ISSN 2029–1701 (print)
ISSN 2335–2035 (online)

Mokslinių straipsnių rinkinys
VISUOMENĖS SAUGUMAS IR VIEŠOJI TVARKA
PUBLIC SECURITY AND PUBLIC ORDER
2012 (7) Scientific articles

ELEKTRONINĖS ERDVĖS SAUGUMO EKONOMINIAI ASPEKTAI

Darius Amilevičius*

Mykolo Romerio universiteto Viešojo saugumo fakulteto Humanitarinių mokslų katedra
Putvinskio g. 70, LT-44211 Kaunas
Telefonas 30310
El.paštas: d.amilevicius@mruni.eu

Santrauka. Elektroninės erdvės saugumo ekonomika - nauja ekonomikos mokslo sritis, apimanti už ją anksčiau atsiradusias saugumo ekonomiką ir informacijos ekonomiką. Užsienio mokslininkai jau kuris laikas pabrėžia, kad kibernetinio saugumo neįmanoma pasiekti vien technologinėmis priemonėmis. Tai tarpdisciplininių studijų, kur ekonomika užima svarbią vietą, objektas. Daug šios srities problemų galima žymiai geriau paaiškinti ekonomikos kalba (viešosios gėrybės, informacijos asimetrija ir t.t.), o ekonominė logika sudaro prielaidas ribotus išteklius naudoti išmintingai, apsaugant individus, įmones ir organizacijas nuo kibernetinių atakų, bei pasirinkti optimalų investicijų į kibernetinį saugumą dydį. 2011 m. patvirtintoje pirmoje Nacionalinėje elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metams programoje stinga dėmesio ekonominio pagrįstumo, mokslinio pagrįstumo ir teisėtumo principų sinerginei sąveikai, todėl investicijų į kibernetinį saugumą dydžio klausimas lieka atviras politinėms manipuliacijoms. Straipsnyje šios problemos svarstomos iš elektroninės erdvės saugumo ekonomikos taško, ieškant ekonominio pagrindo investicijų dydžio ir investavimo krypčių sprendimams.

Pagrindinės sąvokos: elektroninė erdvė, elektroninės erdvės saugumas, elektroninės erdvės saugumo ekonomika, elektroniniai nusikaltimai, viešoji gėrybė, privati gėrybė.

ĮVADAS

Prasidėjus interneto erai prie keturių žmogaus veiklos erdvių (žemė, oras, jūra, kosmosas) prisidėjo penkta - elektroninė erdvė. 2011 metais McKinsey&Company paskelbė studiją, kurioje išanalizuotas interneto poveikis pasaulio ekonomikai. Remiantis gausiai statistiniais duomenimis daroma išvada, kad internetas vidutiniškai 3-4 procentais padidina išsivysčiusių šalių bendrąjį vidaus produktą[1]. Tačiau „Norton Cybercrime Report 2011“ atskleidžia ir kitą medalio pusę. Šio tyrimo rezultatai rodo, kad dėl kibernetinio nusikalstamumo pasaulyje kasmet prarandama apie 388 mlrd. JAV dolerių. Kibernetinis saugumas tapo ypač svarbi ir dėmesio reikalaujanti sritis – elektroninė erdvė tampa vis labiau pažeidžiama. Akivaizdu, kad kibernetinėje erdvėje išpuolių niekada nepavyks išvengti. Jie vykdomi kasdien, su tuo susiduria visi, turintys interneto ryšį. Tradiciniai kriminaliniai nusikaltimai, nors baugina visus, bet turi žymiai mažiau tiesioginių aukų, palyginus su elektroniniais nusikaltimais, kurie jau kelia grėsmę ne tik viešajam saugumui kibernetinėje erdvėje, bet ir šalies ekonomikai.

[1] McKinsey&Company, Internet matters: The Net's sweeping impact on growth, jobs, and prosperity [interaktyvus]. 2011. [žiūrėta 2012.04.10]. <http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters>.

ISSN 2029–1701 (print)
ISSN 2335–2035 (online)

Mokslinių straipsnių rinkinys
VISUOMENĖS SAUGUMAS IR VIEŠOJI TVARKA
PUBLIC SECURITY AND PUBLIC ORDER
2012 (7) Scientific articles

Temos aktualumas. Remiantis Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT-LT duomenimis, 2011 metais pranešimų apie elektroninės erdvės pažeidimus skaičius išaugo daugiau kaip dvigubai. 18 kartų šoktelėjo informacinių sistemų užvaldymo incidentų atvejai - jų 2011 m. nuo 477 pagausėjo iki 8057. Dauguma šių išpuolių buvo atlikti automatizuotomis priemonėmis, pasitelkiant ir „botnet“ - virusų sukuriamus ir iš išorės valdomus tinklus, kai vartotojas net nenutuokia, kad per jo kompiuterį gali būti vykdomos kibernetinės atakos. Institucija kasdien tokių kompiuterių Lietuvoje užfiksuoja apie 8000[2]. 2011 m. birželio mėn. Vyriausybė patvirtino pirmą Nacionalinę elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metams programą[3], kurioje nurodytos pagrindinės strateginės kryptys ir gairės kibernetinio saugumo srityje. Programos tikslas - sudaryti prielaidas kibernetinio saugumo plėtojimui Lietuvoje 2011-2019 metais, bet programos vykdymui lėšų neskirta. Šis teisės aktas labai svarbus, nes iki tol Lietuvoje nebuvo dokumentų, kuriais būtų apibrėžtos elektroninės informacijos saugos gairės. Tačiau jame stokojama vientisumo, nestinga trūkumų, tekstas organizuojamas apie dvi pagrindines tematines ašis - technologiniai sprendimai ir teisinės bazės kūrimas/stiprinimas. 2011 m. gruodį Nacionalinio saugumo ir gynybos komiteto posėdyje, kuriame buvo aptartas programos vykdymas, atsakingų institucijų vadovai akcentavo specialistų ir finansavimo stygių[4]. Po 2012 m. sausį įvykusių DDoS atakų prieš Lietuvos Banko interneto sistemas premjeras Andrius Kubilius prabilo apie investicijų didinimą elektroninės erdvės skydui stiprinti. Tai eilinį kartą patvirtina, kad kibernetinės erdvės saugumas Lietuvoje tapo įkaitu politinių deklaracijų, neegzistuojančio finansavimo ir augančių grėsmių. Nors užsienio mokslininkai jau kuris laikas įrodinėja, kad kibernetinės erdvės saugumas neišsprendžiamas vien technologinėmis arba teisinėmis priemonėmis, o daugelį šios srities problemų galima žymiai geriau paaiškinti ekonomikos kalba (viešosios gėrybės, informacijos asimetrija ir t.t.), bet Nacionalinėje elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metams programoje stinga dėmesio ekonominio pagrįstumo ir mokslinio pagrįstumo principams. Todėl ir klausimas apie papildomas investicijas yra retorinis, nes vien technologiniai arba teisiniai svarstymai neduos atsakymo į

[2] CERT-LT: metinė ir ketvirtinė incidentų statistika [interaktyvus]. Vilnius, 2011 [žiūrėta 2011.09.30]. <https://www.cert.lt/statistika.html>.
[3] Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programa. Valstybės Žinios, 2011-07-09, nr. 83-4033 (Valstybės Žinios, 2011-08-27, nr. 106 Atitaisymas (programos priedo 47 punkto))
[4] 2011 m. gruodžio 21 d. pranešimas VIR. [interaktyvus]. [žiūrėta 2012.04.10] <http://www3.lrs.lt/pls/inter/w5_show?p_r=4463&p_d=119407&p_k=1>.

savo prigimtimi ekonominius klausimus: kas turi investuoti? kiek investuoti? kokia laukiama investicijų grąža?

Tyrimo tikslas – ištirti elektroninės erdvės saugumo stiprinimo ekonominius aspektus ir ekonominio patikimumo principo sąryšį su mokslinio patikimumo ir teisėtumo principais.

