AUKŠČIAUSIOJI
AUDITO INSTITUCIJA
NAUDINGI • VERTINAMI • ATPAŽĮSTAMI

VALSTYBINIO AUDITO ATASKAITA

AR VEIKSMINGAI KOVOJAMA SU ELEKTRONINIAIS NUSIKALTIMAIS

2020 m. liepos 16 d.

Nr. VAE-7

Valstybės kontrolės – aukščiausiosios valstybinio audito institucijos – pagrindinė funkcija – prižiūrėti, ar teisėtai ir efektyviai valdomi ir naudojami valstybės finansai ir kitas turtas bei kaip vykdomas valstybės biudžetas. Aukščiausioji audito institucija, teikdama audito pastebėjimus ir rekomendacijas, siekia didinti viešojo sektoriaus efektyvumą ir jo kuriamą naudą visuomenei, o savo darbui keldama aukščiausius kokybės reikalavimus – būti pavyzdžiu visam viešajam sektoriui.

Auditą atliko: Dainoras Bagavičius (grupės vadovas iki 2019-11-22), Venera Michalovska (grupės vadovas nuo 2019-11-25 iki 2020-05-29), Gytis Tamulevičius (grupės vadovas nuo 2020-06-01), Linas Balčiūnas, Denis Voišnis, Diana Nikitina, Viktorija Danaitytė.

Valstybinio audito ataskaita pateikta: Lietuvos Respublikos Seimo Audito ir Nacionalinio saugumo ir gynybos komitetams, Lietuvos Respublikos generalinei prokuratūrai, Lietuvos Respublikos vidaus reikalų ministerijai, Lietuvos Respublikos krašto apsaugos ministerijai, Lietuvos Respublikos teisingumo ministerijai, Policijos departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos, Kalėjimų departamentui prie Lietuvos Respublikos teisingumo ministerijos.

TURINYS

PAGRINDINIAI FAKTAI

1 288

2019 m. Nusikalstamų veikų žinybiniame registre užregistruota nusikalstamų veikų, padarytų elektroninėje erdvėje. Tai sudaro 2,5 proc. visų atitinkamais metais registruotų nusikalstamų veikų (51,4 tūkst.).

81

pareigūnas 2019 m. specializavosi nusikaltimų elektroninėje erdvėje srityje. Jų skaičius nuo 2015 m. augo (2015 m. – 49, 2016 m. – 65, 2017 m. – 74, 2018 m. – 78). Šie tyrėjai dirba Lietuvos kriminalinės policijos biuro ir 10-yje apskričių vyriausiųjų policijos komisariatų įsteigtuose kriminalinės policijos specializuotose padaliniuose.

264

prokurorai (apylinkių, apygardų prokuratūrų ir Generalinės prokuratūros) 2019 m. specializavosi nusikaltimuose, kurie būdingi nusikaltimų elektroninėje erdvėje sričiai.

2,1 mln. Eur

2019 m. skirta Lietuvos kriminalinės policijos biuro ir nusikaltimų elektroninėje erdvėje specializuotų padalinių išlaikymui.

17 proc.

2019 m., palyginus su 2016 m., sumažėjo registruojamų nusikalstamų veikų, padarytų elektroninėje erdvėje.

29 proc.

2019 m. kriminalinės policijos specializuotų padalinių atliktų nusikaltimų elektroninėje erdvėje ikiteisminių tyrimų perduota į teismą. Palyginus su 2016 m., šis rodiklis sumažėjo 9 proc. punktais.

40 proc.

2016–2019 m. baigtų nusikaltimų elektroninėje erdvėje ikiteisminių tyrimų truko ilgiau nei 9 mėn.

11 proc.

2017–2019 m. prokurorų panaikinta tikrintų sprendimų sustabdyti, nutraukti arba atsisakyti pradėti nusikaltimų elektroninėje erdvėje ikiteisminį tyrimą.

~ 62 proc.

nusikaltimų elektroninėje erdvėje ikiteisminių tyrimų 2016–2019 m. atliko nespecializuoti pareigūnai. Iš jų vidutiniškai 11 proc. nusikaltimų priskirtina Baudžiamojo kodekso 196–198[2] str., kurie yra specializuotų padalinių kompetencija.

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 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.

---

[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.

[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/.

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].
- 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.

[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.

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

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

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. 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.).

[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.

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 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

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

[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.

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. 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.

[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“.

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).

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)

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

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);

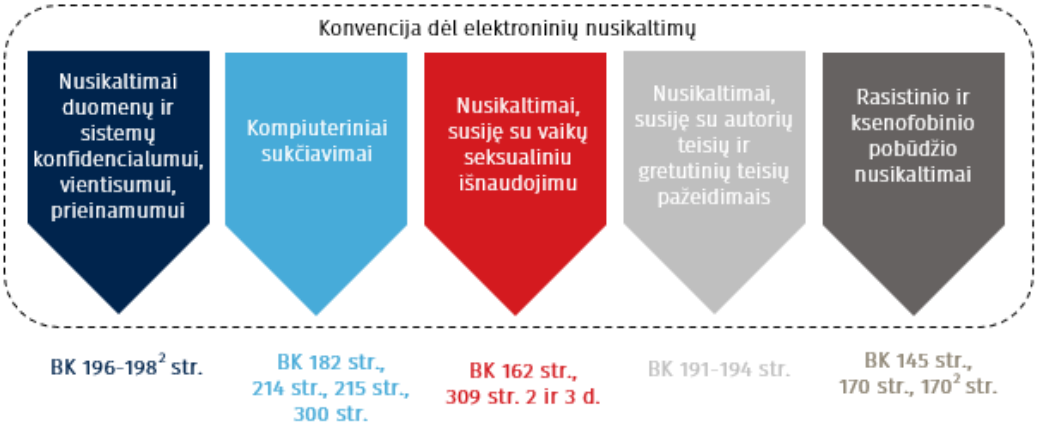
9.2. tobulinti nusikaltimų elektroninėje erdvėje vertinimo kriterijus, suvienodinant juos visuose strateginio planavimo dokumentuose ir sudarant sąlygas matuoti visų šių nusikaltimų ištyrimo būklę (4-asis pagrindinis audito rezultatas).

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

ĮŽANGA

Konvencija dėl elektroninių nusikaltimų[21], kuri mokslinėje literatūroje laikoma vienu iš svarbiausių tarptautinių teisės aktų, reguliuojančių elektroninius nusikaltimus, išskiria šias jų grupes: nusikaltimai kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui; kompiuteriniai sukčiavimai; nusikaltimai, susiję su vaikų seksualiniu išnaudojimu internete; nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais; rasistinio ir ksenofobinio pobūdžio nusikaltimai, padaryti naudojant informacines technologijas. Šios nusikalstamos veikos yra kriminalizuotos Baudžiamajame kodekse (žr. 1 pav.).

1 pav. Elektroninių nusikaltimų grupės



Šaltinis – Valstybės kontrolė pagal Konvenciją dėl elektroninių nusikaltimų

Baudžiamojo kodekso XXX skyriuje (196–198[2] str.) išvardytos vadinamosios grynosios nusikalstamos veikos, kurios gali būti įvykdytos tik elektroninėje erdvėje. Tuo tarpu kitos veikos gali būti įvykdytos ir fizinėje erdvėje. Šių grynųjų elektroninių nusikaltimų kėsinimosi objektas yra elektroninių duomenų ir informacinių sistemų saugumas, t. y.[22]:

- neteisėtas prisijungimas prie informacinės sistemos, pvz.: svetimos elektroninės bankininkystės paskyros, elektroninės pašto dėžutės, *Facebook*, SKYPE, kitų paskyrų, įvairių neviešo pobūdžio duomenų talpyklų, registrų;
- neteisėtas elektroninių duomenų perėmimas ir panaudojimas, pvz.: neviešo pobūdžio duomenų bazėje esančių duomenų neteisėtas stebėjimas, fiksavimas, gavimas, laikymas, pasisavinimas, paskleidimas ar kitoks panaudojimas;
- neteisėtas poveikis elektroniniams duomenims, pvz., neteisėtas prisijungimas prie tinklalapio turinio valdymo sistemos ir elektroninių duomenų pakeitimas ar pašalinimas;
- neteisėtas poveikis informacinei sistemai, pvz.: DoS (angl. *Denial of Service*) ir DDoS (angl. *Distributed Denial of Service*) atakos prieš internetinius puslapius,

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

[22] Prieiga per internetą: https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasis-persekiojimas/nusikaltimai-elektronineje-erdveje/185.

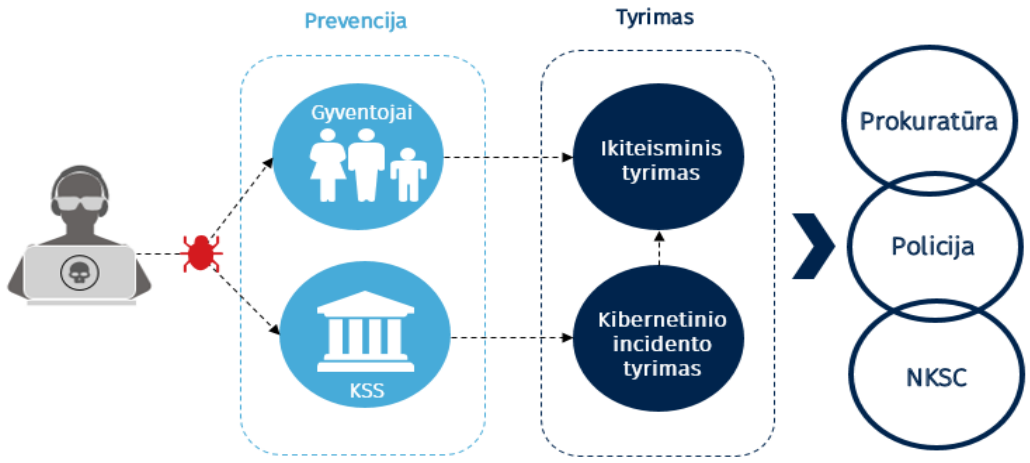
tarnybines stotis. Šiomis atakomis siekiama paveikti informacinę sistemą arba tinklą taip, kad kompiuterinės paslaugos taptų neprieinamos vartotojams;

- neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, pvz.: kenkėjiška programine įranga, kuri renka klientų duomenis[23], neteisėtas disponavimas svetimų elektroninių paskyrų slaptažodžiais, prisijungimo kodais.

Nusikalstamų veikų žinybiniame registre 2019 m. buvo užregistruotos 1 288 nusikalstamos veikos, padarytos elektroninėje erdvėje. Didžiausią jų dalį sudaro elektroniniai sukčiavimai – 58 proc., nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui – 34 proc., vaikų išnaudojimas pornografijai – 6 proc., kiti[24] – 2 proc.

Nusikaltimams elektroninėje erdvėje būdingas latentiškumas[25], todėl visuomenė itin pažeidžiama, o švietėjiška veikla turi užtikrinti gyventojų atsparumą jiems. Be to, šiems nusikaltimams būdingas sistemiškumas, jie vykdomi naudojant įvairius technologinius išteklius. Tai reikalauja institucijų veiksmingo reagavimo ištiriant šiuos nusikaltimus (žr. 2 pav.).

2 pav. Nusikaltimų elektroninėje erdvėje užkardymas ir tyrimas



Šaltinis – Valstybės kontrolė

Nusikaltimus elektroninėje erdvėje užkardo, atskleidžia ir tiria Lietuvos kriminalinės policijos biuro Sunkaus ir organizuoto nusikalstamumo tyrimo 5-oji valdyba (SO5) ir dešimtyje apskričių vyriausiųjų policijos komisariatų nuo 2015 m. įsteigti kriminalinės policijos nusikaltimų elektroninėje erdvėje specializuoti padaliniai. Šioms funkcijoms įgyvendinti 2015-2019 m. skirta 9,6 mln. Eur (2015 m. 1 mln. Eur; 2016 m. 1,6 mln. Eur; 2017 m. 1,8 mln. Eur; 2018 m. 3,1 mln. Eur; 2019 m. 2,1 mln. Eur)[26].

[23] Pvz., „Trojos arkliai“ – programinė įranga, turinti kenkėjiškų funkcijų ir besislepianti kitose programose; „keylogger“ – kenkėjiška programinė įranga, nežinant vartotojui fiksuojanti kiekvieną klaviatūros paspaudimą.

[24] Autorių teisių ir ksenofobinio pobūdžio nusikaltimai.

[25] Latentinis nusikalstamumas (lot. *latens* – nepastebėtas, nepastebimas) – padarytų, bet nepatekusių į apskaitą, neužregistruotų ar neatskleistų nusikalstamų veikų visumos raiškos procesai. Visuotinė lietuvių enciklopedija, T. XI (Kremacija-Lenzo taisyklė). – Vilnius: Mokslo ir enciklopedijų leidybos institutas, 2007. 559 psl.

[26] Suma apima lėšas, skirtas darbo užmokesčiui, pareigūnų mokymams, komandiruotėms, įrangai, reikalingai nusikaltimams elektroninėje erdvėje tirti ir užkardyti, įsigyti.

Prokuratūra organizuoja ikiteisminį tyrimą ir jam vadovauja[27]. Už kibernetinių incidentų valdymo organizavimą, stebėseną ir analizę nacionaliniu lygiu atsakingas Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos.

[27] Konstitucija, 118 str.; BPK, 164 str.

AUDITO REZULTATAI

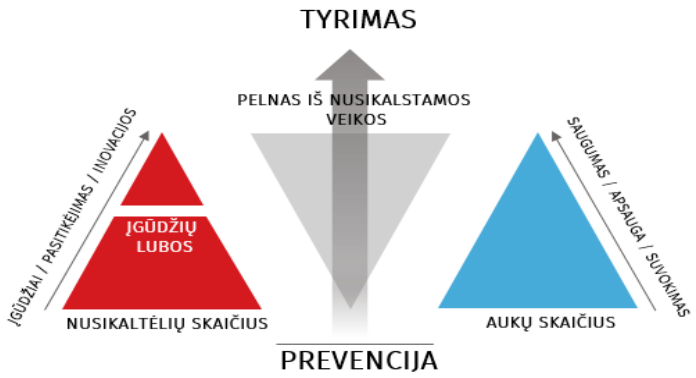
1. VISUOMENĖS SAUGUMAS ELEKTRONINĖJE ERDVĖJE TURI BŪTI DIDINAMAS

1. Skaitmeninės ekonomikos ir visuomenės indeksas (DESI)[28] rodo, kad didelė dalis Lietuvos gyventojų naudojasi internetu, kiekvienais metais ši dalis auga, t. y. 2017 m. internetu naudojosi 75 proc. šalies gyventojų, 2018 m. – 78 proc., 2019 m. – 81 proc. Visuomenės gyvenimas vis labiau skaitmenizuojasi: internetu perkamos prekės, atliekamos finansinės operacijos, skaitmeninėje erdvėje bendraujama ir pan. Atitinkamai keičiasi ir nusikalstamas pasaulis: tradiciniai nusikaltimai, panaudojus technines priemones, gali būti vykdomi ne tik fizinėje, bet ir elektroninėje erdvėje, randasi naujų būdų juos atlikti.

2. Pagal Europolo Europos kovos su elektroniniu nusikalstamumu centro (EC3)[29] duomenis, kovojant su NEE ir siekiant apsaugoti visuomenę nuo galimų nusikaltimų, būtina investuoti į jų prevenciją. Kiekvienas asmuo, susipažinęs su galimomis nusikaltimų grėsmėmis, geba geriau jas atpažinti ir turi mažesnę tikimybę tapti nusikaltimo auka.

3. Europolo Europos kovos su elektroniniu nusikalstamumu centro NEE trichotomijos modelis[30] (žr. 3 pav.) rodo, kad NEE aukų skaičius mažėja, kai visuomenės branda dėl NEE auga ir tai priklauso nuo efektyviai įgyvendinamos švietėjiškos veiklos. Esant didesniam nusikaltėlių profesionalumui, teisėsaugos institucijų atsakas turi būti paremtas tradicinėmis nusikaltimų tyrimo priemonėmis ir procesais, kurie sudarytų sąlygas veiksmingai reaguoti į NEE.

3 pav. NEE trichotomijos modelis



Šaltinis – Europolo Europos kovos su elektroniniu nusikalstamumu centro (EC3) 2015 m. IOCTA ataskaita

[28] Skaitmeninės ekonomikos ir visuomenės indeksas (DESI), 2020 m. Lietuvos ataskaita. Prieiga per internetą: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66948..

[29] Nacionalinė sunkaus ir organizuoto nusikalstamumo grėsmių vertinimo 2015 m. ataskaita (IOCTA), 63 psl. Prieiga per internetą: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2015.pdf.

[30] Ten pat. NEE trichotomijos modelis parodo ryšius tarp nusikaltėlių skaičiaus, priklausomai nuo nusikaltėlio vykdomos nusikalstamos veikos technologinio sudėtingumo, potencialių nusikaltimo aukų skaičiaus, priklausomai nuo aukos sąmoningumo ir apsaugos lygio, bei tikėtino pelno iš nusikalstomos veikos.

4. Siekiant veiksmingai mažinti NEE grėsmes, būtina vykdyti nusikalstamų veikų ir kitų teisės pažeidimų kompleksinę prevenciją. Ji apima priemones, kuriomis siekiama užkirsti kelią nusikalstamoms veikoms ir kitiems teisės pažeidimams, nustatant ir pašalinant jų priežastis ir sąlygas, taip pat individualiai veikiant asmenis, kurie linkę ar ateityje gali daryti nusikalstamas veikas ar kitus teisės pažeidimus arba gali nukentėti nuo šių veikų ar kitų teisės pažeidimų[31].

5. Laikytasi nuostatos, kad NEE prevencinė veikla veiksminga, kai:
   - ji yra kryptingai planuojama atsižvelgiant į NEE grėsmes[32];
   - visuomenės dalis, žinanti apie NEE grėsmes bei kam pranešti apie NEE, yra ne mažesnė nei ES vidurkis[33];
   - NEE prevencinių priemonių planavimas ir jų įgyvendinimas koordinuojamas su visomis suinteresuotomis institucijomis[34];
   - pagal nustatytus kriterijus vertinamas įgyvendintų NEE prevencinių priemonių poveikis[35].

1.1. Nusikaltimų elektroninėje erdvėje prevencinė veikla šalies mastu turi būti planuojama, įgyvendinama ir vertinamas jos poveikis

6. Siekdami įvertinti, kokios 2015–2019 m. įgyvendintos policijos prevencinės veiklos NEE srityje, surinkome ir išanalizavome 10 AVPK, PD ir LKPB informaciją apie jų vykdytas veiklas. Nustatėme, kad šios policijos įstaigos minėtu laikotarpiu įgyvendino apie 1,5 tūkst. įvairių prevencinių priemonių, kurios yra orientuotos į šviečiamąją veiklą. Šių priemonių mastas nuo 2015 iki 2019 m. išaugo 80 proc. (žr. 4 pav.). Be to, NEE prevenciniais tikslais LKPB vykdė interneto stebėjimą techninėmis priemonėmis[36] pagal temines iniciatyvas (detaliau žr. 4 priede).

[31] Seimo 2015-05-07 nutarimu Nr. XII-1682 patvirtinta Viešojo saugumo plėtros 2015–2025 metų programa, 17 p.

[32] Lietuvos policijos generalinio komisaro 2017-12-29 įsakymu Nr. 5-V-1092 patvirtintas Policijos prevencinės veiklos organizavimo aprašas, 8 p., 2016 m. organizuoto nusikalstamumo internete grėsmės vertinimo ataskaita (IOCTA), 13 psl.

