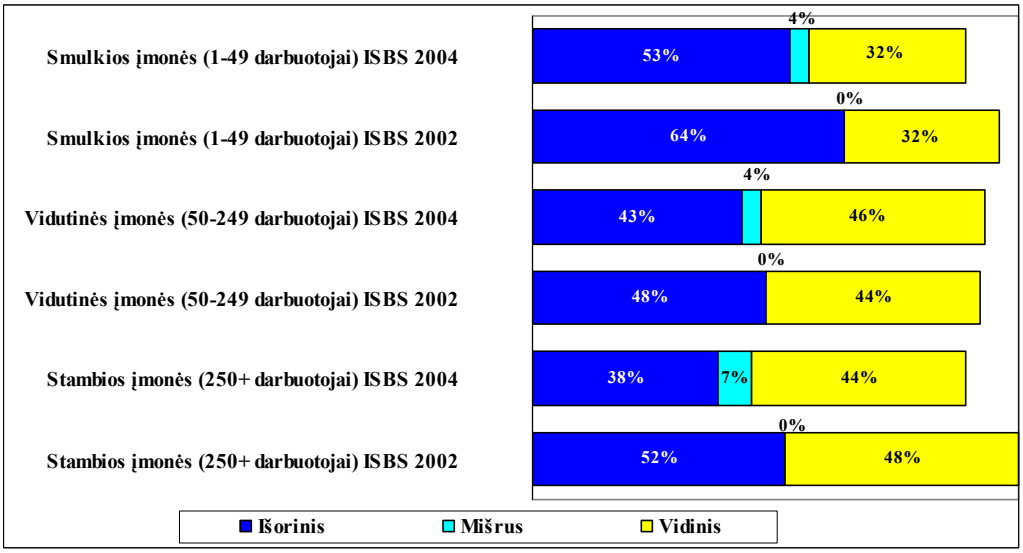
stebimas prieš ketverius metus, kai atsitiktiniai incidentai viršijo tyčinius. Šių metų tyrimas parodė visiškai priešingą santykį – tyčiniai incidentai keletą kartų viršija atsitiktinius.

Stambiosios įmonės buvo patyrusios apytiksliai tris kartus daugiau saugumo pažeidimų, nei mažosios ir jos nuo incidentų nukenčiančia vidutiniškai vieną kartą per savaitę. To priežastys gali būti, kad stambiosios įmonės turi daugiau sistemų, kurios gali sugesti, taip tokiose įmonėse dirba žymiai daugiau darbuotojų, kurie su sistemomis gali netinkamai elgtis, jos linkusios labiau naudotis trečiųjų šalių paslaugomis. Be to, stambiųjų įmonių interneto tinklų sąsajos zonduojamos vidutiniškai vieną kartą per dvi savaites, tai tris kartus dažniau negu vidutiniškai smulkiųjų įmonių. Tačiau iš kitos pusės, stambiosios įmonės yra linkusios sėkmingiau atremti atakas. Mažiau kaip vienas toks zondavimas šimtui stambiųjų įmonių baigiasi įsiskverbimu į jų sistemą. Tuo tarpu smulkiųjų įmonių atveju sėkmingai baigiasi vienas zondavimas iš penkiasdešimties. Labiausia saugumo incidentai paplitę buvo tarp finansinių paslaugų ir technologijų įmonių, bei valdžios institucijų. Tuo tarpu žemės ūkio, laisvalaikio, sveikatos apsaugos ir švietimo įmonės saugumo incidentų patyrė mažiausiai.

Susumavus tiesioginės interneto apklausos rezultatus paaiškėjo, kad respondentai nurodė labai panašius saugumo pažeidimų paplitimus, kaip ir stambiosios įmonės telefoninėje apklausoje, t.y. respondentai nurodė, kad jų įmonės praėjusiais metais turėjo 92 procentus incidentų.

11. IŠORINIAI AR VIDINIAI INCIDENTAI?

Kai rodo daugelio metų patirtis, daugiausia saugumo incidentų sukelia „savi žmonės". Tačiau ISBS 2002 identifikavo esminį šios padėties pasikeitimą. Šio tyrimo metu paaiškėjo, kad beveik du trečdalius incidentų mažose įmonėse sudarė išoriniai incidentai, o stambiose įmonėse pusė incidentų buvo vidiniai ir pusė išoriniai (21 pav.).



21 pav. Koks blogiausio saugumo incidento šaltinis – išorinis ar vidinis, buvo įmonėse?

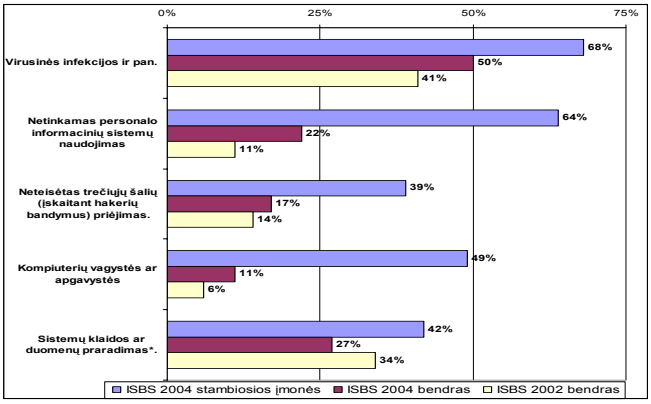
2004 m. tyrime, respondentai pirmą kartą galėjo identifikuoti incidentą, kurį iššaukė vidinių ir išorinių veiksnių kombinacija. 4 procentai respondentų pranešė, kad blogiausias incidentas buvo abiejų veiksnių kombinacija. Tokios rūšies incidentu labiausiai paveiktos buvo stambiosios įmonės (7 %). Tyrimo metu buvo pateikti šių trijų šaltinių pavyzdžiai: viruso paplitimas įmonės darbuotojo veiksmais, sistemos sutrikimas dėl išorinių veiksnių (tokių kaip įtampos sutrikimas) ir nelegalus personalo bendravimas su pašaliečiais. Mišriam šaltiniui priskiriami 4 procentai, atrodo, šiek tiek sumažintas skaičius, nes ketvirtis respondentų virusų infekciją, kuri yra išorinė grėsmė, priskyrė prie vidinių veiksnių. Organizatoriai mano, kad tam tikras pakoregavimas dėl vidinių ir išorinių šaltinių sumaišymo galėtų padidėti iki 23%.

Šie pateikti skaičiai beveik atitinka žurnalo „*CIO Magazine*" pateikiamais skaičiais, atlikus pasaulinį informacijos saugumo tyrimą (*Worldwide Information Security Survey*). Šio tyrimo metu nustatyta, kad apie du trečdaliai incidentų šaltiniai buvo išoriniai ir vienas trečdalis – vidiniai. Taigi skirtumas tarp šių dviejų tyrimų yra labai mažas.

12. SAUGUMO INCIDENTŲ TIPAI

Kaip matyti iš 22 pav. nuo 2002 m. augo beveik visi tyčinių saugumo incidentų tipai. Sumažėjo tik incidentai dėl sistemos klaidų ar duomenų praradimo (čia pateikti ne 2002 m., o 2000 m. duomenys). Ir kaip matyti stambiosios įmonės incidentų patiria žymiai daugiau negu mažosios.

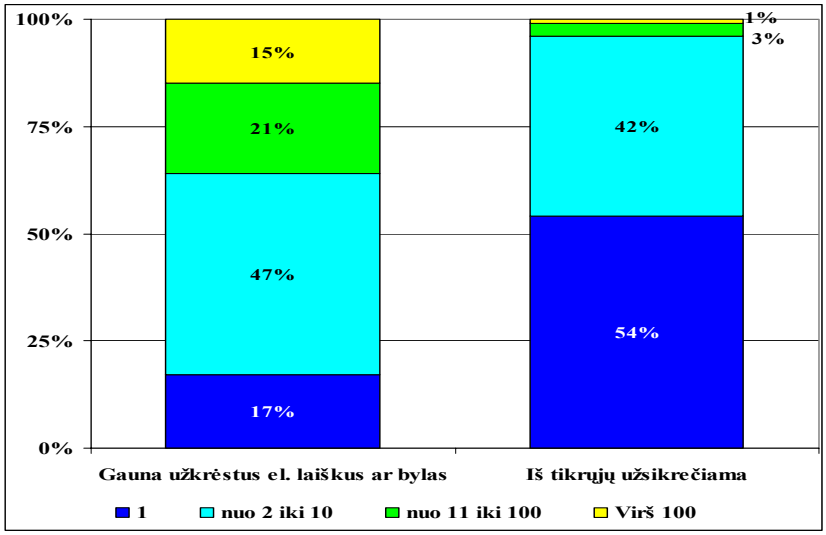
Virusų infekcijos tęsia saugumo pažeidimų tradiciją ir turi didžiausią skaičių incidentų. Du trečdaliai įmonių, turėjusios saugumo incidentus, pripažino, kad virusų infekcijos iššaukė pačius blogiausius incidentus. Jie užėmė didžiausią dalį incidentų nepriklausomai nuo įmonės dydžio. Daugelis įmonių vis labiau pradeda kalbėti apie vis didėjančią grėsmę jų veiklai, tai nepageidaujami elektroniniai laiškai „spam'as", kurio metu saugumas tiesiogiai nors ir nėra pažeidžiamas, bet jis labai trukdo normalų darbą ir IT bei saugumo personalas ieško efektyvių kovos priemonių su nepageidaujamais elektroniniais laiškais.



22 pav. Dažniausia pasitaikantys saugumo pažeidimai.

Respondentų pranešimuose virusai ir tyčiniai kodai be jokių abejonių buvo priskiriami prie pačiu dažniausiai pasitaikančiu saugumo incidentų. Jie taip pat sudaro du trečdalius pačių rimčiausių incidentų. Beveik trys ketvirtadaliai Jungtinės Karalystės įmonių pranešė, kad elektroniniu paštu jos turėjo gavusios elektronines bylas, turinčias virusus ar Trojos arklius. Stambiąsias įmones virusai veikė labiau negu smulkiąsias. Tikėtina, kad šis skaičius galėjo būti sumažintas, nes 7 procentai įmonių neturėjo įdiegusios antivirusinės programinės įrangos ir todėl galėjo nenujausti, kad jų sistemas paveikė virusai. Šią išvadą patvirtina ir įmonių analizė. Tarp įmonių, kurios pranešė apie tai, kad buvo atakuotos virusų, daugiausia buvo finansinių paslaugų įmonių, kurios daugiausia buvo įdiegusios antivirusines programas. Tyrimo metu paaiškėjo, kad visos finansinių paslaugų įmonės turėjo įsidiegusios antivirusines programas ir 97 procentai jų pranešė, kad buvo gavusios infekuotus elektroninius laiškus ar bylas. Priešingoje vertinimų skalės pusėje buvo žemės ūkio įmonės, kurių tik 60 procentų pranešė apie gautus infekuotus elektroninius laiškus ar bylas, bet tik 78 procentai šių įmonių turėjo pas save įsidiegusios antivirusinę programinę įrangą.

Kaip rodo patirtis, kad pažeidimas virusais, kirminais ir Trojos arkliais labai retai būna izoliuotas incidentas. Viena iš šešių įmonių pranešė, kad per paskutiniuosius metus gavo vidutiniškai apie 100 infekuotų elektroninių laiškų ar bylų. Kukliais vertinimais kiekviena Jungtinės Karalystės įmonė per mėnesį vidutiniškai gauna po du virusus, o stambiosios įmonės dvigubai daugiau. Kiti tyrimai nurodo netgi didesnius skaičius. Aukštų technologijų nusikaltimų tyrimas NHTCU 2003 savo ataskaitoje nurodė respondentus, kurie buvo atakuoti virusais vidutiniškai 254 kartų per metus (23 pav.).



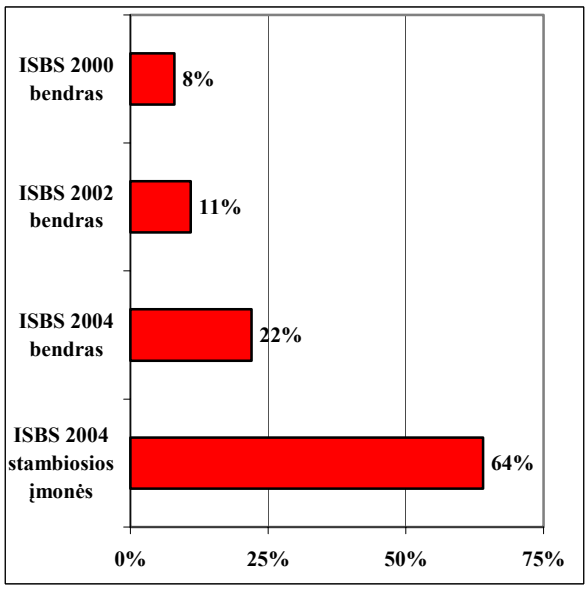
23 pav. Kaip dažnai įmonės gavo užkrėstus el. laiškus ir bylas ir kaip dažnai užsikrėtė.

Ne kiekviena įmonė gavusi virusus ar kirminus buvo užkrėsta. Be to, vidutinis virusų protrūkių skaičius buvo žymiai mažesnis nei gautų virusų. Tik 5 procentai įmonių pranešė, kad paskutiniaisiais metais patyrė daugiau kaip dešimt virusų protrūkių. Iš to kas pasakyta, galima padaryti išvadą, kad antivirusinė apsauga yra pakankamai efektyvi.

