Daiktų interneto technologijos taikymo versle nauda ir rizika

Laima Zalieckaitė

Vilniaus universiteto Ekonomikos fakulteto
Ekonominės informatikos katedros docentė
Vilnius University, Faculty of Economics,
Economics Informatics Department, Assoc. prof.
Saulėtekio al. 9, II rūmai, 309 kab.
El. paštas: laima.zalieckaite@ef.vu.lt

Raimundas Žilinskas

Vilniaus universiteto Ekonomikos fakulteto
Ekonominės informatikos katedros docentas
Vilnius University, Faculty of Economics,
Economics Informatics Department, Assoc. prof.
Saulėtekio al. 9, II rūmai, 309 kab.
El. paštas: raimundas.zilinskas@ef.vu.lt

Daiktų interneto technologija yra viena iš naujausių ir sparčiai besivystančių informacinių ir komunikacinių technologijų krypčių. Ji atsirado šio amžiaus pradžioje, tačiau versle ėmė plisti antrajame dešimtmetyje. Daiktų internetas yra ne tik technologija, kurios paslaugos skirtos verslui, bet ir naujas verslo modelis. Kaip rodo pasaulinė šių technologijų taikymo patirtis ir naujausi tyrimai, daiktų interneto paslaugų ir taikymų mastai versle per pastaruosius metus nepaliaujamai didėja ir ateityje tik didės. Didžioji dalis verslo įmonių pripažįsta, kad daiktų interneto technologija gali vienaip ar kitaip padėti efektyviau organizuoti veiklą, spartinti technologinius ir verslo komunikacinius procesus, didinti veiklos efektyvumą. Kartu pripažįstama, kad naudojanti daiktų internetą verslo aplinka plečiasi, tampa atviresnė, bet ir labiau pažeidžiama. Dėl to daiktų interneto naudojimas ir plitimas neišvengiamai didina informacinių sistemų, o sykiu ir verslo rizikingumą. Naudojant daiktų internetą įranga sąveikauja tarpusavyje, o asmenys bendrauja naudodamiesi daiktų interneto įranga kaip netiesioginio bendravimo tarpininku – tai savo ruožtu yra didelė saugumo problema, susijusi su apsimetinėjimu, įsilaužimais ir kitomis elektroninėmis grėsmėmis. Šiame straipsnyje analizuojama daiktų interneto technologijos taikymo nauda verslui, jos rizika ir priemonės rizikai apriboti.

Pagrindiniai žodžiai: *daiktų internetas, radijo dažnių atpažinimo technologija, saugumas, rizika.*

Įvadas

Internetas suteikė naujų galimybių verslui plėsti. Laikui bėgant verslas suprato, kad internetas – tai ne tik puikus reklamos šaltinis. Šio amžiaus pirmajame dešimtmetyje atsirado nauja technologija – daiktų internetas, kuris leidžia sujungti verslo procesus ir įrenginius į vieną tinklą ir didinti informacijos kaupimo mastus bei valdymo našumą. Daiktų internetas (angl. *Internet of Things* – IoT) tarnauja verslui, nes, kaip rodo didžiausios pasaulyje audito ir kon-

sultacijų bendrovės „Deloitte Touche Tohmatsu Ltd.“ (DTTL) prognozės, 2015 m. bus nupirkta daugiau nei 60 proc. iš 1 mlrd. pasaulinių bevielių IoT įrenginių, o už juos sumokės ir juos naudos verslas. Pasaulio verslo lyderiai trimatį spausdinimą, daiktų internetą ir biotechnologijas apibūdina kaip proveržio technologijas, kurios artimiausiu metu iš esmės keis kasdienybę ir turės daug įtakos verslo plėtrai. Tai rodo KPMG atlikta inovacijų technologijų srities apklausa, kurioje dalyvavo 768 technologijų verslo lyderiai iš viso pasaulio (KPMG..., 2014).

Proveržio technologijos – tai sparčiai besivystančios technologijos, kurios, sudarydamos sąlygas atsirasti naujoms paslaugoms ir prekėms, kartu paskatins kurti naujus verslo modelius bei iš esmės transformuos kai kuriuos verslo sektorius. KPMG apklausa rodo, kad visų šių sričių staigų kilimą lemia keletas veiksnių, t. y. palankios makroekonomikos sąlygos, vietinio lygmens iniciatyvos ir bendras inovacijų technologijų srities augimas visame pasaulyje, kartu skatinantis ir platesnius verslo pokyčius.

Manoma, kad didžiausią potencialą augti ateityje turi mažmeninės prekybos srities verslai (20 proc.), automatines sistemas namuose diegiantys verslai (14 proc.) ir apsaugos bei socialinio bendravimo sričių verslai (po 12 proc,). Paklausus, kokie sektoriai dėl proveržio technologijų labiausiai pasikeis per artimiausius trejus metus, daugiausia nurodyta technologijų sektorius (21 proc.), vartotojų rinkos (12 proc.), sveikatos apsaugos sektorius (11 proc.) ir transporto bei gamybos sektoriai (po 10 proc.).

Daiktų internetas – viena iš trijų besiformuojančios vientisos globalios operacinės sistemos dalių kartu su informacijos ir logistikos internetu. Tai sumaniosios infrastruktūros revoliucijos pasaulyje dalis.

Vis daugiau pastatų, transporto priemonių, buitinių prietaisų bus aprūpinta jutikliais ir sujungta su sumaniais matuokliais bei daiktų interneto platforma. Tai, savo ruožtu, padidins gamybos, elektros ir kitų išteklių vartojimo efektyvumą.

Daiktų internetas būtų neįmanomas be šiuolaikinių koncepcijų ir technologijų, t. y.:

- radijo dažnių atpažinimo (RDA), suteikiančio galimybę identifikuoti objektus ir nuskaityti jų informaciją be prisilietimo prie jų, technologija;
- integruojamos į daiktus ir aplinką įrangos gabaritų minimizavimas;
- duomenų perdavimo ir apdorojimo pajėgumų didėjimas;
- dirbtinis intelektas ir pan.

Daiktų internetas vykdo perversmą ne tik asmens gyvenime, bet ir įvairiose verslo šakose, valstybės infrastruktūros lygmeniu. Daiktų internetas suteikia galimybę gauti duomenis apie tai, kaip naudojami fizinio pasaulio daiktai. Vartojamų daiktų aprūpinimas davikliais leidžia verslui gauti tikslesnę informaciją apie vartotojų įpročius, elgseną ir poreikius. Tai savo ruožtu padeda tobulinti produktus, efektyviau organizuoti jų tiekimą ir pan. (Bandyopadhyay, Sen, 2011).

Daiktų internetas tiesiogiai ar netiesiogiai veikia verslą, sudaro sąlygas spartinti verslo procesus, didinti apyvartą, tačiau kartu dindina verslo sistemų atvirumą, pažeidžiamumą ir riziką.

Straipsnio tyrimo objektas – daiktų interneto technologijos procesai.

Straipsnio tikslas – išanalizuoti daiktų interneto technologijos taikymo versle galimą naudą ir riziką.

Daiktų interneto technologija

Informacinių technologijų prietaisai ir internetas tapo gyvenimo atributais. Visose vers-

lo srityse valdymas vykdomas internetu ir skaitmeniniais prietaisais, sąveikaujančiais per tinklą. Duomenys tinklu perduodami atliekant sąveiką tarp įrenginių – interneto daiktų. Daiktų internetas yra nauja tinklų konfigūracija, apimanti fizinių objektų komunikaciją ir objektų bei žmonių sąveiką internete. Daiktų interneto kontekste daiktu laikomas fizinio pasaulio objektas (fizinis daiktas) arba informacijos pasaulio objektas (virtualusis daiktas), kuris gali būti identifikuotas ir integruotas į ryšių tinklus (ITU..., 2012).

