ISSN 2029-1701
ISSN 2335-2035 (Online)

Mokslinis žurnalas
VISUOMENĖS SAUGUMAS IR VIEŠOJI TVARKA
PUBLIC SECURITY AND PUBLIC ORDER
2020 (25) Research Journal

IŠŠŪKIAI KIBERNETINIAM SAUGUMUI: SOCIALINĖ INŽINERIJA INSTITUCINIO IZOMORFIZMO KONTEKSTE

Aurimas Šidlauskas[1]

[1]*Mykolo Romerio universitetas*
Ateities g. 20, LT-08303 Vilnius, Lietuva
Telefonas +370 683 36681
El. paštas: aurimas868@gmail.com

Svajūnė Ungurytė-Ragauskienė[2]

[2]*Mykolo Romerio universitetas*
Ateities g. 20, LT-08303 Vilnius, Lietuva
Telefonas +370 602 13885
El. paštas: svajune.unguryte@gmail.com

DOI: 10.13165/PSPO-20-25-26

Anotacija. Kibernetinės atakos sudėtingėja ir tampa vis labiau rafinuotos. Vis daugiau kibernetinių incidentų paremti manipuliavimu žmonėmis, jų silpnybėmis, siekiama apeiti informacijos apsaugos sistemas bei pavogti ir užvaldyti konfidencialią informaciją. Pastebimas socialinės inžinerijos metodais paremtų kibernetinių incidentų skaičiaus didėjimas. Tokia statistika verčia organizacijas reaguoti į pokyčius ir prisitaikyti prie vyraujančio institucinio lauko, tobulinti esamą teisinį reguliavimą. Straipsnio tikslas – išanalizavus socialinės inžinerijos sąvokos turinį ir tokio tipo kibernetinių atakų atsiradimo prielaidas bei kibernetinių incidentų valdymo reglamentavimą nacionalinėje teisėje, pateikti išvadas ir rekomendacijas kibernetinio saugumo reguliavimo tobulinimui institucinio izomorfizmo kontekste. Atlikta analizė atskleidė, jog šiuo metu Lietuvoje socialinės inžinerijos institucinis izomorfizmas nukreiptas tik į techninius kibernetinį saugumą užtikrinančius veiksnius, o žmogiškajam faktoriui skiriama nepakankamai dėmesio. Siekiant įveikti socialinės inžinerijos keliamus iššūkius išauga darbuotojų švietimo kibernetinio saugumo tematika poreikis. Augant socialinės inžinerijos rūšies kibernetiniams incidentams taip pat svarbu vadovautis geroja praktika, kuri kartu su nacionalinės teisės aktais būtų įtvirtinta organizacijų kibernetinio saugumo politikoje, numatant aiškią kibernetinių incidentų valdymo procedūrą.

Pagrindinės sąvokos: socialinė inžinerija, kibernetiniai incidentai, kibernetinis saugumas, institucinis izomorfizmas.

ĮVADAS

Nacionalinėje kibernetinio saugumo būklės ataskaitoje (2019) rašoma, kad 2018 m. užfiksuotas 25 procentais didesnis socialinės inžinerijos metodais paremtų kibernetinių incidentų skaičius. To priežastis yra žmogaus veiksnio išnaudojimas kibernetinėms atakoms realizuoti. Išaugo kibernetinių incidentų sudėtingumas, atakos tampa vis labiau rafinuotos. Pasaulinių rizikų ataskaitoje (2020) nurodoma, kad ateityje kibernetinių atakų tik daugės. Krašto apsaugos ministerijos bendradarbiaujant su „Kurk Lietuvai“ išleistame kibernetinio

saugumo vadove (2020) rašoma, kad socialinės inžinerijos technikos keičiasi ir atsiranda vis naujesnių apgavystės metodų. Tokia kibernetinių incidentų statistika verčia organizacijas reaguoti į pokyčius ir prisitaikyti prie vyraujančio institucinio lauko, tobulinant esamą teisinį reguliavimą, pateikiant rekomendacijas ar numatant vidaus veikimo politiką. Grėsmių nacionaliniam saugumui vertinime (2020) rašoma, kad kenkėjiškos veiklos aktyvumas Lietuvos kibernetinėje erdvėje išlieka aukštas, todėl labai svarbus yra tokios situacijos detalus nagrinėjimas. Viena iš teorijų, leidžiančių nagrinėti tokio prisitaikymo galimybes yra iš institucionalizmo kilusi institucinio izomorfizmo koncepcija, kuri remiasi trimis mechanizmais – reguliaciniu, reiškiančiu reguliavimą iš „išorės“, normatyviniu, apimančiu organizacijos vidaus politika ir imitaciniu, paremtu veiksmų ar strategijų atkartojimu.

Mokslinė problema – kokios yra socialinės inžinerijos incidentų atsiradimo prielaidos ir kaip tobulinti kibernetinio saugumo reguliavimą institucinio izomorfizmo kontekste?

Straipsnio tikslas – išanalizavus socialinės inžinerijos sąvokos turinį ir tokio tipo kibernetinių atakų atsiradimo prielaidas bei kibernetinių incidentų valdymo reglamentavimą nacionalinėje teisėje, pateikti išvadas ir rekomendacijas kibernetinio saugumo reguliavimo tobulinimui institucinio izomorfizmo kontekste. Išsikeltam tikslui pasiekti numatyti **uždaviniai**:

Įvardinti socialinės inžinerijos sąvoką ir rūšis.

Išanalizuoti kibernetinių incidentų valdymo reglamentavimą nacionalinėje teisėje.

Išnagrinėti socialinę inžineriją pasitelkus institucinio izomorfizmo koncepcijos tris mechanizmus.

Siekiant atsakyti į išsikeltus uždavinius buvo taikomas sisteminės literatūros ir duomenų analizės **metodas**, apimantis kibernetinių incidentų statistikos apžvalgą, socialinės inžinerijos sąvokos ir rūšių apibrėžimus. Surinkti duomenys analizuojami pasitelkiant institucinio izomorfizmo koncepcijos tris jos mechanizmus – priverstinį arba reguliacinį, normatyvinį ir mimetinį. Atlikta analizė atskleidė, jog nagrinėjant socialinės inžinerijos atvejį priverstinio izomorfizmo pagrindu didžiausias dėmesys turi būti skiriamas reguliavimui nacionaliniu lygmeniu. Remiantis normatyviniu izomorfizmu lemiamą vaidmenį atlieka vidiniai reiškiniai organizacijoje ir profesionalų žinios, galinčios padėti įveikti socialinės inžinerijos keliamus iššūkius organizacijoms tikslingai vykdomų mokymų dėka. Socialinės inžinerijos nagrinėjimo atveju mimetizmas gali pasireikšti per jau išaiškintų kibernetinių nusikaltimų atvejų viešinimą ir sėkmingai taikomų praktikų atkartojimą.

