ISSN 2029-1701
ISSN 2335-2035 (Online)

Mokslinių straipsnių rinkinys
VISUOMENĖS SAUGUMAS IR VIEŠOJI TVARKA
PUBLIC SECURITY AND PUBLIC ORDER
2015 (15)
Scientific

KRIMINALINIO PROFILIAVIMO PRITAIKYMO GALIMYBĖS NUSIKALTIMŲ ĮVYKDYTŲ ELEKTRONINĖJE ERDVĖJE TYRIMUI

Birutė Balsevičienė*, Laima Ruibytė**

Mykolo Romerio universiteto Viešojo saugumo fakulteto Humanitarinių mokslų katedra
Putvinskio g. 70, LT-44211 Kaunas
Telefonas (8~37) 30 36 65
El. paštas: laimaruibyte@mruni.eu; birutebalse@gmail.com

Anotacija. Straipsnyje analizuojamos kriminalinio profiliavimo panaudojimo galimybės tiriant nusikaltimus elektroninėje erdvėje, kadangi šių nusikaltimų skaičius kasmet[1] didėja. Kriminalinis profiliavimas tai - technika, kuria nustatomos, apibūdinamos pagrindinės nusikaltėlio asmenybės ir elgesio charakteristikos, remiantis nusikaltimo, kurį jis padarė, analize[2]. Kriminalinis profiliavimas turi remtis įrodymais grįstais metodais, o taip pat mokslinių tyrimų rezultatais. Nusikaltimai elektroninėje erdvėje tiriami naudojant panašias tyrimo technikas kaip ir tiriant kitokio pobūdžio nusikaltimus. Ir viena jų – kriminalinis profiliavimas. Pastaruoju metu dažniausiai naudojamos indukcinės ir dedukcinės kriminalinio profiliavimo technikos bei technikos, kurios įtraukia abu šiuos metodus. Kol kas nėra aiškių siūlymų, kaip naudoti šias dvi technikas kartu ir kaip jas taikyti nusikaltimų elektroninėje erdvėje tyrimui. Šiame straipsnyje teikiamas algoritmas gali būti naudingas tiek ankstyvose, tiek ir vėlesnėse tyrimo stadijose.

Pagrindinės sąvokos: Nusikaltėlio profilis, nusikaltimas elektroninėje erdvėje

ĮVADAS

Sparčiai augantis nusikaltimų internete skaičius skatina vis daugiau dėmesio skirti šiai problemai, ieškoti naujų būdų ir priemonių jos sprendimams. Vien tik per 2012 metus Jungtinių Amerikos valstijų Internetinių nusikaltimų centras (the Internet Crime Complaint Center (IC3)) pateikia duomenis apie tai, kad nusikaltimų elektroninėje erdvėje per pastaruosius vienerius metus išaugo 8,3 procentais.[3] Lietuvoje nusikaltimų įvykdytų elektroninėje erdvėje statistika nėra pateikiama. Kaip teigia Kalpokas (2012)[4], augantis interneto vartotojų skaičius per pastaruosius metus kai kurios šalyse padidėjo 1000 procentų. Vartotojų skaičiaus augimas lemia ir vis dažnėjančius nusikaltimus elektroninėje erdvėje. Internetiniai nusikaltimai kenkia ne tik pavieniams asmenims pažeidžiant jų teises ar orumą,

[1] Kalpokas, V., & Marcinauskaitė, R.Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos.* 2012, 77(2), p. 30-52.
[2] Douglas J. E., Ressler R.K., Burgess a. W., Hartman C.R. Criminal profiling from scene analysis. *Behavioral Sciences and the Law.* 1986, 4, p. 401-421.
[3] Annual Report. (2012). Internet Crime Report. Internet Crime Complaint Center (IC3), p. 4.
[4] Kalpokas, V., Marcinauskaitė, R. *supra* note 2, p. 30-52.

tačiau tai sukelia ir milžiniškus nuostolius. Pavyzdžiui, JAV šie nuostoliai siekia apie 525 milijonus dolerių per metus[5].

Svarbu atkreipti dėmesį į tai, kad nusikaltimas elektroninėje erdvėje kol kas neturi aiškaus apibrėžimo. Šio pobūdžio nusikaltimai yra dalis nusikaltimų, kurie priskiriami kompiuteriniams nusikaltimams[6]. Jungtinės Tautos apibrėžia nusikaltimą elektroninėje erdvėje kaip bet kokį nelegalų veiksmą, kuris yra įvykdomas kompiuterinėje sistemoje ar tinkle, įtraukiant ir tokius nusikaltimus kaip informacijos nutekinimas ir pan.[7,8]. Taip pat nusikaltimams elektroninėje erdvėje gali būti priskiriami bet kokie nusikalstami veiksmai, kurie atliekami panaudojant kompiuterį ar kitas informacines technologijas. Šiuo atveju technologijos gali būti tiek priemonė, tiek nusikaltimo objektas[9]. Mokslininkai ir praktikai nesutaria ne tik dėl paties nusikaltimo apibrėžimo, bet ir dėl jo priskyrimo kokiai nors kategorijai – vieni laikosi nuomonės, kad tai visiškai nauja nusikaltimų rūšis[10], tačiau kiti teigia, kad pakito tik nusikaltimų erdvė ir priemonės, o nusikaltimų pobūdis ir motyvacija išliko tokie patys (sukčiavimas, prievarta ir pan.)[11]. Teigiantys, kad tai kitokio pobūdžio nusikaltimai, kaip esminį šių nusikaltimų išskirtinį bruožą, laiko erdvės ir laiko apribojimų nebuvimą[12,13].