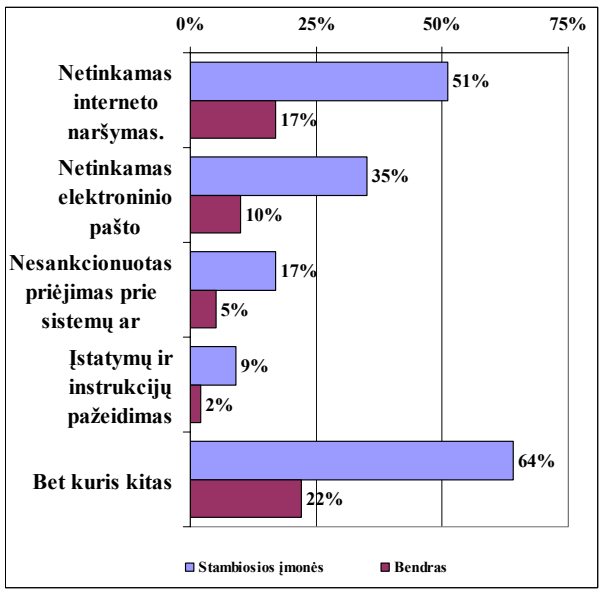
Trys kirminai - *Blaster, Sobig* ir *Bugbear* buvo priežastimi daugiau kaip trijų ketvirtadalių blogiausių virusų protrūkių. Būtent kirminai iškelia į pirmąjį planą virusines grėsmes. Jie sudaro grėsmių mišinį, sugebantį apeiti tradicines antivirusines programas ir atakuoti tinklą. Tarp didžiųjų įmonių kirminas *Blaster* buvo ypač nesuvaldomas, jis sukėlė apie 56 procentus pavojingiausių incidentų. Laiku neatnaujintos antivirusinės programos buvo labai dažna saugumo pažeidimo virusais priežastimi.

13. NETINKAMAS PERSONALO INFORMACINIŲ SISTEMŲ NAUDOJIMAS

Per pastaruosius dvejus metus žymiai išaugo incidentų skaičius dėl personalo netinkamo informacinių sistemų naudojimo. Beveik ketvirtadalis įmonių pranešė apie tokio pobūdžio incidentus. Tai lygiai dvigubai daugiau, negu tokių pažeidimų buvo 2002 m. (24 pav.). Tokį išaugusį padidėjimą sąlygojo padidėjęs interneto vartojimas. Piktnaudžiavimas elektroniniu



24 pav. Kiek įmonių nukentėjo nuo personalo



25 pav. Kokio tipo personalo netinkamo

netinkamo informacinių sistemų naudojimo? naudojimo klaidos paveikė įmones?

Kad saugumo incidentų priežastis, bus netinkamas personalo informacinių sistemų naudojimas stambiosiose įmonėse buvo tris kartus labiau tikėtina, negu mažosiose. Daugiau personalo, didesnė tokio tipo incidentų tikimybė. Tačiau iš kitos pusės stambiosios įmonės labiau tikėtina, turės įsidiegusios stebėjimo priemones, kurios padės efektingiau aptikti incidentus.

Įmonės, kuriose buvo piktnaudžiaujama internetu, metų bėgyje vidutiniškai turėjo po vieną incidentą per savaitę. Įdomu pažymėti ir tai, kad smulkiosios įmonės turėjo maždaug tiek pat pažeidimų kaip ir stambiosios, nepaisant to, kad jos turėjo mažiau darbuotojų.

Viena iš dvylikos įmonių pranešė, kad jų blogiausias metų saugumo incidentas buvo susijęs su darbuotojų netinkamu interneto naudojimu. Maždaug viena iš penkių įmonių turėjo labai rimtą poveikį. Pernelyg didelis personalo elektroninis paštas buvo priežastimi trečdalio incidentų. Priėjimas prie netinkamų svetainių buvo kita labiausiai žymi priežastis ir sudarė ketvirtadalį incidentų. Vienas iš penkių blogiausių metų incidentų buvo susijęs su pernelyg dideliu interneto naršymu. Kitos nurodomos priežastys - netinkamų elektroninių laiškų siuntimas arba leidimas pašaliniams asmenims naudotis elektroniniu paštu.

Tiesioginės internetinės apklausos respondentai pranešė, kad jų įmonės žymiai daugiau patyrė incidentų susijusių su netinkamu sistemos naudojimu, negu telefoninio tyrimo respondentai. Virš pusė jų, panašiai kaip ir stambiųjų kompanijų respondentai telefoniniame tyrime, pranešė apie piktnaudžiavimus susijusius su interneto naršymu. Elektroninio pašto piktnaudžiavimai tiesioginės internetinės apklausos respondentų nuomone sudarė 45 procentus, tai daugiau net negu buvo nurodžiusios stambiosios kompanijos telefoninėje apklausoje.

Viena įmonė pranešė, kad keli jų darbuotojai slapta naudojo įmonės kompiuterių sistemas savo privačiam verslui. Šios įmonės interneto prieiga tai leido daryti.

Daugiausia incidentų – 39 procentai susijusių su interneto naršymo piktnaudžiavimu ir 26 procentai su netinkamu elektroninio pašto naudojimu, turėjo finansinių paslaugų įmonės. Daugelyje bankų ir draudimo bendrovių dirba pakankamai daug darbuotojų, kurie turi priėjimą prie interneto ir elektroninio pašto. Kiekviena šio sektoriaus įmonė turi etikos kodeksą ir čia yra įdiegtos personalo netinkamo elgesio stebėjimo sistemos. Priešingoje matavimų skalės pusėje yra žemės ūkio įmonės, kurios faktiškai nepranešė apie tokio tipo incidentus. Čia paprastai personalas neturi nuolatinės darbo vietos ir turi žymiai mažiau galimybių prieiti prie interneto arba elektroninio pašto.

Didžiausias skirtumas tarp tiesioginės internetinės apklausos ir telefoninio tyrimo buvo stebimas nesankcionuoto priėjimo prie sistemų srityje. Apie trečdalis tiesioginės internetinės apklausos respondentų pranešė apie incidentus šioje kategorijoje, ir tik 5 procentai įmonių bendrai bei 17 procentų stambiųjų įmonių pranešė apie tokio pobūdžio incidentus telefoninio tyrimo metu. Tai ir vėlgi galima paaiškinti tuo, kad tiesioginės internetinės apklausos respondentai turėjo geresnes pažeidimų kontrolės sistemas, o smulkiosios įmonės, neturinčios tokių sistemų, paprasčiausia galėjo neaptikti šio pobūdžio pažeidimų.

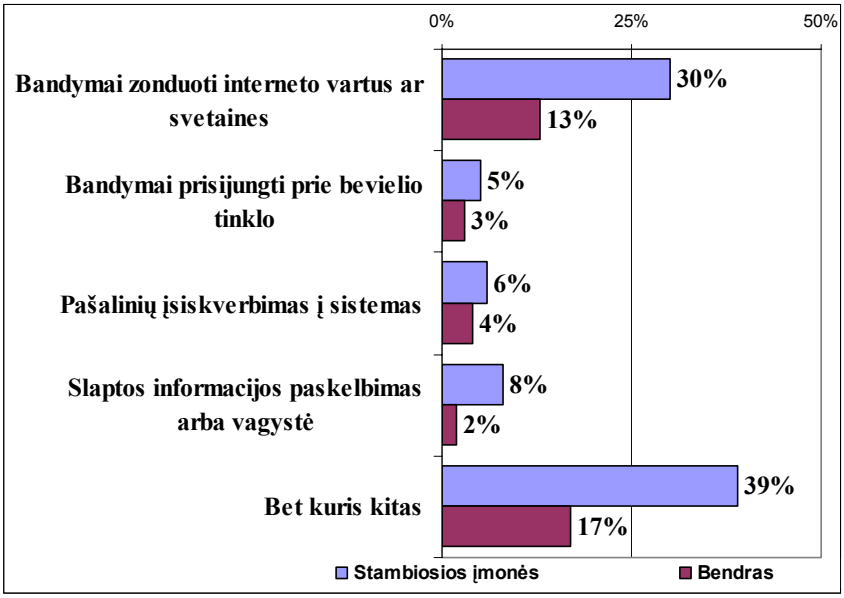
Taip pat reikia pažymėti ir tokius incidentus, kai darbuotojai bando atspėti ar išgauti kito darbuotojo slaptažodžius, ir tuo pasinaudoję nesankcionuotai prieiti prie sistemų ar duomenų. Nors tokio pobūdžio incidentų nuolatos mažėja, bet vis dėlto viena iš dvidešimt smulkiųjų ir beveik viena iš penkių stambiųjų įmonių pranešė, kad turėjo tokius incidentus. Taigi per metus virš pusės įmonių turėjo daugiau negu vieną tokio tipo incidentą.

Siekiant išvengti šių pažeidimų Jungtinėje Karalystėje buvo priimtas Duomenų apsaugos įstatymas arba Netinkamo kompiuterių naudojimo aktas. Tai, kad stambiosios įmonės pranešė keturis kartus daugiau turėjusios pažeidimų, negu smulkiosios, labiau tikėtina, kad jos turėjo priėmusios įstatyme numatytas procedūras ir labiau tikėtina, kad suprato, kas sudaro

pažeidimus. Kelioms vidutinio dydžio įmonėms, šių įstatymų nesilaikymas baigėsi blogiausiu metų saugumo incidentu.

14. NESANKCIONUOTAS PAŠALINIŲ PRIĖJIMAS

Įmonės turinčios savo interneto svetaines, yra atviros pašaliniams, tame tarpe ir tiems, kas turi piktavališkų tikslų įsilaužti į įmonės kompiuterių tinklą. Vienas iš stulbinančių šio tyrimo rezultatų – padidėjęs bandymų skaičius zonduoti įmonių interneto vartus. Jeigu prieš dvejus metus apie bandymus zonduoti pranešė tik dvylika Jungtinės Karalystės įmonių, tai dabar kas aštunta įmonė ir kas trečia stambi įmonė (26 pav.), pranešė apie tokius bandymus. Labai tikėtina, kad šie skaičiai yra sumažinti, nes daugelis įmonių turi silpnas ugniasienes ir pamatyti zondavimo bandymus jos yra nepajėgios. Tyrimas užfiksavo labai skirtingus skanavimo lygius. Penktadalis įmonių pranešė, kad jos per metus identifikavo vieną skanavimo atvejį, ir daugiau kaip ketvirtadalis įmonių per metus identifikavo daugiau kaip šimtą skirtingų zondavimų. Atsargiais vertinimais, kurie pagrįsti šio tyrimo rezultatais, galima teigti, kad Jungtinės Karalystės įmonių interneto vartai vidutiniškai zonduojami bent vieną kartą per savaitę.



26 pav. Kokius bandymus iš pašalinių pusės nesankcionuotiems priėjimams patyrė įmonės?

Dažniausiai buvo zonduojamos vidutinės įmonės. Tai atitinka rezultatams, kurie buvo stebimi ir prieš dvejus metus. Šios įmonės hakeriams yra pakankamai įdomios kaip taikiniai, nes dažnai stokoja reikiamų saugumo kontrolės priemonių. Viena vidutinio dydžio įmonė paaiškino, kad ji buvo skanuojami beveik kiekvieną dieną. Nors tik nedaugelis bandymų baigėsi įsiveržimu, bet didelė bandymų apimtis kėlė daug problemų.

Bevielis tinklas ir suvoktas jo saugumo silpnumas, taip pat praėjusiais metais jautė didelį saugumo spaudimą. Kaip jau buvo minėta anksčiau trečdalis įmonių šiuo metu naudoja bevielį tinklą. Technologijų ir telekomunikacijų įmonės yra didžiausi bevielio tinklo naudotojai. 60 procentų šio sektoriaus įmonių naudoja bevielį tinklą. Kaip tik čia buvo užfiksuotas didžiausias saugumo incidentų prieaugis. 3 procentai įmonių pranešė apie bandymus įsikirsti į jų bevielį tinklą, tai daugiau negu buvo prieš dvejus metus. Tada buvo užfiksuotas vienas iš dešimties nesankcionuotų prisijungimų į bevielius tinklus. 15 procentų įmonių pranešė, kad į jų bevielį tinklą buvo bandoma įsiveržti daugiau nei šimtą kartų.