SOCIALINĖS INŽINERIJOS SĄVOKA, PSICHOLOGINIAI ĮTAKOS VEIKSNIAI IR TIPAI

Socialinė inžinerija informacijos saugumo kontekste yra psichologinio manipuliavimo forma, kuri apima socialines priemones nukreiptas ir vykdomas atliekant sistemos puolimą per netechninius vektorius. Tai yra labai sėkmingas kibernetinių užpuolikų įrankis, nes jis priklauso nuo žmonių polinkio pasitikėti vienas kitu. Paprastai tai apima socialinius įgūdžius, leidžiančius užpuolikams surinkti reikiamą informaciją, reikalingą apeiti organizacijos saugumo protokolus (Gobeo, 2018). Socialinės inžinerijos terminas siejamas su informacijos saugumo pažeidimais pasinaudojus žmogiškuoju faktoriumi. Žmogus, pirmiausia yra individas, kurio negali užprogramuoti veikti pagal tam tikras taisykles, bet kurioje situacijoje. Jis pasielgs taip, kaip jam atrodo teisingiausia ir priimtiniausia. Taigi socialinių inžinierių taikinys žmogus ir jo silpnybės, kurias jie meistriškai išnaudoja siekdami užsibrėžto tikslo (Dirgėla, 2007). Socialinė inžinerija siejama su žmonių klaidinimu ir manipuliavimu, o ne technologijomis ar kitais mechanizmais. Šis metodas yra populiarus, nes žmogiškasis elementas dažnai yra silpniausia sistemos dalis ir labiausiai linkęs į klaidas (Shimonski, 2016).

Socialinė inžinerija reiškia psichologinį žmonių manipuliavimą atliekant veiksmus ar konfidencialios informacijos atskleidimą. Tai yra pasitikėjimo savimi būdas rinkti informaciją, sukčiauti ar gauti prieigą prie sistemos. Socialinė inžinerija dažnai yra tik viena iš kompleksinės atakos dalių. Visi socialinės inžinerijos metodai yra pagrįsti specifiniais žmogaus sprendimų priėmimo atributais, vadinamais kognityviniais šališkumais – žmogiško faktoriaus klaidomis, siekiant atlikti išpuolius (Smith, 2015). Šiandien žmonės greičiau nei bet kada anksčiau gali rinkti informaciją apie asmenis ir organizacijas. Internetinėse duomenų bazėse, viešuose įrašuose ir socialinės žiniasklaidos svetainėse yra stulbinantis gausumas informacijos, ir daugeliu atvejų šie duomenys yra nemokami. Daugelis žmonių skelbia išsamią asmeninę informaciją apie savo kasdienę veiklą visam pasauliui. Kai užpuolikas surenka informaciją apie vidinius procesus, žmones ar sistemas, jie gali naudoti ją sudėtingesnėms atakoms vykdyti (Andress, 2019). Vis daugiau žmonių naudojasi socialinių tinklų svetainėmis, siekdami skatinti socialinius ryšius. Nors teikiamų paslaugų pranašumai yra akivaizdūs, dažnai nepaisoma vartotojų privatumo trūkumų ir kylančių padarinių (Huber et al.,2009), norint saugiai naudotis socialinio tinklo paslaugomis, būtina didinti vartotojų informuotumą ir juos šviesti apie galimas grėsmes (Albladi ir Weir, 2020).

Socialinė inžinerija tapo rimta grėsme virtualiose bendruomenėse ir yra veiksminga priemonė pulti informacines sistemas (Krombholz, 2015). Kibernetiniai nusikaltėliai socialinės inžinerijos metodais bando išvilioti naudotojų pinigus prašydami atlikti pinigines perlaidas, apsimesdami organizacijų vadovais, siūlydami įsigyti prekes suklastotose interneto svetainėse. Šiuo metu socialinės inžinerijos metodai neapsiriboja elektroninių laiškų, suklastotų interneto svetainių kūrimu ar žinučių socialiniuose tinkluose siuntimu – kibernetiniai nusikaltėliai gali paskambinti telefonu, bandyti susisiekti kitais būdais.

Hatfield (2018) teigia, kad po įvairiais socialinės inžinerijos išsireiškimais slypi trys pagrindinės idėjos – episteminė asimetrija, technokratinis dominavimas ir teleologinis pakeitimas:

Episteminė asimetrija atsiranda tada, kai asmuo ar grupė turi didelį žinių pranašumą prieš kitą asmenį ar grupę tam tikroje srityje.

Technokratinis dominavimas atsiranda tada, kai asmuo, turintis aukštą techninių žinių lygį, naudoja tas žinias norėdamas pakeisti kitų elgesį, kai dėl tokio elgesio nukentėjusieji turi mažesnę galią ar valdžią.

Teleologinis pakeitimas įvyksta tada, kai asmuo ar grupė kitame asmenyje ar grupėje pakeičia pirminį savo elgesio tikslą ar tikslą su savuoju – dažnai pakeisdami patį taikinio elgesį.

Socialinės inžinerijos metodais paremti kibernetiniai incidentai susiję su manipuliavimu naudotojų veiksmais internete ir apgaule. Jų metu vyksta informacijos rinkimas, platinama kenkimo programinė įranga, išnaudojami pažeidžiamumai. Siunčiami apgaulingi ir klaidinantys elektroniniai laiškai, rašomos žinutės socialiniuose tinkluose su kenkėjišku kodu ar nuorodomis į kenkėjiškas interneto svetaines. Užpuolikai gali bandyti apgauti darbuotojus, kad jie atskleistų vartotojų vardus ir slaptažodžius, arba gali suteiktų papildomą prieigą (O'Hanley ir Tiller, 2013). T. Kiškis (2012) nurodo socialinės inžinerijos taikymo sritis – įvairaus tipo kritinių duomenų vagystės, pramoninis šnipinėjimas, finansinės machinacijos, sukčiavimas, šantažas, informacijos rinkimas.

