MYKOLO ROMERIO UNIVERSITETAS

SOCIALINĖS INFORMATIKOS FAKULTETAS

ELEKTRONINIO VERSLO KATEDRA

RIMA DAGELYTĖ

Elektroninio verslo vadyba

SAUGOS REIKALAVIMAI VERSLO ĮMONIŲ ELEKTRONINIUOSE ATSISKAITYMUOSE

Magistro baigiamasis darbas

Darbo vadovė –

prof. dr. D. Dzemydienė

Vilnius, 2009

TURINYS

SUTRUMPINIMŲ SĄRAŠAS

SSL - kriptografinis protokolas, skirtas informacijos, sklindančios internete apsaugojimui, šifravimui.

WS-Security - standartų grupė, nurodanti kaip galima užtikrinti interneto paslaugos saugumą.

HTTPS - saugus hiperteksto perdavimo protokolas.

URL – internetinė nuoroda.

SOAP - paprastas kreipties į objektus protokolas.

PKI (angl. Public Key Infrastructure) - techninės sistemos saugus modelis, leidžiantis sukurti elektroninius parašus.

SWIFT-as - organizacinė techninė sistema, yra (arba gali tapti) pagrindinis finansų ir kredito įstaigų perdavimo tinklas.

VAM - tai virtualus autorizacijos modulis.

ISO - tarptautinių standartų organizacija.

X.25 tinklas – skirtas finansinių institucijų duomenims perduoti .

ĮVADAS

Temos aktualumas. Elektroniniai finansiniai atsiskaitymai susiję su kompiuterinės informacijos apdorojimu bei jos perdavimu, o tai gali sukelti didelį asmeninės informacijos pažeidžiamumą bei didesnės galimybės pažeisti informacijos saugumą, pavogti, sunaikinti ar pakeisti duomenis. Kompiuterinės informacijos saugumą gali pažeisti žmonės, aplinkos ir gamtos keliami pavojai. Tačiau didžiausią pavojų kelia žmonės, kurie kompiuterinės informacijos saugumą gali pažeisti tyčia arba dėl neatsargumo. Informacinės technologijos žmonėms, turintiems nusikalstamų tikslų, suteikia išskirtines galimybes. Atsiranda organizuotos kompiuterių nusikaltėlių grupės, kurių nariai – iš viso pasaulio. Beje, kompiuteriniai nusikaltėliai yra pelnę didesnį visuomenės palankumą nei tradiciniai nusikaltėliai. Nuomonė, kad kompiuterinis nusikaltėlis yra mažiau pavojingas, neteisinga. Manoma, kad tikėtinas pavojus bus beveik proporcingas informacinių technologijų privalumams. Todėl specialistai, kurie kuria programas bankams, elektroninėms parduotuvėms ar programas, skirtas naudotis įmonių viduje, visada stengiasi apgalvoti ir panaudoti reikiamus įrankius ir sprendimus, kurie padėtų sukurti saugią programą, norint išsaugoti konfidencialią informaciją ir pinigus.

Tarptautinėje kasmet vykstančioje „E. saugumo ir skaitmeninės ekspertizės“ konferencijoje, Londone[1] 2008 metais buvo įvardinta, kad praktiškai organizuojant nelegalias finansinių resursų panaudojimo operacijas, informacinių technologijų priemonėmis skaitmeniniame pavidale saugomi finansiniai resursai 95% gali būti pažeidžiami. Įžvelgiant tokius saugos pažeidimus Europos Sąjunga teikia priemonių planus ir direktyvas e. atsiskaitymu saugumui užtikrinti (Direktyva 95/46/EC, Direktyva 2002/58/EC ir kt.). Taip pat Europos Sąjungos iniciatyva organizuojamos horizontaliosios ir vertikaliosios priemonės informacinių technologijų saugos reikalavimų vykdymui.

Svarbu ir tai, kad netinkamai apsaugoti pinigų pavedimai internetu kelia grėsmę, kadangi nusikalstamu būdu įgytų pinigų srautai pervedant lėšas gali pakenkti finansinio sektoriaus stabilumui ir reputacijai bei sukelti grėsmę vidaus rinkai[2]. Todėl kasdien vis labiau tobulinami saugumo sprendimai bei saugumo programos leidžiančios saugiai atlikti operacijas ir transakcija naudojant konfidencialius duomenis internete.

Saugos reikalavimų vykdymas šiandien yra aktuali tema visame pasaulyje. Asmenys bei įmonės, siekiančios perduoti svarbią informaciją, daryti perlaidas ar pavedimus naudojant elektroninį banką, siekia apsaugoti savo bei klientų duomenis, kurie gali būti pasiekiami esant saugumo stokai. Taip pat yra siekiama apsaugoti konfidencialius duomenis ir svarbius dokumentus savo vidinėse sistemose, nes didelė dalis nusikalstamumo yra įvykdoma pačių darbuotojų, dėl laisvo priėjimo prie duomenų ir dokumentų esančių įmonės sistemoje.

[1] Annual International Conference: Electronic Security and Digital Foriensics, 2008, London.
[2] Finansinių nusikaltymų tarnyba prie Vidaus Reikalų Ministerijos. Prieiga per internetą: http://www.fntt.lt/lt/99

Siekiant gerinti saugumą e. finansiniuose atsiskaitymuose kuriami nauji ir tobulinami seni saugumo standartai, reikalavimai bei sistemos, kuriose vyksta finansiniai atsiskaitymai internetu. Kasdien plečiantis informacinių technologijų sričiai, esami saugumo sprendimai tampa neefektyvūs. Saugumo sritis tampa neišsemiama dėl dažnai pasirodančių naujųjų technologijų.

Problematika. Lietuvoje kaip ir pasaulyje susiduriama su skaitmeninės saugomos informacijos rizika(pvz. banko kortelių ar slaptos informacijos, kaip slaptažodžių, ar banko kortelių duomenų, nuskaitymais bei duomenų sunaikinimais ir kt.).

Pagrindinės šiuo metu problemos, dėl e. atsiskaitymų:

- ✓ Tretieji asmenys dažnai nelegaliai gauna svarbią informaciją, kuri nėra tinkamai apsaugota (pavyzdžiui 2009 spalio mėnesio incidentas su banko kortelėmis, kai tretieji asmenys pavogė slaptą informaciją ir bankai masiškai privalėjo blokuoti kreditines korteles). Ši problema yra svarbi dėl žmonių pasitikėjimo bankais ir e. atsiskaitymais;
- ✓ Internetiniai įsilaužėliai dažnai bando prieiti prie masinių asmeninių žmonių duomenų, kaip gyvenamosios vietos, paso ir asmens numeriai, taip perduodami juos teroristinėms grupėms, kurios, savo ruožtu, šiuos duomenis gali panaudoti prieš pačius žmones ar net valstybę. Darbe aprašomos technologijos, kurios padeda apsaugoti konfidencialius duomenis nuo įsilaužėlių atakų;
- ✓ Internetinės šiukšlės nesenai taip pat buvo pripažintos kaip internetinis nusikaltimas, kai žmogus kiekvieną dieną gauna reklaminius laiškus ar virusus prieš tai pasisavinus, perimus ar pavogus el. pašto adresą.

Informacijos apsaugojimas nuo virusų bei kitokių piktybinės įrangos grėsmių yra pagrindinis tikslas ir uždavinys el. finansiniuose atsiskaitymuose. Magistriniame darbe aprašomos konkrečios technologijos ir būdai kaip to išvengti bei pateikiamos rekomendacijos remiantis konkrečiais įmonių, naudojančių el. finansinius atsiskaitymus, pavyzdžiais.

Magistrinio darbo objektas yra saugumo reikalavimai e. atsiskaitymuose ir e. finansinių operacijų apsaugos technologijos bei jų efektyvumo tyrimai.

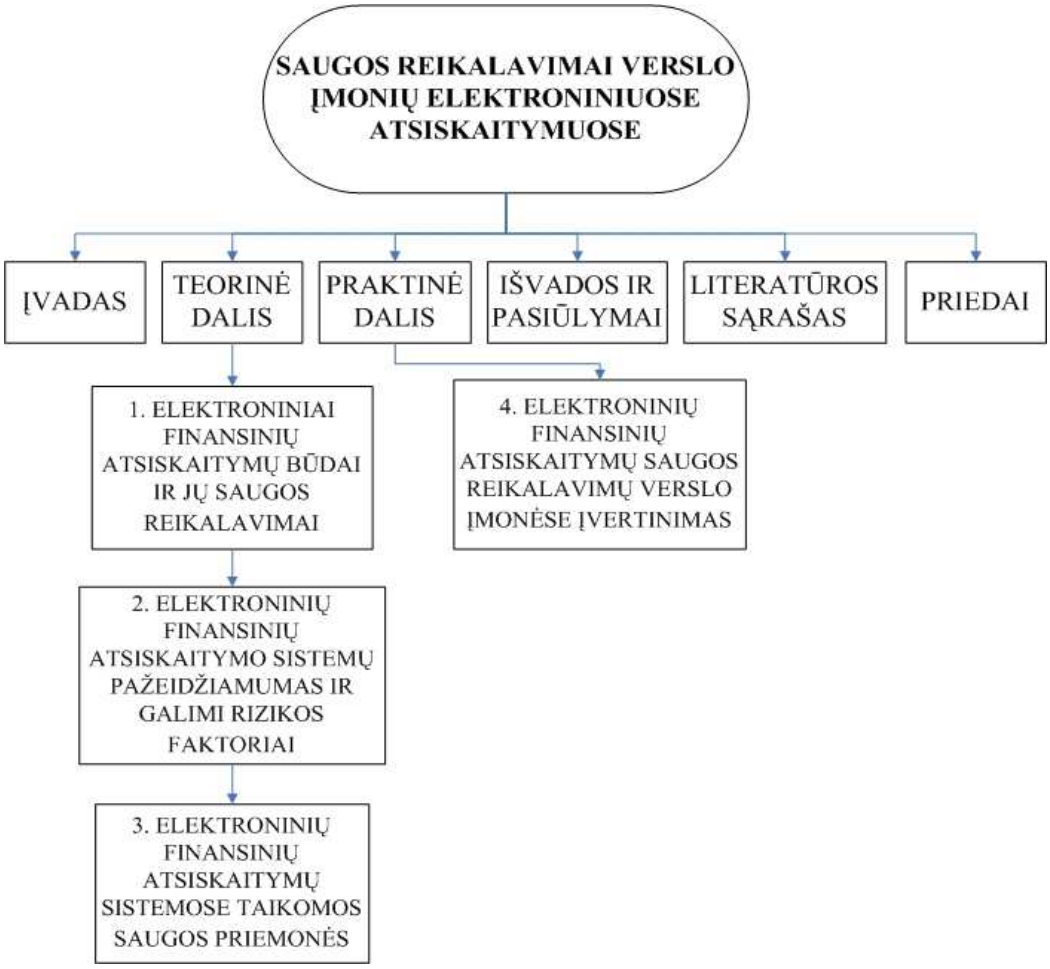
Magistrinio darbo tikslas: elektroninių finansinių atsiskaitymų saugos reikalavimai, galimų rizikų komponenčių vertinimas ir e. finansinių atsiskaitymų saugumo trūkumai verslo įmonių apskaitos procesuose bei rekomendacijos kaip saugiai juos vykdyti.

Šiam tikslui pasiekti keliami magistriniam uždaviniai:

- Išnagrinėti e. finansinių atsiskaitymų saugumo reikalavimus ir vykdymo priemones verslo įmonėse;
- Išanalizuoti galimus finansinių e. atsiskaitymų pažeidimų būdus bei rizikos faktorius;
- Išanalizuoti e. finansinių atsiskaitymų apsaugos priemonių infrastruktūrą (komponentes), jų integruotumą bendroje sistemoje vykdančioje finansinius atsiskaitymus.

- Atlikti eksperimentinį tyrimą, kuris leis įvertinti kompiuterinių saugumo priemonių taikymą ir jų efektyvumą įmonėse diegiančiose ir naudojančiose sistemas, kuriose yra vykdomi e. finansiniai atsiskaitymai, požiūrį į saugumo efektyvumą, lyginant su rizikos galimybėmis ir pateikti siūlymus saugumo didinimui.

Magistrinio darbo struktūra:



1 pav. **Magistrinio darbo pateikimo schema**

Svarbiausia naudota mokslinė literatūra:

- Security for Electronic B2B Transactions, 2003.
- Angelopoulou O. ir kt. O-nline ID theft techniques, investigation and response // International Journal of Electronic Security and Digital Forensics, 2007.
- Commission Staff Working Paper on B2B Internet Trading Platforms: Opportunities and barriers for SMEs – A first assessment.

Taikyti mokslinio darbo tyrimo metodai:

- Literatūros ir mokslinių straipsnių apžvalga bei analizė.
- Interviu ir anketavimo tyrimu pagrįsta statistinė apklausos duomenų analizė.
- Statistinių duomenų, susijusių su e. atsiskaitymų sauga lyginamoji ir koreliacinė (Pearsono) analizė.

1. ELEKTRONINIAI FINANSINIŲ ATSISKAITYMŲ BŪDAI IR JŲ SAUGOS REIKALAVIMAI

Šiame skyriuje bus nagrinėjami e. atsikaitymo būdai, saugos reikalavimai, kurie yra keliami tokiems e. atsiskaitymams. Pagrindinė šių dienų problema yra saugumo trukumas internete perduodant arba gaunant konfidencialius duomenis. Tačiau nauja verslo rūšis, kuri vis populiarėja tarp verslo įmonių ir gyventojų netektų prasmės, jei elektroninės įrangos nebūtų galima panaudoti atliekant sandorio šalių tarpusavio atsiskaitymus.

1.1. Elektroninių finansinių atsiskaitymų būdai

Pastaruoju metu Lietuvoje ir pasaulyje keičiasi žmonių požiūris į atsiskaitymus už prekes bei paslaugas internete. Žmonės vis labiau pasitiki interneto galimybėmis bei jo pagalba atliekamais procesais dėl paprastumo, patogumo bei efektyvumo. Žmogui, kuris naudojasi e. finansinių atsiskaitymų paslaugomis, suteikiamos galimybės atlikti reikalingas operacijas, sandorius, ar pirkimus virtualiai 24 valandas per parą 7 dienas per savaitę, kas suteikia laisvės ir patogumo atlikti procesus namie, naudojant kompiuterį ir internetą.

Pagal randamus šaltinius gali būti apibrėžiami bendriausia prasme elektroniniai atsiskaitymai yra atsiskaitymai , kurie inicijuojami ir apdorojami elektroninių būdu naudojant modernias informacinių technologijų priemones. Pagal J. Šatą (2006), **elektroniniu atsiskaitymu** vadinamas atsilyginimas (mokėjimas) už prekes, paslaugas ar darbus, atliekamus elektroninėmis mokėjimo priemonėmis.

Kitaip nei atsiskaitymams tradicinėje komercijoje, pasak J. Šato (2006), elektroninėje komercijoje būtina specifinė, susidedanti iš keturių pagrindinių dalių, infrastruktūra:

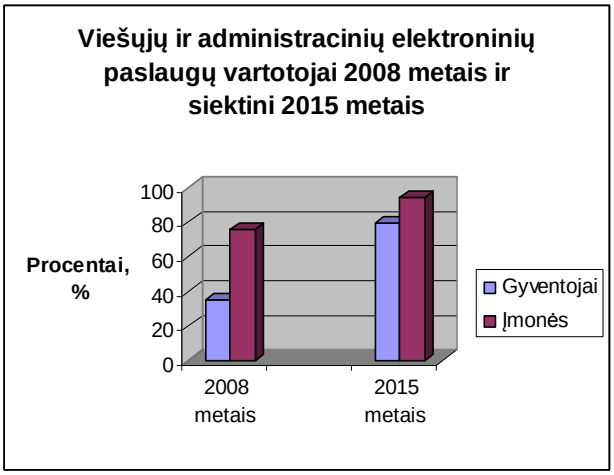
- tinklo paslaugų (nuolatinės prieigos prie interneto) teikiančios dalies;
- techninės įrangos (asmeninio kompiuterio, serverio ir kt.);
- programinės įrangos (elektroninio verslo sprendimo ir kt.);
- atsiskaitymo paslaugas (elektroninio mokėjimo, jo autentiškumo užtikrinimo, sertifikavimo, tinklo diagnostikos ir kt.) teikiančios dalies.

Atsiskaityti už prekes ar paslaugas galima įvairiai. Taigi yra išskiriamos alternatyvios atsiskaitymo sistemos, kurios skirstomos į pagrindines tris grupes pagal Šatą (2006):

- Sąskaitos valdymas per internetą;
- Elektroninių pinigų naudojimas, atsiskaitant su parduotuvėmis, kitais paslaugų tiekėjais;
- Atsiskaitymas grynaisiais už pristatytas prekes ir suteiktas paslaugas.

Šiuo metu vis populiaresnė tampa e. mokėjimų sistema ir vis daugiau šalies gyventojų ir įmonių pradeda naudotis tokiomis paslaugomis. Pagal Lietuvos informacinės visuomenės plėtros 2009-2015 metų strategiją galima pastebėti būsimą ir esamą gyventojų ir įmonių naudojimą viešųjų ir administracinių e. paslaugų augimą 2008 metais ir 2015 metais[3], kuris paspartins ir e. atsiskaitymų plėtrą.

Pagal pateiktus duomenis (žr. 2 pav), nuo 2008 metų iki 2015 naudojimasis vešiosiomis ir administracinėmis e.paslaugomis turėtų išaugti gyventojams 40%, o įmonėms 15%.



Šaltinis. Sudaryta pagal Lietuvos Respublikos Vyriausybes nutarimą (2008 m.).

2 pav. Viešųjų ir administracinių elektroninių paslaugų vartojimo pokytis darantis įtaką e. atsiskaitymams

Pagal informacijos slaptumo užtikrinimo lygį reikalinga skirtingas informacinių technologijų apsaugos lygis. Sodžiūtės ir Sūdžiaus darbe (2003) nagrinėjami yra daugiau tradiciniai būdai, kuriais žmonės, atliekantys finansinius e. atsiskaitymus, gali naudotis taikydami e. mokėjimų būdus:

- ✓ banko mokomasias korteles;
- ✓ elektroninius čekius;
- ✓ skaitmeninius pinigus;
- ✓ elektroninius pinigus.

Banko mokomoji kortelė – elektroninės formos atsiskaitymų pinigais dokumentas, kurį išleidžiantis bankas (ar kita kredito įstaiga) patvirtina, kad tame banke (ar kitoje kredito įstaigoje) atidarytoje kortelės turėtojui sąskaitoje, neviršijant joje esančios sumos (arba suteikto kredito limitų), gali būti atliekami atsiskaitymai. Tai savotiška elektroninė piniginė, raktas į kliento sąskaitą, galimybė atsiskaityti negrynais pinigais. Kartu ji yra ir viena iš sąskaitos valdymo priemonių, užtikrinanti saugų ir greitą atsiskaitymą. Mokėjimo kortelė naudojama atsiskaitant tiesiogiai nebendraujant su kredito įstaiga. Ji turėtojui leidžia patogiau, saugiau, be didelių laiko sąnaudų pasinaudoti banke laikomomis

[3] Lietuvos informacinės visuomenės plėtros 2009-2015 metų strategija. Lietuvos Respublikos Vyriausybes nutarimas (2008 m.).

lėšomis. Bet kuriuo paros metu kortelės turėtojas per bankomatą (automatinį grynųjų pinigų išėmimo įrenginį) gali nusiimti nuo savo sąskaitos reikiamą pinigų sumą arba sumokėti už prekes ar paslaugas negrynaisiais pinigais (Šatas, 2006).

Naudojantis banko mokomosiomis kortelėmis visada iškyla pavojus prarasti pinigus, nors yra teigiama, kad tai yra patikimas būdas. Šiuo metu dominuoja tokie apgavysčių būdai, kaip suklastota kortelė (tai yra nelegaliai pagaminta kortelė ir reljefiniu būdu atspausta, kartais elektroniniu būdu vogta užkoduota magnetine kortele. Tokias korteles, kurias spausdina reljefiniu būdu išlygina arba išpjauna, ar išspaudžia su skylamušiu, ir spaudžia naujas korteles), vagystėmis, pvz. iš automobilių (vagiamos kortelės ir naudojamos), „nuėmimas“ (tai nusikaltėlių padirbinėjimo būdas, kai yra nukopijuojama informacija, kuri sukaupta elektroniniuose takeliuose. Tokie nusikaltimai dažniausiai vyksta pardavėjo vietose, kai atliekamas sandoris ir jo metu visi duomenys yra nukopijuojami). Taip pat nusikaltimai yra vykdomi tada, kai duomenys iš pardavėjo yra išsiunčiami su autorizacijos suteikimu į kita vietą. Tokia informacija gaunama slapta prisijungus prie ryšiui naudojamos telefono linijos arba fiksuojant iš žemės palydovo siunčiamas oro bangas (Štilis, Laurinaitis, 2008).

Elektroniniai čekiai – tai dokumentas, kuriame mokėtojas nurodo savo bankui apie pinigų pervedimą. E. atsiskaitymo čekis turi tas pačias savybes kaip ir paprastas popierinis atsiskaitymo čekis: jų struktūra ir naudojimo ypatumai tokie pat. Mokėtojas parengia čekį ir apsaugo elektroniniu parašu. Pateikia čekį e.paštu pardavėjui, kuris yra piniginio mokėjimo gavėjas. Pardavėjas, savo ruožtu, gavęs čekį, jį pasirašo ir persiunčia savo bankui, pagal kurį gauna pinigus. Po to čekis grįžta pirkėjui ir yra apmokėjimo įrodymas. Pardavėjas pristato prekę pirkėjui į namus (Sodžiūtė ir kt., 2003).

Tokie pinigų perdavimai yra taip pat nevisapusiškai apsaugoti, nes duomenys yra perduodami per internetą, o tai reiškia, kad visada yra galimybė prarasti pinigus. Todėl tokių siunčiamų duomenų kodavimas yra būtinas, kad kas nors gavęs informaciją, negalėtų jos nutekinti.

Skaitmeniniai pinigai – popierinių grynųjų pinigų analogas. Jie turi piniginių ženklų pavidalą. Skaitmeniniai pinigai – tai kuponų komplektas. Kuponai – tai skaičių grandinės, vaizduojančios atitinkamą pinigų kiekį. Bankas, kuris išleido šiuos kuponus, kiekvieną kuponą patvirtina skaitmeniniu parašu. Prieš perduodant kuponą į pinigų gavėjo kompiuterį, bankas patvirtina jį savo skaitmeniniu antspaudu. Tuo atveju, kaip prekės pirkėjas norės išleisti parduotuvėje tam tikrą skaitmeninių pinigų kiekį, jis tik perduoda pardavėjui reikiamą kuponų kiekį. Pardavėjas perduoda šiuos kuponus bankui patikrinti. Kiekvienas kuponas gali būti panaudotas tik vieną kartą. Kad kuponas nebūtų panaudotas keletą kartų, bankas užsirašo kiekvieno išleisto kupono numerį. Jeigu pasirodys, kad kuponas jau buvo panaudotas ir yra įrašytas duomenų bazėje, tai reiškia, kad kuponą bando panaudoti dar kartą. Bankas iš karto informuoja pardavėją apie kupono negaliojimą. Skaitmeninių pinigų technologija labiausiai tinka nedidelių sumų mokėjimams realaus laiko režimu per internetą. Ir šie mokėjimai dažniausiai susiduria su informacijos perdavimu ir galimu pasikėsinimu.