Nepaisant konkretaus apibrėžimo nebuvimo ir skirtingų bandymų aiškinti šių nusikaltimų pobūdį, nusikaltimai elektroninėje erdvėje turi motyvus, kaip ir bet kuris kitas nusikaltimas, todėl čia galima taikyti kriminalinio profiliavimo metodus. Jungtinių Tautų atlikto tyrimo duomenimis daugiau nei 80 proc. nusikaltimų atliekamų elektroninėje erdvėje yra susiję su gana organizuotomis veikomis, kuomet pirmiausiai užkrečiamas konkretus kompiuteris kenkėjiškomis programomis, kurių pagalba pavagiami asmeniniai ir finansiniai

[5] *Ibid.*, p.30-52
[6] Shinder, D., and Tittel, E. Scene of the cybercrime – computer forensics handbook, 1st edition. Syngress Publishing, 2002.
[7] *Ibid*., p.156.
[8] Warikoo, A. (2014). Proposed Methodology for Cyber Criminal Profiling. Information Security Journal: A Global Perspective. 2014, 23(4-6), p.172-178.
[9] *Ibid*., p.172-178.
[10] Capeller W. Not Such a Neat Net: Some Comments on Virtual Criminality. Social & Legal Studies. 2001, Nr. 10 (2), p. 229–242.
[11] Grabosky P. N. Virtual Criminality: Old Wine in New Bottles? Social & Legal Studies. 2001, 10 (2), p. 243–249
[12] *Ibid.*, p.243-249.
[13]Kalpokas, V., & Marcinauskaitė, R. Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos.* 2012, 77(2), 30-52.

duomenys, ir vėliau išgryninami pinigai[14]. Kaip jau minėta, nusikaltimai elektroninėje erdvėje pasižymi erdvės ir laiko nebuvimu, yra latentiški, todėl iškyla asmenų darančių tokius nusikaltimus identifikavimo problemos.

Elektroninėje erdvėje padaromų nusikaltimų profiliavimas - dar labai nauja mokslo ir praktikos šaka, todėl naudojantis juo galimi įvairūs netikslumai, klaidingos išvados ir interpretacijos, jeigu duomenims apdoroti, surinkti ir pateikti nėra naudojama tinkama mokslinė metodologija[15]. Iš to kyla standartizuotos metodologijos poreikis, kuri būtų naudojama kriminaliniam profiliavimui elektroninėje erdvėje. Standartizuota metodika gali tapti naudingu įrankių tiek moksliniams tyrimams, tiek ir praktikams.

Šio straipsnio tikslas – išanalizuoti asmenų, vykdančių nusikaltimus elektroninėje erdvėje, profiliavimo ypatumus, susisteminant esamus profiliavimo metodus, bei pateikti rekomendacijas, kurios galėtų būti naudingos specialistams dirbantiems su tokio pobūdžio nusikaltimais. **Straipsnio objektas** – profiliavimo metodų pritaikymas asmenų, vykdančių nusikaltimus elektroninėje erdvėje, profilio sudarymui. Iškeltam tikslui pasiekti naudojamas **mokslinės literatūros analizės metodas**. Straipsnyje aptariama: profiliavimo metodas, pagrindiniai jo tipai, metodo, skirto nusikaltėlių elektroninėje erdvėje profiliavimui, sudarymo principai bei rekomendacijos psichologams, kriminalistams, teisininkams ir kitų sričių specialistams dirbantiems elektroninių nusikaltimų tyrimų srityje.

Profiliavimas. Pagrindinis šio metodo naudojimo tiriant nusikaltimus tikslas yra susiaurinti potencialių įtariamųjų ratą ir įvertinti tikimybę, kad konkretus įtariamasis galėjo įvykdyti konkretų nusikaltimą. Kriminalinis profiliavimas yra mokslinė technika skirta įvertinti ir analizuoti nusikaltimo vietą (*angl. scene of crime*) ir dedukciniu būdu apibūdinti nusikaltėlio, kuris atliko šį nusikaltimą elgesio ypatumus[16,17]. Sudarytas nusikaltėlio profilis dažniausiai apibrėžia įvairias nusikaltėlio charakteristikas, kuriomis dažniausiai pasižymi tokio pobūdžio nusikaltimus atliekantys asmenys[18,19]. Profiliavimo metodai dažniausiai remiasi dvejomis prielaidomis:

- nusikaltėlis elgsis panašiai atlikdamas visus savo nusikaltimus,

[14]Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., and Ignatuschtschenko, E. Comprehensive study on cybercrime. United Nations Office on Drugs and Crime. 2013, p. 38–39.
[15] Broucek, V., and Turner, P. Winning the battles, losing the war? Rethinking methodology for forensic computing research. *Journal in Computer Virology*. 2006, p. 3–12.
[16] Kirwan, G., and Power, A. The psychology of cybercrime, 1st edition. IGI Global, 2011.
[17] Bloom, R. Foundations of Psychological Profiling: Terrorism, Espionage, and Deception. Crc Press, 2013.
[18] Shinder, D. & Tittel, E., *supra* note 4.
[19] Bloom, R., *supra* note 14.

- panašūs nusikaltimai yra įvykdomi panašiomis charakteristikomis pasižyminčių asmenų.

Taigi, šiuolaikinėje kriminalistikoje yra taikomi du pagrindiniai kriminalinio profiliavimo metodai– *dedukcinis ir indukcinis*. Indukcinis metodas dažniausiai taikomas naudojantis duomenų bazėmis, kuriose jau yra surinkti duomenys apie nusikaltėlius įvykdžiusius tokio tipo nusikaltimus. Profiliuotojas analizuoja duomenis, ieško panašumų ir iš to daro išvadas apie galimas nusikaltėlio charakteristikas [20]. Dedukcinis profiliavimas skiriasi tuo, kad pirmiausiai analizuojami konkretaus nusikaltimo įkalčiai ir auka tam, kad nustatyti galimus nusikaltimo motyvus ir iš to daryti išvadas apie numanomus nusikaltėlio bruožus[21]. Nors kai kurie autoriai kritikuoja abu šiuos metodus, teigdami, kad jų efektyvumas nėra pakankamai įrodytas moksliniais tyrimais[22], tačiau dauguma praktikų ir mokslininkų pripažįsta, kad tai yra vienas iš būdų galinčių padėti tiriant nusikaltimus[23,24].