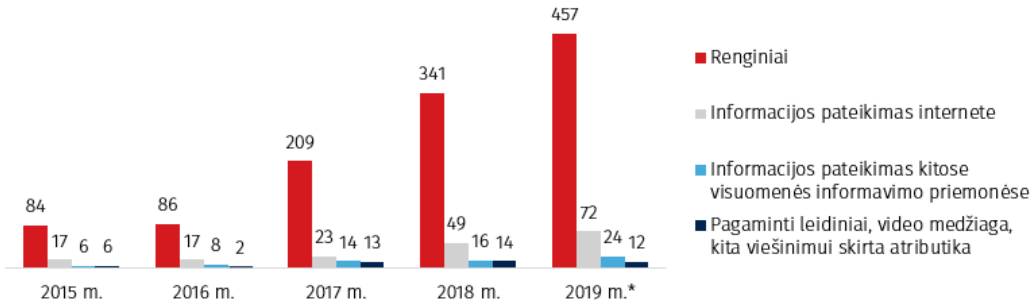
[33] 2016 m. organizuoto nusikalstamumo internete grėsmės vertinimo ataskaita (IOCTA), 13 psl., prieiga per internetą: https://www.europol.europa.eu/sites/default/files/documents; Seimo 2015-05-07 nutarimu Nr. XII-1682 patvirtinta Viešojo saugumo plėtros 2015–2025 m. programa, 45.4.2 p.

[34] Ten pat. ES Tarybos 2017-10-02 galutinė ataskaita dėl Europos kibernetinio nusikalstamumo prevencijos ir kovos su tokiu nusikalstamumu politikos praktinio įgyvendinimo ir veikimo septintojo tarpusavio vertinimo etapo, 31 psl., prieiga per internetą: http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/lt/pdf.

[35] Lietuvos policijos generalinio komisaro 2017-12-29 įsakymu Nr. 5-V-1092 patvirtintas Policijos prevencinės veiklos organizavimo aprašas, 9 ir 12–15 p.; 2016 m. organizuoto nusikalstamumo internete grėsmės vertinimo ataskaita (IOCTA), 13 psl.

[36] Pažymėtina, kad interneto stebėsena vykdoma NEE užkardymo tikslais ar siekiant surinkti NEE IT reikiamą informaciją, taip pat stebėsena gali būti atliekama užtikrinant saugumą šalyje organizuojamų ir įgyvendinamų svarbių renginių (pvz., rinkimus) metu arba kitais policijos organizaciniais klausimais.

4 pav. 2015–2019 m. policijos įgyvendintų NEE prevencinių priemonių skaičius, vnt.

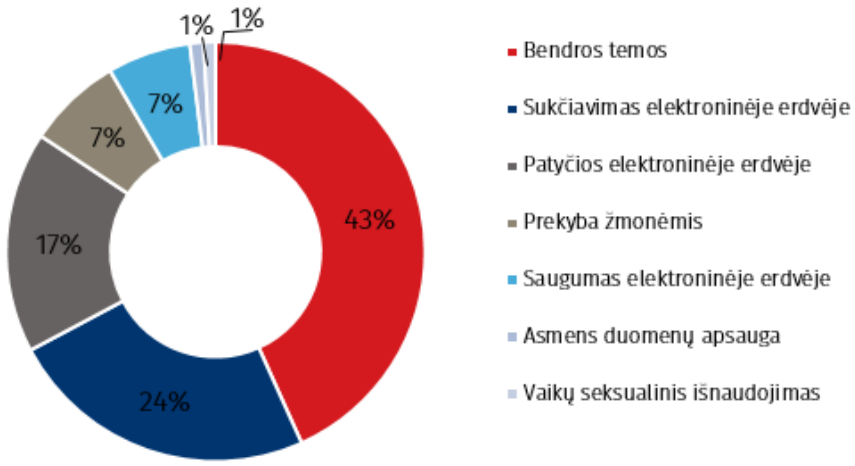


* 2019 m. sausio–spalio mėn. duomenys

Šaltinis – Valstybės kontrolė pagal AVPK pateiktą informaciją

7. Policijos įstaigose 2015–2019 m. didžioji dalis įgyvendinamų prevencinių priemonių buvo skirtos bendroms temoms[37] (43 proc. (659 iš 1523)), sukčiavimui (24 proc. (365 iš 1523) ir patyčioms elektroninėje erdvėje (17 proc. (260 iš 1523)) (žr. 5 pav.).

5 pav. Policijos 2015–2019 m. įgyvendintos NEE prevencinės priemonės pagal temas



Šaltinis – Valstybės kontrolė pagal AVPK pateiktą informaciją

8. Audito metu nustatėme, kad visuomenės šviečiamąją veiklą NEE srityje įgyvendino ir kitos institucijos: Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija[38], Valstybinė vartotojų teisių apsaugos

[37] Bendros priemonės laikytinos priemonėmis, kurios susijusios su keliomis ar visomis sritimis: asmens duomenų apsauga, patyčios, saugumas ir sukčiavimas elektroninėje erdvėje, prekyba žmonėmis elektroninėje erdvėje, vaikų pornografija.

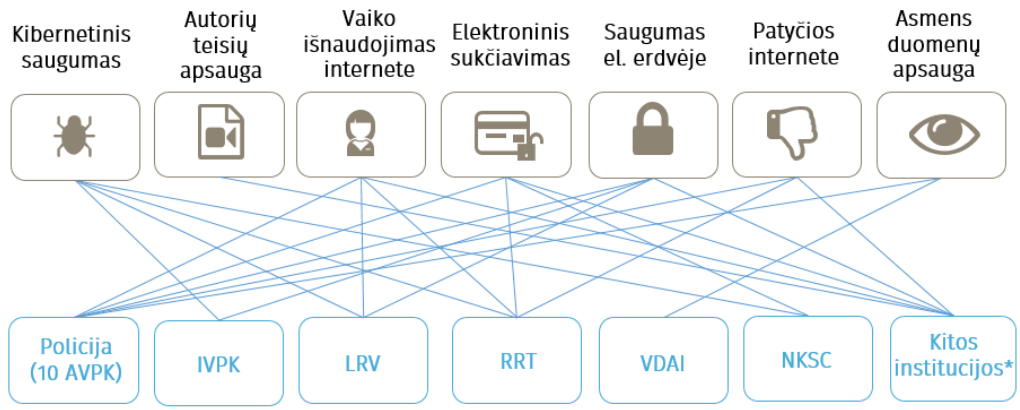
[38] Vykdoma prevencinė veikla tiek, kiek tai susiję su asmens duomenų apsauga ir šių duomenų vagystėmis.

tarnyba[39], Žurnalistų etikos inspektoriaus tarnyba[40], Kultūros ministerija[41], Informacinės visuomenės plėtros komitetas[42], Vyriausybės kanceliarija[43] (detaliau žr. 4 priede)[44].

9. Įvertinę visų minėtų institucijų įgyvendintas prevencines veiklas nustatėme, kad šalies mastu institucijų įgyvendinamos prevencinės priemonės orientuotos į IOCTA ataskaitose, teritorinio ir nacionalinio sunkaus ir organizuoto nusikalstamumo grėsmių vertinimo ataskaitose nurodytas pagrindines NEE grėsmes: elektroniniai sukčiavimai, nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui (kibernetinis nusikalstamumas), vaikų išnaudojimas pornografijai.

10. Susipažinę su visų NEE prevencinę veiklą vykdžiusių institucijų funkcijomis ir įvertinę prevencinių priemonių planavimą ir įgyvendinimą kai kuriose jų, nustatėme, kad jos veikia tik savo veiklos srityse ir pagal savo nustatytus prioritetus, bendrų NEE prevencinių priemonių neplanuoja ir jų įgyvendinimo tarpusavyje nekoordinuoja (žr. 6 pav.).

6 pav. Institucijų įgyvendintos nekoordinuotos prevencinės priemonės pagal NEE tematiką



* Valstybinė vartotojų teisių apsaugos tarnyba, Žurnalistų etikos inspektoriaus tarnyba, Kultūros ministerija.

Šaltinis – Valstybės kontrolė pagal institucijų pateiktą informaciją apie įgyvendintas NEE prevencines priemones

11. Taip organizuodamos prevencinę veiklą, institucijos įgyvendina panašias priemones (žr. pavyzdį).

Panašios prevencinės veiklos pagal temas įgyvendinimo pavyzdžiai

- Elektroninio sukčiavimo klausimais mokymus, susitikimus organizuoja ir informaciją viešumoje teikia policija, Valstybinė vartotojų teisių apsaugos tarnyba, Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, „Sustiprink imunit@ą!“ projekto vykdytojai.
- Vaiko seksualinio išnaudojimo ar kitais vaiko saugumo klausimais švietėjišką veiklą vykdo AVPK, Ryšių reguliavimo ir Žurnalistų etikos inspektoriaus tarnybos, „Sustiprink imunit@ą!“ projekto vykdytojai.

[39] Vykdoma prevencinė veikla tiek, kiek tai susiję su vartotojų teisių apsauga ir elektroniniais sukčiavimais.

[40] Vykdoma prevencinė veikla tiek, kiek tai susiję su rasistinio ir ksenofobinio pobūdžio nusikaltimais.

[41] Vykdoma prevencinė veikla tiek, kiek tai susiję su autorių teisių ir gretutinių teisių apsauga ir šio pobūdžio nusikaltimais.

[42] Vykdoma prevencinė veikla tiek, kiek tai susiję su įgyvendinamu projektu „Prisijungusi Lietuva“.

[43] Vykdoma prevencinė veikla tiek, kiek tai susiję su viešinimo kampanijos „Sustiprink imunit@ą!“ įgyvendinimu.

[44] Šis sąrašas nėra galutinis ir NEE prevencinę veiklą gali vykdyti ir daugiau institucijų, kurios pagal savo veiklos funkcijas susijusios su aktualiomis NEE grėsmėmis, pvz., bankai.

- Yra sukurtos svetainės, skirtos skelbti informaciją apie grėsmes ir pavojus internete NEE tematika, pvz., Ryšių reguliavimo tarnyba administruota svetainę www.esaugumas.lt, joje skelbiama įvairi informacija apie NEE grėsmes, kaip apsaugoti vaikus internete, nuo elektroninių klastočių, teikiami kiti patarimai kaip būti saugiau internete. „Sustiprink imunit@ą!“ projekte sukurta svetainė www.sustiprinkimuniteta.lt, kurioje teikiama informacija, kaip apsaugoti vaikus internete, kaip padėti tėvams išvengti sukčių, kaip naudotis saugiau internetu, pateikiami įvairus patarimai kaip saugiai naudotis Wi-Fi ir pan.

12. Audito metu nustatėme, kad neatliekamas prevencinės veiklos NEE srityje poveikio vertinimas. Policijoje prevencinės veiklos rezultatai vertinami remiantis kriminogeninės situacijos ir gyventojų saugumo jausmo pokyčiais[45], bet šis vertinimas atliekamas kompleksiškai, ataskaitos pagal atskiras nusikaltimo sritis, tarp jų ir NEE, nerengiamos[46], o gyventojų saugumo jausmo pokyčių vertinimai atliekami tik dėl fizinės aplinkos saugumo. Kitos institucijos poveikio vertinimo šioje srityje taip pat neatlieka[47]. Šalyje nesant NEE prevencinės veiklos poveikio matavimo sistemos, kuri sudarytų sąlygas matuoti gyventojų saugumo jausmo pokyčius ne tik fizinėje, bet ir elektroninėje erdvėje, nesudaromos sąlygos įvertinti, ar vykdomos NEE prevencinės priemonės yra veiksmingos.

13. Dėl šių prevencinės veiklos organizavimo trūkumų, auditorių vertinimu, prevencinė veikla NEE srityje nepasiekia reikiamo rezultato. Tai patvirtina 2019 m. atliktas Eurobarometro tyrimas[48]: šalyje didelė gyventojų dalis nėra pakankamai informuota apie NEE grėsmes, o rezultatai dėl gyventojų pajėgumų apsisaugoti nuo NEE grėsmių ir žinojimo apie oficialius kanalus, kuriais galima pranešti apie NEE ar kitą neteisėtą veiklą internete, nesiekia ES vidurkio (žr. 7 pav.). Pažymėtina, kad 2019 m., palyginus su 2018 m., 16 proc. padaugėjo gyventojų, kurie mano, kad nėra pajėgūs apsisaugoti nuo NEE (nuo 28 iki 44 proc.), ir Lietuva užėmė 26 vietą ES.

7 pav. Visuomenės saugumo lygis elektroninėje erdvėje

Šaltinis – Valstybės kontrolė pagal Eurobarometro 2019 m. tyrimą

[45] Lietuvos policijos generalinio komisaro 2017-12-29 įsakymu Nr. 5-V-1092 patvirtintas Policijos prevencinės veiklos organizavimo aprašas.

[46] Lietuvos kriminalinės policijos biuro 2019-07-22 pateikta informacija.

[47] Įgyvendinant su prevencija susijusius projektus („Sustiprink imunit@ą!“, „Prisijungusi Lietuva“, kt.) nustatyta, kad tam tikri visuomenės tyrimai, susiję su gyventojų elgesiu ir saugumu elektroninėje erdvėje yra atliekami, tačiau nėra kriterijų, kurie sudarytų sąlygas įvertinti atliekamos prevencinės veiklos veiksmingumą.

[48] Europos Komisijos užsakymu, 2019 m. spalio mėn. 28 ES šalyse atlikta apklausa. Iš viso dalyvavo 27 607 asmenų iš įvairių ES šalių, 1 000 iš jų buvo apklausta Lietuvoje. Prieiga per internetą: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2249.

14. Vyriausybė 1997 m. įsteigė VšĮ Nusikalstamumo prevencijos Lietuvoje centrą, kuriam buvo pavesta formuoti nusikalstamumo prevencijos politiką, inicijuoti, organizuoti ir koordinuoti šios prevencijos programas ir priemones[49], bet jis aktyvios veiklos nuo 2009 m. nevykdo[50]. Auditorių vertinimu, peržiūrėjus šio centro teisinį statusą, tikslus ir uždavinius bei išteklių poreikį, būtų galima išnaudoti jį tarpinstituciniam NEE srities prevencinės veiklos planavimui, koordinavimui ir poveikio vertinimui.

15. Siekiant, kad NEE prevencinės veiklos įgyvendinimas darytų didesnį poveikį šalies gyventojų gebėjimui atpažinti NEE grėsmes ir keltų saugumo elektroninėje erdvėje lygį, reiktų užtikrinti tarpinstitucinį prevencinės veiklos NEE srityje planavimą, koordinavimą ir poveikio matavimą.

1.2. Turi būti sudarytos sąlygos šalinti neteisėtą ir žalingą turinį elektroninėje erdvėje

16. Informacinės technologijos sudaro sąlygas skaitmenizuoti įvairią informaciją ir lengvai bei greitai padaryti ją prieinamą vartotojams internetinėje erdvėje. Bendrame informacijos sraute internete gausu ne tik vartotojams naudingos, bet ir žalingos ar neskelbtinos informacijos. Todėl, siekiant apsaugoti visuomenę nuo šių grėsmių ir užkardyti galimai vykdomus nusikaltimus, svarbu turėti veiksmingas prevencines priemones, kurios sudarytų sąlygas blokuoti ir šalinti interneto turinį, kuris gali būti žalingas jo vartotojams.

17. Siekiant sudaryti sąlygas kovoti su žalinga ir neskelbtina informacija bei kitomis nusikalstamomis veikomis internete bei užkardyti nusikaltimus, įvairioms institucijoms pagal jų priežiūros sritis yra suteikiamos blokavimo teisės taikyti privalomus nurodymus viešųjų ryšių tinklų, informacijos prieglobos, skaitmeninių paslaugų tiekėjams. Privalomus nurodymus paslaugų teikėjams blokuoti interneto svetaines ar panaikinti prieigą prie jose esančios informacijos pagal kompetenciją turi teisę duoti: policija[51], NKSC[52], Lošimų priežiūros tarnyba[53], Lietuvos bankas[54], Lietuvos radijo ir televizijos komisija[55], Ryšių reguliavimo tarnyba[56], Valstybinė vartotojų teisių apsaugos tarnyba[57]. Institucijos

[49] Vyriausybės 1997-07-21 nutarimas Nr. 788 „Dėl Nusikalstamumo prevencijos Lietuvoje centro steigimo“; Seimo 1998-06-25 nutarimu Nr. VIII-810 patvirtinti Teisinės sistemos reformos metmenys (nauja redakcija), VI skyrius.

[50] 2020-01-09 susitikime direktorius nurodė, kad šis centras nuo 2009 m. negauna finansavimo iš valstybės biudžeto, tačiau panaikintas nebuvo. Šiuo metu centras vykdo projektą, susijusį su pagalba nusikaltimų aukoms bei dalyvauja Europos nusikalstamumo prevencijos tinklo (angl. *European Crime Prevention Network*) susitikimuose.

[51] Kibernetinio saugumo įstatymas, 10 str.

[52] Ten pat, 8 str.

[53] Lošimų priežiūros tarnybos direktoriaus 2015-12-29 įsakymu Nr. DI-717 patvirtintas Galimybių pasiekti informaciją, kuri naudojama siekiant vykdyti nelegalią nuotolinių lošimų veiklą, panaikinimo užtikrinimo tvarkos aprašas.

[54] Lietuvos banko įstatymas, 42 str. 7 d.

[55] Autorių teisių ir gretutinių teisių įstatymas, 78 str. 2-4 d.

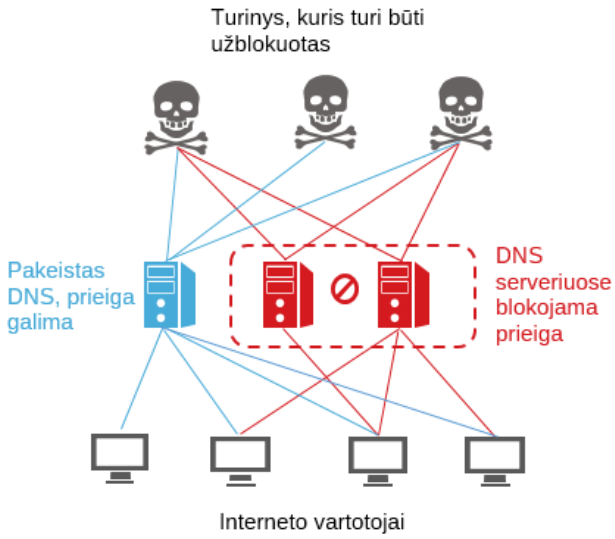
[56] Švietimo įstatymas, 23(2) str. 3 d.

[57] Vartotojų teisių apsaugos įstatymas, 49(1) str.

privalomus nurodymus viešųjų ryšių tinklų, informacijos prieglobos ar skaitmeninių paslaugų tiekėjui blokuoti DNS[58] ar IP adresus[59] gali duoti tik gavusios teismo leidimą[60].