Uždaviniai:

- ištirti ar elektroninės erdvės saugumas yra viešoji gėrybė;
- ištirti elektroninės erdvės saugumo kaip privačios gėrybės trūkumus;
- atskleisti ekonominio pagrįstumo, mokslinio pagrįstumo ir teisėtumo principų bei jų sąveikos svarbą, siekiant elektroninės erdvės saugumo optimalių ekonominių kaštų ir investicijų dydžio.

Tyrimo objektu pasirinktas elektroninės erdvės saugumas kaip privati ir viešoji gerybė, jos optimalių gamybos kaštų ir investicijų dydžio nustatymo principai.

Tyrimo metodai. Siekiant užsibrėžto tikslo buvo taikyti empiriniai tyrimo metodai. Dokumentų analizės metodas ir jo atskiras porūšis - teisinių dokumentų analizė. Mokslinės literatūros analizės metodas leido atskleisti, įvertinti ir panaudoti tyrime kituose mokslinės literatūros šaltiniuose sukauptas naujausias mokslo žinias ir teoriškai pagrįsti atskirus teiginius. Kontentinės analizės metodas taikytinas analizuojant straipsnius elektroninėje žiniasklaidoje. Tyrimuose buvo naudotas antrinės duomenų analizės metodas, kuriuo, atsižvelgiant į kitą turimą informaciją, buvo analizuojami ir vertinami įvairių institucijų surinkti duomenys. Atskiriems klausimams tirti buvo taikyti ir teoriniai tyrimo metodai (analitinis - kritinis, alternatyvų, analogijos, apibendrinimo, dedukcijos, indukcijos).

ELEKTRONINĖS ERDVĖS SAUGUMAS - VIEŠOJI GĖRYBĖ

Nacionalinis saugumas, kaip ir viešasis saugumas, yra nekonkurencinė viešoji gėrybė, kurią vartoja visi šalies piliečiai. Iš kitos pusės, piliečiui (vartotojui) neįmanoma uždrausti naudotis nacionaliniu saugumu, net jei jis nemoka mokesčių. Tarptautiniame kontekste globalus saugumas irgi yra viešoji gėrybė. Anksčiau klasikiniais pagrindiniais globalaus saugumo pavyzdžiais buvo pateikiami branduolinio karo grėsmė, klimato užterštumas, šiltnamio efektas, tarptautinis terorizmas. Nuo 2000 m., o ypač po 2001 m. rugsėjo 11 d. įvykusių teroristų atakų, sparčiai besivystančių ekonomikos šakų - elektroninės erdvės saugumo ekonomikos, saugumo ekonomikos ir informacijos ekonomikos - atstovai ieško atsakymų į keturis esminius klausimus. Pirmasis - ar elektroninės erdvės saugumas gali būti laikomas viešąja gėrybe? Jei taip, tai kokiu mastu valstybė turi gaminti šią gėrybę? Koks

optimalus šios viešosios gėrybės santykis su privačia? Kaip spręsti kibernetinės erdvės saugumo, kaip privačios gėrybės, eksternalitetų (išorinių efektų) problemą?

Viešosios gėrybės - tai tokios prekės ir paslaugos, kuriomis vienu metu gali naudotis daug asmenų ir dėl to jos naudingumas kiekvienam iš jų nesumažėja. Klasikiniai pavyzdžiai - jūros švyturys. Privatus sektorius niekada neinvestuos į švyturio statybą, nes švyturys naudingas daugeliui, bet jo statyba brangiai kainuoja ir neįmanoma uždrausti juo naudotis arba imti mokestį už jo teikiamą naudą[5]. Rinka yra veiksminga, jei ekonominė gėrybė - prekė ar paslauga - teikia naudą tik ją įsigijusiam vartotojui. Viešųjų gėrybių gamybą efektyviai gali organizuoti tik valstybė, nes jų išorinis naudingumas yra labai didelis lyginant su vidiniu, o vidinis naudingumas labai mažas lyginant su jos gamybos kaštais. Naudojimosi viešosiomis gėrybėmis negalima apriboti, todėl jos visada vartojamos kolektyviai. Ekonomikos teorija, analizuodama rinkos trūkumus ir jos keliamas problemas, bei siekdama išsiaiškinti priemones šiems trūkumams panaikinti ar bent sumažinti, pagrindiniais rinkos mechanizmo ribotumą lemiančiais veiksniais nurodo viešųjų gėrybių neefektyvią gamybą bei paskirstymą, informacijos asimetriją, eksternalitetus (šalutinius efektus), neveiksmingą socialinių problemų sprendimą, rinkos polinkį į monopolizavimą[6].

Prasidėjus interneto erai prie keturių žmogaus veiklos erdvių (žemė, oras, jūra, kosmosas) prisidėjo penkta - elektroninė erdvė. Elektroninės ekonomikos plėtra teigiamai paveikė šalių ir pasaulinę ekonomiką. 2011 metais McKinsey&Company paskelbė studiją, kurioje išanalizuotas interneto poveikis pasaulio ekonomikai. Remiantis gausiai statistiniais duomenimis daroma išvada, kad internetas vidutiniškai 3-4 procentais padidina išsivysčiusių šalių bendrąjį vidaus produktą[7]. Remiantis 2011 m. Lietuvos Statistikos departamento duomenimis, Lietuvoje tai sudarytų 4240,25 mln. Lt[8]. Tai sudarytų vidutiniškai daugiau nei žemės ūkio, miškininkystės ir žuvininkystės sektorius (A), informacijos ir ryšių sektorius (J), arba finansinė ir draudimo veikla (K)[9]. Plečiantis elektroninei ekonomikai neatsilieka ir kibernetinis nusikalstamumas. Andrew P. Morriss mano, kad šiuo metu elektroninė erdvė prilygintina „laukiniams Vakarams“, kur žmogui atsiveria neribotos galimybės, bet kur

[5] Davulis, G., *Ekonomikos teorija*. Vilnius, 2009: 214.
[6] Ten pat, 211-226.
[7] McKinsey&Company, Internet matters: The Net's sweeping impact on growth, jobs, and prosperity [interaktyvus]. 2011. [žiūrėta 2012.04.10]. <http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters>
[8] Lietuvos Statistikos Departamentas: BVP 2011 kainomis buvo 106 006,347 mln. litų [žiūrėta 2012.04.10]. <http://db1.stat.gov.lt/statbank/SelectVarVal/saveselections.asp>.
[9] Lietuvos Statistikos Departamentas: Lietuvos bendrosios pridėtinės vertės struktūra [žiūrėta 2012.04.10]. <http://db1.stat.gov.lt/statbank/selectvarval/saveselections.asp?MainTable=M2010253&PLanguage=0&TableStyle=&Buttons=&PXSId=18531&IQY=&TC=&ST=ST&rvar0=&rvar1=&rvar2=&rvar3=&rvar4=&rvar5=&rvar6=&rvar7=&rvar8=&rvar9=&rvar10=&rvar11=&rvar12=&rvar13=&rvar14=>.

nevaržomai plinta smurtas ir prievarta, o niekadėjai nesulaukia pelnytos bausmės[10]. Anne S.Y. Cheung teigia, kad nors internetas daugeliui žmonių sudarė iki tol neturėtas prieinamumo, betarpiškumo, anonimiškumo galimybes, bet kartu tapo iššūkiu žmogaus teisėms, asmens ir visuomenės saugumui[11]. Elektroninių nusikaltimų ypač sparčiai pradėjo gausėti nuo pasaulinės finansų krizės pradžios, kai nemažai IT profesionalų neteko darbo. 2011 m. atliktų tyrimų rezultatai rodo, kad dėl kibernetinio nusikalstamumo pasaulyje kasmet prarandama apie 388 mlrd. JAV dolerių[12]. Tradiciniai kriminaliniai nusikaltimai, nors baugina visus, bet turi žymiai mažiau tiesioginių aukų, palyginus su elektroniniais nusikaltimais. Elektroniniai nusikaltimai virtualiai daro poveikį beveik visiems šalies gyventojams ir beveik visoms įmonėms ir organizacijoms. Ekonominiai ir kiti kibernetiniai nusikaltimai jau kuris laikas kelia rimtą grėsmę tiek viešajam saugumui, tiek nacionaliniams saugumui, tiek globaliam saugumui elektroninėje erdvėje. Šioje situacijoje jau nepakanka, kad valstybė dalyvautų kibernetinės erdvės saugumo užtikrinime vien kurdama ir/ar tobulindama teisinę bazę. Neišvengiamas jos dalyvavimas ir ekonomine prasme - kuriant viešąsias gėrybes, kurios ne rinkos sąlygomis kuriamos efektyviau nei rinkos.

