ISSN 2029-2341 print / ISSN 2029-2252 online
2013 5(1): 46–52 doi:10.3846/mla.2013.07

IT RIZIKOS IDENTIFIKAVIMO PROCESO ANALIZĖ

Rasma Janeliūnienė[1], Vida Davidavičienė[2]

[1, 2]Vilniaus Gedimino technikos universitetas, Verslo vadybos fakultetas
El. paštas: [1]rasma.janeliuniene@vgtu.lt; [2]vida.davidaviciene@vgtu.lt

Santrauka. Išaugusi verslo procesų, kartu ir verslo sėkmės, priklausomybė nuo informacinių technologijų (IT) šiuo metu yra glaudžiai susijusi su IT rizika. Tai daro įtaką augančiam IT rizikos valdymo ir kontrolės poreikiui. Nepaneigtina tai, kad identifikuota, išanalizuota ir sumažinta sistemos rizika leidžia išvengti nepageidaujamų pasekmių, tokių kaip informacijos praradimas, nutekėjimas ar duomenų sugadinimas. Pagrindinis sėkmės veiksnys siekiant užtikrinti organizacijos sėkmę valdant IT yra sistemingas ir tęstinis IT rizikos valdymas. Straipsnyje keliamas tikslas išanalizuoti vieną iš IT rizikos valdymo proceso etapų – rizikų identifikavimą. Straipsnyje pasitelkiami tokie metodai, kaip mokslinės literatūros analizė, sisteminimas, apibendrinimas.

Reikšminiai žodžiai: IT rizika, IT rizikos identifikavimas, IT rizikos valdymas, informacinės technologijos.

Įvadas

Įmonės veikloje ypač svarbus vaidmuo tenka informacinėms technologijoms (IT), jas taikant galima optimizuoti resursus, pagerinti sprendimų priėmimą, tobulinti valdymą, didinti įmonės konkurencingumą ir skatinti verslą bei pelningumą (Davidavičienė 2008; Davidavičienė, Raudeliūnienė 2010; Paliulis *et al.* 2012; Paliulis, Uturytė-Vrubliauskienė 2012). Organizacijai, naudojančiai IT kaip vertę kuriantį įrankį, būtina atsižvelgti ne tik į naudą, bet ir į kylančias rizikas. Pabrėžtina, kad su IT susiję neapibrėžtumai ar trikdžiai tiek informacinėje, tiek verslo sistemose gali sukelti rimtų pasekmių įmonei ar jos veiklos tęstinumui. Kaip nustatė Smith, McKeen (2009), paprastai organizacijos, savo veikloje naudojančios IT, neatlieka išankstinių IT rizikos valdymo veiksmų, nesusieja IS rizikos su verslo strategija ir nepakankamai investuoja į galimų problemų sprendimą. Kaip pasekmė gali atsirasti nepageidaujami reiškiniai (tokie kaip gamybos sutrikdymas, darbo nutraukimas) įmonės viduje ir kilti pavojų informaciniam ar materialiam įmonės turtui. Svarbus tampa rizikos organizacijoje supratimas (kaip ji kyla sistemoje, kaip ją galima nustatyti, kaip valdyti pasirinkus tinkamą sistemos apsaugos strategiją ir pan.). Vadovaujantis moksliniu apibrėžimu, kad IT rizika sistemose kyla tuomet, kai IT sistemoje ar jos aplinkoje esanti pažeidžiama vieta sudaro tinkamas sąlygas grėsmės realizacijai (Stoneburner *et al.* 2002; VITA 2006; ISACA 2009), galima teigti, kad pagal atsiradimo kilmę IT rizika yra dviejų sąlyginių įvykių rezultatas. Tai patvirtina IT rizikos identifikavimo etapo svarbą. Pabrėžtina IT rizikos identifikavimo etapo svarba, kur rizikos identifikavimas sistemoje yra kompleksinis uždavinys, kuriuo reikia įvertinti grėsmes ir pažeidžiamas vietas.

Straipsnio tikslas – išanalizuoti IT rizikos identifikavimo procesą kaip vieną iš svarbiausių IT rizikos valdymo etapų, siekiant identifikuoti IT rizikos nustatymo etapus. Straipsnyje taikomi mokslinės literatūros analizės, sisteminimo, sintezės, apibendrinimo metodai.

