AUKŠČIAUSIOJI AUDITO INSTITUCIJA
NAUDINGI • VERTINAMI • ATPAŽĮSTAMI

AR VEIKSMINGAI KOVOJAMA SU ELEKTRONINIAIS NUSIKALTIMAIS

2020 m. liepos 16 d.

Nr. VAE-7

SANTRAUKA

Audito svarba

Nepaisant to, kad informacinių technologijų raida lėmė daug teigiamų pokyčių, ji turėjo įtakos ir nusikalstamų veikų elektroninėje erdvėje atsiradimui. Pagal Konvenciją dėl elektroninių nusikaltimų [1] šiuos nusikaltimus apima nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui, ir kitos nusikalstamos veikos elektroninėje erdvėje: elektroniniai sukčiavimai, nusikaltimai, susiję su vaikų seksualiniu išnaudojimu, autorių teisių ir gretutinių teisių pažeidimai, rasistinio ir ksenofobinio pobūdžio nusikaltimai.

2015 m. ES Tarybos išvadose dėl atnaujintos 2015–2020 m. ES Vidaus saugumo strategijos[2] paskelbta, kad kova su nusikaltimais elektroninėje erdvėje yra vienas iš trijų pagrindinių saugumo prioritetų. Pagal Europos kibernetinio saugumo strategiją[3], Europolo Europos kovos su elektroniniu nusikalstamumu centro (EC3) Nacionalinę sunkaus ir organizuoto nusikalstamumo grėsmių vertinimo 2019 m. ataskaitą[4] ir Pasaulio Ekonomikos Forumo 2020 m. visuotinės rizikos ataskaitą[5] prognozuojama, kad nusikalstamų veikų elektroninėje erdvėje mastas ir galima žala ateityje tik didės, o spartūs informacinių ir ryšių technologijų pokyčiai (pvz., debesų kompiuterija) gali lemti ir naujus iššūkius. Nusikalstamos veikos šioje erdvėje vertintinos kaip auganti rimta grėsmė viešajam saugumui. JAV kompiuterių saugumo

[1] Konvencija dėl elektroninių nusikaltimų, priimta Budapešte 2001-11-23, ratifikuota Lietuvos Respublikos 2004-01-22 įstatymu Nr. IX-1974, o 2006-06-08 įstatymu Nr. X-674 – Konvencijos dėl elektroninių nusikaltimų Papildomas protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo.

[2] Prieiga per internetą: https://vrm.lrv.lt/uploads/vrm/documents/files/LT_versija/Viesasis_saugumas/Strategijos/2015_Tarybos_isvados_del_VSS.pdf.

[3] Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex:52017JC0450.

[4] Prieiga per internetą: https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf.

[5] Ten pat.

programinės įrangos įmonės „McAfee“ kartu su Strateginių ir tarptautinių studijų centru 2018 m. atliktas tyrimas[6] rodo, kad pasaulio verslo išlaidos dėl nusikaltimų elektroninėje erdvėje siekė beveik 700 mlrd. Eur[7], tai sudarė 0,8 proc. viso pasaulio BVP.

JAV programinės įrangos įmonės „WebsiteBuilderExpert“ kibernetinių nusikaltimų rizikos ES šalyse 2018 m. tyrimo[8] duomenimis, Lietuva yra 6 vietoje tarp 28 ES valstybių kaip viena didžiausių kibernetinių nusikaltimų rizikų turinti šalis. 2019 m. atlikto Eurobarometro tyrimo duomenimis, 73 proc. Lietuvos gyventojų mano, kad didėja rizika tapti nusikaltimų elektroninėje erdvėje auka, o 42 proc. gyventojų nėra gerai informuoti apie nusikaltimų šioje erdvėje grėsmes.

Siekdami įvertinti, ar rezultatyviai organizuojama elektroninių nusikaltimų prevencija ir ištyrimas, nusprendėme atlikti nusikaltimų elektroninėje erdvėje prevencijos ir ištyrimo sistemos auditą.

Audito tikslas ir apimtis

Audito tikslas – įvertinti, ar nusikaltimų elektroninėje erdvėje tyrimai ir užkardymas užtikrina visuomenei saugią aplinką šioje erdvėje.