Bruce H. Kobayashi, tirdamas elektroninės erdvės saugumo optimalaus lygio nustatymo metodus mano, kad kai kuriais aspektais elektroninės erdvės saugumą galima lyginti su tradiciniu saugumu[13]. Pavyzdžiui, piliečiui, besirūpinančiam savo saugumu, žymiai paprasčiau įsidėti sudėtingos konstrukcijos durų spyną, nei laukti kol valstybė sugebės efektyviai kovoti su vagystėmis bendrai. Tokiu būdu vagis paprasčiausiai nukreipiamas pas kaimyną, kurio durų spyna lengviau įveikiama. Atsakingos valstybės institucijos, sugriežtindamos baudžiamąją atsakomybę už nusikaltimus, gali be ekonominės veiklos kovoti su bendru nusikalstamumo didėjimu. Elektroninių nusikaltimų atveju tai padaryti nėra paprasta. Jau vien tikimybė, kad elektroninis nusikaltėlis bus surastas, yra labai maža. Valstybė gali bandyti kovoti su elektroniniais nusikaltimais *ex ante* sugriežtindama atsakomybę ir padidindama bausmes, tačiau elektroninių nusikaltimų srityje tai neduos laukiamo rezultato. Galimybės atskleisti didžiąją elektroninių nusikaltimų dalį šiuo metu yra tokios menkos, kad tik neadekvačiai didelės bausmės gal kažkiek kažkurią elektroninių

[10] Morriss, A. P. The Wild West Meets Cyberspace. *The freeman: ideas on liberty* [interaktyvus]. 1998, 48(7) [žiūrėta 2011.09.30]. <http://www.thefreemanonline.org/featured/the-wild-west-meets-cyberspace/print/>.
[11] Cheung, A. S. Y. A Study of Cyber-Violence and Internet Service Providers' liability: Lessons from China. *Pacific Rim Law & Policy Journal*. 2009, 18(2): 345.
[12] Norton Cybercrime Report 2011. [interaktyvus]. [žiūrėta 2012.04.10]. <http://uk.norton.com/cybercrimereport/promo>.
[13] Kobayashi, B. H., Private versus Social Incentives in Cerbersecurity: Law and Economics. *The Law and Economics of Cybersecurity.* Cambridge University Press, 2006: 13.

nusikaltėlių dalį atbaidytų nuo šios rūšies nusikaltimų. Įmonės ir organizacijos gali įdiegti efektyvias individualias informacinių sistemų apsaugos priemones, bet jos tik nukreips elektroninių nusikaltėlių dėmesį į įmones ir organizacijas, kurių apsaugos priemonės ne tokios efektyvios. Individualiai vykdoma kova su elektroniniais nusikaltimais apsaugo individą, bet neprisideda prie kovos su elektroniniais nusikaltimais bendrai. Nors piliečių pastangos užkirsti kelią individualiam nusikaltėlių persekiojimui, individualiam susidorojimui su jais bei piliečių pagalba teisėsaugos organams yra gyvybiškai svarbūs elementai, organizuojant efektyvų kriminalinių nusikaltimų kontrolės procesą[14], bet kibernetinės erdvės saugumą galima užtikrinti tik kolektyvinėmis pastangomis kuriant sąveikaujančias privačias ir viešąsias gėrybes, kaip yra, pavyzdžiui, kovos su oro tarša atveju.

Grynosios viešosios gėrybės ir privačios gėrybės yra ekonominių gėrybių kraštutiniai atvejai. Tarpiniai ekonominių gėrybių variantai yra negrynosios viešosios ir mišriosios gėrybės. Pagal imtį viešosios gėrybės yra globalios, nacionalinės ir lokalios. Nors viešųjų gėrybių rūšių yra ir daugiau, bet elektroninės erdvės saugumas negali būti priskirtas nei vienai konkrečiai. Pavyzdžiui, jei dėl globalaus saugumo nebuvimo nacionalinis saugumas gali nenukentėti, tai kalbėti vien apie nacionalinį elektroninės erdvės saugumą yra keblu, arba netgi beprasmiška.

Nors klasikinė ekonomikos teorija anksčiau nesvarstė viešųjų ir privačių gėrybių substitucijos klausimo, jei privačių gėrybių kiekis ar kokybė netenkina vartotojo, ekonomistai apie tai prabilo nuo praėjusio amžiaus devinto dešimtmečio. Pavyzdžiui, Charles L. Vehorn, remdamasis trijų atvejų - policijos veiklos, priešgaisrinė apsaugos ir švietimo - analize, teigia, kad nors anksčiau apie viešų ir privačių gėrybių substituciją buvo nekalbama dėl specifinės viešųjų gėrybių prigimties, tačiau išties pakitęs požiūris į vartotoją atveria plačias tokios substitucijos galimybes[15]. Šiai nuomonei prieštarauja Bruce H. Kobayashi. Šis mokslininkas sumodeliavo kibernetinės erdvės kaip viešosios ir privačios gėrybės rinkos pusiausvyrą. Remdamasis atliktos analizės rezultatais, Bruce H. Kobayashi teigia, kad kibernetinės erdvės saugumas yra kompleksinė ekonominė realybė, kurios rinkos pusiausvyra ekonomiškai pagrįstais kaštais ir optimaliomis investicijomis pasiekiama tik tada, kai gerai sukoordinuota ir subalansuota viešosios ir privačios gėrybės gamyba. Jos apimtys priklauso nuo kibernetinių

[14] Cook P. J., MacDonald J.; Public Safety Through Private Action: An Economic Assessment Of Bids. *The Economic Journal.* 2011, N. 121 (May): 445.
[15] Vehorn, Ch. L., (1981), Substitution Between Public And Private Goods: An Overview Of The Market Meeting Consumer Preferences. *Advances in Consumer Research*. 1981, Vol. 08: 523-524.

atakų skaičiaus. Priešingu atveju ekonominiai kaštai ir investicijų dydis nėra optimalūs, ir juntama perteklinės produkcijos tendencija[16].

PRIVAČIOS GĖRYBĖS ELEKTRONINĖS ERDVĖS SAUGUMO TRŪKUMAI

Elektroninės erdvės saugumas turi visus privačios gėrybės požymius. Šiame skyriuje aptarsime keturis rinkos mechanizmo ribotumą lemiančius veiksnius, kurie neigiamai veikia elektroninės erdvės saugumo kaip privačią gėrybės efektyvumą. Tai - neefektyvi viešųjų gėrybių gamyba, eksternalitetai (išorės efektai), polinkis į rinkos monopolizavimą ir informacijos asimetrija.