Elektroniniai pinigai – tai piniginių lėšų pervedimas iš vienos sąskaitos į kitą, procentų apskaičiavimas nuo įnašų ir kiti elektroninių signalų perdavimai be popierinių nešiotojų dalyvavimo. E.pinigais naudojasi bankai, stambios įmonės, kurios turi galimybę gauti leidimą pervesti mokėtojo pinigines lėšas ir susitarti dėl apmokėjimo sąlygų su pinigų gavėju. Pinigų pervedimas tarp bankų atliekamas naudojant paprastus bankų tinklus (Sodžiūtė, Sūdžius, 2003).

Šiandien e. pinigais naudojasi beveik visi, tačiau vis dar yra trūkumų, kurie įtakoja ir e. atsiskaitymų saugumą:

- Nepakankamas saugumo lygis;
- Mažas transakcijų atlikimo greitis (lyginant su paprastos informacijos perdavimu internetu). Jei transakcija vyksta tame pačiame banke ji užtrunka nuo 5 iki 30 minučių, jei pervedimas yra į kita banką, tai gali užtrukti net kelias paras, o jei reikia skubaus pervedimo, tai reikia mokėti papildomai;
- Anonimiškumo ir privatumo nebūvimas. Jei klientas atidaro sąskaitą banke, jam tenka pilnai identifikuoti savo duomenis, kas kartais gali tapti pavojinga, jei ši informacija kur nors nutekėtų;
- Sudėtingumas. Siekiant bankinių atsiskaitymų saugumo imtasi papildomų priemonių, tokių, kaip ribojami kliento veiksmai. Apribojimai atliekami tam tikroms operacijoms, naudojamos sudėtingos atpažinimo sistemos;
- Didelė transakcijų savikaina.
- Neįmanomas nenuostolingų mažų mokėjimų atlikimas. Norint atlikti mažą mokėjimą, tokia paslauga gali būti, kad kainuos daugiau nei pati paslauga (Laurinaitis, 2007).

Aukščiau išvardinti dalykai turi būti tobulinami, kad sumažinti riziką prarasti pinigus, ar kitą jautrią asmeninę informaciją.

1.2. Elektroninių finansinių atsiskaitymų sistemos saugos reikalavimų samprata

Informacijos apdorojimas kompiuterinėse sistemose susijęs su informacijos bei programinių priemonių pažeidžiamumu, galimybėmis įsiveržti per tinklų sistemas į saugomas duomenų bazes ir informacines sistemas. Dažniausiai taikomasi pavogti, sunaikinti ar pakeisti duomenis. Kadangi duomenų ir informacijos pažeidžiamumas yra vienas iš svarbiausių komponentų informacinėse sistemose, be to apsaugos priemonės turi nemažai intelektualioms sistemos būdingų bruožų. Kompiuterinės informacijos pažeidžiamumą lemia kai kurie faktoriai bei pačios skaitmeniniu būdu apdorojamos informacijos savybės, pagal D. Dzemydienės (2006), yra:

- Tinklų prieinamumas - kuo didesnį vartotojų ratą ir teritoriją apima kompiuteriniai tinklai, tuo labiau jie yra pažeidžiami, kadangi prisijungimas galimas daugelyje vietų ir neįmanoma kontroliuoti vartotojų vykdomus veiksmus.
- Informacijos ir procesų tankumas bei koncentruotumas (šiuolaikinės informacinės technologijos leidžia išsaugoti didelius duomenų kiekius ir per mažą laiko tarpą pasiųsti juos dideliais atstumais). Atsiranda galimybės per trumpą laiko tarpą, esant dideliu atstumu nuo kėsinimosi objekto, perimti duomenis, juos sugadinti ar persiųsti.
- Šiuolaikinių kompiuterinių tinklų sudėtingumas. Šiuolaikiniuose kompiuteriniuose tinkluose operacijų skaičius bei duomenų apdorojimo būdai bei lygiai artėja prie neapibrėžtumo, dažnai, net patys šių tinklų įkūrėjai gali nesuprasti kai kurių dalykų. Tuo naudojasi nusikaltėliai, pasinaudodami įvairiomis programinės įrangos ar apsauginių programų klaidomis, bei mažai žinomomis kompiuterinių tinklų programinės įrangos silpnybėmis.
- Elektroninis pažeidžiamumas susijęs su galimybe informaciją paveikti, kaip ir kitus elektroninius prietaisus, elektromagnetinių bangų, elektromagnetinės radiacijos ir kitomis technologijomis. Toks poveikis gali silpninti apsaugos programas ir gali sudaryti sąlygas priėjimui prie duomenų.
- Elektroninių duomenų apdorojimo proceso priemonių pažeidžiamumas. Dėl elektroninių duomenų apdorojimo proceso nematomumo, personalas dirbantis su duomenų failų persiuntimu, dažnai, nežino šių duomenų turinio. Fiziniai bei programiniai netikslumai gali sąlygoti apsauginių programų susilpnėjimą bei su tuo susijusį duomenų nutekėjimą.

Todėl vykdomas saugumas e. finansinių atsiskaitymų sistemose, naudojant kompiuterines technologines saugos preimones, kurios palaiko saugos reikalavimus, yra užtikrinama žmonių ir verslo įmonių informacijos konfidencialumą ir apsaugą nuo vagysčių bei svarbių duomenų paviešinimo.

Saugumą palaikančios sistemos skirtos e. finansiniams atsiskaitymams turi būti kuriamos laikantis saugumo reikalavimų bei standartų, visada atnaujinamos bei tobulinamos, nes atsiranda vis nauja pažeidžiamumo rizika. Toliau bus aprašomas saugumas įmonių viduje, kurios verčiasi elektronine prekyba ir naudoja e. finansines sistemas. Taip pat apžvelgsime saugumo sampratą pačių e. finansinių atsiskaitymų sistemose.

1.2.1. Informacijos saugumo samprata verslo įmonės viduje bei finansinių atsiskaitymų sistemoje

Asmeninius vartotojų duomenis ar verslo įmonės slaptus duomenis gali paviešinti ar pasinaudoti patys įmonės darbuotojai. Visos didžiosios valstybinės įstaigos, piliečių ir įmonių duomenų turėtojos, jau yra apsaugojusios savo elektronines laikmenas nuo savų informacijos potencialių vagysčių. Visa, kas daroma e.sistemoje, fiksuoja esamos informacinės technologijos. Bet kada galima pažiūrėti koks darbuotojas kada kokius duomenis žiūrėjo ar kopijavo. Bet kokių įstaigų turimus duomenis jų administratoriai gali panaudoti piktam tik tuo atveju, jeigu jie nėra reikiamai apsaugoti ir nėra patvirtinto darbo su turima informacija reglamento. Be to, įstaigose turi būti ne vienas e.sistemos administratorius, galintis daryti tam tikrus pakeitimus, nes jie gali būti maskuojantys neleistinus žingsnius sistemoje. Ar visi darbuotojai, turintys galimybę prieiti prie duomenų sistemos, elgiasi pagal reglamentą, turėtų tikrinti šiam tikslui sukurtas vidinis auditas. Įmonės – didžiųjų registrų tvarkytojos, tokias audito sistemas turi. Kas darosi mažose – informacijos nėra, nes nėra kokios nors specializuotos, visas įmones audituojančios organizacijos[4].

Saugumas e. finansinių atsiskaitymų sistemose yra svarbus, nes tik nuo jo priklauso sėkmingų finansinių operacijų atlikimas bei konfidencialių duomenų apsaugojimas.

E. finansinių atsiskaitymų sistemos visų pirma turi palaikyti saugumo reikalavimus tokius kaip: autentiškumo patvirtinimas, autorizacija, auditas, konfidencialumas, privatumas, vientisumas, prieinamumas, minimalios privilegijos, paprastumas, nuodugni apsauga, naudoti internetinius standartus, registruoti audito įrašus. Sistemai palaikyti tokius saugumo reikalavimus reikalingi techniniai apsaugos mechanizmai tokie kaip: ugniasienės, kurios, pasak internetinio portalo www.elektronika.lt, yra labiausiai paplitęs būdas į savo kompiuterį įsileisti tik tai, ką vartotojas pats pasirenka. Tai yra programa, kuri apsaugo nuo nepageidaujamų svečių bei blokuoja įtartinų failų įėjimą bei išėjimą. Jeigu ugniasienė yra naudojama kartu su antivirusine programa, tuomet interneto grėsmių nėra ko baimintis, nes naudojama geriausia apsaugos kombinacija. Taip pat saugumo reikalavimo palaikymui yra būtini saugumo standartai kaip HTTPS (saugus hiperteksto perdavimo

[4] Išmokime apsaugoti elektroninę erdvę. Lietuvos Respublikos Vidaus Reikalų Ministerijos straipsnis, 2009. Prieiga per internetą http://www.vrm.lt/index.php?backPID=129&id=602 .

protokolas), SSL (kriptografinis protokolas, skirtas informacijos, sklindančios internete apsaugojimui šifruojant), WS-Security (standartų grupė, nurodanti kaip galima užtikrinti interneto serviso saugumą) ir kt. Taip pat, saugumo užtikrinimui, reikia, kad sistemoje būtų įdiegtas mechanizmas, kuris sektų ar fiksuotų asmenis ir jų veiksmus, kurie prisijungia prie sistemos. Tam gali būti panaudoti įvairūs sistemos audito moduliai.

1.2.2 Europos Sąjungos direktyvos duomenų privatumo ir tinklo informacijos saugumui užtikrinti

Paskutiniu metu labiausiai išsivysčiusios pasaulio šalys daug dėmesio skiria „jautrios“ informacijos saugumui. Tokios informacijos kategorijai priskirtini: žmonių bei įmonių duomenys susiję su finansinių atsiskaitymų operacijomis. ES direktyvos ir reglamentai apibrėžiantys tokios informacijos saugumo kriterijus ir standartus tampa svarbiais dokumentais visoms ES šalims narėms. Jais remiantis, kiekviena įmonė privalo įdiegti atitinkamas naujausias saugumo technologijas atitinkančias reglamentuose ir direktyvose aprašomus standartus bei nurodymus.

Šiuo metu naujausios išleistos Europos Sąjungos institucijų saugumo direktyvos[5] yra šios:

- 9.1 Regulation (EC) 300/2008 – Europos Parlamento ir Tarybos reglamentas dėl pagrindinių taisyklių civilinės aviacijos saugumo sferoje.
- 9.2 Direktyva 95/46/EC – Individų saugumas apdorojant jų asmeninius duomenis ir jų laisvame judėjime.
- 9.3 Direktyva 2002/58/EC – Asmeninių duomenų apdorojimas ir privatumo apsauga elektroninėje komunikacijos sferoje. (Privatumo ir elektroninio komunikavimo direktyva).
- 9.4 COM(2007) 251: Privatumą apsaugančių technologijų duomenų apsaugos populiarinimas (PETs)

Remiantis šiomis ir kitomis direktyvomis ir reglamentais ir yra kuriamos naujos saugumo technologijos užtikrinančios asmens duomenų apsaugą ir el. finansinių atsiskaitymo srityje.

Europos Standartų Organizacijos (ESOs) yra pakviestos pratęsti duomenų saugos standartizavimą pagal 95/46/EC direktyvą skaitant Mandate M/289 standartizacijos ataskaitą. ESOs taip pat pakviestos atkreipti dėmesį į kitų standartizavimo institucijų atliktus darbus kaip ISO/IEC JTC1/SC27, tai yra saugus indentitetų valdymas, identifikavimo procesai ir pan.

[5] European Commission: 2009 ICT Standardisation Work Programme

ESOs taip pat pakviestos atlikti kodavimo technologijų standartizaciją, atkreipiant dėmesį į kompiuterinių sistemų skaičiavimo vykdymo programavimą ir ateities prieinamumą prie plačių kompiuterinių resursų užtikrinančių asmens privatumą per GRID platformas.

ESOs dėmesys labiausiai turi būti sutelktas į ISO standartus juos tobulinant ir peržiūrint ypatingą dėmesį kreipiant į tuos, kuriuos labiausiai įtakotų būtent pridėtas Europos indėlis, kaip ISO/IEC Informacijos Apsaugos technikos – praktikos kodas nurodantis informacijos saugumo valdymą darant saugumo taisyklių kūrimą ir implementavimą.

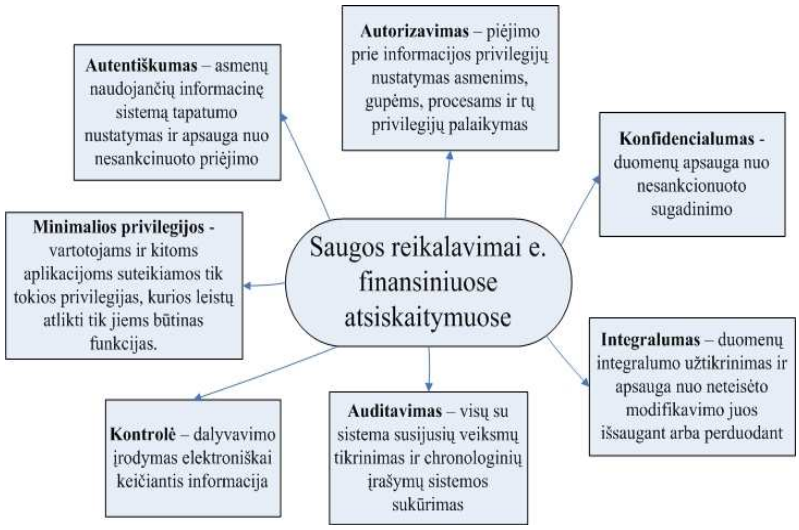
1.3. Saugos reikalavimai naudojami elektroniniuose finansiniuose atsiskaitymuose

Atliekant finansinius atsiskaitymus elektroninėje erdvėje yra keliami reikalavimai, kurie užtikrina mokančiojo asmens asmeninės informacijos neliečiamumą. Reikalavimai skirti apsaugoti duomenis ir identifikuoti žmogų, kuris jungiasi prie sistemos, kad atliktų e. atsiskaitymą. Galima išskirti tokius reikalavimus:

- Autentiškumo patvirtinimas. Šio reikalavimo pagrindas yra į įmonių sistemas integruojami komponentai, kurie identifikuoja prisijungusią sistemą arba asmenį. Tokiu būdu sistema yra apsaugoma nuo pašalinių žmonių ar kitų sistemų blogo poveikio. Autentiškumo komponentai kiekvienoje sistemoje yra skirtingi, tai priklauso nuo įmonės paslaugų pobūdžio. Vienoms įmonėms užtenka identifikuoti vartotoją, jam įvedant prisijungimo vardą bei slaptažodį. Kitose įmonėse, kurioms reikia apsikeisti svarbiais duomenimis yra naudojama kriptografija, kad užšifruoti siunčiamus duomenis ir jie būtų apsaugoti, bei nepasiekiami pašaliniams asmenims.
- Autorizacija. Autorizacija identifikuoja ką prisijungusi sistema ar vartotojas gali daryti e.sistemoje. Yra trys savybės pagal kurias nustatoma prie kokių duomenų yra prileidžiamas identifikuotas vartotojas ar sistema:
    a. kas tu esi (anonimas ar identifikuotas vartotojas) ir kokia tavo rolė sistemoje.
    b. kokius sistemos duomenis ar informaciją norima matyti, keisti, naudoti.
    c. kokius veiksmus bandai atlikti.
- Auditas. Auditas yra reikalingas tam, kad būtų sekama ir įrašoma į sistemą, kas buvo atlikta ir kokiu metu. Tokie įrašai leidžia sistemos administratoriui sekti ką koks vartotojas atliko ir, jei buvo nelegalių veiksmų, imtis saugumo priemonių.
- Konfidencialumas. Konfidencialumas yra sistemų ir tinklų apsauga, kuri neleidžia neautorizuotiems asmenims prieiti prie sistemos, taip pat vartotojas gali būti tikras, kad jo duomenų saugumas bus išsaugomas. Privatumas yra taip pat dalis konfidencialumo. Duomenų saugojimas privačiai yra būtinybė tokiam konfidencialumo reikalavimui.

- Privatumas. Privatumas susijęs su neviešų, privačių duomenų individualumu ir šie duomenys negali būti paversti viešais, neturint individualios autorizacijos sistemoje.
- Vientisumas. Vientisumas yra visapusiška apsauga informacinėje sistemoje nuo tyčinio ar atsitiktinio informacijos pakeitimo.
- Prieinamumas. Prieinamumas yra garantas, kad kompiuterinė sistema yra prieinama autorizuotiems asmenims tada, kai tik jiems prireikia.
- Minimalios privilegijos. Suteikti vartotojams ir kitoms aplikacijoms kuo mažiau privilegijų. Suteikti tik tokias privilegijas, kurios leistų atlikti tik jiems būtinas funkcijas.
- Paprastumas. Sistemai keliamas reikalavimas paprastumas, nes sunkumas yra saugumo priešas. Sudėtingos sistemos yra sunkios formuoti bei patikrinti.
- Nuodugni apsauga. Niekada nepasitikima tik vienu saugumo mechanizmu.
- Naudoti internetinius standartus. Kada tik įmanoma naudoti standartinius protokolus, technologijas, algoritmus bei duomenų formatus. Geriausias būdas įsitikinti, kad vartotojo sąsaja (angl. interface) yra saugūs, tai panaudoti žinomas ir gerai išbandytas technologijas ir duomenų formatus.
- Registruoti audito įrašus. Kiekviena organizacija turėtų įrašyti saugomų įvykių audito įrašus, kad atsekti kas, ką ir kada kiekvienai B2B (t.y. verslas verslui) transakcijai. Tikrinimas yra kritiškas saugumo komponentas, kuris yra dažnai pražiūrimas.

Apibendrinant saugumo reikalavimus pateikiama pagrindinių saugos reikalavimų diagrama (žr. 3 pav.), kuroje yra įvardijama autentiškumas, autorizavimas, konfidencialumas, minimalios privilegijos, integralumas, kontrolė ir auditavimas. Čia yra patys svarbiausi saugumo reikalavimai, tačiau kiti nepateikti shemoje taip pat yra labai svarbus. Be šių saugos reikalavimų, nebūtų galimybės visiškai apsaugoti savo duomenų naudojant kompiuterines technologijas.



Šaltinis. Sudaryta autorės.

3 pav. **Pagrindiniai saugos reikalavimai**

2. ELEKTRONINIŲ FINANSINIŲ ATSISKAITYMO SISTEMŲ PAŽEIDŽIAMUMAS IR GALIMI RIZIKOS FAKTORIAI

Saugumo priemonių imtasi, kad būtų saugomos sistemos nuo kenkėjiškų programų ar žmonių, kurie pradėjo gadinti vienokiu ar kitokiu būdu įmonių finansines bei kitas sistemas, vogti, savintis konfidencialią informaciją bei, naudodamiesi vogtais duomenimis, siekti asmeninės naudos. Tokie kėsinimosi būdai į programinę įrangą ar duomenis, įveikiant technines apsaugos priemones bei duomenų apdorojimo procedūras, gali būti klasifikuojami pagal kėsinimosi objektą:

- ✓ Pasikėsinimas į programinę įrangą (angl. Software attacks) - tai programinės įrangos pakeitimai, modifikavimas, nelegalus panaudojimas.
- ✓ Pasikėsinimai į duomenis (angl. Data attacks) apima pažeidimus, susijusius su duomenų, esančių valstybine, komercine firmos ar asmens paslaptimi, panaudojimą ar nuskaitymą.

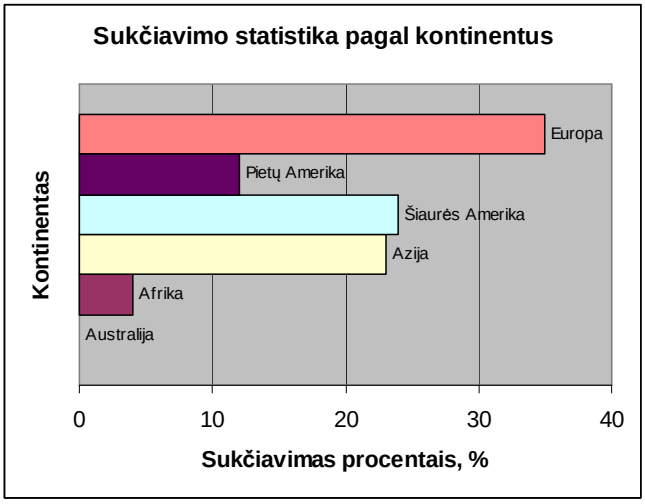
Nusikaltėliai kuria vis naujas strategijas, kaip įsilaužti į sistemas ir kokiais būdais tai būtų galima padaryti. Galima išvardinti keletą iš daugelio įsibrovimų į kompiuterinę sistemą metodų:

- Slaptažodžių nužiūrėjimas;
- Slaptažodžio parinkimas naudojant labiausiai paplitusių slaptažodžių sąrašus arba žinias apie konkrečius asmenis;
- Specialių programų įterpimas į kompiuterines sistemas, kurios “sugauna” įvedamą kodą;
- Kodo parinkimo programų panaudojimas;
- Vidinės dokumentacijos kurioje kalbama apie sistemos apsaugą analizė;
- Pirminių tekstų ir dvejetainių kodų programų registracijos ir apsaugos analizavimas ir klaidų jose ieškojimas ir tokių programų pakeitimas savomis;
- Specialių aparatinių priemonių naudojimas, kad perimti pranešimus lokaliuose tinkluose;
- Kompiuterinių virusų kūrimas ir t.t.

Šiame skyriuje ir bus apžvelgiama, kokiais įrankiais įgyvendinami nusikaltimai, kaip pasikėsinimas į programinę įranga ar kompiuterines sistemas, ar pasikėsinimas į konfidencialius duomenis ir pan.

2.1. Sukčiavimo galimybės ir įtaka elektroniniams finansiniams atsiskaitymams

Sukčiavimas (angl. Phishing) - taip apgaulingas procesas, kuris padeda gauti nelegalią informaciją, kaip vartotojo vardai, slaptažodžiai ir kreditinės kortelės duomenys, dar įvardijamas, kaip „**žuviavimas**“. Tokia informacija gaunama siunčiant elektroninius laiškus, kurie tarsi ateina iš patikimų organizacijų. Gauti laiškai nekelia nepasitikėjimo, nes laiškai tarsi gaunami iš bankų, draudimo agentūrų ir kreditinės kortelės kompanijų, tačiau ne visada tokia informacija yra tikra. Žinutės atrodo autentiškos naudojant kompanijos emblemas, ir apipavidalinamos panašiai kaip ir oficialioje kompanijoje, kurią bandoma pamėgdžioti. Gaunant tokį laišką kyla grėsmė, nes tokiuose laiškuose yra prašoma asmeninių duomenų, tokių kaip slaptažodžiai, sąskaitos numeriai ir kita privati informacija, kuri tarsi reikalinga patikrinimui. Taip žmonės yra apgaunami ir tuo pasinaudoję kompiuteriniai nusikaltėliai siekia sau naudos, taip pat nutinka ir tokių atvejų, kai elektroninėje erdvėje veikiantys nusikaltėliai siunčia elektroninius laiškus, taip “žvejodami” sau pagalbininkus pinigų “plovimui” ir interneto apgavystėms vykdyti. Jie pažada dalį apgavystės keliu įgyjamų pajamų ir iš tikrųjų nedelsiant sumoka(Angelopoulou O. ir kt, 2007). Tai dažnas sukčiavimo būdas, kuris paplitęs po visa pasaulį. Pagal „Marshal8e6“ svetainės atliktus tyrimus galime matyti koks pasiskirstymas yra išsidėstęs visame pasaulyje ir matome iš paveikslo numeris 2, kad mūsų žemyne, Europoje, toks sukčiavimo būdas yra labiausiai paplitęs, Todėl ir kovoti su šiuo nusikalstamu sukčiavimu reikia sutelkti visas įmanomas priemones.