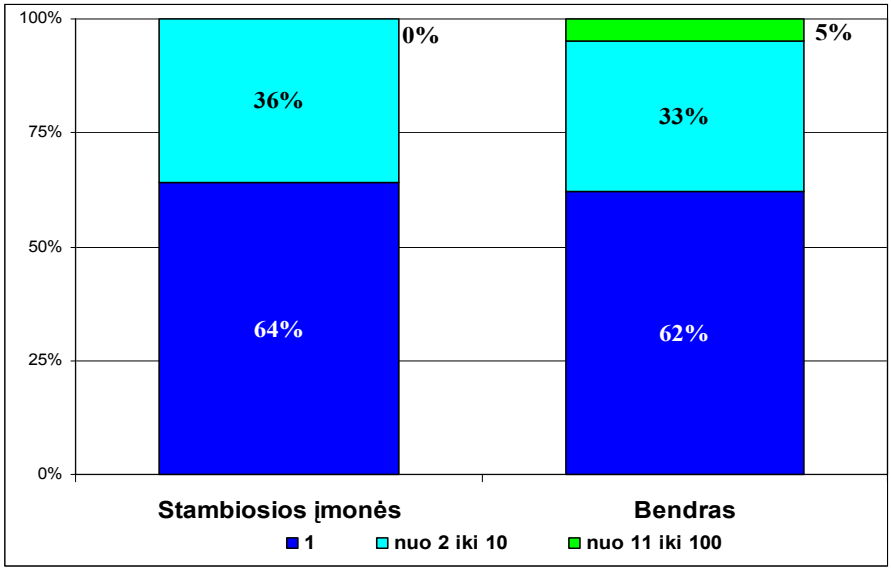
Laimei, kad labai mažai šių bandymų baigėsi tikrais įsiskverbimais. Tik 4 procentai įmonių pranešė apie pastaraisiais metais pavykusius įsiskverbimus. Kadangi kai kurios įmonės, turinčios labai silpnas kontrolės priemones, galėjo nesuprasti apie buvusius įsiskverbimus, todėl

tikri skaičiai galėjo būti didesni. Bet kuriuo atveju, tai didžiulis padidėjimas nuo 2002 m., kai buvo pranešta tik apie 1 procentą sėkmingų įsiskverbimų.

Beveik du trečdaliai įmonių, kurios pranešė apie įsiskverbimus, turėjo tik po vieną tokį incidentą (27 pav.). Ir tik viena iš dvidešimties įmonių pranešė, kad turėjo daugiau negu dešimt incidentų. Reikia pažymėti, kad skirtingai nuo kitų tipų saugumo pažeidimų, nagrinėtų šiame tyrime, buvo stebimas labai nedidelis atsakymų skirtumas tarp skirtingo dydžio įmonių.

Tyrimas atkreipė dėmesį, kad kai kurie sektoriai labiau įdomūs hakeriams nei kiti. Finansinių ir telekomunikacinių paslaugų tiekėjai buvo dukart labiau zonduojami nei mažmeninės prekybos. Tačiau nežiūrint į didesnį zondavimo dažnumą, į jų sistemas buvo įsiveržiama žymiai rečiau. Ir priešingai, technologijų įmonės pranešė vidutiniškai tris kartus daugiau įsiskverbimų į jų sistemas.

Daugelis kompanijų, į kurias buvo įsiskverbta, tokius įsiskverbimus vertino kaip blogiausius metų saugumo incidentus (viršijančiu virusinę infekciją ir t.t.).



27 pav. Kiek įsiveržimų į sistemas iš pašalinių pusės patyrė įmonės?

Tokie saugumo incidentai, kaip slaptos informacijos paskelbimas ar vagystė yra sąlyginai reti. Tik 2 procentai įmonių turėjo tokio tipo pažeidimus. Be to, daugeliu atvejų tai buvo pavieniai incidentai. Tačiau reikia paminėti ir tą faktą, kad kai šie pažeidimai įvyksta, jie visada būna labai rimti. Daugiau kaip pusė įmonių, kurios turėjo tokius pažeidimus, vertino juos kaip pačius blogiausius metų saugumo incidentus.

Stambiosios įmonės turėjo keturis kartus daugiau konfidencialumo pažeidimų negu mažosios. Technologijų įmonės vidutiniškai tris kartus daugiau turėjo tokių incidentų negi kitos. Tuo tarpu ir vėlgi, žemės ūkio įmonės nepranešė apie tokius pažeidimus. Toks pasiskirstymas atspindi ir tai, kiek ir kokios vertės slaptos informacijos saugo įmonės.

Tiesioginės internetinės apklausos respondentai pranešė daugiau nesankcionuoto priėjimo incidentų negu telefoninio tyrimo respondentai. 56 procentai tiesioginės internetinės apklausos respondentų pranešė apie jų įmonių interneto vartų skanavimą ar zondavimą. Tai yra žymiai daugiau, negu apie tokius bandymus pranešė stambiųjų kompanijų atstovai telefoninio tyrimo metu. Slaptos informacijos paskelbimas ir vagystės buvo dėsningi stambioms kompanijoms.

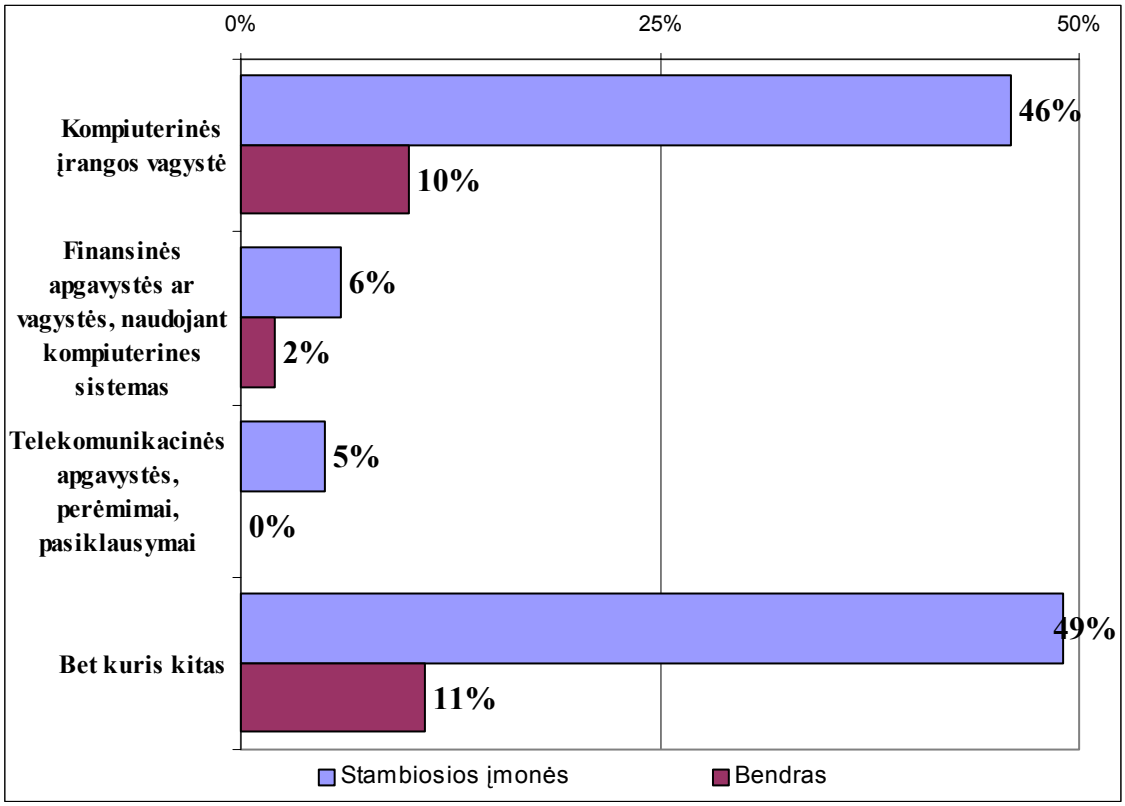
15. KOMPIUTERIŲ VAGYSTĖS IR KOMPIUTERINIAI SUKČIAVIMAI

Šioje kategorijoje pats populiariausias incidentas - kompiuterinės įrangos vagystės (28 pav.). Viena iš dešimties įmonių per paskutinius metus turėjo incidentus, kai buvo pavogti kompiuteriai. Stambiose įmonėse tokie incidentai buvo keturis kartus dažnesni nei smulkiosiose. Tai tik patvirtina tą faktą, kad vagys eina ten, kur tikisi didesnio grobio. Panašiai

yra ir su technologijų įmonėmis, kuriose vagys tikisi daugiau modernesnės ir brangesnės įrangos. Jos pranešė, kad turėjo dukart daugiau vagysčių negu vidutiniškai.

Viena stambi profesionalių paslaugų įmonė pranešė, kaip vagys buvo nusitaikę į jų įmonę. Savaitgaliai jie įeidavo į pastatą ir išnešdavo įvairią kompiuterinę įrangą. Tačiau vagys labiausiai dėmesį atkreipdavo į nešiojamuosius kompiuterius, dažnai palikdami kitą vertingą įrangą nepaliestą, nes nešiojamų kompiuterių portatyvumas ir lengvumas darė juos patraukliu taikiniu.

Fizinės vagystės buvo atskiri atvejai. Daugiau kaip du trečdaliai įmonių pranešė apie vienetinius atvejus ir nei viena jų nepranešė, kad turėjo daugiau nei dešimt vagysčių. Tokių incidentų, kaip pavagiami kompiuteriai daugiausia pasitaikydavo technologijų ir energetikos sektoriaus įmonėse.



28 pav. Kokio tipo vagystes ir apgavystes patyrė įmonės?

Finansinės apgavystės ir vagystės, naudojant kompiuterines sistemas, išlieka santykinai retais atvejais. Tik 2 procentai įmonių praėjusiais metais turėjo incidentus, susijusius su sukčiavimais, naudojant kompiuterinę įrangą. Trys ketvirtadaliai atvejų, tokie sukčiavimai buvo minimi kaip izoliuoti incidentai. Tačiau du trečdaliai įmonių kompiuterinį sukčiavimą įvertino kaip blogiausią metų incidentą, viršijusį net virusinę infekciją.

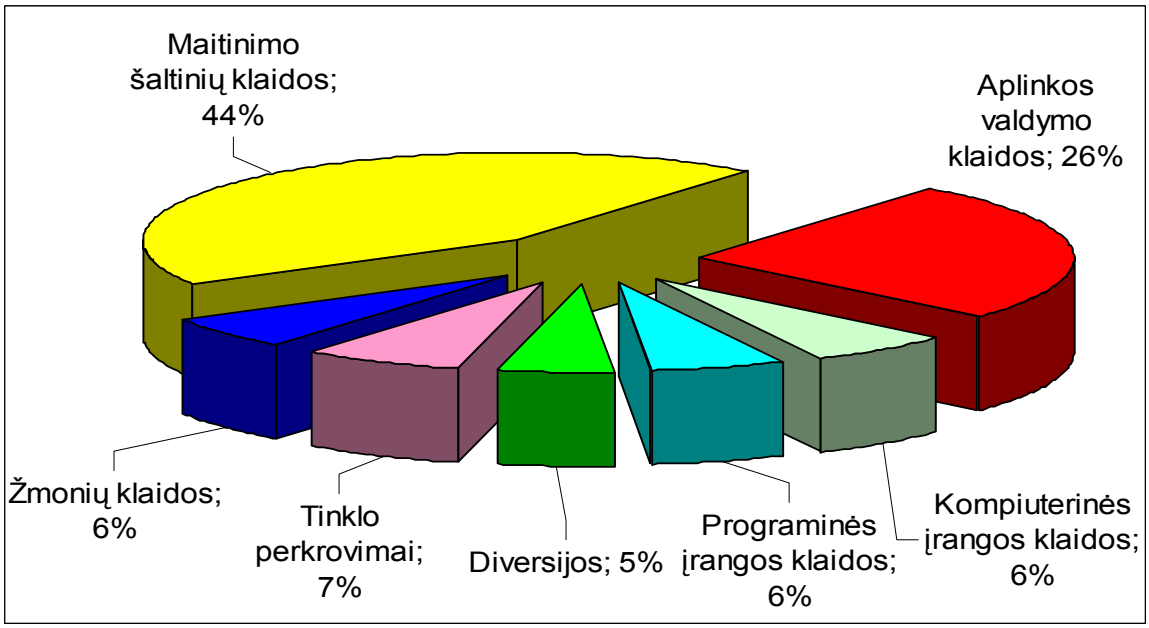
Stambiosios įmonės užfiksavo tris kartus daugiau kompiuterinių sukčiavimų atvejų nei smulkiosios. Jos taip pat daugiau patyrė ir daugiakartinių sukčiavimų. Telekomunikacinių paslaugų tiekėjai turėjo daugiausia tokių incidentų, ir kai kuriais pranešimais per metus jų pasikartojo daugiau negu dešimt kartų. Trečdalis gamybos įmonių taip pat patyrė daugiakartinius kompiuterinius sukčiavimo atvejus.

Telekomunikacinių apgavysčių atvejai, kai buvo perimami pokalbiai arba, kai buvo jų pasiklausoma, turėjo sąlyginai nereikšmingą poveikį. Apie didžiausius tokio pobūdžio incidentus pranešė finansinių paslaugų sektorius, ir stambiosios įmonės visuose kituose sektoriuose.

16. SISTEMOS GEDIMAI IR DUOMENŲ PRARADIMAS

Tyrimo metu nustatyta, kad ketvirtadalis Jungtinės Karalystės įmonių patyrė žymius sistemos gedimus ir duomenų praradimus. Ir čia stambiosios įmonės buvo labiau paveiktos tokio tipo incidentų nei mažosios ir vidutinės įmonės, dėl tos paprastos priežasties, kad jos paprastai kelia didesnius reikalavimus tinkamai sistemų veiklai. Jos taip pat linkusios daugiau naudoti informacinių sistemų, sukurtom pagal jų specialius užsakymus, nei įsigytom prekybos sistemoje. Tuo pat metu jos turi įdiegusios labiau griežtus pakeitimų valdymo ir atstatymo procesus, kurios leidžia fiksuoti daugiau incidentų.

Finansinių paslaugų ir technologijų sektoriaus įmonės turėjo du kartus daugiau šio tipo incidentų negu mažmeninės prekybos ir leidybos įmonės, turėjusios mažiausiai problemų. Incidentų kiekis aiškiai priklausė nuo informacinių sistemų skaičius ir jų sudėtingumo.