Išpuolių, pagrįstų socialine inžinerija, paskatinimas yra tas, kad žmonės tobulina technologijas. Kai išmokstama atakas atremti technologinėmis priemonėmis, psichologinis manipuliavimas sistemos vartotojais ar operatoriais tampa vis patrauklesnis. Taigi saugos inžinierius tiesiog turi suprasti pagrindinę psichologiją ir saugumo pritaikomumą (Anderson, 2008). J. Mikejan (2017) nurodo socialinės inžinerijos psichologinius įtakos veiksnius:

Socialinis programavimas ir smalsumas. Socialinis programavimas yra įtakos instrumentas, kuriuo siekiama paveikti žmonių elgesį, kad jie pradėtų elgtis pagal socialinio inžinieriaus elgesio modelį. Įdomiai suformuluotas žinutės tekstas arba netikėtas, tačiau pažįstamas šaltinis sudomina. Išnaudojamas žmonių noras pirmauti, norėdami parodyti savo vertę, be svarstymų atskleidžia kibernetiniam nusikaltėliui jo prašomą informaciją.

Baimė ir skubėjimas. Kibernetiniai nusikaltėliai žino, kad žmogaus emocijos ir protas ne visada bendradarbiauja, nes kiekvienas žmogus kažko bijo. Priimami skubūs ir neapgalvoti sprendimai, gavus laišką neatkreipiamas dėmesys į jo šaltinį ir turinį.

Pranašumas ir pripažinimas (atlygis). Pranašumas yra būsena, kuomet žmonės jaučiasi daugiau žinantys ir turinčiu didesnę vertę lyginant su kitais. Sukčiavimo aukai ypač svarbi kitų nuomonė, ji gali būti perdėtai giriama. Sukuriama iliuzija, kad bus gaunama kažkokia nauda.

Pasitikėjimas ir empatija. Daug lengviau yra patikėti gauta informacija, nei ją tikrinti ir kritiškai įvertinti. Žmonėms gali būti tiesiog nepatogu kažkam prieštarauti ir išreikšti tam tikras abejones, ypač jei kalba visuomenėje labai gerai žinomas veikėjas. Svarbiausias faktorius – autoritetas. Socialinės inžinerijos metodą naudojantis apgavikas gali manipuliuoti aukos emocijomis – pagalba, užuojauta, globa, motinystė ir tėvystė.

P. Kamat et al. (2018) nurodo šiuos socialinės inžinerijos tipus:

Pretekstas (angl. *Pretexting*). Kibernetinis nusikaltėlis didelį dėmesį skiria patikimo scenarijaus kūrimui, kurį panaudoja kaip pretekstą bandydamas pavogti savo aukų informaciją ar asmeninius duomenis. Sukuriamas melagingas pasitikėjimo jausmas, gali būti apsimetama – bendradarbiu, privačios arba valstybės įmonės darbuotoju. Pavogti asmens duomenys yra panaudojami tapatybės vagystėms ir antriniams išpuoliams įvykdyti.

Masalas (angl. *Baiting*). Apgavystei panaudojamas melagingas pažadas, išnaudojant sukčiavimo aukos godumą ar smalsumą. Aukos įviliojamos į spąstus, pavagiama jų asmeninė informacija arba užkrečiamos informacinės sistemos kenkėjiška programine įranga. Pavyzdžiui, kibernetiniai nusikaltėliai matomose vietose palieka masalą – kenkėjiškų programų užkrėstą USB raktą, tikėdamiesi, kad auka jį ras ir juo pasinaudos. Masalo efektui sustiprinti, USB raktas gali būti išskirtinės išvaizdos, taip pat panaudojamas žinomos įmonės logotipas ir užrašomas tekstas „konfidencialu“, „neskaityti“, „privatu“ ir t.t. Sukčiavimas nebūtinai turi būti vykdomos fiziniame pasaulyje, internete viliojančios reklamos sukčiavimo aukas nukreipia į kenksmingas svetaines arba siūlo atsisiųsti įvairaus skaitmeninio turinio kartu su kenkėjiška programine įranga.

Panika (angl. *Scareware*). Kibernetinių nusikaltėlių aukos atakuojamos melagingais pavojaus signalais ir fiktyviais grasinimais. Pavyzdžiui, interneto naršyklės lange iššoka reklaminės juostos įspėjančios apie pavojų jūsų kompiuteriui, kuriose rašoma „Jūsų kompiuteris užkrėstas virusais, išvalyti“, „Jūs turite virusų, paspauskite šią nuorodą“ ir t. t. Paspaudus tokią reklamą nukreipiama į užkrėstą svetainę arba pradedama siųsti kenkėjiška programinė įranga.

„*Fišingas*“ (angl. *Phishing*). Daugybei žmonių siunčiami suklastoti laiškai su kenksmingu programiniu kodu prisegtuke arba nuorodoje, pranešantys netikėtą loterijos laimėjimą, programinės įrangos gedimą, neapmokėtą sąskaitą, kurią neva siunčia jūsų vadovas arba programinės įrangos teikėjas.

Siekdamos padidinti efektyvumą ir produktyvumą, įmonės linkusios dažniau reorganizuotis ir nuolat tobulina savo IT infrastruktūrą. Dėl to per pastaruosius kelerius metus dauguma organizacijų patyrė reikšmingų pokyčių ir dabar yra labai priklausomos nuo savo IT infrastruktūrų ir joms palaikyti reikalingų įgūdžių rinkinių (Purser, 2004). „*IBM*“ kompanijos ir „*Ponemon*“ instituto tyrimas (2019) parodė, kad beveik kas antras duomenų pažeidimas įvyksta dėl netyčinės žmogaus klaidos ar sistemų pažeidimų. Taip pat 70 proc. informacijos saugos vadovų išskiria kompetentingų darbuotojų trūkumą kaip didžiausią iššūkį siekiant užtikrinti įmonės kibernetinį saugumą. Anot D. Gibson (2014), jei darbuotojai ir vartotojai nesupranta saugumo praktikos vertės, jie mažiau linkę imtis konkrečių veiksmų. Kibernetinio saugumo subjektai skiria daug išteklių ryšių ir informacinių sistemų (toliau – RIS) atsparumui didinti, infrastruktūrai apsaugoti techninėmis priemonėmis, tačiau vis dar per mažai dėmesio skiriama darbuotojams šviesti ir sąmoningumui didinti. Laikomasi nuomonės, kad kibernetinis saugumas yra informacinių technologijų specialistų kompetencijos ir techninės įrangos klausimas. Įvykus kibernetiniam incidentui, atsakomybė dažniausiai yra perkeliama naudotojui, kuris iki įvykio dažniausiai deramai neinformuojamas ar nešviečiamas, kaip valdyti su kibernetiniu saugumu susijusias rizikas (Nacionalinė kibernetinio saugumo būklės ataskaita, 2019). Šiuolaikinei organizacijai svarbu suprasti kibernetinių nusikaltimų galimą žalą ir gebėti tinkamai panaudoti prevencijos priemones (Panavas, 2020). Deja, šių išpuolių negalima sustabdyti naudojant tik technologijas (Salahdine, Kaabouch, 2019).