Svarbi abiejų metodų naudojamos informacijos dalis yra viktimologija. Kalbant apie nusikaltimus elektroninėje erdvėje, nusikaltimai pagal tai, kas buvo auka ir koks motyvas, gali būti skirstomi į penkias pagrindines grupes[25]: a) nusikaltimai, kurie įvykdyti dėl to, kad nustatyti/išgauti tam tikrus duomenis (dažniausiai tam, kad perduoti rastą informaciją trečiosioms šalims); b) nusikaltimai, kurie įvykdyti dėl emocinių priežasčių (persekiojimas aukos elektroninėje erdvėje); c) nusikaltimai, kurių pagrindinis motyvas kyla iš seksualinių impulsų (pedofilija ir pan.); d) politiniai motyvai; e) nusikaltimai, kurie nėra itin pavojingi kitiems (pvz.: filmų vagystės nepaisant autorinių teisių pažeidimo ir pan.).

Kriminalinis nusikaltimų elektroninėje erdvėje profiliavimas. Viena iš svarbiausių šio metodo užduočių išskirti konkretų nusikaltimą padariusį asmenį iš daugelio asmenų ir tokiu būdu susiaurinti galimų įtariamųjų ratą[26]. Pastaruoju metu kylanti diskusija dėl

[20] Bloom, R., *supra* note 14.
[21] Tennakoon, H (2011). The need for a comprehensive methodology for profiling cyber-criminals. New Security Learning. [interaktyvus] [žiūrėta 2015-09-25].<www. newsecuritylearning.com>.
[22] Snook, B., Cullen, R., Bennell, C., Taylor, P. J., & Gendreau, P. The criminal profiling illusion: What's behind the smoke and mirrors? *Criminal Justice and Behavior*. 2008, *35*, p. 1257–1276.
[23] Scott, D., Lambie, I., Henwood, D., & Lamb, R. Profiling stranger rapists: Linking offence behaviour to previous criminal histories using a regression model. *Journal of sexual aggression*. 2006, 12(3), p. 265-275.
[24] Bloom, R. *supra* note 14.
[25] Shinder, D. (2010) Profiling and categorizing cybercriminals. [interaktyvus] [žiūrėta 2015-09-25]. <http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069 >.
[26] Jahankhani, H., and Al-Nemrat, A. Examination of cybercriminal behavior. *International Journal of Information Science and Management.* 2010, p. 41–48.

kriminalinio profiliavimo patikimumo[27,28], skatina naudojantis šiuo metodu laikytis gana griežtų numatytų taisyklių ir standartizuotų metodų. Kriminalinis nusikaltimų elektroninėje erdvėje profiliavimas turi remtis panašiais principais kaip ir kitų nusikaltimų profiliavimas, tačiau nusikaltimų atliktų elektroninėje erdvėje tyrimas vis dėl to kelia ir kitokius iššūkius tyrėjams. Vienas iš jų – tas, kad nusikaltimą įvykdęs asmuo gali gyventi visiškai kitame žemyne nei tyrėjas. Tiriant tokio pobūdžio nusikaltimus reikalingos ne tik kriminologijos, psichologijos žinios, bet taip pat ir žinios susijusios su techniniais elektroninės erdvės ypatumais.

Psichologai, dalyvaujantys tiriant įvairius nusikaltimus, dažnai naudoja nusikaltėlio profilio sudarymo metodiką, kuri pritaikoma ir tiriant nusikaltimus elektroninėje erdvėje. Viena iš dažniausiai naudojamų Federalinio Tyrimo biuro profiliavimo technikų yra induktyvus (*angl. inductive*) profiliavimas[29]. Šis metodas naudoja duomenų surinkimo technikas, kurios padeda aptikti tam tikrą nusikaltėlio braižą, o taip pat naudoja duomenis, kurie jau surinkti apie tam tikrų asmenybės tipų ar elgesio profilius, kurie būdingi būtent tokio tipo nusikaltimams[30].

Užsienio šalyse mokslininkai kuria ir duomenų bazes, kuriose renkami duomenys apie dažniausiai pasitaikančius, labiausiai būdingus asmenų vykdančių nusikaltimus elektroninėje erdvėje bruožus ir daromus nusikaltimus. Dažniausiai į šias duomenų bazėse yra įtraukiami tokie duomenys, kaip demografiniai rodikliai, socioekonominis statusas, socialiniai santykiai ir psichologiniai bruožai[31]. Kirwan ir Power (2011) kelia klausimą, ar asmenys, kurie rašo virusines programas gali būti, kad pasižymi tais pačiais ar panašiais asmenybės bruožais. Vis dėl to iš jau turimų duomenų galima kelti prielaidą, kad ir asmenys, kurie įvykdo nusikaltimus elektroninėje erdvėje, pasižymi tam tikromis charakteristikomis, kurias galima grupuoti ir analizuoti[32]. Tarkime, autoriai skiria, programišius (*angl. hacker*) ir virusinių programų programuotojus. Nes atlikti įsilaužimą reikia įvairių sisteminių ir panašių žinių, kurios tuo pačiu atskleidžia ir to asmens išsilavinimo, gebėjimų lygmenį, kai tuo tarpu tik

[27] Kocsis, R. N. Applied criminal psychology: An introduction to forensic behavioral sciences. Springfield, IL: CC Thomas, 2009.
[28] Kocsis, R. N., Middledorp, J., Karpin, A. Taking stock of accuracy in criminal profiling: The theoretical quandary for investigative psychology. *Journal of Forensic Psychology Practice*. 2008, *8*(3), p. 244–261.
[29] Jahankhani, H. & Al-Nemrat, A., *supra* note 23, p. 41–48.
[30] Wheelbarger, S (2009). CyberForensics. Criminal justice collaboratory. Colby Community College. [interaktyvus] [žiūrėta 2015-09-25].<www.colbycriminaljustice.wikidot.com/cyberforensics>.
[31] Kirwan, G. & Power, A., *supra* note 13.
[32] Nykodym, N., Taylor, R. and Vilela, J. Criminal profiling and insider cybercrime, Computer Law & Security Report. 2005, 21 (5), p. 408-414.