Pirmas iš pagrindinių rinkos mechanizmo ribotumą lemiančių veiksnių yra viešųjų gėrybių arba ekonominių gėrybių, turinčių viešosios gėrybės požymius, neefektyvi gamyba bei paskirstymas. Kaip jau buvo minėta, rinka yra veiksminga, jei ekonominė gėrybė - prekė ar paslauga - teikia naudą tik ją įsigijusiam vartotojui. Todėl elektroninės erdvės saugumas kaip privati gėrybė netaps visiškai neveiksminga, nes visada bus vartotojai (individai ir organizacijos), turintys poreikį privačiam saugumui. Tačiau globaliame ar nacionaliniame kontekste, jau nekalbant apie viešojo saugumo elektroninėje erdvėje užtikrinimą, tokia gėrybė bus nepakankamai veiksminga, dėl privataus sektoriaus vengiamų eksternalitetų (išorinių efektų).

Eksternalitetas (išorinis efektas) - viena iš rinkos ydų. Eksternalitetas yra kai žmogus ar įmonė užsiima veikla, kuri turi poveikį kitam žmogui ar firmai, ir kai pastariesiems už tai nemokama ar jie nemoka. Eksternalitetų paveiktos rinkos lemia neefektyvų išteklių paskirstymą. Gamybos lygiai ir išlaidos, nukreiptos kontroliuoti eksternalitetą, bus neteisingi. Kai kuriais atvejais žmogaus ar įmonės veiksmai duoda nekompensuotą naudą kitiems. Jie yra vadinami teigiamais eksternalitetais (išoriniais efektais). Veiksmai, kurie kitus veikia nepalankiai, yra vadinami neigiamais eksternalitetais (išoriniais efektais). Neigiamų išorinių efektų gamyba reiškia, kad ribiniai socialiniai kaštai viršija ribinius privačius kaštus, ir rinkos pusiausvyroje prekės gamyba bus per didelė. Eksternalitetų pasekmės yra dvi. Privatus sektorius linkęs į perteklinę prekių, sukuriančių neigiamus eksternalitetus, gamybą ir nepakankamą prekių, sukuriančių teigiamus eksternalitetus, pasiūlą. Bendrai, kai yra

[16] Kobayashi, B. H., Private versus Social Incentives in Cerbersecurity: Law and Economics. *The Law and Economics of Cybersecurity.* Cambridge University Press, 2006: 17-19.

eksternalitetai, rinkos pusiausvyra nebus efektyvi. Prie eksternaliteto problemos reikėtų pridėti „zuikiavimo“ problemą[17], kurios čia nenagrinėsime dėl straipsnio apimties limitų.

Dar viena rinkos yda - polinkis į monopolizavimą. Visiems žinoma, kad didelė dalis kompiuterinių virusų ir kitų kenkėjiškų programų nutaikyti į firmos Microsoft programinę įrangą. Taip atsitinka ne todėl, kad Microsoft gamina nekokybišką ar labiau pažeidžiamą programinę įrangą nei kiti gamintojai. Programišiai ir kibernetiniai nusikaltėliai žino, kad kenkėjiškos programos, rašomos Microsoft programinei įrangai, leis per trumpą laiką pasiekti žymiai gilesnę rinkos skverbtį, todėl tos pačios sąnaudos duos žymiai didesnį ekonominį ir/ar veiklos[18] efektą. Programinės įrangos atveju rinkos polinkis į monopolizavimo glaudžiai siejamas su programinės įrangos tiražavimo kaštais ir iš to gaunamais pelnais[19]. Programinės įrangos tiražavimas gamintojui nekainuoja beveik nieko, todėl pelnas auga eksponentiškai, priklausomai nuo gamintojo padėties rinkoje arba lobizmo. Dėl šios priežasties, esant teisinio reguliavimo prielaidoms[20], programinės įrangos gamintojas gali legaliai monopolizuoti rinką ir užpildyti šalies kritinę infrastruktūrą vienalype programine arba kompiuterine įranga. Tokiu atveju visos kritinės šalies infrastruktūros tampa lengvu ir ekonomiškai naudingu kibernetinių nusikaltėlių taikiniu.

Informacijos asimetrija arba asimetrinė informacija - dar vienas rinkos mechanizmo ribotumą lemiantis veiksnys. Daugiau kaip prieš 30 metų šią sąvoką pirmasis pavartojo Nobelio premijos laureatas G. A. Akerlof. Savo mintis apie asimetrinę informaciją jis išdėstė istoriniame straipsnyje „Niekalo rinka: neapibrėžtis dėl kokybės ir rinkos mechanizmas“ (The Market for Lemons: Quality Uncertainty and the Market Mechanism), paskelbtame 1970 m. Šis jo darbas buvo pripažintas fundamentaliu bei didelės svarbos ekonomikos srityje ir atvėrė kelią dabartinių elgsenos ekonomikos teorijų plėtojimui. Jis nagrinėja prekės rinką, kurioje pardavėjas turi daugiau informacijos apie jos kokybę negu pirkėjas. Tai iliustruoja naudotų automobilių rinkos pavyzdžiu. Pardavėjas turi informaciją apie automobilio būklę, o pirkėjas gali tik tikėtis, kad tai nėra niekalas. Pirkėjas įtariai žiūri į tokią prekę ir daro išvadas apie jos kokybę, nes turi ribotą informaciją. Taigi pirkėjas gali nenorėti mokėti už automobilį tiek, kiek jis vertas, jeigu, tarkime, automobilis nėra niekalas. G. A. Akerlof parodo, kad hipotetiškai informacijos problema gali arba sužlugdyti rinką, arba susiaurinti ją iki žemos

[17] Davulis, G., *Ekonomikos teorija*. Vilnius, 2009: 222.
[18] Jei tikslas neekonomis, bet chuliganiškas arba politinis - nusikaltėlio tikslas yra kuo greičiau su mažiausiomis sąnaudomis suformuoti didelį botnet tinklą.
[19] Iwamura, M. *The Economics of Cyber-Security* [interaktyvus]. Institute for International Policy Studies (Japan), Perspectives Series, 2003 [žiūrėta 2012.04.10] <http://www.iips.org/Perspective_Iwamura.pdf>
[20] Tokias prielaidas sudaro Viešųjų pirkimų įstatymo nuostatos, kurios pagrindiniu kriterijumi laiko žemiausią kainą.

kokybės produktų nepalankaus pasirinkimo. Jo nuomone, normalios rinkos yra dėl to geros, kad jos leidžia žmonėms prekiauti sąžiningai. Esant asimetrinei informacijai, sąžiningos prekybos situacijos nėra. Svarbus dalykas, atskleistas straipsnyje apie „niekalą", yra tas, kad ūkio subjektai gali turėti didelių paskatų kompensuoti nepalankių informacijos padarinių poveikį rinkos efektyvumui. Atsižvelgdamas į tai, G. A. Akerlof įrodinėja, jog daugelis rinkos institucijų atsiranda mėgindamos išspręsti problemas, kylančias dėl asimetrinės informacijos. Vienas iš tokių pavyzdžių yra automobilių prekybos agentų garantijos, kiti - prekių ženklai, parduotuvių tinklai, franšizė ir įvairių rūšių sutartys.[21]. Tai, ką G. A. Akerlof įžvelgė tirdamas naudotų automobilių rinką, galima pritaikyti kitoms rinkoms, kuriose nėra informacijos pusiausvyros, pavyzdžiui, elektroninės erdvės saugumo rinkai. Pateiksime du pavyzdžius - kibernetinio saugumo priemonių rinka bei įmonės vertė rinkoje. R. Anderson labai teisingai pastebi, kad kibernetinio saugumo kontekste informacijos asimetrija sukelia ypač sunkias pasekmes tada, kai vartotojas vertinantis nuslėptą niekalą nėra tas, kuris nukenčia dėl jo vartojimo sukeltų pasekmių. Įmonių vadovai linkę pirkti garsių gamintojų produktus, nors ir žino ar įtaria juos esant nepakankamos kokybės. Tokiu būdu perkantysis gali išvengti atsakomybės už pasekmes.[22]