Daiktų internetas yra gana nauja sąvoka, todėl šiuo metu yra keletas daiktų internetą apibūdinančių sampratų. Pateiksime jas:

- Daiktų internetas yra laiko momentas, kai objektų arba daiktų, prijungtų prie interneto, yra daugiau negu žmonių (Chase, 2014);
- Globalus tinklas, jungiantis išmaniuosius objektus (Atzori et al., 2010);
- Daiktų internetas – dinaminio globalaus tinklo infrastruktūra, kurioje fiziniai ir virtualūs „daiktai“ turi savo tapatybes ir fizinius atributus (Fries, Vermesan, 2014);
- Fizinių objektų tinklas, kuriame yra integruotos technologijos, skirtos komunikuoti, identifikuoti ir reaguoti į vidinius tinklo elementų arba į išorės elementų pasikeitimus (Mioradi, 2013).

Apibendrindami galime teigti, kad daiktų internetas yra tinklas, kuriame fiziniai objektai sujungti tarpusavyje, žmonių ir objektų bendravimas vyksta per fizinius objektus, o valdymas vykdomas virtualiai. Kiekvienas objektas turi savo identifikaciją – elektroninę žymą – ir yra nuolat prijungtas prie duomenų bazės bei tinklo, todėl objektus galima kontroliuoti ir valdyti. Be to, pabrėžtina, kad daiktų interneto paskirtis – patogesnis ir greitesnis IoT įrenginių komunikavimas tarpusavyje bei „daiktų“ naudojimas įvairioms paslaugoms (Li, 2015).Veiksniai, kurie padarė įtaką daiktų interneto atsiradimui (Jankowski et al., 2014):

- IoT įrenginių kainų mažėjimas;
- Internetinio ryšio kokybės ir pralaidumo didėjimas;
- Duomenų apdorojimo greičio didėjimas ir kainos mažėjimas;
- Išmaniųjų telefonų tapsmas sąsaja, leidžiančia kreiptis į daiktų internetą;
- Belaidžio interneto technologija, kuri leidžia verslui pritraukti klientus naudotis nenutrūkstama interneto terpe;
- Didieji duomenys (angl. *Big date*). Daiktų internetas yra terpė apdoroti ir analizuoti didžiuosius duomenis. Didieji duomenys gali būti apdorojami įvairiomis technologijomis, tačiau daiktų internetas šią funkciją atliks geriausiai;
- Nauji internetinio ryšio palaikymo standartai (IPv6 technologija, kuri yra interneto protokolų 6 versija).

Taigi daiktų interneto atsiradimą lėmė įvairialypės technologijos ir jų plėtra. Daiktų internetas yra technologija, leidžianti valdyti verslo procesus, tačiau ji turi savo privalumų ir trūkumų, kuriuos panagrinėkime detaliau.

Daiktų interneto privalumai verslui:

- *Informacijos pateikimas ir analizė*. Kiekviena verslo sritis privalo kaupti ir analizuoti informaciją, kuri yra susijusi su verslo procesų įgyvendinimu. Analizė padeda verslui ne tik įvertinti esamą situaciją rinkoje, bet ir priimti būtinus sprendimus. Surinkta informacija turi būti pateikta laiku, ji turi būti teisinga, patikima, aiški, nesidubliuojanti, nes netikslumai gali iškreipti duomenų analizės rezultatus. Daiktų internetas gali išspręsti šią problemą, nes duome-

nys renkami automatiniu būdu. Daiktų interneto technologija galima surinkti daugiau ir tikslesnės informacijos, nes kiekvienas IoT įrenginys, prijungtas prie daiktų interneto tinklo, pateikia savo veiklos informaciją. Didesnis ir tikslesnės informacijos kiekis leidžia parengti gilesnes analizes ir priimti verslui tinkamus sprendimus.

- *Nuolatinė stebėsena*. Kiekviename versle svarbu nuolat stebėti verslo objektus. Stebėsena vykdoma siekiant laiku pamatyti galimą problemą ir jos atsiradimo priežastis. Laiku pastebėta problema lengviau ištaisoma. Daiktų internetas gali vykdyti stebėseną savarankiškai ir informuoti apie problemų atsiradimo židinius.
- *Darbo laiko taupymas ir verslo sąnaudų mažinimas*. Verslo informacijos rinkimas ir stebėsena yra daug laiko reikalaujantys ir brangūs procesai. Daiktų interneto technologija leidžia taupyti verslo organizacijos laiką ir pinigus, nes renka informaciją savarankiškai ir informuoja darbuotojus apie atsiradusias problemas.

Daiktų interneto trūkumai:

- *Suderinamumo problemos*. Šiuo metu nėra bendro daiktų interneto taikymo ir naudojimo standarto. Tai gali sukelti nepatogumų, kai kelios verslo įmonės nori sujungti savo turimus tinklus ir įrangą bei pasidalyti sukaupta informacija.
- *Naudojimo problemos*. Nors iš pirmo žvilgsnio atrodo, kad daiktų internetas yra gana paprastas darinys, tačiau jis gali sunkinti sudėtingų verslo procesų funkcionavimą. Realūs verslo procesai turi daug išimčių ir apribojimų, kurie turi būti perkelti į daiktų interneto erdvę.
- *Privatumo ir saugumo problemos*. Daiktų internetas suteikia verslui galimybę valdyti didelį duomenų kiekį. Sukaupta informacija yra labai vertinga verslui, tačiau daiktų interneto technologijos diegimas į verslo procesus gali sukelti grėsmę unikaliems verslo duomenims.

Kadangi daiktų internetas yra naujas darinys, kuris padeda verslui augti ir įgyvendinti išsikeltus tikslus, taikant versle naują technologiją privalu atsižvelgti į keletą veiksnių. Pirmiausia, daiktų internetas reikalauja didesnių duomenų saugumo reikalavimų ir naujų dalijimosi informacija tarp verslo įmonių standartų. Antra, unikalios verslo patirties perkėlimas į daiktų interneto terpę yra sudėtingas procesas, kuriam reikia daug laiko.

Daiktų interneto aprėptis ir nauda verslui

Daiktų interneto aprėptis yra milžiniška, nes gali būti naudojamas tiek individo kasdieniame gyvenime, tiek verslo, tiek viešajame sektoriuose. Be to, ateityje daiktų internetas gali būti efektyviai naudojamas ir visos valstybės lygmeniu.

Didelė daiktų interneto aprėptis lemia, kad jis gali būti taikomas įvairiuose verslo sektoriuose ir jo teikiama nauda verslui yra didžiulė. Galima teigti, kad daiktų internetas yra puikus variklis naujiems verslo produktams ir paslaugoms kurti. Be to, jis skatina ekonominį efektyvumą.