Pagrindiniai audito klausimai:

- ar prevencinė veikla planuojama ir įgyvendina taip, kad užtikrintų nusikaltimų elektroninėje erdvėje prevencinės veiklos tikslų pasiekimą;
- ar užtikrinamas nusikaltimų elektroninėje erdvėje ištyrimas;
- ar sudarytos sąlygos nusikaltimų elektroninėje erdvėje srities tyrimų tobulinimui.

Audituojamieji subjektai:

- Generalinė prokuratūra, kuri vadovauja teritorinėms prokuratūroms ir kontroliuoja jų veiklą, formuoja vienodą nusikalstamų veikų ikiteisminio tyrimo ir baudžiamojo proceso veiksmų kontrolės praktiką, organizuoja prokurorų profesinį rengimą ir kvalifikacijos tobulinimą[9].
- Policijos departamentas prie Vidaus reikalų ministerijos, kuris organizuoja, koordinuoja ir kontroliuoja policijos uždavinių vykdymą, taip pat organizuoja ir įgyvendina pavaldžių policijos įstaigų valdymą[10].
- Krašto apsaugos ministerija, kuri formuoja kibernetinio saugumo politiką ir organizuoja, kontroliuoja ir koordinuoja jos įgyvendinimą[11].

[6] „Kibernetinių nusikaltimų įtaka ekonomikai“. Prieiga per internetą: https://www.mcafee.com/enterprise/en-us/forms/gated-form-thanks.html?docID=5fee1c652573999d75e4388122bf72f5&tag=ec&eid=18TL_ECGLQ1_CT_WW.

[7] Tyrime nurodyta beveik 600 mlrd. JAV dolerių išlaidų suma perskaičiuota eurais.

[8] Prieiga per internetą: https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/.

[9] Prokuratūros įstatymas, 8 str.

[10] Vyriausybės 2001-01-29 nutarimu Nr. 98 patvirtinti Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos nuostatai, 10 p.

[11] Kibernetinio saugumo įstatymas, 4 str.

- Teisingumo ministerija, kuri formuoja politiką baudžiamosios teisės, baudžiamojo proceso, bausmių vykdymo srityse ir organizuoja, koordinuoja ir kontroliuoja šių valstybės politikų įgyvendinimą[12].

Audituojamasis laikotarpis – 2015–2019 m. Siekiant įvertinti pokyčius ir palyginti duomenis, kai kuriais atvejais audito įrodymams surinkti buvo naudojami ankstesnių ir 2020 m. duomenys.

Audito metu nevertinome ikiteisminio tyrimo procesinių sprendimų teisėtumo ir pagrįstumo, nes pagal Prokuratūros įstatymą prokurorų proceso veiklą kontroliuoja aukštesnysis prokuroras ir teismas[13]. Vertinome nusikaltimų elektroninėje erdvėje ištyrimo sistemą, kuri turėtų sudaryti sąlygas šiuos sprendimus priimti išsamiai ir greitai. Atlikdami ikiteisminių tyrimų analizę neanalizavome 2015 m. baigtų ikiteisminių tyrimų statistinių duomenų, nes, Lietuvos kriminalinės policijos biuro duomenimis, 2015 m. pradėjus veikti Integruotai baudžiamojo proceso informacinei sistemai, dalis duomenų gali būti netikslūs.

Auditas atliktas pagal Valstybinio audito reikalavimus ir tarptautinius aukščiausiųjų audito institucijų standartus. Audito apimtis ir taikyti metodai išsamiau aprašyti 2 priede „Audito apimtis ir metodai“ (71 psl.).

Pagrindiniai audito rezultatai

Visuomenei vis daugiau veiklos perkeliant į skaitmeninę erdvę, ten persikelia ir nusikalstamos veikos. Augant elektroninių nusikaltimų mastui, visuomenė turi būti pasiruošusi atpažinti nusikaltimų elektroninėje erdvėje grėsmes ir sugebėti nuo jų apsisaugoti. Turi būti suformuotos pajėgos, gebančios užkardyti ir ištirti šio pobūdžio nusikaltimus, tačiau elektroninių nusikaltimų užkardymo ir tyrimo procesuose nustatyta trūkumų ir visuomenei vis dar nėra užtikrinama saugi aplinka elektroninėje erdvėje.