SOCIALINĖS INŽINERIJOS KIBERNETINIŲ INCIDENTŲ VALDYMAS

Lietuvos Respublikos kibernetinio saugumo įstatyme (toliau – KSĮ) kibernetinis incidentas apibrėžiamas, kaip įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį RIS perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys RIS veikimą, valdymą ir paslaugų jomis teikimą. Iki 2019 m. pradžios kibernetiniai incidentai buvo skaičiuojami atsižvelgiant į automatinėmis priemonėmis apdorotų ir išsiųstų pranešimų bei specialistų betarpiškai (rankiniu būdu) apdorotų kibernetinių incidentų skaičių. Metinėse nacionalinėse kibernetinio saugumo būklės ataskaitose yra pateikiama kibernetinių incidentų skaičiaus statistika (žr. 1 lentelę).

1 lentelė. Kibernetinių incidentų skaičius Lietuvoje 2014 - 2018 m.

Metai	Kibernetinių incidentų skaičius Lietuvoje
2014	36136
2015	41583
2016	49463
2017	54414
2018	53183

Šaltinis: sudaryta autorių pagal nacionalines
2014 – 2018 m. kibernetinio saugumo būklės ataskaitas

Nacionalinis kibernetinio saugumo centas (toliau – NKSC), atsižvelgdamas į būtinybę incidentus klasifikuoti pagal poveikį, nuo 2019 m. kibernetiniais incidentais traktuoja atvejus, kada specialistai įvykius apdoroja betarpiškai – priskiria poveikio reikšmę bei nustato incidento kategoriją. Nuo šiol atskiriami automatinėmis priemonėmis ir programomis apdoroti procesai, kurie traktuojami kaip kibernetiniai įvykiai. Tokia klasifikacija, kai kibernetiniai įvykiai atskiriami nuo kibernetinių incidentų, įvesta siekiant suvienodinti klasifikavimą pagal ES kibernetinio saugumo agentūros bei kitų šalių kibernetinių incidentų valdymo komandų taksonomiją. Didinami pajėgumai ir gerinama kibernetinio saugumo branda leido aiškiau identifikuoti kibernetines grėsmes. Lietuvoje 2019 m. registruotas 3241 kibernetinis incidentas, kai jų tyrimams atlikti reikėjo tiesioginio specialistų dalyvavimo. Automatinėmis priemonėmis apdorotų kibernetinių įvykių skaičius Lietuvos IP rėžyje siekė daugiau kaip 300000, rašoma Nacionalinėje kibernetinio saugumo būklės ataskaitoje (2020).

Kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą, reglamentuojama KSĮ. Lietuvos Respublikos Vyriausybės patvirtintame nacionaliniame kibernetinių incidentų valdymo plane (toliau – Planas) nurodoma, kad už kibernetinių incidentų valdymo organizavimą, stebėseną ir analizę nacionaliniu lygiu atsakingas NKSC, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija ir kitos institucijos, kurių funkcijos susijusios su kibernetiniu saugumu. Kibernetinio saugumo subjektai pateikia NKSC atsakingų asmenų, su kuriais galima susisiekti visą parą, telefono numerius, elektroninio pašto adresus, kitą kontaktinę informaciją, sudarančią sąlygas visą parą keistis informacija kibernetinio incidento valdymo metu. Kibernetinio saugumo subjektas – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros (toliau – YSII) valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas, apibūdinama KSĮ.

Kibernetinio saugumo subjektai Plane nustatytomis sąlygomis ir tvarka praneša NKSC apie jų valdomose ir (arba) tvarkomose RIS įvykusius kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones. Svarbu pabrėžti, kad ši nuostata netaikoma skaitmenines paslaugas Lietuvos Respublikoje ir (arba) kitoje Europos Sąjungos valstybėje narėje teikiančioms mažoms ir labai mažoms įmonėms, kurios yra apibrėžtos Smulkiojo ir vidutinio verslo plėtros įstatyme.

Kibernetinių incidentų poveikis (arba poveikio kategorija) – pavojingas, didelis, vidutinis ir nereikšmingas, skirstomas pagal kriterijus (žr. 1 pav.).

Nereikšmingas (bent vienas iš kriterijų) • RIS trikdoma < 1 val. • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 % • Paslauga teikiama, bet trikdoma • Nuostoliai < 250 000 Eur	**Vidutinis** (bent du iš kriterijų) • RIS trikdoma ≥ 1 val., bet < 2 val. • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 % • Paslauga trikdoma dalyje šalies teritorijos • Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas • Nuostoliai ≥ 250 000, bet < 500 000 Eur
Didelis (bent du iš kriterijų) • RIS trikdoma ≥ 2 val. • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 % • Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje • Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas • Nuostoliai ≥ 500 000 Eur	**Pavojingas** (bent vienas iš kriterijų) • RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas • Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 % • Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše

1 pav. Kibernetinių incidentų poveikis pagal kriterijus
Šaltinis: sudaryta autorių pagal Nacionalinį kibernetinių incidentų valdymo planą

Kibernetinių incidentų poveikį, atsižvelgdami į nustatytus kriterijus, priskiria kibernetinio saugumo subjektai, kurių RIS nustatyti kibernetiniai incidentai, išskyrus pavojingus kibernetinius incidentus, jų kategoriją turi teisę priskirti tik NKSC. Priklausomai nuo kibernetinio incidento kategorijos skiriasi informavimo ir tyrimo procedūros. Kibernetinio saugumo subjektai apie incidentą NKSC gali pranešti telefonu, e. paštu arba užpildę specialią formą jų internetiniame puslapyje. Pranešime informuojant apie didelio ar vidutinio poveikio kibernetinius incidentus pateikiama Plane įvardinta informacija:

1. Kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija.
2. Trumpas kibernetinio incidento apibūdinimas.
3. Tikslus laikas, kada kibernetinis incidentas įvyko ir buvo nustatytas.
4. Kibernetinio incidento šalinimo tvarka (nurodant, ar tai prioritetas, ar ne).
5. Tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita.
6. Plano kriterijų, kuriais vadovaujantis kibernetiniai incidentai priskiriami kibernetinių incidentų kategorijoms, sąraše yra nurodyta socialinės inžinerijos grupė, pogrupis ir galima poveikio kategorija (žr. 2 lent.).