Daiktų interneto įtaka ekonomikai didėja, kai vartotojai, verslas, miestų valdžia, medicina ir pan. randa naujų daiktų interneto technologijos taikymo atvejų. Pagal tyrimo bendrovės *Gartner* vertinimus, bendra pelno apimtis iš daiktų interneto paslaugų 2015 m. sudarys 69,5 mlrd. dolerių, o

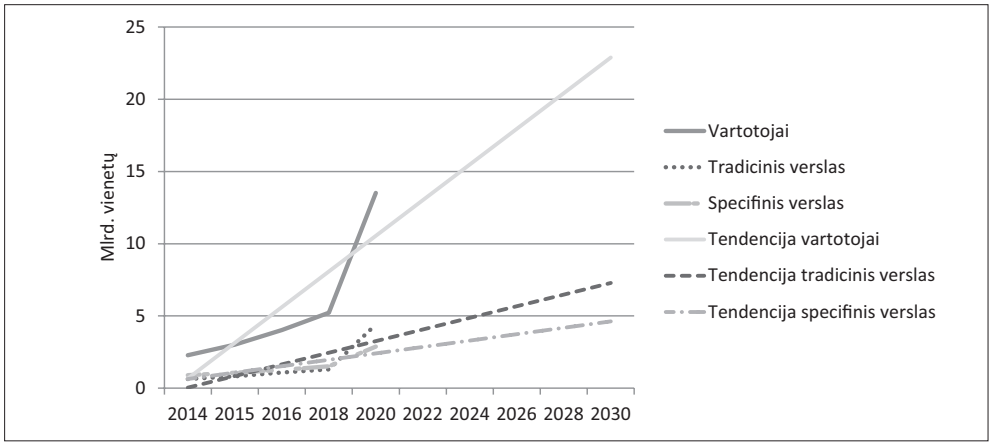
2016 m. – 22 proc. daugiau, t. y.84,8 mlrd. dolerių (Gartner ..., 2015). Tačiau verta pažymėti, kad vartojamieji taikymai palaiko prijungiamų IoT įrenginių skaičiaus augimą, o didžiąją dalį pelno augimo lemia taikymai versle. *Gartner* prognozuoja, kad 2016 m. visame pasaulyje bus naudojama 6,4 milijardo susijusių IoT įrenginių. Apibendrindami šiuos duomenis, detalizuodami IoT įrenginių skaičių pagal vartotojų pobūdį kiekvienais metais ir ekstrapoliuodami turimus duomenis, galime atlikti IoT įrenginių kiekio kitimo tendencijos prognozę iki 2025–2030 m., naudodami kitimo krypties funkcijas. Nustatytos tendencijos rodo, kad daiktų interneto įrenginių skaičius po 2025 m. ir vėliau augs, tačiau augimo tempai bus lėtesni nei 2014–2020 m. dėl to, kad internetas bus prisotintas įrenginių (1 pav.).

IoT įrenginius galima skirstyti į dvi dideles klases. Pirmoji klasė naudojama tradiciniame versle horizontaliu lygiu – tradicinėse ir tarpšakinėse verslo srityse. Antroji klasė – tai specifiniai įrenginiai, kurie gali būti naudojami ypatingose specializuotose verslo šakose (specifiniu vertikaliu pjūviu).

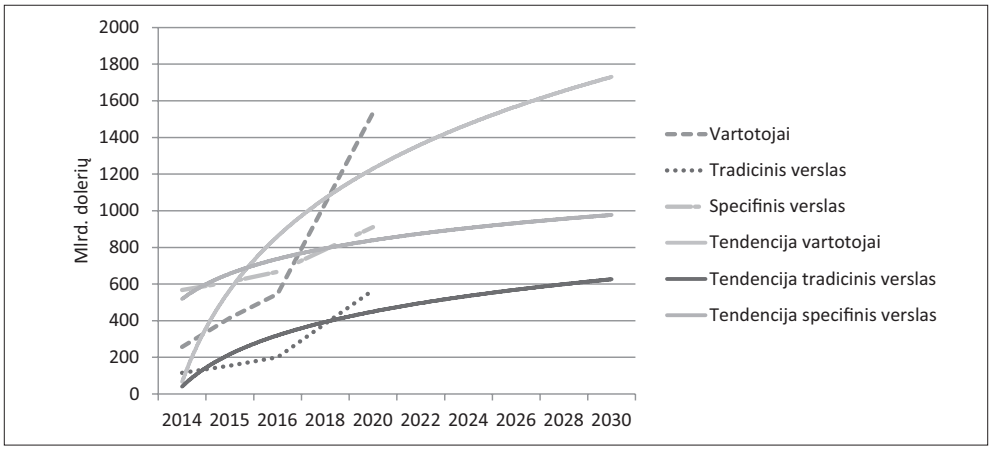
Vertinant išlaidas, skirtas IoT įrenginiams, vartotojų išlaidos pasieks 546 mlrd. JAV dolerių 2016 m., o verslui bendrai – 868 mlrd. JAV dolerių (Gartner ..., 2015). Remdamiesi šiais duomenimis ir pasinaudodami analogišku metodu, kaip ir formuodami duomenis 1 paveikslui, galime atlikti išlaidų IoT įrenginiams prognozę iki 2025–2030 m. (2 pav.).

Nors specifiniame versle naudojamos įrangos kiekis 2014–2015 m. viršys tradiciniame versle naudojamos įrangos kiekį, tačiau prognozuojama, kad po 2018 m. padėtis pasikeis (1 pav.). Išlaidų IoT technologijai struktūra gerokai skiriasi nuo naudojamos įrangos kiekio struktūros. Išlaidos specifinei įrangai (specifinis verslas) yra gerokai didesnės už išlaidas įrangai, naudojamai tradiciniame versle, nors prognozuojamas specifinės įrangos kiekis yra mažesnis. Tai paaiškinama tuo, kad specifinės įrangos vieneto kaina yra gerokai didesnė už serijinės įrangos kainą. Kaip rodo tendencijos kreivės (2 pav.), ateityje skirtumas tarp šių išlaidų mažės. Be to, išlaidų įrangai didėjimo tempai yra mažesni, palyginti su įrangos kiekio didėjimo tempais, nes įrangos kainos palaipsniui mažėja.

Prie daiktų interneto prijungti įrenginiai (bankomatai, keleivių registracijos



1 pav. ***IoT įrenginių skaičiaus*** *(mlrd. vienetų)* ***prognozė***



2 pav. ***Išlaidų daiktų interneto technologijoms prognozė*** *(mlrd. dolerių)*

terminalai oro uostuose) „atrandami“ iš naujo, nes įgyja skaitmeninius sensorius, komunikacines ir skaičiavimų atlikimo galimybes. Galima sakyti, kad daiktai įgauna „skaitmeninį balsą“, t. y. galimybę kurti ir perduoti informacijos srautus apie savo būklę ir išorinę aplinką. Tai leidžia verslui siūlyti naujas paslaugas ir naujus įrenginių naudojimo scenarijus, t. y. kurti naujus verslo modelius.

Kaip mano ekspertai, artimiausiais metais į IoT įrenginius įdiegtas tam tikras intelektualumo ir komunikacinių galimybių lygis taps standartu, kuris pasieks ir plataus vartojimo produktus bei paslaugas.

Daiktų internetas turi savybes, kurios yra labai naudingos verslo sektoriui (Dave, 2012):

- Daiktų internetas – tai nauja rinka, jungianti į visumą žmones, verslo procesus, IoT įrenginius. Daiktų internetas gali sujungti 99 proc. visų pasaulio elementų (vienas procentas jau yra sujungtas į dabartinį interneto tinklą). Elementų jungimas leidžia efektyviai valdyti išteklius, atlikti išsamesnes verslo informacijos analizes ir optimizuoti verslo procesus.
- Daiktų internetas – tai visa ko sujungimas. Svarbu pabrėžti, kad daiktų internetas nesiekia sujungti visų pasaulio kompiuterių į vieną tinklą. Pagrindinė ir išskirtinė daiktų interneto savybė – jungti daiktus, kurie nėra kompiuteriniai įrenginiai. Taigi daiktų internetas sujungia skirtingos paskirties daiktus tam, kad jų veikla galėtų būti koordinuota ir tikslinga. Todėl pagrindinė daiktų interneto teikiama nauda šia prasme yra verslo procesų automatizavimas ir veiklos valdymas. Be to, daiktų interneto technologija suteikia bet kokiai verslo veiklai skaidrumą, nes pateikia patikimus analitinius duomenis, kurių pagrindu galima rengti kokybiškas veiklos ataskaitas ir tobulinti verslo procesus.
- Daiktų internetas – tai išorinis darinys, reikalaujantis apsaugos priemonių. Daiktų interneto technologija, įdiegta bet kurioje verslo organizacijoje, tampa ne tik vidiniu verslo organizacijos elementu, bet ir išoriniu, nes nuo jos tampa priklausomi verslo ištekliai ir procesai. Todėl ypač svarbu užtikrinti saugų daiktų interneto funkcionavimą. Pažymėtina, kad kiekvienas įrenginys, kuris prijungtas prie daiktų interneto tinklo, turi būti ne tik tinkamai apsaugotas, bet ir užtikrintas bei palaikomas

jo patikimumas. Saugumo reikalavimai garantuoja gyvybiškai svarbių verslo organizacijos duomenų apsaugą, patikimumo lygį ir atkūrimo veiksmus.