Šaltinis. Statistiniai duomenys, pateikti internetinėje svetainėje www.marshal8e6.com .

4 pav. **Sukčiavimo statistika pagal pasaulio kontinentus**

Yra išskiriami keli kovojimo būdai su tokiu sukčiavimu bei sistemų klonavimu (angl. Web-spoofing). Tam, kad apsisaugoti, pasak, Neil Chou ir kt., reikia atlikti tokius tikrinimus prieš jungiantis prie sistemų ar pateikiant tam tikrus jautrius duomenis:

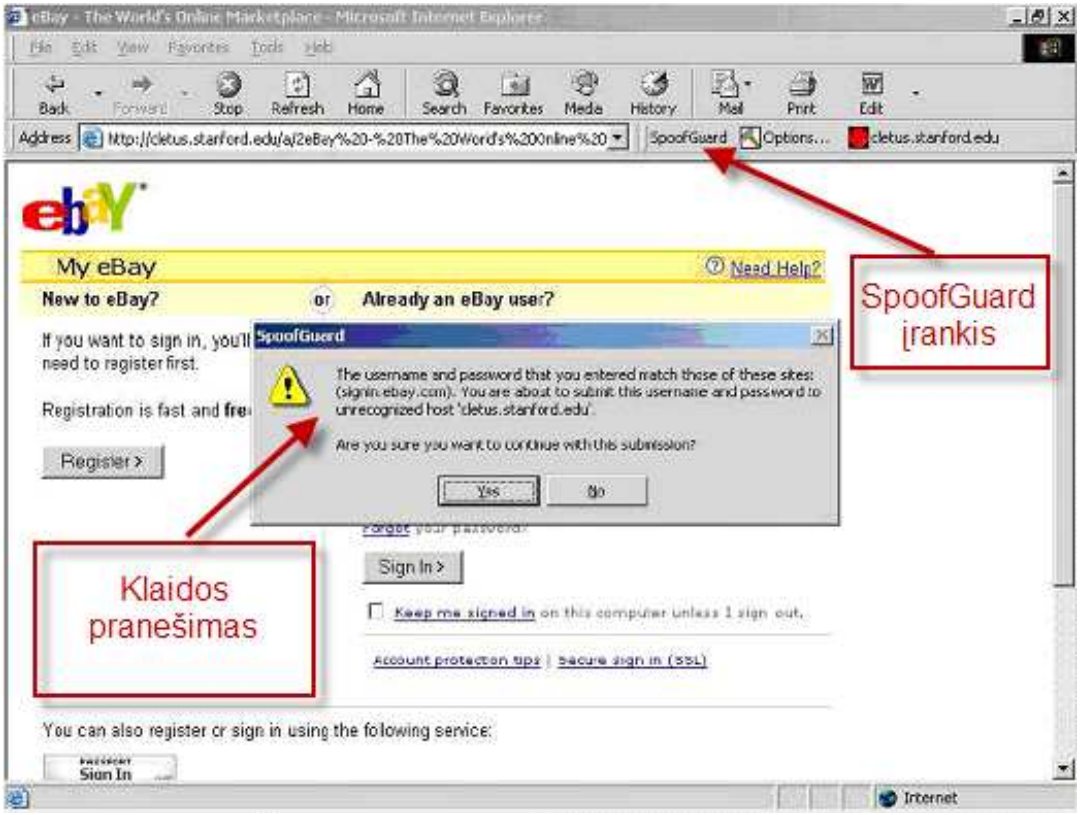
- URL adreso tikrinimas. Reikia gavus laišką ar nuorodą būtinai atkreipti dėmesį į gauto laiško ar nuorodos URL adresą, nes kyla grėsmė, kad yra atidaroma sukčiautojų sukurtas dokumentas, per kurį jie gaus svarbius asmens duomenis ir jais pasinaudos siekiant asmeninės naudos.
- Puslapio, laiško tikrinimas. Dažnai tokiuose puslapiuose, ar laiškuose būna įdėti paveikslėliai, kurie yra kopijuoti iš tikrųjų puslapių ar laiškų. Todėl žmogus turi būti atidus ir stebėti prieš jungdamasis, ar skelbdamas svarbią savo informaciją bei duomenis.
- Nuorodų tikrinimas. Tai taip pat svarbu tikrinti nuorodą, ar tai tikrai yra ta nuoroda, kurios asmuo tikisi.
- Slaptažodžio puslapio tikrinamas. Jei yra jungiamasi prie puslapio, kuris reikalauja slaptažodžio ir kitų svarbių duomenų įvedimo, reikia patikrinti ar tikrai yra jungiamasi per HTTPS protokolą ir ar kompiuteryje yra gautas sertifikato patvirtinimas.
- Domeno tikrinimas. Svarbu yra tikrinti domeną ir peržiūrėti, ar nėra kokių smulkių pakitimų, nes pridėta viena raide ar simbolis reiškia, kad jau yra gautas netikras, apgaulingas laiškas, ar atidarytas apgaulinga internetinė svetainė.
- Vaizdo domenų asociacijų apsauga. Tai gali būti įmonės logotipai, ar paveikslėliai, kuriuos paspaudus gali būti nukreipiama ne į tikrojo puslapio svetainę, bet į padirbtą puslapio svetainę. Tokiu atveju kompiuteryje turi būti įdiegta apsisaugojimo sistema nuo tokių apgavimo būdų, kuri tikrina ar jungiamasi tikruoju adresu, ar yra nukreipiama kitur.

2.2. Sistemų klonavimas ir jo rizika informacijos saugumui

Sistemų klonavimas (angl. Web-spoofing) – tai metodas, kuriuo vartotojai mano, kad juos nukreipė į oficialią kompanijos žiniatinklio svetainę. Vietoj to, juos iš tikrųjų nukreipė į „spoofed“ žiniatinklio svetainę, kur bet kokie asmeniniai duomenys, kurie yra įvesti, bus sukaupti ir panaudoti piktais tikslais. Tokie tinklalapiai suprojektuoti kvalifikuotų tinklo projektuotojų ir yra dažnai tiksli originalios kompanijos žiniatinklio svetainės kopija. Svarbus skirtumas yra tas, kad yra smulkių pakeitimų, kurie atsižvelgia į vartotojų informaciją, kuri yra sukaupta ant „fraudster“ serverių (Angelopoulou O. ir kt, 2007)

Apsisaugojimo priemonės nuo sistemų klonavimo yra pateiktos 2.1. skyriuje. Tie būdai reikalauja atidumo pateikiant duomenis, ar jungiantis prie bankinių sistemų, ar kitų svarbių svetainių. Taip pat čia Neil Chou ir kt. teigia, kad nuo sistemų klonavimo padeda apsisaugoti ir „SpoofGuard“, kuris vadinamas Internet Explorer naršyklės pagalbinis objektas. Šis objektas padeda atpažinti internetinės svetainės netikrumą. Jei asmuo jungiasi prie netikros svetainės ir joje nori suvesti savo slaptažodžius ar kai asmuo būna nukreipiamas ne į tą puslapį, šis „SpoofGuard“ objektas praneša, kad

yra tikimybė, kad jūsų duomenys pateks į kita svetainę ir pan. Apačioje pateikiamas vaizdinis pranešimas, kaip yra pranešama, kad duomenys yra vedami į klonuotą „ebay“ svetainę.



Šaltinis. Informacija pateikta internetinėje svetainėje http://ltforum.destinysphere.net/ .

5 pav. **pranešimas apie naudotojo svetainės klonavimo galimybę - „SpoofGuard“**

2.3. Piktybinės programinės įrangos poveikis saugumui

Piktybonė programinė įranga – šiai grupei galima būtų priskirti tokias kenkėjiškas programas, kaip:

- Šnipinėjimo programinė įranga „spyware“;
- Virusus;
- Specifiškai organizuojamus trojanus ir kt.;

Šią kenkėjišką programinę įrangą kuriama sąmoningai šnipinėti kompiuterio duomenis, kurie yra naudojami piktais tikslais norint pasipelnyti, arba tiesiog pakenkti. Šioje dalyje bus apžvelgiama tokia programinė įranga ir pateikiama jos kenksmingumas.

2.3.1. Šnipinėjimo programų ypatumai

Šnipinėjanti programa (angl. Spyware) – tai programa, kuri be vartotojo sutikimo bei be konkretaus perspėjimo jungiasi į internetą, užmezga slaptą interneto jungtį ar kanalą apie kurį vartotojas nieko nenutuokia. Taigi, spyware galime vadinti bet kurią programinę įrangą, kuri daro ne tik tai, dėl ko ji buvo suinstaliuota (pvz. naudotis el. paštu, keistis failais ir pan.), tačiau dar ir veikia pogrindyje. Tokios programos renka informaciją apie tam tikrą veiklą, kuri yra atliekama kompiuteryje ir siunčia ją į milžiniškas duomenų bazes. Dabar vis dažniau spyware apibrėžiamas kaip rinkodaros (marketingo) įrankis, padedantis stebėti vartotoją, nustatyti jo pomėgius ir siūlyti atitinkamo turinio reklamą. Kartais tokios programos žargonu dar vadinamos trojan-ware ar reklaminiais trojanais, nes jos prisidengia kitomis programomis - vartotojas diegiasi sau vienokią programą, o šalia jos, nežinodamas dar įsidiegia ir šnipinėjimo programą (Spyware, 2009).

2.3.2. Virusų daroma žala

Virusas - tai kompiuterinio kodo dalis, kuri prisijungia prie programos ar failo, kad galėtų plisti iš kompiuterio į kompiuterį kartu su siunčiama programa ar failu. Virusai gali sugadinti techninę ar programinę įrangą, ar failus. Kodas, parašytas specialiai taip, kad jis galėtų atsikartoti (pasidauginti). Kompiuteriniai virusai gali būti įvairiausi: nuo erzinančių, bet praktiškai nekenksmingų iki pažeidžiančių kritinius failus ar įrangą. Tačiau tikras virusas sklinda tik tuo atveju, kai prie to prisideda žmogus, pavyzdžiui, bendrai naudodamasis failu arba siųsdamas elektroninį laišką ir pan.(Microsoft Security, 2009).

Virusai yra pavojingi ir gali padaryti žalą. Galima būtų išskirti tokius žalos padarymo atvejus:

- programų užkrėtimas - kai kurios užkrėstos programos nustoja veikti arba veikia blogai;
- garso ir video efektai - pvz., krintantys simboliai, įvairūs ekrano režimų trukdymai muzika ir kt., trukdantys kompiuterio darbą;
- sistemos darbo lėtėjimas, pvz. įvedimo-išvedimo metu;
- tam tikrų operacijų, pvz., programų vykdymo arba OS kelties trukdymas kompiuteryje;
- nepastebimas duomenų failų modifikavimas, pvz., skaičių sukeitimas failuose;
- informacijos diskuose sunaikinimas, pvz. formatuojant diską, ar trinant tam tikras disko sritis;
- failų sistemos sugadinimas - failų išdėstymo lentelės, katalogų, disko sistemos kelties ir kieto disko paskirstymo lentelės modifikavimas.

2.3.3. Trojos arklio pavojingumo faktoriai

Trojos arklys veikia tuo pačiu principu, kaip ir mitologijoje minimas Trojos arklys, kuris atrodė kaip auka dievams, bet iš tikrųjų leido į miestą patekti ir jį užimti graikų kareiviams: tai kompiuterinės programos, kurios atrodo kaip naudingos programos, bet iš tiesų kelia grėsmę saugumui ir gali padaryti daug žalos kompiuteriui. Trojos arkliai dauginasi, kai žmonės yra suviliojami atidaryti programą, nes jie tiki, kad ji buvo pateikta iš patikimo šaltinio. Taip pat Trojos arklių gali pasitaikyti programinėje įrangoje, kurią žmonės siunčiasi nemokamai (Microsoft Security, 2009).

Kompiuteriniame pasaulyje Trojos arklio metodas yra naudojamas įterpti tam tikrus duomenis į programą, kurie šią programą performuoja neautorizuotoms funkcijoms atlikti. Tai įprastas būdas įterpti į sistemą virusus, taip pat įprastas būdas vykdyti sukčiavimus kompiuterio pagalba. Nieko neįtariantis programos vartotojas gali kartu su gauta programa instaliuoti savo sistemoje papildomus duomenis, kurie leidžia nusikaltėliui, žinančiam atitinkamus kodus prisijungti prie kompiuterinio tinklo darbo vietos ir gauti joje esančią informaciją(David Icove, 1995).

Šio tipo kenkėjiškos programos yra kenksmingos dėl to, kad jos dėka galima valdyti kito žmogaus, įmonės ir pan. kompiuterį per atstumą, t.y. kad kompiuteris gali buti kitoje valstybėje ir pan. Trojos arklio veikimo principas yra paprastas, t.y. žmogus, kuris nori pakenkti, turi paleisti tame kompiuteryje failą, tai dažniausiai būna *.exe, tada reikia sužinoti to kompiuterio IP adresą ir tada “nusikaltėlio” yra paliežiama programa, kuri leidžia valdyti aukos kompiuterį, kai jis yra įjungtas, to jam net nežinant.

Bandant apsisaugoti nuo trojos arklių, priimant kiekviena failą, privalu atkreipti dėmesį į tai kas yra siunčiama, taip pat koks tai failas, ar jis nesibaigia galūne *.exe ir pan. svarbu atkreipti dėmesį ir į siuntėją, net ir žinomas siuntėjas gali atsiųsti, net ir jo kompiuteris gali būti apkrėstas ir kažkas iš jo kompiuterio siunčia piktybinį failą.

3. ELEKTRONINIŲ FINANSINIŲ ATSISKAITYMŲ SISTEMOSE TAIKOMOS SAUGOS PRIEMONĖS

3.1. IT saugumo standartai naudojami elektroniniuose atsiskaitymuose

SSL protokolas (angl. Secure Sockets Layer) – rinkos standartu tapusi technologija, kuri garantuoja saugų perdavimą internetu. Šį protokolą sukūrė JAV kompanija "Netscape" 1996-aisiais metais. SSL greitai buvo pripažintas kaip saugaus duomenų perdavimo standartas. SSL naudoja dauguma interneto naršyklių bei WEB serverių, nes jo dėka duomenis internetu galima perduoti itin saugiai. SSL naudoja viešą- privatų raktų šifravimo sistemą.

SSL protokolas reikalauja, kad serveryje būtų instaliuota skaitmeninis sertifikatas. Skaitmeninis sertifikatas yra e. dokumentas, kuris leidžias nustatyti svetainės tapatumą. Skaitmeninis sertifikatas tarnauja kaip skaitmeninis pasas, kuris patvirtina serverio autentiškumą prieš sukuriant SSL ryšio kanalą. Dažniausiai skaitmeninius sertifikatus pasirašo nepriklausomi bei patikimos trečiosios šalys, kurios užtikrina sertifikato galiojimą bei pagrįstumą. Sertifikatą pasirašančioji šalis yra žinoma kaip "Sertifikato Įrodymas" (angl. Certification Authority).

SSL užtikrina saugų bendravimą kombinuodamas šiuos du elementus:

1. Autentifikacija. Autentifikacija atliekama naudojant skaitmeninius sertifikatus. Jie yra saugių elektroninių sandorių pagrindas, nes identifikuoja sandorio dalyvius ir lengvai patikrina kitų dalyvių identifikaciją.
2. Duomenų šifravimas. Šifravimas yra procesas, kuriuo metu duomenys yra užšifruojami, kad juos neperskaitytu nepageidaujami asmenys. Šiuos duomenys gali būti perimami trečiosios šalies, bet jų nebus įmanoma perskaityti, nes trečioji šalis neturi šifro rakto.

SSL dažniausiai naudojama užtikrinti perduodamų duomenų saugumą tarp interneto naršyklės bei interneto serverio. Taip pat SSL gali būti naudojamas užtikrinant serverių bendravimą.

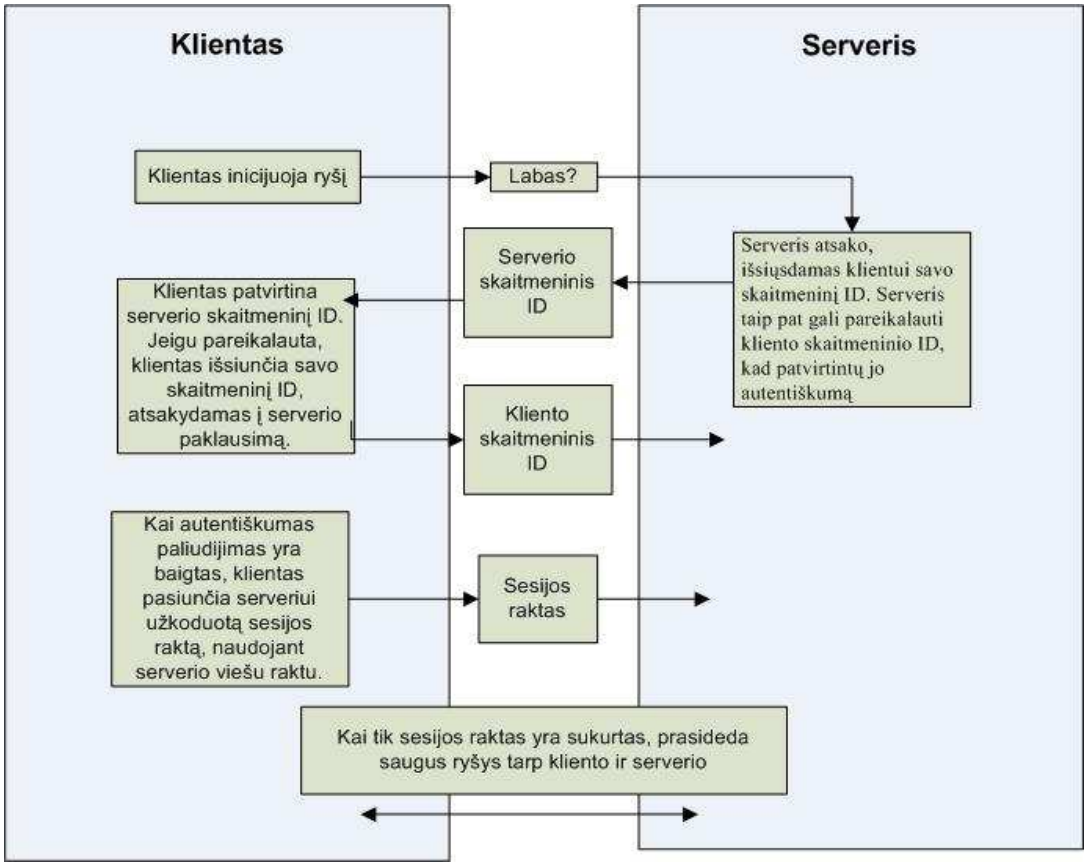
Paprastai skaitmeninis sertifikatas susideda iš:

- Savininko viešo rakto
- Savininko vardo
- Viešo rakto galiojimo termino
- Skaitmeninį sertifikatą teikiančios organizacijos (CA) pavadinimo
- Skaitmeninio sertifikato serijinio numerio
- Sertifikatą teikiančios organizacijos skaitmeninio parašo.

Skaitmeninių sertifikatų veikimas yra pagrįstas kodavimo viešuoju raktu technologija, veikiančia naudojant porą tarpusavyje "surištų" raktų - privatų ir viešą. Viešasis raktas turi būti žinomas visiems, kas nori susisiekti su raktų poros savininku. Jis gali būti panaudotas pranešimo, pasirašyto privačiuoju

raktu, patikrinimui arba pranešimo, kuris galės būti iššifruotas tik privačiuoju raktu, kodavimui. Tokiu būdu užšifruotų pranešimų saugumas yra pagrįstas privataus rakto saugumu, kuris turi būti gerai apsaugotas nuo neteisėto priėjimo.

Ketvirtas paveikslėlis (žr. 6 pav.) iliustruoja procesą (t.y. kaip gauti saugų SSL ryšį), kuris garantuoja apsaugotą komunikaciją tarp web serverio ir kliento. Visas SSL pažymėjimų keitimas įvyksta per sekundes. Taip pat serveris patvirtina savo autentiškumą su interneto naršyklės skaitmeniniu sertifikatu, bei patikrinama ar skaitmeninis sertifikatas gautas iš žinomo sertifikavimo centro, jei ne klientas turi būti informuotas. Dar patikrinamas ir ar skaitmeninio sertifikavimo laikas nepasibaigęs[6].



Šaltinis. Business Guide: Guide of securing your e-government web site.

6 pav. **SSL protokolo duomenų perdavimo schema**

HTTPS - saugus hiperteksto perdavimo protokolas. Jis yra ryšio protokolas, skirtas perduoti užkoduotus duomenis tarp kompiuterių per internetą. HTTPS yra sudarytas iš HTTP (HyperText Transfer Protocol) ir SSL. HTTPS leidžia saugius elektroninės prekybos sandorius, pavyzdžiui, internetinės bankininkystės, e. finansiniuose atsiskaitymuose ir pan. Interneto naršyklės, pvz. Internet Explorer ir Firefox, ar kitos interneto naršyklės, rodo saugumo piktogramą, kuri reiškia, kad interneto svetainė yra saugi. Saugumą taip pat rodo ir adreso juostos pradžia (pvz. https://). Kai vartotojas

[6] Business Guide: Guide of securing your e-government web site, informacija internete, adresu: http://www.verisign.com/static/005568.pdf

prisijungia prie interneto puslapio naudojant HTTPS protokolą, puslapis užkoduoja sesiją naudojant skaitmeninį sertifikatą**.** Duomenys yra perduodami HTTP protokolui, paskui perduodama SSL protokolui, kas juos užšifruotų. Taip duomenys užšifruojami ir saugiai perduodami. Šis protokolas yra orientuotas siųsti saugioms žinutėms. Beje, siunčiant tokias žinutes, ar kitokius duomenis, juos šifruoja HTTPS pagalba. Klientas gali būti tikras, kad jo siunčiama informacija ar kiti duomenis yra apsaugoti.

Vartotojas gali pasakyti, jeigu jis yra prijungtas prie saugaus tinklalapio, tai atpažinti padeda svetainės adresas “https://” vietoj “http://”. Daugiausiai protokolą HTTPS naudoja internetiniams pirkimams, keitimams ar privačios informacijos gavimui. Prieiga prie saugaus serverio dažnai reikalauja tam tikros registracijos, prisijungimo vardų, ar kitokių būtinų duomenų [14,15].

Interneto servisas – tai protokolų ir standartų rinkinys, naudojamas duomenų apsikeitimui tarp aplikacijų ir sistemų. Įvairiomis programavimo kalbomis parašytos aplikacijos, veikiančios skirtingose operacinėse sistemose, naudoja interneto servisus duomenų mainams kompiuteriniuose tinkluose.

WS-Security – tai standartų grupė, nurodanti kaip galima užtikrinti interneto serviso saugumą. Keli iš tokių būdų yra sertifikavimo tarnybų naudojimas, uždarų vartotojų grupių sudarymas. WS-Transaction yra standartų grupė ,užtikrinanti patikimą transakcijų vykdymą tarp verslo partnerių. WS-ReliableMessaging standartas užtikrina, kad pranešimai pasieks adresatą reikiama tvarka bei nebus dubliuojami. Šie standartai nėra galutiniai, jie nuolat tobulinami. Tai tik maža dalis, vadinamos WS-*, standartų šeimos (Kairaitis, 2007).