2 lentelė. Socialinė inžinerija Plano kriterijų sąraše

Kibernetinio incidento grupės	**Kibernetinio incidento poveikis** / **Kibernetinio incidento pogrupiai**	**Nereikšmingas (N)**	**Vidutinis (V)**	**Didelis (D)**	**Pavojingas (P)**
Informacijos rinkimas (angl. *information gathering*) Žvalgyba ar kita įtartina veikla (angl. *scanning, sniffing*), manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. ***social engineering***), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti naudotoją atskleisti informaciją (angl. *phishing*) arba atlikti norimus veiksmus	3.1. RIS paketų / informacijos perėmimas		V	D	P
	3.2. RIS klastojimas, siekiant surinkti prisijungimo ar kitą svarbią informaciją, tiksliniai laiškai, kuriuose, pasinaudojant **socialinės inžinerijos** principais, siekiama išvilioti prisijungimo ir (ar) kitą svarbią informaciją, priversti atlikti norimus veiksmus (pvz., finansines operacijas)		V	D	P
	3.3. Vykdoma perimetro priemonių žvalgyba (nebandant įsilaužti)	N	V		
	3.4. Naudojami **socialinės inžinerijos** metodai, siekiant išvilioti prisijungimo prie RIS ir (ar) kitą svarbią informaciją	N	V		

Šaltinis: sudaryta autorių pagal Nacionalinį kibernetinių incidentų valdymo planą

Kibernetinio saugumo subjektai NKSC informuoja apie:

1. Didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per vieną valandą nuo jų nustatymo;
2. Vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per keturias valandas nuo jų nustatymo;
3. Nereikšmingo poveikio kibernetinius incidentus – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

Plane papildomos sąlygos ar išimtys taikomos skaitmeninių paslaugų teikėjams, YSII valdytojams ir asmenims, kuriems teisės aktuose nėra nustatytos pareigos pranešti apie kibernetinius incidentus. Skaitmeninių paslaugų teikėjai NKSC informuoja tik apie didelio poveikio kibernetinius incidentus ir tik tuo atveju, kai gali naudotis informacija, kuri reikalinga incidento poveikiui įvertinti. YSII valdytojai, kurių paslaugų teikimas priklauso nuo skaitmeninių paslaugų teikėjų teikiamų paslaugų, nustatę neigiamą poveikį jų valdomos YSII veiklai, kurį lėmė skaitmeninių paslaugų teikėjų ryšių ir informacinėse sistemose įvykę

sutrikimai, apie šį neigiamą poveikį nedelsdami, bet ne vėliau kaip per vieną valandą nuo neigiamo poveikio nustatymo informuoja NKSC ir skaitmeninių paslaugų teikėjus, kurių RIS įvyko nurodyti sutrikimai. Asmenys, kuriems teisės aktuose nėra nustatytos pareigos pranešti apie kibernetinius incidentus jų valdomose RIS, turi teisę savanoriškai pranešti NKSC apie kibernetinius incidentus ir taikytas kibernetinių incidentų tyrimo ar valdymo priemones.

NKSC gavęs informaciją apie kibernetinį incidentą, turi teisę patikslinti kibernetinio incidento kategoriją (priskirti didesnės ar mažesnės reikšmės kibernetinių incidentų poveikio kategorijai). Taip pat prašyti papildomos informacijos, reikalingos kibernetinio saugumo subjekto RIS kibernetinio saugumo būsenai vertinti, nurodant informacijos pateikimo terminą. NKSC, įvertinęs gautą informaciją, patvirtina, patikslina arba savarankiškai priskiria kibernetinio incidento poveikio kategoriją, ir ne vėliau kaip per vieną valandą nuo informacijos gavimo arba, jeigu kibernetinio saugumo subjekto prašoma papildomos informacijos, nuo papildomos informacijos gavimo informuoja apie tai pranešėją. Kai būtina informuoti visuomenę siekiant išvengti kibernetinio incidento arba valdyti vykstantį kibernetinį incidentą, NKSC, pasikonsultavęs su kibernetinio saugumo subjektu, pranešusiu apie kibernetinį incidentą, informuoja visuomenę apie pavienius kibernetinius incidentus arba reikalauja, kad tai padarytų kibernetinio saugumo subjektas.

Lietuvos Respublikos administracinių nusižengimų kodekso 479 straipsnio 1 dalyje yra įtvirtinta atsakomybė, už KSĮ nuostatų dėl pareigos teikti informaciją pažeidimus, kuri užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims dėl informacijos apie kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones nepateikimo NKSC arba šios informacijos teikimo tvarkos pažeidimo. Pažeidimų pakartotinis padarymas užtraukia griežtesnes baudas.

Nacionalinėje kibernetinio saugumo ataskaitoje (2020) rašoma, organizacijos dažnai atitinka arba beveik atitinka saugos politikos *de jure* kriterijų. Tikrinami subjektai turi formaliai apsibrėžę saugos procesus, gaires, tačiau saugos užtikrinimas dažnai vertinamas kaip biurokratinė našta. Saugos dokumentai būna parengti formaliai, pagal nebegaliojančius Lietuvos Respublikos teisės aktus, o dokumentų turinyje apibrėžti procesai nebūna priskirti pagal kompetenciją.