- Daiktų internetas – tai inovatyvių sprendimų priėmimo sistema, kuriai būtina verslo partnerystė, nes daiktų internetas yra taikomas ir įvairiose verslo srityse. Todėl, norint priimti tinkamus verslo sprendimus, būtina atsižvelgti ne tik į vidinius, bet ir į išorinius verslo atžvilgiu veiksnius ir papildyti verslo organizacijos kompetencinius išteklius. Verta pabrėžti, kad partnerystės savybė užtikrina nenutrūkstamą ir nuolat profesionaliai palaikomą daiktų interneto infrastruktūrą.

Taigi viena iš svarbiausių daiktų interneto savybių yra ta, kad į daiktų interneto tinklą galima įtraukti bet kokius IoT įrenginius, o tai ir daro ją unikalia technologija. Be to, daiktų internetas yra nauja ir labai perspektyvi rinka, todėl šioje rinkoje yra puikios sąlygos verslo organizacijai parodyti savo unikalų produktą, užimti stabilią padėtį rinkoje ir palaikyti verslo plėtrą.

Pagrindinės verslo sritys, kuriose labiausiai taikytinas daiktų internetas, galėtų būti šios:

- Aplinkosauga – jutikliais integruoti daiktai stebi poveikį aplinkai, gauna ir apdoroja įrangos pateiktą informaciją, seka aplinkos ir vandens taršą, analizuoja rezultatus ir prireikus įjungia atitinkamo lygio pavojaus signalus.
- Žemės ūkis – daiktų internetas padeda sukurti ūkius, aprūpintus išmaniąja įranga, kurios pateikiami rezultatai leidžia racionalizuoti procesus, užtikrinti atliekų perdirbimą, racionalų technikos panaudojimą ir didinti žemės ūkio našumą.
- Transportas – automobiliuose, keliuose, sankryžose, avaringuose kelio ruožuose įdiegta įranga padeda organizuoti eismą keliuose, sumažina spūstis, reguliuoja automobilių išmetamąsias dujas pagal eismo sąlygas, interaktyviai analizuoja automobilių gedimus, pateikia pasiūlymus, kaip racionaliausiai juos pašalinti. Numatoma automobilių techninės būklės analizatorių informaciją tiesiogiai perduoti gamintojui, kuris, išanalizavęs tipinius gedimus, galės tobulinti naujus automobilius.
- Logistika – daiktų internetas sudaro galimybes stebėti ir valdyti prekių judėjimą, paskirstymą ir transportavimą, automatizuoti logistikos procesus, sutrumpinant pristatymo terminus, tinkamai panaudojant turimus išteklius, minimizuojant žmogiškąsias klaidas.
- Prekyba – daiktų interneto įranga sudaro galimybę stebėti ir valdyti užsakymų srautus, sumažinti parduotuvėse vagystes ir nuostolius, racionalizuoti pirkėjų pirkimo įpročius, individualizuoti pirkėjų atsiskaitymą už prekes, mažinti klientų eiles, didinti apyvartą. Taip pat sudaroma galimybė valdyti besibaigiančių galioti prekių srautus, užtikrinant jų kokybę, padidinti klientų pasitikėjimą prekybos įstaigomis.
- Sveikatos apsauga – daiktų internetas sveikatos apsaugos įstaigose yra labiausiai pažengusi sritis. Nuotoliniu būdu fiksuojami ir apdorojami duomenys, kurie yra reikalingi tikslingam gydymui paskirti, interaktyviai dalijamasi informacija su užsienio specialistais, ypač sudėtingų operacinių intervencijų bei sudėtingų retų ligų atvejais. Interaktyvūs daiktai leidžia žmonėms stebėti kraujospūdį, cukraus, cholesterolio kiekį organizme, širdies veiklą ir kt. bei šiuos duomenis operatyviai perduoti gydymo įstaigai. Ši sritis plečiasi ir plėsis

didžiausiu tempu, palyginti su kitomis sritimis, ir tai padės aukščiausiu lygiu užtikrinti kokybišką visuomenės sveikatos priežiūrą.

Daiktų interneto rinkos potencialas versle sparčiai auga, o jo nauda verslui neįkainojama. Galima išskirti kelis pagrindinius sektorius, kuriuos stipriai veikia ši technologija (Saminath, Jung, 2015):

- IoT įrenginių sujungimas, kuris suteikia verslo objektams fizinę galimybę būti arčiau vienas kito;
- Išmanieji namai, kurie suteikia verslui galimybę jaustis savo biurų patalpose saugiau ir patogiau;
- Išmanieji miestai, kurie suteikia verslui komforto jausmą, reguliuoja transporto eismą ir efektyviai naudoja elektros išteklius;
- Išmanieji ofisai, kurie suteikia galimybę vykdyti verslą bet kurioje pasaulio vietoje, turint tokią pačią duomenų ir programinės įrangos prieigą, kaip ir pagrindinė verslo būstinė.

Vertinama, kad šiais metais pasaulio miestuose yra 1,1 mlrd. IoT įrenginių, iš kurių pusė yra išmaniuosiuose namuose ir komerciniuose pastatuose (Gartner..., 2015). Išmanieji miestai yra nauja verslo sektoriaus rinka, kuri lemia pelningą verslą. Didžioji dalis investicijų į daiktų interneto technologijas, skirtas išmaniajam miestui, ateina iš verslo sektoriaus, nes privačiame sektoriuje viešųjų pirkimų ciklas yra trumpesnis negu viešajame sektoriuje. Ekonomikos požiūriu išmaniesiems miestams pagrindinis veiksnys – investicijos į infrastruktūrą, tačiau daiktų interneto paslaugų teikėjams realų pelną duoda paslaugos ir analitika.

Apie daiktų interneto naudą verslui byloja naujos pramoninio daiktų interneto koncepcijos atsiradimas. Pramoninis daiktų internetas yra palyginti nauja koncepcija, kuri reiškia naujų skaitmeninių paslaugų ir verslo modelių vystymosi etapą, kai prie interneto prijungiami ir tarpusavyje sujungiami intelektualūs įrenginiai ir mašinos (Bi et al, 2014). Šios koncepcijos taikymas neabejotinai gali prisidėti prie ekonomikos augimo.

Kompanijos *Accenture* atliktas tyrimas, kurio metu buvo apklausta 1400 verslo vadovų iš viso pasaulio, parodė, kad potenciali IoT nauda nėra tokia akivaizdi. Taip yra todėl, kad 73 proc. apklaustųjų kompanijų vadovų neturi konkrečių jo panaudojimo planų ir tik 7 proc. sudarė IoT investicijų strategiją.

Tyrimas taip pat parodė, kad verslo kompanijų vadovai neturi konkrečių IoT diegimo planų, nes jame nemato naujų pelno šaltinių. Daugelis apklaustų verslo lyderių (57 proc.) mano, kad ši nauja technologija yra priemonė didesnėms pajamoms gauti. Didžioji apklaustų kompanijų dalis nori taikyti IoT technologiją tam, kad padidėtų verslo efektyvumas keliant darbo našumą ir mažinant operatyvias išlaidas (atitinkamai 46 proc. ir 44 proc.).