Saugumas - tai pagrindinis faktorius apibūdinantis interneto serviso kokybę. Saugumo sritis ir web service apima daug reikalavimų pagrindų, kurie naudojami SOAP žinutėms persiųsti. Interneto serviso saugumo standartams sukurti reikia daug pastangų.

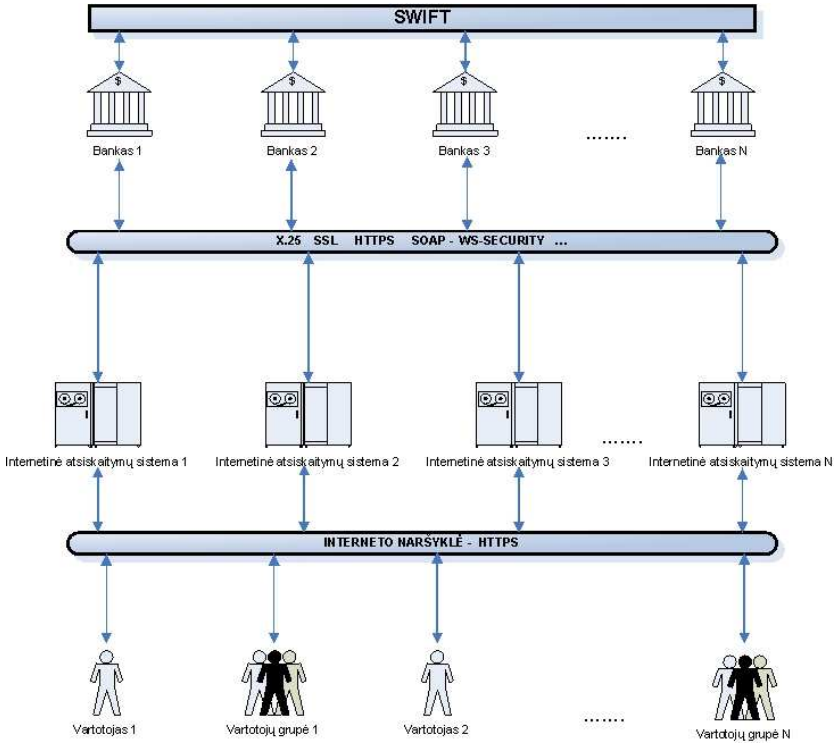
WS-Security protokolas aprašo SOAP žinučių praplėtimus, kad padidinti apsaugos kokybę per žinučių vientisumą, konfidencialumą ir kiekvienos žinutės autentikaciją. Šis mechanizmas gali taikyti įvairius saugumo modelius ir šifravimo technologijas. WS-Security taip pat suteikia bendro pobūdžio mechanizmą apjungti saugumo artefaktus ir žinutes. WS-Security nereikalauja specifinių saugumo artefaktų. Jis yra sukurtas taip, kad palaikytų keletą saugumo technologijų. Jame taip pat yra praplėtimo mechanizmas, kuris gali būti panaudotas tolesniam kredencialų charakteristikų aprašymui, esančių žinutėje.

Ši specifikacija siūlo eilę SOAP praplėtimų, kurie galėtų būti panaudoti kuriant saugius interneto servisus, kad sukurti vientisumą ir konfidencialumą. WS-Security yra lankstus ir yra panaudotas kaip pagrindinė konstrukcija plačiam spektrui saugumo modelių, kaip PKI, Kerberos ir SSL. Specifiškai WS-Security suteikia palaikymą daugialypėms saugumo technologijoms, daugialypiams patikimiems domenams, daugialypiams parašo formatams ir daugialypiams šifravimo technologijoms. WS-Security yra pagrindinis elementas, kuris gali būti sujungtas su kitais interneto serviso praplėtimais ir aukšto

lygio specifinių reikalavimų protokolais, kad būtų pritaikytas plačiam spektrui saugumo modelių ir šifravimo technologijų (IBM Corporation, 2005).

3.2. Saugumo sprendimų taikymas elektroninių finansinių atsiskaitymų sistemose

Šiame skyrelyje bus nagrinėjami elektroninių finasinių atsiskaitymų sprendimai pradedant bankais ir baigiant galutiniu elektroninės parduotuvės ar sistemos vartotoju. Žemiau pateiktoje shemoje yra pavaizduotos bendros atsiskaitymų schemos, susietos su saugumo tehnologijomis, kurios yra nagrinėjamos šiame darbe.



Šaltinis. Sudaryta autorės.

7 pav. **Elektroninių atsiskaitymų shema**

7 paveikslėlyje yra pateikiama, kaip galutinis vartotojas naudodamas internetine naršykle jungiasi prie internetinės atsiskaitymų sistemos ir, tarpininkaujant bankui, apmoka už prekes ar paslaugas. Taip pat matoma, kad bankai, taip pat turi tarpbankinę sistema, kuri dalyvauja atsiskaitymuose. Sekančiuose skyriuose bus detaliau nagrinėjamos šios atsiskaitymų sistemos bei jų saugumo technologijos.

3.2.1. Saugumo užtikrinimas tarpbankinių pranešimų sistemos „SWIFT“ pagalba

Tarptautinių bankų sąveikos finansinių nuotolinio ryšio tinklo organizacijos sistema - **SWIFT-as** (angl. Society of Worldwide Interbank Financial Telecomunication), skirtą tarpbankinių atsiskaitymų apsaugai.

SWIFT-as, kaip organizacinė techninė sistema, yra (arba gali tapti) pagrindinis finansų ir kredito įstaigų perdavimo tinklas, jungianti ir organizuojanti sistema, turinti bendrą kalbą ir nuotolinio ryšio elementus. Kad nebūtų išstumti iš tarptautinių mokėjimo rinkos, bankai konkurenciniais sumetimais jungiasi prie SWIFT-o. SWIFT-as veikia dvišaliu (dviejų dalyvių) pagrindu, atitinka ISO (Tarptautinių standartų organizacijos) ir ICC (Tarptautinių prekybos rūmų) standartų reikalavimus. Nors vienkartiniai stojimo į Asociaciją ar asocijuotus narius mokesčiai yra dideli, tačiau SWIFT-as yra pigesnis už analogiškas operacijas faksu.

SWIFT-as yra pranešimų sistema, kuri:

- užtikrina bendrą kalbą, informacijos perdavimą ir priėmimą bei apdorojimą;
- užtikriną abipusį (bet ne daugiašalį) ryšį su tolimaisiais klientais ir korespondentais;
- leidžia atlikti (bet neatlieka) mokėjimo operacijas be popierinių mokėjimo dokumentų;
- perduoda per bankų nuotolinio ryšio tinklą pervedimus, kurie įskaitomi per atitinkamas nostro ar loro sąskaitas;
- tikslai patikimai perduoda 11 kategorijų 130 tipų pranešimus;
- sudaro paprastos ir visa apimančios kontrolės galimybę gaunamai ir siunčiamai informacijai;
- šifruoja ir saugo pranešimus nuo nesankcionuotos priėjimo ir informacijos praradimo išsijungus sistemai;
- sumažina klaidų, klastojimo ir kitų neigiamų padarinių riziką (Sodžiūtė ir kt., 2003).

3.2.2. Virtualaus autorizacijos modulio panaudojimas

Virtualus autorizacijos modulis (VAM) pagal UAB „Penki kontinentai“ parengtą sistemą leidžia prisijungti prie bankinių sistemų e.parduotuvės, tarsi prie mokėjimo terminalo. Tokiu būdu e.parduotuvėje galima naudotis visomis populiariausiomis Lietuvoje bankų mokamosiomis kortelėmis.

VAM - iš esmės laikytina specialiuoju mokėjimų serveriu. Trumpai sistemos veikimo principą galima paaiškinti taip: pirkėjas nurodo internete savo kortelės duomenis, kurie siunčiami į VAM serverį užkuoduotu pavidalu. VAM serveris paverčia tuos duomenis suprantamais banko sistemai ir siunčia juos į banką ne per internetą, o per specialų - X.25 tinklą. Visame pasaulyje X.25 tinklai naudojami finansinių institucijų duomenims perduoti ir yra itin patikimi, jų saugumas netgi neaptarinėjamas. Po to, kai banko sistema gauna duomenis, atliekama kortelės autorizacija, kuri trunka kelias sekundes. Tada pirkėjas gauna autorizacijos patvirtinimą. Pinigai iš pirkėjų kortelių sąskaitų pervedami į pardavėjo banko sąskaitą taip pat, kaip tai vykdoma autorizuojant korteles naudojant įprastus mokėjimo terminalus parduotuvėse. Sistema apsaugota nuo nesankcionuoto naudojimo:

- Įdiegti apsaugos raktai bei tikrinamas kiekvieno prisijungiančiojo įrenginio identifikacijos numeris;
- Įdiegta įranga ribojanti priėjimą prie sistemos;
- Įdiegta programuotė neleidžianti įsiskverbti į sistemą iš išorės.

Duomenų perdavimo ir atsiskaitymo sistemų saugumas finansinių ir kredito įstaigose palaikomas iš karto keliais lygiais:

- Duomenų perdavimo kanalo šifravimas;
- Slaptažodžių bei autorizacijos kodų sistema ir jų šifravimas;
- Transakcijų autorizavimas;
- Kliento darbo sesijos stebėjimas;
- Veiksmų žurnalizacija.

Duomenys perduodami iš kliento kompiuterio į interneto linijos tarnybinę stotį ir, atvirkščiai, yra apsaugoti. Kanalui apsaugoti naudojamas 128 bitų SSL protokolas. 128 bitų atviruųjų raktų algoritmo šifravimas yra visiškai patikimas ir yra laikomas internetu perduodamu finansinių transakcijų šifravimo standartu. Apsaugotas kanalas taip pat neginčijamai patvirtina, kad pirkėjas naudojasi konkrečios finansų ir kredito įstaigos elektroninės bankininkystės tarnybine stotimi (Sodžiūtė ir kt., 2003).

3.2.3. Internetinių mokėjimų sistemos „PayPal“ apsaugos preimonės

PayPal – tai populiari internetinių mokėjimų sistema pasaulyje. Ši sistema skirta saugiai ir lengvai apmokėti už prekes internetu, taip pat saugiai siųsti pavedimus šios sistemos pagalba visame pasaulyje internetu. Ši sistema palaiko mokančiojo asmens privatumą, todėl pinigų gavėjas negali matyti mokančiojo asmens kreditinės kortelės ar banko sąskaitos numerio. Jis gali matyti tik elektroninio pašto adresą, prisiregistravimo datą, taip pat ir patvirtinimą apie operacijos užbaigtumą.

Šaltinis PayPal internetinė svetainė, 2009.

8 pav. PayPal sistemos veikimo principo pavyzdys

Šiame paveikslėlyje pateikiami trys PayPal sistemos veikimo principo etapai:

1. pirmajame žingsnyje vartotojas norėdamas atlikti mokėjimą, pasirenką finansavimą iš PayPal sąskaitos, banko sąskaitos ar kreditinės korteles;
2. antrajame žingsnyje PayPal sistema užkoduoja vartotojo duomenis, t.y. banko sąskaitos ar kreditinės kortelės numerius, ir elektroniniu paštu išsiunčia pranešimą gavėjui, kad yra gautas mokėjimas jo vardu;
3. trečiajame žingsnyje gavėjas gauna pinigus nematydamas pirkėjo informacijos.

Vienas iš svarbiausių kriterijų finansiniuose atsikaitymuose yra saugumas ir pasitikėjimas. PayPal technologija suteikia transakcijoms ir finansiniams atsiskaitymams saugumą ir privatumą. Palaikyti privatumui ir saugumui PayPal atlieka tokius veiksmus:

- antiapgaulės pavojaus modelis. Šis modernus ir patentuotas pavojaus modelis padeda atskleisti ir numanyti apgaulingas transakcijas, kol jos nepasiekė verslo;
- naudojamas pirmaujantis rinkoje duomenų šifravimo algoritmas. PayPal technologijoje duomenų šifravimas daug labiau naudojamas, nei kitose finansinėse įmonėse;
- apsaugoma finansinė informacija. PayPal sistema neleidžia gavėjui prieiti prie pirkėjo duomenų, tokiu būdu leisdami pirkėjui pasijusti saugiam naudojantis PayPal mechanizmu;
- naudojamas standartinis servisas. PayPal naudoja rinkoje žinomus adresų atpažinimo servisus bei kortelių apsaugojimo kodus, kad būtų atpažįstami nusikaltėliai;
- atliekamas patikrinimas. Atliekamas banko sąskaitos tikrinimas, kaip papildomas lygis autentifikacijai patikrinti;

- PayPal saugumo užtikrinimo komanda. Šia komandą sudaro apie 2000 žmonių iš viso pasaulio. Jie dirba 24 valandas per parą ir 7 dienas per savaitę, kad užtikrintų transakcijų saugumą, bei informacijos privatumą.

Saugumas finansinės ir asmeninės informacijos yra vienas iš svarbiausių prioritetų. Dėl šios priežasties PayPal sistema automatiškai šifruoja informaciją tarp pirkėjo kompiuterio ir serverio. Šifruojant informaciją atliekami tokie žingsniai:

- Visų pirma pirkėjui registruojantis ar jungiantis prie PayPal puslapio yra tikrinama, ar pirkėjo naršyklė naudoja Secure Sockets Layer 3.0 (SSL), ar aukštesnę versiją;
- Informacija apsaugoma SSL su šifravimo raktu sudarytu iš 128 bitų (tai aukščiausias apsaugos lygis);
- Asmeninė informacija yra stipriai saugoma serveryje, tiek fiziškai tiek ir elektroniškai. Tolimesnė apsauga yra ta, kad serveris, kuriame laikoma informacija, neturi prieigos prie interneto (PayPal, 2009).

3.2.4. Elektroninės sistemos „Google Checkout" atsiskaitymų ypatumai

Google Checkout – tai viena iš e. atsiskaitymų sistemų, kuri išsaugoja kreditinių, ar debetinių kortelių duomenis ir pristatymo adresus ir leidžia greitai ir patogiai apsipirkti interneto parduotuvėse. Vartotojui užtenka užsiregistruoti tik vieną kartą (tinka Gmail ar kitų Google paslaugų prisijungimo duomenys).

Naudojantis Google Checkout sistema nebereikia e.parduotuvėje papildomos registracijos ar autorizacijos, visi mokėjimai yra patvirtinami su Google prisijungimo vardu ir slaptažodžiu. Visi atlikti mokėjimai yra saugomi Google sistemoje ir ten galima peržiūrėti mokėjimų istoriją. Priešingai nei pardavėjai, jie nemato operacijų istorijos, taip pat kreditinės kortelės duomenų, pagal atskirus reikalavimus nepateikiamas ir pirkėjo e.paštas.

Google Checkout sistema yra saugoma tokiais būdais:

- Mokėjimo kortelių ir pirkimų duomenys yra laikomi tik Google serveriuose, prisijungimas prie Checkout sistemos reikalauja vartotojo vardo ir slaptažodžio.
- Prisijungimo sistema apsaugota nuo slaptažodžio nulaužimo automatinio perrinkimo būdu.
- Vartotojo informacija perdavimo tarp skirtingų serverių metu šifruojama panaudojant saugiausią ir atitinkančią tarptautinius standartus SSL (Secure Sockets Layer) kriptografinį protokolą.
- Prisijungimas ir naršymas Google Checkout sistemoje vyksta saugiu HTTPS protokolu (Hypertext Transfer Protocol over Secure Sockets Layer).

- Informacija apie vartotojo naudojimąsi paslauga. Siekiant apsaugoti vartotojus nuo sukčiavimo, slaptos informacijos kaupimo, gali būti renkama informacija apie vartotojų naudojimąsi paslauga, kuri padėtų patvirtinti vartotojo tapatybę, ar aptikti potencialiai apgavikišką elgesį. Pvz. Gali būti tikrinama, kaip greitai vartotojas surenka savo slaptažodį bei prisijungimo vardą, kad būtų apsisaugota nuo hakerių atakų.
- Registro informacija. Naudojantis Google Checkout, jų serveriai įrašo informaciją apie vartotojo IP adresą, naršyklės tipą, kalbą ir netgi prisijungimo datą bei laiką.
- Informacija gaunama iš trečiųjų asmenų. Siekdama apsisaugoti nuo sukčiavimo, Google gali rinkti informacija apie vartotojus ir iš kitų institucijų tam, kad įsitikintų pateiktų duomenų tikrumu.

4. ELEKTRONINIŲ FINANSINIŲ ATSISKAITYMŲ SAUGOS REIKALAVIMŲ VERSLO ĮMONĖSE VERTINIMAS

4.1. Elektroninių finansinių atsikaitymų saugumo reikalavimų taikymo įmonėse tyrimo metodika

Eksperimentinio tyrimo tikslas yra ištirti e. finansinių atsiskaitymų saugumo reikalavimų taikymą įmonėse, kurios naudoja e. atsiskaitymus. Taip pat anonimiškai apklausti Lietuvos įmones, kurios naudoja e. atsiskaitymus ir nustatyti kokį dėmesį skiria šių atsiskaitymų apsaugojimui ir kaip vyksta tas apsaugojimas bei ištirti saugumo reikalavimų vykdymą, tokiuose atsiskaitymuose.

Eksperimentinio tyrimo objektas yra pasirinktos Lietuvos įmonės, kurios verčiasi skirtinga veikla ir skiriasi jų e. finansinių atsikaitymų būdai.

Eksperimentinio tyrimo uždaviniai:

- Atlikti kokybinę saugumo reikalavimų taikymo e. finansiniuose atsikaitymuose analizę Lietuvos verslo įmonėse apklausiant ekspertus dirbančius saugos priemonių sistemų realizavime.
- Atlikti kiekybinę Lietuvos verslo įmonių e. atsiskaitymų analizę, kuri leistų išsiaiškinti saugumo reikalavimų taikymo priemonių efektyvumą atliekamuose e. finansiniuose atsiskaitymuose.
- Nustatyti tiriamų įmonių pagrindinius naudojamus įrankius saugumo reikalavimams įvykdyti bei priemones e. finansiniuose atsikaitymuose, kurie turi didžiausią įtaką šių įmonių konfidencialių duomenų pažeidžiamumui.
- Įvertinti e. finansinių atsiskaitymų saugumo būklę Lietuvos įmonėse taikant, interviu su įmonių ekspertais bei anonimiškos apklausos verslo įmonėms, būdus atlikti eksperimentinį tyrimą.

Eksperimentinio tyrimo planas. Pirmiausia naudojantis metodine mokslinės literatūros analizę, kuri leis įvertinti e. finansinių atsikaitymų saugumo ryšį bei pažeidžiamumą ir išskirti pagrindinius e. atsiskaitymų pažeidimo faktoriai ir būdus. Pagal šią informaciją sudaryta anketa, klausimynas įmonės specialistams ekspertams, kuri leistų pasirinkti jų įmonei tinkančius variantus ir leistų joms papildyti bei pateikti naudingos informacijos apie saugumo reikalavimų vykdymą. Renkantis dvi įmones, stengtasi išsirinkti skirtingomis veiklomis bei skirtingais e. finansinių atsikaitymų būdais besinaudojančiomis įmonėmis.

Buvo pasirinkta UAB „Baltjuta“, kuri verčiasi naujų ir naudotų kompresorių pardavimu, nuoma, technine jų priežiūra ir remontu, atsarginių detalių ir eksploatacinių medžiagų tiekimu. Taip pat

raštinės reikmenimis ir verslo dovanomis prekiaujanti įmonė X, kuri saugumo sumetimais nenorėjo, kad būtų atskleidžiamas jos pavadinimas, nes yra kalbama apie jautrius įmonės duomenis.

Siekiant atlikti kokybinę bei kiekybinę analizes, buvo sudaryta anketa pavadinimu „Įmonių, naudojančių elektroninius finansinių atsiskaitymų sistemas, apklausa“[7].

Pasirinktoms įmonėms buvo pasirinkta kokybinės analizės tyrimas, nes kiekvienoje įmonėje viskas interpretuojama ir naudojama skirtingai, taip pat kokybinėje analizėje duomenys yra laikomi visuma, kuri suteikia informaciją apie kokio nors loginio vieneto struktūrą, kaip šiuo atveju įmonės vieneto struktūra, nes šio tyrimo metu įvertinsime įmonės saugumo užtikrinimo procesą iš arti. Taigi šiame tyrime bus nagrinėjamos įmonių saugumo reikalavimų įgyvendinti skirtos priemonės ir e. finansiniuose atsikaitymuose taikomi įrankiai. Taip pat bus atlikta lyginamoji analizė su kitomis nagrinėjamomis kiekybinės analizės metu apklaustomis įmonėmis, kurių apklausti buvo pasirinkta 46 įmones[8]. Visoms įmonėms bus pateikiamos rekomendacijos atsižvelgiant į jų taikomus saugumo įrankius bei priemones ir galimus taikyti saugesnius saugumo sprendimus.

Šiuose tyrimuose naudota priemonė – anketa, kuri yra pateikiama 1 priede. Šios anketos klausimai buvo parengti atsižvelgiant į tai, kad tyrimas vyksta apie e. finansinių atsikaitymų saugumo reikalavimų įgyvendinimą naudojant tam tikrus įrankius bei priemones. Norima išsiaiškinti, kokie saugumo reikalavimų sprendimai naudojami įmonėse, ar jie yra pakankami saugūs, ar reiktų įdiegti kokias papildomas saugumo sistemas.

Anketoje stengiamasi suformuluoti kuo tikslesnius klausimus su uždarais atsakymais, iš anksto parengtais tiksliais atsakymų variantais. Tokie apklaustųjų (t.y. respondentų) atsakymai leidžia tiksliau ir paprasčiau padaryti išvadas bei gauti rezultatus ir apibendrinti tyrimą. E. finansinių atsikaitymų saugumo reikalavimų įvertinimo tyrimo rezultatais siekiama įvardinti saugumo lygį įmonėse bei pateikti joms rekomendacijas, kad įmonės saugumo lygis būtų aukštas.

[7] Pirmoji anketos dalis patalpinta internete tokiu adresu : http://www.surveymonkey.com/s.aspx?sm=SLxvgjHFz8a85pRWAeHMnw_3d_3d .
Antroji anketos dalis patalpinta tokiu adresu internete: http://www.surveymonkey.com/s.aspx?sm=Ns_2bqE9_2fQGW_2bB_2fBNVNGG2JQ_3d_3d .

[8] Įmties dydis apskaičiuotas pagal internetinėje svetainėje „ http://www.apklausos.lt/imties-dydis” pateiktos skaičiuoklės paskaičiavimus. Paklaidos dydis pasirinktas 14,5, tikimybė pasirinkta 95%, o populiacijos kiekis, t.y. įmonių skaičius, 160000 pagal 2007 metais pateiktus duomenys.

4.2. Elektroninių finansinių atsiskaitymų būdų ir jų saugumo sprendimų įvrtinimas UAB „Baltjutoje“

UAB „Baltjuta“ įkurta prieš dešimt metų Klaipėdoje. Bendrovės veiklos kryptys – naujų ir naudotų kompresorių pardavimas, nuoma, techninė priežiūra ir remontas, atsarginių detalių ir eksploatacinių medžiagų tiekimas. Ši įmonė yra profesionalią pneumatinę įrangą gaminančios JAV-Prancūzijos SULLAIR, Turkijos DALGAKIRAN atstovas Lietuvoje. Jie siūlo didelį įvairios paskirties mobilių ir stacionarių kompresorių bei pneumatinių įrankių pasirinkimą (UAB „Baltjuta“, 2009).