Socialinės inžinerijos incidentas, priklausomai nuo pogrupio ir poveikio kategorijos, gali būti priskiriamas nereikšmingam, vidutinio, didelio arba pavojingo svarbumo incidentui. Nevaldomas arba netinkamai valdomas, priklausomai nuo pogrupio ir poveikio kategorijos,

nereikšmingas socialinės inžinerijos incidentas gali tapti vidutiniu, o vidutinis – dideliu arba pavojingu. Kibernetinio saugumo subjektai privalo laikytis atitinkamų teisinio reguliavimo procedūrų, už jų nesilaikymą numatyta administracinė atsakomybė. Asmenys, kuriems teisės aktuose nėra nustatytos pareigos apie kibernetinius incidentus pranešti NKSC, turi teisę tai padaryti savanoriškai. Tinkamas reagavimas į kibernetinius incidentus sumažina galimą patirti žalą, siekiant užtikrinti kibernetinį saugumą.

SOCIALINĖ INŽINERIJA INSTITUCINIO IZOMORFIZMO KONTEKSTE

Nagrinėjant socialinės inžinerijos reiškinį pasitarnauja institucinio izomorfizmo teorija, kuri remiasi trimis svertais – priverstiniu arba reguliaciniu, normatyviniu ir mimetiniu. Priverstinis arba reguliacinis izomorfizmas pasireiškia per taisykles, standartus arba įstatymus. Šio mechanizmo atsiradimo prielaida yra išorės spaudimas. Poveikis arba išorės spaudimas, kurį organizacijoms oficialiai ir neformaliai daro kitos organizacijos, nuo kurių jos yra priklausomos (Amor-Esteban et al., 2018). Mokslinėje literatūroje priverstinis izomorfizmas remiasi įstatymų ir kitų teisės aktų bei suinteresuotųjų šalių reikalavimais (Kasperavičiūtė-Černiauskienė, 2014). Nagrinėjant socialinės inžinerijos atvejį priverstinio izomorfizmo pagrindu didžiausias dėmesys turi būti skiriamas reguliavimui nacionaliniu lygmeniu.

Didžiausia grėsmė kyla paprastiems naudotojams dėl kibernetinio saugumo ir IT raštingumo stokos. Ši grėsmė taip pat labai aktuali ir verslo subjektams, kurie dėl socialinės inžinerijos metodais pagrįstų kibernetinių incidentų praranda konfidencialią informaciją arba patiria tiesioginius finansinius nuostolius. Nacionalinėje kibernetinio saugumo būklės ataskaitoje (2020) pateikiamos socialinės inžinerijos metodais pagrįstų kibernetinių incidentų grėsmių valdymo rekomendacijos (pavyzdžiui, kritiškai vertinti reklamas internete ir elektroniniu paštu siunčiamuose laiškuose (ypač siūlomas dideles nuolaidas); prašymus atlikti pinigines perlaidas tikrinti kitais būdais, pavyzdžiui, pasitikslinti aplinkybes paskambinus telefonu, neatlikti skubotų veiksmų, nepasiduoti emocijoms, iki galo išsiaiškinti veiksmų, kuriuos prašoma atlikti, būtinumą ir kt.). Tačiau, šios rekomendacijos nėra pakankamos. Labai svarbu tikslingai parengtos taisyklės, nuolat atnaujinamos rekomendacijos ir tinkamai parengta teisinė bazė.

Socialinę inžineriją taip pat galima analizuoti per dar vieną institucinio izomorfizmo mechanizmą – normatyvinį. Normatyvinis izomorfizmas neatsiejamas nuo organizacinės elgsenos. Organizacijos tam tikros tvarkos laikosi ne todėl, kad išorės veikėjus supranta kaip

galingus, nusistovėjusi vidaus praktika tiesiog tampa savaime suprantama. Normatyvinis izomorfizmas organizacijose gali atsirasti dėl profesionalizacijos proceso, specializacijos ir sudėtingų profesinių standartų svarbos (Ali ir Frynas, 2018). Šis mechanizmas akcentuoja moralinį legitimacijos aspektą, reiškiantį pageidaujamą ar tinkamą elgesį (Kasperavičiūtė-Černiauskienė, 2014). Jeigu priverstinis arba reguliacinis izomorfizmas reiškiasi per poveikį iš išorės, remiantis normatyviniu izomorfizmu lemiamą vaidmenį atlieka vidiniai reiškiniai organizacijoje.

Technologijos vaidina tam tikrą vaidmenį mažinant socialinės inžinerijos išpuolių poveikį, tačiau pažeidžiamumas priklauso nuo žmogaus elgesio – impulsų ir psichologinių polinkių. Nors literatūra remia psichologinio jautrumo riziką socialinės inžinerijos išpuoliams, investicijos į organizacinio švietimo kampanijas suteikia optimizmo, kad socialinės inžinerijos išpuolius galima sumažinti (Conteh ir Schmick, 2016). Pagrindinis dėmesys turėtų būti skiriamas saugumo supratimui ir įmonės darbuotojų mokymui (O'Hanley ir Tiller, 2013). Didžiausią dalį kibernetinio saugumo situacijos gerinimo veiksnių apima profesinis žinojimas. Galima daryti prielaidą, kad šiuo metu būtent šis elementas yra vienas aktualiausių viešojo sektoriaus organizacijose (Grincevičius, 2019). Rezultatai rodo, kad supratimas apie socialinę inžineriją yra teigiamas saugumo apsaugos praktikos numatytojas. Taigi, siekdami sumažinti socialinės inžinerijos išpuolių galimų padarinių tikimybę, organizacijos turėtų ne tik stengtis stiprinti darbuotojų žinias apie saugumą, bet ir investuoti į darbuotojų supratimo apie socialinę inžineriją didinimą (Aldawood et al., 2020). Normatyvinis izomorfizmas, paremtas profesionalų žiniomis gali padėti įveikti socialinės inžinerijos keliamus iššūkius organizacijoms tikslingai vykdomų mokymų dėka.

Trečiasis institucinio izomorfizmo mechanizmas – mimetizmas. Remiantis šia izomorfizmo forma, galima teigti, jog ilgainiui organizacijos keičiasi, kad taptų panašesnės į kitas organizacijas savo aplinkoje (Heather ir Haveman, 1993). Mimetizmas, tai kitų sėkmingų organizacijų veiklos, procesų ar strategijų atkartojimas. Mokslinėje literatūroje teigiama, jog atkartojamos tik sėkmingos organizacijos ar procesai. Socialinės inžinerijos nagrinėjimo atveju mimetizmas gali pasireikšti per jau išaiškintų kibernetinių nusikaltimų atvejų viešinimą ir sėkmingai taikomų praktikų atkartojimą.