Aukščiau aptarta viena informacijos asimetrijos pusė - asimetrinė informacija apie prekę/paslaugą. Kita pusė - asimetrinė informacija apie prekės/paslaugos gamintoją. Įmonės reputacija yra fundamentali jos ekonominei dabarčiai ir ateičiai. Informacija apie jos informacinės sistemos neatsparumą kibernetinėms atakoms arba apie jos patirtas sėkmingas kibernetines atakas gali labai pakenkti įmonės reputacijai, sumažinti įmonės akcijų vertę ir pakirsti klientų pasitikėjimą. Kas patikės savo pinigus bankui, jei žinoma, jog to banko elektroninė sistema neatspari kibernetinėms atakoms? Tyrimai rodo, kad investicijų į elektroninį saugumą dydis skirtingas atskiruose sektoriuose (bankai investuoja daugiau nei pvz. mažmeninės prekybos maisto produktais įmonės), tačiau reta įmonė investiciją į elektroninę saugą traktuoja kaip alternatyvią investiciją į įmonės įvaizdį.[23] Užsienio įmonių tyrimo rezultatai rodo, kad jos dažniausiai naudoja sudėtingas apskaitos ir analizės sistemas, kurių tikslas - mažinti kaštus ir didinti pelną. Bet reta įmonė nusistato aiškius standartus kokio

[21] Akerlof, George A., "The Market for 'Lemons:' Quality Uncertainty and the Market Mechanism," *Quarterly Journal of Economics*. August 1970, N. 84: 488-500.
[22] Anderson, R.; Why Information Security is Hard - An Economic Perspective. *Computer Security Applications Conference, 2001. Proceedings 17th Annual.* Conference Publications. ACSAC 2001: 593.
[23] Kiely, M.; Kobe, E.; MacArthur, A.; Polk, M.; Rains, E.; Andrijcic, E.; Crawford, J.; Horowitz, B., Macro-Economic Cyber Security Models. *Systems and Information Engineering Design Symposium, 2006 IEEE, Conference publication.* Charlottesville, University of Virginia, 2006: 288-289.

lygio elektroninio saugumo jai reikia ir kiek reikia į tai investuoti. Nacionaliniu ar globaliu mastu nustatytų standartų nebuvimas šį procesą palieka pačių įmonių nuožiūrai[24].

Ne visos kibernetinės erdvės grėsmės nukreiptos į asmenis ar privatų sektorių. Prie to pridėję rinkos mechanizmo ribotumą lemiančius veiksnius ir asmenų bei privataus sektoriaus tendencijas nepakankamai investuoti į apsaugą nuo kibernetinių grėsmių, galime konstatuoti, kad formuojasi situacija, kai kibernetinės atakos gali turėti katastrofiškas pasekmes nacionaliniam saugumui. Be valstybinio reguliavimo asmenys ir privataus sektoriaus įmonės niekada savanoriškai nepasieks reikiamo atsparumo kibernetinėms grėsmėms lygio, nes kibernetinis saugumas kaip privati gėrybė turi perteklinę tendenciją (lokalizuojama aukščiau pusiausvyros taško). Todėl asmenis ir privataus sektoriaus įmones bei organizacijas būtina įtraukti į kibernetinės erdvės kaip viešosios gėrybės kolektyvinę gamybą.

Bruce H. Kobayashi mano, kad rinkos mechanizmo ribotumą lemiantys veiksniai ir koordinavimo tarp viešosios ir privačios gėrybės stygius skatina privačios gėrybės gamybos apimčių deficitines tendencijas, todėl ekonominiai kaštai bei investicijų dydis nėra optimalūs[25].

EKONOMINIO IR MOKSLO PAGRĮSTUMO BEI TEISĖTUMO PRINCIPŲ SVARBA VIEŠOSIOS IR PRIVAČIOS GĖRYBIŲ KŪRIME

2011 m. Vidaus reikalų ministerijos specialistai parengė, o 2011 m. birželio mėn. Vyriausybė patvirtino pirmą Nacionalinę elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metams programą[26], kurioje nurodytos pagrindinės strateginės kryptys ir gairės kibernetinio saugumo srityje. Programos tikslas - sudaryti prielaidas kibernetinio saugumo plėtojimui Lietuvoje 2011-2019 metais. Siekiant šio tikslo už kibernetinio saugumo plėtrą atsakingoms institucijoms iškelta apie 60 uždavinių, tarp jų - suformuoti grėsmių ir pažeidžiamumų kibernetinėje erdvėje valdymo sistemą, sukurti elektroninės informacijos saugos sistemą, stiprinti teisinę bazę, reikalingą efektyviam reagavimui į saugumo incidentus elektroninių ryšių tinkluose ir pan. Šis teisės aktas labai svarbus, nes iki tol Lietuvoje nebuvo dokumentų, kuriais būtų apibrėžtos elektroninės

[24] Rowe, B. R.; Gallaher, M. P.; Private Sector Cyber Security Investment Strategies: An Empirical Analysis. *The Fifth Workshop on the Economics of Information Security (WEIS 2006).* Robinson College, University of Cambridge, 2006. [interaktyvus]. [žiūrėta 2012.04.10] <http://www.weis2006.econinfosec.org/docs/18.pdf> (The study funded by the U.S. Department of Homeland Security)

[25] Kobayashi, B. H., Private versus Social Incentives in Cerbersecurity: Law and Economics. *The Law and Economics of Cybersecurity.* Cambridge University Press, 2006: 30-32.

[26] Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programa. Valstybės Žinios, 2011-07-09, nr. 83-4033 (Valstybės Žinios, 2011-08-27, nr. 106 Atitaisymas (programos priedo 47 punkto))

informacijos saugos gairės. Tačiau stokojama vientisumo, nestinga trūkumų, atskleidžiančių kad Lietuva dar tik žengia pirmuosius žingsnius elektroninės erdvės saugumo kaip viešosios kolektyvinės gėrybės kūrimo linkme. Dokumento tekstas organizuojamas apie dvi pagrindines ašis - technologiniai sprendimai ir teisinės bazės kūrimas/stiprinimas. Pasaulinė praktika jau atskleidė, kad vien technologiniai sprendimai nepajėgūs garantuoti pakankamą kibernetinės erdvės saugumo lygmenį[27], o be ekonominės logikos kuriama/stiprinama teisinė bazė neduos ekonomiškai efektyvaus rezultato.

2003 m. patvirtintoje Nacionalinėje nusikaltimų kontrolės ir prevencijos programos[28] punkte 24 konstatuojama, kad nusikaltimų prevencijos ir kontrolės veiklos efektyvumas gali būti užtikrintas tik jei vadovaujamasi nustatytais reikalavimais ir pagrindiniais sėkmingos veiklos principais, kurių sąrašas susideda iš 14 principų. Paminėsime du. Punkte 24.6 aprašytas efektyvumo ir ekonominio pagrįstumo principas: „Nustatant numatomų vykdyti priemonių ekonominį pagrįstumą, vertinama ne tik poveikio efektyvumas bei priemonės vykdymo išlaidos, bet ir tikėtina jos vykdymo ekonominė nauda. Prioritetas teikiamas ne pigiausioms, bet labiausiai ekonominiu ir efektyvumo požiūriu pagrįstoms priemonėms“. Punkte 24.14 aprašomas mokslinio pagrįstumo principas: „Nusikaltimų prevencijos ir kontrolės planai turi būti pagrįsti moksliškai, jie turi būti vykdomi tik esant pakankamai racionalių mokslinių argumentų, rodančių tikėtiną šių planų veiksmingumą“. Kalbant apie Nacionalinę elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metams programą, jos rengėjai nepasivargino nustatyti bent kažkokius principus, kas verčia suabejoti programos rengėjų kompetencija arba pačios programos pasiektų rezultatų efektyvumu. Ekonominio pagrįstumo ir mokslinio pagrįstumo principai glaudžiai susiję ir duoda sinergijos efektą.