Tikrasis ekonominis efektas bus pasiektas tada, kai verslo vadovai supras gyvybišką informacijos reikšmę tokiose svarbiose srityse kaip išėjimas į naujas rinkas ir naujus pelno šaltinius. O tai reiškia radikalias požiūrio į verslą permainas, t. y. naujus darbo su konkurentais metodus, naujų verslo partnerių paieškas, organizacinės struktūros keitimą ir pan.

Accenture atliktas tyrimas išskiria tris sritis, kuriose verslo kompanijoms vertėtų įdėti daugiau pastangų:

- Peržiūrėti tarpšakinius modelius, t. y. valdymo struktūrą, partnerius ir operatyvią veiklą;
- Kapitalizuoti duomenų vertę, t. y. diegti naujus duomenų suderinamumo ir sau-

gumo standartus, kad būtų galima keistis duomenimis su kitomis kompanijomis;
- Parengti naują darbo aplinką, t. y. išplėsti kreipties į informaciją galimybes ir decentralizuoti darbo aplinką.

Daiktų interneto technologija jungia milijonus objektų, perduodama ir pateikdama informaciją, o kartu didina verslo vertę ir konkurencinį pranašumą, t. y. kuria naujas verslo galimybes.

Įvairūs daiktų interneto technologijos projektai dažnai neleidžia verslui įžvelgti galimybių, esančių rinkoje. Todėl verslui siūlomi tokie pagrindiniai daiktų interneto technologijos taikymo modeliai, kurių kiekvienas pateikia aiškias verslo galimybes vartotojams:

1. Operatyvus valdymas – stebėti objekto būseną tam, kad padidėtų jo naudojimo efektyvumas. Šis modelis leidžia optimizuoti išteklių naudojimą tam tikroje aplinkoje.
2. Apmokestinimas – paskaičiuoti ištekliaus naudojimo kainą. Tai ypatingas verslo modelis, kuris nukreiptas į fizinio ištekliaus apmokestinimą pagal tikslią jo naudojimo apskaitą. Jis leidžia už brangiai kainuojančius kapitalo aktyvus mokėti jų naudojimo kainą. Tai suteikia galimybę kapitalinius įdėjimus pakeisti einamosiomis išlaidomis, tiksliau planuoti ištekliaus gyvavimo ciklą ir palaikyti techninį ištekliaus aptarnavimą.
3. Įrenginių eksploatavimas – objekto išorinės aplinkos valdymas. Šis modelis skverbiasi į eksploatacinių technologijų sritį ir ją raiškiai keičia, t. y. naudojamos tipinės technologijos, programinė įranga, architektūra ir pan. Taigi įrenginių eksploatavimas tampa IT specialistų veiklos sritimi.
4. Galimybių plėtra – papildomos informacijos arba paslaugų pateikimas per objektą. Pavyzdžiui, fizinė tiekimo grandinė baigiasi, kai įrenginys pateikiamas užsakovui. Jei objektas prijungtas prie interneto, tai lieka egzistuoti skaitmeninė tiekimų grandinė, kurioje skaitmeniniai produktai ir paslaugos gali būti susieti su šiuo objektu.

Daiktų interneto technologija keičia ir spartina verslo procesus bei skatina atsirasti naujas verslo sritis, kurios gali prisidėti prie ekonomikos augimo. Prognozuojama, kad 2025 m. verslas daiktų interneto dėka turės apie 3,9 trilijono ekonominę naudą (Manyika et al., 2015). Išanalizavę dėl IoT gaunamų pajamų ir ekonominės naudos duomenis, pateikiamus įvairiuose šaltiniuose (Gartner ..., 2015; Manyika et al., 2015; HP..., 2014; Understanding..., 2014; Dave, 2015), 1 lentelėje pateikiame IoT naudos (milijardais dolerių) išvestinę 2015–2030 metų prognozę.

Kaip rodo 1 lentelės duomenys, daiktų internetas paveiks įvairiausias verslo sritis, tas poveikis yra stiprus ir vis didės.

Atsižvelgiant į tai galima teigti, kad daiktų interneto technologija lemia verslo permainas, nes:
- atsiranda naujos rinkos, kurias gali užpildyti nauji rinkos dalyviai;
- daiktų internetas leidžia tradicinėms verslo rinkoms teikti naujas paslaugas vartotojams, kurios jiems tampa pigesnės ir patogesnės.

Bendra daiktų interneto nauda verslui yra tokia:
- verslo įmonės pajamų didinimas, nes daiktų interneto kuriamos naujos prekės ir paslaugos didina pelną;
- darbo našumo didinimas ir išlaidų mažinimas, nes daiktų interneto technologija leidžia didinti produktyvumą ir mažinti verslo išlaidas.

Apibendrinant galima teigti, kad pagrindinis daiktų interneto technologijos prana-

1 lentelė. ***Ekonominė IoT nauda verslo sritims (milijardais dolerių)***

Verslo sritis	*2015 m.*	*2025 m.*	*2030 m.*
Pramonė	363	1200	1633
Mažmeninė prekyba ir paslaugos	124	410	523
Statyba	48	160	363
Vartotojai	51	170	440
Logistika	169	560	705
Išmanieji miestai	281	930	1295
Automobilių pramonė	64	210	475
Išmanieji namai	61	200	275
Išmanieji ofisai	21	70	110

šumas yra galimybė jį taikyti bet kuriame verslo sektoriuje ir gauti ekonominę naudą.

Daiktų interneto saugumo užtikrinimas bei rizikos apribojimas

Milijardams žmonių, besinaudojančių internetu dabar ir naudosiančių ateityje (jų skaičius nuolat didėja), daiktų internetas sudaro prielaidas vykti milžiniškiems pokyčiams, kurie gali paveikti kiekvieną verslą bei visus asmeniškai. Pagrindiniai pokyčiai naudojant daiktų internetą yra ne tai, kad įranga sąveikauja tarpusavyje, bet kad asmenys bendrauja tarpusavyje, naudodamiesi daiktų interneto įranga kaip netiesioginio bendravimo tarpininku, o tai savo ruožtu yra didelė saugumo problema, susijusi su apsimetinėjimu, tapatybės vagystėmis, įsilaužimais ir kitomis elektroninėmis grėsmėmis. Dėl to ypatingą reikšmę įgauna daiktų interneto ir juo besinaudojančių elementų saugumas, kurį būtų galima apibūdinti kaip aplinką ir instrumentiką, skirtą apsaugoti įrangai ir kompiuterių tinklams, prijungtiems prie daiktų interneto.

Daiktų internetas yra pažeidžiamas dėl to, kad jo įranga veikia bevieliu ryšiu ir didžiąją laiko dalį yra be priežiūros, o tai palengvina neteisėtą prieigą prie jos. Be to, didžioji dalis įrangos yra miniatiūrinė ir neturi aukšto lygio techninės ir programinės saugos priemonių, galinčių užtikrinti visišką vartotojų autentiškumą ir duomenų vientisumą.

Pagrindinė saugos problema yra ta, kad daiktų interneto įrangos ir kitų objektų sąveikos technologijos yra palyginti naujos, o į jų saugumą ne visada buvo atsižvelgiama projektuojant informacines sistemas ar jų dalis. Be to, naudotojai dažnai nesugeba tinkamai pakeisti numatytųjų autentifikavimo rekvizitų išmaniuosiuose įrenginiuose ir nesugeba parinkti pakankamai stiprių prieigą ribojančių elementų (Jing et al., 2014). Siekiant pagerinti saugumą, daiktų interneto įrenginiai, kurie yra prieinami per internetą, turi būti segmentuoti į atskirus tinklus, o prieiga prie tinklo ir įrenginio turi būti apribota. Tinklo segmentas turėtų būti stebimas siekiant nustatyti netinkamas prieigas bei turėtų būti imamasi veiksmų, jei yra pažeidimų ar iškyla pažeidimo problemų (Security..., 2015).