Remiantis nacionalinio kibernetinio saugumo būklės ataskaita (2019), populiariausi socialinės inžinerijos metodais pagrįsti kibernetiniai incidentai pagal 2018 m. statistiką Lietuvoje buvo „phishing“ elektroniniu paštu, žinučių socialiniuose tinkluose siuntimas arba

naudotojų viliojimas į suklastotas interneto svetaines. Kibernetiniai nusikaltėliai šiais metodais dažnai siekia finansinės naudos. Ypač tokio pobūdžio kibernetinių incidentų padaugėja šventiniais periodais, kai naudotojai yra viliojami nuolaidomis, ir vertingai atrodančiais pasiūlymais ir pan. Dažnas atvejis, kai kibernetiniai nusikaltėliai, apsimesdami įmonių vadovais, prašo buhalterių atlikti pinigines perlaidas. Šidlauskas (2017) teigia, kad dažniausiai tokio pobūdžio atakos būna nukreiptos prieš bankų klientus, siekiant sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Sukčiai išsiunčia tūkstančius vienodo turinio žinučių ir tikisi, jog keli ar keliolika vartotojų „*užkibs ant kabliuko*“. Pavojaus signalai – beasmenė žinutė, žinutė iš paslaugų teikėjo kurio paslaugomis niekada nesinaudojote, laiške nurodytos neaiškios nuorodos ir (ar) prisegti neaiškūs priedai (failai), įtartinas el. pašto adresas, nenaudojamas „*https*“ protokolas, nerišlūs sakiniai ir gramatinės klaidos, keistos vizualinės detalės.

Perpratus tokio pobūdžio kibernetinių nusikaltimų veikimo ir įgyvendinimo principus aiškiai sumažėja jų rizika. Sėkmingai išaiškinus socialinės inžinerijos incidentų pobūdį galima parengti atitinkamas rekomendacijas-namų vartotojams ir organizacijoms bei tobulinti teisinę bazę. Remiantis mimetinio izomorfizmo mechanizmu galima pagerinti priverstinio arba reguliacinio bei normatyvinio izomorfizmo lemiamus aspektus.

IŠVADOS

Socialinės inžinerijos reiškinys mokslinėje literatūroje dar nėra plačiai išanalizuotas, tačiau augantis tokio pobūdžio kibernetinių nusikaltimų skaičius atkreipia vis didesnį mokslininkų teoretikų ir praktikų dėmesį. Socialinės inžinerijos incidentas, priklausomai nuo pogrupio ir poveikio kategorijos, gali būti priskiriamas nereikšmingam, vidutinio, didelio arba pavojingo svarbumo incidentui. Nevaldomas arba netinkamai valdomas, priklausomai nuo pogrupio ir poveikio kategorijos, nereikšmingas socialinės inžinerijos incidentas gali tapti vidutiniu, o vidutinis – dideliu arba pavojingu.

Straipsnyje atlikta analizė atskleidė, jog šiuo metu Lietuvoje socialinės inžinerijos institucinis izomorfizmas nukreiptas tik į techninius kibernetinį saugumą užtikrinančius veiksnius, o žmogiškajam faktoriui skiriama nepakankamai dėmesio. Kadangi socialinės inžinerijos keliami iššūkiai kompleksiniai ir dinamiški, jų žala tiesiogiai priklausoma nuo žmogaus pasirengimo tokios atakos atrėmimui.

Kibernetinio saugumo subjektai privalo laikytis atitinkamų teisinio reguliavimo procedūrų, už jų nesilaikymą numatyta administracinė atsakomybė. Augant socialinės inžinerijos rūšies kibernetiniams incidentams taip pat svarbu vadovautis gerąja praktika, kuri kartu su nacionalinės teisės aktais būtų įtvirtinta organizacijų kibernetinio saugumo politikoje, numatant aiškią kibernetinių incidentų valdymo procedūrą. NKSC teigia, kad organizacijos dažnai atitinka arba beveik atitinka *de jure* saugumo politikos kriterijų. Audituojami subjektai turi oficialiai apibrėžtus saugos procesus ir gaires, tačiau saugumo užtikrinimas dažnai laikomas biurokratine našta.

Nacionalinėje kibernetinio saugumo būklės ataskaitoje (2020) pateikiamos socialinės inžinerijos metodais pagrįstų kibernetinių incidentų grėsmių valdymo rekomendacijos nėra pakankamos. Siekiant įveikti socialinės inžinerijos keliamus iššūkius išauga darbuotojų švietimo kibernetinio saugumo tematika poreikis. Organizacijos be visų aukščiau išvardintų priemonių turėtų rengti mokymus ir šviesti darbuotojus apie kibernetinį saugumą. Taip pat kasmet atlikti rizikos vertinimą ir kartas nuo karto rengti pratybas, kurių tikslas būtų įvertinti organizacijos atsparumą kibernetinėms grėsmėms.

Lietuvoje veikiančioms organizacijos, pasitelkus institucinio izomorfizmo prielaidas, pravartu atsižvelgti į kitose šalyse taikomus būdus kovojant su kibernetinio saugumo, konkrečiai socialinės inžinerijos iššūkiais. Kovai su socialine inžinerija neįmanoma pasiūlyti universalaus sprendimo, todėl svarbiu tampa kompleksinis atsakas į šias grėsmes, apimantis nacionalinį reguliavimą, organizacijos vidaus politiką ir sėkmingų praktikų atkartojimą.

LITERATŪRA

1. Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), 1-19.
2. Aldawood, H., Alashoor, T., & Skinner, G. (2020). 'Does awareness of social engineering make employees more secure? *International Journal of Computer Applications*, *975*, 8887.
3. Ali, W. & Frynas , J. G.(2018) The Role of Normative CSR-Promoting Institutions in Stimulating CSR Disclosures in Developing Countries. Corporate Social Responsibility and Environmental Management, Vol. 25, pp. 373–390
4. Amor-Esteban, V., Garcıa-Sanchez, I.-M. & Galindo-Villardon, M.-P. (2018) Analysing the Effect of Legal System on Corporate Social Responsibility (CSR) at the Country Level, from a Multivariate Perspective. Soc Indic Res, Vol. 140, pp. 435–452
5. Anderson, R. (2008). *Security engineering*. John Wiley & Sons.
6. Andress, J. (2019). *Foundations of Information Security: A Straightforward Introduction*. San Francisco
7. Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6* (23), 31.