IT rizikos valdymo koncepcija

Kadangi IT rizika gali būti suvokiama skirtingai, atsižvelgiant į kontekstą, tikslinga išanalizuoti bei detalizuoti pačią IT rizikos koncepciją. Remiantis vienu iš dažniausiai pasitaikančių požiūrių, IT rizika – tai neigiamą poveikį organizacijai ir jos sistemai turintis ir su informacinių technologijų naudojimu susijęs įvykis, kuris atsitinka tuomet, kai grėsmė realizuojasi dėl sistemoje esančių silpnų ir lengvai pažeidžiamų vietų (Stoneburner *et al.* 2002; VITA 2006; ISACA 2009). Tačiau Fratila ir Tantau (2008) riziką traktuoja ne tik kaip problemų šaltinį, bet ir kaip galimą sėkmės veiksnį. Smith, McKeen (2009) pastebi, kad šiais laikais rizikos apibrėžimas keičiasi, jis apima ne tik praradimus ar pavojaus tikimybę ir neaiškumą, o žymiai daugiau. IT rizikos valdymas yra daugiasluoksnė koncepcija, teigianti, kad IT rizikos įvykiai kenkia tiek įmonei, tiek jos klientams (viduje ar už jos ribų kenkia įmonės reputacijai ir atskleidžia silpnąsias įmonės valdymo komandos vietas) (Smith, McKeen 2009). Svarbiausia, kad IT rizikos slopina organizacijos konkurencingumą (Smith, McKeen 2009). IT rizikos kyla iš neadekvataus procesų ir informacinių technologijų valdymo (Savić 2008), o grėsmių realizavimosi priežastys yra informacinių sistemų ištekliuose atsiradusios pažeidžiamos vietos (Stoneburner

et al. 2002, 2004; Elky 2006; Gao *et al*. 2011). Westerman ir Hunter (2007) pažymi, kad dažniausiai IT rizikos kyla ne dėl techninių ar žemos kompetencijos darbuotojų veiklos padarinių, bet dėl spragų įmonės valdymo sistemoje ir nepakankamo IT procesų valdymo. Tokie trikdžiai lemia daug prastų sprendimų ir netinkamą IT resursų vertinimą. NIST SP 800-27 kompiuterių saugumo ataskaitoje nurodyta, kad su IT susijusių rizikų šaltiniai yra: 1) neteisėtas (kenksmingas ar atsitiktinis) informacijos atskleidimas, pakeitimas arba sunaikinimas; 2) netyčinės klaidos ir aplaidumas; 3) IT sutrikimai dėl stichinių ar žmogaus sukeltų nelaimių; 4) nesugebėjimas tinkamai prižiūrėti IT sistemą (Stoneburner *et al.* 2004). Dėl tokių įvairialypių IT rizikos atsiradimo priežasčių IT rizikos klausimo sprendimas priskiriamas ne tik IT skyriui ar techniniams darbuotojams, bet ir vadybininkams (ISACA 2009). Galima teigti, kad grėsmių neįmanoma išvengti, tačiau jas galima suvaldyti. Išskiriami tokie rizikos valdymo tikslai: 1) apsaugoti IT sistemas, kurios susijusios su organizacijos informacijos saugojimu, apdorojimu ir perdavimu; 2) sudaryti galimybę vadovams priimti savalaikius rizikos valdymo sprendimus; 3) sudaryti sąlygas autorizuoti informacines sistemas, remiantis dokumentais (Stoneburner *et al.* 2002).

Taigi kaip pagrindinis rizikos valdymo tikslas gali būti išskiriamas rizikos identifikavimas ir vertinimas siekiant efektyvaus jos valdymo. O rizikos valdymas yra procesas, leidžiantis IT vadybininkams subalansuoti operacines ir ekonomines apsaugos priemonių sąnaudas ir pasiekti naudą apsaugant IT sistemas bei duomenis, kurie palaiko organizacijos misiją (Stoneburner *et al.* 2004; Janeliūnienė *et al.* 2011). Taigi rizikos valdymas yra procesas, kai rizikos identifikuojamos, įvertinamos ir imamasi priemonių, kaip sumažinti rizikas iki priimtino lygio.

Rizikų valdymo nauda neabejotina, atkreipiant dėmesį į tai, kad atsiradusios rizikos gali visokeriopai paveikti organizaciją ir jos klientus (pvz.: finansiniai, moraliniai nuostoliai, sutrikdyta veikla, sumenkinta reputacija). Nagrinėjant su technologiniais pokyčiais ir jų valdymu susijusius iššūkius, rizikos valdymas gali būti kritinis veiksnys, o tinkama saugumo strategija – lemti sistemos apsaugos nuo žalingo poveikio efektyvumą. Tai patvirtina, kad rizikos identifikavimas pirmas ir svarbiausias etapas, leidžiantis organizacijai toliau sėkmingai vystyti rizikos analizės, rizikos poveikio sumažinimo bei rizikos stebėjimo etapus. Juk aiškiai suvokusi riziką, organizacija gali ją įvertinti ir suteikti prioritetą bei priimti atitinkamus sprendimus ir imtis veiksmų siekiant sumažinti galimus nuostolius (Azizi, Hashim 2010).

Pastaruoju metu ypač išaugus IT sprendimų kiekiui tiek verslo, tiek privačiame sektoriuje bei IT naudojimo galimybėms (Pabedinskaitė 2009, 2010) ir kartu kompiuterinių nusikaltimų kiekiui, padidėjo su IT rizikos valdymu susijusių sprendimų pasiūla. Gerai žinomos organizacijos, tokios kaip ISACA, ITIL, *Virginia Information Technologies Agency*, SANS Institute, *Symantec Corp*., siūlo savo sukurtus produktus IT valdyti ir auditui atlikti. Tačiau šie produktai ir IT valdymo sprendimai savaime nebus veiksmingi, būtinas ir pačių organizacijų indėlis. Tam tikslinga iš esmės suvokti patį procesą.