29 pav. Kokios pagrindinės sistemų gedimo ir duomenų praradimo priežastys?

Daugiausia sistemų gedimų įvyko dėl maitinimo šaltinių gedimų. Tokio pobūdžio gedimai sudaro 44 procentus, tai beveik pusė visų gedimų. Tarp stambiųjų įmonių ypač populiarus buvo maitinimo šaltinių gedimas.

11 procentų įmonių sistemos gedimus ir duomenų praradimus įvertino kaip blogiausius metų incidentus. Šis santykis buvo labai panašus tarp įvairaus dydžio įmonių, tačiau labai žymus skirtumas buvo tarp įvairių sektorių. Sistemų gedimas kaip blogiausias metų incidentas dažniausiai buvo minimas valdžios institucijose, gamybos, technologijų ir mažmeninės prekybos sektoriuose. Finansinių paslaugų ir kituose sektoriuose tokio pobūdžio incidentai buvo mažiausiai minimi kaip blogiausi metų incidentai.

Tiesioginėje internetinėje apklausoje daugiau negu pusė (53%) respondentų pranešė apie sistemų gedimo ar duomenų praradimo incidentus. Tai žymiai daugiau nei telefoninio tyrimo metu pranešė ne tik bendrai įmonės (27%), bet ir stambiosios įmonės (42%).

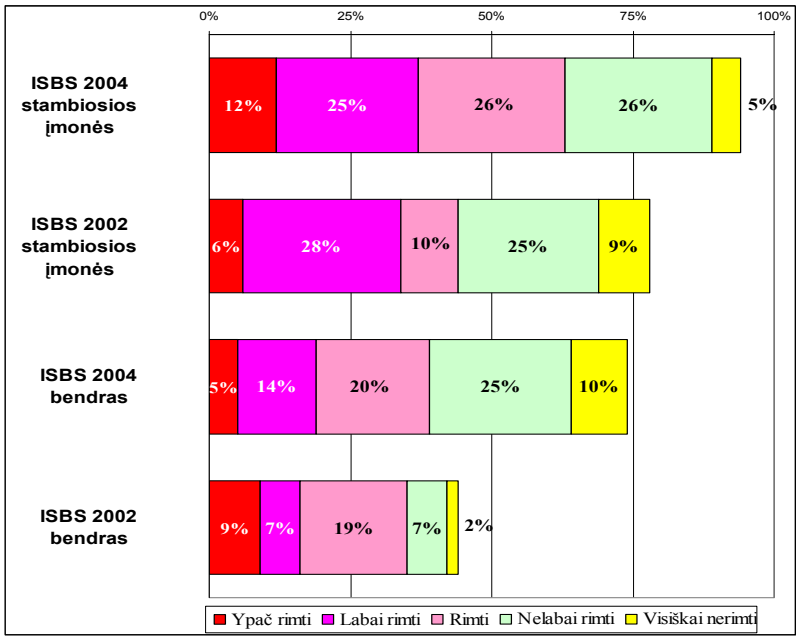
17. PAŽEIDIMŲ POVEIKIS

Rizikos įvertinimas visada bus efektyvus, jeigu įmonės supras ne tik incidentų skaičiaus tendenciją, bet ir jų poveikį.

Pusė visų įmonių, kurios buvo patyrusios saugumo incidentus, laikė, kad jų blogiausias incidentas buvo ir pats rimčiausias. Ketvirtadalis įmonių turėjo labai rimtus pažeidimus. Palyginus su praėjusiu tyrimu ISBS 2002 stebimas labai nedidelis rimtų incidentų sumažėjimas (30 pav.). Tačiau tai klaidinantis įspūdis. Pažeidimų skaičius augo palyginti sparčiai, kad, bendrai paėmus, daugelis kompanijų rimtų incidentų turėjo daugiau nei prieš du metus. Ypač tai

teisinga, kalbant apie stambiąsias įmones, kur net du trečdaliai įmonių pripažino, kad patyrė rimtus sistemų pažeidimus.

Daugelis informacijos saugumo tyrimų organizatorių incidentų vertinimui, kaip matavimo vienetą pilnam poveikiui įvertinti, naudoja incidentų kainą. Organizatoriai paprastai prašo, kad respondentai įvertintų bendrą kainą. Bet daugeliui respondentų tai yra labai sunkus klausimas. Informacijos pažeidimai gali turėti daug įvairių paveikių. Vienos iš jų - tiesioginės grynųjų išlaidos. Tačiau privalo būti įtrauktas ir kitos sąnaudos, pavyzdžiui tokios kaip laikas, skirtas pažeidimui ištirti ir į jį sureaguoti. Kiti poveikiai, tokie kaip veiklos sužlugdymo kaina ar reputacijos pažeidimas, kiekybiškai yra sunkiai įvertinamos.

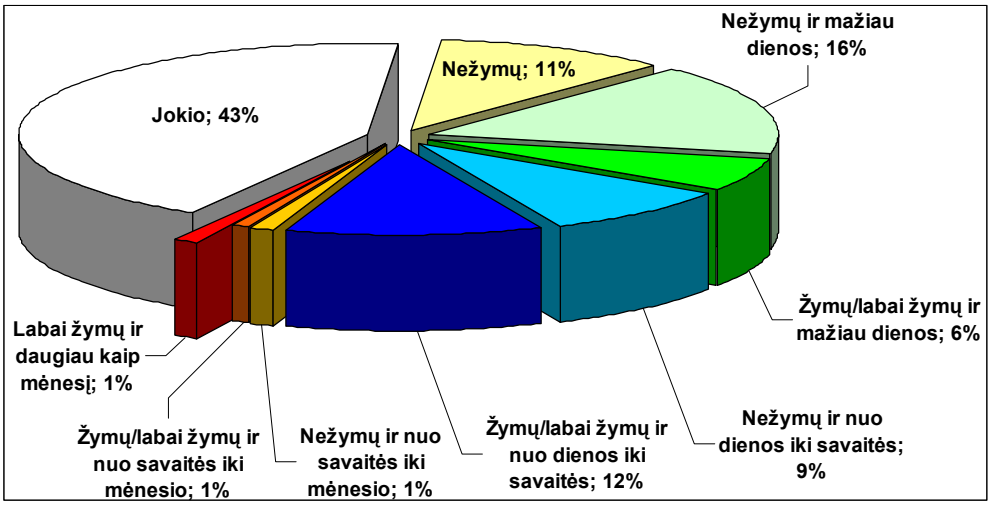


30 pav. Kiek įmonės turėjo rimtų incidentų?

Pažeidimų sudedamųjų dalių kainos analizė turėtų suteikti aiškumą, įvertinant incidentų kainą.

18. VEIKLOS SUŽLUGDYMAS

Pats didžiausias blogiausių incidentų poveikis yra įmonių veiklos sužlugdymas. Pusė iš jų baigėsi normalios veiklos pertraukimu. Ketvirtadalis baigėsi daugiau negu vienos dienos praradimu. Buvo užfiksuota keletas atvejų, kai normalus darbas buvo sutrikdytas daugiau kaip mėnesį. Sistemos gedimas, virusinė infekcija ir slaptumo pažeidimai iššaukė ilgalaikius darbo sutrikimus. Tokie incidentai, kaip įmonių svetainių atakos (aptarnavimo atmetimo incidentas) turėjo tik trumpalaikius veiklos sutrikimus.



31 pav. Kokį poveikį įmonių veiklai padarė blogiausi saugumo incidentai?

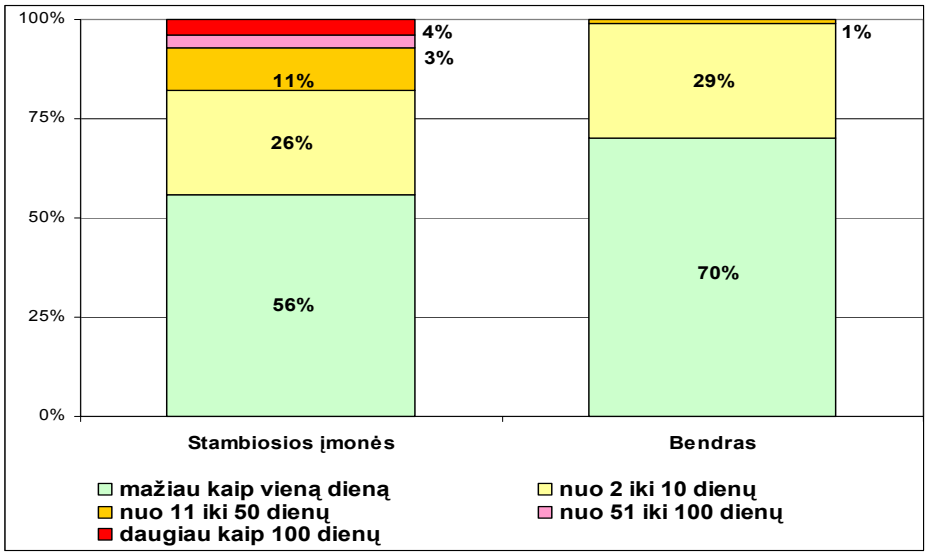
Kuo ilgesnis normalios veiklos pertraukimas, tuo toks incidentas rimčiau vertinamas. Respondentai pažymėjo, kad konfidencialumo pažeidimai turėjo didžiausią neigiamą poveikį jų veiklai. Bet toks pažeidimas labiausia buvo aktualus įmonių vadovams, negu darė neigiamą poveikį pačioms informacinėms sistemoms. Prie kitų incidentų, kurie iššaukė pagrindinius veiklos pažeidimus, respondentai priskyrė sistemų gedimus, netinkamą personalo informacinių sistemų naudojimą ir pašalinių asmenų įsiskverbimus į sistemas.

Viena leidybos įmonė pranešė, kad jų sistemas užkrėtus *Blaster* kirminu, jų normali veikla patyrė labai didelis sutrikdymus ilgiau negu mėnesį laiko. Tyrimo metu buvo nustatyta, kad įvykus blogiausiam metų saugumo incidentui vidutiniškai mažosios įmonės patyrė veiklos sužlugdymus nuo vienos iki dviejų dienų, o tuo tarpu stambiųjų įmonių veikla vidutiniškai buvo sustabdyta nuo vienos iki trijų dienų.

Galima pateikti tik grubų incidento vertės įvertinimą, sužlugus įmonės veiklai, paskaičiavimams naudojant vidutinę apyvartą ir prielaidą apie poveikį veiklai. Taigi smulkiosioms įmonėms blogiausi metų incidentai apytiksliais paskaičiavimais vidutiniškai kainavo nuo 5 000 iki 10 000 svarų sterlingų, o stambiosioms įmonėms nuo 50 000 – 150 000 svarų sterlingų.

19. REAGAVIMO Į INCIDENTUS KAINA

Respondentai pažymėjo, kad daugumą incidentų pavyko santykinai lengvai ištirti ir nustatyti. Du trečdaliai blogiausių incidentų tam pareikalavo mažiau nei vienos žmogaus darbo dienos ir nereikalavo grynųjų išlaidų incidento pasekmių likvidavimui (32 pav.).



32 pav. Kiek laiko užtruko atsakyti į blogiausią incidentą?

Tačiau trečdalis blogiausių incidentų buvo susiję su žymiomis išlaidomis. Keletas smulkiųjų įmonių turėjo pažeidimus, kurių pasekmėms likviduoti reikėjo daugiau negu 50 žmogaus darbo dienų. Šioms įmonėms tai buvo labai sunki našta.

Viską susumavus vidutiniškai kiekviena Jungtinės Karalystės įmonė sunaudojo po dvi – keturias žmogaus darbo dienas, kad sureaguoti į jų blogiausią metų saugumo incidentą. Tai prilyginama nuo 500 iki 1 000 svarų sterlingų. Buvo pastebėta tendencija, kad stambiosios įmonės incidentų pasekmių likvidavimui naudojo daugiau laiko, ir vidutiniškai sugaišo nuo 10 iki 20 žmogaus darbo dienų jų blogiausių metų pažeidimo pasekmių likvidavimui. Tai prilyginama nuo 3 000 iki 6 000 svarų sterlingų.

Tyrimo organizatoriai atkreipė dėmesį į tai, kad konfidencialumo ir įstatymo pažeidimų nagrinėjimas ir pasekmių šalinimas užėmė daugiausia laiko, atakos į įmonių svetaines - mažiausiai.

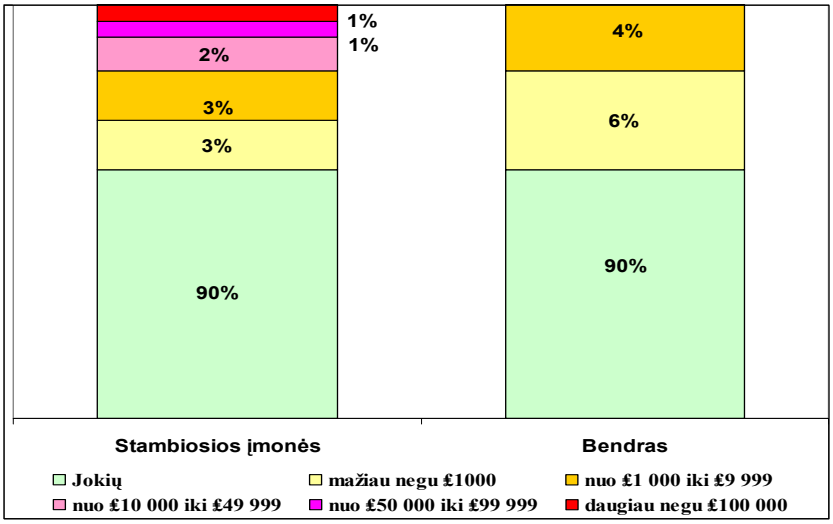
Prie tų sąnaudų, kurios buvo pateiktos aukščiau papildomai blogiausio metų incidento pasekmių likvidavimui vidutiniškai įmonės sunaudojo nuo 1 000 iki 2 000 svarų sterlingų, o stambiosios nuo 5 000 iki 10 000 svarų sterlingų.