Verslas turi rengtis esminiams informacijos saugumo ir duomenų privatumo pokyčiams, nes daiktų interneto panaudojimas vis plinta ir per ateinančius kelerius metus apims daugelį verslo ir gyvenimo sričių. Daiktų interneto elementų įvairovė ir daugybė būdų, kuriais jie sujungiami vienas su kitu, bei panaudojimas per verslo kompiuterių tinklus kelia vis naujus informacinių technologijų valdymo ir elektroninio saugumo rūpesčius (Tysiac, 2015). Dėl to

turės būti atlikti esminiai pokyčiai, susiję tiek su informacinėmis technologijomis, tiek su daiktų interneto saugumo valdymu.

Kadangi daiktų internetą sudaro daugybė įrangos, kompiuterių įsilaužėliai gali ne tik įgyti prieigos teises, kad pavogtų duomenis ar pinigus, sugadinti duomenis ir programas, bet ir įvykdyti kitus nusikaltimus, susijusius su įrangos sąveikos sutrikdymu ypatingos svarbos struktūrose, tokiuose kaip elektros ir ryšių tiekimo, aviacijos sistemų ir kt. Verslas, naudodamas informacines technologijas, siekia padidinti pajamas, pagerinti veiklos efektyvumą ir rasti naujų būdų plėtoti verslą. Tačiau tai taip pat kelia ir naujų grėsmių. Kiekvienas daiktų interneto elementas – jutiklis ir prietaisas – galimas saugumo pavojaus šaltinis. Apie 70 procentų dažniausiai naudojamų daiktų interneto įrenginių turi rimtų saugumo spragų (Reynolds, 2015). Net labiausiai saugumu besirūpinančios organizacijos gali būti nepasirengusios visiškam saugumui daiktų interneto aplinkoje, nes dešimtys milijardų prietaisų ir daiktų yra prijungti prie interneto.

Daiktų interneto infrastruktūros negalima apibrėžti kokiais nors nusakomais objektais, nes ją sudaro įrangos įvairovė bei nevienalyčiai skirtingų lygių tinklai. Dėl didėjančių šių tinklų apkrovų bei augančio duomenų poreikio dauguma daiktų internetą aptarnaujančios techninės įrangos turės būti pertvarkyta apkrovoms atlaikyti ir saugumui užtikrinti, nes didžiulis įrangos kiekis bus naudojamas milžiniškam sąveikos kiekiui aptarnauti, kas sukels rimtų problemų sprendžiant duomenų privatumo, apsaugos, valdymo ir pasitikėjimo klausimus. Numatoma, kad daiktų internetas privalės turėti jutimo, analizavimo ir vaizdinimo priemones, kurios bus prieinamos visiems bet kuriuo metu ir bet kurioje pasaulio vietoje asmeniniu, komerciniu ar nacionaliniu lygiu (Sorbeo, 2015). Kartu su daiktų internetu vystysis ir informacinės technologijos. Antai debesų kompiuterija, didieji duomenys ir jų technologijos yra vieni iš esminių daiktų technologijos raidos pagrindų, todėl kartu su daiktų internetui kartu turės vystytis ir minėtos, ir kitos informacinės technologijos. Daiktų internetas skatina įmones gaminti išmaniuosius įrenginius, jutiklius ir kitą jį aptarnaujančią įrangą, taip pat kurti programinę įrangą, šia kryptimi tobulinti rinkodarą bei didinti konkurenciją. Tačiau didėjantis naudojamos išmaniosios įrangos bei ją aptarnaujančios programinės įrangos kiekis bei įvairovė mažina sistemos saugumą, didina jos riziką.

Rizikos kilmės, rizikos veiksnių ir jų poveikio verslui negalima traktuoti tuo pačiu pagrindu. Kai rizikos kilmė ir jos veiksniai yra realūs ir jie įvyksta, tai būtina įvertinti verslo pažeidimo laipsnį ir pasekmes. Jeigu pažeidimo laipsnis yra mažas, tai ir pasekmė verslui bus menka. Visa tai priklauso nuo verslo saugos lygio. Rizikos grėsmės ir jos pasekmių sąveikos grandinę būtų galima pateikti taip: Rizikos kilmė → Rizikos grėsmė → Rizikos poveikis → Pažeidimas → Pažeidimo pasekmės.

Daugelis daiktų interneto galimybių pasireiškia per technologijų integraciją ir sąveiką, kuri tik didės ir taps vis sudėtingesnė ir kompleksiškesnė, todėl didėjant kompleksiškumui sistemos rizika auga. Daiktų interneto plitimas reiškia, kad ribos tarp verslo įmonių nyksta, o dėl to rizika tampa sunkiai valdoma. Elektroniniai įsilaužėliai kuria vis naujus metodus, leidžiančius pralaužti verslo įmonių saugumo sistemas ir prieiti prie įmonių ir jų darbuotojų privačios informacijos, sutrikdyti įmonių kompiuterines sistemas, pavogti informaciją. Kiekvieną dieną jų atakos tampa vis sudėtingesnės

ir vis sunkiau nuo jų apsisaugoti (Maynard, 2015). Kadangi daiktų internetas gerokai išplečia įrangos ir duomenų prieigą per visuomeninius tinklus, jų pažeidžiamumo galimybė taip pat didėja.

Daiktų interneto rizikos apribojimo veiksniai

Siekiant užtikrinti verslo įmonių kompiuterinę apsaugą labai svarbu, kad verslo įmonės saugos klausimais galėtų bendrauti su savo verslo partneriais. Įtaką kompiuteriniam saugumui turi ir teisinė sistema, ir fizinė aplinka, ir verslo aplinka. Galėtume apibrėžti, kad daiktų interneto rizikos aplinką sudaro: verslo infrastruktūra, teisinė sistema, duomenų ir programų visuma, fizinė aplinka, vadyba, darbuotojai, trečiosios šalys (pardavėjai, tiekėjai, vartotojai). Tik bendras požiūris į saugumo svarbą gali apriboti riziką, kylančią naudojantis daiktų internetu.

Dažniausiai daiktų internetas pažeidžiamas per interneto sąsajas autentifikavimo ir autorizavimo režimu, perduodant duomenis, kai jų šifravimas ir sistemos saugumo konfigūravimas yra nepakankamas, kai nepakankama įrenginių fizinė ir programinė apsauga. Verslo įmonės turi stengtis peržiūrėti saugumo spragas, jas ištaisyti atsižvelgdamos į silpniausias saugos grandinės vietas. Kadangi daiktų interneto technologija remiasi bevieliu ryšiu, silpnai fiziškai apsaugotais davikliais ir kita įranga, labai dideliu elementų ir vartotojų kiekiu, saugumo spragos yra linkusios didėti. Todėl verslo įmonių kompiuterių tinklai turi būti per saugos šliuzus atskirti nuo daiktų interneto taip, kad nebūtų pažeidžiami nuosavi verslo tinklai, kai pažeidžiami kiti tinklai ar jų įranga. Siekiant minimizuoti saugos spragas būtina, kad daiktų interneto programinės įrangos kūrėjai įdiegtų į jas apsaugos priemones ir jas tobulintų kartu su daiktų interneto plėtra. Daiktų interneto saugumas turi būti nediskutuojama ir privaloma kategorija visoms verslo ir technologijų grandims, nepriklausomai – įmonė to nori ar ne, nes saugumo spraga vienoje daiktų interneto grandyje gali pažeisti kitas grandis ir net kitų verslo įmonių tinklus.