Kalbant apie programos pirmą tikslą „pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas“ (punktas 6.1), dokumento autoriai konstatuoja, kad „...trūksta Lietuvos viešojo ir privataus sektoriaus subjektų bendradarbiavimo...“. Akivaizdu, kad jie mokslą priskiria viešajam sektoriui, o mokslo rezultatus traktuoja kaip viešąją gėrybę, nes apie Lietuvos mokslo tam tikrą dalyvavimą elektroninės erdvės saugumo užtikrinime užsimenama tik dokumento priedo punkte 22. Šiame punkte uždavinio 1.4 „skatinti elektroninės informacijos saugos (kibernetinio saugumo) projektų įgyvendinimą“ vienu iš vertinimo kriterijų nurodoma „Šalies ūkio subjektų ir mokslo įstaigų iniciatyvų (tyrimų, projektų, sprendimų ir

[27] Stein Schjolberg, S.; Ghernaouti-Helie, S., *A Global Treaty on Cybersecurity and Cybercrime*. Oslo, 2011: 31-32.
[28] Nacionalinė nusikaltimų prevencijos ir kontrolės programa prevencijos programa. *Valstybės žinios*. 2003, Nr.: 32 - 1318.

panašiai), prie kurių įgyvendinimo prisidėjo valstybės institucijos, dalis, procentais“, o už kriterijaus įgyvendinimą atsakingomis institucijomis skiriamos Švietimo ir mokslo ministerija, Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba, LITNET taryba. UNESCO 1998 m. paskelbtoje Pasaulinėje deklaracijoje dėl aukštojo mokslo[29] visuose šešiuose misijos apibrėžimuose yra išryškinti viešosios gėrybės akcentai, tačiau mokslo kuriamos gėrybės statusas, nepriklausomai nuo mokslo institucijos juridinio statuso, yra specifinis. Jis užima tarpinę poziciją tarp viešosios ir privačios gėrybės. Todėl mokslo erdvė yra pati tinkamiausia efektyviam bendradarbiavimui ir dialogui tarp trijų sektorių: viešojo, privataus ir mokslo. Ypač tai svarbu kolektyvinės viešosios gėrybės kūrimo atveju, nes mokslas, nesant suformuotos mokslo politikos ir finansavimo šaltinių, gali apsiriboti vien fundamentaliais tyrimais ir viešajam bei privačiam sektoriams neaktualia tematika. Pavyzdžiui, iš 90 paraiškų, pateiktų Žmogiškųjų išteklių plėtros veiksmų programos 3 prioriteto „Tyrėjų gebėjimų stiprinimas“ įgyvendinimo priemonės „Parama mokslininkų ir kitų tyrėjų mokslinei veiklai (visuotinė dotacija)“ II kvietimo konkursui, vienintelis Mykolo Romerio universiteto projektas „Lietuvos valstybės pajėgumo kovoti su elektroniniais nusikaltimais ir užtikrinti kritinės elektroninės informacijos infrastruktūros apsaugą tyrimas“, kuriam pajėgas sujungė Viešojo saugumo ir Socialinės informatikos fakultetų mokslininkai, siekia kompleksiškai tirti valstybės pajėgumus kovoti su elektroniniais nusikaltimais ir pasiūlyti kompleksinius veiklos gerinimo pasiūlymus[30]. Atkreiptinas dėmesys į tai, kad iki šiol nei vienoje Lietuvos mokslo programoje elektroninės erdvės saugumas nėra išryškintas kaip prioritetinė mokslinių tyrimų kryptis ir sritis. Tai, be jau minėto komunikacijos tarp sektorių stygiaus, rodo komunikacijos stygių viešojo (valstybinio) sektoriaus viduje.

Laukiamo ekonominio rezultato nebus įmanoma pasiekti, jei jau minėta ekonominio pagrįstumo ir mokslinio pagrįstumo principų sąveika nepapildys teisėtumo principas, kuriam Programoje skirtas pirmo tikslo uždavinys 1.2: „tobulinti elektroninės informacijos saugos (kibernetinio saugumo) teisinį reguliavimą“. Bet ar galima tikėtis laukiamo rezultato, teisingumo principas - kurį galima traktuoti kaip mokslinio pagrįstumo principo posistemę - nesąveikauja su ekonominio pagrįstumo principu?

[29] UNESCO, Pasaulinė deklaracija dėl aukštojo mokslo dvidešimt pirmajame amžiuje: vizija ir veiksmai, 1998 m. spalio 9 d. [žiūrėta 2012.04.10] <http://www.unesco.org/education/educprog/wche/declaration_spa.htm>.
[30] Lietuvos mokslo taryba: Visuotinės dotacijos priemonės II konkursui pateiktų paraiškų sąrašas [interaktyvus]. Vilnius, 2012 [žiūrėta 2012-04-12].
<http://www.lmt.lt/download/1627/2012%2003%2008_vd_ii%20kv_%20pateiktos%20paraiškos.pdf>

Ekonomikos teorija teigia, kad viešojo sektoriaus sprendimai išoriniams efektams skirstomi į dvi plačias grupes: rinka besiremiantys sprendimai ir tiesioginis reguliavimas[31]. Remiantis Naujosios viešosios vadybos paradigma, reguliavimas turi būti rezultatais besiremiantis ir į juos orientuotas[32]. Abiejų grupių sprendimai įgyvendinami per teisinės sistemos tobulinimą, nes ši sistema gali saugoti nuo išorinių efektų net kai nuosavybės teisės nėra idealiai apibrėžtos. Teisės sistema neleidžia vienai šaliai pakenkti kitai, ir "pakenkimas" yra interpretuojamas kaip apimantis įvairovę ekonominių kaštų kitiems. Ne rinkos ribotumas lemia informacinių sistemų nepakankamą atsparumą elektroniniams nusikaltimams. Problema yra ta, kad asmenys ir firmos nesugeba atsižvelgti į socialinius kaštus, susijusius su jų sukeliamais išoriniais efektais, ir pasekmėje, elektroninės erdvės saugumo lygis gali būti pernelyg menkas. Vyriausybės užduotis yra padėti privačiam sektoriui pasiekti socialiai efektyvų atsparumo kibernetinėms atakoms lygį, kad paskatintų žmones ir firmas veikti tokiu būdu, kad jie atsižvelgtų į jų veiksmų pasekmes kitiems. Todėl būtina lyginti kaštus ir naudą, susijusius su atsparumo kontrole. Kadangi tikėtina, kad įmonė ar individas gauna nedidelę tiesioginę naudą iš atsparumo didinimo (dauguma naudos tenka tiems, į kuriuos nukreipiamos kompiuterių „zombių“ vykdomos kibernetinės atakos), nesant baudai už pakankamų apsaugos priemonių netaikymą, jie turi nedaug paskatų išleisti pinigus atsparumo didinimui. Todėl viešojo sektoriaus sprendimų grupės tampa trys: 1) rinka besiremiantys sprendimai; 2) tiesioginis reguliavimas; 3) baudų sistema. Toliau trumpai juos aptarsime ir įvertinsime jų poveikį inovacijų skatinimui.

Rinka besiremiantys sprendimai mėgina paveikti paskatas, siekiant užtikrinti ekonomiškai efektyvias pasekmes. Pavyzdžiui, imant analogus iš kitų sričių, gali būti naudojamos baudos už aplinkos teršimą, kad firmos susidurtų su tikrais jų veiksmų socialiniais kaštais, tuo sumažinant jų paskatas teršti. Vietoje to, kad apmokestintų teršimą, vyriausybė turėtų subsidijuoti teršimo mažinimo išlaidas. Tačiau ši priemonė nepasiekia socialiai efektyvaus išteklių paskirstymo. Priežastis yra paprasta: bendrieji ribiniai gamybos socialiniai kaštai apima vyriausybės subsidijos už teršimo sumažinimą kaštus. Firmos dažnai į tai neatsižvelgia, spręsdamos apie gamybos lygį. Tokiu būdu kaip prieš tai, ribiniai socialiniai gamybos kaštai viršija ribinius privačius kaštus. Teršimo mažinimo subsidijos sumažina ribinius gamybos socialinius kaštus, tačiau jos taip pat sumažina ribinius privačius kaštus. Tai paskatina perprodukciją.