1. Prevencinė veikla nesudaro sąlygų, kad visuomenė elektroninėje erdvėje jaustųsi saugiai

Prevencinę veiklą nusikaltimų elektroninėje erdvėje atlieka policija ir kitos institucijos: Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija, Valstybinė vartotojų teisių apsaugos tarnyba, Žurnalistų etikos inspektoriaus tarnyba, Kultūros ministerija, Informacinės visuomenės plėtros komitetas, Vyriausybės kanceliarija. Vien tik policijos įstaigos per 2015–2019 m. įgyvendino apie 1,5 tūkst. įvairių prevencinių priemonių, daugiausia orientuotų į šviečiamąją veiklą renginių metu ir informaciją teikiant internete. Tačiau dalyvaujančios institucijos veikia savo kompetencijos srityje ir pagal savo nustatytus prioritetus, prevencinių priemonių tarpusavyje nederina, neatlieka prevencinės veiklos nusikaltimų elektroninėje erdvėje poveikio vertinimo, šalies mastu nesukurta tarpinstitucinė prevencinės veiklos planavimo, koordinavimo ir poveikio matavimo sistema. Dėl šių priežasčių įgyvendinamos panašios prevencinės priemonės (pvz., elektroninio sukčiavimo tema švietėjišką veiklą vykdė 5 institucijos), kurios neduoda reikiamo rezultato.

[12] Vyriausybės 1998-07-09 nutarimu Nr. 851 patvirtinti Lietuvos Respublikos teisingumo ministerijos nuostatai, 7 p.

[13] Prokuratūros įstatymas, 4 str. 2 d.

Eurobarometro tyrimo duomenimis, 2019 m., palyginus su 2018 m., Lietuvoje yra 16 proc. daugiau (atitinkamai nuo 28 iki 44 proc.) gyventojų, kurie mano, kad nėra pajėgūs apsisaugoti nuo NEE (1.1 poskyris, 18 psl.).

Blokavimo teisės, kurios turėtų apriboti prieigą prie nepageidaujamo ir žalingo turinio internete, suteiktos 7 institucijoms. Nustatėme, kad iki 2020 m. vasario mėn. šalies mastu iš viso buvo užblokuota 511 svetainių. Atlikus blokavimo veiksmus, sukuriama kita veidrodinė svetainė[14], pvz., iš 397 Lošimų priežiūros tarnybos blokuotų svetainių 297 buvo veidrodinės. Nepageidaujamą ir žalingą turinį internete platinantys asmenys geba apeiti blokavimo mechanizmą, todėl šios priemonės yra laikino pobūdžio, o neteisėtas ir žalingas turinys lieka nepašalintas. Dėl to gyventojams ir toliau išlieka grėsmė nukentėti nuo galimai vykdomų nusikaltimų, o pakartotiniai blokavimo veiksmai didina administracinę naštą institucijoms ir privalomus nurodymus įgyvendinančioms įmonėms. Institucijos, įgyvendindamos blokavimo įgaliojimus, taiko skirtingus teisės aktus, kuriuose nustatyta skirtinga blokavimo teisių įgyvendinimo tvarka: skirtingi procedūriniai veiksmai, jų terminai, blokavimo būdų pasirinkimai (1.2 poskyris, 22 psl.).

2. Kibernetinių incidentų valdymo trūkumai nesudaro sąlygų identifikuoti visų incidentų, kurie galimai yra nusikalstamos veikos