programavimas laikomas kur kas mažiau norinčios atkreipti į save dėmesį asmenybės veikla. Tačiau šių autorių sudaromos duomenų bazės labiau remiasi savižinos klausimynais, nei pačių hakerių ar nusikaltėlių atliekamais veiksmais. Donato (2009)[33] siūlo, kaip pagerinti nusikaltimų atliekamų elektroninėje erdvėje ištyrimą. Šioje metodikoje esminis principas yra nustatyti asmens, kuris atakuoja elektroninę erdvę, įgūdžių lygį, pobūdį, ir tuo remiantis daryti išvadas apie jo psichologines charakteristikas. Šioje metodikoje nesiremiama demografiniais duomenimis ar ankstesniais sudarytais nusikaltėlių profiliais. Viena iš pagrindinių priežasčių, kodėl tai gali būti tinkamesnė technika tiriant nusikaltimus elektroninėje erdvėje, yra spartūs informacinių technologijų pokyčiai. Tačiau, kaip teigia Warikoo[34], remiantis tik indukciniu metodu, atmetama didelė informacijos dalis, ir tyrėjams, kurie skiriasi įgūdžių, gebėjimų ir žinių lygiu tenka naudotis tik mažai apčiuopiamais spėjimais, todėl reikėtų abu šiuos metodus integruoti.

Metodas. Atsižvelgiant į anksčiau išsakytus teorinius ir praktinius abiejų dabar naudojamų profiliavimo metodų ypatumus, Warikoo[35] siūlo integruoti šių abiejų metodų principus nusikaltėlių, kurie įvykdo nusikaltimus elektroninėje erdvėje profiliavimui. Pirminis šio metodo etapas yra dedukcinis, o statistinė analizė yra atliekama vėliau tam, kad būtų identifikuoti bendri modeliai ir charakteristikos. Skaitmeniniai nusikaltimo duomenys patys savaime pateikia tam tikras užuominas apie užpuolėją. Pagal skaitmeninius duomenis galima daryti prielaidas apie užpuolėjo išsilavinimą, motyvaciją, naudojamus įrankius bei jo pažeidžiamas vietas[36]. Nusikaltėliai, kurie vykdo nusikaltimus elektroninėje erdvėje, taip pat, kaip ir tradicinių nusikaltimų atveju, turi savo veikimo modelius, kurie kartojasi kiekvieno nusikaltimo metu[37].

Warikoo[38] siūloma metodika turi šešis profilio identifikavimo požymius (Profile Identification Metrics):

1. **Atakos parašas** – analizuojami įrankiai, kurie buvo panaudoti atakos metu. Patariama analizuoti skaitmeninius įkalčius, kurie padėtų surinkti informaciją apie atakos pobūdį. Tarkime analizuojamos, taip vadinamos, nulinės dienos atakos (*angl. zero days*

[33]Donato, L. An introduction to how criminal profiling could be used as a support for computer hacking investigations. Journal of Digital Forensic Practice. 2009, 2, p. 183–195.
[34] Warikoo, A. *supra* note 6, p. 172-178.
[35] Warikoo, A. *supra* note 6, p. 172-178.
[36]Kwan, L., Ray, P., and Stephens, G. Towards a methodology for profiling cyber criminals. IEEE Computer Society. Proceedings of the 41st Hawaii International Conference on System Sciences. 2008, p. 3–5.
[37] Shinder, D. & Tittel, E. ., *supra* note 4.
[38] Warikoo, A., *supra* note 6, p. 172-178.

attack) - kai sistemos (pvz.: Windows) saugumo spragos dar nespėjo pastebėti kūrėjai, o nusikaltėliai pastebėję ją, pasinaudoja tuo nusikaltimui įvykdyti. Jei įkalčiai leidžia daryti prielaidą apie nulinės dienos ataką, tai galima toliau daryti prielaidą apie tai, kad skaitmeninis kodas buvo sukurtas būtent tai atakai.

2**. Atakos metodas** - koks metodas buvo naudojamas atakos metu. Socialinės inžinerijos, kenkėjiškos programos, kompiuterinės atakos, kai interneto serveris atakuojamas daugybe užklausų iš skirtingų vietų ir dėl staigaus apkrovimo padidėjimo serveris išeina iš rikiuotės, nebegali atsakyti į tikras užklausas (*angl. DdoS*), brukalų siuntimas ir bandymai išvilioti asmeninius duomenis yra dažniausi metodai naudojami nusikaltėlių, kurie vykdo nusikaltimus elektroninėje erdvėje.

3**. Motyvacijos lygis** – pagrindinis būdas nustatyti nusikaltėlio elgesio ypatumus. Remiamasi atakos kompleksiškumo nustatymu. Ataka, kuri yra kompleksiška rodo, kad pats užpuolėjas turi gebėti pastebėti įvairius pažeidžiamumus sistemose ir dažniausiai tai leidžia daryti prielaidą apie aukštą nusikaltėlio motyvaciją. Dažniausiai šie nusikaltėliai yra mėgstantys rizikuoti ir yra gana atkaklūs. Dažniausiai nusikaltėlis, kuris turi vidutinio lygio motyvaciją, atlieka vieną, dvi atakas, tačiau nėra toks atkaklus.

4. **Gebėjimų faktorius** – pagal tai, kokius įrankius ir metodikas užpuolėjas naudoja, galima spręsti apie jo gebėjimus bei resursus. Tarkime, mažai pažengę užpuolėjai naudoja laisvai prieinamus kodus ir įrankius. pažengęs užpuolėjas dažniausiai naudoja jo paties sukurtus ir pakeistus kodus, bei nulinės dienos ataką (*angl. zero days exploits*).