Rizikos identifikavimo proceso analizė

IT rizikos identifikavimas yra pirmas etapas IT rizikos valdymo procese, reikalaujantis daug dėmesio ir žinių. Rizikos identifikavimo etapo tikslas yra pateikti galinčių IT sistemą paveikti rizikų sąrašą. Šiame etape atliekama įmonės IT sistemos analizė, kurios metu nustatomos tą sistemą galinčios paveikti grėsmės bei identifikuojamos sistemos pažeidžiamos vietos, dėl kurių kyla rizikos grėsmių (Stoneburner *et al.* 2002; Elky 2006; VITA 2006). Šio etapo rezultatas yra įvestis į kitą etapą ir informacijos šaltinis priimant sprendimus dėl tolesnių rizikos valdymo veiksmų. Nuo jo priklauso rizikos valdymo efektyvumas. Objektyvus rizikos identifikavimas lemia teisingą ir efektyvią rizikos analizę, kontrolę ir valdymą (Tchankova 2002). Rizikos nustatymas yra svarbus, nes analizuojant sistemą nustatomi incidentų, problemų ir klaidų šaltiniai. Pabrėžtina tai, kad nenustatytos rizikos lieka neįvertintos, o kartais net nežinomos, o tai lemia grėsmę organizacijai. Taip atsitinka, kai rizikos identifikavimo procesas būna paviršutiniškas. Tokiu atveju yra tikimybė, kad lieka nepastebėtų, nenustatytų ar nepakankamai gerai įvertintų rizikų. Taigi šis proceso etapas privalo būti vykdomas itin kruopščiai. Pabrėžtina, kad tikslinga vertinti kiekvieną riziką, nesvarbu, kokią žalą ji gali padaryti. Tik po šio etapo organizacija gali ištirti veiklas ir vietas, kur jos ištekliai yra neapsaugoti ir kur ji yra pažeidžiama.

Rizikos identifikavimo procesas naudingas organizacijai, nes tokia procedūra ypač svarbi įmonės veiklai organizuoti ir vystyti bei siekiant užtikrinti sėkmę ateityje. Siekiant identifikuoti IT turtą, atliekama IT sistemos analizė, kuri leidžia įvertinti verslo procesus, vykdomas funkcijas, sudaro galimybę nustatyti darbuotojų vaidmenį sistemoje ir pan.

Pažymėtina tai, kad rizikos nustatymas yra tęstinis procesas, nulemtas technologijų tobulėjimo ir naujovių, kurios sukuria naujas grėsmes organizacijai, atsiradimo spartos. Taigi, pasikeitus bet kuriam IT sistemos elementui, t. y. įdiegus naują programinę įrangą, ar atnaujinus senąją, gali atsirasti spragų sistemoje. Tansley (2007) rekomen-

duoja rizikos vertinimo procesą kartoti kas trejus metus. Tačiau šio proceso dažnis gali skirtis priklausomai nuo situacijos. Pavyzdžiui, kasmetinis procedūros kartojimas yra pasirenkamas tose organizacijose, kur aktyviai stebimos naujos pažeidžiamos vietos ir grėsmės (Microsoft Corporation 2008). Akivaizdu, kad šis procesas turi būti lankstus (Tansley 2007).

Rizikai identifikuoti siūloma daug metodologijų bei priemonių. Jų įvairovė suteikia galimybę kiekvienai organizacijai nustatyti riziką jai patogiu būdu ir priimtinu metodu. Siekiant kokybiško IT rizikos valdymo, rekomenduotina kreiptis į specialistus. Tačiau, kalbant apie smulkaus ir vidutinio dydžio įmonę, kuri negali skirti pakankamai lėšų rizikai valdyti ir kurios IT infrastruktūra nėra sudėtinga, reikalingi paprastesni ir lengvai suvokiami IT rizikos valdymo proceso sprendimai. Tokiu atveju įmonės pačios galėtų atlikti rizikos valdymo, taip pat ir identifikavimo procedūras. Rizikos nustatymo procese turėtų dalyvauti visi asmenys, dirbantys su IT. Nepriklausomai nuo to, ar įmonė naudojasi IT rizikos specialistų paslaugomis, ar ne, šiame procese turi dalyvauti įmonės darbuotojai. Potencialūs dalyviai yra aukščiausio ir vidutinio lygmens vadovai, ryšių su visuomene, IT, informacijos saugumo ir kiti specialistai (Stoneburner *et al.* 2002; ESRMO 2011). Dalyvių skaičius IT rizikos valdymo procese priklauso nuo organizacijos dydžio ir jos veiklos ypatybių.

Taigi, prieš pradedant rizikos identifikavimo procedūrą, reikia suprasti visą organizacijos aplinką, t. y. išsiaiškinti, kas vyksta įmonės viduje, kokie procesai vykdomi ir kokios atliekamos funkcijos, kokie įrenginiai ir priemonės pasitelkiami siekiant organizacijos tikslų. Tam detalizuojama įmonės sistema, kuri išskaidoma į komponentus, o atskira kiekvieno sistemos komponento analizė padeda suprasti jų paskirtį, charakteristikas, naudojimo tvarką, kartu ir nuokrypius bei galimus nuostolius. Paskui identifikuojamos kiekvieno IT sistemos elemento grėsmės, analizuojant grėsmes numatoma, kas gali įvykti, t. y. kas gali grėsti įvykti, o analizuojant pažeidžiamas vietas nustatoma, kaip tai gali atsitikti. Kitaip tariant, analizuojama, kada grėsmės santykis su pažeidžiama vieta gali padaryti nuostolių (Stoneburner *et al.* 2002, 2004; VITA 2006; Gregg 2007; ISACA 2009).