Su šios įmonės vadovu buvo kalbėta apie saugumo reikalavimų vykdymą elektroniniuose įmonės sistemos finansiniuose atsiskaitymuose, taip pat aptarta kas ją prižiūri bei kaip vyksta tie e. atsiskaitymai.

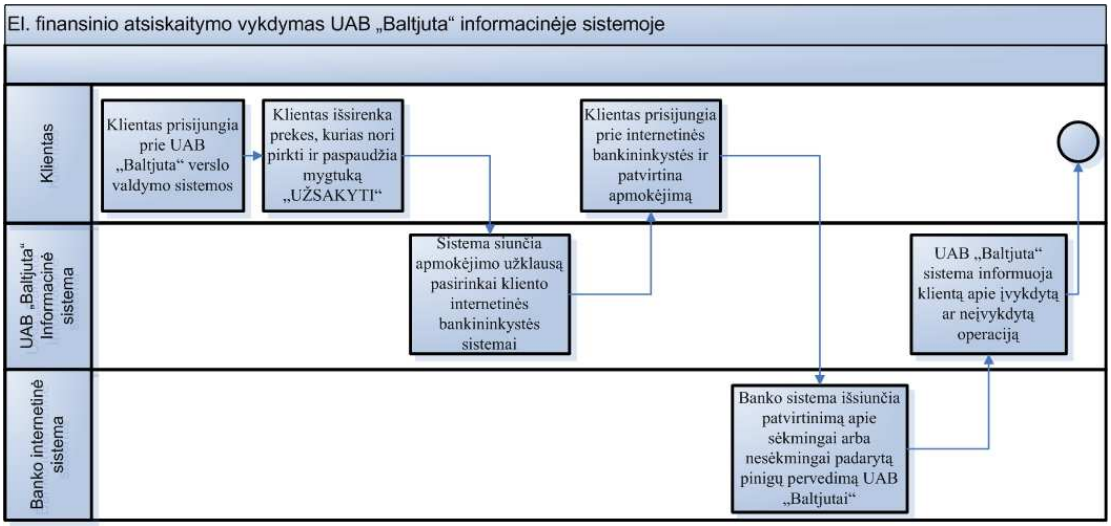
UAB „Baltjuta“ vadovas Raidas Latakas teigė, kad jie naudoja savo įmonės verslo procesams pritaikytą verslo valdymo sistemą, kuri yra skirta ir jų esamiems klientams, kurie gali prie jos prisijungti per internetą bei žiūrėti savo pirktas prekes ar įsigytas paslaugas. Taip pat ši aplikacija yra skirta užsisakyti prekes bei paslaugas ir iš karto už jas atsiskaityti. Vadovas aiškino, kad tai patogu, nes visada klientas žino ką yra nusipirkęs, mato istoriją bei čia pat gali išsirinkti prekes ir už jas atsikaityti. Dar vienas pliusas yra tas, kad šią informaciją mato ir įmonės darbuotojai, todėl galima greitai nustatyti, ką reikia paruošti ir ką pristatyti klientui.

Žemiau pateikiami žingsniai kaip vyksta apmokėjimas elektroninėje erdvėje prisijungus prie UAB „Baltjuta“ klientams skirtos aplikacijos:

- Klientas prisijungia prie UAB „Baltjuta“ verslo valdymo sistemos;
- Klientas išsirenka prekes ir įdeda jas į užsakymų krepšelį;
- Tada klientas turi teisę nueiti į užsakymų krepšelį ir peržiūrėti ar visos jam reikalingos ir tinkamos prekės yra jame;
- Kai klientas apsisprendžia, kad visos prekės yra pasirinktos, tada jis spaudžia mygtuką „APMOKĖTI“.
- Klientas yra nukreipiamas susimokėti už prekes per jo turimą banko finansinių atsikaitymų, internetinių pavedimų sistemą;
- Prisijungęs prie savo elektroninės bankininkystės jis tik suveda savo identifikavimo duomenis ir spaudžia mygtuką „Patvirtinti“.
- Klientas nukreipiamas atgal į įmonės puslapį, kur pateikiama informacija apie gautą apmokėjimą.

Paanalizavus sistemos veikimą iš vidaus matome: kai klientas išsirenka prekes, jo prekių krepšeliui yra priskiriamas numeris, kuris yra siunčiamas į banką kartu su įmonei priskirtu numeriu

(nes su banku yra sudaromos sutartys ir įmonei yra priskiriamas unikalus numeris, kuris identifikuoja kam turi būti skirti pinigai), kai klientas pasirenka banką per kurį moka. Kliento ar įmonės numeris ir suma siunčiami į banką. Bankas, gavęs patvirtinimą iš žmogaus apie apmokėjimą, siunčia įmonei užklausos atsakymą. Tada įmonės sistema automatiškai sugeneruoja laišką klientui su apmokėjimo patvirtinimu arba klaidos pranešimu bei sistemoje užrezervuoja prekes ir siunčia darbuotojams pranešimus, kad šios prekės turi būti pristatytos klientui. Žemiau pateiktame paveikslėlyje galime pamatyti visą prekių pasirinkimo bei apmokėjimo schemą.



Šaltinis. Sudaryta autorės.

9 pav. **UAB „Baltjutos“ kliento apsimokėjimo už prekės per jų sistemą schema**

Tokia sistema turi būti saugoma nuo pašalinių kenkėjų, t.y. virusų, sukčiavimų, bei kitos piktybinės programinės įrangos, kuri gali pakenkti įmonės veiklai. Todėl ši įmonė didelį dėmesį skiria saugumo reikalavimų bei apsisaugojimo vykdymams. Įmonės vadovo žodžiais, didžiausias dėmesys yra skiriamas autentiškumo patvirtinimui, autorizacijai, prieinamumui, minimalioms privilegijoms darbuotojams bei klientams, sistemos paprastumui, internetinių saugumo standartų naudojimui, audito įrašų registravimui bei konfidencialumui. Šioje įmonėje dirba asmuo, kuris nuolat prižiūri įmonės sistemą, taip pat įmonėje esančius kompiuterius. Jis nuolat atnaujina kompiuteriuose esančias antivirusines sistemas, ugniasienes bei, kas savaitę, daro dokumentų kopijas, kad neprarastų svarbios informacijos. Taip pat jis, kartą į mėnesį, atlieka saugumo testus, kurie leidžia patikrinti, ką reikėtų atnaujinti, ar keisti sistemoje. Šia sistema per mėnesį pasinaudoja iki 200 klientų.

Sistema naudoja HTTPS protokolą, kuris naudoja SSL protokolą. Tai yra vienas iš pagrindinių dalykų norint apsaugoti duomenų perdavimą internetu. Duomenys yra perduodami internetu per banką, o tai jau yra grėsmė, kad kažkas nuskaitys duomenis. Taigi duomenų perdavimas turi būti šifruotas, kad, siunčiant duomenis, jų niekas nesugebėtų perskaityti.

Nepaisant visų apsisaugojimų, vieną kartą šiai įmonei teko atrasti saugumo spragas, kai buvo susidūrę su virusu, kuri naikina duomenys sistemos viduje. Tačiau nepaisant viruso padarytos žalos,

nuostolių pavyko išvengti visada daromos dokumentų bei duomenų kopijos, kurios leido atstatyti savo programą. Šis virusas buvo „pagautas“, dėl netikslingai darbuotojo naudojamo interneto. Todėl nuo to laiko darbuotojai turi minimalias privilegijas naudojantis kompiuterį bei įmonės duomenis, bei priėjimą prie duomenų.

4.3. Įmonės X jos elektroninių finansinių atsiskaitymų būdai ir apsaugos priemonės

Prieš dešimtmetį buvo įkurta kanceliarinių prekių ir verslo dovanų įmonė X. Laikui bėgant ši įmonė plėtėsi, atidarė ne vieną savo filialą skirtinguose miestuose ir, galiausiai, 2005 metais, naudojantis naujomis technologijomis ir naujomis galimybėmis sukūrė savo e.parduotuvę. Ši įmonė platina garsių gamintojų kokybiškas bei nekasdienes prekes, todėl viena iš geriausių reklamų ir pardavimo būdų yra prekyba internetu. Tai leidžia žmonėms ir įmonėms įsigyti prekes neišėjus iš namų sutaupant laiko. Tačiau bendradarbiaujant internetu su klientu būtina jautrių duomenų apsauga ir apsauga nuo kenkėjiškos programinės įrangos.

Šios įmonės e.parduotuvė veikia jau seniai, ja naudojasi apie 2000 žmonių per mėnesį, šie žmonės jau yra prisiregistravę prie svetainės ir visada naudojasi paprastu ir patogiu būdu apsipirkti. Tačiau ne tik seniau prisiregistravę asmenys gali naudotis šios parduotuvės duomenimis, naujiems klientams norint pradėti naudotis, tereikia prisiregistruoti, nurodant vardą, pavardę, tikslų adresą, kontaktinius numerius ir pan. Užsiregistravęs žmogus jau gali pirkti parduotuvėje virtualiai.

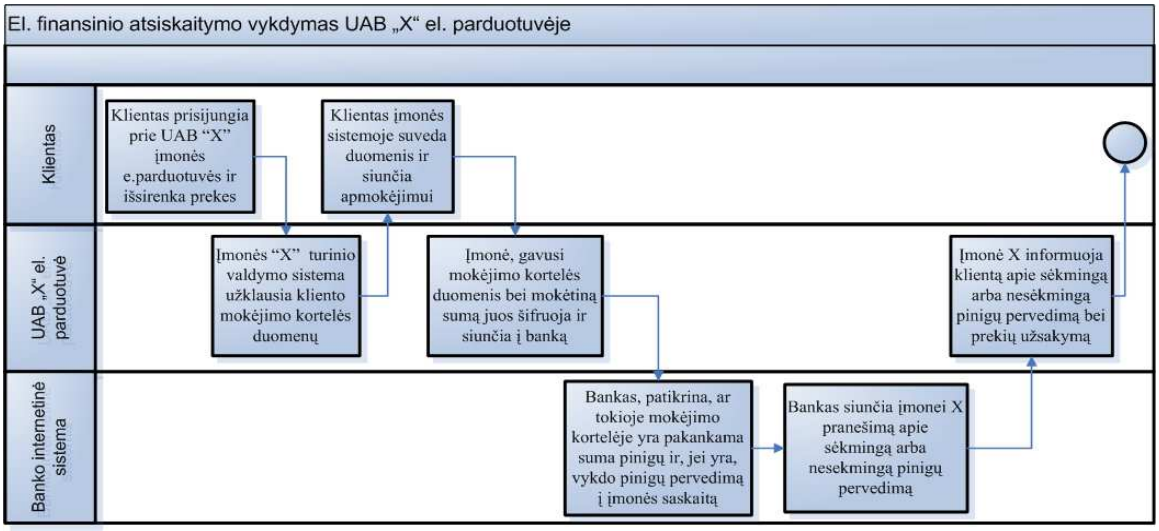
Ši e.parduotuvė buvo sukurta naudojant vieną iš daugelio esamų turinio valdymo sistemų. Pagal save ši įmonė pakoregavo turinio valdymo sistemą, pakeitė modulius finansiniams atsiskaitymams, kad būtų tinkamiausi jų e. parduotuvei. Tokia turinio valdymo sistema buvo pasirinkta todėl, kad ji palaiko HTTPS protokolą. Taip pat ši turinio valdymo sistema palaiko daug būtinų saugumo reikalavimų, tokių kaip autentiškumo patvirtinimas, autorizacija, konfidencialumas, vientisumas, minimalios darbuotojų privilegijos, sistemos nesudėtingumas, paprastumas, audito įrašų registravimas, internetinių standartų naudojimas. Vadovas teigė: „Mes esame patenkinti, nes nei karto neteko susidurti su kažkokias mėginimais įsilaužti, virusais ir panašiai. Taip pat, tai nesudėtingas apmokėjimo ir prekių užsakymo būdas. Mes sutaupome ne tik laiko kontaktuodami, bet ir pinigų.“

Veikimo principas yra paprastas:

- Vartotojas užsiregistruoja e.parduotuvės tinklalapyje, suvesdamas būtiniausius duomenis apie save;
- Klientas turi galimybę vaikščioti virtualiai po parduotuvę ir rinktis prekes, kurias jis įdėtų į užsakymų krepšelį;

- Sudėjus visas prekes klientas pasirenka krepšelį ir pasitikrina, ar viskas yra krepšelyje ko jam reikia;
- Išsirinkęs ir sutikrinęs prekes klientas spaudžia mygtuką „UŽSAKYTI“ ir yra nukreipiamas prisijungti prie jau turimos paskyros, arba ten užsiregistruoti.
- Paprašoma patikslinti kokiu adresu turi būti pristatomos prekės;
- Prašoma įvesti kokias nors pastabas apie pristatymą, pristatymo laiką ir pan.;
- Tada vartojas pasirenka mokėjimo būdą, ar jis mokės mokėjimo banko kortele, ar grynaisiais pinigais atsiimant prekę;
- Klientui įvedus savo mokėjimo kortelės duomenis, jie siunčiami sistemai ir sistema šiuos duomenis siunčia užklausai į banką, kad būtų nuskaitomi pinigai nuo to žmogaus sąskaitos;
- Kai sugrįžta iš banko atsakymas, kad pinigai yra nuskaityti nuo pirkėjo sėkmingai, sistemos pirkėjui yra išsiunčiamas patvirtinimas į elektroninį paštą apie sėkmingą prekių užsakymą;

Kliento prekių pasirinkimą bei už prekes atsiskaitymą elektroniniu būdų galima pateikti schemoje (žr. 10 pav.).



Šaltinis. Sudaryta autorės.

10 pav. **Kliento prekių užsakymo bei apmokėjimo schema UAB „X“ turinio valdymo sistemoje**

Visi duomenys, kurie yra siunčiami į banką, ar vartotojo duomenys į sistemą yra šifruojami. Duomenų siuntimui ir šifravimui sistema yra susieta su VAM technologija, kuri leidžia užtikrinti duomenų nepasiekiamumą pašaliniams asmenims. Į šios įmonės saugumą niekas nebuvo pasikėsinęs, tačiau įmonės duomenys visada yra kopijuojami kas mėnesį, taip pat atliekami saugumo testai ir atnaujinimai karta į pusmetį. Duomenims apsaugoti yra diegiamos kompiuteriuose antivirusinės programos bei ugniasienės. Įmonė nesutiko atskleisti kokias dar papildomas apsisaugojimo priemones naudoja, tačiau pabrėžė, kad šios sistemos ir jų kompiuterių saugumas yra svarbus, nes juose saugoma

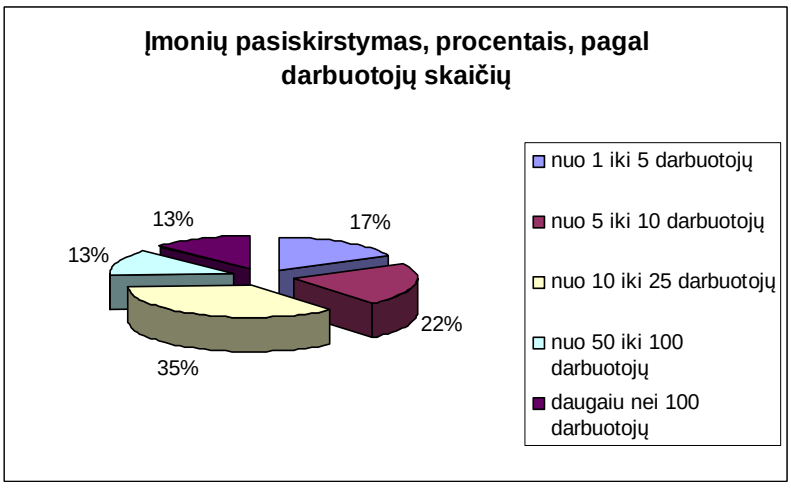
jautri informacija, kuri gali pakenkti ne tik vartotojams, kurie naudojasi šios įmonės paslaugomis, bet ir įmonei atnešti didelių nuostolių.

4.4. Įmonių elektroninių finansinių atsiskaitymų saugumo tyrimo rezultatai ir analizė

Atliktame kiekybiniame tyrime, kuris buvo atliktas sudarius anketa ir siunčiant ja anonimiškai respondentams, buvo sulaukta 46 respondentų atsakymų, nors išsiųsta anketų buvo per 300-tams įmonių. Toks didelis skirtumas siųstų bei atsakytų laiškų yra todėl, kad dažna įmonė nesutinka paviešinti jautrios informacijos net ir anonimiškai.

Anketa buvo sudaryta iš 20 klausimų, visi anketoje pateikti klausimai yra esminiai ir atspindi su įmonės e. finansiniais atsiskaitymais susijusius duomenis. Ši anketa pateikta pirmajame priede. 1-2 kausimai yra skirti išsiaiškinti kokio dydžio yra įmonė ir kokia veikla ji užsiima, 3-4 klausimai skirti išsiaiškinti įmonės atsiskaitymo būdus bei per ką jie yra vykdomi. 5-6 klausimai skirti nurodyti, kas naudojasi atsiskaitymo sistema ir, jei tai vartotojai, tai koks srautas vartotojų ja naudojasi. 7 klausimas skirtas sužinoti, ar kas nors prižiūri įmonės finansinių atsiskaitymų sistemas bei kompiuterius. Toliau dėmesys skiriamas sistemų įsilaužimams. 8-11 įmonėms klausimai pateikiami klausimai apie saugumo standartus bei reikalavimus. Kaip dažnai kopijuojami duomenys, ar testuojamas sistemų saugumas 12-19 klausimai. Paskutinis klausimas nurodo kiek pinigų įmonės skiria sistemų saugumui.

Pagal pateiktą anketą atsakė 46 įmonės iš jų 16 yra vidutinio dydžio, kuriose dirba nuo 10 iki 25 darbuotojų. Jos buvo pačios aktyviausios, o mažiausiai buvo gauta atsakymų iš mažesnių įmonių.

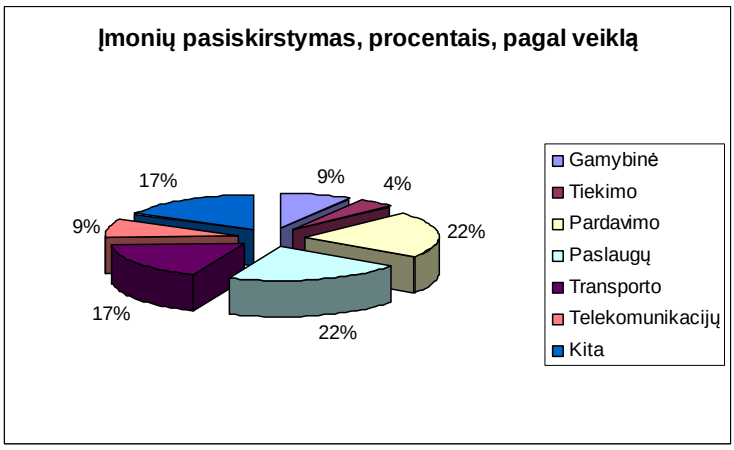


Šaltinis. Sudaryta autorės.

11 pav. **Įmonių pasiskirstymas pagal dydį**

Dar svarbu, kokios įmonės sutiko atsakyti apie savo įmones finansinių atsiskaitymų saugumą, kokios įmonės kokį saugumą taiko savo sistemose. Taigi 12 paveikslėlyje pateikta diagrama, kuri

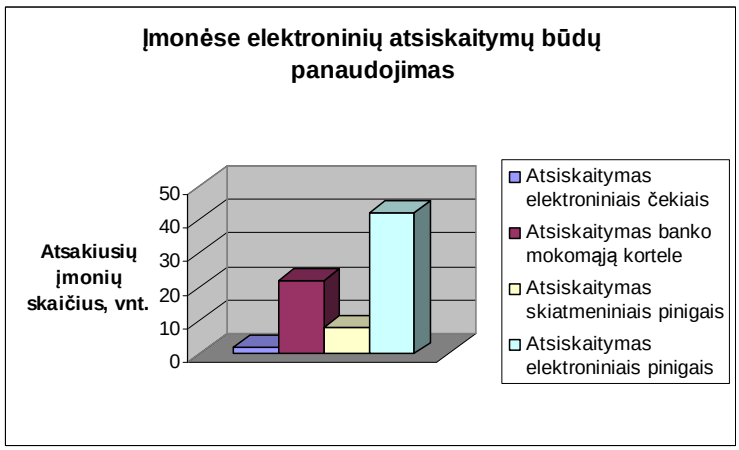
parodo įmonių veiklos sritis. 21,7 % įmonių yra pardavimo ir paslaugų, nedaug atsiliko transporto įmonės ir kitos. Kitos įmonės, kurios nebuvo pateiktos sąraše buvo informacinių technologijų bei administracinę veikla užsiimančiomis įmonėmis.



Šaltinis. Sudaryta autorės.

12 pav. **Įmonių užsiimančios veiklos diagrama**

Šiuo metu yra išskiriami keli e. finansiniai atsiskaitymai, nuo kurių priklauso ir sistemos, kurios yra naudojamos įmonėse. Sistemų naudojimas įtakoja vartotojų bei klientų pasitikėjimą, nes dauguma klientų domisi, kokiu būdu bus atsiskaitoma, kaip bus saugomi duomenys ir pan. Pasak Sauliaus Pakrijausko, kuris savo straipsnyje “Saugus atsiskaitymas internete”, teigė, kad yra svarbu patikrinti, kokias saugumo technologijas naudoja pardavėjas. Jeigu duomenys išsaugomi jo individualioje duomenų bazėje, o vėliau persiunčiami el. paštu ar faksu, tai netgi saugiai pateikti duomenys gali būti perimti. Apklaustosios įmonės daugiausiai pasisakė naudojančios atsiskaitymus e.pinigais 91,3 % bei beveik pusė (t.y. 47,8 % apklaustųjų) įmonių taip pat dar naudoja mokėjimo korteles.

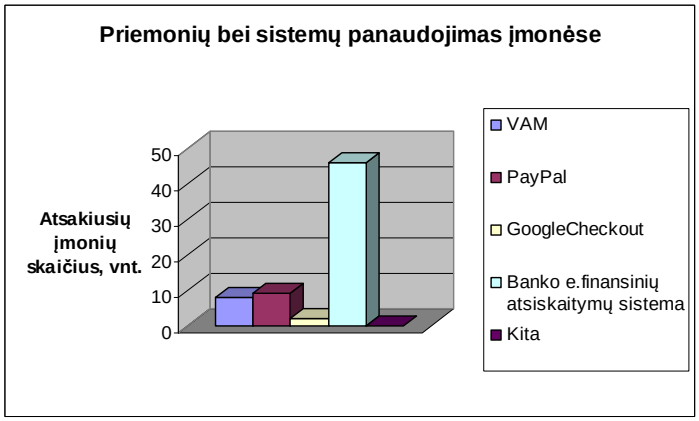


Šaltinis. Sudaryta autorės.

13 pav. **Elektroninių atsiskaitymo būdų panaudojimas**

Apklaustosios įmonės pasisakė daugiausiai (t.y. visi 100 % apklaustų įmonių) naudojančios banko e. finansinių atsiskaitymų sistemas, tik kelios dar pasisakė už kitokias finansinių atsiskaitymų

sistemas, nes, kaip matoma iš duomenų, yra įmonių, kurios naudoja ne vieną finansinių atsiskaitymų sistemą (žr. 14 pav.).