18. Surinkus informaciją apie šalyje atliktus blokavimo veiksmus nustatyta, kad nuo 2016 iki 2020 m. vasario mėn. iš viso buvo užblokuotos 511 interneto svetainės[61]. Tačiau užblokavus, atsiranda jų veidrodinės kopijos[62]. Atlikus vien tik Lošimų priežiūros tarnybos užblokuotų interneto svetainių analizę nustatyta, kad iš visų 397 blokuotųjų 297 (75 proc.) buvo veidrodinės. Nepageidaujamą ir žalingą turinį internete platinantys asmenys geba apeiti DNS blokavimą[63], todėl ši priemonė yra tik laikino pobūdžio. Neteisėtas ir žalingas turinys nėra pašalinamas, o žalinga ir neskelbtina informacija vartotojams lieka pasiekiama. Todėl gyventojams ir toliau yra grėsmė nukentėti nuo galimai vykdomų nusikaltimų (žr. 8 pav.). Pažymėtina, kad tokia situacija didina ir administracinę naštą, nes institucijoms tenka pakartotinai kreiptis į teismus, siekiant gauti leidimą dėl blokavimo ir vėl teikti privalomus nurodymus viešųjų ryšių tinklų, informacijos prieglobos, skaitmeninių paslaugų teikėjams.

8 pav. Interneto svetainių blokavimo DNS būdu apėjimo pavyzdys



Šaltinis – Valstybės kontrolė

19. Valstybės institucijų įgaliojimus duoti privalomus nurodymus dėl interneto svetainių blokavimo ir šių įgaliojimų įgyvendinimo tvarką nustato skirtingi įstatymai, pavyzdžiui: Lietuvos banko – Lietuvos Respublikos Lietuvos banko įstatymas, Lošimų priežiūros tarnybos – Lietuvos Respublikos azartinių lošimų įstatymas, Ryšių reguliavimo tarnybos – Lietuvos Respublikos švietimo įstatymas, Valstybinės vartotojų teisių apsaugos tarnybos

[58] Domeninių vardų lygmens blokavimas, kai panaikinama prieiga prie tam tikrų puslapių (www adresų), pakeičiant domeninių vardų tarnybinę stotį (DNS).

[59] IP adresas blokuojamas, kai apribojamos paslaugos klientams užblokuojant klientui priskirtą IP adresą, iš kurio yra užfiksuota kenkėjiška veikla (pvz., kibernetiniai incidentai).

[60] Išimtys dėl teismo leidimo taikomos kibernetinių incidentų atveju, 48 valandoms paslaugų teikimą galima apriboti be teismo sankcijos, ilgesniam laikui – su apylinkės teismo sankcija.

[61] Lošimų priežiūros tarnyba užblokavo 397 svetaines, Lietuvos radijo ir televizijos komisija – 62, Lietuvos bankas – 51, Valstybinė vartotojų teisių apsaugos tarnyba – 1.

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

[63] Galimas DNS keitimas į *Open DNS, Google, Cloudflare* ir kt., yra *Proxy* serveriai, VPN (virtualus privatus tinklas), kitos technologinės priemonės, kurios sudaro sąlygas apeiti blokavimą.

– Lietuvos Respublikos vartotojų teisių apsaugos įstatymas, Lietuvos radijo ir televizijos komisijos – Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas. Šiuose įstatymuose ir poįstatyminiuose teisės aktuose nustatyta skirtinga blokavimo teisių įgyvendinimo tvarka (žr. pavyzdį).

Skirtingo DNS blokavimo teisių įgyvendinimo teisinio reglamentavimo pavyzdžiai[64]

- Nustatytas skirtingas įgyvendinimo procesas. Valstybinė vartotojų teisių apsaugos tarnyba ir Lietuvos radijo ir televizijos komisija prieš kreipdamosi į teismą su prašymu išduoti leidimą taikyti nurodymą privalo kreiptis į interneto svetainės administratorių ar pardavėją su raginimu pašalinti pažeidimus. Jei administratorius į raginimą nereaguoja, kreipiamasi į teismą. Lošimų priežiūros tarnybai, Ryšio reguliavimo tarnybai, Lietuvos bankui pareiga teikti šį raginimą nėra nustatyta.
- Nustatyti skirtingi teismo nutarties priėmimo terminai. Teismas turi priimti sprendimą dėl Lošimų priežiūros tarnybos ir Lietuvos radijo ir televizijos komisijos nurodymo per 3 kalendorines dienas, dėl Lietuvos banko – per 3 darbo dienas, dėl Valstybinės vartotojų teisių apsaugos tarnybos – per 5 kalendorines dienas. Teismo nutarties priėmimo terminas dėl Ryšių reguliavimo tarnybos nurodymo atskirai nereglamentuotas.
- Nustatyti skirtingi nurodymų įvykdymo terminai. Interneto prieigos paslaugų teikėjas turi įvykdyti Lošimų priežiūros tarnybos bei Lietuvos radijo ir televizijos komisijos nurodymą per 5 kalendorines dienas, Valstybinės vartotojų teisių apsaugos tarnybos – per 3 darbo dienas. Ryšių reguliavimo tarnybos ir Lietuvos banko nurodymo įvykdymo terminas nereglamentuotas.
- Nustatytas skirtingas nurodymų įvykdymo būdas. Reglamentuota, kad interneto prieigos paslaugų teikėjas Lošimų priežiūros tarnybos nurodymą vykdo DNS būdu, Lietuvos radijo ir televizijos komisijos – DNS arba kitais būdais, Valstybinės vartotojų teisių apsaugos tarnybos – vykdymo būdus ir priemones pasirenka savarankiškai. Ryšių reguliavimo tarnybos bei Lietuvos banko nurodymų vykdymo būdai nereglamentuoti.

20. Ryšių reguliavimo tarnybos nuomone[65], visiškai efektyvaus DNS blokavimo nėra, reikėtų orientuotis į draudžiamo turinio šalinimą toje vietoje, kur jis yra skelbiamas, pvz., su vaikų seksualiniu išnaudojimu susijęs turinys šalinamas ne blokuojant prieigą prie jo, o iš informacijos prieglobos paslaugų teikėjų tarnybinių stočių (serverių), kur yra saugomas. Be to, reikėtų vykdyti prevencines – šviečiamojo pobūdžio veiklas. Be to, tarnybos teigimu, svarstytinas blokavimo tvarkos suvienodinimo poreikis, kai vienu teisės aktu galėtų būti patvirtinta bendra nurodymų blokuoti turinį davimo ir blokavimo tvarka.

21. Lietuvos radijo ir televizijos komisijos nuomone[66], DNS blokavimo tikslas yra apriboti prieigą prie interneto svetainių, kurios pažeidžia teisės aktų reikalavimus, ir jis yra pasiekiamas. Pritariama, kad DNS blokavimo būdas nėra absoliutus ir neužtikrina svetainėje esančio turinio neprieinamumo, tačiau siekiama ieškoti efektyvesnių būdų šiai problemai spręsti.

22. 2015–2019 m. policija 181 kartą teikė nurodymus šalinti nusikalstamų veikų priežastis ir 64 kartus teikti nurodymai apriboti 48 val. paslaugų teikimą (IP adresus). IP adresų blokavimas taip pat turi trūkumų, nes jie yra dinamiški ir palyginti lengvai keičiami, todėl

[64] Azartinių lošimų įstatymas, 27^1 str. 1 d. 3, 4 p., 2 d.; Lošimų priežiūros tarnybos direktoriaus 2015-12-29 įsakymu Nr. DI-717 patvirtintas Galimybių pasiekti informaciją, kuri naudojama siekiant vykdyti nelegalią nuotolinių lošimų veiklą, panaikinimo užtikrinimo tvarkos aprašas; Lietuvos banko įstatymas, 42 str. 7 ir 8 d.; Autorių teisių ir gretutinių teisių įstatymas, 78 str.; Švietimo įstatymas, 23^2 str. 3 d.; Vartotojų teisių apsaugos įstatymas, 49^1 str.; teisingumo ministro 2019-08-28 įsakymu Nr. 1R-242 patvirtintas Privalomų nurodymų taikymo interneto prieigos paslaugų teikėjams tvarkos aprašas.

[65] Ryšių reguliavimo tarnybos 2020-05-18 pateikta nuomonė apie blokavimą.

[66] Lietuvos radijo ir televizijos komisijos 2020-05-20 raštas Nr. S-241.

paprasta išvengti apribojimo. Be to, tuo pačiu IP adresu gali dalytis keletas subjektų, todėl paslaugos gali būti apribotos ir kitiems nesusijusiems asmenims.

23. Saugumo ekspertų atlikti tyrimai[67] internete rodo, kad elektroninėje erdvėje yra daug grėsmių tapti auka, pvz., 2019 m. nustatyta per 400 interneto svetainių, kurios vagia kreditinių kortelių informaciją ir kitus asmens duomenis. Taikomos užkardymo priemonės nesudaro sąlygų interneto aplinką padaryti švaresnę ir saugesnę vartotojui. Pastebime, kad Ryšių reguliavimo tarnyba 2020 m. ėmėsi iniciatyvos dėl švarios interneto aplinkos (žr. pavyzdį).

Gerosios praktikos pavyzdys

2020-02-04 Ryšių reguliavimo tarnyba paskelbė elektroninės informacijos prieglobos paslaugų teikėjų, vykdančių veiklą Lietuvoje, memorandumą dėl švarios interneto aplinkos[68]. Paslaugų teikėjai, prisijungę prie memorandumo, įsipareigoja gavę „Notice and Take Down“ nurodymą pašalinti savo tarnybinėse stotyse (serveriuose) saugomą draudžiamą informaciją arba panaikinti galimybę ją pasiekti. 2020-04-24 duomenimis, prie memorandumo yra prisijungę beveik 10 paslaugų teikėjų, o prisijungusių skaičius nuolat didėja. Auditorių nuomone, ši iniciatyva yra geras bendradarbiavimo su ryšio operatoriais pavyzdys, siekiant mažinti elektroninėje erdvėje esančias grėsmes.

24. Siekiant šalies mastu užtikrinti rezultatyvesnį nusikalstamos veikos elektroninėje erdvėje užkardymą, mažinant galimybes gyventojams tapti NEE aukomis, siūloma numatyti priemones, kurios sudarytų sąlygas šalinti neteisėtą ir žalingą turinį internete ir užtikrinti bendrą blokavimo įgaliojimų įgyvendinimo tvarką.

[67] Prieiga per internetą: https://tyrimai.esec.lt/index.php?option=com_content&view=article&id=47:platus-tapatybes-bei-finansiniu-vagysciu-tinklas-lietuvoje&catid=2&Itemid=101.

[68] Prieiga per internetą: https://svarusinternetas.lt/memorandumas/10/?c-2/t-11.

2. KIBERNETINIŲ INCIDENTŲ VALDYMAS TURI SUDARYTI SĄLYGAS VEIKSMINGIAU IDENTIFIKUOTI NUSIKALSTAMĄ VEIKĄ ELEKTRONINĖJE ERDVĖJE

25. Kibernetinių incidentų statistika ir tyrimai rodo, kad šalyje NEE grėsmių mastas yra didelis ir auga:

    - Nacionalinio kibernetinio saugumo būklės ataskaitų duomenimis, 2015–2018 m. šalyje buvo užfiksuota beveik 200 tūkst.[69], o 2019 m. – 309 tūkst.[70] kibernetinių įvykių[71] (detalesnė informacija apie kibernetinius įvykius pateikiama 5 priede), o kibernetinių incidentų[72] mastas per paskutinius metus padidėjo beveik dvigubai: 2017 m. jų užfiksuota 1 821[73], 2018 m. – 1 701[74], 2019 m. – 3 241[75].
    - 2019 m. atlikto Eurobarometro tyrimo[76] duomenimis, 47 proc. Lietuvos gyventojų[77] per pastaruosius 3 metus susidūrė su NEE, o 1 proc.[78] – su asmeninių duomenų vagyste. Pažymėtina, kad, palyginus su 2018 m.[79], tokių gyventojų, kurie susidūrė su NEE, padaugėjo 3 proc. punktais (nuo 44 iki 47 proc.). „Swedbank“ tyrimo duomenimis [80], daugėja šalyje gyventojų, susidūrusių su elektroniniais ar telefoniniais sukčiais, kurie siekė pasinaudoti jų asmeniniais duomenimis ar pinigais (2016 m. – 21 proc.; 2019 m. – 29 proc.), ir didėja dalis gyventojų, kurie dėl to patyrė materialinės žalos (2016 m. – 9 proc., 2019 m. – 17 proc.) (žr. 9 pav.).

[69] Ryšių reguliavimo tarnybos tinklų ir informacijos saugumo departamento saugumo incidentų tyrimų skyriaus 2015 ir 2016 m. veiklos ataskaitos; Nacionalinio kibernetinio saugumo būklės 2017 ir 2018 m. ataskaitos.

[70] Nacionalinio kibernetinio saugumo būklės 2019 m. ataskaita.

[71] Pagal pasikeitusią incidentų skaičiavimo metodiką automatizuotomis priemonėmis nustatyti incidentai nuo 2019 m. traktuojami kaip kibernetiniai įvykiai.

[72] Incidentus kibernetiniams nuo 2019 m. betarpiškai apdoroja specialistas: priskiria poveikio reikšmę ir nustato kategoriją.

[73] NKSC 2020-01-17 pateikta informacija apie rankiniu būdu apdorotus kibernetinius incidentus.

[74] Ten pat.

[75] Nacionalinio kibernetinio saugumo būklės 2019 m. ataskaita.

[76] Europos Komisijos užsakymu, 2019 m. spalio mėn. 28 ES šalyse atlikta apklausa. Iš viso dalyvavo 27 607 asmenų iš įvairių ES šalių, 1 000 iš jų apklausta Lietuvoje. Prieiga per internetą: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2249.

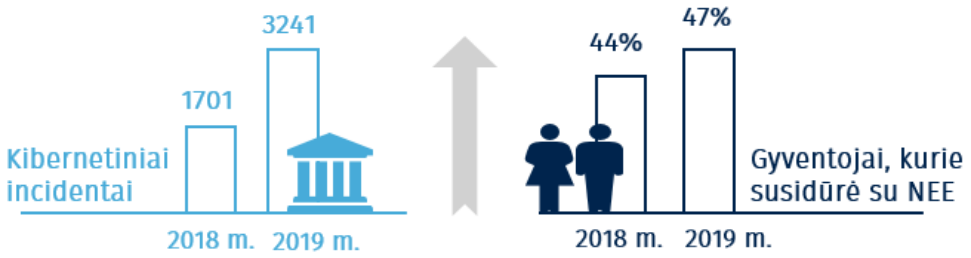
[77] Tai sudaro 984 950 gyventojų. Skaičiavimo algoritmas: 2 794 184 (2019 m. Lietuvos gyventojų skaičius pagal Statistikos departamento skelbiamą informaciją) * 75 proc. (Lietuvos gyventojai, kurie pagal Eurobarometro 2019 m. apklausą naudojasi internetu) * 47 proc. (Lietuvos gyventojai, kurie pagal Eurobarometro 2019 m. apklausą nurodė, kad per pastaruosius trejus metus jie, jų šeimos nariai ar pažįstami susidūrė su el. nusikaltimais arba buvo jų aukos) = 984 950 gyventojų.

[78] Tai sudaro 20 956 gyventojus. Skaičiavimo algoritmas: 2 794 184 (2019 m. Lietuvos gyventojų skaičius pagal Statistikos departamento skelbiamą informaciją) * 75 proc. (Lietuvos gyventojai, kurie pagal Eurobarometro 2019 m. apklausą naudojasi internetu) * 1 proc. (Lietuvos gyventojai, kurie pagal Eurobarometro 2019 m. apklausą nurodė, kad susidūrė su asmeniniu duomenų vagyste) = 20 956 gyventojai.

[79] Eurobarometro apklausa apie apsisaugojimą internete rezultatus. Ši apklausa buvo atlikta 2018 m. spalio-lapkričio mėn. Europos Komisijos užsakymu, 28 ES šalyse. Iš viso dalyvavo 27 339 asmenų iš įvairių ES šalių, 1 000 iš jų buvo apklausta Lietuvoje. Prieiga per internetą: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/85495.

[80] „Swedbank“ Finansų instituto 2020-02-20 pateikta informacija apie 2019 m. tyrimą „Gyventojų elgsenos susidūrus su telefoniniais ar elektroniniais sukčiais tyrimo“.

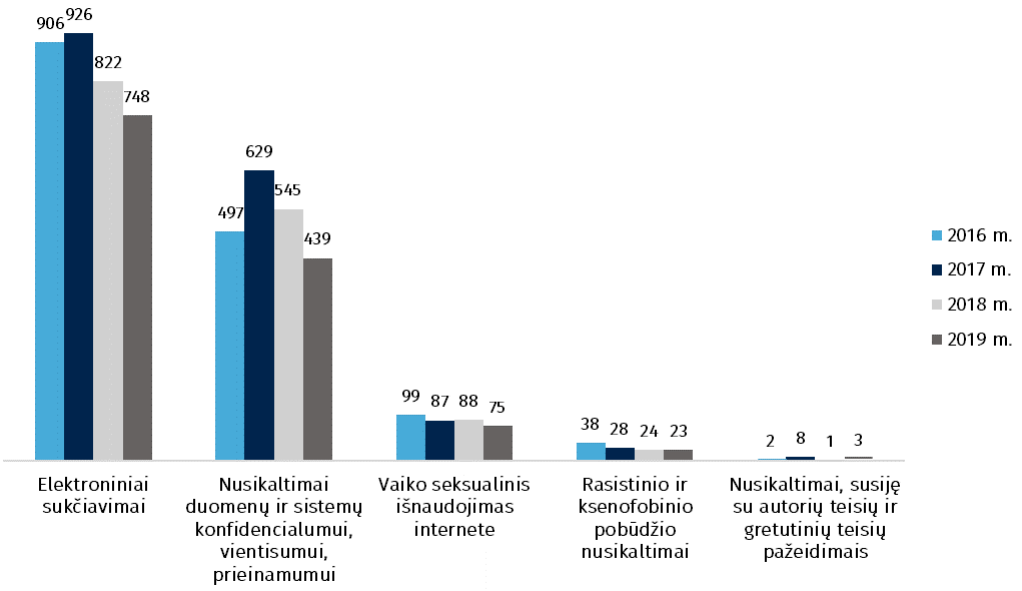
9 pav. Kibernetinių incidentų ir gyventojų, kurie susidūrė su NEE, augimo tendencija



Šaltinis – Valstybės kontrolė

26. Nusikalstamų veikų, padarytų elektroninėje erdvėje, policijoje registruojama mažai, jų apimtys pastaraisiais metais mažėja. Informatikos ir ryšių departamento duomenimis, 2019 m. Nusikalstamų veikų žinybiniame registre[81] užregistruotos 1 288 šios veikos. Nuo 2016 iki 2019 m. jų sumažėjo 17 proc. (2016 m. – 1 542, 2017 m. – 1 678, 2018 m. – 1 480, 2019 m. – 1 288) (žr. 10 pav.).