Todėl rizikų identifikavimo procesas susideda iš toliau pateiktų etapų (Stoneburner *et al.* 2004; Bowen *et al.* 2006; VITA 2006; Gregg 2007):

1. Turto identifikavimas ir IT sistemos charakteristikos.
2. Grėsmių identifikavimas.
3. Pažeidžiamų vietų sistemoje identifikavimas.
4. IT rizikų identifikavimas.

Siekiant įvertinti procesą sisteminiu požiūriu, kiekvienas etapas analizuojamas detaliau.

Turto identifikavimas ir IT sistemos charakteristikos. Organizacijos IT infrastruktūra susideda iš atskirų komponentų, susijusių tarpusavyje ir atliekančių tam tikras funkcijas (saugo ir apdoroja duomenis, juos priima iš išorės ir perduoda kitiems įrenginiams ar procesams ir t. t.), todėl būtina įvertinti visus sistemos elementus (1 lentelė).

1 lentelė. Organizacijos resursų sąrašas, skirtas turto identifikavimo ir IT sistemos charakterizavimo procedūrai (sudaryta autorių)
Table 1. List of ressources for assets and IT system characteristics (compiled by authors)

Šaltinis	Organizacijos resursai
Stoneburner *et al.* (2002)	Kompiuterinė įranga Programinė įranga Sistemos sąsajos Duomenys ir informacija Žmonės, palaikantys ir atnaujinantys IT sistemą Sistemos misija
Farahmand *et al.* (2003)	Informacija Programinė įranga Kompiuterinė įranga Žmonės Sistemos
Gregg (2007)	Kompiuterinė įranga Programinė įranga Darbuotojai Paslaugos Reputacija Dokumentacija

Analizuojant sistemą kaip atskirų elementų visumą, rizika yra lengviau aptinkama nei vertinant ją kaip vieną elementą. Turto identifikavimo proceso tikslas yra apibrėžti organizacijos sistemą (taip pat ir IT sistemą), siekiant nustatyti rizikos vertinimo ribas ir komponentus, identifikuoti IT sistemą ir duomenų pažeidiamumą (VITA 2006). Turtas gali būti apčiuopiamas arba neapčiuopiamas (Gregg 2007). Apčiuopiamas turtas yra fiziniai įrenginiai, kurie yra naudojami įmonės veikloje (tokie kaip informacinės sistemos, kompiuterinė įranga ir pan.), o neapčiuopiamas turtas – tai linkęs į informacinių sistemų atakas turtas (toks kaip finansiniai duomenys, reputacija, slapta įmonės informacija ir pan.). Identifikuojant IT sistemos riziką, visų pirma įvardijami sistemos ar jos dalių naudotojai, nustatoma jų atsakomybė ir vykdomos funkcijos. Apibrėžiant IT sistemos ribas ir komponentus, aprašomi naudojami įrenginiai (tokie kaip kompiuterio modelis, naudojama operacinė sistema, galingumas, talpa ir kiti parametrai), nustatoma IT infrastruktūra ir tinklo sąsajos (kai duomenys perduodami iš vienos sistemos kitai). Galiausiai parengiamas dokumentas, kuriame aprašomi IT sistemos komponentai, tinklo architektūra ir informacijos srautai.

Išanalizavus visus IT sistemos komponentus, juos suklasifikavus, nustatomos sistemos ribos, funkcijos, sistemos bei duomenų pažeidžiamumas (Stoneburner *et al.* 2004).

Grėsmių identifikavimas. Grėsmės gali būti suprantamos kaip rizikų priežastys. Tai yra bet kokia aplinkybė ar įvykis, kuris turi potencialą negatyviai paveikti turtą, kai pasinaudojama nesankcionuotu prisijungimu, galimybe ką nors sunaikinti, atskleisti, keisti duomenis (Gregg 2007). Elky (2006) pabrėžia, kad pati grėsmė nėra įvykis, grėsmė turi būti susieta su grėsmės sukėlėju tam, kad taptų pavojinga turtui, kitaip tariant, grėsme įvardijamas žalingų veiksmų potencialas, o kiekvienas grėsmės šaltinis gali būti susijęs su skirtinga tikimybe. Mokslininkai vieningai sutaria, kad grėsmė – tai galimybė grėsmės sukėlėjui sėkmingai pasinaudoti tam tikra pažeidžiama vieta (Stoneburner *et al.* 2002, 2004; Elky 2006; VITA 2006; Gregg 2007). Farahmand *et al.* (2003) pateikia kitokį požiūrį į grėsmę, išskirdami grėsmę į grėsmės agentą ir skverbties metodiką, paaiškindami, kad grėsmė pasireiškia tuomet, kai grėsmės agentas pasinaudoja konkrečia skverbties metodika, siekdamas sukelti nepageidaujamą poveikį tinkle.