Daiktų interneto rizika susijusi su grėsmėmis pažeisti verslą, o priklausomai nuo pažeidimo lygio galimi arba amortizuojami nuostoliai, arba net tie, kurie lemia bankrotą. Verslo pažeidžiamumo tikimybinio lygio priklausomybei nuo rizikos grėsmės nustatyti galime suformuoti ryšio matricą, vadovaudamiesi šio straipsnio autoriaus sukurtu metodu (Žilinskas, Skyrius, 2009).

Vadovaudamasis šia priklausomybės matrica (2 lentelė), verslas gali nustatyti saugos priemones ir jų lygį. Jeigu priklausomybės lygis neviršija 0,3, reali pažeidimo grėsmė minimali; kai lygis nuo 0,4 iki 0,6 (dešiniau ir aukščiau punktyrinės linijos), pakankamai amortizuojamos pažeidimo pasekmės; kai lygis yra didesnis nei 0,7 (dešiniau ir aukščiau dvigubos linijos), pažeidimo pasekmės gali būti labai rimtos.

2 lentelė. ***Verslo pažeidžiamumo lygio priklausomybės nuo rizikos grėsmės matrica***

	Verslo pažeidžiamumo lygis		
	Žemas	*Vidutinis*	*Didelis*
Didelė rizikos grėsmė	0,3	0,6	1
Vidutinė rizikos grėsmė	0,1	0,4	0,7
Maža rizikos grėsmė	0	0	0,05

Kai lygio reikšmė yra 0–0,3, diegiamos standartinės informacinių sistemų saugos priemonės, užtikrinančios autentifikaciją ir autorizaciją; kai lygio reikšmė 0,4–0,6, papildomai diegiamos specialiosios saugos priemonės, ypač duomenų vientisumo ir integralumo kontrolės srityje; kai lygio reikšmė 0,7–1, papildomai diegiamos fizinės ir programinės įrangos apsaugos priemonės. Tokia matrica turėtų būti sudaroma periodiškai, ne rečiau kaip kartą per mėnesį, ir matricų grandinės pagrindu sudaroma vidurinių reikšmių tendencijų matrica. Jeigu tendencijų matricoje punktyrinės ir ypač dvigubos linijos pasistumia į kairę, rizikos grėsmė didėja ir būtina taikyti aukštesnio lygio saugos priemones. Jeigu tendencijos matricoje punktyrinės ar dvigubos linijos pasistumia į dešinę arba nekinta, įdiegtos saugos priemonės laikytinos pakankamomis.

Siekdama apriboti daiktų interneto riziką, verslo įmonė turėtų nustatyti, kad įmonės apsauga nuo kompiuterinių įsilaužimų vykdoma trimis lygiais: aktyviuoju, adaptaciniu, išankstiniu (Cybersecurity..., 2015). Aktyvusis lygis yra tas, kuriame taikomos turimos apsaugos priemonės. Adaptacinis lygis – apsauga, kai taikomos naujos ar keičiamos esamos apsaugos priemonės į naujesnes, atsižvelgiant į besikeičiančią projektuojamą ar modifikuojamą aplinką. Išankstinis yra tas lygis, kai yra taikomos apsaugos priemonės, kurios kuriamos žvelgiant į ateitį (kompiuterinės grėsmės intelektą, potencialius įsilaužėlius ir jų priemones) ir taikomos iš anksto, kol įsilaužimai dar nėra įvykę ar gali įvykti. Kiekviename lygyje rizikai apriboti kaip pagrindinės priemonės turėtų būti taikomos šios: autentifikavimo ir autorizavimo kontrolė, duomenų ir ryšio kodavimas, duomenų vientisumo ir integralumo kontrolė, virtualios ugniasienės, fizinė įrangos apsauga, tinklų segmentacija, tinklų prieigos kontrolė, apsauga nuo pažangių kenkimo programų, sistemos stebėsena, programų sąveikos ir sąsajų kontrolė, debesų kompiuterijos grėsmių analizė, saugumo lygio testavimas ir įvertinimas, apsaugos priemonių vystymas. Be pagrindinių, taikomos ir specifinės riziką ribojančios techninės bei programinės priemonės.

Kartu naudojamos visos priemonės – saugumo problemų supratimas, išankstinis grėsmių numatymas ir priemonių rizikai apriboti taikymas – gali užtikrinti palyginti saugų daiktų interneto sistemos funkcionavimą ir apriboti galimą jos riziką.

Išvados

Permaininga išorinė aplinka verčia verslo organizacijas aktyviai ir sparčiai reaguoti į rinkos pokyčius bei verslo procesų tobulinimui ir plėtrai taikyti šiuolaikines informacijos technologijas, įskaitant ir daiktų interneto technologiją. Atsiradusi šio amžiaus pradžioje daiktų interneto technologija leidžia verslo organizacijai sukurti savo technologijos naujoves (*know how*) ir jas plėtoti.

Pasaulinių IT ir konsultacinių kompanijų tyrimai rodo, kad daiktų interneto technologijos taikymo verslo organizacijose mastai per pastaruosius metus nepaliaujamai didėja ir ateityje tik didės, todėl verslo organizacijoms būtina imtis šiuolaikinių IT sprendimų. Dauguma verslo organizacijų pripažįsta, kad daiktų interneto technologijos sprendimai gali vienaip ar kitaip padėti efektyviau organizuoti veiklą.

Daiktų interneto technologijos savybių analizė leidžia daryti išvadą, kad ji keičia ir spartina visus verslo procesus visose verslo srityse. Daiktų internetas reikalauja naujo požiūrio į verslo partnerius, nes jo aprėptis yra neribota, todėl reikalingi patikimi part-

neriai, kurie konsultuotų organizaciją šios technologijos palaikymo klausimais.

Daiktų interneto technologija didina verslo objektų pajamingumą ir pelningumą, skatina rastis naujas verslo sritis, kurių pagrindu kuriasi naujos verslo rinkos ir nauji rinkos dalyviai. Didėjant verslo rinkai pinga verslo paslaugos. Taigi daiktų interneto technologija skatina naujus verslo produktus ir paslaugas, o tai didina ekonominį efektyvumą.

Daiktų internetas plečia verslo aplinką, ji tampa atviresnė, tačiau kartu didėja jos pažeidžiamumas. Daiktų interneto naudojimas ir plitimas neišvengiamai didina informacinių sistemų, o kartu ir verslo rizikingumą.

Naudojant daiktų internetą ne tik įranga sąveikauja tarpusavyje, bet ir asmenys bendrauja tarpusavyje šio interneto priemonėmis. O tai yra didelė saugumo problema, nes akivaizdžiai padidėja grėsmės, susijusios su apsimetinėjimu, tapatybės vagystėmis, įsilaužimais ir kitais saugumo pažeidimais. Todėl ypač svarbu užtikrinti daiktų interneto ir juo besinaudojančių elementų ir asmenų saugumą, kurį būtų galima apibūdinti kaip aplinką ir instrumentus, skirtus apsaugoti įrangai ir kompiuterių tinklams, prijungtiems prie daiktų interneto.

Siekiant pagerinti verslo saugumą, daiktų interneto įrenginiai turi būti atskiriami į atskirus tinklų segmentus, griežtai apribojant prieigą prie jų. Tinklo segmentas turėtų būti stebimas siekiant nustatyti netinkamas prieigas bei imamasi veiksmų, jei yra pažeidimų ar iškyla pažeidimo problemų. Verslo įmonių kompiuterių tinklai turi būti per saugos šliuzus atskirti nuo daiktų interneto taip, kad nebūtų pažeidžiami nuosavi verslo tinklai, pažeidus kitus tinklus ar jų įrangą. Kuriant ir tobulinant daiktų interneto programinę įrangą būtina įdiegti apsaugos priemones ir jas tobulinti kartu su daiktų internetu. Daiktų interneto saugumas turi būti nediskutuojama ir privaloma kategorija visoms verslo ir technologinėms grandims.