Policija nevaldo visos informacijos apie kibernetinius incidentus, kurie galimai yra nusikalstamos veikos, nes ne visi kibernetinio saugumo subjektai (19 iš 143 auditorių apklaustų) praneša policijai apie kibernetinius incidentus, kurie galimai yra nusikalstamos veikos elektroninėje erdvėje. Valstybinė duomenų apsaugos inspekcija tokios informacijos policijai 2015–2019 m. nė karto neteikė, o Nacionalinis kibernetinio saugumo centras nurodo kibernetinio saugumo subjektams patiems kreiptis į policiją. Policija ir Nacionalinis kibernetinio saugumo centras nesikeičia turimais duomenimis apie elektroninėje erdvėje vykstančius įvykius ir incidentus. Šią situaciją lemia kibernetinių incidentų valdymo trūkumai. Nenustatyti kriterijai (bendra taksonomija[15]), pagal kuriuos būtų galima identifikuoti, kurie kibernetiniai incidentai galimai yra nusikaltimai elektroninėje erdvėje. Taip pat nėra aiškiai reglamentuota, ką kibernetinio saugumo subjektai privalo informuoti – policiją ar Nacionalinį kibernetinio saugumo centrą apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių. Trūksta metodinio vadovavimo, konsultacijų ir mokymų, kurie stiprintų kibernetinio saugumo subjektų gebėjimus atpažinti ir reaguoti į nusikalstamas veikas: 64 proc. apklaustiems kibernetinio saugumo subjektams nėra aišku, kaip įvertinti nusikaltimo nuostolį ar žalą, 51 proc. – kaip tinkamai surinkti ir išsaugoti elektroninius įrodymus, o 27 proc. – kaip reaguoti į galimai vykdomą nusikaltimą elektroninėje erdvėje. Be to, nesudarytos sąlygos kibernetinius incidentus, kurie galimai yra nusikaltimai elektroninėje erdvėje, valdyti taikant vieno langelio principą.

Lietuvos kriminalinės policijos biuras aktyviai nevykdo kibernetinių incidentų, kurie galimai yra nusikalstamos veikos, stebėsenos ir analizės, tam neskiria pakankamai žmogiškųjų išteklių (su kibernetiniais incidentais dirba vienas pareigūnas, per 2015–2019 m. jis atliko 9 kibernetinių incidentų tyrimus). Nevaldant visos informacijos apie kibernetinius incidentus, kurie galimai yra nusikaltimai elektroninėje erdvėje, policija gali

[14] Veidrodinės svetainės - tokios interneto svetainės, kurių interneto domeno vardas yra beveik tapatus pirminei interneto svetainei – pridedamos arba pašalinamos kelios raidės, skaičiai, kiti ženklai, pasikeičia domeno galūnė ar pan.

[15] Tam tikrų požymių aprašymai (nuorodos į teisės aktus), kurie sudaro sąlygas skirtingų tipų kibernetinius incidentus susieti su tam tikromis nusikalstamomis veikomis.

laiku nesureaguoti į elektroninėje erdvėje vykdomas nusikalstamas veikas, neįvertinti, koks yra šių grėsmių mastas (2 skyrius, 26 psl.).

3. Nesudarytos sąlygos rezultatyviai atlikti nusikaltimų elektroninėje erdvėje tyrimus

Apskričių vyriausiuose policijos komisariatuose 2015 m. pradėjo veikti kriminalinės policijos nusikaltimų elektroninėje erdvėje specializuoti padaliniai, kuriems pavesta savo teritorijoje užkardyti, atskleisti ir tirti nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, elektroninėje erdvėje padarytas nusikalstamas veikas. Šių padalinių veiklos rezultatyvumas nėra pakankamas. Nustatėme, kad 2019 m., palyginus su 2016 m., 9 proc. sumažėjo perduotų į teismą ikiteisminių tyrimų ir jis nesiekia nustatyto[16] 40 proc. dydžio (2016 m. – 38 proc., 2017 m. – 39 proc., 2018 m. – 37 proc., 2019 m. – 29 proc.). 40 proc. nusikaltimų elektroninėje erdvėje ikiteisminių tyrimų trunka ilgiau nei siektinas 9 mėn. terminas[17]. Be to, 11 proc. (21 iš 191) nusikaltimų šioje erdvėje tikrintų ikiteisminių tyrimų procesinių sprendimų sustabdyti, nutraukti ar atsisakyti pradėti ikiteisminį tyrimą prokurorų buvo panaikinti per 2017–2019 m. Šių tyrimų rezultatyvumui įtaką daro nepakankamai veiksmingas specializuotų padalinių valdymo modelis ir pareigūnų bei prokurorų ugdymo organizavimas.