Tačiau bendruoju atveju rekomenduotina grėsmių identifikavimą traktuoti kaip procesą, kurio metu identifikuojamos visos potencialiai galimos grėsmės, nekreipiant dėmesio į jų įvykimo tikimybę. Šio proceso rezultatas yra sąrašas, kuriame pateiktos visos galimos įvykti grėsmės. Virdžinijos informacinių technologijų agentūra (VITA) pabrėžia, kad grėsmių identifikavimo tikslas yra pateikti IT sistemoje galinčių atsirasti grėsmių sąrašą, bet ne sukurti universalų bendrų grėsmių sąrašą (VITA 2006). Nustatant grėsmes, VITA (2006) siūlo atsižvelgti į esamą IT sistemą, jos ypatybes.

Pradinis taškas pradedant išskirti ir charakterizuoti aktualias grėsmes gali būti rastas įvykių istorijoje ar remiantis geros praktikos atvejais (Sackmann 2008). Siekiant efektyviau nustatyti galimas grėsmes, rekomenduojama jas suklasifikuoti (2 lentelė).

Identifikuojant grėsmes galima pasinaudoti tokių agentūrų, kaip NIPC, OIG, FedCIRC, pagalba ar publikuojamais universaliais grėsmių sąrašais. Pavyzdžiui, detalus sąrašas pateiktas *IT-Grundschutz Manual* grėsmių kataloge, kuriame yra apie 370 grėsmių, suskirstytų į kategorijas (BSI 2008; Sackmann 2008).

Apibendrinant galima teigti, kad vieni mokslininkai grėsmes klasifikuoja į smulkesnes grupes, kiti į stambesnes, taip pat skirsto jas pagal tai, kurioje aplinkoje jos gali pasireikšti. Pažymėtina, kad, analizuojant suklasifikuotas grėsmių grupes, tikimybė praleisti vieną ar kitą grėsmę žymiai sumažėja. Pabrėžtina tai, kad grėsmių sąrašuose grėsmės taip pat klasifikuojamos, todėl naudojimasis tokiais

2 lentelė. Grėsmių klasifikacija (sudaryta autorių)

Table 2. List of threats classification (compiled by authors)

Šaltinis	Grėsmių rūšys
Bayne (2002)	Kylančios iš žmogaus (programišiai, vagystės, netechniniai darbuotojai, atsitiktinumai ir kt.) Kylančios ne iš žmogaus (potvyniai, žaibai, virusai ir kt.)
Farahmand *et al.* (2003)	Grėsmių agentai (įgaliotas vartotojas, neleistini vartotojai, aplinkos veiksniai) Prasiskverbimo technikos (fizinės, susijusios su žmonėmis, kompiuterinė įranga, programinė įranga, procedūros)
Elky (2006)	Natūralios grėsmės (potvyniai, audros ir kt.) Žmogiškos grėsmės (tyčinės ar netyčinės) Aplinkos grėsmės (elektros energijos tiekimo sutrikimai ir kt.)
Gregg (2007)	Fizinės grėsmės ir vagystės Žmogiškos klaidos Programos klaida Įrangos gedimas Aplinkos pavojai Kenkėjiška programinė įranga
BSI (2008)	Nenumatytos aplinkybės (personalo kaita, žaibas, gaisras ir kt.) Organizaciniai trūkumai (kompetencijos trūkumas ir kt.) Žmonių klaidos Techniniai gedimai Tyčiniai veiksmai
IntegrIT (2008)	Fizinės grėsmės (vagystė, ugnies ar potvynio žala) Elektroninės grėsmės (programišiai, virusai, Trojos arkliai ir kt.) Techniniai gedimai Infrastruktūros gedimai Žmogaus klaidos

sąrašais padeda tikslingai ir struktūrizuotai siekti tikslo. Kiti būdai, padedantys nustatyti grėsmes, yra „kas, jeigu“ analizė. Šis būdas labiausiai tinkamas mažose žmonių grupėse, naudojant minčių šturmo metodą (IntegrIt 2008). Scenarijų kūrimas gali būti naudingas tada, kai įmonė yra nedidelė ir IT sistema yra nesudėtinga. Taigi, kai organizacija IT riziką identifikuoja pati, siūloma rinktis SVV įmonėms rekomenduotinus metodus, o kai IT riziką identifikuoja samdomi specialistai, metodai yra parenkami pačių tyrėjų atsižvelgiant į organizacijos dydį, tyrėjų darbo įgūdžius bei taikytų metodikų patirtį ir pan.

Pažeidžiamų vietų IT sistemoje identifikavimas. Pažeidžiamos vietos arba defektai saugumo sistemose, programinėje įrangoje ar procedūrose (Gregg 2007) gali būti atsitiktinai sukelti arba tyčia jais pasinaudota (Stoneburner *et al.* 2004). Pažeidžiamos vietos yra apibrėžiamos kaip sistemos jautrumo grėsmių scenarijams matmuo (Ezell 2007). Pažeidžiama vieta pati savaime nesukelia žalos, tai

greičiau sąlyga arba sąlygų visuma, kuri sudaro prielaidas įvykti grėsmėms ir padaryti žalą turtui. Stoneburner *et al*. (2004) teigia, kad pažeidžiamumą lemia saugumo procedūrų, t. y. projektavimo, įgyvendinimo, ar vidaus kontrolės priemonių, kurios tūrėtų būti panaudotos sistemos pažeidimo atveju, trūkumas. Taigi pažeidžiamumas bendrąja prasme gali būti apibūdinamas kaip sistemos silpnoji vieta, kurią galima paveikti padarant žalą.