Kompiuterinės įrangos fizinis pavogimas baigdavosi didžiausiomis grynųjų pinigų išlaidomis. Vidutiniškai po vagystės grynųjų pinigų buvo išleidžiama tris kartus daugiau, negu po kurio nors kito incidento. Ir priešingai, atakos į svetaines ar įsiskverbimas į sistemas baigdavosi daugiau kaip 1 000 svarų sterlingų išleidimu, kad pašalinti incidento pasekmes.

Tyrimo organizatoriai abejoja, kad įmonės įvertino ir nurodė visas saugumo incidentų atstatymo išlaidas. Vienos įmonės informacijos saugumo vadovas prisipažino, kad daugiausia laiko ir pinigų buvo išleista tam, kad ištirti ir sutvarkyti patį blogiausio metų saugumo incidentą. Tačiau jis negali kiekybiškai įvertinti nei grynųjų pinigų išlaidų, nei laiko vertės.

20. TIESIOGINIAI FINANSINIAI NUOSTOLIAI

Tyrimas pažymėjo, kad įmonės pranešė atvejus, kai dėl tam tikrų saugumo pažeidimų jos patyrė tiesioginius finansinius nuostolius, tokius kaip baudos ar kompensacijos už padarytą žalą. Keletas tokių incidentų baigėsi žymiu grynųjų pinigų praradimu. Prie tokių incidentų galima priskirti finansines apgavystes ir fizines vagystes. Patys didžiausi tiesioginiai grynųjų nuostoliai buvo patirti dėl duomenų konfidencialumo pažeidimo. Viena vidutinio dydžio įmonė pranešė, jog dėl konfidencialių duomenų vagystės patyrė 250 000 svarų sterlingų tiesioginių finansinių nuostolių. Dėl tokio santykinai mažo tiesioginių finansinių nuostolių dydžio įmonės vidutiniškai patiria nuo 200 iki 500 svarų sterlingų, o stambiosios įmonės nuo 2 000 iki 4 000 svarų sterlingų tokių išlaidų.



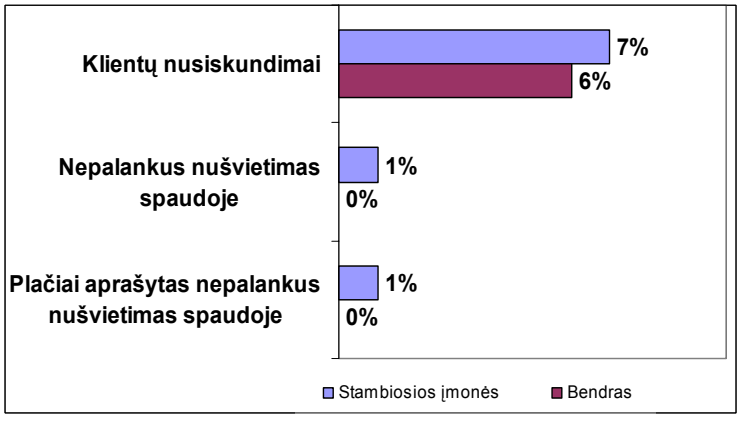
33 pav. Kokius tiesioginius finansinius nuostolius dėl blogiausių incidentų patiria įmonės?

21. PAKENKIMAS REPUTACIJAI

Respondentai buvo vieningos nuomonės, kad dienraščių pirmuosiuose puslapiuose pasirodantys pranešimai apie saugumo pažeidimus, kiekvienam saugumo vadovui košmariškas scenarijus. Įmonėms, kurių vardas šalyje ir pasaulyje gerai žinomas, linkusios ypač bijoti bet kokio pakenkimo jų reputacijai. Įmonės siekia savo saugumo incidentus nuo savo klientų ir masinių informacijos priemonių laikyti paslaptyje.

Pagal tyrimo tik vienai įmonei iš penkiolikos jų saugumo incidentai baigėsi klientų nusiskundimu (34 pav.). Dažniausiai klientai skundėsi dėl nesankcionuoto slaptos asmeninės informacijos paskelbimo. Kitos priežastys dėl kurių skųsdavosi klientai buvo finansinės apgavystės, atsitiktiniai sistemų gedimai ir virusų proveržiai, kurie laikinai sutrikdydavo sistemų darbą ir tuo gadino klientams nuotaiką.

Keletas stambiųjų įmonių pranešė apie ypač nepalankius pranešimus spaudoje, kur buvo rašomą apie jų įmonėje įvykusius saugumo pažeidimus. Spauda ypač domėjosi virusų infekcijomis ir netinkamu personalo interneto naudojimu. Daugiausia buvo rašoma apie gamybos, sveikatos apsaugos ir švietimo sektoriuose įvykusius incidentus.



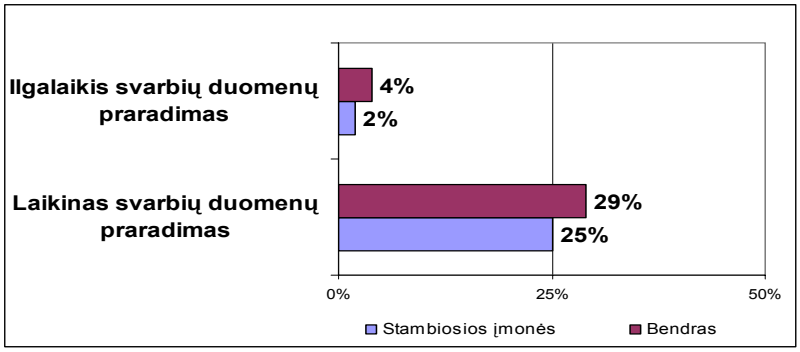
34 pav. Kaip saugumo incidentai pakenkė įmonių reputacijai?

Poveikį reputacijai išreikšti skaičiais yra labai sunku. Respondentai pateikė daug pavyzdžių, kai vienos įmonės dėl neigiamo incidentų nušvietimo spaudoje patyrė minimalius nuostolius, o kitas toks spaudos dėmesys tiesiog sužlugdydavo. Dėl žemo tokių incidentų skaičiaus, tyrimo organizatorių vertinimu vidutinė pakenkimo reputacijai kaina yra taip pat

žema ir apytikriai įmonėms sudaro nuo 100 iki 300 svarų sterlingų, o stambiosioms nuo 5 000 iki 20 000 svarų sterlingų.

22. DUOMENŲ PRARADIMAS

Tyrimo metu apie du trečdaliai įmonių nenurodė, kad dėl jų blogiausio metų saugumo incidento buvo prarasti svarbūs duomenys. Likusieji nurodė, kad jie patyrė laikinus svarbių duomenų praradimus, bet buvo pajėgūs atstatyti juos iš savo rezervinių kopijų. Tačiau beveik viena iš dvidešimties įmonių prarado dalį svarbios informacijos ilgam (35 pav.).



35 pav. Saugumo incidento pasekmės duomenų praradimui?

Tyrimo organizatoriai nurodė, kad apie pusė visų konfidencialumo pažeidimų buvo susiję su vienokia ar kitokia duomenų vagyste. Trečdalis fizinių vagysčių buvo susijusios su kompiuterių, kurie turėjo svarbius duomenis, pavogimu. Pusė respondentų paminėjo, kad jie duomenis prarado dėl sistemos klaidų. Sistemų gedimai buvo svarbiausia ilgalaikė svarbių duomenų praradimo ar sugadinimo priežastis.

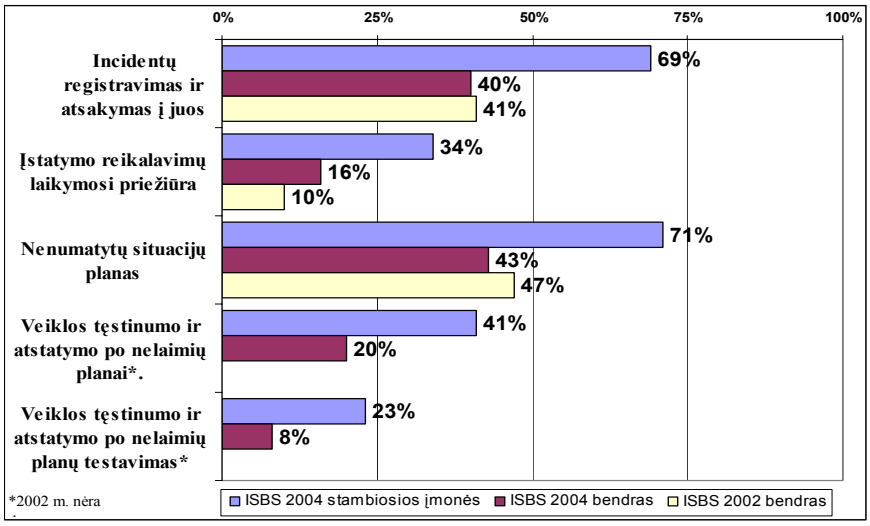
23. BENDRA INCIDENTO KAINA

Apibendrinus visus šiuos skirtingus saugumo incidentų poveikius, tyrimo organizatoriai paskaičiavo, kad Jungtinės Karalystės įmonės, įvykus jose blogiausiam metų incidentui, vidutiniškai patyrė nuo 7 000 iki 14 000 svarų sterlingų nuostolių. Stambiosioms įmonėms nuostoliai žymiai didesni ir svyravo nuo 65 000 iki 190 000 svarų sterlingų. Vidutinės išlaidos lyginant su 2002 m., kai jos buvo įvertintos 30 000 svarų sterlingų truputį sumažėjo. Tai atitinka mažėjančiai vidutinei rimtų pažeidimų kreivei. Daugelis įmonių ateities atžvilgiu nusiteikusios pesimistiškai. Įmonės supranta, kad joms reikės žymiai padidinti pastangas, siekiant sumažinti incidentų skaičių ir jų poveikį, nes priešingu atveju nuostoliai bus žymiai didesni.

24. REAKCIJA Į INCIDENTUS IR NENUMATYTŲ SITUACIJŲ PLANAVIMAS

Kaip jau buvo minėta ankščiau, 2004 m. tyrimas parodė, kad Jungtinės Karalystės įmonės vis dažniau patiria saugumo incidentus, kurie jų veiklai turi žymų poveikį. Šiuolaikinėje aplinkoje, įmonės turi prieš atakas priešpastatyti efektyvią savo gynybą, tačiau ši gynyba niekada nebus šimtu procentų neklystanti. Tai suprasti yra gyvybiškai svarbu ir įmonės turi būti gerai pasiruošusios sureaguoti į įvairiausius incidentus ir turėti pas save patvirtintus nenumatytų situacijų planus. Tokie planai turi padėti joms žymiai sumažinti atstatymo po įvykusių incidentų laiką ir pastangas.

Pirmaeilis uždavinys įvykus saugumo incidentui - gebėjimas reaguoti greitai ir efektyviai. Incidentų registravimas ir personalo gebėjimas atsakyti į juos yra kritiškai svarbūs. Panašus skaičius įmonių, kaip ir prieš dvejus metus atliktame tyrime, turėjo aprašytas incidentų registravimo procedūras. Tarp stambiųjų įmonių šis skaičius didesnis - du trečdaliai jų turėjo aprašytas incidentų registravimo procedūras (36 pav.).



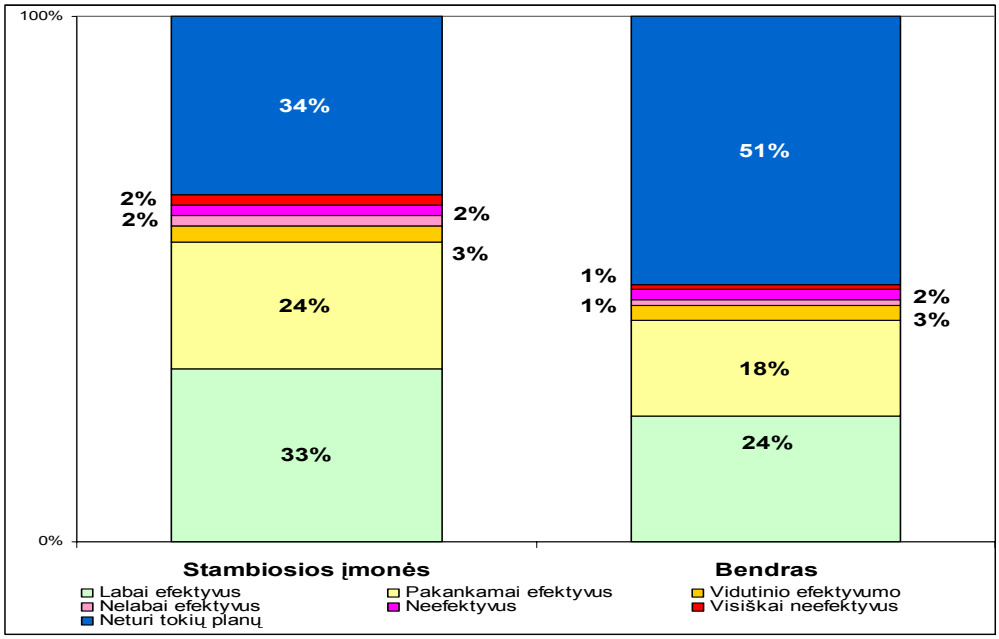
36 pav. Kokias įmonės turi procedūras, padedančias joms atsakyti į saugumo incidentus?