[31] Jakutis, A., *Ekonomikos teorijos pagrindai*. Vilnius, 2006: 344-346.
[32] Thom, N., Ritz, N.; *Viešoji vadyba. Inovaciniai viešojo sektoriaus valdymo metmenys*. Vilnius, 2004: 61-64.

Vienas iš svarių argumentų už tai, kad viešojo sektoriaus sprendimai turi remtis gamybos veiksniais ir praktikomis, yra tai, kad jie gali būti lengviau stebimi. Gali būti sudėtinga arba neįmanoma išmatuoti įmonės informacinės sistemos atsparumą kibernetinėms atakoms, tačiau jei žinoma, kad įmonė naudoja bent minimaliai priimtinas apsaugos priemones, atsparumas bus didesnis nei tuo atveju, kai priemonės nenaudojamos.

Metodų, besiremiančių gamybos veiksniais, o ne rezultatais kritikai teigia, kad tokie metodai neefektyvūs ir neskatina inovacijų ir stumia jas bloga kryptimi. Vietoje to, kad siektų efektyviausio būdo sumažinti išmetimus iš anglis deginančių energijos gamyklų, tyrimai skirti sukurti pigiausią filtrą. Be to tyrimai, skirti pagerinti gebėjimą tiksliai stebėti taršą (taip sumažinant būtinumą remtis gamybos veiksnių reguliavimu), nėra skatinami.

Viena iš priežasčių rezultatais besiremiančiam reguliavimui ir baudų/mokesčių sistemai būtų siekis tiesiogiai spręsti problemą - kibernetinės erdvės saugumo lygis - ir skatinti inovacijas, tokias kaip nauji apsaugos būdai ar naujos technologijos. Taip atsirastų suinteresuotumas didinti saugumą mažesniais kaštais

Vyriausybė gali naudoti tiesioginį reguliavimą, kad ribotų išorinius efektus (kaip privalomų išmetimo standartų automobiliams atveju). Reguliavimo šalininkai teigia, kad jis lemia didesnį apibrėžtumą: jei firmoms draudžiama teršti vandenį daugiau už duotą teršimo lygį, tada žinome maksimalų teršimo lygį, o esant baudoms, teršimo lygis priklauso nuo teršimo lygio sumažinimo kaštų. Iš tikrųjų, pagrindinė reguliavimo kritika yra ta, kad jis nesumažina teršimo efektyviausiu būdu: skirtingos firmos gali susidurti su skirtingais ribiniais tolesnio teršimo mažinimo kaštais. Be to, reguliavimas paprastai teikia nedaug ar jokių paskatų firmoms sumažinti teršimą daugiau už nustatytą standartą, nepaisant to, kokie nedideli to kaštai.

Vyriausybė gali naudoti tiesioginį reguliavimą, kad ribotų rinkos polinkį į monopolizavimą. Tačiau aktualios Viešųjų pirkimų įstatymo nuostatos, sutelkiančios dėmesį tik į mažiausios kainos kriterijų, veikia priešingai - sudaro sąlygas monopolizuoti valstybinio sektoriaus informacinių sistemų rinką, ją užpildant vieno gamintojo kompiuterine ir programine įranga. Kaip jau buvo minėta, tai ypatingai susilpnina kritinių infrastruktūrų atsparumą kibernetinėms atakoms.

Nors šiandien informacinių sistemų ir kritinių infrastruktūrų atsparumo lygis negali būti tiesiogiai matuojamas, gerai sukurta reguliavimo sistema, kreipianti dėmesį į rezultatus, gali teikti paskatas inovacijoms, didinančioms gebėjimą stebėti. Todėl kur galima, yra pageidautina taikyti tiek reguliavimą, tiek rinka besiremiančiuos sprendimus.

Praktika rodo, kad kai kuriais atvejais griežtas reguliavimas vietoje inovacijų skatinimo gali paskatinti bylinėjimąsi: įmonei gali atrodyti pigiau mėginti įtikinti teismą, kad reguliavimas yra neprotingas, nei išleisti pinigus ir atitikti reguliavimo nustatytus standartus. Kai kuriais atvejais, firmos gali žaisti "viščiuką", spėdamos, kad jei jos nesugebės atitikti standartų, vyriausybės jų neuždarys, bijodamos politinio darbuotojų, kurie tapo bedarbiais, keršto. Nors elektroninės erdvės saugumas yra pakankamai svarbi priežastis kryptingai formuoti ekonomikos politiką, įvedančią privalomus standartus ir baudas, kai kuriais atvejais darant sprendimą dominuoja politinė, o ne ekonominė logika.

Apibendrinant galima teigti, kad Nacionalinėje elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metams programoje stinga dėmesio ekonominio pagrįstumo, mokslinio pagrįstumo ir teisėtumo principams bei jų sąveikai. Kaip buvo išryškinta straipsnyje, iš šių trijų ekonominio pagrįstumo principas yra svarbiausias, nes tik jis garantuoja ekonomiškai pagrįstą taikomąją mokslinių tyrimų ir teisinės bazės kūrimo/stiprinimo vertę.

IŠVADOS

Elektroninės erdvės saugumas turi visus viešosios gėrybės požymius, tačiau kibernetinės erdvės saugumas yra kompleksinė ekonominė realybė, kurios rinkos pusiausvyra ekonomiškai pagrįstais kaštais ir optimaliomis investicijomis pasiekiama tik tada, kai gerai sukoordinuota ir subalansuota viešosios ir privačios gėrybės gamyba. Jos apimtys priklauso nuo kibernetinių atakų skaičiaus. Priešingu atveju ekonominiai kaštai ir investicijų dydis nėra optimalūs, ir juntama perteklinės produkcijos tendencija.

Elektroninės erdvės saugumas turi visus privačios gėrybės požymius, tačiau rinkos mechanizmo ribotumą lemiantys veiksniai neigiamai veikia elektroninės erdvės saugumo kaip privačios gėrybės gamybos efektyvumą. Tai - neefektyvi viešųjų gėrybių gamyba, eksternalitetai (išorės efektai), polinkis į rinkos monopolizavimą ir informacijos asimetrija. Šie veiksniai ir koordinavimo tarp viešosios ir privačios gėrybių gamybos stygius skatina privačios gėrybės gamybos apimčių deficitines tendencijas, todėl ekonominiai kaštai bei investicijų dydis nėra optimalūs

Nacionalinėje elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metams programoje dominuoja dėmesys technologiniams sprendimams ir stinga dėmesio ekonominio pagrįstumo, mokslinio pagrįstumo ir teisėtumo principams bei jų sąveikai. Kaip buvo išryškinta straipsnyje, šie trys principai formuoja sinerginės sąveikos

kompleksą, kuriame ekonominio pagrįstumo principas yra svarbiausias, nes tik jis garantuoja taikomąją mokslinių tyrimų ir inovacijų bei teisinės bazės kūrimo/stiprinimo vertę, o taip pat kibernetinės erdvės saugumo optimalius ekonominius kaštus ir investicijų dydį.