Supratus konkrečią grėsmę, pažeidžiamas vietas galima nustatyti minčių šturmo būdu, pasinaudojus kontroliniu sąrašu ar pažeidžiamų vietų skenavimo programine įranga (pvz.: NESSUS, *SystemScanner*, *Retina*, *NetRecon*, Whisker, CyberCop), o dokumentuojant rekomenduojama nurodyti techninį pavyzdį. Galimos pažeidžiamų vietų sritys pateikiamos 3 lentelėje. Akcentuotina tai, kad kiekviena grėsmė gali pažeisti keletą silpnųjų sistemos vietų (Vidalis, Jones 2003; Microsoft Corporation 2008).

3 lentelė. Pažeidžiamų vietų sritys (sudaryta autorių)
Table 3. Areas of vulnerabilities (compiled by authors)

Šaltinis	Sritys
Stoneburner *et al.* (2002)	Pažeidžiamų vietų šaltiniai Sistemos saugumo bandymai Saugumo reikalavimų kontroliniai sąrašai
Vidalis, Jones (2003)	Fiziniai veiksniai Natūralūs veiksniai Kompiuterinės ir programinės įrangos veiksniai Žiniasklaidos veiksniai Komunikacijos veiksniai Žmogiškieji veiksniai

Pažeidžiamų vietų nustatymo metodai gali skirtis priklausomai nuo IT sistemos pobūdžio ir nuo to, kuriame sistemos gyvavimo etape ji yra (Stoneburner *et al.* 2002):

- Jei IT sistema kuriama, pažeidžiamų vietų nustatymo sistema tūrėtų būti paremta organizacijos saugumo politika, saugumo procedūrų planavimu ir sistemos reikalavimų nustatymu bei produkto pardavėjų arba kūrėjų produkto apsaugos analize.
- Jei IT sistema yra diegiama, pažeidžiamų vietų nustatymo sąrašą tikslinga praplėsti informacija atsižvelgiant į papildomas planuojamas apsaugines priemones, nurodomas naujai diegiamos sistemos dokumentuose ir pan.
- Jei IT sistema yra veikianti, pažeidžiamų vietų identifikavimo procesas turėtų apimti IT sistemos apsaugos ir saugumo kontrolės analizę, naudojant technines priemones.

Apibendrinant analizės rezultatus, galima teigti, kad vienas iš paprastesnių būdų nustatant pažeidžiamas sistemos vietas yra pasinaudoti specialiai tam tikslui skirta programine įranga. Tačiau praktikoje galėtų būti naudojama Vidalis ir Jones (2003) pasiūlyta klasifikacija, kurioje pažeidžiamos vietos skirstomos pagal jų kilmę. Nustatant pažeidžiamas IT sistemos vietas reikia atsižvelgti į IT saugumo strategijas, procedūras, įvertinti technologinius saugumo aspektus, saugumo kontrolę, veiklas, procesus ir kt. Vidalis ir Jones (2003) rekomenduoja naudoti pažeidžiamų vietų medį, siekiant geriau suprasti ir išanalizuoti skirtingus galimų atakų scenarijus.

Taigi nagrinėjant pažeidžiamas vietas ir jų ryšius, galima identifikuoti potencialių grandininių reakcijų scenarijus (Vidalis, Jones 2003). Remiantis šiais scenarijais yra galimybė įvertinti pavojus ir užkirsti jiems kelią.

IT rizikų identifikavimas. Nei grėsmė viena savaime, nei pažeidžiama vieta be grėsmės nekelia pavojaus organizacijai. Todėl identifikuojant IT rizikas vertinami ir analizuojami grėsmių ir pažeidžiamų vietų santykiai. Pažymėtina, kad viena grėsmė gali realizuotis keliose skirtingose pažeidžiamose sistemos vietose ir taip sukelti kelias skirtingas rizikas (Stoneburner *et al.* 2002; Vidalis, Jones 2003). Norint identifikuoti šias rizikas, rekomenduojama sudaryti grėsmių ir pažeidžiamų vietų matricą. Paskui, siekiant nustatyti būsimų nepalankių įvykių tikimybę, IT sistemos grėsmės turi būti analizuojamos kartu su potencialiomis pažeidžiamomis vietomis ir IT kontrolės mechanizmais organizacijoje (Stoneburner *et al.* 2004). Šį etapą Elky (2006) vertina kaip vieną iš sunkesnių visame rizikų valdymo procese.