Kadangi vis daugiau klientų, gindami savo pažeistas teises, linkęs bylinėtis teismuose, įmonės privalo turėti reikiamus įrodymus, kurie tenkintų juridinius standartus, kad jos laikosi šalyje priimtų įstatymų reikalavimų. Teismai vis labiau atkreipia į tai dėmesį. Viena iš šešių įmonių yra pajėgi užtikrinti tokią įstatymų reikalavimų laikymosi priežiūrą. Nors šie skaičiai ir nėra pakankamai, bet pagerėjimo požymiai nuo 2002 m. matomi, kai tada viena iš dešimties įmonių buvo pajėgi užtikrinti tokią priežiūrą pagal įstatymų reikalavimus.

Nenumatytų situacijų planas turėtų duoti įmonėms tam tikrą ramybę, kad įvykus saugumo pažeidimui, poveikis įmonės veiklai būtų minimalus. Kaip parodė tyrimas, apie pusė įmonių turi tokius nenumatytų situacijų planus, o stambiųjų įmonių grupėje apie tris ketvirtadalius įmonių. Tyrimo organizatoriai tikėjosi, kad įmonės nenumatytų situacijų planus plačiai įtrauks į atstatymo po nelaimių planus ir juos testuos. Tačiau, atrodo, taip neatsitiko. Tik viena iš penkių įmonių turėjo atstatymo po nelaimių planą ir mažiau negu viena iš dešimties testuoja šį planą. Stambiosiose įmonėse ir vėl situacija dvigubai geresnė negu smulkiosiose.

Kai įmonės patyrė blogiausius metų incidentus, tik apie pusė jų turėjo veikiančius nenumatytų situacijų planus. Beveik ketvirtadalis įmonių nurodė, kad jos pasitikėjo savo rezervine kopija ir nenumatytų situacijų planu, kurie turėjo patikimai užkirsti kelią blogiausiam jų saugumo incidentui. Du trečdaliai šių įmonių prisipažino, kad po saugumo pažeidimų pagerino savo rezervines kopijas ir nenumatytų situacijų planus.

Tyrimo organizatoriai nustatė, kad po incidentų dauguma įmonių buvo nusiteikusios pakeisti jų saugumo valdymo sistemą taip, kad ateityje jos nepatirtų panašių pažeidimų arba, kad tas poveikis būtų silpnesnis. Tačiau ir toliau išlieka ta pati problema, kad įmonės linkusios laukti, kol patiria saugumo incidentą, o po to vertinti riziką.



37 pav. Nenumatytų situacijų planų efektyvumas, įvykus blogiausiam saugumo incidentui.

Jeigu buvo pažeista saugumo politika, įmonės labai greitai prieš personalą imasi drausminančių veiksmų. Jeigu tokių incidentų priežastys būdavo darbuotojų netinkami veiksmai, tai tokios drausminančios priemonės buvo normaliai vertinamos. Virusų infekcijų atveju, visi buvo bendros nuomonės, kad niekas neturi teisės pažeisti nustatytų taisyklių. Tačiau tik kelios jų ėmėsi atitinkamų teisinių veiksmų. Respondentai išreiškė norą, kad būtų labiau kovojama su virusų rašytojais.

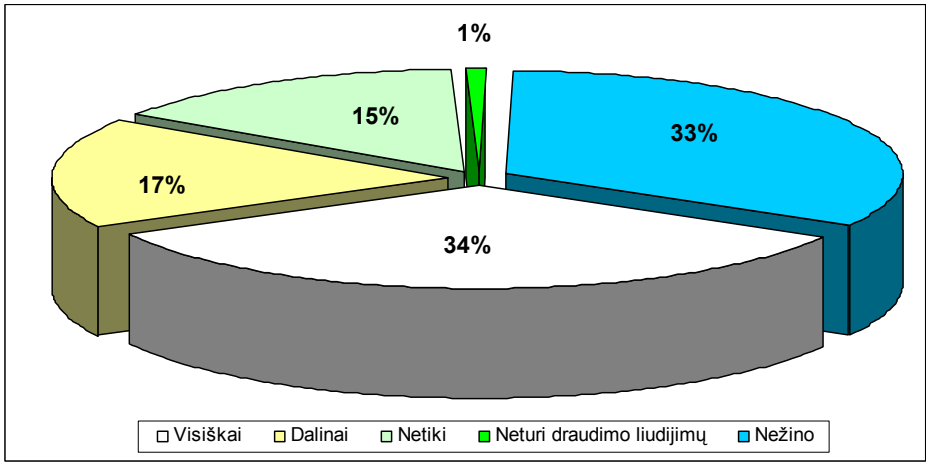
25. DRAUDIMAS

Su bet kokia rizika galima elgtis labai įvairiai, galima priimti ją kai reiškinį ir nieko nedaryti, siekti sumažinti ją, sudarant įmonėse atsakomąsias priemones, siekiant užkirsti kelią jų pasirodymui, ar perduoti jas kitiems, pvz. draudimo kompanijoms. Saugumo rizikos beveik niekuo nesiskiria nuo kitų rizikų.

Tačiau paskutiniųjų metų statistika rodo, kad draudimo kompanijos vis labiau siekia atskirti rizikas, susijusių su informacijos saugumo incidentais, nuo bendros saugumo politikos. Daugeliui įmonių tai sukėlė netikrumo jausmą, ar jos turi draudimo priedangą. Atsiradus šioje srityje tokių paslaugų trūkumui, keletas draudimo bendrovių turėjo pristatyti IT specifines draudimo paslaugas. Tačiau šių specialių draudimo paslaugų naudojimas vis dar labai mažas.

Įvertinant tai, kas čia buvo pasakyta, gali būti keista, kad trečdalis įmonių visiškai tiki tuo, kad jų turimi įprasti draudimo liudijimai, suteikia pilną garantiją, kad bus atlyginti nuostoliai, kuriuos įmonės patirs dėl saugumo pažeidimo ar duomenų praradimo (38 pav.).

Tai atitinka lygį, buvusį prieš dvejus metus. Trečdalis įmonių, kurios prisipažino, kad nežino ar yra apsaugotos, atrodo labiausiai realistiškos. Viena iš šešių netiki, kad jos yra visiškai apsaugotos, ir labai panašus skaičius įmonių tiki tuo, kad turimi draudimo liudijimai jas dalinai saugo.



38 pav. Ar įmonės tiki, kad turimi jų įprasti draudimo liudijimai apsaugo juos nuo saugumo pažeidimo ir duomenų praradimo?

Tyrimo organizatoriams, aptariant su respondentais draudimo klausimą, viena saugumo vadovė sakė, kad draudimas nepriklauso jos kompetencijai. Ji atsakinga už informacijos saugumą, ir neužsiima bendrais informacijos rizikos klausimais. Tie, kurie derasi su draudimo kompanijos dėl draudimo liudijimų, su ja nesikonsultuoja.

Tyrimas parodė, kaip svarbu šiandien įmonėms suprasti, ar turimi draudimo liudijimai pilnai apsaugo nuo galimų nuostolių, kuriuos įmonės gali patirti saugumo pažeidimų atveju. Jeigu tai nėra, jos turi papildyti esamus draudimo liudijimus papildomomis sąlygomis, suteikiančioms apsaugą nuo pasirodančių saugumo grėsmių.

26. ELEKTRONINIO PAŠTO IR INTERNETO NAUDOJIMAS

Interneto ir elektroninio pašto naudojimas dabar įprastas dalykas kiekvienoje įmonėje. Devynios iš dešimties įmonių suteikia personalui priėjimą interneto. Labai gaila, kad su šia galimybe atsiranda daug papildomų problemų - virusai, netinkamas interneto ir elektroninio pašto naudojimas, nepageidaujami laiškai.

Be jokios abejonės, virusai ir piktavališki kodai yra didžiausias įmonių rūpestis. 93 procentai įmonių bendrai ir 99 procentai stambiųjų turi įdiegusios serveriuose ir kompiuteriuose antivirusines programas. Beveik visos įmonės, kurios jungiasi prie interneto naudoja antivirusinę programinę įrangą. Stambiosios įmonės linkusios naudoti daugialaipsnę apsaugą. Virš pusės stambiųjų įmonių tikrina ateinančius elektroninius laiškus ir perkėlimus iš interneto. Nežiūrint visa to, virusinių infekcijų incidentai nuolatos auga. Tyrimo organizatoriai įžvelgia dvi pagrindines priežastis.

Pirma, antivirusinė programinė įranga yra gera tik tada, kada ji turi pačius paskutinius atnaujinimus. 95 procentai įmonių automatiškai atnaujina antivirusinę programinę įrangą, kai tik identifikuojami naujo viruso požymiai. Kitais atvejais tai niekada nedaroma.

Antra, virusai nuolatos evoliucionuoja. Vis labiau įmonės susiduria su kompleksinėmis grėsmėmis, turinčiomis virusų, kirminų ir Trojos arklių savybių, kurios meistriškai apsijungia, kad įsibrauti į įmonių duomenų bazes. Tokios kompleksinės grėsmės (pvz. *Blaster*) gali apeiti antivirusines programas ir atakuoti silpniausias tinklo saugumo sritis.

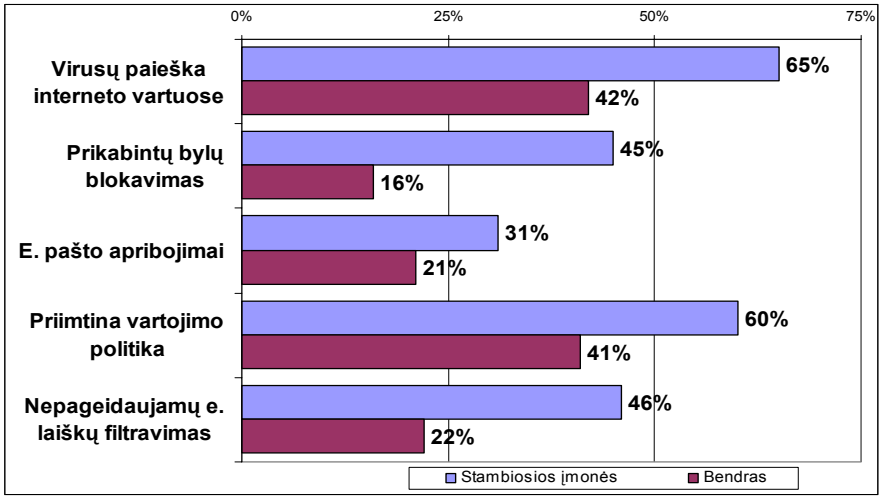
Ypač didelį susirūpinimą įmonėse kelia netinkamos darbuotojų interneto ir elektroninio pašto naudojimas. Faktiškai kiekviena įmonė, kuri turi pas save turi įdiegusi pilną saugumo politiką, turi taip pat ir tiksliai apibrėžtą elektroninio pašto ir interneto naršymo politiką. Įmonės, kurios riboja personalo priėjimą prie interneto ir elektroninio pašto ar turi įdiegusios atitinkamas politikas, turi žymiai mažiau šios rūšies piktnaudžiavimo incidentų.

Vidutinis elektroninio pašto ir interneto naršymo kontrolės lygis yra žemesnis nei buvo prieš dvejus metus. Viena pagrindinių to priežasčių, sunku įgyvendinti kontrolės mechanizmą.

Daugelis įmonių nustojo blokuoti elektroniniu pašto perduodamas bylas, supratę, kad tai užima daug laiko.

Įmonės, kurios registruoja ir stebi darbuotojų priėjimus prie interneto, pranešė apie didelį piktnaudžiavimo internetu mastą. Vadinasi, įmonėse, kuriose nėra įdiegtų kontrolės mechanizmų, panašūs incidentai negali būti aptikti.

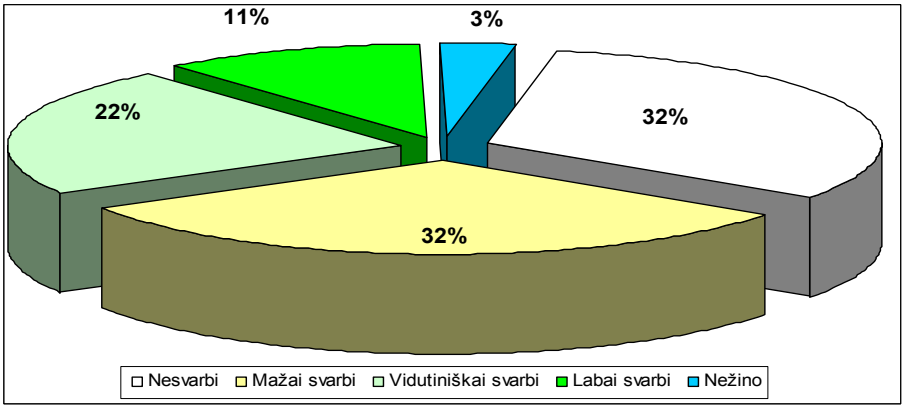
Apie potencialius netinkamo elektroninio pašto naudojimo poveikius stambiosios įmonės žino daugiau, nei smulkiosios. Pavyzdžiui, stambiosios įmonės tris kartus labiau linkusios naudoti teisinius elektroninio pašto naudojimo reglamentavimus, nei smulkiosios. Jos taip pat tris kartus labiau linkusios derėtis su darbuotojais, prašant jų sutikimo (kad nebūtų pažeistos darbuotojų teisės), kad saugumo incidentų tyrimo metu gali būti skaitomi darbuotojų laiškai.