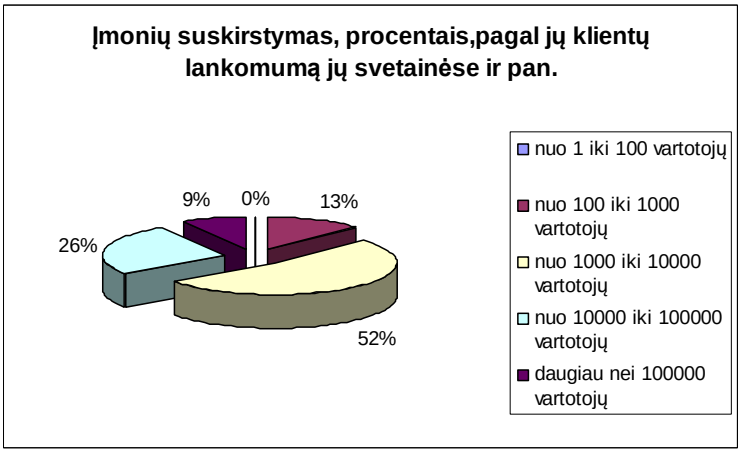
Šaltinis. Sudaryta autorės.

14 pav. **Įmonių naudojamos saugos priemonės bei sistemos vykdyti e. atsiskaitymus**

Lietuvoje nėra populiarus trečiųjų šalių atsiskaitymo būdas. Užsienyje naudojimasis kitokiais nei banko sistemomis atsiskaitymo būdais yra populiarūs, kaip PayPal ar jo konkurentinė sistema Google Checkout. Pagal internetinio puslapio „http://ltforum.destinysphere.net“ darytą apklausą „Ar reikalinga PayPal sistema (žr. 15 pav.)?“ Beveik 56 % apklaustųjų atsakė, kad jiems užtenką ir bankinės sistemos. Todėl ir daugiausiai įmonių taiko klientui prieinamas sistemas, kuriomis klientas atsiskaitydamas jaustųsi gerai ir vėl norėtų grįžti pas juos [28].

15 pav. PayPal sistemos reikalingumo įvertinimas

Įmonių pateiktais duomenimis, net 78,3% e. finansinės atsiskaitymo sistemos yra skirtos plačiam ratui vartotojų, todėl būtina pateikti paprastą ir lengvą atsiskaitymo būdą bei saugoti duomenis, nes, esant daug vartotojų, reikia didelės apsaugos, kad nebūtų įsilaužimų, ar kitokios nusikalstamos veiklos. Dauguma įmonių (52,2 %) pasisakė, kad jų sistema per mėnesį pasinaudoja nuo 1000 iki 10000 (žr. 16 pav.). Kuo daugiau vartotojų tuo didesnė tikimybė, kad klientai perduos virusus, ar pan. Taip pat 47,8 % įmonių sistemomis naudojasi patys įmonės darbuotojai.

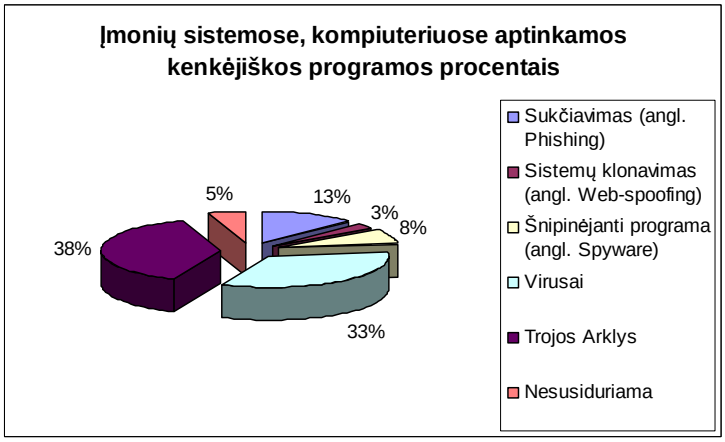


Šaltinis. Sudaryta autorės.

16 pav. **Įmonių sistemų lankomumas per mėnesį**

Kadangi daug žmonių naudojasi sistemomis, ne tik įmonės darbuotojai, bet ir tūkstančiai vartotojų, reikalingas žmogus, kuris būtų atsakingas už įmonės sistemų bei kompiuterių saugumą. 65,2% respondentų teigė, kad jie turi specialistus, kurie atsakingi už sistemų saugumą, kiti, likę 34,8%, neturi tokio specialisto bet atsižvelgiant į prieš tai buvusius rezultatus 18 iš apklaustųjų įmonių yra mažos, kuriose dirba nuo 1 iki 10 vartotojų, todėl jiems ir nesamdo žmogaus, kuris visą laiką prižiūrėtų sistemą, kuria naudojasi minimalus skaičius vartotojų.

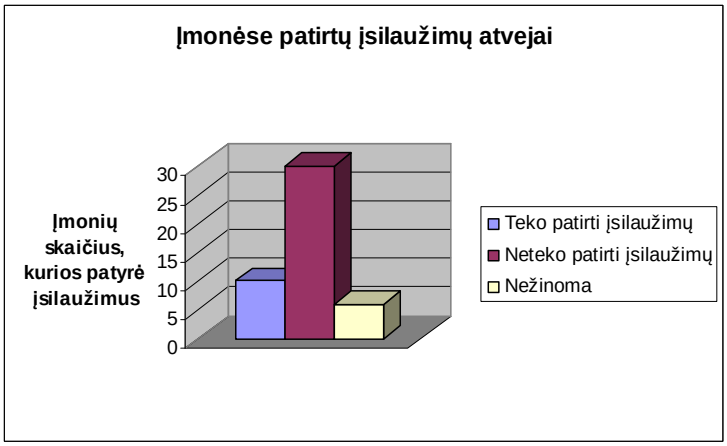
Atkreipiant dėmesį į grėsmes kylančias įmonėms naudojančioms atsiskaitymų sistemas, taip pat laikančias informaciją savo kompiuteriuose, kyla pavojus ne tik užkrėsti informaciją piktybinės įrangos daromomis žalomis, bet klientui gali kilti galimybė būti apgautam jį nukreipus ne pas pardavėją. Taigi klausiam įmonių, su kokia saugumo rizika ir faktoriais jos susiduria. Net 65,2% įmonių yra susidūrusios su „Trojos arkliu“, taip pat neatsilieka ir įvairūs virusai - tai 56,5% apklaustų įmonių. Keturios iš atsakiusių įmonių dar niekada nėra susidūrusios su šia saugumo rizika. Kiti saugumo faktoriai, kaip sukčiavimas, sistemų klonavimas, šnipinėjanti programa dar nėra paplitusios Lietuvoje, todėl ir tenka susidurti mažiau.



Šaltinis. Sudaryta autorės.

17 pav. **Rizikos faktoriai su kuriais dažniausiai susiduria įmonės**

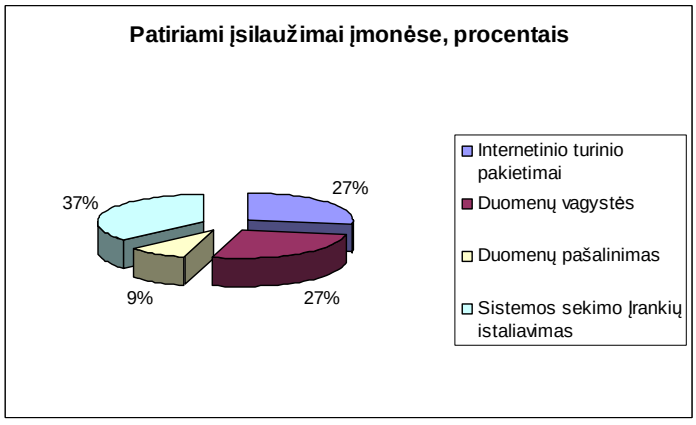
Respondentams buvo užduodamas klausimas apie tai, ar buvo, nepaisant virusų, ar kitokių piktybinės įrangos darinių, bandyta įsilaužti į įmonės naudojamą e. finansinių atsikaitymų sistemą (žr. 18 pav.) Daugiau nei pusė apklaustų įmonių dar neteko patirti tokių įsilaužimų. O įmonės, kurioms teko patirti tokius bandymus įsilaužti, iš jų 8 patyrė nuo 1 iki 5 įsilaužimų, o dar dvi įmonės patyrė net iki 10-ties bandymų įsilaužti.



Šaltinis. Sudaryta autorės.

18 pav. **Įmonėse įsilaužimo duomenys**

Paklausus, kokie buvo tie įsilaužimai, respondentai atsakė tokius, kaip sistemos sekimo įrankių instaliavimo, duomenų vagystės, interneto puslapio pakitimai bei duomenų šalinimas (žr. 19 pav.). Šie įsilaužimai yra pavojingi, nes šių įsilaužimų padariniai gali būti tokie, kaip klientų nepasitikėjimas, didelių pinigų praradimai. Dėl tokių dalykų ir reikia naudotis visais saugumo reikalavimais.

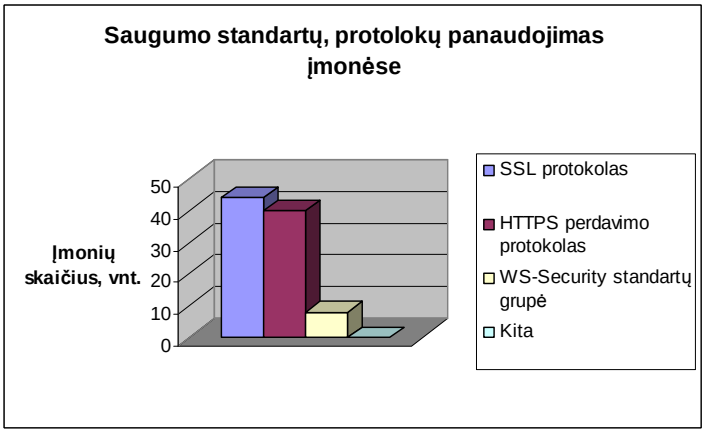


Šaltinis. Sudaryta autorės.

19 pav. **Įmonių įsilaužimų būdai bei pagal tipus jų dažnumas**

Apžvelgus įsilaužimus bei rizikos komponentes, reikia apžvelgti, kas yra daroma įmonėse, kad būtų išvengiami susidūrimai su įsilaužimais bei piktybinėmis įrangomis. Svarbu apžvelgti, kokius saugumo standartus bei saugumo protokolus naudoja apklausiamos įmonės (žr. 20 pav.). Dauguma įmonių pasisakė naudojančios SSL protokolą, kurį prieš tai analizavome teorinėje dalyje. Tai vienas iš svarbiausių protokolų, kurio dėka duomenys yra šifruojami. Taip pat tos pačios įmonės, kurios naudoja SSL protokolą, pasisakė naudojančios taip pat saugumo standartą bei protokolą HTTPS, nes jo dalis ir

yra SSL protokolas. Tik kelios įmonės pasisakė naudojančios WS-Security standartų grupę, nors dar viena skiltis buvo įmonėms, kad pateiktų kokius dar saugumo standartus naudoja, tačiau keli respondentai pateikė pastabas, kad didesnių duomenų nenori pateikti, dėl vidinės įmonės saugos. Todėl šiose srityse, kaip saugumo standartai bei reikalavimai yra vienas iš jautriausių klausimų, kuriuos įmonės stengėsi atsakinėti atsargiai.



Šaltinis. Sudaryta autorės.

20 pav. **Saugumo standartų bei protokolų panaudojimas įmonėse**

Toliau analizuojant, kokiu būdų įmonės saugo savo sistemas bei kompiuterius nuo įsilaužimų reikia apžvelgti kokias saugumo priemones tam taiko. Nes įmonės viduje turi buti įdiegtos tam tikros sistemos, priemonės, kad būtų užtikrinamas saugumas, t.y. antivirusinės programos, ugniasienės, saugus serveris, duomenų kopijos, duomenų kodavimas. Šie dalykai yra būtini, jei yra pažeidžiami duomenys, apsisaugojimui nuo pašalinių žmonių prisijungimo ir pan. Lietuvos statistikos departamentas 2008 metais pateikia statistiką, kurioje pateikiama procentais elektroninė sauga ir naudojamos priemonės įmonėse.

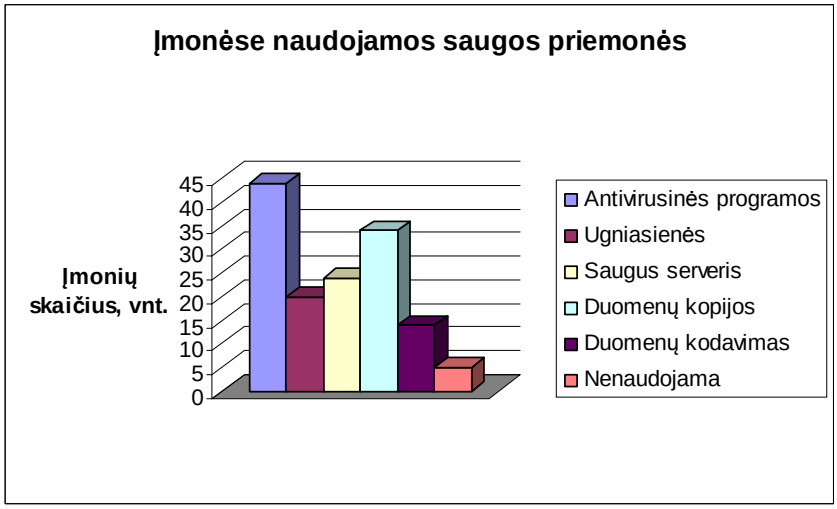
Analizuojant naudojamas įmonių, kurios atsakė į anketos klausimus, priemones matyti, kad kelios priemonės nuo 2008 metų yra kitokios. Antivirusinės programos bei ugniasienės nedaug nuklysta savo procentiniais duomenimis nuo 2008 metų, tačiau tokie dalykai kaip duomenų kodavimas, duomenų kopijos, bei saugus serveris yra ženkliai pasikeitė rodikliai, šie dalykai šiuo metų yra daug daugiau į juos kreipiama dėmesio. Teigti šimtą procentų negalime, nes atsakiusių įmonių yra tik 46, todėl atsiranda netikslumo paklaida vertinant ir lyginant šiuos duomenis. Nors atkreipiant dėmesį į ankstesnius metus, galima pastebėti, kad kiekvienais metais, kai kurios sritys po truputį auga. Kiekvienais metais vis dažniau atsiranda naujų piktybinių įrangų ir vis dažniau sistemas reikia atnaujinti bei diegti naujus sistemos apsisaugojimo būdus.

1. lentelė. Elektroninė sauga ir naudojamos priemonės įmonėse

	2004	2005	2006	2007	2008
Naudoja elektroninės saugos priemones	**93,6**	**92,7**	**94,3**	**94,9**	**95,2**
Antivirusinės programos	86,6	88,0	89,6	89,8	91,8
Ugniasienės	25,1	30,9	34,1	37,2	40,4
Saugus serveris	29,0	22,3	27,8	28,9	33,4
Duomenų kopijos	39,0	40,3	44,3	47,3	48,0
Duomenų kodavimas	11,1	10,1	11,3	11,8	18,6
Turėjo elektroninio saugumo problemų	**37,4**	**40,2**	**39,9**	**39,3**	**...**

„...“ - nėra duomenų, nors toks reiškinys (rodiklis) atitinkamu laikotarpiu buvo.

Šaltinis. Lietuvos statistikos departamentas prie Lietuvos Respublikos Vyriausybės.



Šaltinis. Sudaryta autorės.

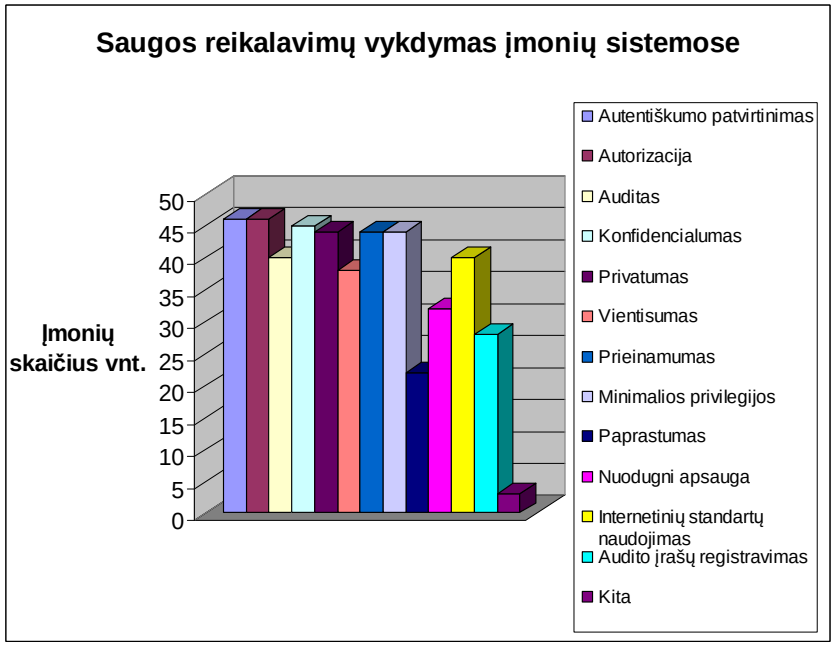
21 pav. **Saugumo užtikrinimui naudojamos saugumo priemonės verslo įmonės viduje**

Analizuojant toliau įmonės saugumo taikymą e. finansiniuose atsiskaitymuose svarbiausias dalykas yra, kokie saugos reikalavimai yra vykdomi įmonėse ir kokią įtaką jie daro. 22 paveikslėlyje yra pateikiami visi standartai, kurie yra naudojami įmonės viduje, stengiantis apsaugoti įmonės ir kliento svarbius duomenis bei apsisaugoti nuo piktybiškų programų bei įsilaužimų.

Dauguma įmonių, t.y. visos 100%, pasisakė už tai, kad yra naudojančios priemones, apsaugančias konfidencialumą, autentiškumo patvirtinimą, autorizaciją, internetinių standartų naudojimą bei audito įrašų registravimą. Tačiau ne tik šitie reikalavimai yra patys svarbiausi, svarbūs yra visi reikalavimai, nes niekada nėra žinoma, su kokia rizika gali susidurti, nors taip pat reiktų

atsižvelgti ir į reikalavimų naudojimą. Taigi ne visoms įmonėms reikalingi visi išvardinti reikalavimai, nes atsiskaitymų sistemos elektroninėje erdvėje yra skirtingos, dėl to ir atskirų reikalavimų vykdymai įmonėse gali skirtis. Kas bus būtina vienai įmonei, kitai įmonei gali būti visai neaktualu.

Žvelgiant į pateiktą diagramą matyti, kad įmonės ne visos pasisakančios už paprastumą, tačiau ne visos įmonės ir gali leisti sau paprastumą, dėl jau esamų ir įdiegtų sistemų. Tačiau visi kiti parodymai rodo, kad apklaustos įmonės daug naudojančios saugos reikalavimų, todėl ir parodymai dėl įsilaužimų yra geri, nes tik de6imt įmonių yra susidūrusios su įsilaužimais. Virusų bei piktybinės įrangos rodikliai yra žymiai didesni, tačiau ir jie yra dažnesni bei stipriai platinami.



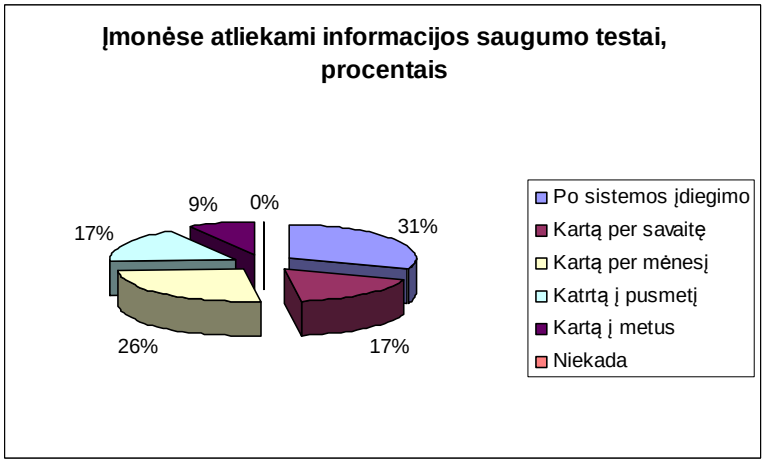
Šaltinis. Sudaryta autorės.

22 pav. **Saugos reikalavimai, kurie yra taikomi įmonėse**

Taip pat net 73,9% apklaustų įmonių teigė, kad pas juos yra įdiegtas sistemos atstatymo mechanizmas sistemos klaidos, ar perkrovimo (”nulūžimo”) atveju, nes sistemos klaida ar tyčinis sistemos perkrovimas gali padaryti nepataisomos žalos. Vėlgi, tai priklauso ir nuo sistemos. Tačiau daugumai sistemų toks mechanizmas yra būtinybė. Taip pat 73,9% įmonių pasisakė, kad duomenų kopijavimas pas juos atliekamas kasdien, kitos įmonės teigė tai darančios kartą per savaitę, dar kitos kartą į mėnesį. Įmonių, kurios tai atliktų kartą į pusmetį ar metus neatsirado, nes tokių duomenų kaita yra didelė ir, jei kopijos bus daromos retai, tai gali ir neišgelbėti tų duomenų.

Analizuojant įmonės e. finansinių atsikaitymų saugumo reikalavimų vykdymą yra svarbu tikrinti, ar viskas funkcionuoja taip, kaip turėtų. Todėl buvo užduotas klausimas, kaip dažnai yra vykdomi saugumo testai sistemose (žr. 23 pav.). 30,4% įmonių pasisakė, kad testai atliekami iš kart po sistemos įdiegimo, 26,1% teigė, tai atliekantis kartą per mėnesį, po 17,4% atsakė tai atliekančios kartą per savaitę. Kitos kartą į pusmetį, visos likusios kartą į metus. Tokie testai parodo, kad dauguma įmonių

daro juos dažnai tikrindami, ar reikia kurią nors sistemos vietą saugoti papildomomis priemonėmis, kurios užtikrintų visapusišką sistemos saugumą.



Šaltinis. Sudaryta autorės.

23 pav. **Įmonėse atliekamų informacijos saugumo testų dažnumas**

Dauguma įmonių taip pat naudoja bankines e. finansinių atsiskaitymų sistemas, arba naudoja savas sistemas taip pat susietas su bankinėmis sistemomis. Visi pinigai vis tiek galiausiai keliauja per banką, todėl ir buvo užduodamas klausimas įmonėms, ar jos yra kada susidūrusios su bankinės atsiskaitymų sistemos klaidomis ar saugumo spragomis? Visos apklaustos įmonės vienareikšmiškai atsakė, kad joms neteko susidurti su tokiomis saugumo spragomis.