Išvados

Suvokiant IT riziką kaip verslo riziką ir įvertinus tai, kad ji kyla dėl netinkamo sistemos apsaugos įgyvendinimo ar įmonės valdymo, siektina detaliai išanalizuoti organizacijos sistemą ir nustatyti gresiančias IT rizikas. IT rizikos identifikavimas yra sudėtinis procesas, susidedantis iš keturių etapų (turto ir IT sistemos charakteristikų identifikavimo, grėsmių identifikavimo, pažeidžiamų vietų sistemoje nustatymo ir IT rizikų identifikavimo), o jo rezultatas yra rizikų sąrašas. Kiekvienas etapas yra savitas ir atliekamas pasirenkant konkretų būdą:

- Turtas ir IT sistemos charakteristikos identifikuojamos pasitelkiant organizacijos resursų skirstymą pagal jų paskirtį.
- Sėkmingai grėsmės identifikuojamos pasitelkiant grėsmių klasifikaciją. Smulkioms ir vidutinio dydžio įmonėms rekomenduotina grėsmes nustatyti minčių šturmo būdu, modeliuojant scenarijus. Taip pat naudinga pasinaudoti siūlomais grėsmių sąrašais.

- Pažeidžiamoms vietoms sistemoje nustatyti gali būti naudojama tam tikslui skirta speciali skenavimo programinė įranga. Pažeidžiamų vietų medžio analizė leidžia sėkmingai identifikuoti potencialių grandininių reakcijų scenarijus.
- Kiekviena grėsmė gali realizuotis dėl vieno ar kelių organizacijos sistemoje esančių pažeidžiamų vietų, todėl įvardijama viena ar kelios rizikos. Tam tikslui rekomenduojama sudaryti grėsmių ir pažeidžiamų vietų matricą.

Atlikta vieno iš IT rizikos valdymo proceso etapų – IT rizikos identifikavimo – analizė leido nustatyti IT rizikos identifikavimo skirtumus, atsižvelgiant į organizacijos dydį, IT infrastruktūrą ir pan. Atlikus tyrimą nustatyti IT rizikos identifikavimo metodai rekomenduojami SVV įmonėms; jie skiriasi nuo pasaulyje pripažintų ir plačiai taikomų tradicinių IT rizikos valdymo metodikose rekomenduojamų metodų.

Literatūra

Azizi, N.; Hashim, K. 2010. Enterprise Level IT Risks: An Assessment Framework and Tool, in *Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conference on 9–11 July 2010* 3**:** 333-336. http://dx.doi.org/10.1109/ICCSIT.2010.5563565

Bayne, J. 2002. *An Overview of Threat and Risk Assessment*, SANS Information Security Reading Room [interaktyvus], [žiūrėta 2012 m. rugsėjo 22 d.]. Prieiga per internetą: http://www.sans.org/reading_room/whitepapers/auditing/overview-threat-risk-assessment_76

Bowen, P.; Hash, J.; Wilson, M. 2006. Information Security Handbook: A Guide for Managers, *NIST Special Publication 800-100.*

BSI 2008. BSI Standard 100-2 IT-Grundschutz Methodology [interaktyvus], [žiūrėta 2012 m. rugsėjo 22 d.]. Prieiga per internetą: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile

Davidavičienė, V. 2008. Change management decisions in the information age, *Journal of Business Economics and Management* 9(4): 299–307. http://dx.doi.org/10.3846/1611-1699.2008.9.299-307

Davidavičienė, V.; Raudeliūnienė, J. 2010. ICT in tacit knowledge preservation, in *The 6th International Scientific Conference "Business and Management' 2010"*. Selected Papers (2): 436–442. ISSN 2029-4441, http://dx.doi.org/10.3846/bm.2010.109

Elky, S. 2006. An introduction to information system risk management, *SANS Institute InfoSec Reading Room* [interaktyvus], [žiūrėta 2012 m. spalio 12 d.]. Prieiga per internetą: http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204

ESRMO 2011. Risk Management Guide [interaktyvus], [žiūrėta 2012 m. spalio 20 d.]. Prieiga per internetą: http://www.esrmo.scio.nc.gov/riskManagement/default.aspx

Ezell, B. C. 2007. Infrastructure Vulnerability Assessment Model (I-VAM), in *Risk Analysis* 27(3): 571–583. http://dx.doi.org/10.1111/j.1539-6924.2007.00907.x

Farahmand, F.; Navathe, S. B.; Sharp, G. P.; Enslow, P. H. 2003. Managing vulnerabilities of information systems to security incidents, in *ICEC '03 Proceedings of the 5th International Conference on Electronic Commerce*: 348–354. http://dx.doi.org/10.1145/948005.948050

Fratila, L.; Tantau, A. 2008. Aspects of IT Risk Management for a company, in *International Scientific Conference "European Integration – New Challenges for the Romanian Economy", 4th Edition.* Orade, Romania 30–31 May 2008. Section: Economy and business administration: 163–168. ISSN-1582-5450.

Gao, G.; Li, X.; Zhang, B.; Xiao, W. 2011. Information Security Risk Assessment Based on Information Measure and Fuzzy Clustering, *Journal of Software* 6(11): 2159–2166.

Gregg, M. 2007. *CISA Exam Prep*. Publisher: Pearson Certification. 600 p. Print ISBN-10: 0-7897-3573-3, Print ISBN-13: 978-0-7897-3573-7.