Nepakankamai veiksmingas nusikaltimų elektroninėje erdvėje specializuotų padalinių valdymo modelis

Audito metu nustatyta specializuotų padalinių valdymo trūkumų:

- Šalies mastu nepakankamai identifikuojami sisteminiai nusikaltimai elektroninėje erdvėje. Nors apskričių vyriausiųjų policijos komisariatų lygiu atliekama duomenų analizė, siekiant nustatyti sisteminius nusikaltimus, tačiau Generalinė prokuratūra skirtinguose komisariatuose nustato atliekamus ikiteisminius tyrimus, kurie neidentifikuojami kaip sisteminio nusikaltimo dalis ir nėra sujungiami. Pvz., nuo 2019-08-19 iki 2020-02-18 skirtingose ikiteisminio tyrimo įstaigose buvo pradėti 68 ikiteisminiai tyrimai, kurie nebuvo sujungti į vieną sisteminį. Lietuvos kriminalinės policijos biuras neturi visos informacijos apie nustatomus sisteminius nusikaltimus. Nuo 2018 m. birželio iki 2020 m. kovo mėn. Lietuvos kriminalinės policijos biuras gavo 11 tarnybinių pranešimų apie sisteminius nusikaltimus elektroninėje erdvėje iš Vilniaus apskrities vyriausiojo policijos komisariato, kiti padaliniai tokios informacijos neteikė. Neidentifikavus visų sisteminių nusikaltimų, prarandama galimybė įvertinti tikrąjį nusikalstamų veikų žalos mastą, nukentėjusiųjų ir kaltininkų skaičių.
- Trūksta specializuotų pajėgumų tirti nusikaltimus elektroninėje erdvėje. Keturiuose daugiausiai nusikaltimų elektroninėje erdvėje ikiteisminius tyrimus atliekančiuose specializuotuose padaliniuose viršijamas priimtinas (ne daugiau kaip 6 ikiteisminiai tyrimai vienu metu) pareigūnų darbo krūvis. Kai kurių pareigūnų krūviai iki 3 kartų viršija nustatytą normą (pvz., Vilniaus specializuotame padalinyje kai kurie pareigūnai vienu metu atliko 16–20 ikiteisminių tyrimų, Kaune – 14). Šie darbo krūviai susidaro, nes specializuoti padaliniai yra nesukomplektuoti: 2019 m.

[16] Lietuvos kriminalinės policijos biuro viršininko 2017-07-14 įsakymu Nr. 38-V-80-(1.10-38E) patvirtintas Lietuvos kriminalinės policijos biuro vykdomų policijos pagrindinės veiklos vidaus kontrolės priemonių taikymo tvarkos aprašas, 2 priedas.

[17] Ten pat.

neužimtų nusikaltimus elektroninėje erdvėje tiriančių pareigybių procentinė dalis vidutiniškai sudarė 22 proc. Taip pat krūvius didina neužkardomi nusikaltimai elektroninėje erdvėje, vykdomi iš laisvės atėmimo vietų. Pavyzdžiui, Vilniaus, Kauno ir Klaipėdos specializuotų padalinių tiriami elektroniniai sukčiavimai iš laisvės atėmimo vietų 2019 m. sudarė 8–16 proc. visų tais metais registruotų šio pobūdžio nusikaltimų. Siekiant perskirstyti ir mažinti darbo krūvius vienam pareigūnui, ikiteisminius tyrimus paskiriama atlikti žvalgybos funkciją vykdantiems pareigūnams, taip mažinant žvalgybos veiksmų apimtis šioje srityje. Dėl nepakankamų žmogiškųjų išteklių nesudaromos prielaidos kokybiškai ir per trumpiausius terminus atlikti ikiteisminius tyrimus.

- Nepakankamai išgryninta policijos padalinių ir prokurorų specializacija nusikaltimų elektroninėje erdvėje. Esamos specializacijos tvarkos ir susiformavusi praktika neužtikrina, kad nusikaltimai elektroninėje erdvėje, kurie turi būti tiriami specializuotose padaliniuose, būtų nukreipti tirti tik specializuotiems pareigūnams ir jiems vadovautų tik specializuoti prokurorai. 2016–2019 m. nespecializuoti pareigūnai atliko vidutiniškai 62 proc. visų nusikaltimų elektroninėje erdvėje ikiteisminių tyrimų, iš jų vidutiniškai 11 proc. nusikaltimų priskirtina Baudžiamojo kodekso XXX skyriui, kurie yra specializuotų padalinių kompetencija. Specializuotų padalinių ikiteisminiams tyrimams vadovavo 28 proc. nespecializuotų prokurorų. Dėl nepakankamai išgrynintos specializacijos dalį sudėtingų tyrimų gali atlikti ir jiems vadovauti nepakankamai specialių žinių turintys pareigūnai ir prokurorai.
- Ilgos informacinių technologijų objektų tyrimų eilės, pvz., Vilniaus apskrities vyriausiojo policijos komisariato kriminalistinių tyrimų skyriuje objektų tyrimo tenka laukti apie 19 mėn., Kriminalistinių tyrimų centre – apie 10 mėn. Dėl šių eilių užtrunka nusikaltimų elektroninėje erdvėje ištyrimo laikas, dėl to gali būti prarasti tyrimui svarbūs skaitmeniniai duomenys.