10 pav. Nusikalstamų veikų žinybiniame registre užregistruotų nusikalstamų veikų, padarytų elektroninėje erdvėje, skaičius, vnt.[82]



Šaltinis – Valstybės kontrolė pagal Informatikos ir ryšių departamento duomenis

27. Registruojamų nusikalstamų veikų, padarytų elektroninėje erdvėje, mastas ir skaičiaus mažėjimas nerodo faktinių NEE grėsmių ir jų augimo tendencijų. Kadangi tobulėjančios technologijos sudaro geresnes sąlygas elektroninėje erdvėje veikti anonimiškai, nusikalstamos veikos gali būti mažiau pastebimos. Todėl svarbu atlikti šios erdvės stebėseną, joje vykstančių įvykių, incidentų, reiškinių analizę, siekiant suprasti galimas

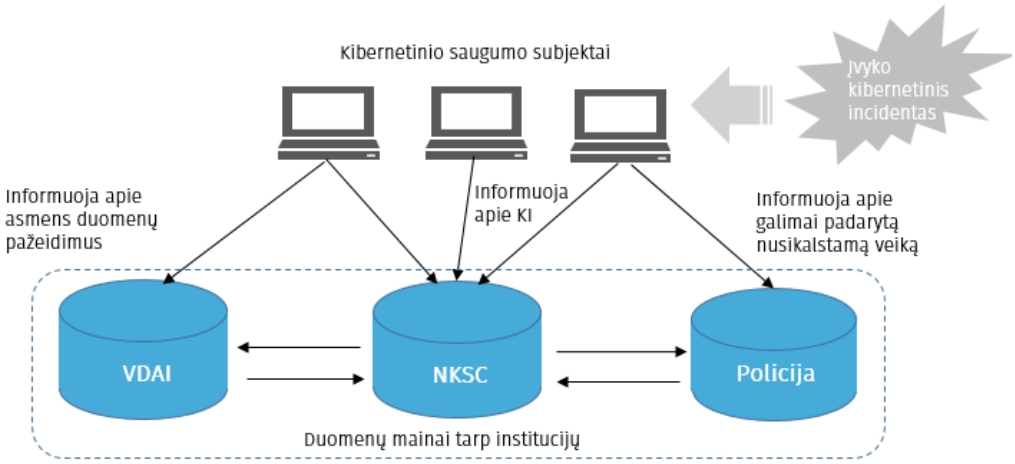
[81] 2020-06-26 pateikti duomenys iš Nusikalstamų veikų žinybinio registro apie nusikalstamas veikas elektroninėje erdvėje 2016–2019 m.

[82] Nusikalstamos veikos, padarytos elektroninėje erdvėje, pagal BK straipsnius: 145, 162, 170, 170[2], 182, 191–194, 196–198[2], 214, 215 ir 309 str. 2 ir 3 d.

NEE grėsmes ir jų mastą. Tai leistų laiku reaguoti į nusikalstamus įvykius ir užkardyti galimybę vykdyti nusikalstamas veikas.

28. Už kibernetinių incidentų valdymo organizavimą, stebėseną ir analizę nacionaliniu lygiu atsakingas NKSC. Policija ir VDAI pagal kompetenciją tiria ar dalyvauja juos valdant[83]. Apie įvykusį kibernetinį incidentą KSS[84] praneša NKSC, VDAI (jei susijęs su asmens duomenimis) ar, Lietuvos policijos generalinio komisaro nustatyta tvarka[85], teikia informaciją policijai (jei susijęs su galimai nusikalstama veika)[86] (žr. 11 pav.). KSS ir kibernetinius incidentus valdančios ir (ar) tiriančios institucijos (NKSC, policija, VDAI) tarpusavyje keičiasi aktualia informacija[87].

11 pav. Pranešimų apie kibernetinį incidentą schema



Šaltinis – Valstybės kontrolė

29. Laikytasi nuostatos, kad kibernetinių incidentų analizė, siekiant nustatyti galimus NEE, yra veiksminga, kai:

    - nustatyti kriterijai, kuriais remiantis kibernetinis incidentas priskiriamas incidentams, galimai turintiems NEE požymių [88]; nustačius kibernetinius incidentus, turinčius NEE požymių, informacija apie juos perduodama policijai[89];

[83] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Nacionalinis kibernetinių incidentų valdymo planas.

[84] Kibernetiniai saugumo subjektai: ypatingos svarbos informacinės infrastruktūros valdytojai, valstybės informacinių išteklių valdytojai ir tvarkytojai, skaitmeninių paslaugų ir prieglobos paslaugų teikėjai (vidutinės ir didelės įmonės), interneto paslaugų teikėjai. Kibernetinio saugumo subjektų yra per 500.

[85] Lietuvos policijos generalinio komisaro 2015-02-02 įsakymu Nr. 5-V-101 patvirtintas Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veiklos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetiniu incidentų tyrimo tvarkos aprašas.

[86] Kibernetinio saugumo įstatymas, 11 str.

[87] Nacionalinis kibernetinių incidentų valdymo planas, 3 p.

[88] ENISA pirmasis praktikų rinkinys „CERT ir teisėsaugos institucijų bendradarbiavimas kovojant su elektroniniais nusikaltimais“ (angl. *Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime*), 2012 m., prieiga per internetą: https://www.enisa.europa.eu/publications/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices.

[89] Kibernetinio saugumo įstatymas, 11 str., Nacionalinis kibernetinių incidentų valdymo planas, 44 p.

- policija atlieka kibernetinių incidentų, turinčių NEE požymių, stebėseną ir analizę pagal gaunamus duomenis apie kibernetinius incidentus[90] ir nustačiusi nusikalstamos veikos požymių, inicijuoja NEE ikiteisminį tyrimą[91].

30. Policijoje kibernetinių incidentų valdyme dalyvauja LKPB Sunkaus ir organizuoto nusikalstamumo tyrimo 5-oji valdyba (SO5)[92]. Šis padalinys, gavęs informaciją apie kibernetinį incidentą, turintį nusikalstamos veikos požymių, atlieka kibernetinio incidento tyrimą ir, nustatęs nusikalstamos veikos požymius, turi pradėti ikiteisminį tyrimą. Kitais atvejais ši informacija naudojama analizei ar pridedama prie kito jau pradėto kibernetinio incidento tyrimo[93].

31. Surinkus informaciją apie 2015–2019 m. NKSC, VDAI policijai teiktus pranešimus apie kibernetinius incidentus, kurie galimai yra nusikalstamos veikos, taip pat atlikę KSS, kurie atsakingi už informacinių išteklių valdymą ir tvarkymą, apklausą[94], nustatėme, kad policijai nėra teikiama visa informacija apie kibernetinius incidentus, turinčius NEE požymių:

    - NKSC neperduoda policijai informacijos apie nusikalstamas veikas, tik nurodo KSS patiems kreiptis į policiją[95];
    - VDAI duomenimis tokia informacija policijai teikta nebuvo[96];
    - 26 proc. (37 iš 143) audito metu apklaustų KSS nurodė, kad buvo nustatę atvejų, kai kibernetiniai incidentai galimai turėjo NEE požymių, tačiau iš jų daugiau nei pusė (51 proc., (19 iš 37)) nurodė, kad informacijos policijai neperdavė arba perdavė ne visais atvejais.

32. Peržiūrėjus kibernetinių incidentų valdymo mechanizmą, išanalizavus teisinį šios srities reguliavimą, nustatyta, kad policija negauna visos informacijos apie šiuos incidentus, kurie galimai yra NEE, nes:

    - *Nėra kriterijų (bendros taksonomijos), pagal kuriuos būtų galima identifikuoti, kurie kibernetiniai incidentai galimai yra NEE*. ENISA tyrime[97] pabrėžia, kad, siekiant užtikrinti būtiną policijos ir kibernetinio saugumo bendruomenės bendradarbiavimą, reikia keistis informacija pagal bendrą suderintą taksonomiją. Kibernetinio saugumo ir teisinio žodyno suderinimas gali

[90] Lietuvos policijos generalinio komisaro 2015-02-02 įsakymu Nr. 5-V-101 patvirtintas Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veiklos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetiniu incidentų tyrimo tvarkos aprašas.

[91] Lietuvos policijos generalinio komisaro 2015-02-02 įsakymas Nr. 5-V-101.

[92] Lietuvos kriminalinės policijos biuro viršininko 2016-01-19 įsakymas Nr. 38-V-22 „Dėl Lietuvos kriminalinės policijos biuro struktūrinių padalinių nuostatų ir struktūros schemų patvirtinimo“.

[93] Lietuvos policijos generalinio komisaro 2015-02-02 įsakymu Nr. 5-V-101 patvirtintas Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veiklos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetiniu incidentų tyrimo tvarkos aprašas.

[94] Siekdami įvertinti, ar KSS informuoja policiją apie kibernetinius incidentus, kurie galimai turi nusikalstamos veikos požymių, atlikome KSS apklausą. Nuo 2019-11-22 iki 2019-12-16 apklausti visi 165 www.registrai.lt duomenimis valstybės informacinių sistemų, registrų valdytojais ir/ar tvarkytojai. Į apklausą iš viso atsakė 143 (86,67 proc.) apklaustų KSS.

[95] 2019-07-02 susitikimo su Nacionalinio kibernetinio saugumo centro atstovais protokolas.

[96] VDAI 2019-08-29 raštas Nr. 2R-4066 (1.29.E).

[97] 2019 m. tyrimas „Reagavimo į saugumo incidentus tarnybų ir policijos bendradarbiavimo žemėlapis“ (angl. *Roadmap on the cooperation between CSIRTS and LE*), 25–27 psl., prieiga per internetą: https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation.

pagerinti CERT ir policijos tarpusavio supratimą apie šiuos incidentus, kurie galimai susiję su nusikalstamomis veikomis[98].

Nacionaliniame kibernetinių incidentų valdymo plane[99] yra nustatyti požymiai, pagal kuriuos šie incidentai skirstomi į kategorijas, tačiau nėra kriterijų, kurie sudarytų sąlygas tiek KSS, tiek NKSC atpažinti, kuris kibernetinis incidentas galimai susijęs su nusikalstama veika, ir perduoti informaciją policijai. Auditorių atlikta apklausa rodo, kad 32 proc. (46 iš 143) KSS nurodė, kad nėra aišku, kaip identifikuoti kibernetinį incidentą, kuris galimai yra NEE. Kaip vieną pagrindinių priežasčių 85 proc. (39 iš 46) KSS nurodė, kad nėra aiškių nusikalstamos veikos identifikavimo požymių ar kriterijų.

- *Nėra aiškios policijos informavimo apie kibernetinius incidentus, kurie galimai yra NEE, tvarkos.* Kibernetinio saugumo įstatyme įtvirtinta, kad apie įvykusius kibernetinius incidentus privaloma pranešti NKSC Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka bei Lietuvos policijos generalinio komisaro nustatyta tvarka teikti policijai informaciją, reikalingą teisės pažeidimams, turintiems nusikalstamų veikų požymių, kibernetinėje erdvėje užkardyti ir tirti.[100] Pagal šį planą kibernetinius incidentus valdančios ir tiriančios institucijos (NKSC, VDAI), gavusios informaciją apie kibernetinius incidentus ir nustačiusios, kad pastarieji gali turėti nusikalstamos veikos požymių, privalo apie juos informuoti policiją[101]. Lietuvos policijos generalinio komisaro nustatytoje tvarkoje[102] įtvirtinta, kad informacijos teikėjai vykdydami savo veiklą ir nustatę teisės pažeidimus kibernetinėje erdvėje ar kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymius, informaciją policijai gali teikti ir savo iniciatyva. T. y. nėra nustatytas imperatyvus reikalavimas KSS visais atvejais informuoti policiją[103]. Atsižvelgiant į tai, nėra aišku ar NKSC, įvertinęs informaciją apie kibernetinį incidentą ir nustačiusi, kad jis galimai turi nusikalstamos veikos požymių, privalo informuoti policiją, ar tai turi daryti KSS. Tai patvirtina ir auditorių apklausoje dalyvavę KSS: 27 proc. (39 iš 143) jų nurodė, kad nėra aišku, kam pranešti apie kibernetinius incidentus, kurie galimai yra NEE.
- *Trūksta metodinio vadovavimo, konsultacijų ir mokymų, kurie stiprintų KSS gebėjimus atpažinti ir reaguoti į nusikalstamas veikas.* ENISA[104] pastebi, kad kibernetinio saugumo bendruomenė gali nežinoti baudžiamojo proceso reikalavimų. Kita vertus, teisėsaugos institucijos gali neturėti išsamių žinių apie CSIRT veikimą ir galimybes, todėl skatintina organizuoti bendrus mokymus ir pratybas, taip stiprinant susijusių bendruomenių gebėjimus ir kompetencijas.

[98] Gerąja praktika ENISA pateikia Čekijos parengtą kibernetinio saugumo žodynėlį.

[99] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Nacionalinis kibernetinių incidentų valdymo planas.

[100] Kibernetinio saugumo įstatymas, 11 str. 1 d. 3 ir 4 p.

[101] Vyriausybės 2016-01-25 nutarimu Nr. 87 patvirtintas Nacionalinis kibernetinių incidentų valdymo planas, 16 p. (redakcija, galiojusi iki 2018-03-05) ir 15 p. (redakcija, galiojusi iki 2018-12-31), 2018-08-13 nutarimu Nr. 818 patvirtintas Nacionalinis kibernetinių incidentų valdymo planas, 44 p. (redakcija, galiojanti nuo 2019-01-01).

[102] Lietuvos policijos generalinio komisaro 2015-02-02 įsakymu Nr. 5-V-101 patvirtintas Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veiklos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetiniu incidentų tyrimo tvarkos aprašas, 4 ir 10 p.

[103] Ten pat, 12 p.

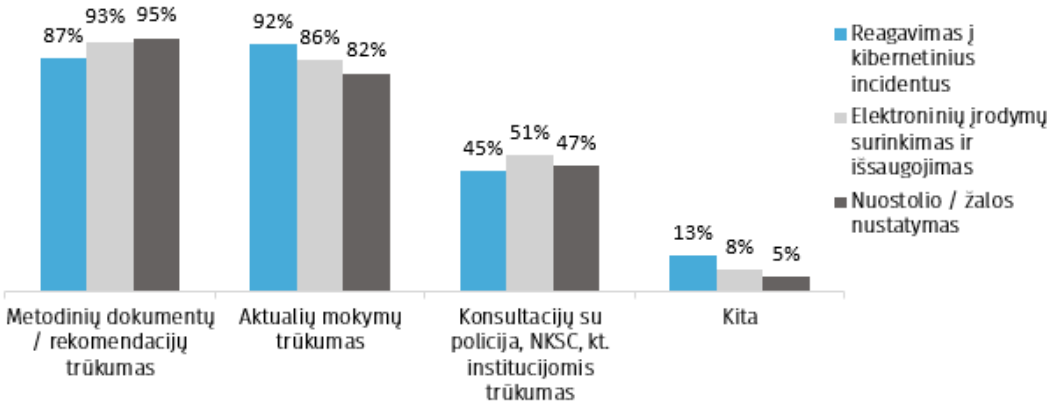
[104] 2019 m. tyrimas „Reagavimo į saugumo incidentus tarnybų ir policijos bendradarbiavimo žemėlapis“.

ENISA [105] pažymi, kad CSIRT taikomos priemonės ir veiksmai, susiję su kibernetinio incidento suvaldymu, galėtų panaikinti elektroninius įrodymus ir taip pakenkti policijos tyrimui. Saugumo standartų, taikomų elektroninių įrodymų rinkimui ir išsaugojimui, nustatymas gali padėti užtikrinti šių įrodymų priimtinumą baudžiamajame procese. NKSC organizuoja kibernetinio saugumo pratybas[106], vykdo mokymus KSS[107], bet auditorių apklausos rezultatai rodo, kad KSS nėra aišku:

- kaip įvertinti kibernetinio incidento, kuris galimai yra NEE, nuostolį ar žalą (64 proc.: 92 iš 143);
- kaip tinkamai surinkti ir išsaugoti elektroninius įrodymus, reikalingus tolesniam kibernetinio incidento tyrimui (51 proc.: 73 iš 143);
- kaip reaguoti į kibernetinius incidentus, kurie galimai yra NEE (27 proc.: 39 iš 143).

KSS nurodo, kad susiduria su minėtais neaiškumais, nes trūksta metodikų ir mokymų (vidutiniškai 89 proc.) bei konsultacijų su NKSC, policija, kitomis institucijomis (vidutiniškai 48 proc.) (žr. 12 pav.).

12 pav. Priežastys, dėl kurių KSS susiduria su neaiškumais reaguojant į kibernetinius incidentus, kurie galimai yra NEE



Šaltinis – Valstybės kontrolė pagal KSS apklausos duomenis

Lietuvoje nėra parengtų elektroninių įrodymų (įkalčių) rinkimo, analizės, išsaugojimo, kibernetinio incidento nuostolio ar žalos įvertinimo metodinių rekomendacijų. Auditorių vertinimu, šie metodiniai dokumentai ypač svarbūs siekiant nustatyti kibernetinio incidento poveikį organizacijai, kiek jis susijęs su nusikalstama veika, ir, prireikus, veiksmingai reaguoti ir tinkamai surinkti elektroninius įrodymus.

- *Nesudarytos sąlygos kibernetinius incidentus, kurie galimai yra NEE, valdyti taikant vieno langelio principą.* ENISA nurodo [108], kad CSIRT ir policijos

[105] Ten pat.

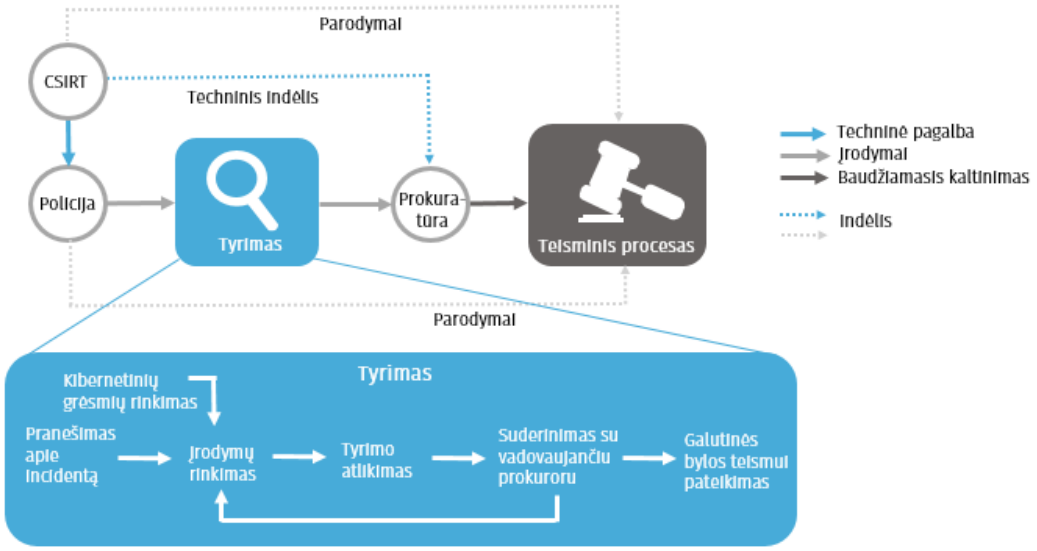
[106] Pagal Nacionalinio kibernetinio saugumo būklės 2019 m. ataskaitą nacionaliniuose kibernetinio saugumo pratybose „Kibernetinis skydas 2019“ dalyvavo per 800 specialistų iš daugiau nei 100 viešojo ir privataus sektoriaus organizacijų. Taip pat buvo organizuotos ir įgyvendintos tarptautinės pratybos.

[107] Apibendrinta informacija apie Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano įgyvendinimo 2019 m. rezultatus. Prieiga per internetą: https://www.nksc.lt/doc/saugumo_strategijos_ataskaitos /2019/TVP_ataskaita_apibendrinimas_2019m_stil.docx.