39 pav. Kokią saugumo kontrolę internetui ir elektroniniam paštui naudoja įmonės?

Elektroninio pašto šifravimas ir elektroninio parašo naudojimas kol kas nėra populiarus, ir daugelis įmonių siunčia elektroninius laiškus internetu atviru tekstu.

Paskutiniuoju metu įmonės vis labiau susirūpina didėjančiu nepageidaujamų laiškų (*spam*) srautu. Viena iš dešimties įmonių nepageidaujamus laiškus vertina kaip labai svarbią problemą, dėl kurios švaistomas darbuotojų darbo laikas (40 pav.). Gal būt todėl, beveik viena iš keturių įmonių, ir beveik pusė stambiųjų įmonių, filtruoja įeinančius laiškus nuo nepageidaujamų (39 pav.).



40 pav. Kaip įmonėms yra svarbi nepageidaujamų laiškų (spam) problema?

27. ĮMONĖS SAUGUMAS

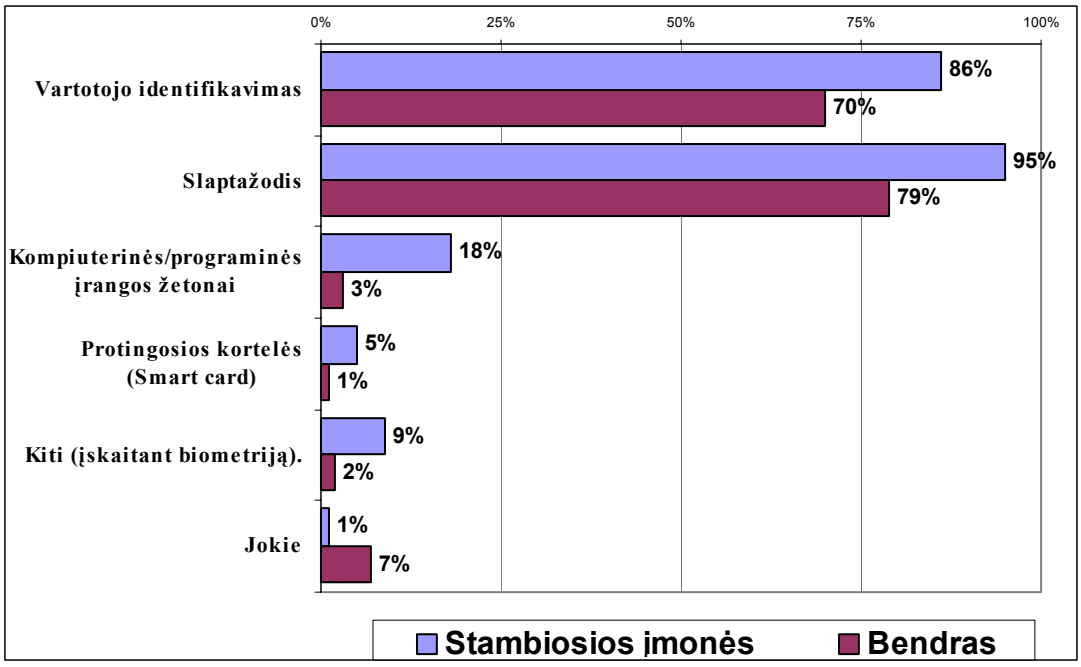
Įmonėms kiekvienu atveju būtina įsitikinti, kad reikiami žmonės reikiamu laiku turi priėjimą prie reikiamų sistemų ir labai svarbu blokuoti priėjimą prie sistemų, neturintiems teisės prie jų prieiti.

Pagrindinis įmonės saugumo elementas yra tapatumo valdymas, kuris turi būti pakankamai tvirtas, kad būtume įsitikinę, kad vartotojas:

- yra tas kas sakosi esąs;
- gali matyti tik jam skirtą informaciją, ir
- efektyviai ir nedelsiant pajungiamas prie sistemos, kai prisijungia ir išmetamas iš sistemos, kai išvyksta.

Didėjantis IT sistemų sudėtingumas turi sudėtingesnį vartotojų priėjimo valdymą. Kadangi daugelis įmonių savo sistemas atveria tiesioginiam priėjimui klientams, verslo partneriams ir tiekėjams, padidėja įmonės išbandymas. Vidutiniam vartotojui jo kasdieniniam darbui dažnai būtina prieiti prie keleto skirtingų IT sistemų. Kuo didesnė įmonė, tuo daugiau sistemų kiekvienas individualiai naudoja. To rezultate, įmonės vis labiau automatizuoja vartotojų priėjimo prie sistemų suteikimo, pakeitimo ir išmetimo procesą. Dabar tą jau daro 16% visų įmonių ir 31% stambiųjų įmonių.

Visos organizacijos siekė turėti vienintelę registraciją, kai vartotojas visoms sistemoms turi vieną vartotojo tapatybės dokumentą (ID) ir slaptažodį. Šiuo atveju, mažai tikėtina, kad vartotojas pasirinks lengvą slaptažodį ar jį kur nors įrašys. Tačiau tokia vienintelė registracija, gali leisti nesankcionuotą priėjimą prie visų sistemų, kurias asmuo naudoja. Tačiau naudojant griežtą tapatybės patvirtinimą (protingos kortelės (*smart cards*), biometrija) riziką galima sumažinti. Tačiau kaip atskleidė tyrimas, tokios priemonės naudojamos pakankamai retai (41 pav.).



41 pav. Kokie naudojami tapatybės patvirtinimo metodai?

Įmonės su vienintele registracija ir neturinčios griežto autentiškumo patvirtinimo patyrė aukštesnį nei vidutinis nesankcionuoto priėjimo incidentų skaičių. Ir priešingai, pirmieji griežto tapatumo patvirtinimo naudotojai patyrė žymiai mažiau tokių incidentų.

Įmonės saugumas yra ne tik konfidencialumas, bet ir sistemų prieinamumas bei jų vientisumas. Daugelis įmonių nukenčia nuo atsitiktinių sistemos gedimų ar duomenų praradimų. Galima tik pasidžiaugti, kad 95 procentai įmonių turi įdiegusios įvairių formų rezervinių kopijų darymo procesus. Tačiau kelia nerimą tai, kad šie procesai daugeliu atvejų

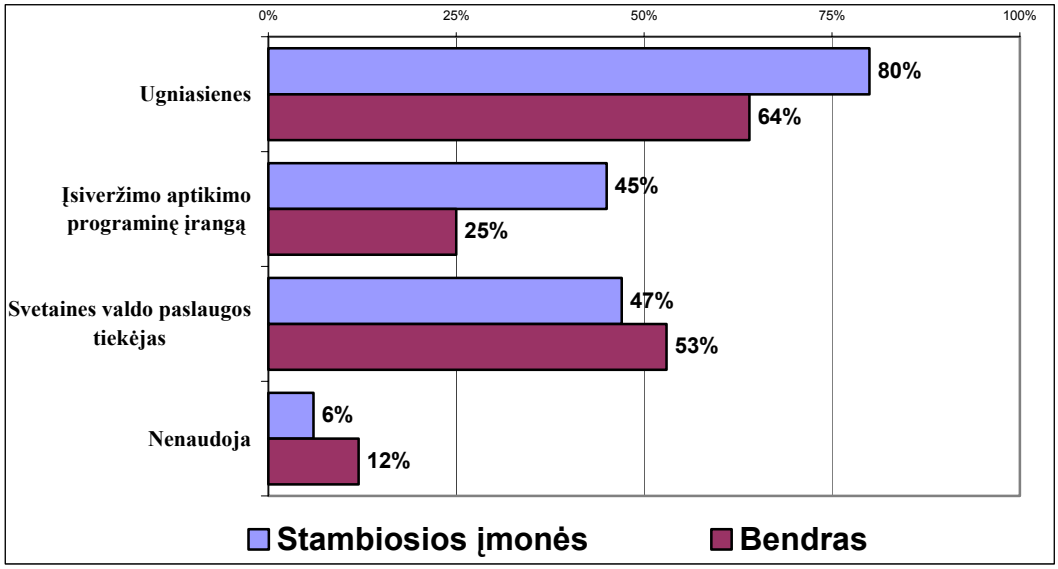
atrodo neatitinka jiems keliamų reikalavimų. Tiktai trečdalis įmonių savo kopijas saugoja ne ten, kur jos yra daromos. Be to, kopijų kokybė labai stipriai priklauso nuo juostų saugojimo sąlygų, nekalbant jau apie gerai visiems žinomas juostų patikimumo problemas. Į šiuos pastebėjimus daugelis įmonių, nesuvokdamos savo duomenų reikšmės, apie tai pradeda galvoti tik tada, kai jau būna per vėlu apie tai galvoti.

Kaip matėme iš 36 paveikslo tik 20 procentų įmonių ir 41 procentų stambiųjų turėjo parengusios atstatymo po nelaimių planus, ir tik 8 procentai bei 23 procentai stambiųjų įmonių praktiškai patikrino šiuos savo planus, kad įsitikintų ar tikrovėje jie veikia.

28. TINKLO SAUGUMAS

Daugeliui įmonių jų tinklo tradicinė riba baigiasi ties interneto vartais. Įmonių dėmesio centre buvo perimetro apsaugojimas, mažiau dėmesio kreipiant, vidinio kompiuterius tinklo apsaugai. Įprasta malda buvo „Kompiuterinė įranga išorei, programinė įranga vidui".

Įmonių svetainės „sėdi" ant tinklo perimetro ir jų saugumas santykinai tvirtas, nes čia įmonės visada linkusios prieš įsibrovimus dislokuoti preventyvią techniką. Trys ketvirčiai įmonių vidinių svetainių apsaugai naudoja ugniasienes, bet daugiau kaip pusei jų tai vienintelė apsauga. Stambiosios įmonės be ugniasienių savo svetaines saugo su įsiveržimų aptikimo programine įranga (42 pav.).



42 pav. Ką įmonės naudoja savo svetainių apsaugai?

Beveik pusė visų įmonių savo svetaines laiko pas paslaugos tiekėjus išorėje. Įmonės pasitiki paslaugų tiekėjo teikiamu saugumu. Tačiau daugelis įmonių prisipažino, kad nežino, kokias paslaugų tiekėjai naudoja saugumo priemones prieš svetainių atakas.

Tinklo perimetro ribos išsiplečia, dėl vis labiau populiarėjančios galimybės suteikti personalui priėjimą prie įmonės sistemų iš išorės. Tuo dabar naudojasi daugiau kaip pusė įmonių. Tačiau toks didėjantis nuotolinio priėjimo įsisavinimas reikalauja papildomo saugumo valdymo priemonių įdiegimo. Tyrimas parodė, kad taip dar nėra. Ketvirtis įmonių, kurios teikia darbuotojams priėjimą prie sistemų per nuotolinį neturi jokio papildomo valdymo. Tik ketvirtis įmonių šifruoja savo perdavimus, naudodamos VPN privataus tinklo technologijas.

Kad suteiktų darbuotojams lengvesnį priėjimą prie reikiamos informacijos, įmonės taip pat naudoja delniukus - asmeninius skaitmeninius pagalbininkus (*Personal Digital Assistants - PDAs*). Tai elgiasi trečdalis įmonių (ir pusė stambiųjų). Vis daugiau PDAs įrenginiuose laikoma įslaptintų duomenų, tačiau mažiau kaip pusė įmonių naudoja kokias nors saugumo priemones tai informacijai saugoti.

2002 m. tyrimas nustatė, kad tik 2 procentai Jungtinės Karalystės įmonių turėjo bevielį tinklą. Šiuo metu jį jau trečdalis įmonių. Tačiau tik pusė jų savo bevieliams tinklams turi įdiegusios kokias nors saugumo priemones. Tik vienas iš penkių įmonių naudoja laidinio ekvivalento privatumo (WEP) ar kitas papildomas šifravimo funkcijas, saugant savo informaciją nuo nesankcionuoto paviešinimo. Nors stambiosios įmonės labiau suvokia saugumą, bet net ir čia trečdalis bevielių tinklų yra neapsaugoti.

Plečiantis tinklo perimetrui, tradiciniai perimetro saugos modeliai jaučia vis didesnę įtampa, nes, pavyzdžiui, sumaišytos virusų grėsmės vis labiau linkusios atakuoti tinklo saugumo silpnąsias vietas.

29. PASLAUGŲ NUOMA

Vis daugiau Jungtinės Karalystės įmonių kviečia trečiuosius asmenis atlikti jų IT priežiūrą. Šiuo metu tuo naudojai beveik pusė įmonių. Dažniausia tretieji asmenys teikia taikomųjų programų kūrimo ir priežiūros, sistemų ir svetainių administravimo, pagalbos tarnybų paslaugas.