Šie valdymo trūkumai nesudaro sąlygų, kad nusikaltimai elektroninėje erdvėje būtų atskleisti greitai ir išsamiai, ir neišnaudojamos visos galimybės šias nusikalstamas veikas ištirti apsaugant valstybės ir visuomenės interesus (3.1 poskyris, 36 psl.).

Nepakankamai veiksmingai organizuojamas specializuotų pareigūnų ir prokurorų ugdymas

Nėra parengta nusikaltimų elektroninėje erdvėje mokymų programa besispecializuojantiems pareigūnams, o mokymai jiems vyksta tik pagal poreikius, kurie neapima IOCTA ataskaitose rekomenduojamų mokymų krypčių. Nustatėme, kad 2015-2019 m. 30 proc. specializuotų pareigūnų nė karto nedalyvavo mokymuose. Taip pat organizuojami pavieniai bendri mokymai prokurorams ir pareigūnams. 70 proc. auditorių apklaustų specializuotų prokurorų ir pareigūnų nurodė, kad mokymų šioje srityje nepakanka.

Vis dar visu pajėgumu neveikia nusikaltimų elektroninėje erdvėje specializuotų prokurorų tinklas ir nesukurtas pareigūnų tinklas, kuriame sistemos dalyviai galėtų keistis gerąja praktika ir patirtimi. Be to, 68 proc. auditorių apklaustų prokurorų ir 62 proc. pareigūnų nurodė, kad trūksta naujų metodinių dokumentų, kurie galėtų palengvinti praktinį nusikaltimų elektroninėje erdvėje tyrimą, ypač elektroninių įrodymų surinkimo ir išsaugojimo, specifinių kibernetinių nusikaltimų tyrimą. Dėl nepakankamai veiksmingai organizuojamo ugdymo

nesudaromos sąlygos kelti specializuotų pareigūnų ir prokurorų kompetenciją ir pasiekti didesnį veiklos rezultatyvumą (3.2 poskyris, 49 psl.).

4. Neskiriamas pakankamas dėmesys nusikaltimų elektroninėje erdvėje srities prevencijos ir ištyrimo gerinimui

Viešojo saugumo plėtros 2015–2025 m. programoje [18] ir Nacionalinėje kibernetinio saugumo strategijoje[19] numatytos priemonės kovai su nusikaltimais elektroninėje erdvėje yra nepakankamos, nes nesprendžia problemų, susijusių su prevencine veikla; neteisėto ir žalingo turinio internete pašalinimu; kibernetinių incidentų, kurie galimai yra nusikaltimai elektroninėje erdvėje, valdymu; sisteminių nusikaltimų elektroninėje erdvėje indentifikavimu; specializuotų kompetencijų ugdymu; ilgomis informacinių technologijų objektų tyrimų eilėmis; nepakankamu nusikaltimų elektroninėje erdvėje profiliavimu. Skiriant nepakankamai dėmesio nusikaltimų elektroninėje erdvėje prevencijai ir ištyrimo gerinimui, tokio pobūdžio nusikaltimų ištyrimo rezultatai ir visuomenės saugumas elektroninėje erdvėje ateityje gali dar labiau sumažėti.