5. **Atakos dydis/apimtis/poveikis** – kokio lygmens nuostoliai, kuriuos sukėlė ataka. Klasifikuojama dažniausiai pagal tokius principus: maža (nėra apčiuopiamos žalos įmonei/nukentėjusiajam), vidutinė (vidutinio dydžio žala), didelė (turi didelės žalos veiklai) ir kritinė (įmonė subankrutuoja patyrusi ataką).

6. **Demografiniai duomenys.** Geografinė padėtis yra viena iš svarbiausių aspektų profilio sudaryme. Dažnai egzistuojantys ir dažniausiai naudojami kitokios rūšies nusikaltimų profiliavimo metodai nedaug remiasi geografiniu profiliavimu [39]. Tačiau duomenys rodo, kad dažniausiai tam tikro tipo nusikaltimai netgi elektroninėje erdvėje yra atliekami iš tam tikrų šalių. Tarkime, dažniausiai nusikaltimai susiję su šnipinėjimu elektroninėje erdvėje yra atliekami iš Kinijos.

[39] Tompsett, B. C., Marshall, A. M., and Semmens, N. C. Cybrprofiling: Offender profiling and geographic profiling of crime on the Internet. Computer Network Forensics Research Workshop, 2005, p. 1.

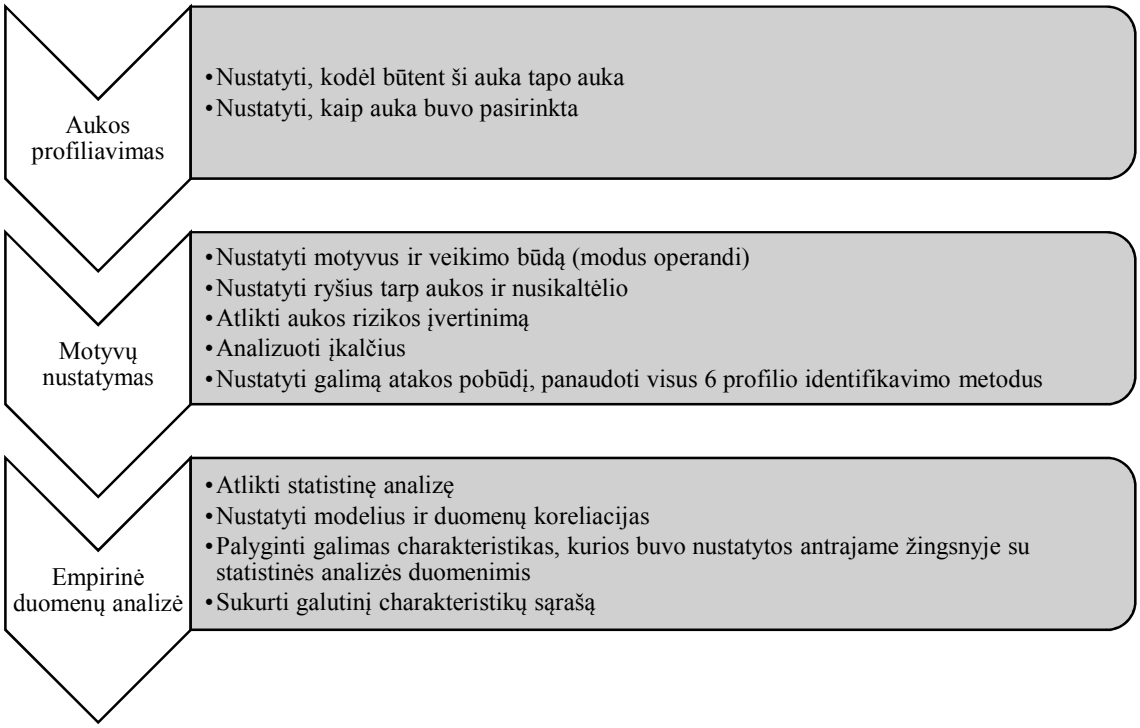
Siūloma metodologija susideda iš 4 etapų (1 pav.):

1**. Aukos profiliavimas**. Nustatyti įvairias aukos – asmens ar įstaigos – charakteristikas.

2. **Motyvų nustatymas.** Motyvas yra gana glaudžiai susijęs su auka. Tarkime, jei auka yra valstybinė įstaiga gali būti, kad tai labiau susiję su politiniais motyvais nei su finansine nauda. Šiame etape taip pat yra analizuojami skaitmeniniai nusikaltimo įkalčiai.

3**. Empirinė duomenų analizė**. Atliekant statistinę analizę ieškoma tendencijų, kurios padėtų nustatyti nusikaltėlio elgesį ir savybes.

4. **Galutinis profilio sudarymas**. Remiantis ankstesnėse stadijose gautais duomenimis sudaromas nusikaltėlio portretas.



1 pav. Nusikaltėlio profilio sudarymo metodikos etapai (pgl. A. Warikoo, 2014)

Nusikaltėliai, kurie vykdo nusikaltimus elektroninėje erdvėje yra klasifikuojami į 6 pagrindinius tipus (1 lentelė):

1. **Politiškai aktyvūs programišiai** yra politiškai motyvuoti ir jų taikinys yra valstybinės įstaigos. Jų įsilaužimų elektroninėje erdvėje pagrindiniai motyvai yra pranešti kažkokią žinią susijusią su politika. Dauguma jų nėra organizuoti, naudojasi laisvai

prieinamais įrankiais[40]. Jų gebėjimų ir įgūdžių lygis dažniausiai svyruoja nuo bazinio lygmens iki vidutinio.

2. **Kibernetinės erdvės nusikaltėliai** (*angl. cyber criminals*) – dažniausiai esminis veikimo tikslas yra finansinė nauda. Dažnai yra gana organizuoti ir gebėjimai svyruoja nuo bazinio lygmens vartotojo iki vidutinio.