8. Dirgėla, R. (2007). *Žmogiškasis veiksnys informacijos sistemų apsaugoje: Magistro darbas*. Vilnius: Vilniaus universitetas.
9. Gibson, D. (2014). *Managing risk in information systems*. Jones & Bartlett Publishers.
10. Gobeo, A., Fowler, C., & Buchanan, W. J. (2018). *GDPR and Cyber Security for Business Information Systems*. River Publishers.
11. Grincevičius, R. (2019). *Kibernetinio saugumo valdymo gerinimas taikant atsparumo modelius organizacijose: Daktaro disertacija*. Vilnius: Mykolo Romerio universitetas.
12. Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102-113.
13. Heather, A. & Haveman, A. (1993) Follow the Leader: Mimetic Isomorphism and Entry Into New Markets. Administrative Science Quarterly, Vol. 38, No. 4 (Dec., 1993), pp. 593-627
14. Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009, August). Towards automating social engineering using social networking sites. *In 2009 International Conference on Computational Science and Engineering* (Vol. 3, pp. 117-124). IEEE.
15. Kamat, P., Gautam, A. S., Tavares, J., Mishra, B., Kumar, R., Zaman, N., & Khari, M. (2018). Recent trends in the era of cybercrime and the measures to control them. *Handbook of e-business security*, 243-258.
16. Kasperavičiūtė-Černiauskienė, R. (2014) *Pasirinkimas diegti kokybės vadybos priemones: ISO9001 standarto atvejis Lietuvos aukštojo mokslo ir studijų institucijose: daktaro disertacija*. – Vilnius: Mykolo Romerio universitetas, 264 p.
17. Kiškis, T. (2012). *Privatumo ir saugos lygio vertinimo interneto svetainėse metodo parengimas ir taikymas: Magistro darbas*. Kaunas: Kauno technologijos universitetas.
18. Krašto apsaugos ministerija ir „Kurk Lietuvai“. (2020) Kibernetinis saugumas ir verslas. Prieiga per internetą: https://www.nksc.lt/doc/Kibernetinio_saugumo_vadovas_verslui_2020.pdf
19. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, 22, 113-122.
20. Lietuvos Respublikos administracinių nusižengimų kodeksas. (2015). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/b8d908c0215b11e58a4198cd62929b7a/asr
21. Lietuvos Respublikos kibernetinio saugumo įstatymas. (2014). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr
22. Lietuvos Respublikos valstybės saugumo departamentas ir Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos (2020). Grėsmių nacionaliniam saugumui vertinimas. Prieiga per internetą: https://www.vsd.lt/wp-content/uploads/2020/02/2020-Gresmes-LT-.pdf
23. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“. (2018). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
24. Mikejan, J. (2017). *Socialinio tinklo vartotojų pažeidžiamumų tyrimas, naudojant socialinės inžinerijos metodus: Magistro darbas*. Vilnius: Vilniaus Gedimino technikos universitetas.
25. Nacionalinio kibernetinio saugumo būklės ataskaita už 2016 metus. (2017). Prieiga per internetą: https://www.nksc.lt/doc/nksc_metine_ataskaita_uz_2016.pdf
26. Nacionalinio kibernetinio saugumo būklės ataskaita už 2017 metus. (2018). Prieiga per internetą: https://www.nksc.lt/doc/NKSC_ataskaita_2017_lt.pdf
27. Nacionalinio kibernetinio saugumo būklės ataskaita už 2018 metus. (2019). Prieiga per internetą: https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf
28. Nacionalinio kibernetinio saugumo būklės ataskaita už 2019 metus. (2020). Prieiga per internetą: https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf

29. O'Hanley, R., & Tiller, J. S. (2013). Information Security Management Handbook, *Sixth Edition, Volume 7*. Auerbach Publications.
30. Panavas, S. (2020). *Šiuolaikinių kibernetinių nusikaltimų grėsmės prevencijos planas Generolo Jono Žemaičio Lietuvos karo akademijai: Bakalauro darbas*. Vilnius: Generolo Jono Žemaičio Lietuvos karo akademija.
31. Ponemon Institute, IBM Security (2019). Cost of a Data Breach Study 2019.
32. Purser, S. (2004). *A practical guide to managing information security*. Artech House.
33. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89.
34. Shimonski, R. (2016). *CEH v9: Certified Ethical Hacker Version 9 Study Guide* (Vol. 9). John Wiley & Sons.
35. Smith, K. (2015) *The Ultimate Hacking for Beginners*. Kevin Smith
36. Šidlauskas, A. (2017). *Vartotojų elektroninių duomenų apsaugos ypatumai: Magistro darbas*. Vilnius: Mykolo Romerio universitetas.
37. World Economic Forum. The Global Risks Report. (2020). Prieiga per internetą: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

CHALLENGES FOR CYBER SECURITY: SOCIAL ENGINEERING IN THE CONTEXT OF INSTITUTIONAL ISOMORPHISM

Aurimas Šidlauskas[1], Svajūnė Ungurytė-Ragauskienė[2]
Mykolas Romeris University

Summary

Cyber attacks are becoming more complex and sophisticated. More and more cyber incidents are based on manipulation of people and their weaknesses, the aim is to deceive information security systems, steal and seize confidential information. There has been an increase in the number of cyber incidents based on social engineering methods. Such statistics force organizations to respond to change and adapt to the prevailing institutional field, to improve the existing legal framework. The aim of the article is to present conclusions and recommendations for the improvement of cyber security regulation in the context of institutional isomorphism after analyzing the content of the concept of social engineering and the preconditions for the emergence of this type of cyber attacks and the regulation of cyber incident management in national law. The aim of the article is to analyze the content of the concept of social engineering and the preconditions for the occurrence of this type of cyber attacks and the regulation of cyber incident management in national law, to provide conclusions and recommendations for improving cyber security regulation in the context of institutional isomorphism. The analysis revealed that currently in Lithuania the institutional isomorphism of social engineering is focused only on the technical factors ensuring cyber security, and insufficient attention is paid to the human factor. In order to overcome the challenges posed by social engineering, the need to educate employees on cyber security is growing. Given the growth of social engineering cyber incidents, it is also important to follow good practices, which, together with national legislation, are enshrined in organizations' cyber security policies, with a clear cyber incident management procedure.

Keywords: Social engineering, cyber incidents, cyber security, institutional isomorphism.