IntegrIT 2008. Identifying & Managing IT Risks to Your Business [interaktyvus], [žiūrėta 2012 m. liepos 12 d.]. Prieiga per internetą: http://www.integrit-network.com/bcp/IntegrIT-Identifying_Managing_IT_Risks_Your-Business.pdf

ISACA 2009. RiskIT Brochure [interaktyvus], [žiūrėta 2012 m. rugsėjo 10 d.]. Prieiga per internetą: http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx

Janeliūnienė, R.; Liberytė, G.; Davidavičienė, V. 2011. IT auditas Lietuvos smulkaus ir vidutinio dydžio įmonėse, *Mokslas – Lietuvos ateitis*. *Verslas XXI amžiuje* 3(4): 13–20. Vilnius: Technika. ISSN 2029-2341.

Microsoft Corporation 2008. *The Security Risk Management Guide*, Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence [interaktyvus], [žiūrėta 2012 m. liepos 08 d.]. Prieiga per internetą: http://trygstad.rice.iit.edu:8000/Books/TheSecurityRiskManagementGuide-Microsoft.pdf

Pabedinskaitė, A. 2009. Successful implementation of ERP Systems, in *The 9th international conference "Liberec Economic Forum 2009"*, 15–16 September 2009. Liberec, Czech Republic, 275–283. ISBN 9788073725235.

Pabedinskaitė, A. 2010. Factors of successful implementation of ERP systems, *Ekonomika ir vadyba* 15: 691–697. Prieiga per internetą: http://www.ktu.lt/lt/mokslas/zurnalai/ekovad/15/1822-6515-2010-691.pdf. ISSN 1822-6515

Paliulis, N. K.; Uturytė-Vrubliauskienė, L. 2012. Performance measurement system to evaluate the efficiency of e-business, in *The 7th international scientific conference "Business and Management 2012"*. Selected papers. May 10–11, 1: 895–903. ISSN 2029-4441. Prieiga per internetą: http://leidykla.vgtu.lt/conferences/BM_2012/information_and_communication/895_903_Paliulis.pdf

Paliulis, N. K.; Mačiulytė-Šniukienė, A.; Vizbaras, A. 2012. Informacinės visuomenės plėtros ir jos įtakos darbo produktyvumui vertinimas: Lietuva Europos Sąjungos šalių kontekste, *Ekonomika ir vadyba: aktualijos ir perspektyvos* 2(26): 17–32. ISSN 1648-9098.

Sackmann, S. 2008. A Reference Model for Process-Oriented IT Risk Management, in *Proceedings of ECIS 2008*. 246 p. [interaktyvus], [žiūrėta 2012 m. balandžio 01 d.]. Prieiga per internetą: http://aisel.aisnet.org/ecis2008/246

Savić, A. 2008. Managing IT-Related Operational Risks, *Economic Annals* 53(176): 88–109. http://dx.doi.org/10.2298/EKA0876088S

Smith, H. A.; McKeen, J. D. 2009. A Holistic Approach to Managing IT-based Risk, in *Communications of the Association for Information Systems* 25(41): 519–530.

Stoneburner, G.; Goguen, A.; Fering, A. 2002. Risk Management Guide for Information Technology Systems, *NIST Special Publication 800-30.*

Stoneburner, G.; Hayden, C.; Feringa, A. 2004. Engineering Principles for Information Technology Security, *NIST Special Publication 800-27 Rev A* June 2004.

Tansley, N. 2007. A Methodology for Measuring and Monitoring IT Risk, *Master Technologiae in Business Information Systems*.

Tchankova, L. 2002. Risk identification – basic stage in risk management, *Environmental Management and Health* 13(3): 290–297. http://dx.doi.org/10.1108/09566160210431088

Vidalis, S.; Jones, A. 2003. *Using Vulnerability Trees for Decision Making in Threat Assessment*, School of Computing Technical Report CS-03-2. School of Computing, University of Glamorgan, Pontypridd, CF37 1DL, Wales, UK.

VITA 2006. Information Technology Risk Management Guideline, *ITRM Guideline SEC506-01, Appendix D – Risk Management Guideline Assessment Instructions* [interaktyvus], [žiūrėta 2012 m. spalio 25 d.]. Prieiga per internetą: http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/unmanaged/library/RiskManagementGuideline.pdf

Westerman, G.; Hunter, R. 2007. *IT Risk. Turning Business Threats into Competitive Advantage*. Harvard Business School Press. 221 p. ISBN-10: 1422106667 / ISBN-13: 978-1422106662.

IT RISK IDENTIFICATION PROCESS ANALYSIS

R. Janeliūnienė, V. Davidavičienė

Abstract

Business processes and business success that depends on information technology (IT) is now closely associated with IT risks, which is influenced by growing IT risk management and control needs. It is vitally important to identify, analyse and reduce systemic risk in order to avoid undesirable consequences, such as information loss, data leaks or damage. A critical success factor in this situation is the systematic and continuous IT risk management. This paper aims to analyse one part of the IT risk management process –risk identification. The article invoked the methods of literature analysis, synthesis, comparison, and generalization.

Keywords: IT risk, IT risk identification, IT risk management, information technology.