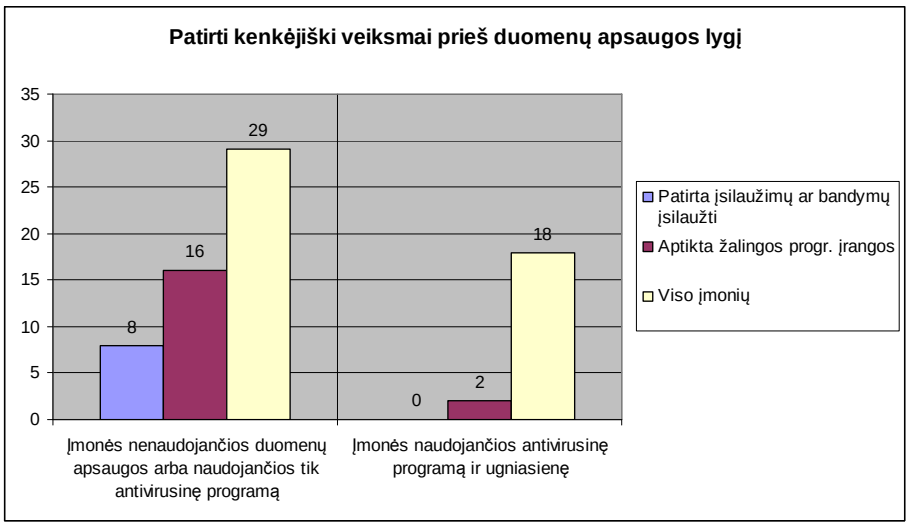
Toliau kalbant apie saugumo reikalavimų vykdymą viskas susiveda į tai, kiek įmonė gali sau leisti palaikyti sistemų saugumą. Apklausos metu keturios įmonės pasisakė, kad jie saugumo užtikrinimui skiria 1000 litų, dar keturios įmonės teigė skiriančios 100000 litų, o visos likusios skiria po 10000 litų. Taigi iš rezultatų matyti, kad dauguma įmonių skiria 10000 litų metams ir tai nepriklausomai nuo įmonių dydžio, nes sistema yra viena ir jai apsaugoti yra naudojamos tos pačios piniginės sumos.

4.5. Apklaustų įmonių rezultatų lyginamoji analizė

Šiame skyriuje atliksime atskirų įmonių apklausos rezultatų lyginamąją analizę ir įvertinsime įmonių patiriamų įsilaužimų priklausomai nuo apsisaugojimo priemonių kiekius, kokio tipo įmonės kreipia didžiausią dėmesį į savo duomenų saugą ar kaip priklauso įmonių duomenų saugumas nuo saugai skiriamų lėšų.

Pirmiausia išanalizuosime labiausiai pažeidžiamus dalykus, tai yra įsilaužimai į įmonių internetines sistemas. Tyrimas parodė, kad daugiausiai bandymų įsilaužti ar įsilaužimų patyrė tos įmonės, kurios arba apskritai nenaudojo jokių interneto sistemų apsisaugojimo priemonių arba naudojo jų nepakankamai. Sekančiame grafike matosi, kad daugiausiai – net 8 iš 10 įmonių, nenaudojančių

arba naudojančių tik antivirusinę apsaugą (44) yra tekę patirti įsilaužimų ir net 18 įmonėms, kurios naudoja geriausią apsisaugojimo būdą, tai yra antivirusinė programa ir ugniasienė, neteko patirti įsilaužimų išvis. Panašūs duomenys gauti ir dėl aptiktos žalingos programinės įrangos. Daugiausiai jos aptiko įmonės nenaudojančios ugniasienės ir antivirusinės programos „dueto“ – 16. Ir tik 2 įmonės aptiko tokią programinę įrangą naudojančios ugniasienę.



Šaltinis. Sudaryta autorės.

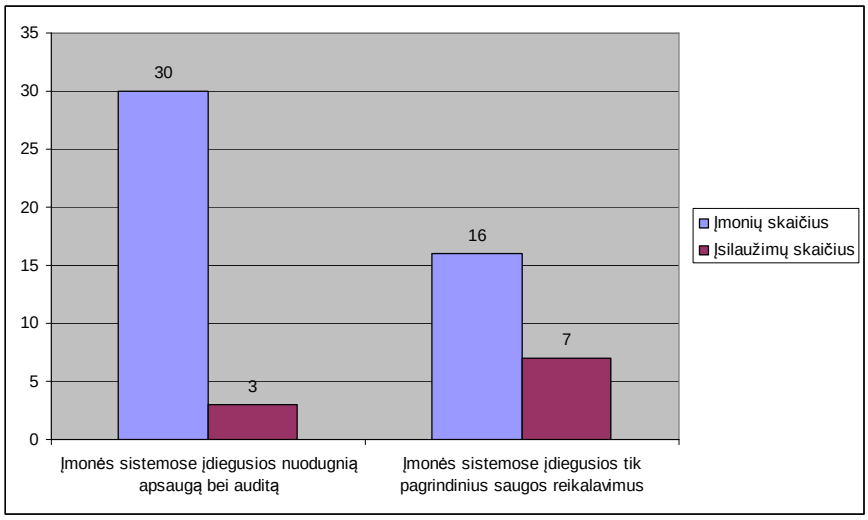
24 pav. **Patirti kenkėjiški veiksmai lyginant su turimu duomenų apsaugos lygiu**

Apskaičiavę įmonių patirtų įsilaužimų ir atrastos kenkėjiškos programinės įrangos atvejų dažnumą priklausomai nuo nepakankamo apsaugos lygio koreliaciją, iš gauto rezultato - ~0,422 pastebėtume, kad šie du dydžiai koreliuoja. Koreliacijai apskaičiuoti buvo pasirinktas Pearsono koreliacijos koeficientas, kuris buvo apskaičiuotas naudojant Microsoft “Excel” programos Pearsono statistinę funkciją. Koreliacija buvo skaičiuojama imant Array1 – „Patyrė įsilaužimą arba aptiko kenkėjišką programinę įrangą“ ir Array2 – „Neturi įdiegtos antivirusinės programos ir ugniasienės“ (žr. priedas 2).

Nustatyti ar buvo nelegaliai perimti duomenys jų neužkodavus juos siunčiant internetu praktiškai neįmanoma, nes joks nusikalstamą veiką darantis asmuo to nepaviešins.

Tačiau galima tiksliai nustatyti kaip įsilaužimai į sistemas priklauso nuo sistemose realizuojamų saugos reikalavimų kaip autorizacija, konfidencialumas, prieinamumas ir pan. Išanalizavę rezultatus nustatėme, kad labiausiai sėkmingų įsilaužimų statistiką įtakoja „Nuodugnios apsaugos“ ir sistemos „Audito“ nepakankamumas. Kadangi dauguma atsakiusių įmonių užtikrina esminius saugumo reikalavimus kaip autorizacija ir autentikacija, šie rodikliai nepasako kokią įtaką tai daro įsilaužimams. Vis dėlto savaime aišku, kad neįvykdžius šių pagrindinių reikalavimų sistema tiesiog negalėtų funkcionuoti iš esmės.

Sekančiame grafike parodytas sistemų įsilaužimų kiekis priklausomai nuo to ar įmonė yra įdiegusi nuodugnią apsaugą ir auditą.



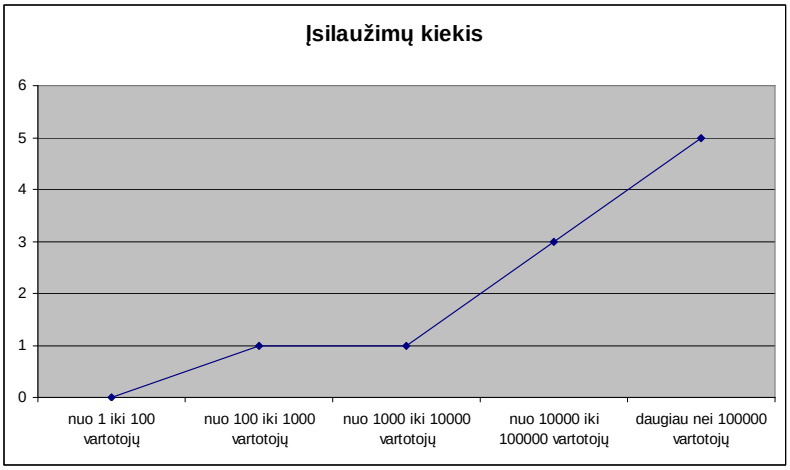
Šaltinis. Sudaryta autorės.

25 pav. **Įsilaužimų kiekis priklausomai nuo saugos reikalavimų įdiegimo sistemose**

Matome, kad įmonės įdiegusios visus saugos reikalavimus įskaitant nuodugnią apsaugą bei auditą patyrė tik 3 įsilaužimus, kai įmonės įdiegusios tik pagrindinius saugos reikalavimus net 7 iš 10.

Paskaičiavus šių dydžių Pearsono koreliaciją gavome -0,474 (žr. priedas 2). Tai rodo, kad šie dydžiai koreliuoja priešingai. Tai parodo, kad įmonės įsidiegusios visus saugos reikalavimus nepatiria įsilaužimų arba patiria kur kas mažiau nei tos, kurios turi įsidiegę tik pagrindinius saugos reikalavimus minėtus aukščiau.

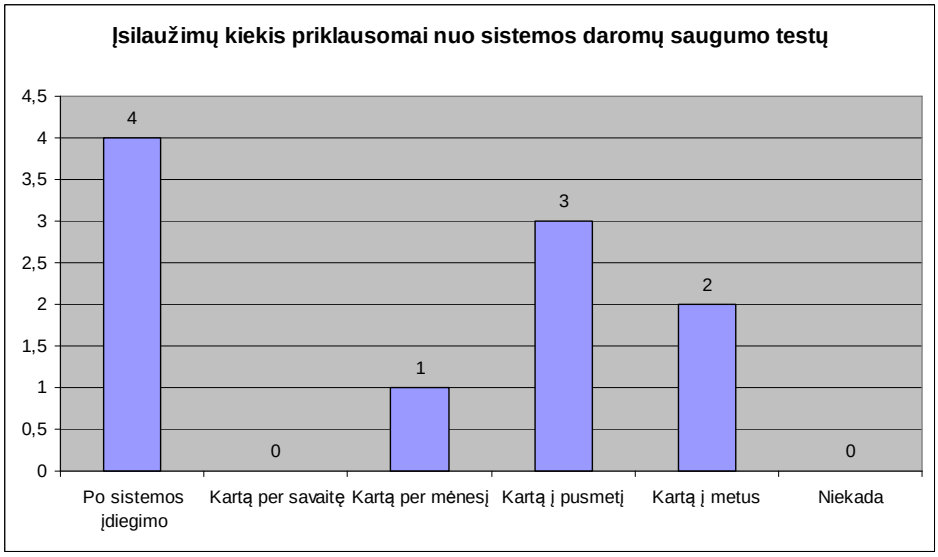
Analizės metu taip pat buvo nustatyta, kad daugiausiai bandymų įsilaužti ir įsilaužimų yra tekę patirti įmonėms, kurių internetinėmis sistemomis naudojasi daugiausiai vartotojų. Tai logiškai galima paaiškinti, kadangi kuo daugiau vartotojų naudojasi sistema, tuo ji yra žinomesnė, tuo daugiau konfidencialių duomenų joje saugoma, tuo daugiau veiksmų sistemoje yra atliekama ir įsilaužimo bandymus yra sunkiau pastebėti. Žemiau pateiktame paveikslėlyje matome, kad daugiausiai tokių atvejų yra nutikę daugiausiai vartotojų aptarnaujančioms sistemoms – 5. Mažiausiai – mažesnius vartotojų srautus aptarnaujančioms sistemoms.



Šaltinis. Sudaryta autorės.

26 pav. Įsilaužimų kiekis priklausomai nuo vartotojų srauto

Dar vienas svarbus faktorius, reikšmingai lemiantis internetinių sistemų saugumą yra nuolat ir periodiškai atliekami saugumo testai bei atnaujinama saugumo programinė įranga. Pasižiūrėjus į įmonių atsakymus galima teigti, jog mažiausiai įsilaužimų ir kenkėjiškos programinės įrangos aptikimų patyrė įmonės dažniausiai atliekančios tokius testus. Pavyzdžiui, iš 4 įmonių, kurių internetines sistemas aplanko daugiau nei 100000 vartotojų 2 įmonėms, kurios saugumo testus atlieka kartą į savaitę ar dažniau pavyko išvengti bandymų įsilaužti, o likusios 2 patyrė net 5 tokius bandymus.



Šaltinis. Sudaryta autorės.

27 pav. **Įsilaužimų kiekis priklausomai nuo sistemos daromų saugumo testų**

Tai aiškiai parodo, kaip svarbu yra nuolat atnaujinti savo saugumo programinę įrangą bei atlikti saugumo testus.

4.6. UAB „Baltjuta“ ir Įmonės X rezultatų palyginamoji analizė su kitomis anonimišku būdu apklaustomis įmonėmis

Šiame skyriuje bus nagrinėjama apklaustųjų įmonių rezultatai su UAB „Baltjuta“ ir įmonės X pateiktais rezultatais. Kadangi įmonėms svarbiausias yra saugumas, tai ir palyginsiu saugumo priemones naudojamas įmonėse bei palaikomus saugos standartus, kurie naudojami e. finansiniuose atsiskaitymuose.

Žemiau pateiktoje lentelėje yra pateikiami abiejų apklaustų įmonių duomenys bei apibendrintai pateikiami anonimiškai apklaustų įmonių rezultatai. Anonimiškai apklaustų įmonių rezultatai pateikiami tie, kurie buvo daugiausiai naudojami visose, t.y. tie kurie daugiausiai surinko procentų.

2 lentelė. Įmonių saugumo priemonių ir saugos reikalavimų palyginamoji lentelė

	UAB „Baltjuta“	Įmonė X	Apklaustosios įmonės
Kokias elektronines finansines atsikaitymo sistemas technologijas naudoja įmonė			
VAM		+	
PayPal			
Google Checkout			
banko elektroninių finansinių atsiskaitymų sistema	+	+	+
kita			
Kokie saugumo standartai įdiegti įmonės finansinių elektroninių atsiskaitymų sistemose			
SSL protokolas	+	+	+
HTTPS perdavimo protokolas	+	+	+
WS-Security standartų grupė			
kita			
Kokias saugumo priemones naudoja elektroninių finansinių atsiskaitymų sistemos saugumui užtikrinti			
antivirusinės programos	+	+	+
ugniasienės	+	+	
saugus serveris			
duomenų kopijos	+	+	+
duomenų kodavimas	+	+	+
kita			
nenaudojame			
Kokie saugumo reikalavimai palaikomi įmonės elektroninių finansinių atsiskaitymų sistemose			
autentiškumo patvirtinimas	+	+	+
autorizacija	+	+	+
auditas			
konfidencialumas	+	+	+
privatumas			+
vientisumas		+	+
prieinamumas	+		+
minimalios privilegijos	+	+	+
paprastumas	+	+	
nuodugni apsauga			+
internetinių standartų naudojimas	+	+	+
audito įrašų registravimas		+	+
kita			
Ar įmonės elektroninių finansinių atsiskaitymų sistemoje yra įdiegtas sistemos atstatymo mechanizmas sistemos klaidos, ar perkrovimo (”nulūžimo”) atveju?			
taip	+		+
ne		+	
nežinau			
Kaip dažnai yra atnaujinamos Jūsų elektroninės sistemos?			
kartą per dieną			
kartą per savaitę			

kartą per mėnesį	+		+
kartą į pusmetį		+	
kartą į metus			
niekada			
Jei atliekamas duomenų kopijavimas, kaip dažnai jis atliekamas?			
kartą per dieną			+
kartą per savaitę	+		
kartą per mėnesį		+	
kartą į pusmetį			
kartą į metus			
niekada			
Kaip dažnai atliekamas elektroninių finansinių atsiskaitymų sistemų saugumo testas?			
po sistemos įdiegimo			+
kartą per savaitę			
kartą per mėnesį	+		+
kartą į pusmetį		+	
kartą į metus			
niekada			

Iš pateiktos lentelės matyti, kad visi rezultatai yra skirtingi ir visos įmonės teikia skirtingą dėmesį skirtingiems dalykams. Abi įmonės, iš kurių buvo imtas interviu skiria didesnį dėmesį vieniems saugumo reikalavimams, tačiau įmonės, kurios buvo apklaustos anonimiškai beveik palaiko visus saugumo reikalavimus. Visos apklaustos įmonės daugiausiai naudoja bankines e. atsiskaitymų sistemas, kurios padeda prekiauti ir gauti pinigus iš klientų. Naudojant visas šias bankines sistemas visos įmonės naudojas SSL ir HTTPS saugumo standartus, kurie užtikrina saugų duomenų perdavimą per internetą. Tai rodo, kad šie standartai yra vieni iš populiariausių ir dažniausiai naudojamų. Taipogi, visos įmonės pasisako, kad yra įdiegtos antivirusinės sistemos, vyksta duomenų kodavimas bei yra dažnai daromos duomenų kopijos, vieni tai daro kasdien, kiti kas savaitę, kiti kas mėnesį, tačiau daro visi, tai rodo, kad duomenų praradimas būtų didelis ir nuostolingas. Tačiau ne visose įmonėse, kurios buvo apklaustos anonimiškai, yra diegiamos ugniasienės, nors ugniasienė yra programinės įrangos programa arba techninės įrangos dalis, kuri padeda apsisaugoti nuo įsilaužėlių, virusų ir kirminų, kurie bando pasiekti kompiuterį per internetą. Taip pat prie šios programos būtinai turi būti instaliuojama ir antivirusinė, tačiau įmonės diegia antivirusines, be ugniasienių.

Toliau nagrinėjant taikomas priemones apsaugoti įmonę bei jos klientus ir duomenis vykstant e. atsiskaitymams ir pan., UAB „Baltjuta“ ir anonimiškai apklaustos įmonės yra įsidiegusios mechanizmus, kurie atstato sistemas po klaidos, ar persikrovimo atveju. Kitaip nei įmonė X tokio mechanizmo neturi, taip pat ji savo sistemas atnaujina tik kartą į pusmetį, priešingai nei visos kitos. Jos sistemas atnaujina karta į mėnesį. Taip pat yra ir su saugumo atliekamais testais, įmonė X juos atlieka kas pusmetį, o visos kitos kas mėnesį, tačiau taip pat didelis kiekis anonimiškai apklaustų įmonių teigė, kad testus dar atlieka po sistemos įdiegimo, kad patikrinti ar viskas gerai suinstaliuota ir ar viskas vyks sklandžiai.

IŠVADOS IR PASIŪLYMAI

1. Saugos priemonių įgyvendinimas įmonių finansiniuose atsiskaitymuos turi užtikrinti:

-vartotojų autentiškumo patvirtinimo, autorizacijos priemones, nustatant vartotojo tapatumą,

- prieigos prie duomenų konfidencialumo lygmenis atsižvelgiant į vartotojų roles šiuose finansiniuose atsiskaitymuose,

-duomenų privatumo ir vientisumo galimybes, (jas dažniausiai realizuoja elektroninių finansinių sistemų pagal bendrus reikalavimus įgyvendinama programinė apsaugos įranga), tačiau įmonės turi jas įsidiegti.

2. Pagal pasaulinės praktikos pavyzdžius, elektroniniai atsiskaitymai tampa žymiai daugiau neapsaugoti ir pažeidžiami, jei tokiai nelegaliai veiklai specialiai organizuojamos technologinės priemonės.

3. Asmenys bei įmonės, siekiančios finansiniuose atsiskaitymuose daryti perlaidas ar pavedimus, naudojant elektroninio banko paslaugas, įsijungia į bendrus saugos reikalavimus palaikančių metodų, programinės įrangos, įrankių šiose sistemose darbą ar vieningos elektroninės mokėjimų erdvės (SEPA) priemonėmis užtikrinamą saugesnę aplinką. Rizikos komponentų įžvalga ir numatymas turi užtikrinti finansiniuose srautuose dalyvaujančių operacijų įmonių bei klientų duomenų saugumą, esant nepakankamai apsaugai įmonės ar organizacijos, tiek bankai gali prarasti svarbią informaciją, skaitmeninius finansinius resursus. Dėl šios priežasties galimi materialiniai nuostoliai, klientų praradimas, įmonės reputacijos smukimas, asmens duomenų apsaugos pažeidimai, bei kiti neigiami padariniai turintys tiesioginius įtakos verslo įmonės veiklai.

4. Vertinant pagrindinius sistemų, atliekančių e. finansinius atsiskaitymus, saugumo reikalavimus kaip pagrindiniai išskirti (jie kurie tampa privalomaisiais ir pagal ES saugos priemonių standartus): autentifikacija, autorizacija, vientisumas, konfidencialumas, privatumas bei nuodugni apsauga, taip pat antrinės priemonės kurios nustato minimalių privilegijų, duomenų archyvavimo ir kopijavimo, auditavimo priemones tikslu užtikrinti pažeistų duomenų analizę, atliktų operacijų atstatymą ir kitas priemones.

5. Horizontaliosioms finansinių e. atsiskaitymų saugos reikalavimų vykdymo priemonėms priskirtinos internetinės saugumo technologijos bei standartai yra SSL, HTTPS ir WS-Security tai protokolai kurie vykdo operacijų taisyklingumo ir saugios aplinkos funkcijas ir tuo pačiu įgalina verslo įmones bei klientus nuo privačios informacijos paviešinimo ar panaudojimo nelegaliais tikslais.

6. Pagal atliktą eksperimentinio tyrimo tikslinę įmonių saugos priemonių finansiniuose atsiskaitymuose analizę, nustatyta, kad pagrindiniai e. atsiskaitymų ir sistemų, kurių pagalba jie yra atliekami, rizikos faktoriai yra piktybinė programinė įranga bendroje aplinkoje yra virusai, trojos arkliai, šnipinėjimo programinė įranga, „programišių“ atakos ir kt. Su tokia programine įranga

susiduria 90% įmonių. Ir specialiai orientuota ir organizuota nusikalstama veikla šioje srityje, kaip sukčiavimas, sistemų klonavimas, kanalų skenavimas ar specialios techninės įrangos prijungimas vykdomų operacijų aplinkose tampa gana grėsmingomis priemonėmis, kurioms užkirsti kelia gali tinkamai organizuojamos daugia-kompleksinės, daugelio lygių apsaugos priemonės. Tai rodo jog elektroninio saugumo spragos yra dažnos, todėl būtina investuoti į elektroninės apsaugos priemones siekiant sumažinti šią riziką.

7. Remiantis atliktu tyrimu, įtakos saugumo užtikrinimui ir atsiskaitymų sistemų saugumo efektyvumui pasiekti turi ir kompleksinės apsaugos priemonės, tokios kaip: antivirusinės programos, ugniasienės, reguliarus atsarginių duomenų kopijavimas ir tinkamas sistemos auditas.

8. Kol kas į savo ir klientų duomenų saugumą Lietuvos įmonės investuoja palyginti nedaug. Tai lemia keletas veiksnių: maža šalis patiria nedaug atakų ir neturi sukaupusi daug konfidencialių duomenų, esant sunkmečiui išlaidos IT sprendimams ir saugumui yra apkarpytos ir ne visos įmonės dar rimtai žiūri į interneto saugumą ir jo rizikas.

9. Kol kas dar pastebima gana gausi e. finansinių atsiskaitymų būdų įvairovė, kaip pvz., atsiskaitymai banko mokėjimo kortelėmis naudojant internetinės bankininkystės sistemas, finansiniai pavedimai naudojantis internetinę bankininkystę. Rečiau pasitaikantys atsiskaitymo būdai: per PayPal ir Google Checkout internetinių mokėjimų sistemas. Nepaisant to, kad minėtosios sistemos populiarumu nusileidžia elektroninei bankininkystei, jų skvarba bei reikšmė vykdant elektroninius atsiskaitymus nuolat auga. Iš to galima spręsti, kad mokėjimo sistemos ateityje sudarys stiprią konkurenciją elektroninės bankininkystes sistemoms bei užims didesnę dalį elektroninių mokėjimų rinkos.

10. Įvardinti pagrindiniai trūkumai, tokie kaip dalinis saugos reikalavimų palaikymas atsiskaitymų sistemose, taip pat nepakankamas apsaugos priemonių panaudojimas, atsainus požiūris į saugos reikalavimus bei papildomų saugumo priemonių diegimą palieka galimybę nusikaltėliams įsibrauti į verslo įmonių sistemas, o tai gali sukelti neigiamus padarinius tiek įmonei, tiek jos klientams.