3. **Kibernetinės erdvės sindikatai** – gerai organizuotos, turinčios ir gana didelių finansinių išteklių, kurias valdo dažniausiai kriminalinės organizacijos. Dažniausiai jie pavagia itin dideles pinigų sumas iš verslo organizacijų ir vartotojų, perka ir parduoda privačią informaciją ir intelektinę nuosavybę, vysto įvairius įrankius skirtus atakoms, nulinės dienos atakos kodus (*angl. zero day exploit code*), kenkėjiškų programų kodus ir pan.[41].

4. **Šnipai elektroninėje erdvėje**. Dažniausiai remiami valstybės ir turi didelius išteklius. Jų pagrindinė motyvacija yra šnipinėjimas ir IP (*angl. Internet Protokol*)* vagystės. Dažniausi jų taikiniais yra valstybinės įstaigos ir įstaigos, kurios naudojasi jautria informacija. Dažniausiai tai itin aukštus gebėjimus turintys asmenys, kurie kuria naujus kodus, įtraukiančius ankstesnių programų pažeidžiamas vietas. Naudoja įvairias aukšto lygio technikas tam, kad nebūtų susekti.

5**. Naujokai**. Turi tik bazinius įgūdžius ir naudojasi tik laisvai prieinamais įrankiais. Dažniausiai nusikaltimus elektroninėje erdvėje vykdo dėl to, kad tai smagu ar dėl pramogos.

6. **Kibernetiniai teroristai**. Turi gerus išteklius. organizuota, įsitraukusi į pirmojo tipo nusikaltimus ir kriminalines veikas[42].

Nors nusikaltimų ir elektroninėje erdvėje daugėja ir Lietuvoje, tačiau kol kas žengiami tik pirmieji žingsniai šių veikų kriminalizavimui[43]. Taip pat skirtingose šalyse yra skirtingos bausmės už atitinkamas veikas, kas leidžia dažniau vykdyti nusikaltimus tose šalyse, kuriose šios bausmės yra mažesnės[44].

[40] Nachreiner, C. (2013). Profiling modern hacktivists, criminals and cyber spies. Watchguard Security Center. [interaktyvus] [žiūrėta 2015-09-25].<www.watchguardsecuritycenter.com>
*IP adresas yra – kompiuterio identifikatorius IP tinkluose. Tai tam tikrame tinkle unikalus skaičius, naudojamas vienareikšmei duomenų paketo siuntėjo ir gavėjo identifikacijai ir skiriamas žmogaus ar organizacijos, administruojančios duotąjį IP tinklą.
[41] Nachreiner, C., *supra* note 40.
[42] Bednarz, A. (2004). Profiling cybercriminals: A promising but immature science. Networkworld. [interaktyvus] [žiūrėta 2015-09-25]. <http://www.networkworld.com>.
[43] Štitilis, D., Pakutinskas, P., Dauparaitė, I., & Laurinaitis, M. (2011). Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai. *Socialinių mokslų studijos.* 2011, (3), 1, p. 153-171.
[44] *Ibid.,* p. 153-171.

1 lentelė. Nusikaltėlių elektroninėje erdvėje profiliai ir jų ypatumai (pgl. A. Warikoo, 2014)

Nusikaltėlio elektroninėje erdvėje profilis	Motyvas	Organizuotumo lygmuo	Motyvacijos lygmuo	Gebėjimų lygis	Atakos apimtis	Atakos metodas
Politiškai motyvuoti programišiai	Politiniai motyvai	Neorganizuoti	Aukštas	Bazinis-vidutinis	Maža - vidutinė	Tapatybės vagystės (angl. phishing); brukalų siuntimas, DdoS*
Kibernetinės erdvės nusikaltėliai	Finansinė nauda	Neorganizuoti, bet pasitaiko tam tikro lygmens bendradarbiavimo	Vidutinis	Vidutinis	Vidutinė - didelė	Brukalų siuntimas, kenkėjiškos programos
Kibernetinės erdvės sindikatai	Finansinė nauda	Organizuoti, gerai finansuojami	Aukštas	Vidutinis – pažengęs vartotojas	Didelė	Kenkėjiškos programos prieinamos juodojoje rinkoje
Šnipai elektroninėje erdvėje	Šnipinėjimas; IP vagystė	Remiami valstybės, itin organizuoti	Aukštas	Aukštas, pažengęs vartotojas	Kritinė	Modifikuoti kodai, nulinės dienos atakos
Naujokai	Smagumas	Neorganizuoti	Žemas	Bazinis	Maža - vidutinė	Laisvai prieinami įrankiai
Kibernetiniai teroristai	Žlugdymas, terorizmas	Gerai finansuojami; dirba mažuose pogrupiuose	Vidutinis	Bazinis - aukštas	Retai - vidutiniškai	DdoS*

* DdoS (*angl. distributed denial of service)*– kompiuterinio nusikaltimo rūšis, kuomet sukurtos kenkėjiškos programos atakuoja serverį daugybe užklausų iš skirtingų vietų ir dėl staigaus apkrovimo padidėjimo serveris išeina iš rikiuotės, nebegali atsakyti į tikras užklausas.