LITERATŪRA

1. Nacionalinė nusikaltimų prevencijos ir kontrolės programa prevencijos programa. *Valstybės žinios*. 2003, Nr.: 32 - 1318.
2. Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programa. *Valstybės Žinios.* 2011, Nr.: 83-4033 (*Valstybės Žinios.* 2011, Nr.: 106 Atitaisymas (programos priedo 47 punkto)).
3. UNESCO, Pasaulinė deklaracija dėl aukštojo mokslo dvidešimt pirmajame amžiuje: vizija ir veiksmai, 1998 m. spalio 9 d. [žiūrėta 2012.04.10] <http://www.unesco.org/education/educprog/wche/declaration_spa.htm>.
4. CERT-LT: metinė ir ketvirtinė incidentų statistika. [interaktyvus]. [žiūrėta 2012.04.10]. <https://www.cert.lt/statistika.html>.
5. McKinsey&Company, Internet matters: The Net's sweeping impact on growth, jobs, and prosperity [interaktyvus]. 2011. [žiūrėta 2012.04.10]. <http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters>.
6. 2011 m. gruodžio 21 d. pranešimas VIR. [interaktyvus]. [žiūrėta 2012.04.10] <http://www3.lrs.lt/pls/inter/w5_show?p_r=4463&p_d=119407&p_k=1>.
7. Lietuvos Statistikos departamentas: Lietuvos BVP 2011 kainomis. [interaktyvus]. [žiūrėta 2012.04.10] <http://db1.stat.gov.lt/statbank/SelectVarVal/saveselections.asp>.
8. Lietuvos Statistikos departamentas: Lietuvos bendrosios pridėtinės vertės struktūra. [interaktyvus]. [žiūrėta 2012.04.10] <http://db1.stat.gov.lt/statbank/selectvarval/saveselections.asp?MainTable=M2010253&PLanguage=0&TableStyle=&Buttons=&PXSId=18531&IQY=&TC=&ST=ST&rvar0=&rvar1=&rvar2=&rvar3=&rvar4=&rvar5=&rvar6=&rvar7=&rvar8=&rvar9=&rvar10=&rvar11=&rvar12=&rvar13=&rvar14=>
9. Norton Cybercrime Report 2011. [interaktyvus]. [žiūrėta 2012.04.10] <http://uk.norton.com/cybercrimereport/promo>.
10. Lietuvos mokslo taryba: Visuotinės dotacijos priemonės II konkursui pateiktų paraiškų sąrašas [interaktyvus]. Vilnius, 2012 [žiūrėta 2012-04-12]. <http://www.lmt.lt/download/1627/2012%2003%2008_vd_ii%20kv_%20pateiktos%20paraiškos.pdf>.
11. Akerlof, G. A., The Market for 'Lemons:' Quality Uncertainty and the Market Mechanism. *Quarterly Journal of Economics*, August 1970, 84: 488-500.
12. Anderson, R.; Why Information Security is Hard - An Economic Perspective. *Computer Security Applications Conference, 2001. Proceedings 17th Annual.* Conference Publications. ACSAC 2001: 358-365.
13. Cheung, A. S.Y. A Study of Cyber-Violence and Internet Service Providers' liability: Lessons from China. *Pacific Rim Law & Policy Journal*. 2009, 18(2): 323-346.
14. Cook P. J., MacDonald J.; Public Safety Through Private Action: An Economic Assessment Of Bids. *The Economic Journal.* 2011, N. 121 (May): 445–462.
15. Davulis, G., *Ekonomikos teorija*. Vilnius, 2009.
16. Iwamura, M. The Economics of Cyber-Security [interaktyvus]. Institute for International Policy Studies (Japan), Perspectives Series, 2003 [žiūrėta 2012.04.10] <http://www.iips.org/Perspective_Iwamura.pdf>.

17. Jakutis, A., *Ekonomikos teorijos pagrindai*. Vilnius, 2006.
18. Kiely, M.; Kobe, E.; MacArthur, A.; Polk, M.; Rains, E.; Andrijcic, E.; Crawford, J.; Horowitz, B., Macro-Economic Cyber Security Models. *Systems and Information Engineering Design Symposium, 2006 IEEE, Conference publication.* Charlottesville, University of Virginia, 2006: 284-291.
19. Kobayashi, B. H., Private versus Social Incentives in Cerbersecurity: Law and Economics. *The Law and Economics of Cybersecurity.* Cambridge University Press, 2006: 13-28.
20. Morriss, A. P. The Wild West Meets Cyberspace. *The Freeman: Ideas on Liberty* [interaktyvus]. 1998, 48(7) [žiūrėta 2011.09.30]. < http://www.thefreemanonline.org/featured/the-wild-west-meets-cyberspace/print/>.
21. Rowe, B. R.; Gallaher, M. P.; Private Sector Cyber Security Investment Strategies: An Empirical Analysis. *The Fifth Workshop on the Economics of Information Security (WEIS 2006).* Robinson College, University of Cambridge, 2006. [interaktyvus]. [žiūrėta 2012.04.10] <http://www.weis2006.econinfosec.org/docs/18.pdf>.
22. Stein Schjolberg, S.; Ghernaouti-Helie, S., A Global Treaty on Cybersecurity and Cybercrime. Oslo, 2011.
23. Thom, N., Ritz, N.; Viešoji vadyba. Inovaciniai viešojo sektoriaus valdymo metmenys. Vilnius, 2004.
24. Vehorn, Ch. L., (1981), Substitution Between Public And Private Goods: An Overview Of The Market Meeting Consumer Preferences. *Advances in Consumer Research*. 1981, Vol. 08: 523-526.

ECONOMIC ASPECTS OF CYBERSECURITY

Darius Amilevičius*
Mykolas Romeris University

S u m m a r y

At the beginning of the Internet era to the four spaces of human activities (land, sea, air, space) was added the fifth - the cyberspace. The world economy loss about 388 billion US dollars annually because of cybercrimes. Cybersecurity has become an area of a particular importance – cyberspace becomes more and more vulnerable to cyber breaches. For some time foreign scholars have been arguing that cyber security issues cannot be resolved solely by technological or legal instruments, while many of the problems in this area could be much better explained in the economic language (public goods, information asymmetry, etc).

National security and public safety, are the non competitive public goods, which are used by all citizens of the country. Since 2000, and especially after the terrorist attacks in 11 September 2001, representatives of rapidly developing branches of the economy - cyberspace security economics, security economics and information economics - are looking for answers to the four substantive issues. First - do cybersecurity could be considered a public good? If so, to which extent the State must produce it? What is the optimum ratio of this public good with the private one? How to deal with the issues of the externalities of the cyber security as a private good? The cybersecurity is the economic reality, the equilibrium point of it using economically justified costs and optimal investitions can be reached only in case when the production of the privat good and public one is well balanced. Its volumes depends on the number of cyber attacks. Otherwise the economic costs and the size of the investment is not optimal, and there is present a surplus trend.

Cybersecurity has all the characteristics of a private good. However, the determinants of market mechanism - the inefficient public goods production, externalities, asymmetry of the information - and the lack of coordination of production between public and private goods of cybersecurity encourages

underproduction trends of private goods, therefore, the economic costs and the size of the investment is not optimal.

National electronic information security (cybersecurity) development programme 2011-2019 is dominated by focus on the technological solutions. There is lack of attention to the principles of economic validity, scientific validity and legality and to their interoperability. As it has been shown is this paper, these three principles form the interoperable complex, which has the synergetic effect. The most important principle is the economic validity, because it shall guarantee the development of research and innovation, shall guarantee the economic value of the scientific researches and of the legal framework, and also the optimal amount of economic costs and investment volume of cybersecurity.

Keywords: cyberspace, cybersecurity, cybersecurity economics, cybercrimes, public goods, privat goods.

Darius Amilevičius*, Mykolo Romerio universiteto Viešojo saugumo fakulteto Humanitarinių mokslų katedros docentas. Mokslinių tyrimų kryptys: elektroninės erdvės saugumo ekonomika, kompiuterinė lingvistika, politinė ir juridinė retorika, žmogaus teisės.

Darius Amilevičius*, Mykolas Romeris University, Faculty of Public security, Department of Humanities, assoc. professor. Research interests: cybersecurity economics, computational linguistic, political and juridical rhetoric, human rights.