[108] 2019 m. tyrimas „Reagavimo į saugumo incidentus tarnybų ir policijos bendradarbiavimo žemėlapis“.

bendradarbiavimas ir dalijimasis turima kibernetinių įvykių ir kibernetinių incidentų informacija yra pagrindinė kibernetinio saugumo užtikrinimo veikla. Todėl reikia kurti didesnę sąveiką tarp CSIRT ir policijos (žr. 13 pav.). ENISA siūlo nustatyti bendradarbiavimo gaires ar memorandumą, detalizuoti kiekvieno vykdytojo pareigas ir atsakomybes, taip pat priemones, kuriomis užtikrinamas koordinavimas, kad būtų išvengta veiklos dubliavimo. Tokios bendradarbiavimo gairės palengvintų susijusių šalių sąveiką.

13 pav. Institucijų sąveika tiriant kibernetinius incidentus



Šaltinis – ENISA

Įvertinus, kaip LKPB SO5 ir NKSC keičiasi informacija apie kibernetinius incidentus ir kokius veiksmus atlieka juos tirdami, nustatyta, kad kibernetinių incidentų srityje bendradarbiaujama prevenciniais tikslais, t. y. policija periodiškai užklausia NKSC, kurie IP[109] adresai[110] susiję su pasikartojančiais kibernetiniais incidentais, vėliau imasi iniciatyvos laikinai blokuoti juos, jei interneto tiekėjai ar vartotojai nepašalina incidento priežasties. Tačiau policija ir NKSC nesikeičia turimais duomenimis apie elektroninėje erdvėje vykstančius įvykius ir incidentus, kurių analizė galėtų suteikti policijai daug žvalgybinės informacijos apie elektroninėje erdvėje vykstančius nusikalstamus reiškinius.

Kibernetinio saugumo taryboje nuo 2015 m. diskutuojama[111] dėl kibernetinių incidentų valdymo vieno langelio principu (kai visi incidentai patenka į NKSC, kur atliekama jų analizė ir tolesnis nukreipimas atitinkamoms tarnyboms), kuris galėtų prisidėti prie efektyvesnio jų įvertinimo ir valdymo. Iki šiol sprendimų dėl tokio principo taikymo nepriimta. ENISA pažymi[112], kad CSIRT ir teisėsaugos institucijų kultūriniai skirtumai laikomi svarbiausia bendradarbiavimo ir keitimosi informacija kliūtimi, todėl svarbu taikyti priemones, kurios sudarytų sąlygas mažinti šiuos skirtumus. Auditorių vertinimu, vieno langelio principas yra vienas iš būdų, kuris

[109] IP adresas – 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. Vidutiniškai nuo 15 iki 30 IP adresų per metus.

[110] Vidutiniškai nuo 15 iki 30 IP adresų per metus.

[111] Kibernetinio saugumo tarybos posėdžių protokolai: 2015-07-24 Nr. VLK-32-(14.3), 2018-05-02 Nr. VLK-25-(14.7).

[112] ENISA 2019 m. tyrimas „Reagavimo į saugumo incidentus tarnybų ir policijos bendradarbiavimo žemėlapis“.

galėtų prisidėti prie glaudesnio NKSC ir policijos bendradarbiavimo ir tarpusavio sąveikos valdant kibernetinius incidentus.

- *NEE būdingas latentiškumas*[113]. Mokslinėje literatūroje nurodoma[114], kad dėl latentiškumo, kuris būdingas visoms nusikalstamoms veikoms, padarytoms elektroninėje erdvėje, institucijoms sunku jas identifikuoti. Be to, policijai gali būti nepranešama apie kibernetinius incidentus, kurie galima yra NEE, dėl tokių priežasčių kaip, pvz., siekiama išvengti galimų išlaidų ir nepatogumų, kurie neigiamai gali įtakoti institucijų ar įmonių veiklą dėl pradėto tyrimo (pvz., kompiuterių paėmimas), nenoras pakenkti institucijos reputacijai. Gali būti nepranešama ir tada, kai padaroma nedidelė žala.

33. Nepaisant nurodytų priežasčių, dėl kurių policija negauna visos informacijos apie kibernetinius incidentus, kurie galimai yra NEE, nustatyta, kad LKPB pajėgumai, skirti atlikti visapusę tokių incidentų stebėseną ir analizę, yra nepakankami. LKPB SO5 su kibernetiniais incidentais dirba vienas pareigūnas[115], per 2015–2019 m. LKPB SO5 savo iniciatyva atliko 9 jų tyrimus. Auditorių vertinimu, ištekliai nėra pakankami, norint užtikrinti veiksmingą elektroninės erdvės įvykių analizę.

34. Pažymėtina, kad siekiant gauti reikiamą informaciją apie kibernetinį incidentą, kuris galimai yra NEE, NKSC tobulina jo pranešimo formą[116]. Policija siūlo ją integruoti su elektroninių paslaugų portalu (www.epolicija.lt), kuriame kibernetinio saugumo subjektai, pranešdami apie kibernetinį incidentą, iš karto galės pranešti ir apie galimai vykdomą nusikalstamą veiką. Auditorių vertinimu, šis pokytis yra teigiamas, tačiau išlieka rizika, kad kibernetinio saugumo subjektai nepraneš apie galimai nusikalstamas veikas policijai, nes neturi reikiamos kompetencijos ir gebėjimų identifikuoti, kurie kibernetiniai incidentai galimai yra NEE.

35. Siekiant gerinti kibernetinių incidentų, kurie galimai yra NEE, identifikavimą, reikia tobulinti esamą valdymo mechanizmą, kuris užtikrintų visų jų privalomą pateikimą vieno langelio principu. Turėtų būti užtikrinta, kad šiuo principu būtų atliekama jų analizė ir tyrimai, užtikrinant didesnę NKSC ir LKPB darbo sąveiką, turimų techninių ir kitų pajėgumų panaudojimą. Siekiant sustiprinti policijos ir NKSC bendradarbiavimą, dalijimąsi turima kibernetinių incidentų informacija, turi būti nustatytos detalios jų bendradarbiavimo gairės. Be to, turi būti suderinta kibernetinio saugumo incidentų ir NEE taksonomija, kuri leistų identifikuoti, kurie kibernetiniai incidentai galimai yra NEE.

36. Nepaisant to, kad bus sukurtas vieno langelio principu veikiantis incidentų valdymo mechanizmas, KSS yra atsakingi už tvarkomų informacinių išteklių saugumą. Siekiant užtikrinti KSS reikiamus gebėjimus identifikuoti kibernetinius incidentus, kurie galimai yra NEE, ir tinkamai reaguoti į juos, siūlome policijai ir NKSC organizuoti bendrus mokymus, kuriuose KSS būtų suteiktos reikiamos teisinės ir techninės žinios, susijusios su NEE, ir parengti KSS metodinius dokumentus dėl incidento žalos ar nuostolio įvertinimo, elektroninių įrodymų rinkimo ir išsaugojimo.

---

[113] Latentinis nusikalstamumas (lot. latens – „nepastebėtas“, „nepastebimas“), padarytų bet nepatekusių į apskaitą, neužregistruotų ar neatskleistų nusikalstamų veikų visumos raiškos procesai. Visuotinė lietuvių enciklopedija, T. XI (Kremacija-Lenzo taisyklė). – Vilnius: Mokslo ir enciklopedijų leidybos institutas, 2007. 559 psl.

[114] D. Štilis, P. Pakutinskas, M. Laurinaitis, I. Dauparaitė. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai. Vilnius: MRU, 2011, 38 psl.

[115] 2019-05-26 susitikimo su Lietuvos kriminalinės policijos biuro atstovais protokolas.

[116] Lietuvos kriminalinės policijos biuro 2020-04-29 pateikta informacija.

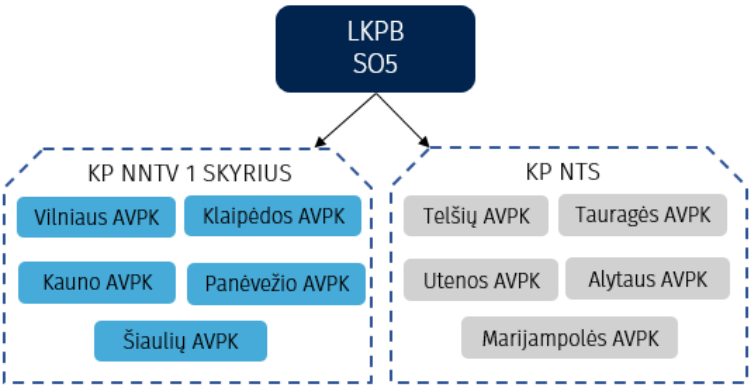
3. TURĖTŲ BŪTI SUDARYTOS SĄLYGOS GERINTI NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE TYRIMŲ REZULTATYVUMĄ

37. Baudžiamojo proceso paskirtis – ginant žmogaus ir piliečio teisės ir laisves visuomenės ir valstybės interesus greitai, išsamiai atskleisti nusikalstamas veikas ir tinkamai pritaikyti įstatymą, kad nusikalstamą veiką padaręs asmuo būtų teisingai nubaustas[117].

38. NEE tyrimai ir jų koordinavimas organizuojamas dviem lygmenimis:

- nacionaliniu lygmeniu veikia LKPB SO5, kurios tikslas pagal kompetenciją vykdyti NEE, kurie yra tarptautinio pobūdžio, sukėlė didelį atgarsį visuomenėje, daro didelę žalą valstybei ar asmenims, užkardymą, atskleidimą ir tyrimą. SO5 koordinuoja AVPK atliekamus NEE tyrimus, užtikrina Konvencijos dėl elektroninių nusikaltimų 24/7 ryšio punkto veiklą šalies mastu[118].
- visuose apskričių vyriausiuose policijos komisariatuose, įgyvendinant kriminalinės policijos pertvarką, 2015 m. pradėjo veikti kriminalinės policijos NEE specializuoti padaliniai: Vilniaus, Kauno, Panevėžio, Šiaulių, Klaipėdos apskričių vyriausiųjų policijos komisariatų Kriminalinės policijos Nusikaltimų nuosavybei tyrimo valdybų atskiri skyriai ir Utenos, Alytaus, Marijampolės, Tauragės, Telšių apskričių vyriausiųjų policijos komisariatų Nusikaltimų tyrimų skyriai, kuriuose atskiro struktūrinio padalinio NEE sričiai nėra, tačiau juose dirba šioje srityje besispecializuojantys pareigūnai. Šiems padaliniams pavesta savo teritorijoje užkardyti, atskleisti ir tirti nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, elektroninėje erdvėje padarytas nusikalstamas veikas[119] (žr. 14 pav.).

14 pav. NEE specializuotų padalinių organizacinė struktūra



Šaltinis – Valstybės kontrolė pagal LKPB informaciją

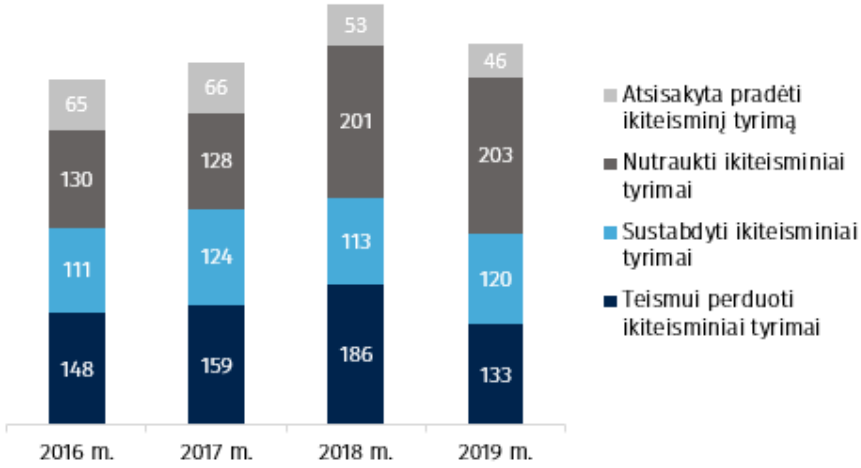
[117] BPK, 1 str.

[118] Lietuvos kriminalinės policijos biuro viršininko 2016-01-19 įsakymas Nr. 38-V-22 „Dėl Lietuvos kriminalinės policijos biuro struktūrinių padalinių nuostatų ir struktūros schemų patvirtinimo“.

[119] Lietuvos policijos generalinio komisaro 2014-05-23 įsakymu Nr. 5-V-476 patvirtinti pavyzdiniai AVPK KP NNTV nuostatai, 1.13 p.

39. Per 2016–2019 m. visose KP NEE specializuotuose padaliniuose pradėta 1 728 NEE ikiteisminių tyrimų[120] (2016 m. – 406, 2017 m. – 495, 2018 m. – 418, 2019 m. – 409). Šiuo laikotarpiu juose priimti 662 sprendimai nutraukti ikiteisminį tyrimą, 626 perduoti į teismą, 468 sustabdyti ir 230 atsisakyti pradėti ikiteisminį tyrimą (žr. 15 pav.).

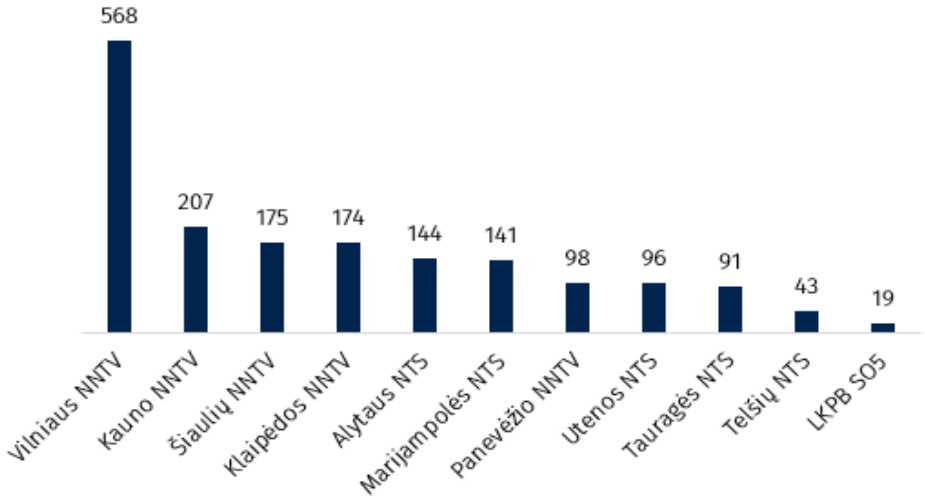
15 pav. KP NEE specializuotose padaliniuose priimtų procesinių sprendimų 2016–2019 m. skaičius, vnt.



Šaltinis – Valstybės kontrolė pagal LKPB pateiktus duomenis

40. Lyginant KP NEE specializuotus padalinius, daugiausiai 2016–2019 m. NEE ikiteisminių tyrimų atliko Vilniaus, Kauno, Šiaulių ir Klaipėdos AVPK KP NEE specializuoti padaliniai (žr. 16 pav.).

16 pav. Baigtų (nutrauktų, sustabdytų ir perduotų į teismą) NEE ikiteisminių tyrimų 2016–2019 m. skaičius, vnt.



Šaltinis – Valstybės kontrolė pagal LKPB pateiktus duomenis

[120] Ikiteisminiai tyrimai pagal BK straipsnius: 145, 170, 1702 – rasistinio ir ksenofobinio pobūdžio nusikaltimai; 191–194 – autorinių ir gretutinių teisių pažeidimai; 196–1982 – nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui; 182, 214, 215, 300 – elektroniniai sukčiavimai; 162, 309 – disponavimas pornografinio turinio dalykais, vaiko išnaudojimas pornografijai (pagal Lietuvos policijos generalinio komisaro 2014-10-17 įsakymu Nr. 5-V-890 patvirtintą Policijos įstaigų padalinių kompetencijų atlikti ikiteisminius tyrimus aprašą specializuoti padaliniai tiria visas 309 str. nusikalstamas veikas, padarytas elektroninėje erdvėje).

41. Laikytasi nuostatos, kad KP NEE specializuotiems padaliniams sudarytos sąlygos rezultatyviai atlikti NEE ikiteisminius tyrimus, kai:

    - atsižvelgiant į darbo krūvius planuojami žmogiškieji ištekliai: vienam NEE ikiteisminius tyrimus atliekančiam pareigūnui vienu metu tenka ne daugiau kaip 6 NEE ikiteisminiai tyrimai, neužimtų NEE tiriančių policijos padalinių pareigybių procentinė dalis sudaro mažiau nei 10 proc.[121];
    - visus NEE ikiteisminius tyrimus atlieka specializuoti policijos pareigūnai, o jiems vadovauja NEE srityje specializuoti prokurorai, funkcionuoja besispecializuojančių pareigūnų ir prokurorų tinklas [122];
    - parengtos specializuotos NEE srities mokymų programos, mokymai atitinka NEE tiriančių pareigūnų ir prokurorų poreikius ir IOCTA ataskaitose rekomenduojamas mokymų kryptis, šie mokymai organizuojami kasmet visiems specializuotiems pareigūnams ir prokurorams, organizuojami bendri mokymai pareigūnams, prokurorams, teisėjams[123];
    - 90 proc. pareigūnų ir prokurorų pakanka metodinių priemonių dėl NEE ištyrimo[124].

3.1. Specializuotų padalinių valdymo modelis turi būti tobulinamas

42. Nuo 2015 m. įgyvendinta kriminalinės policijos reforma [125], kurios metu sukūrus specializuotus nusikaltimų elektroninėje erdvėje padalinius buvo žengtas svarbus žingsnis kovoje su šio pobūdžio nusikaltimais. Remiantis atliktais skaičiavimais pagal LKPB pateiktus NEE ikiteisminių tyrimų duomenis už 2016–2019 m.[126] bei peržiūrėjus LKPB[127] ir GP[128] atliktų tikrinimų ataskaitas, atlikome visų KP NEE specializuotų padalinių rezultatyvumo vertinimą. Nustatyta, kad šių padalinių rezultatyvumas nepakankamas:

[121] CobiT 4.1 metodika – PO7 „Žmogiškųjų išteklių valdymas“, 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.

[122] Bendras komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“ (COM/2000/0890 final), prieiga per internetą: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52000DC0890; 2017 m. ES Tarybos ataskaita, prieiga per internetą: http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf.

[123] Ten pat, Organizuoto nusikalstamumo internete grėsmės vertinimo ataskaitos (IOCTA): 2016 m., prieiga per internetą: https://www.europol.europa.eu/sites/default/files/documents; 2018 m., prieiga per internetą: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

[124] Generalinio prokuroro 2013-05-10 įsakymu Nr. I-123 patvirtintas Lietuvos Respublikos prokuratūros ilgalaikis 2013–2023 m. strateginis veiklos planas, 13.10.2 p. (2019-02-01 įsakymo Nr. I-31 redakcija).

[125] Lietuvos policijos generalinio komisaro 2014-08-28 įsakymas Nr. 5-V-779 „Dėl teritorinių policijos įstaigų kriminalinės policijos veiklos organizavimo pakeitimo metmenų patvirtinimo“.