Nusikaltimų elektroninėje erdvėje profilis apima nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui (Baudžiamojo kodekso XXX skyrius) ir nusikaltimus, susijusius su vaikų seksualiniu išnaudojimu elektroninėje erdvėje, tačiau neapima kitų Konvencijoje dėl elektroninių nusikaltimų [20] nurodytų nusikalstamų veikų, kurios padarytos elektroninėje erdvėje: kompiuterinių sukčiavimų, nusikaltimų, susijusių su autorių teisių ir gretutinių teisių pažeidimais, rasistinio ir ksenofobinio pobūdžio nusikaltimų. Policijos registruose nėra renkama, sisteminama ir analizuojama visa informacija apie šios srities nusikaltimus, todėl neanalizuojama faktinė nusikaltimų elektroninėje erdvėje grėsmių apimtis ir tendencijos. Tai, kad neturima visos informacijos apie šiuos nusikaltimus, gali turėti neigiamos įtakos priimant strateginius sprendimus ir tinkamai reaguoti į pokyčius šioje srityje.

Skirtinguose strateginiuose planavimo dokumentuose nustatytos skirtingos siektinos ištirtų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui (Baudžiamojo kodekso XXX skyrius) rodiklio reikšmės. Nuo 2020 m. Generalinė prokuratūra ir Policijos departamentas siekia ištirti 50 proc. tokių nusikalstamų veikų, o Viešojo saugumo plėtros 2015–2025 m. programos įgyvendinimo tarpinstituciniame veiklos plane nustatytas siektinas 96 proc. ištyrimas (4 skyrius, 55 psl.).

Rekomendacijos

Vidaus reikalų ministerijai

1. Siekiant, kad nusikaltimų elektroninėje erdvėje prevencinės veiklos įgyvendinimas darytų didesnį poveikį šalies gyventojų gebėjimui atpažinti šias grėsmes, užtikrinti tarpinstitucinį prevencinės veiklos nusikaltimų elektroninėje erdvėje srityje planavimą, koordinavimą ir poveikio matavimą (1-asis pagrindinis audito rezultatas).

[18] Seimo 2015-05-07 nutarimas Nr. XII-1682 „Dėl Viešojo saugumo plėtros 2015–2025 metų programos patvirtinimo“.

[19] Vyriausybės 2018-08-13 nutarimas Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“.

[20] Ratifikuota 2004-01-22 įstatymu Nr. IX-1974.

2. Siekiant šalies mastu užtikrinti rezultatyvesnį nusikalstamos veikos elektroninėje erdvėje užkardymą, mažinant galimybes gyventojams tapti šių nusikaltimų aukomis:

   2.1. numatyti priemones, kurios sudarytų sąlygas šalinti neteisėtą ir žalingą turinį internete (1-asis pagrindinis audito rezultatas);

   2.2. užtikrinti bendrą blokavimo įgaliojimų įgyvendinimo tvarką (1-asis pagrindinis audito rezultatas).

Krašto apsaugos ministerijai, Generalinei prokuratūrai ir Policijos departamentui

3. Siekiant gerinti kibernetinio saugumo subjektų kibernetinių incidentų, kurie galimai yra nusikaltimai elektroninėje erdvėje, identifikavimą ir sustiprinti policijos ir Nacionalinio kibernetinio saugumo centro bendradarbiavimą šioje srityje:

   3.1. suderinti kibernetinio saugumo incidentų ir nusikalstamų veikų elektroninėje erdvėje taksonomiją, kuri leistų identifikuoti, kurie kibernetiniai incidentai galimai yra nusikalstamos veikos (2-asis pagrindinis audito rezultatas)

   3.2. pagal suderintą kibernetinių incidentų ir nusikalstamų veikų elektroninėje erdvėje taksonomiją tobulinti esamą kibernetinių incidentų valdymo mechanizmą, kuris užtikrintų visų kibernetinio saugumo subjektų kibernetinių incidentų, kurie galimai yra nusikaltimai elektroninėje erdvėje, privalomą pateikimą tolimesniam jų tyrimui vieno langelio principu (2-asis pagrindinis audito rezultatas).

4. Siekiant stiprinti kibernetinio saugumo subjektų, kurie valdo ir tvarko valstybės informacinius išteklius, gebėjimus identifikuoti kibernetinius incidentus, kurie galimai yra nusikaltimai elektroninėje erdvėje, bei tinkamai reaguoti į juos:

   4.1. organizuoti kibernetinio saugumo subjektams, kurie valdo ir tvarko valstybės informacinius išteklius, mokymus, užtikrinant, kad jų metu būtų suteiktos reikiamos teisinės ir techninės žinios apie nusikaltimus elektroninėje erdvėje (2-asis pagrindinis audito rezultatas);

   4.2. parengti metodinius dokumentus dėl incidento žalos / nuostolio įvertinimo, elektroninių įrodymų rinkimo ir išsaugojimo (2-asis pagrindinis audito rezultatas).