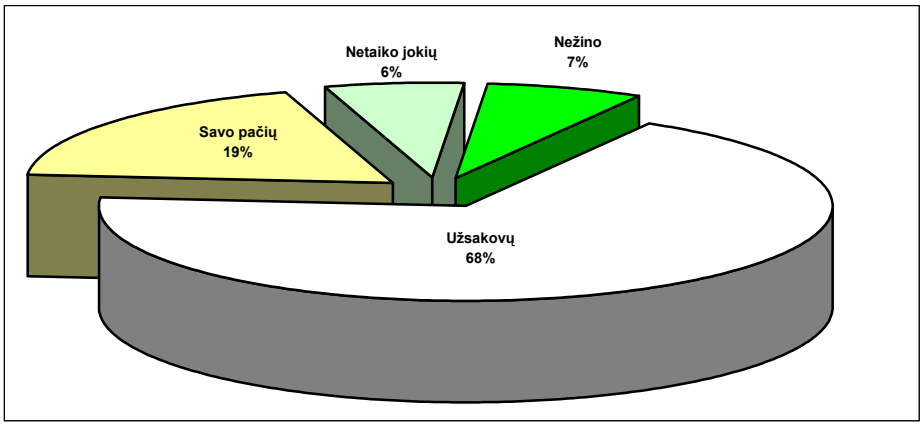
Naudojimosi trečiųjų asmenų paslaugomis laipsnis yra panašus visoms įmonėms, tačiau priežastys dėl ko tai reikia daryti yra skirtingos. Jei smulkesnės įmonės didelį dėmesį kreipia į tokių paslaugų kainą ir paslaugų apimtį, tai stambiosios linkusios atsisakyti veiksmų ir veiklos sričių, kurios nėra įmonės pagrindinė veikla. IT infrastruktūrai darantis vis labiau sudėtingesnei, didėja poreikis turėti labai kvalifikuotą personalą šios IT infrastruktūros priežiūrai, nuolatos kelti jų kvalifikaciją, kas kainuoja labai brangiai ir tuo pačiu skirti didelį dėmesys tos IT infrastruktūros valdymui. Šios sudėtingos problemos sprendimas dažnai matomas kaip IT paslaugų nuoma. Taigi dabar daugelio įmonių saugumas dabar priklauso nuo paslaugos tiekėjų saugumo sistemų.

Du trečdaliai įmonių, kurios IT paslaugoms atlikti kviečia trečiąsias šalis, turi su jomis pasirašiusios priežiūros sutartis (*Service Lavel Agreement - SLA*). Šiose sutartyse paprastai išdėstomi tikslai, kuriuos turi paslaugos tiekėjas pasiekti. Jeigu paslaugos tiekėjas dėl tam tikrų priežasčių neįvykdo sutartyje priimtų įsipareigojimų, įmonė, užsakiusi tas paslaugas, gali pareikalauti sumokėti milžiniškas baudas ir nutraukti sutartį.

Paprastos IT paslaugų sutartys yra nesudėtingos, apibrėžiančios einamąjį priežiūros lygį. Tose sutartyse, kurių paslaugos rezultatas turi būti kainos sumažinimas ar paslaugos pelnas, sutartys yra būti sudėtingesnės, ir jų rengimui pasitelkiami teisininkai ir IT specialistai. Tyrimo metu nustatyta, kad 81 procentas stambiųjų įmonių su paslaugos tiekėjais yra sudariosios tokias priežiūros sutartis. Tai atspindi šių įmonių didelę vidinės kontrolės kultūrą.

Net 90 procentų tokių priežiūros sutarčių išskiriami reikalavimai informacijos saugumui. Tai labai geras rezultatas, nes pirmomis tokių sutarčių pasirašymo dienomis informacijos saugumui nebuvo skiriamo dėmesio. Tačiau stambiosios įmonės tokių sutarčių, kuriose numatyti saugumo reikalavimai, turi tik 71 procentas. To priežastis galėtų būti pačių sutarčių sudėtingumas, siekiant pagrindinių sutarties reikalavimų įgyvendinimo.

Tuo metu kai teikiama paslaugų nuomos paslauga labai svarbu nuspręsti kieno, paslaugos tiekėjo ar paslaugos užsakovo, informacijos saugumo politika ir standartai turi būti taikomi. Dviejuose trečdaliuose paslaugos sutarčių reikalaujama, kad IT paslaugų tiekėjai sutiktų su užsakovo saugumo politika ir standartais (43 pav.).Tai rodo gerą paslaugos tiekėjų lankstumą. Tačiau, didėja reikalavimai ir užsakovams, aiškiai apibūdinant saugumo reikalavimus.



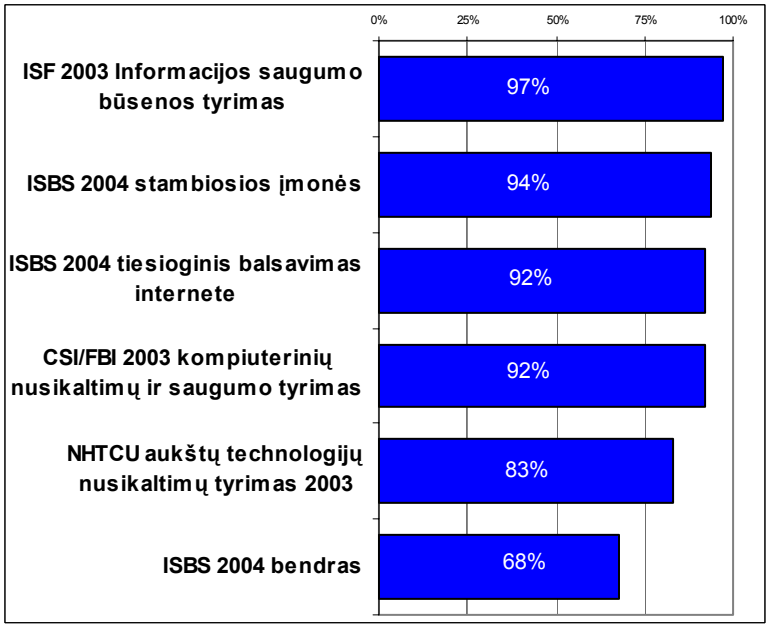
43 pav. Kieno saugumo politiką ir standartus taiko paslaugos tiekėjai?

Tyrimo organizatoriams viena vidutinio dydžio finansinių paslaugų įmonė papasakojo, kad neseniai atliko stropų darbą pas savo paslaugų tiekėją. Apsilankęs paslaugos tiekėjo duomenų centre, IT vadovas buvo labai nustebintas, kad tokia silpna tiekėjo saugumo kontrolė. Jis buvo apstulbintas, kodėl to niekas nepareikalavo anksčiau. Ji primygtinai pareikalavo sugriežtinti saugumo kontrolę numatomoje pasirašyti sutartyje.

Šiuo metu stebima tendencija perkelti IT priežiūros paslaugas į taip vadinamas žemos kainos šalis (Indija, Kinija ir kt.). Labai tikėtina, kad tai padidins griežtesnės saugumo kontrolės poreikį trečiosioms šalims.

30. PALYGINIMAS SU KITAIS ANALOGIŠKAIS TYRIMAIS

Kaip jau buvo minėta šio skyriaus pradžioje, tyrimas ISBS2004 yra didžiausias informacijos saugumo tyrimas Jungtinėje Karalystėje. Todėl labai tikėtina, kad šis tyrimas duoda labiausiai tikslų informacijos saugumo būsenos vaizdą šioje šalyje. Tačiau palyginimas su kitais panašiais vykdomais tyrimais visada yra naudingas gautų rezultatų patikrinimui. Visada kada sulyginami tokie rezultatai, yra svarbu suprasti skirtingų tyrimų traktavimo skirtumus.

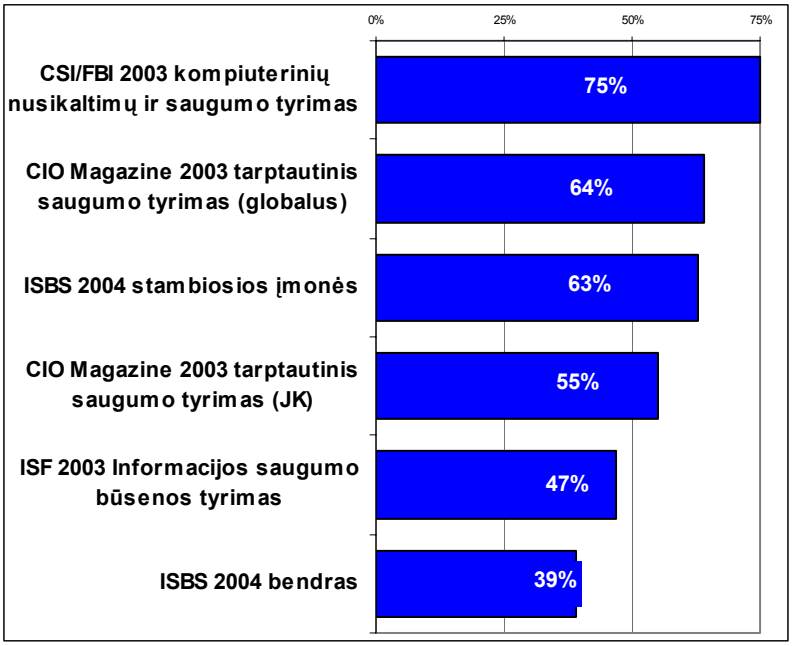


44 pav. Saugumo incidentų lygis palyginant tyrimą ISBS2004 su kitais tyrimais?

Daugelis kitų tyrimų naudoja mažesnes atrankas ir todėl turi didesnes paklaidas. Taip pat gali būti tendencingi stambesnių ir saugumą suprantančių įmonių atžvilgiu. Ir galiausiai, gali skirtis saugumo incidento nustatymas būdas nuo to, kuris buvo naudojamas tyrime ISBS 2004. Šio tyrimo rezultatai lyginami su kitais nesenai atliktais tyrimais.

Tik NHTCU aukštų technologijų nusikaltimų tyrimas buvo atliktas tuo pačiu laiku. Buvo apklausiama 201 įmonė. Pusė šių įmonių turėjo daugiau kaip 1 000 darbuotojų. 83 procentai šio tyrimo respondentų turėjo aukštų technologijų nusikaltimų patirtį. Šis skaičius labai artimas bendram ISBS 2004 tyrimo vidurkiui ir stambiųjų įmonių tyčinių incidentų rezultatui.

Informacijos saugumo forumas (ISF) tai organizacija, galinti surinkti pakankamai duomenų apie informacijos saugumo incidentus iš savo narių, dominuojančių stambiajame versle. Jie savo 2003 m. Informacijos saugumo būsenos tyrime ISF 2003 apklausė 189 respondentus. 97 procentai jų patyrė mažiausiai kaip vieną saugumo incidentą. Tai irgi labai panašu su ISBS 2004 tyrimo rezultatu stambiosioms įmonėms (94 %). ISF 2003 tyrimas taip pat parodė, kad 47 procentai įmonių patyrė mažiausiai kaip vieną rimtą incidentą. Tai irgi atitinka ISBS 2004 tyrimo rezultatams, pagal kuriuos 37 procentai stambiųjų įmonių turėjo patyrusios ypač rimtus incidentus ir 63 procentai įmonių turėjo patyrusios rimtus incidentus.



45 pav. Rimtų saugumo incidentų lygis palyginant tyrimą ISBS2004 su kitais tyrimais?

Jungtinės Karalystės patirties sulyginimas su likusio pasaulio patirtimi taip pat turi tam tikrą vertę. Visų pirma ta patirtis parodo, kad internetas globalizavo saugumo tendencijas.

Vienas iš didžiausių tarptautinių saugumo tyrimų, kurį atliko žurnalas *CIO Magazine* kartu su kompanija *PricewaterhouseCoopers*, 2003 m. balandžio - liepos mėn. Tyrime dalyvavo daugiau kaip septynių tūkstančių organizacijų iš šešių šalių. Penki šimtai organizacijų atstovavo Jungtinei Karalystei. Apie pusė tyrime dalyvavusių organizacijų turėjo daugiau kaip 1000 darbuotojų. Tyrimas apklausė darbuotojus, ar jie patyrė informacijos saugumo pažeidimus, kurie turėjo jų įmonės veiklai neigiamą poveikį. Tai visiškai analogiška ISBS 2004 tyrimo rimtiems incidentams. 64 procentai įmonių globaliu mastu ir 55 procentai įmonių Jungtinėje Karalystėje pranešė mažiausiai apie vieną tokį pažeidimą.

Kitas informacijos saugumo tyrimas, kurį atliko Slaptoji valstybės tarnyba (CSI) ir Federalinis tyrimų biuras (FBI), yra ilgiausia trukęs tyrimas JAV. Tyrimo respondentai buvo tipiški saugumo pareigūnai iš stambiųjų JAV kompanijų. Iš 530 respondentų dalyvavusių

CSI/FBI 2003 tyrime du trečdaliai įmonių turėjo daugiau kaip 500 darbuotojų. 92 procentai įmonių turėjo vienokių ar kitokių saugumo pažeidimų, labai panašiai kaip ir ISBS 2004 tyrime stambiosios įmonės. Trys patys didžiausi pažeidimai buvo virusų infekcija, netinkamas personalo interneto vartojimas ir kompiuterinės įrangos vagystės. Tai taip pat labai atitinka ISBS2004 tyrimo rezultatus. Šiame tyrime net 75 procentai įmonių pripažino po saugumo incidentų patyrusios finansinius nuostolius.