Lietuvoje kol kas sunku tikėtis, kaip teigia Juškevičiūtė [45], kad būtų įkurta atskira tarnyba, kurioje dirbtų keletas psichologų, turinčių pasirengimą profesionaliai sudaryti nusikaltėlio profilius, tačiau straipsnyje pateikiamos gairės ir siūloma metodika gali būti naudinga tiek teisininkams ar kriminalistams, tiek ir psichologams, kurie dirba komandoje kartu su policijos pareigūnais. Nusikaltėlio profilio sudarymas nėra metodas, kuris skirtas nustatyti konkretų nusikaltėlį. Dažniausiai nusikaltėlio profilis gali ir veikia labiau kaip gairės, moksliškai pagrįstas būdas susiaurinti nusikaltimu įtarimų asmenų skaičių. Nusikaltimai elektroninėje erdvėje turi tik jiems būdingus ypatumus ir aspektus, tačiau dažnai

[45] Juškevičiūtė J. Nusikaltėlio profilio sudarymas – naujas netradicinis nusikaltimų tyrimo metodas. *Jurisprudencija.* 2003, 43 (35), p. 17-25.

yra skatinami panašių motyvų, kurie būdingi ir nusikaltimams realioje erdvėje. Tiriantiems nusikaltimus elektroninėje erdvėje ir sudarinėjant nusikaltėlio profilį reikia ne tik psichologijos žinių, bet ir išmanymo apie informacinių technologijų veikimo principus bei komandos, kurioje dirbtų visi šie specialistai.

IŠVADOS

Apžvelgus mokslinės literatūros šaltinius galima teigti, kad nusikaltimas elektroninėje erdvėje kol kas neturi aiškaus apibrėžimo. Nusikaltimas elektroninėje erdvėje suprantamas, kaip bet koks nelegalus veiksmas, kuris yra įvykdomas kompiuterinėje sistemoje ar tinkle, įtraukiant ir tokius nusikaltimus, kaip informacijos nutekinimas ir pan. Taip pat nusikaltimams elektroninėje erdvėje gali būti priskiriami bet kokie nusikalstami veiksmai, kurie atliekami panaudojant kompiuterį ar kitas informacines technologijas.

Nepaisant konkretaus apibrėžimo nebuvimo ir skirtingų bandymų aiškinti šių nusikaltimų pobūdį, nusikaltimai elektroninėje erdvėje turi motyvus, veikimo būdus, kaip ir bet kuris kitas nusikaltimas, todėl aiškinant juos galima taikyti kriminalinio profiliavimo metodus.

Nusikaltimai elektroninėje erdvėje pasižymi erdvės ir laiko nebuvimu, yra latentiški, todėl iškyla asmenų darančių tokius nusikaltimus identifikavimo problemos. Iš to seka standartizuotos metodologijos poreikis, kuri būtų naudojama kriminaliniam profiliavimui elektroninėje erdvėje.

Kriminalinis nusikaltimų elektroninėje erdvėje profiliavimas turi remtis panašiais principais kaip ir kitų nusikaltimų profiliavimas, tačiau nusikaltimų atliktų elektroninėje erdvėje tyrimas vis dėl to kelia ir kitokius iššūkius tyrėjams. Tiriant tokio pobūdžio nusikaltimus reikalingos ne tik kriminologijos, psichologijos žinios, bet taip pat ir žinios susijusios su techniniais elektroninės erdvės ypatumais.

Asmenys, kurie įvykdo nusikaltimus elektroninėje erdvėje, pasižymi tam tikromis charakteristikomis, kurias galima grupuoti ir analizuoti. A.Warikoo (2014) siūlo integruoti indukcinio ir dedukcinio profiliavimo metodų principus nusikaltėlių, kurie įvykdo nusikaltimus elektroninėje erdvėje, profiliavimui. Pirminis šio metodo etapas yra dedukcinis, o statistinė analizė yra atliekama vėliau tam, kad būtų identifikuoti bendri modeliai ir charakteristikos. Warikoo siūloma metodologija susideda iš 4 etapų: aukos profiliavimas; motyvų nustatymas; empirinė duomenų analizė; galutinis profilio sudarymas. Taip pat jis

siūlo šešis profilio identifikavimo požymius: atakos parašas, atakos metodas, motyvacijos lygis, gebėjimų faktorius, atakos dydis/apimtis/poveikis, demografiniai duomenys.

Nors nusikaltimų ir elektroninėje erdvėje daugėja ir Lietuvoje, tačiau kol kas žengiami tik pirmieji žingsniai šių veikų kriminalizavimui. Nusikaltėlio profilio sudarymas nėra metodas, kuris skirtas nustatyti konkretų nusikaltėlį. Dažniausiai nusikaltėlio profilis gali ir veikia labiau kaip gairės, moksliškai pagrįstas būdas susiaurinti nusikaltimu įtarimų asmenų skaičių.

Tiriantiems nusikaltimus elektroninėje erdvėje ir sudarinėjant nusikaltėlio profilį reikia ne tik psichologijos žinių, bet ir išmanymo apie informacinių technologijų veikimo principus bei komandos, kurioje dirbtų visi šie specialistai.

LITERATŪRA

1. Annual Report. (2012). Internet Crime Report. Internet Crime Complaint Center (IC3), p. 4.
2. Bednarz, A. (2004). Profiling cybercriminals: A promising but immature science. Networkworld. [interaktyvus] [žiūrėta 2015-09-25]. <http://www.networkworld.com>.
3. Bloom, R. Foundations of Psychological Profiling: Terrorism, Espionage, and Deception. Crc Press, 2013.
4. Broucek, V., and Turner, P. (2006). Winning the battles, losing the war? Rethinking methodology for forensic computing research. *Journal in Computer Virology*, 3–12.
5. Capeller W. Not Such a Neat Net: Some Comments on Virtual Criminality. *Social & Legal Studies.* 2001, Nr. 10 (2), p. 229–242.
6. Donato, L. An introduction to how criminal profiling could be used as a support for computer hacking investigations. *Journal of Digital Forensic Practice.* 2009, 2, p. 183–195.
7. Douglas J. E., Ressler R.K., Burgess a. W., Hartman C.R. Criminal profiling from scene analysis. *Behavioral Sciences and the Law*. 1986, 4, p. 401-421.
8. Grabosky P. N. Virtual Criminality: Old Wine in New Botles?. *Social & Legal Studies*. 2001, 10 (2), p. 243–249.
9. Jahankhani, H., and Al-Nemrat, A. Examination of cybercriminal behavior. *International Journal of Information Science and Management.* 2001, p. 41–48.
10. Juškevičiūtė J. Nusikaltėlio profilio sudarymas – naujas netradicinis nusikaltimų tyrimo metodas. *Jurisprudencija.* 2003, 43 (35), p. 17-25.
11. Kalpokas, V. Nusikaltimai elektroninėje erdvėje: kriminologinės sampratos dilemos. *Teisės problemos.* 2009, 63(1), p. 75-87.
12. Kalpokas, V., & Marcinauskaitė, R.Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos.* 2012, 77(2), p. 30-52.
13. Kirwan, G., and Power, A. The psychology of cybercrime, 1st edition. IGI Global, 2011.
14. Kocsis, R. N. Applied criminal psychology: An introduction to forensic behavioral sciences. Springfield, IL: CC Thomas, 2009.
15. Kocsis, R. N., Middledorp, J., & Karpin, A. Taking stock of accuracy in criminal profiling: The theoretical quandary for investigative psychology. *Journal of Forensic Psychology Practice*. 2008, *8*(3), p. 244–261.