Siekdama apriboti daiktų interneto riziką, verslo įmonė turėtų nenutrūkstamai vykdyti autentifikavimo ir autorizavimo kontrolę, duomenų ir ryšio kodavimą, duomenų vientisumo ir integralumo kontrolę, naudoti virtualias ugniasienes, vykdyti fizinę įrangos apsaugą, tinklų segmentaciją, tinklų prieigos kontrolę, apsaugą nuo pažangių kenkimo programų, sistemos stebėseną, programų sąveikos ir sąsajų kontrolę, debesų kompiuterijos grėsmių analizę, saugumo lygio testavimą ir įvertinimą, apsaugos priemonių tobulinimą.

Daiktų interneto keliamos rizikos supratimas ir priemonių, užtikrinančių informacinių sistemų saugumą, taikymas gali maksimaliai apriboti riziką, kylančią verslo įmonėms, naudojančioms daiktų internetą. Saugumo problemų supratimas, išankstinis grėsmių numatymas ir rizikos apribojimo priemonių taikymas gali užtikrinti pakankamai saugų daiktų interneto sistemos funkcionavimą ir sumažinti galimą jos riziką.

LITERATŪRA

ATZORI, L.; IERA, A.; MORABITO, G. (2010). The Internet of Things: A survey. *Computer Networks*, vol. 54, iss. 15.

BANDYOPADHYAY, D.; SEN, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*: An International Journal, vol. 58, iss. 1.

BI, Z.; XU, L.; WANG, C. (2014). Internet of Things for enterprise systems of modern manufacturing. *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2.

CHASE, J. (2014). *The Evolution of the internet of things*. Texas Instrumets.

CHUI, M.; LÖFFLER, M.; ROBERTS, R. (2010). The Internet of Things. *McKinsey Quartely*, March.

CYBERSECURITY (2015). Cybersecurity and the internet of things. *Insights on governance, risk and compliance*. March.

DAVE, E. (2012). The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. *Cisco*, White papers.

FEKI, M.; KAWSAR, F.; BOUSSARD, M.; TRAPPENIERS, L. (2013). The Internet of Things: The Next Technological Revolution. *Computer*, vol. 46, iss. 2.

FRIES, P.; VERMESAN, O. (2014). *Internet of Things – From Research and Innovation to Market Deployment.* River Publicher, Denmark.

GARTNER IDENTIFIES (2014). Gartner Identifies Four Fundamental Usage Models to Unlock Value from the Internet of things [interaktyvus]. [žiūrėta 2015 m. spalio 28 d.]. Prieiga per internetą: <http://www.gartner.com/newsroom/id/2699017>.

GARTNER SAYS (2015). Gartner Says 6.4 Billion Connected "Things" will be in use in 2016, up 30 Percent from 2015 [interaktyvus]. [žiūrėta 2015 m. lapkričio 4 d.]. Prieiga per internetą: <http://www.gartner.com/newsroom/id/3165317>.

HP 2014 REPORT (2014). Internet of Things Research Study [interaktyvus]. [žiūrėta 2015 m. spalio 1 d.]. Prieiga per internetą: <http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en>.

INTERNET OF THINGS: RISK AND VALUE CONSIDERATIONS (2015). *ISACA White paper* [interaktyvus]. [žiūrėta 2015 m. rugsėjo 22 d.]. Prieiga per internetą: <http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/internet-of-things-risk-and-value-considerations.aspx>.

ITU RECOMMENDATION (2012) [interaktyvus]. [žiūrėta 2015 m. rugsėjo 19 d.]. Prieiga per internetą: <http://www.itu.int/pub/R-REC>.

JANKOWSKI, S.; COVELLO, J. ; BELLINI, H. (2014).Making sense of the next mega-trend. *Internet of Things*, vol. 1.

JING, O.; VASILAKOS, A.; WAN, J.; LU J.; DECHAO Q. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, vol. 20.

KPMG GLOBAL TECHNOLOGY INNOVATION SURVEY (2014) [interaktyvus]. [žiūrėta 2015 m. rugsėjo 17 d.]. Prieiga per internetą: <https://techinnovation.kpmg.chaordix.com/survey/2014>.

LI, S. (2015).The internet of things: a survey. *Information Systems Frontiers*, vol. 17, iss. 2.

MAYNARD, J. (2015). Vulnerability of Login Credentials at the Heart of Cyberhacks and Data Breaches. *ISACA Journal*, vol. 5.

MANYIKA, J.; CHUI, M.; BISSON, P.; WOETZEL, J.; DOBBS, R.; BUGHIN, J.; AHARON D. (2015). The internet of things: mapping the value beyond the hype. *McKinsey Quarterly,* June.

MEDAGLIA, C.; SERBANATI, A. (2010). An Overview of Privacy and Security Issues in the Internet of Things. *20th Tyrrhenian Workshop on Digital Communications*, January 4.

MIORADI, D. (2013). Internet of things. *Ad Hoc Networks*, vol. 10, iss. 7.

NING, H.; HONG, L.; LAURENCE Y. (2013). Cyberentity Security in the Internet of Things. *Computer*, vol. 46, iss. 4.

REYNOLDS, D. (2015). Internet of Things: A huge realm of opportunity and risk. *Privacy and Data Security Insight*, August 31.

SAMINATH, V.; JUNG, S. (2015). Understanding of Internet of Things (IoT) and Experimental Approach using WICED Sense in Android Platform. *International Journal of Scientific and Research Publications*, vol. 5, iss. 7.

SECURITY (2015). *Security in the internet of things*. *Wind River Systems*, January 1.

SORBEO, G. (2015). Managing the Unmanageable: A Risk Model for the Internet of Things. *RSA Conference*, April 20–24.

TYSIAC, K. (2015). How to manage risks connected with the internet of things. *CGMA Magazine*, January 28.

WEBER, R. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, vol. 26, iss. 1.

WHYTOCK, P. (2014). Maintaining Security for the Internet of Things. *Microwaves & RF*, vol. 53, iss. 1.

ŽILINSKAS, R.; SKYRIUS R. (2009). Management decision support by using early warning environments. *Ekonomika*, t. 86.

THE BENEFITS AND RISKS OF APPLYING THE INTERNET OF THINGS TECHNOLOGY IN BUSINESS

Laima Zalieckaitė, Raimundas Žilinskas

S u m m a r y

The technology of the Internet of Things is one of the newest and rapidly developing information and communication technology policies in the beginning of this century, however, its adaptation in business began to spread only in the second decade. The Internet of Things is not only the technology whose services are designed for businesses, but also a new business model.

As evidenced by the global experience in implementing these technologies and the latest research, the scope of the Internet of Things services and applications in business over the past year is rising relentlessly and in the future will only increase. The majority of business firms recognize that the Internet of Things technology can somehow help organize activities to accelerate the technological and communicative processes of business, to increase its operational efficiency.

While it is recognised that the use of the Internet of Things in the business environment expands, it becomes more open, but also more vulnerable. Using the Internet of Things, things interact with each other and also people interact with each other, using items on the Internet of Things as a mediator for indirect communication, and this, in turn, is a major security problem concern with hackers, fakes and other electronic threats. Therefore, the use and spread of the Internet of Things will inevitably increase the risk of information systems and at the same time the risk profile of the business.

This article analyses the benefits of the Internet of Things applied in business, its risks and the measures to mitigate the risks.

Įteikta 2015 m. spalio 26 d.