Policijos departamentui

5. Siekiant didinti nusikaltimų elektroninėje erdvėje tyrimų rezultatyvumą:

   5.1. peržiūrėti nusikaltimų elektroninėje erdvėje specializuotų padalinių veiklos modelį ir tobulinti jį taip, kad šalies mastu būtų identifikuojami visi sisteminiai nusikaltimai, sutelkti pakankami specializuoti tyrimo atlikimo ir ekspertiniai pajėgumai bei būtų didinamos kriminalinės žvalgybos veiklos apimtys (2-asis ir 3-iasis pagrindiniai audito rezultatai);

   5.2. parengti ir patvirtinti specializuotiems pareigūnams skirtą nusikaltimų elektroninėje erdvėje mokymų programą, atitinkančią pareigūnų ugdymo poreikius šioje srityje, ypač didelį dėmesį skiriant naujų specialiųjų kompetencijų ugdymui, ir ją įgyvendinti (3-iasis pagrindinis audito rezultatas);

5.3. sukurti nusikaltimų elektroninėje erdvėje besispecializuojančių pareigūnų tinklą ir užtikrinti jo aktyvią veiklą (3-iasis pagrindinis audito rezultatas).

6. Siekiant valdyti informaciją apie visus nusikaltimus elektroninėje erdvėje, į jų profilio apimtį įtraukti visas nusikalstamas veikas, padarytas elektroninėje erdvėje, ir užtikrinti šios informacijos rinkimą, sisteminimą ir panaudojimą grėsmių analizei ir strateginiams sprendimams priimti (4-asis pagrindinis audito rezultatas).

Generalinei prokuratūrai

7. Siekiant gerinti nusikaltimų elektroninėje erdvėje ištyrimą:

7.1. tobulinti prokurorų specializacijos tvarką, kad visiems nusikaltimų elektroninėje erdvėje specializuotų pareigūnų ikiteisminiams tyrimams vadovautų šios srities specializuoti prokurorai (3-iasis pagrindinis audito rezultatas);

7.2. didinti nusikaltimų elektroninėje erdvėje mokymų specializuotiems prokurorams apimtis ir užtikrinti, kad šiose mokymuose dalyvautų visi specializuoti prokurorai (3-iasis pagrindinis audito rezultatas);

7.3. parengti bendrą nusikaltimų elektroninėje erdvėje specializuotų pareigūnų ir prokurorų mokymų programą ir ją įgyvendinti (3-iasis pagrindinis audito rezultatas);

7.4. įvertinti metodinių rekomendacijų, skirtų nusikaltimų elektroninėje erdvėje tyrimui, poreikį ir jas parengti (3-iasis pagrindinis audito rezultatas).

Kalėjimo departamentui

8. Siekiant sustabdyti elektroninius nusikaltimus, vykdomus iš laisvės atėmimo vietų, numatyti ir įgyvendinti priemones, kurios užkardytų šiuos nusikaltimus (3-iasis pagrindinis audito rezultatas).

Vidaus reikalų ir Krašto apsaugos ministerijoms

9. Siekiant gerinti nusikaltimų elektroninėje erdvėje užkardymą ir tyrimą:

9.1. nacionaliniuose strateginio planavimo dokumentuose numatyti priemones, kurios spręstų aktualias nusikaltimų elektroninėje erdvėje srities problemas (4-asis pagrindinis audito rezultatas);

9.2. tobulinti nusikaltimų elektroninėje erdvėje vertinimo kriterijus, suvienodinant juos visuose strateginio planavimo dokumentuose ir sudarant sąlygas matuoti visų šių nusikaltimų ištyrimo būklę (4-asis pagrindinis audito rezultatas).

Rekomendacijų įgyvendinimo priemonės ir terminai pateikti ataskaitos dalyje „Rekomendacijų įgyvendinimo planas“ (60 psl.)