16. Kwan, L., Ray, P., and Stephens, G. Towards a methodology for profiling cyber criminals. *IEEE Computer Society. Proceedings of the 41st Hawaii International Conference on System Sciences*. 2008, p. 3–5.
17. Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., and Ignatuschtschenko, E. Comprehensive study on cybercrime. United Nations Office on Drugs and Crime. 2013, p.38-39.
18. Nachreiner, C. (2013). Profiling modern hacktivists, criminals and cyber spies. Watchguard Security Center. [interaktyvus] [žiūrėta 2015-09-25].<www.watchguardsecuritycenter.com>.
19. Nykodym, N., Taylor, R. and Vilela, J. Criminal profiling and insider cybercrime, *Computer Law & Security Report*. 2005, 21 (5), p. 408-414
20. Scott, D., Lambie, I., Henwood, D., & Lamb, R. Profiling stranger rapists: Linking offence behaviour to previous criminal histories using a regression model. *Journal of sexual aggression.* 2006, 12(3), p.265-275.
21. Shinder, D. (2010) Profiling and categorizing cybercriminals. [interaktyvus] [žiūrėta 2015-09-25]. <http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069 >.
22. Shinder, D., and Tittel, E. Scene of the cybercrime – computer forensics handbook, 1st edition. Syngress Publishing, 2002.
23. Snook, B., Cullen, R., Bennell, C., Taylor, P. J., & Gendreau, P. The criminal profiling illusion: What's behind the smoke and mirrors? *Criminal Justice and Behavior*. 2008, *35*, p. 1257–1276.
24. Štitilis, D., Pakutinskas, P., Dauparaitė, I., & Laurinaitis, M. (2011). Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai. Socialinių mokslų studijos. 2011, (3), 1, p. 153-171.
25. Tennakoon, H (2011). The need for a comprehensive methodology for profiling cyber-criminals. New Security Learning. [interaktyvus] [žiūrėta 2015-09-25].<www. newsecuritylearning.com>.
26. Tompsett, B. C., Marshall, A. M., and Semmens, N. C. Cybrprofiling: Offender profiling and geographic profiling of crime on the Internet. Computer Network Forensics Research Workshop, 2005, p. 1.
27. Warikoo, A. Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal: A Global Perspective*. 2014, 23(4-6), p.172-178.
28. Wheelbarger, S (2009). CyberForensics. Criminal justice collaboratory. Colby Community College. [interaktyvus] [žiūrėta 2015-09-25].<www.colbycriminaljustice.wikidot.com/cyberforensics>.

CRIMINAL PROFILING METHODOLOGY ADAPTATION FOR THE INVESTIGATION OF CYBERCRIMES

Birutė Balsevičienė*, Laima Ruibytė**

Mykolas Romeris University

S u m m a r y

The growing number of cyber-crimes draws more attention to this problem and encourages seeking new ways and means of solving it. Despite the lack of clear definition of cybercrimes and different approaches to character of these crimes, cybercrimes have motives, modus operandi very similar to other crimes, so it is possible to use criminal profiling techniques to investigate it. Cybercrimes can be characterized by a lack of concrete space and time. Because of these features arises offenses identification problems. Taking into account the specific of cybercrimes, there is a need of standardized methodology for investigation of these crimes. The proposed methodology is based on a profiling model wherein the initial processes are deductive in nature and inductive statistical analysis is performed to identify common patterns and characteristics. Warikoo proposed methodology is

consisted of four stages: victim profiling, identifying motives, empirical analysis on data, building cyber-criminal profiles. Also it is proposed six Profile Identification Metrics to determine the offender's modus operandi, psychology, and behavior characteristics: attack signature, attack method, motivational level, capability factor, attack severity, demographics. Although cybercrime is increasing in Lithuania, but so far is just at the first steps of criminalization of it. Offender profiling is not a method, which is designed to identify the concrete offender. The most common offender profile can act more as guidelines, scientifically proven way to narrow down the number of allegations of a crime.

Keywords: cybercrimes, criminal profiling.

Birutė Balsevičienė*, Mykolo Romerio universiteto Viešojo saugumo fakulteto Humanitarinių mokslų katedros lektorė. Mokslinių tyrimų kryptys: krizių psichologija, aplinkos ir vaiko psichikos sveikatos sąveika.
Birutė Balsevičienė*, Mykolas Romeris University, Faculty of Public security, Department of Humanities lecturer. Research interest: crisis psychology, the associations between environment and child mental health.

Laima Ruibyte,** daktarė**,** Mykolo Romerio universiteto Viešojo saugumo fakulteto Humanitarinių mokslų katedros vedėja, docentė. Mokslinių tyrimų kryptys: Lyčių skirtumų stereotipai; nuostatos ir stereotipai, stresas organizacijose.
Laima Ruibyte,** PhD, Mykolas Romeris University, Faculty of Public security, head of Department of Humanities Assoc.prof. Research interests: Genders Stereotypes; Attitudes; Organisational Stress; Organisational Values.