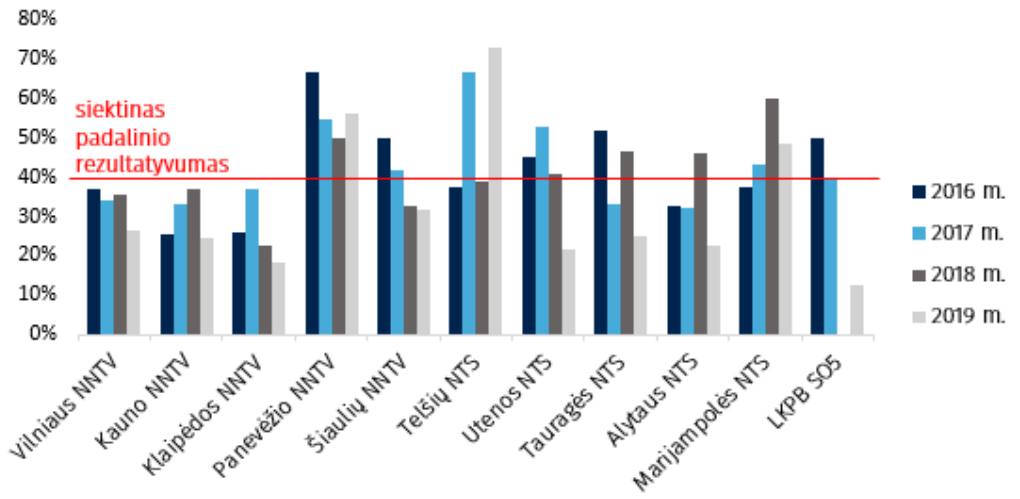
[126] Lietuvos kriminalinės policijos biuro 2019-07-10, 2020-01-17, 2020-02-13 pateikta NEE ikiteisminių tyrimų informacija.

[127] Lietuvos kriminalinės policijos biuro VKKV veiklos patikrinimo ataskaitos: Vilniaus AVPK KP NNTV 2019-04-12, Kauno AVPK KP NNTV 2019-11-05, Klaipėdos AVPK KP NNTV 2018-10-30, Šiaulių AVPK KP NNTV 2020-02-03, Tauragės AVPK KP NTS 2018-11-27, Utenos AVPK KP NTS 2018-04-23, Marijampolės AVPK KP NTS 2018-05-11.

[128] Generalinės prokuratūros Baudžiamojo persekiojimo departamento patikrinimų pažymos dėl BK XXX sk. numatytų nusikalstamų veikų: 2019-06-13 Nr. 17.9-8352, 2018-12-27 Nr. 17.9.-18397, 2018-08-03 Nr. 17.9.-11140, 2019-05-27 Nr. 17.9.-7497, 2017-07-07 Nr. 17.9.-3949, 2020-02-28 Nr. 17.9.-3057.

- *Mažėja perduotų į teismą NEE ikiteisminių tyrimų.* Vadovaujantis LKPB vidaus kontrolės tvarka[129], AVPK KP specializuotų padalinių veiklos rezultatyvumas yra aukštas, kai į teismą perduotų ikiteisminių tyrimų dalis nuo visų baigtų ikiteisminių tyrimų sudaro ne mažiau kaip 40 proc. Nustatyta, kad 2016–2019 m. vidutinis visų KP NEE specializuotų padalinių ikiteisminių tyrimų rezultatyvumas siekė 36 proc. (2016 m. – 38 proc., 2017 m. – 39 proc., 2018 m. – 37 proc., 2019 m. – 29 proc.). 2019 m., palyginus su 2016 m., šis rodiklis sumažėjo 9 proc. punktais. 7 iš 10 AVPK KP NEE specializuotų padalinių 2019 m. veiklos rezultatyvumas yra žemesnis, negu siektinas (žr. 17 pav.).

17 pav. AVPK KP NEE specializuotų padalinių veiklos rezultatyvumas 2016–2019 m.



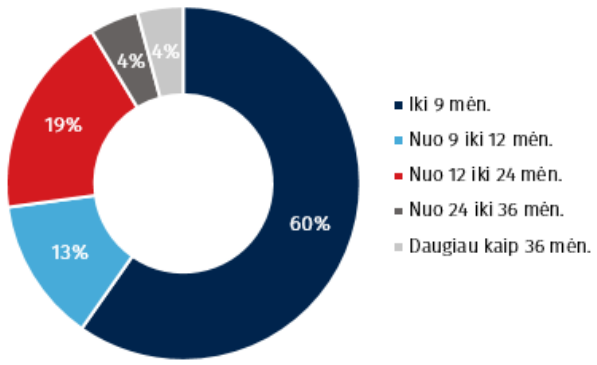
Šaltinis – Valstybės kontrolė pagal LKPB pateiktus ikiteisminių tyrimų duomenis

- *Daugiau negu trečdalis NEE ikiteisminių tyrimų trunka daugiau nei 9 mėn.* NEE pagal pavojingumą yra baudžiamieji nusižengimai bei nusikaltimai, priskirtini prie nesunkių, apysunkių ir sunkių nusikaltimų. Ikiteisminis tyrimas turi būti atliktas per kuo trumpesnius terminus, bet dėl sunkių nusikaltimų ne ilgiau kaip per 9 mėn. Dėl bylos sudėtingumo, didelės apimties ar kitų svarbių aplinkybių terminai gali būti pratęsti[130]. Nustatyta, kad 2016–2019 m. visų KP NEE specializuotų padalinių NEE ikiteisminių tyrimų, trunkančių ilgiau nei 9 mėn., dalis nuo atliekamų ikiteisminių tyrimų vidutiniškai kasmet sudaro 44 proc. (2016 m. tokie ikiteisminiai tyrimai vidutiniškai sudarė 47 proc., 2017 m. – 48 proc., 2018 m. – 46 proc., 2019 m. – 31 proc.). 2019 m., palyginus su 2016 m., matoma ikiteisminių tyrimų trukmės mažėjimo tendencija. Tačiau išanalizavę 2016–2019 m. baigtų ikiteisminių tyrimų trukmę, nustatėme, kad 40 proc. jų trunka daugiau nei 9 mėn. (žr. 18 pav.).

[129] 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.

[130] BPK, 176 str. 2 d.

18 pav. 2016–2019 m. NEE ikiteisminių tyrimų KP NEE specializuotose padaliniuose pasiskirstymas pagal trukmę



Šaltinis – Valstybės kontrole pagal LKPB pateiktus ikiteisminių tyrimų duomenis

- *Nustatomi trūkumai, priimant procesinius sprendimus atsisakyti pradėti, sustabdyti ar nutraukti ikiteisminį tyrimą*. Baudžiamojo proceso paskirtis yra išsamiai atskleisti nusikalstamas veikas ir tinkamai pritaikyti įstatymą, kad nusikalstamą veiką padaręs asmuo būtų teisingai nubaustas ir niekas nekaltas nebūtų nuteistas[131]. Generalinės ir teritorinių prokuratūrų aukštesnieji prokurorai atlieka NEE srities [132] nutrauktų, sustabdytų ikiteisminių tyrimų ar atsisakymų pradėti jį patikrinimus, pagal poreikį atlieka kitus tikrinimus[133]. Pagal pateiktas tikrinimų ataskaitas 2017–2019 m.[134] nustatyta, kad vidutiniškai 11 proc. (21 iš 191) tikrintų NEE ikiteisminių tyrimų procesinių sprendimų sustabdyti, nutraukti ar atsisakyti pradėti ikiteisminį tyrimą buvo panaikinti kaip nepagrįsti (žr. 1 lentelę).

1 lentelė. Generalinės ir teritorinių prokuratūrų specializuotų prokurorų atlikti NEE ikiteisminių tyrimų (BK XXX sk.) tikrinimai

Metai	Tikrinimo laikotarpis pagal tikrinimus	Tikrinti procesiniai sprendimai	Tikrintų ikiteisminių tyrimų skaičius	Panaikintų sprendimų skaičius	Panaikintų sprendimų dalis, nuo tikrintų ikiteisminių tyrimų
2017	2016-07-01 – 2016-12-31	Nutraukti ikiteisminiai tyrimai	14	2	14 proc.
2018	2018-01-01 – 2018-03-30	Nutraukti ir atsisakymai pradėti ikiteisminį tyrimą	52	–	–
2019	2019-01-01 – 2019-03-30	Sustabdyti ikiteisminiai tyrimai	24	2	8 proc.
2019	2019-01-01 – 2019-03-30	Nutraukti ikiteisminiai tyrimai	14	3	21 proc.
2019	2019-01-01 – 2019-03-30	Atsisakymai pradėti ikiteisminį tyrimą	42	6	14 proc.
2019	2019-04-01 – 2019-10-31	Nutraukti ikiteisminiai tyrimai	45	8	18 proc.

Šaltinis – Valstybės kontrolė pagal GP pateiktas tikrinimo pažymas

[131] BPK, 1 str.

[132] BK XXX sk. „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui“.

[133] Generalinio prokuroro 2011-04-05 įsakymu Nr. I-81 patvirtinti Baudžiamojo persekiojimo departamento nuostatai, 8 p.; 2017-04-28 įsakymas Nr. I-131 „Dėl atsisakymų pradėti ikiteisminį tyrimą kontrolės“.

[134] Apskaičiuota pagal Generalinės prokuratūros Baudžiamojo persekiojimo departamento patikrinimų pažymas dėl BK XXX sk. numatytų nusikalstamų veikų: 2020-02-28 Nr. 17.9.-3057, 2019-05-27 Nr. 17.9.-7497, 2019-06-13 Nr. 17.9-8352, 2019-06-27 Nr. 17.9.-8780, 2018-08-03 Nr. 17.9.-11140, 2017-07-07 Nr. 17.9.-3949.

Aukštesnieji prokurorai, atlikdami tikrinimus nustato, kad ne visais atvejais buvo kreiptasi į užsienio valstybes, siekiant gauti tyrimui svarbios informacijos, netinkamai kvalifikuojamos veikos ir nepradedami ikiteisminiai tyrimai pagal kitus susijusius BK straipsnius, neišsamiai atliekami ikiteisminiai tyrimai, nutarimuose daromos išvados prieštarauja tyrimo metu nustatytoms faktinėms aplinkybėms, laiku neatlikti ikiteisminio tyrimo veiksmai, neapklaustas įtariamasis, neatliktos kratos, neištirta kompiuterinė ir kita technika, neatliktos jų apžiūros, kt.

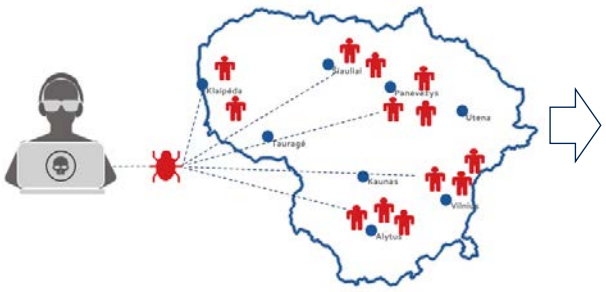
43. Pažymėtina, kad NEE ikiteisminiai tyrimai, kuriems būdingas sistemiškumas, yra sudėtingi ir komplikuoti, nes vykdant šio pobūdžio nusikaltimus naudojama daug įvairių technologinių išteklių. Be to, NEE vykdantys asmenys gali veikti gerai organizuotose grupėse kartu su įvairiose pasaulio šalyse esančiais bendrininkais, todėl kreipiamasi į kitas valstybes, kurios turi ikiteisminiam tyrimui reikšmingų duomenų (informacijos)[135]. Dėl šių aplinkybių NEE ikiteisminiai tyrimai gali užtrukti ilgiau, o tolimesniam tyrimui negavus reikiamos informacijos, jie gali būti nutraukiami ar sustabdomi, todėl pasiekti aukštą veiklos rezultatyvumą yra sudėtinga.

44. Specializuotų padalinių veiklos nepakankamą rezultatyvumui turi įtakos toliau nurodyti valdymo trūkumai.

3.1.1. Sisteminių nusikaltimų elektroninėje erdvėje identifikavimas šalies mastu turi būti veiksmingesnis

45. Vienas svarbiausių AVPK KP NEE specializuotų padalinių veiklos prioritetų yra sisteminiai nusikaltimai[136]. Pagal LKPB pateiktą apibrėžtį – tai dvi ar daugiau apibrėžtu laikotarpiu, apibrėžtoje teritorijoje padarytos tapačios ar panašios nusikalstamos veikos, kurias identifikuoja tokie požymiai: tapatus padarymo būdas (*modus operandi*), vienodas pasikėsinimo dalykas (objektas), panašus nusikalstamos veikos padarymo braižas, tas pats šią veiką padaręs asmuo[137] (žr. pavyzdį 19 pav.).

19 pav. NEE sisteminių nusikaltimų pavyzdys



Tinklalapiuose siūlomas greitas praturtėjimas. Rodomos melagingos įžymių žmonių nuotraukos ir prabangos daiktai, kurių įsigijimui siūloma greitai uždirbti. Aukoms užregistravus platformose, skambina „brokeriai" ir pasiūlo investavimo paslaugas. Atlikus investicijas, pinigai prarandami. Dėl tokių veikų 2019-2020 m. pradėta per 40 ikiteisminių tyrimų. Bendra žala viršija 800 000 Eur.

Šaltinis – Valstybės Kontrolė pagal LKPB pateiktą informaciją

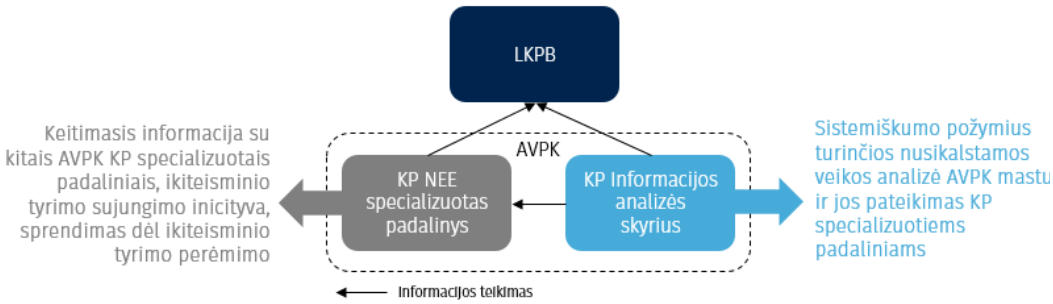
[135] Prieiga per internetą: https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasis-persekiojimas/nusikaltimai-elektronineje-erdveje/185.

[136] Lietuvos policijos generalinio komisaro 2014-08-28 įsakymas Nr. 5-V-779 „Dėl teritorinių policijos įstaigų kriminalinės policijos veiklos organizavimo pakeitimo metmenų patvirtinimo".

[137] Lietuvos kriminalinės policijos biuro 2020-03-27 pateikti pavyzdžiai, schema, lentelės, susirašinėjimas ir kita informacija apie sisteminius nusikaltimus.

46. Nusikaltimai kibernetinėje aplinkoje neturi atskirų teritorijų, ribų, jie dažniausiai įgyvendinami visoje šalies teritorijoje. Siekiant nustatyti nusikalstamų veikų sistemiškumą, AVPK lygmeniu atliekamas pirminis vertinimas pagal žinybiniuose registruose ir informacinėse sistemose esančią informaciją. Vėliau turi būti atliekama detalesnė analizė, vertinamos aplinkybės kiekvienos nusikalstamos veikos, turinčios sistemiškumo požymių[138]. AVPK KP NEE specializuotų padalinių vadovai, nagrinėdami iš AVPK KP Informacijos analizės skyriaus periodiškai gaunamas nusikalstamų veikų suvestines ir pažymas, turi vertinti nusikaltimų sistemiškumą ir inicijuoti susijusių nusikalstamų veikų sujungimą[139]. AVPK KP NEE specializuotų padalinių vadovai privalo informuoti LKPB Veiklos koordinavimo ir kontrolės valdybą apie jų teritorijoje nustatytus sisteminius nusikaltimus, o ši gautą informaciją apibendrina ir teikia siūlymus LKPB viršininkui ir PD Veiklos analizės ir kontrolės valdybai (žr. 20 pav.)[140].

20 pav. Sisteminių nusikaltimų identifikavimo ir keitimosi informacija schema



Šaltinis – Valstybės kontrolė pagal LKPB duomenis

47. Įvertinus LKPB pateiktą informaciją apie sisteminius nusikaltimus[141] ir LKPB Veiklos koordinavimo ir kontrolės valdybos septynių AVPK KP NEE[142] specializuotų padalinių veiklos patikrinimo ataskaitose pateikiamą informaciją nustatyta, kad AVPK lygiu atliekama šių nusikaltimų analizė. Tačiau ne visi su jais susiję atvejai identifikuojami, nes GP nuo 2019 m. atlieka NEE ikiteisminių tyrimų, kurie turi sistemiškumo požymių, stebėseną ir nustato, kad skirtingose teritorijose tiriamos nusikalstamos veikos yra to paties nusikaltimo epizodai, tačiau jie nėra identifikuojami kaip sisteminio nusikaltimo dalis ir nesujungiami (žr. pavyzdį).

GP nustatomi sisteminių nusikaltimų atvejų, kurių neidentifikavo AVPK, pavyzdžiai[143]

- Nuo 2019-08-19 iki 2020-02-18 skirtingose ikiteisminio tyrimo įstaigose buvo pradėti 68 ikiteisminiai tyrimai dėl asmenų, kurie pagal skelbimus internete apgaulės būdu paima daiktus, pateikę fiktyvius mokėjimo dokumentus. Pasikartojantys telefono numeriai, iš kurių skambinama nukentėjusiesiems, ir el. pašto adresai, iš kurių siunčiami suklastoti mokėjimo pavedimų nuorašai, identiškas *modus operandi* ir kitos aplinkybės sudaro pagrindą pagrįstai

[138] Lietuvos kriminalinės policijos biuro 2020-03-27 pateikti pavyzdžiai, schema, lentelės, susirašinėjimas ir kita informacija apie sisteminius nusikaltimus.

[139] Susitikimų su AVPK KP NNTV atstovais protokolai: 2020-02-04 Vilniaus, 2020-02-06 Kauno, 2020-02-12 Klaipėdos.

[140] Lietuvos policijos generalinio komisaro 2017-07-03 įsakymas Nr. 5-V-607 „Dėl informacijos pateikimo“.

[141] Lietuvos kriminalinės policijos biuro 2020-03-27 pateikti pavyzdžiai, schema, lentelės, susirašinėjimas ir kita informacija.

[142] Lietuvos kriminalinės policijos biuro VKKV veiklos patikrinimo ataskaitos: Vilniaus 2019-04-12, Kauno 2019-11-05, Klaipėdos 2018-10-30, Šiaulių 2020-02-03, Tauragės 2018-11-27, Utenos 2018-04-23, Marijampolės 2018-05-11.

[143] Generalinės prokuratūros 2020-02-26 ir 2020-04-23 pateikta informacija.

prielaidai, kad šias veikas daro tų pačių asmenų grupė. Per beveik 5 mėn. nuo seniausiai pradėto ikiteisminio tyrimo šios veikos nebuvo identifikuotos kaip sisteminis nusikaltimas, bendra jų žala jau viršijo 44 tūkst. Eur.

- GP nustatė, kad viename AVPK atliekamas ikiteisminis tyrimas dėl elektroninių sukčiavimų tariamai prekiaujant elektroninėje parduotuvėje. Prie jo prijungta 16 kitų ikiteisminių tyrimų, pradėtų kitose ikiteisminio tyrimo įstaigose toje pačioje apskrityje. Buvo nustatyti 8 ikiteisminiai tyrimai kituose penkiuose AVPK, kurie nebuvo prijungti prie šio ikiteisminio tyrimo.
- Penkiuose AVPK buvo pradėti 5 ikiteisminiai tyrimai dėl sukčiavimų elektorinėje erdvėje: fiktyviai siūlomos paslaugos ar prekės, bet jų nukentėjusysis negauna, nors ir sumoka. GP atliko stebėseną ir nustatė, kad šios nusikalstamos veikos identiškos *modus operandi*, todėl reikia užtikrinti, kad tyrimai būtų tęsiami koordinuotai ir organizuojami vieno prokuroro, juos atliktų viena ikiteisminio tyrimo įstaiga.