Pasiūlymai ir rekomendacijos verslo įmonėms, kurios vykdo e. atsiskaitymus:

1. Užtikrinant pilnavertę apsaugos finansiniuose atsiskaitymo kompleksinė aplinką, svarbu taikyti naujausią siūloma technologinę platformą, kuri užtikrintų tiek Lietuvos įmonių sąveikos ir bendradarbiavimo, tiek tarptautinių finansinių atsiskaitymų saugias galimybes.

2. Žinoma, pastebėti trūkumai dirbant su tokiais svarbiais duomenimis kaip žmogaus asmeniniai ar kortelių duomenys, specializuoto įsilaužimo atvejai, todėl kiekviena kompanija turėtų peržiūrėti, atnaujinti ir nuolat testuoti savo sistemų ir e. finansinių atsiskaitymų saugumą.

3. Be bendrųjų reikalavimų, pastebėti trūkumai UAB “Baltjuta” įmonėje buvo suteiktos rekomendacijos jungtis į vieningą apsaugą realizuojančias sistemas, o dabartinėje situacijoje dažniau atnaujinti savo antivirusinę programinę įrangą bei įsidiegti ugniasienę.

4. Įmonei „X“ buvo rekomenduota atskirti klientų aptarnavimo sistemos techninė ir technologinę bazę bei vidines operacijas atliekamos įrangos darbą. Nesaugoti savo sistemoje konfidencialios vartotojų informacijos, kaip kortelių duomenys bendros prieigos sistemoje. Sumažinant rizika didelius vartotojų srautus aptarnaujančiose įmonėse, e. parduotuvėse vartotojams prisijungus iš naujo užpildant atsiskaitymo duomenis automatiškai, įdiegti priemones neleisiančias nutekinti svarbią informaciją, pastebėti galimus naujų formų įsilaužimo atvejus ir juos programų priemonėmis apriboti.

5. Tolesni darbai šioje srityje galėtų būti atliekami gilinantis į naujuosius e. atsiskaitymo būdus bei interneto servisų „WS-Security“ technologiją pasauliui vis labiau žengiant į paslaugas orientuotos architektūros lygmenį.

LITERATŪRA

1. **Lietuvos Respublikos Vyriausybes nutarimas (2008 m.).** Lietuvos informacinės visuomenės plėtros 2009-2015 metų strategija.
2. **Security for Elektronic B2B Transactions** [PDF HTML kopija] http://www.cieca.com/Documents/OpenDocuments/2003/SecurityforElectronicB2BTransactions-2003-05-19.pdf [žiūrėta 2009 01 09]
3. **B2B Security Concerns within the Automotive Industry White Paper** [PDF HTML kopija]. http://83.170.79.34/WhitePaperAutomotiveSecurity20.pdf [žiūrėta 2009 01 10]
4. **Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee** „Enhancing Trust and Confidence in Business-to-Business Electronic Markets“ [PDF HTMP kopija]. http://www.insme.org/documents/COM_2004_0479_F_EN_ACTE.pdf [žiūrėta 2009 01 12]
5. **Commission staff working paper on B2B Internet trading platforms:** Oppurtunities and barriers for SMEs – A first assessment [PDF HTML kopija]. http://ec.europa.eu/enterprise/ict/policy/b2b/sec2002-1217en.pdf [žiūrėta 2009 01 12]
6. **Saugus duomenų perdavimas internetu: SSL/TLS** // Naujoji komunikacija, 2007, Nr.12. http://www.nk.lt/archyvas/aktualijos/saugus-duomenu-perdavimas-internetu-ssltls/ [žiūrėta 2009 01 28]
7. **Angelopoulou O. ir kt.** Online ID theft techniques, investigation and response // International Journal of Electronic Security and Digital Forensics. – UK, 2007, Nr. 1, psl. 76-88. – ISSN 1751-911X
8. **Europos vartotojų centras:** Siunčiami elektroniniai laiškai, kuriais siekiama “išplauti” pinigus. http://www.ecc.lt/index.php?3996953086 [žiūrėta 2009 02 19]
9. **Spyware:** Spyware apibrėžimas. http://www.spyware.lt/lt/spyware-apibrezimas.html [žiūrėta 2009 02 19]
10. **Microsoft Security:** Virusų, kirminų ir Trojos arklių apžvalga. http://www.microsoft.com/lietuva/security/home/antivirus/virus101.mspx [žiūrėta 2009 02 19]
11. **Lietuvos Respublikos Vidaus Reikalų Ministerija:** Išmokime apsaugoti elektroninę erdvę. http://www.vrm.lt/index.php?backPID=129&id=602 [žiūrėta 2009 02 20]
12. **Business Guide: Guide of securing your e-government web site** [PDF HTML kopija]. http://www.verisign.com/static/005568.pdf [žiūrėta 2009 02 24]
13. **SSL information center**. http://www.verisign.com/ssl/ssl-information-center/index.html [žiūrėta 2009 02 24]

14. **Internet Explorer Developer Center**: https Protocol. http://msdn.microsoft.com/en-us/library/aa767735(VS.85).aspx [žiūrėta 2009 02 26]
15. **Instant SSL by Comodo**: Know what Https is and how SSL works. http://www.instantssl.com/ssl-certificate-products/https.html [žiūrėta 2009 02 26]
16. **Kairaitis K., Tamonis M.** Web Service Technologija // Konferencijos "Mokslas – Lietuvos ateitis" medžiaga. 2007.
17. **IBM Corporation:** Technologies and Standards for Service-Oriented Architecture Project Implementation. 2005, [PDF kopija].
18. **Šatas J.** Tarptautiniai atsiskaitymai: teisiniai pagrindai ir praktika. Vilnius, "Eugrimas", 2006. – 224-264 p.- ISBN 9955-682-40-X
19. **Sodžiūtė L., Sūdžius V.** Elektroninė komercija: prielaidos, struktūra ir procesai. Vilnius, "Petro ofsetas", 2003. – ISBN 9955-534-19-2
20. **PayPal.** https://www.paypal.com/lt/cgi-bin/webscr?cmd=_home-general&nav=0 [žiūrėta 2009 03 18]
21. **Čėsna R., Štilis D.** Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime. Lietuvos teisės akademija, 2000. – ISBN 9955-442-08-5
22. **Apsauga nuo įsilaužėlių: ugniasienė.** http://www.elektronika.lt/tips/theme/190/2320/ [žiūrėta 2009 06 09]
23. **Lietuvos statistikos departamentas prie Lietuvos Respublikos Vyriausybės.** http://www.stat.gov.lt/uploads/docs/3_IT_panaud_imonese_2008_1.doc [žiūrėta 2009 06 10]
24. **Marshal8e6.** http://www.marshal8e6.com/TRACE/phishing_statistics.asp [žiūrėta 2009 06 11]
25. **Dzemydienė, D.** Intelektualizuotų informacinių sistemų projektavimas ir taikymas. Mykolo Romerio universitetas, 2006. – ISBN 955-19-051-5
26. **Client-side defense against web-based identity theft** [PDF HTML kopija]. http://www.isoc.org/isoc/conferences/ndss/04/proceedings/Papers/Chou.pdf [žiūrėta 2009 06 15]
27. **UAB „Baltjuta".** http://www.baltjuta.lt/ [žiūrėta 2009 07 08]
28. **Destiny Sphere**. http://ltforum.destinysphere.net/viewtopic.php?t=90 [žiūrėta 2009 09 16]
29. **Laurinaitis. M.**. Elektroninių pinigų sąvoka. Mykolo Romerio universitetas.Informatikos ir statistikos katedra, 2007.
30. **Štilis D., Laurinaitis M.** Alternative Payment Systems: Lithuanian outlook. 2008.
31. **European Commission Enterprise and Industry Directorage – General:** 2009 ICT Standardisation Work Programme. http://portal.etsi.org/stfs/process/Forms/EC_2009_ICT_Standardisation_WP_v42.doc [žiūrėta 2009 11 02]

32. **Finansinių nusikaltimų tarnyba** prie Vidaus Reikalų Ministerijos.Pinigų plovimo prevencija. http://www.fntt.lt/lt/99 [žiūrėta 2009 11 04]
33. **David Icove**. Computer Crime: A Crimefighter`s Handbook. *O`Reylly Associates, Inc*., 1995.
34. **European Commission Enterprise and Industry Directorage – General:** 2008 ICT Standardisation Work Programme [PDF HTML kopija]. http://ec.europa.eu/enterprise/sectors/ict/files/wp2008_en.pdf [žiūrėta 2009 12 05]

Dagelytė R. Saugos reikalavimai verslo įmonių elektroniniuose atsiskaitymuose/ Elektroninio verslo vadybos magistro baigiamasis darbas. Vadovė prof. dr. D. Dzemydienė. – Vilnius: Mykolo Romerio universitetas, Socialinės informatikos fakultetas, 2009. – 65 p.

ANOTACIJA

Magistro baigiamajame darbe išnagrinėta e. finansinių atsiskaitymų saugos reikalavimų vykdymas įmonėse, taip pat išnagrinėtos įmonėms keliamos grėsmės bei rizikos vykdant atsiskaitymus. Išnagrinėjus įmonių saugumą, buvo pateikti pasiūlymai, kurie padėtų įmonėms efektyviau apsaugoti savo ir klientų duomenis bei jų bankų sąskaitas. Pirmojoje šio darbo dalyje pateikiami e. finansinių atsikaitymo būdai bei saugumo samprata. Antrojoje dalyje yra apžvelgiama e. finansinių sistemų pažeidžiamumas, galimos rizikos bei faktoriai. Trečiojoje dalyje yra išanalizuojamos saugos priemonės, kurios gali būti taikomos apsaugant elektroninių finansinių atsikaitymų sistemas ir vidinę įmonės kompiuterių saugą. Taip pat yra apžvelgiama saugumo sistemos, kurios padeda saugiai perduoti duomenys juos šifruojant. Taipogi, dar didelis dėmesys skiriamas ir internetinėms mokėjimo sistemoms, kurias naudoja ne viena įmonė, taip pat ir daugybė žmonių visame pasaulyje. Ketvirtojoje dalyje yra vertinamas e. finansinių atsiskaitimų saugos reikalavimų vykdymas įmonėse UAB „Baltjuta“ bei įmonėje X, taip pat anonimiškai apklaustose įmonėse, taipogi jų susidūrimai su rizikomis. Taip pat pateikiama dviejų prieš tai minėtų įmonių ir anonimiškai apklaustų įmonių rezultatų lyginamoji analizė, leidžianti nustatyti konkrečių nagrinėjamų įmonių saugumo lygį lyginant su Lietuvos įmonių vidurkiu.

Dagelytė R. Security Requirements for Electronic Payments in Business Companies/ Electronic business management master work. Advisor prof. dr. D. Dzemydienė. – Vilnius: Mykolas Romeris University, Social Informatics cathedral, 2009 – 65 p.

ANOTATION

In the master degree work it was analyzed how electronic payment security requirements are executed in Lithuanian middle size companies. There was also analyzed the potencial risk factors for such e-transactions. As an output the security recommendations were provided for companies to more effectively secure their and their client data and bank accounts. Available e-payments and security requirements are descirbed in the first master work part. In the second part all available security risks and holes are written with explanation of their principals and consequences. The third part descirbes the security technologies which prevent system for malicious software and hacker attacks.It also includes the abstract of internet security technologies responsible for safe and secure data transfer through internet. In the last paper part it is analyzed e-payment security level in the UAB „Baltjuta“ and anonymous company „X“ companies as well as anonymous survey for all middle size Lithuanian companies about their system and payments security. Finally the comparing analysis is done between the two concrete companies and the anonymous survey results to find out the difference from the average level.

Dagelytė R. Saugos reikalavimai verslo įmonių elektroniniuose finansiniuose atsiskaitymuose/ Elektroninio verslo vadybos magistro baigiamasis darbas. Vadovė prof. dr. D. Dzemydienė. – Vilnius: Mykolo Romerio universitetas, Socialinės informatikos fakultetas, 2009. – 65 p.

SANTRAUKA

Elektroninio verslo vadybos magistro darbo tema “Saugos reikalavimai verslo įmonių elektroniniuose atsiskaitymuose” yra aktuali, nes saugumas atsiskaitant internete yra vienas iš svarbiausių faktorių. Įmonės, teikiančios e. finansinius atsiskaitymus naudojant jų sistemas susietas su banku, turi užtikrinti nepriekaištingą saugumą. Dėl šios priežasties jos privalo palaikyti visus saugos reikalavimus skirtus užtikrinti atsiskaitymų saugumą bei duomenų slaptumą.

Šiame darbe buvo atliekama analizė išsiaiškinti, kokius saugos reikalavimus įmonės įdiegusios savo sistemose ir kaip tai įtakoja jų saugumą. Taip pat kokius pažeidimus patiria žmonės ir įmonės bei su kokiomis rizikomis bei grėsmėmis kovoja. Apklausus dvi įmones interviu ir 46 įmones anonimiškai pateikiant anketas internete, paaiškėjo, kad ne visi saugos reikalavimai bei standartai yra palaikomi ir ne visos saugos priemonės yra taikomos. Dėl šios priežasties ir yra susiduriama su pažeidimais bei duomenų pasisavinimu ir kita.

Magistriniame darbe apibrėžiami pagrindiniai saugos reikalavimai, kurie turėtų būti taikomi e. finansinių atsiskaitymų sistemose, kad užtikrinti besąlygišką sistemos saugumą. Taip pat pateikiami dažniausiai sutinkami pažeidžiamumo elementai, t.y. virusai, piktybinė programinė įranga ir pan. Kartu pateikiama informacija kokiu būdu pasireiškia šie elementai ir kaip tai paveikia sistemas.

Darbo tikslas - išnagrinėti saugos reikalavimus e. finansiniuose atsiskaitymuose bei atlikti tyrimą, kurio pagalba būtų galima išanalizuoti ir pateikti e. finansinių atsiskaitymų saugos trūkumus. Taip pat iškelti uždaviniai šiam tikslui pasiekti. Jie buvo pilnai įgyvendinti pateikiant rekomendacijas, kaip reikalavimas atnaujinti sistemas bent kartą per savaitę, dažnai ir reguliariai atlikti saugumo testus ir kt. Savaime suprantama, sistemos turi turėti paruoštus atstatymo mechanizmus, įsilaužimo atveju.

Sprendžiant iš pateiktos statistikos matyti, kad žmonės vis daugiau naudojasi internetu ir jame teikiamomis paslaugomis apsimokėti už prekes ir paslaugas internetu. Dėl ko taip pat kyla vis didesnė aplinkos rizika, todėl ir įmonės teikia vis didesnį dėmesį saugos reikalavimų palaikymui.

Dagelytė R. Security Requirements for Electronic Payments in Business Companies/ Electronic business management master work. Advisor prof. dr. D. Dzemydienė. – Vilnius: Mykolas Romeris University, Social Informatics cathedral, 2009 – 65 p.

SUMMARY

The Master work “Security requirements for electronic payments in business companies” for Electronic business management subject is essential, because the internet security in payment systems is one of the major factors. Companies providing the e-payments through their systems and banking systems must also provide the excellent security level. Because of this reason they must apply all security requirements to secure the payments and data.

The proper analysis in this work was done to find out what security requirements companies are using in their systems and how they influence its security. Also what kind of vulnerabilities the users and systems get while executing business payments transactions. Two particular companies were interviewed and 46 anonymous companies filled the survey. It was found out that not all security requirements were applied to their payment systems. This is one of the main reasons why companies still face attacks and data steel.

In this Master work there are defined all main security requirements which must be applied to e-payments systems. There is also defined major maliciuos software and elements like viruses, trojans together with how they work and what impact have on the systems.

The main target of the work was to analyze existing security requirements in the e-payment systems and do the research who helped to find out common e-payment systems security issues. There are also the tasks descirbed to accomplish the target. They were fullfilled by providing recommendations like the requirement to update the system at least once in a week, often and regular do system security tests and also the requirement to have a backup system mechanism ready, etc.

Considering the gathered statistics it was assessed that more and more users are using the internet and e-payment systems every day. This is adding more risk to the e-payment systems thus it is essential to give more attention to the system security and their requirement all the time.

PRIEDAI

1 PRIEDAS, anketa „Įmonių, naudojančių elektroninių finansinių atsiskaitymų sistemas, apklausa“:

Įmonių, naudojančių elektronines finansinių atsiskaitymų sistemas, apklausa

1. Kiek žmonių dirba Jūsų įmonėje?

□ nuo 1 iki 5
□ nuo 5 iki 10
□ nuo 10 iki 25
□ nuo 50 iki 100
□ daugiau nei 100

2. Kokio tipo yra Jūsų įmonė?

□ gamybinė įmonė
□ tiekimo įmonė
□ pardavimo įmonė
□ paslaugų įmonė
□ transporto įmonė
□ telekomunikacijų įmonė
□ kita, įrašyti.....

3. Kokius elektroninius atsiskaitymo būdus naudojate savo įmonės veikloje?

□ atsiskaitymas elektroniniais čekiais
□ atsiskaitymas banko mokomąją kortele
□ atsiskaitymas skaitmeniniais pinigais
□ atsiskaitymas elektroniniais pinigais

4. Kokias elektronines finansines atsikaitymo sistemas naudoja įmonė?

□ VAM
□ PayPal
□ Google Checkout
□ banko elektroninių finansinių atsiskaitymų sistema
□ kita, įrašyti.....

5. Kokiam ratui žmonių yra skirta Jūsų elektroninių finansinių atsikaitymų sistema?

□ įmonės darbuotojams
□ plačiam ratui vartotojų
□ kita, įrašyti.....

6. Jei tai vartotojams skirta sistema, kiek vidutiniškai per mėnesį vartotojų naudojasi Jūsų sistema?

□ nuo 1 iki 100
□ nuo 100 iki 1000
□ nuo 1000 iki 10000
□ nuo 10000 iki 100000
□ daugiau nei 100000

7. Ar Jūsų įmonėje dirba už sistemų saugumą atsakingas specialistas?

□ taip dirba
□ ne nedirba

8. Su kokia saugumo rizika ir faktoriais susiduriate savo įmonėje naudojant elektroninių finansinių atsiskaitymų sistemas ir būdus?

□ sukčiavimas (angl. Phishing)
□ sistemų klonavimas (angl. Web-spoofing)
□ šnipinėjanti programa (angl. Spyware)
□ virusai
□ trojos arklys
□ nesusiduriame
□ kita, įrašyti.....

9. Ar teko kada patirti mėginimus įsilaužti į Jūsų naudojamą elektroninių finansinių atsiskaitymų sistemą?
□ taip
□ ne
□ nežinau

10. Ar teko patirti įsilaužimų ir jei taip, tai kiek kartų?
□ neteko
□ nuo 1 iki 5
□ nuo 5 iki 10
□ nuo 10 iki 25
□ nuo 50 iki 100
□ daugiau nei 100

11. Jei teko patirti įsilaužimus, kokie jie?
□ internetinio puslapio turinio pakeitimai
□ duomenų vagystės
□ duomenų pašalinimas
□ sistemos sekimo įrankių instaliavimas
□ kita, įrašyti.....

12. Kokie saugumo standartai įdiegti Jūsų įmonės finansinių elektroninių atsiskaitymų sistemose?
□ SSL protokolas
□ HTTPS perdavimo protokolas
□ WS-Security standartų grupė
□ kita, įrašyti.....

13. Kokias saugumo priemones naudojate elektroninių finansinių atsiskaitymų sistemos saugumui užtikrinti?
□ antivirusinės programos
□ ugniasienės
□ saugus serveris
□ duomenų kopijos
□ duomenų kodavimas
□ kita, įrašyti.....
□ nenaudojame

14. Kokie saugumo reikalavimai palaikomi įmonės elektroninių finansinių atsiskaitymų sistemose?
□ autentiškumo patvirtinimas
□ autorizacija
□ auditas
□ konfidencialumas
□ privatumas
□ vientisumas

□ prieinamumas
□ minimalios privilegijos
□ paprastumas
□ nuodugni apsauga
□ internetinių standartų naudojimas
□ audito įrašų registravimas
□ kita, įrašyti.....

15. Jeigu naudojate ir banko elektroninių finansinių atsiskaitymo sistemą,ar teko susidurti su jos klaidomis ar saugumo spragomis?
□ taip
□ ne
□ nežinau

16. Ar Jūsų elektroninių finansinių atsiskaitymų sistemoje yra įdiegtas sistemos atstatymo mechanizmas sistemos klaidos, ar perkrovimo (”nulūžimo”) atveju?
□ taip
□ ne
□ nežinau

17. Kaip dažnai yra atnaujinamos Jūsų elektroninės sistemos?
□ kartą per dieną
□ kartą per savaitę
□ kartą per mėnesį
□ kartą į pusmetį
□ kartą į metus
□ niekada

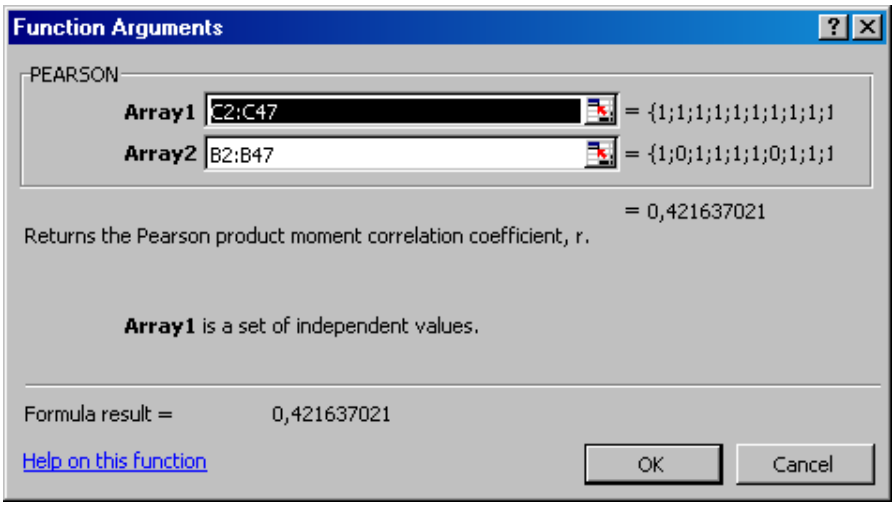
18. Jei atliekamas duomenų kopijavimas, kaip dažnai jis atliekamas?
□ kartą per dieną
□ kartą per savaitę
□ kartą per mėnesį
□ kartą į pusmetį
□ kartą į metus
□ niekada

19. Kaip dažnai atliekate elektroninių finansinių atsiskaitymų sistemų saugumo testus?
□ po sistemos įdiegimo
□ kartą per savaitę
□ kartą per mėnesį
□ kartą į pusmetį
□ kartą į metus
□ niekada

20. Kiek skiriama pinigų sistemos saugumo užtikrinimui per metus?
□ neskiriama
□ iki 100 litų
□ iki 1000 litų
□ iki 10000 litų
□ iki 100000 litų
□ daugiau nei 100000 litų

2 PRIEDAS

Pearsono koreliacijos apskaičiavimo paveikslas „Įmonių patirtų įsilaužimų ir atrastos kenkėjiškos programinės įrangos priklausomybė nuo nepakankamo apsaugos lygio“:



Pearsono koreliacijos koeficiento apskaičiavimas „Įsilaužimų kiekio priklausomybė nuo saugos reikalavimų įdiegimo sistemose“ :