48. Nustatyta, kad LKPB neturi visos informacijos apie sisteminius nusikaltimus: nuo 2018 m. birželio iki 2020 m. kovo mėn. gavo 11 tarnybinių pranešimų apie sisteminius NEE iš Vilniaus AVPK, kiti padaliniai tokios informacijos neteikė[144]. AVPK vadovai turi imtis iniciatyvos dėl sisteminių nusikaltimų sujungimo ar perėmimo, tačiau, auditorių nuomone, padalinių dideli krūviai, nepakankami ištekliai gali paveikti šiuos sprendimus, todėl turi būti užtikrinama LKPB papildoma NEE ikiteisminių tyrimų, kurie turi sistemiškumo požymių, stebėseną šalies mastu.

49. GP nuomone[145], sisteminiai nusikaltimai plinta Lietuvos mastu, ypač sukčiavimo atvejai, tačiau jie nėra identifikuojami. Prokuratūra taip pat nurodo, kad tokia situacija didina administracinę naštą, tyrimai atliekami neefektyviai, veiksmai dubliuojami, teisėjai ar prokurorai skirtinguose tyrimuose daro tuos pačius veiksmus. Tyrimus atliekant atskirai, nematomas nusikaltimo mastas, šie nusikaltimai kvalifikuojami kaip nesunkūs, o apjungti jie būtų didesnio sunkumo.

50. Siekiant užtikrinti rezultatyvų sisteminių NEE identifikavimą ir ištyrimą, turi būti tobulinamas sisteminių nusikaltimų identifikavimo procesas, užtikrinant, kad LKPB atliktų NEE ikiteisminių tyrimų, kurie turi sistemiškumo požymių, stebėseną šalies mastu.

3.1.2. Nusikaltimų elektroninėje erdvėje tiriančių specializuotų padalinių pajėgumai turi būti stiprinami

51. Pagal gerąją valdymo praktiką[146], siekiant įgyvendinti užsibrėžtus tikslus, reikia turėti pakankamai išteklių (ir žmogiškųjų, ir kitų), kurie sudarytų sąlygas tinkamai veikti ir gauti norimus rezultatus. Žmogiškųjų išteklių valdymas labai svarbus, nes darbuotojai yra reikšmingas turtas: valdymo ir vidaus kontrolės aplinka labai priklauso nuo jų motyvacijos ir kompetencijos. 2017 m. ES Tarybos ataskaitoje[147] nurodoma, kad šalys narės turėtų išlaikyti ir kiek galima didinti teisėsaugos pareigūnų, tiriančių NEE, specializaciją.

52. Pagal LKPB aprašą[148] laikoma, kad prielaidos kokybiškai ir per trumpiausius terminus atlikti ikiteisminius tyrimus sudarytos, kai vienu metu vienam pareigūnui tenka ne

[144] Lietuvos kriminalinės policijos biuro 2020-03-27 pateikta informacija.

[145] 2020-02-04 susitikimo su Generalinės prokuratūros atstovais protokolas.

[146] CobiT 4.1 metodika – PO7 „Žmogiškųjų išteklių valdymas“.

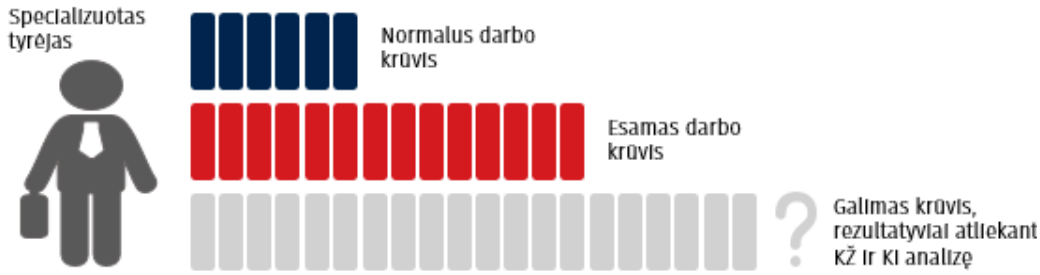
[147] Prieiga per internetą: http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/lt/pdf.

[148] 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.

daugiau kaip 6 ikiteisminiai tyrimai (maža rizika). Siekdami įvertinti KP NEE specializuotų padalinių darbo krūvius, išnagrinėjome LKPB Veiklos koordinavimo ir kontrolės valdybos minėtų septynių AVPK KP NEE specializuotų padalinių veiklos patikrinimo ataskaitose pateiktą informaciją[149]. Nustatyta, kad krūviai viršija numatytą priimtiną normą tuose padaliniuose, kuriuose daugiausiai atliekama NEE ikiteisminių tyrimų: Vilniaus AVPK KP NEE specializuoto padalinio vieno pareigūno vidutinis darbo krūvis yra 12–15 ikiteisminių tyrimų, Kauno – 12–14, Šiaulių ir Klaipėdos – po 7[150]. Pastebime, kad kai kurių pareigūnų krūviai iki trijų kartų viršija normą, pvz., Vilniaus AVPK KP NEE specializuotame padalinyje kai kurie pareigūnai vienu metu tyrė 16–20 ikiteisminių tyrimų, Kaune – 14.

53. Pažymėtina, kad, esant veiksmingesnei kibernetinių incidentų analizei (žr. 1.3 poskyryje) ir rezultatyvesnei kriminalinei žvalgybai NEE srityje, NEE ikiteisminių tyrimų skaičius ir atitinkamai pareigūnų darbo krūviai, tikėtina, bus didesni, nei dabar esami (žr. 21 pav.).

21 pav. AVPK KP NEE specializuotų padalinių pareigūnų krūviai



Šaltinis – Valstybės kontrolė

54. Esant dideliems KP NEE specializuotų padalinių krūviams:

- *Didėja NEE specializuotų darbuotojų kaita*. Įvertinus LKPB pateiktą informaciją[151] nustatyta, kad 2018 m., palyginus su 2015 m., išėjusiųjų NEE specializuotų pareigūnų padidėjo 4 proc. punktais (2015 m. – 6 proc., 2016 m. – 3 proc., 2017 m. – 9 proc., 2018 m. – 10 proc.). Pažymėtina, kad 60 proc. 2018 m. išėjusiųjų turėjo 4 metų specializacijos darbo patirtį. Auditorių vertinimu, specializacijos patirtį turinčių pareigūnų praradimas ir naujų įdarbinimas gali veikti darbo rezultatus ir jų kokybę, nes naujų pareigūnų parengimas ir gebėjimo bei žinių NEE srityje formavimas reikalauja daug pastangų ir laiko.
- *Neišnaudojamas kriminalinės žvalgybos potencialas NEE srityje*. Pagal LKPB ataskaitose pateiktus duomenis apie ikiteisminį tyrimą atliekančių bei kriminalinę žvalgybą vykdančių pareigūnų funkcijų pasiskirstymą nustatyta, kad KP NEE specializuoti padaliniai krūvių problemą bando spręsti perskirstydami darbus ir ikiteisminius tyrimus ar kitus nesudėtingus procesinius veiksmus pavesdami atlikti kriminalinės žvalgybos funkciją vykdantiems pareigūnams (žr. pavyzdį).

[149] Lietuvos kriminalinės policijos biuro VKKV veiklos patikrinimo ataskaitos: Vilniaus 2019-04-12, Kauno 2019-11-05, Klaipėdos 2018-10-30, Šiaulių 2020-02-03, Tauragės 2018-11-27, Utenos 2018-04-23, Marijampolės 2018-05-11.

[150] Ten pat.

[151] Lietuvos kriminalinės policijos biuro 2019-11-12, 2019-12-19, 2020-02-05 pateikta informacija apie NEE srityje besispecializuojančius pareigūnus.

NEE ikiteisminių tyrimų darbų perskirstymo kriminalinę žvalgybą atliekantiems pareigūnams pavyzdžiai

Kauno AVPK KP NNTV kriminalinės žvalgybos funkciją turinčiai vykdyti vyresniajai pareigūnei buvo pavesta atlikti 14 ikiteisminių tyrimų[152].

Vilniaus ir Klaipėdos AVPK KP NNTV kriminalinės žvalgybos ištekliai buvo naudojami nesudėtingoms procesinėms prievartos priemonėms atlikti (pvz.: kratai, poėmiui, informacijai gauti), o tai priklauso ikiteisminio tyrimo funkcijai[153].

Esant tokiai situacijai, nepakankamai išnaudojamas žvalgybos potencialas NEE srityje. Kriminalinės žvalgybos elektroninėje erdvėje tyrimų apimtis riboja ir esamo teisinio reguliavimo trūkumai[154], kadangi pagal Kriminalinės žvalgybos įstatymą[155] šios žvalgybos tyrimai negali būti atliekami dėl nusikalstamų veikų, numatytų BK XXX skyriuje, išskyrus BK 198 str. 2 d.

55. Viena pagrindinių priežasčių, kuri lemia didelius KP NEE specializuotų padalinių krūvius, yra nepakankamai suformuoti padalinio žmogiškieji ištekliai. Pagal LKPB pateiktą informaciją apie Vilniaus, Kauno, Klaipėdos, Panevėžio, Šiaulių AVPK KP NEE specializuotų padalinių 2019 m. patvirtintus ir neužpildytus etatus[156] auditoriai apskaičiavo, kad neužimtų NEE tiriančių pareigybių buvo vidutiniškai 22 proc. (13 iš 60 etatų)[157]. Kiekviename padalinyje neužimtų pareigybių dalis skiriasi: daugiausiai jų Kauno AVPK KP NEE specializuotame padalinyje – 44 proc., Vilniaus ir Šiaulių po 20 proc., Klaipėdos ir Panevėžio po 13 proc. KP NEE specializuotų padalinių nuomone, surasti tinkamus darbuotojus yra sudėtinga dėl reikalingų specifinių kompetencijų šioje srityje.

Vilniaus, Kauno, Klaipėdos AVPK KP NEE specializuotų padalinių nuomonė[158]

Naujų darbuotojų paieška ir jų priėmimas vyksta nuolatos, kandidatų ieškoma įvairiais būdais, tiek teisėsaugos sistemos viduje, tiek išorėje, tai atlieka patys specializuoti padaliniai. Tačiau ypač sudėtinga surasti darbuotoją, kuris turėtų tinkamus gebėjimus dirbti NEE srityje, todėl naujus darbuotojus surasti yra problematiška.

56. Siekiant gerinti specializuotų padalinių veiklos rezultatyvumą, reikia priimti valdymo sprendimus, kurie sudarytų sąlygas mažinti KP NEE specializuotų padalinių darbo krūvius. Be to, siekiant labiau išnaudoti kriminalinės žvalgybos potencialą NEE srityje, siūloma peržiūrėti teisinį reguliavimą ir imtis priemonių, kad didėtų jos veiklos apimtis elektroninėje erdvėje.

[152] Lietuvos kriminalinės policijos biuro VKKV Vilniaus AVPK KP NNTV veiklos patikrinimo 2019-04-12 ataskaita.

[153] Lietuvos kriminalinės policijos biuro VKKV Kauno AVPK KP NNTV veiklos patikrinimo 2019-11-05 ataskaita.

[154] 2020-03-02 susitikimo su Lietuvos kriminalinės policijos biuro SO5 atstovais protokolas.

[155] Kriminalinės žvalgybos įstatymas, 8 str. 1 d. 1 p.

[156] Lietuvos kriminalinės policijos biuro duomenimis, istorinė informacija personalo sistemoje nėra kaupiama, todėl viso audituojamo laikotarpio komplektacijos analizės atlikti nebuvo galimybės. Nebuvo vertinama ir NTS komplektacija, nes šio padalinio pareigybės nėra skirtos tirti tik NEE.

[157] Skaičiavimo algoritmas: neužimtų etatų dalis nuo visų patvirtintų etatų Vilniaus, Kauno, Klaipėdos, Panevėžio, Šiaulių AVPK KP NEE specializuotuose padaliniuose.

[158] Susitikimų AVPK KP NNTV atstovais protokolai: 2020-02-04 Vilniaus, 2020-02-06 Kauno, 2020-02-12 Klaipėdos.

Specializuotų padalinių krūvį didina neišspręstos problemos laisvės atėmimo vietų sistemoje

57. Įvertinę Vilniaus, Kauno, Klaipėdos KP NEE specializuotų padalinių pateiktą informaciją apie 2019 m. registruotus ikiteisminius tyrimus[159], nustatėme, kad dalis jų yra vykdoma iš laisvės atėmimo vietų.

58. Kadangi informacija apie NEE, vykdomų iš laisvės atėmimo vietų, policijoje nėra renkama ir sisteminama, auditoriai neturėjo galimybių įvertinti viso tokio pobūdžio nusikaltimų masto. Remdamiesi Vilniaus, Kauno ir Klaipėdos KP NEE specializuotų padalinių pateiktais duomenimis, apskaičiavome, kad 2019 m. elektroniniai sukčiavimai vykdyti iš laisvės atėmimo vietų sudarė nuo 8 iki 16 proc. (žr. pavyzdį). Pažymėtina, kad vien tik Kauno apskrityje žala dėl tokio pobūdžio nusikaltimų 2019 m. sudarė 179 tūkst. Eur[160].

2019 m. ikiteisminių tyrimų, kurie susiję su elektroniniais sukčiavimais, vykdytais iš laisvės atėmimo vietų, apimčių pavyzdžiai

- Vilniaus AVPK KP NEE specializuoto padalinio ikiteisminiai tyrimai dėl elektroninių sukčiavimų, vykdytų iš laisvės atėmimo vietų, sudarė 13 proc. visų padalinyje registruotų tokio pobūdžio nusikaltimų;
- Klaipėdos AVPK KP NEE specializuoto padalinio ikiteisminiai tyrimai dėl elektroninių sukčiavimų, vykdytų iš laisvės atėmimo vietų, sudarė 16 proc. visų padalinyje užregistruotų tokio pobūdžio nusikaltimų;
- Kauno AVPK KP NEE specializuoto padalinio ikiteisminiai tyrimai dėl elektroninių sukčiavimų, vykdytų iš laisvės atėmimo vietų, sudarė 8 proc. nuo visų tirtų ikiteisminių tyrimų.

59. GP atstovų nuomone[161], šio pobūdžio nusikaltimai galėtų sudaryti net 80–85 proc. visų ikiteisminių tyrimų dėl elektroninių sukčiavimų.

60. Kalėjimų departamento duomenimis[162], užkardyti NEE, vykdomus iš laisvės atėmimo vietų, bandoma tokiomis priemonėmis kaip: diegiant laisvės atėmimo vietose radijo ryšio blokavimo ir (ar) detektavimo sistemas (joms 2008–2017 m. valstybė išleido 890 tūkst. Eur); perkeliant asmenis, įtariamus vykdant tokias nusikalstamas veikas, į laisvės atėmimo vietas, kur veikia šios sistemos; atliekant kratas; organizuojant kitus veiksmus. Tačiau šios priemonės nėra veiksmingos, nes tokie nusikaltimai ir toliau vykdomi. Pažymėtina, kad dėl to teismas priteisia žalos atlyginimą nukentėjusiesiems iš Lietuvos valstybės (žr. pavyzdį).

Priteistos iš valstybės žalos atlyginimo pavyzdžiai[163]

- Lietuvos vyriausiojo administracinio teismo 2020-01-29 nutartimi administracinėje byloje Nr. eA-267-442/2020 (teisminio proceso Nr. 2-68-3-29909-2016-7) pareiškėjai priteista 2 000 Eur turtinei žalai atlyginti.

[159] AVPK KP NNTV pateikta informacija: Vilniaus 2020-02-11; Kauno 2020-02-25 ; Klaipėdos 2020-02-13.

[160] Kauno AVPK KP NNTV 2020-02-25 pateikta informacija apie ikiteisminius tyrimus, kurie susiję su nusikaltimais vykdytais iš laisvės atėmimo vietų.

[161] 2020-02-26 susitikimo su GP atstovais protokolas.

[162] Kalėjimų departamento 2020-03-03 pateikta informacija.

[163] Teismo sprendimų pavyzdžiai. Prieiga per internetą:
http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id =16da4276-873d-4edc-b2cc-0cb54e6f89a1;
http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=9365c8f5-9349-4cec-bd38-984f36fcbdfa;
http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=6efb0119-cef8-4694-89a9-e06eb99091bb.

- Lietuvos vyriausiojo administracinio teismo 2019-03-07 nutartimi administracinėje byloje Nr. A-864-662/2019 (teisminio proceso Nr. 2-68-3-10876-2015-9) pareiškėjai priteista 600 Eur turtinei žalai atlyginti ir 1 200 Eur neturtinei žalai atlyginti.
- Regionų apygardos administracinio teismo 2019-11-19 sprendimu administracinėje byloje Nr. eI-26-283/2019 (teisminio proceso Nr. 2-54-3-00786-2016-4) pareiškėjai priteista 1 300 Eur neturtinei žalai atlyginti.

61. Siekiant užkardyti elektroninius nusikaltimus, vykdomus iš laisvės atėmimo vietų, reikia numatyti ir įgyvendinti veiksmingas priemones, kurios sudarytų sąlygas nuteistiesiems daugiau jų nevykdyti.

3.1.3. Nepakankamai išgryninta privaloma specializacija nusikaltimų elektroninėje erdvėje ikiteisminiuose tyrimuose

62. Pareigūnų specializacija nustatoma, siekiant didinti proceso veiklos efektyvumą, sudaryti prielaidas tikslingiau kelti kvalifikaciją, veiksmingiau formuoti bendrąją praktiką ir nustatyti aiškias bylų paskirstymo taisykles, mažinti korupcijos pasireiškimo riziką[164]. ES Taryba[165] skatina šalis nares didinti institucijų specializacijos lygį, kad būtų veiksmingai patraukiama baudžiamojon atsakomybėn ir skiriami apkaltinamieji nuosprendžiai už kibernetinius nusikaltimus *stricto sensu* ir nusikaltimus pasinaudojant kibernetine erdve.

Nusikaltimus elektroninėje erdvėje, kurie turi būti tiriami specializuotose padaliniuose, tiria nespecializuoti pareigūnai

63. Nuo 2015 m. iki 2019 m. pareigūnų, kurių specializacija – NEE, skaičius nuosekliai augo: 2015 m. – 49, 2016 m. – 65, 2017 m. – 74, 2018 m. – 78, 2019 m. – 81[166]. Kompetencijų apraše[167] apibrėžtos AVPK KP NEE specializuotų padalinių veikimo ribos (kompetencija) (detaliau žr. 6 priede).

64. Atlikę 2016–2019 m. ikiteisminių tyrimų pasiskirstymo pagal KP NEE specializuotus ir nespecializuotus padalinius analizę nustatėme, kad nespecializuoti pareigūnai vidutiniškai atliko 62 proc. visų NEE ikiteisminių tyrimų[168]. Pažymėtina, kad iš jų: 11 proc. sudarė ikiteisminiai tyrimai pagal BK XXX skyrių (nėra sutapties su kitomis nusikalstamomis veikomis NEE srityje), 33 proc. – susiję su vaiko išnaudojimu pornografijai (BK 162 str., 309 str.), 72 proc. – su elektroniniais sukčiavimais (BK 182 str., kartu su 214 ir (ar) 215 str.), 87 proc. – su netikromis elektroninio mokėjimo priemonėmis ir neteisėtų jų panaudojimu (BK 214 ir/ar 215 str.). Tai rodo, kad dalis ikiteisminių tyrimų, kurie priklauso specializuotų padalinių kompetencijai, nėra tiriami šiuose padaliniuose.

65. AVPK KP NEE specializuotuose padaliniuose susiformavo praktika, kad, siekiant neapkrauti jų nereikšmingais darbais, nesudėtingi ir mažareikšmiai NEE ikiteisminiai tyrimai (kurie nereikalauja gilesnių techninių žinių), gali būti tiriami nespecializuotuose padaliniuose.

[164] Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.436535/asr.

[165] Prieiga per internetą: http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/lt/pdf.

[166] Apskaičiuota pagal LKPB Lietuvos kriminalinės policijos biuro pateiktą informaciją apie specializuotus pareigūnus. Į šį skaičių neįtraukti vadovaujančias pareigas užimantys pareigūnai.

[167] Lietuvos policijos generalinio komisaro 2014-10-17 įsakymu Nr. 5-V-890 patvirtintas Policijos įstaigų padalinių kompetencijų atlikti ikiteisminius tyrimus aprašas.

[168] Skaičiavimo algoritmas: nespecializuotų pareigūnų tirtų IT dalis nuo visų NEE IT.

66. Siekdamas išgryninti NEE tiriančių padalinių kompetenciją, LKPB parengė Kompetencijų aprašo pakeitimo projektą. Juo planuojama KP NEE specializuotų padalinių kompetencijų apimtį sumažinti ir perduoti ikiteisminius tyrimus dėl šmeižimo (BK 154 str.), netikrų pinigų, mokėjimo priemonių ir jų neteisėto panaudojimo (BK 213–215 str.), pornografinio turinio platinimo (BK 309 str. 1 d.) tirti nespecializuotiems padaliniams. Manome, kad šie pokyčiai prisidės prie NEE specializuotų padalinių kompetencijų išgryninimo, tačiau išlieka rizika, kad nespecializuotiems padaliniams, neturintiems specifinių ar techninių žinių, ir toliau bus perduoti sisteminiai ar sudėtingi ikiteisminiai tyrimai, priskirtini specializuotiesiems.

67. Siekiant, kad visi NEE ikiteisminiai tyrimai, kurie yra sisteminiai ir reikalauja specializuotų žinių, būtų tiriami KP NEE specializuotose padaliniuose, reikia tobulinti šių ikiteisminių tyrimų paskirstymo mechanizmą.

Specializuotų pareigūnų atliekamiems nusikaltimų elektroninėje erdvėje ikiteisminiais tyrimams vadovauja nespecializuoti prokurorai

68. 2012 m. įsigaliojusiose rekomendacijose[169] numatyta, kad prokurorų specializacija yra nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui, nusikalstamos veikos, padarytos elektroninėje erdvėje, ir elektroniniai sukčiavimai. Atsižvelgiant į priskirtą specializaciją, prokurorams skirstomi ikiteisminiai tyrimai. Išanalizavus GP pateiktus 2015–2019 m. specializacijos įsakymus, nustatyta, kad 2019 m. 264 prokurorai specializavosi NEE srityje[170]. Iš jų 5 proc. dirba GP, 24 proc. apygardos prokuratūrose, 71 proc. apylinkės prokuratūrose. Nuo 2015 m. iki 2019 m. šių prokurorų skaičius didėja: 2015 m. jų buvo 96, 2016 m. – 223, 2017 – 238, 2018 m. – 260, 2019 m. – 264.

69. Atlikę 2016–2019 m. ikiteisminių tyrimų, kuriems vadovavo specializuoti prokurorai, analizę, nustatėme, kad KP NEE specializuotų padalinių ikiteisminiais tyrimams vidutiniškai vadovavo 28 proc. nespecializuotų prokurorų[171]. Tokiais atvejais specializuoti pareigūnai, atlikdami NEE ikiteisminius tyrimus, bendradarbiauja su prokurorais, kurių dalies specializacija nėra NEE sritis (žr. pavyzdį). Auditorių nuomone, tai mažina pareigūnų ir prokurorų sinergiją tiriant NEE, nes skiriasi specializuotų ir nespecializuotų pareigūnų srities supratimas, turima praktika ir žinių lygis.

NEE ikiteisminių tyrimų specializacijos pasiskirstymo pavyzdžiai

- Vilniaus AVPK KP NNTV vieno specializuoto pareigūno byloms vadovavo 12 prokurorų, iš jų 7 specializacija nėra NEE;
- Kauno AVPK KP NNTV vieno specializuoto pareigūno byloms vadovavo 18 prokurorų, iš jų 7 specializacija nėra NEE;
- Klaipėdos AVPK KP NNTV vieno specializuoto pareigūno byloms vadovavo 4 prokurorai, iš jų 3 specializacija nėra NEE;

[169] Generalinio prokuroro 2012-10-30 įsakymu Nr. I-318 patvirtintos Rekomendacijos dėl prokurorų specializacijos baudžiamajame procese ir ikiteisminių tyrimų paskirstymo prokurorams.

[170] Įvertinta pagal BK 145, 162, 170, 182, 191–194, 196–198[2], 214, 215 ir 309 str., kurie atitinka Konvencijoje dėl elektroninių nusikaltimų numatytas nusikalstamas veikas. Visų BK XXX sk. specializacijos prokurorų specializacija yra ir kitos sritys, pvz.: BK 129–134 str. (nužudymai), 135 str. (sveikatos sutrikdymas).

[171] Skaičiavimo algoritmas: NEE IT dalis, kuriems vadovavo nespecializuoti prokurorai (įsakymais neįtraukti kaip besispecializuojantys), nuo visų NEE IT, kuriuos tyrė AVPK KP NEE specializuotų padalinių pareigūnai 2016–2019 m.

- Šiaulių AVPK KP NNTV vieno specializuoto pareigūno byloms vadovavo 9 prokurorai, iš jų 4 specializacija nėra NEE.

70. Tokia situacija susidaro, nes, siekiant mažinti prokurorų krūvius ir atsižvelgiant į nusikalstamų veikų sudėtingumą, NEE ikiteisminiai tyrimai gali būti skirstomi ir nespecializuotiems prokurorams [172]. Auditorių vertinimu, siekiant užtikrinti NEE specializacijos tarp pareigūnų ir prokurorų nuoseklumą, reiktų tobulinti esamą prokurorų specializacijos tvarką, kad NEE specializuotų pareigūnų ikiteisminiams tyrimams vadovautų šios srities specializuoti prokurorai.

GP nuomonė [173]

Būtina siekti, kad nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui visais atvejais organizuotų specializuoti prokurorai, o kitų nusikaltimų, padarytų elektroninėje erdvėje bylas, specializuoti prokurorai turėtų organizuoti taip pat daugumoje atvejų. Bet gali būti taikomos išimtys, kai tyrimas nėra sudėtingas, nes visi prokurorai turėtų turėti bazines žinias apie nusikaltimus elektroninėje erdvėje, nes tokių nusikaltimų dalis nusikaltimų struktūroje gali augti.

3.1.4. Informacinių technologijų objektų tyrimų eiles reiktų trumpinti

71. Siekiant surasti nusikalstamos veikos pėdsakus ir kitus objektus, turinčius reikšmės tyrimui, nustatyti įvykio situaciją ir kitas reikšmingas bylai aplinkybes, atliekamas įvykio vietos, patalpų, dokumentų ir kitokių objektų tyrimas[174]. NEE ikiteisminiuose tyrimuose atliekami IT objektų (kompiuterių, telefonų, vidinių ir išorinių diskų, atminties ir kitų įrenginių) ekspertiniai tyrimai.

72. Viena įsisenėjusių problemų, dėl ko NEE ikiteisminiai tyrimai užtrunka, tai ilgai trunkantys IT objektų tyrimai. Pagal policijos skelbiamą informaciją jų laukti gali tekti net 19 mėn. (žr. 22 pav.). Pagrindiniai veiksniai yra nepakankami šios sistemos žmogiškųjų išteklių ir techninės įrangos pajėgumai[175].

22 pav. IT tyrimų eilės ekspertinius tyrimus atliekančiose įstaigose

Šaltinis – KTC skelbiami duomenys[176]

[172] Generalinio prokuroro 2012-10-30 įsakymu Nr. I-318 patvirtintos Rekomendacijos dėl prokurorų specializacijos baudžiamajame procese ir ikiteisminių tyrimų paskirstymo prokurorams, 9.2 ir 22 p.

[173] Generalinės prokuratūros 2020-01-10 pateikta informacija.

[174] BPK, 205 str.

[175] LTEC 2019-07-05 ir Lietuvos kriminalinės policijos biuro 2019-07-22 pateikta informacija.

[176] Prieiga per internetą: http://ktc.policija.lrv.lt/uploads/ktc.policija/documents/files/Eiles_LPKTC_LTEC_korekcija0217.pdf.

73. 2016 ir 2017 m. Valstybės kontrolė[177], siekdama gerinti situaciją dėl ilgų ekspertinių tyrimų rezultatų teikimo terminų, teikė rekomendacijas optimizuoti valstybės finansuojamų laboratorijų (LTEC, KTC, AVPK) tinklą, tačiau problemos iki šiol nėra išspręstos.

74. 91 proc. auditorių apklausoje dalyvavusių NEE ikiteisminius tyrimus atliekančių pareigūnų[178] mano, kad IT objektų tyrimai užtrunka per ilgai. Auditorių vertinimu, tai neigiamai veikia šių tyrimų rezultatyvumą, nes, kol gaunama reikiama informacija apie IT objektų tyrimų rezultatus, kiti svarbūs tyrimui skaitmeniniai duomenys gali būti prarasti, nes saugomi ribotą laiką, pvz., informacija apie IP adresų priklausomybės nustatymą saugoma ne ilgiau kaip 6 mėn.[179]

75. Kai kurie AVPK KP NEE specializuoti padaliniai, IT objektų tyrimus pavesdavo atlikti padaliniuose dirbantiems specialistams ir pareigūnams, kad jie būtų atlikti greičiau (žr. pavyzdį).

AVPK KP NEE specializuotų padalinių IT objektų tyrimų ar apžiūrų atlikimo pavyzdžiai

- Kadangi Vilniaus AVPK KTS 2019 m. dirbo 3 specialistai, kurių krūvis sudarė po 200–300 apžiūrų per metus, ir IT objektų tyrimai ar apžiūros skyriuje užtrunka metus ir ilgiau, AVPK KP NNTV 1-ojo skyriaus pareigūnai kompiuterių apžiūras ar tyrimus KTS specialistams pavesdavo atlikti tik išimtiniais atvejais. Skyrius ėmėsi iniciatyvos šiuos darbus atlikti savo turimais ištekliais[180]: Vilniaus AVPK buvo įsteigtos 2 karjeros valstybės tarnautojų pareigybės atlikti apžiūras, šių darbuotojų priėmimas sumažino apžiūrų terminus[181].
- Kauno AVPK KPNNTV 1-ojo sk. viršininkas nurodė, kad 2019 m. daugelio tyrimų objektų apžiūras (117) darė patys pareigūnai. Trijuose ikiteisminiuose tyrimuose paskirtos užduotys LTEC arba KTV (55 objektai) ir visi tyrimai užtruko ilgiau nei 6 mėn.

76. Pažymėtina, kad ir kitų šalių praktika rodo, kad NEE srityje ekspertų ir tyrimų padalinių darbas organizuojamas kartu, siekiant pagreitinti NEE ištyrimą (žr. pavyzdį).

Užsienio šalių pavyzdžiai

- Lenkijos nacionaliniame kibernetinių nusikaltimų biure ir daugelyje regioninių elektroninių nusikaltimų departamentų veikia specializuota skaitmeninės kriminalistikos laboratorija arba dirba specializuoti pareigūnai, kurie talkina policijos pareigūnams, nagrinėjantiems šiuos nusikaltimus.[182]
- Norvegijos nacionalinį kibernetinių nusikaltimų centrą sudaro keturi padaliniai, kurie pasitelkę pažangias kompiuterinės kriminalistikos technologijas padeda regionams tirti

[177] Valstybino audito ataskaitos: 2016-11-17 Nr. VA-P-40-3-23 „Teismo ekspertizių atlikimo organizavimas“, 2017-09-29 Nr. FA-2017-P-60-5-7-1 „Lietuvos Respublikos 2016 metų valstybės konsoliduotųjų finansinių ir biudžeto vykdymo ataskaitų rinkinių teisingumas ir valstybės biudžeto vykdymo vertinimas“.

[178] Apklausai atrinkti 95 (iš 203) pareigūnai, arba 47 proc. 2019 m. dirbusių ir NEE tyrimus atlikusių, kuriems buvo pateiktas klausimynas. 37 (39 proc.) į klausimyną atsakė, iš jų 10 specializuotų pareigūnų.

[179] Elektroninių ryšių įstatymas, 66 str. 5 d. Duomenų saugojimo terminai nustatyti atsižvelgiant į 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje reikalavimus. Europos Tarybos 2001-11-23 Konvencijos dėl elektroninių nusikaltimų 29 str. 7 d. nustatytas įpareigojimas jos šalims užtikrinti, kad duomenys būtų saugomi ne trumpiau kaip 60 dienų. Atsižvelgdamos į didžiųjų paslaugų teikėjų taikomą politiką, šalys dažniausiai duomenis saugo 90 dienų su galimybe pratęsti terminą dar 90 dienų (generalinio prokuroro 2017-06-20 įsakymu Nr. I-223 patvirtintos Metodinės rekomendacijos dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tyrimo atlikimo ir kvalifikavimo ypatumų, 20 p.).

[180] Lietuvos kriminalinės policijos biuro VKKV Vilniaus AVPK KP NNTV veiklos patikrinimo 2019-04-12 ataskaita.

[181] 2020-02-04 susitikimo su Vilniaus AVPK KP NNTV atstovais protokolas.

[182] Lietuvos kriminalinės policijos biuro 2020-04-09 pateikta informacija apie užsienio šalių praktiką.

elektroninius nusikaltimus, atlieka interneto ir kompiuterių įsibrovimų tyrimus, analizuoja internetinę vaikų seksualinės prievartos medžiagą.[183]

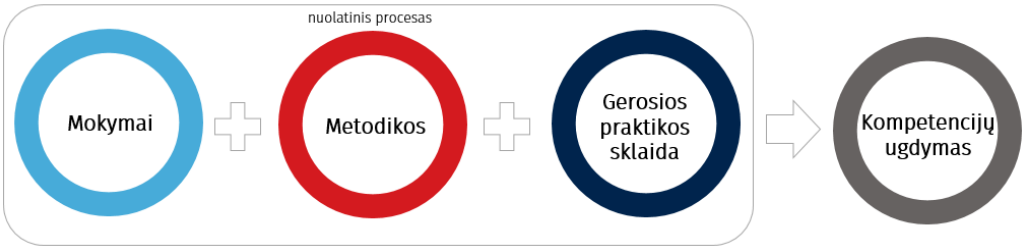
- Prancūzijos nacionalinis kibernetinių nusikaltimų tyrimo padalinys turi teismo medicinos laboratoriją ir atsakingas už paramą kitiems skyriams: renka ir analizuoja elektroninius įrodymus[184].
- Airijoje veikia Nacionalinis kovos su kibernetiniais nusikaltimais biuras, kuriam pavesta konfiskuotų kompiuterinių laikmenų teismo ekspertizė[185].

77. Siekiant užtikrinti laiku atliekamus IT objektų tyrimus ir rezultatyviai ištiriamus NEE, surenkant reikiamus įrodymus, siūloma KP NEE specializuotų padalinių darbą organizuoti kartu su reikiamais ekspertiniais pajėgumais.

3.2. Specializuotų pareigūnų ir prokurorų kompetencijų ugdymo organizavimas turėtų būti tobulintinas

78. Europos Komisijos komunikate[186] nurodyta, kad būtina dėti reikšmingas pastangas, siekiant užtikrinti nuolatinius ir specializuotus mokymus teisėsaugos personalui. IOCTA ataskaitose[187] pabrėžiama, kad pareigūnai turi nuolat ugdyti kompetencijas ir gebėjimus įvairiose srityse. Pažymėtina, kad naujos technologijos (pvz.: dirbtinis intelektas, daiktų internetas) sudaro sąlygas vykdyti sudėtingesnius ir mažiau pastebimus NEE. Siekdami ištirti šiuos nusikaltimus, pareigūnai ir prokurorai privalo turėti ne tik geras teisines, bet ir technologines žinias. Ugdant kompetencijas svarbūs įvairūs bendradarbiavimo formatai, leidžiantys keistis gerąja patirtimi, ir reikiamos metodikos, kurios suteikia daugiau žinių ir palengvina ikiteisminių tyrimų atlikimą (žr. 23 pav.).

23 pav. Kompetencijų ugdymo elementai



Šaltinis – Valstybės kontrolė pagal gerąją praktiką

[183] Ten pat.

[184] Specializuoti kibernetinių nusikaltimų padaliniai: gerosios praktikos, 2011 m. Prieiga per internetą: https://www.google.lt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiqy9KHoePpAhVPxosKHagSDLUQFjAAegQIARAB&url=https%3A%2F%2Frm.coe.int%2F2467-htcu-study-v30-9nov11%2F16802f6a33&usg=AOvVaw3rgEVkyBABX93hj3Bq7G1c.

[185] Prieiga per internetą: https://www.garda.ie/en/about-us/specialist-units/garda-national-cyber-crime-bureau-gnccb-/, Specializuoti kibernetinių nusikaltimų padaliniai: gerosios praktikos studija, 2011 m.

[186] Bendras komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“ (COM/2000/0890 final).

[187] Prieigos per internetą: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016; https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

79. Tam, kad NEE ikiteisminiai tyrimai atliekami nepakankamai rezultatyviai (žr. 3.1 poskyryje), įtakos turi toliau nurodyti specializuotų pareigūnų ir prokurorų kompetencijų ugdymo organizavimo trūkumai.

Nepakanka specializuotų nusikaltimų elektroninėje erdvėje mokymų pareigūnams ir prokurorams

80. Nuo 2014 m. LKPB pradėjęs veikti Kriminalinės žvalgybos mokymo centras (skyriaus teisėmis) organizuoja mokymus LKPB ir AVPK pareigūnams[188]. Mokymų programos formuojamos atsižvelgiant į poreikius pagal darbuotojui būtinas suteikti žinias, užtikrinant pareigybei keliamas kompetencijas. Atliekamas trijų lygių poreikio vertinimas: ekspertinis (LKPB SO5 apklausa dėl galimų temų); bendrasis (vadovų apklausa); individualus (pareigūnų apklausa vertinant metų veiklą). Pagal vertinimo rezultatus turėtų būti parengiamos ir patvirtinamos reikiamos mokymų programos[189].

81. Prokurorų ir prokuratūros personalo mokymą ir kvalifikacijos kėlimą užtikrina GP Mokymų skyrius[190]. Jis atsakingas už mokymo ir kvalifikacijos kėlimo programų ir planų rengimą, jų įgyvendinimo organizavimą. Mokymų poreikį skyrius nustato apibendrinęs GP padalinių ir teritorinių apygardų prokuratūrų pateiktus duomenis ir teikia pasiūlymus ir išvadas dėl prokurorų ir prokuratūros personalo mokymų ir kvalifikacijos tobulinimo.

82. Įvertinus GP[191] ir LKPB[192] pateiktą informaciją apie 2015–2019 m. vykdytus NEE mokymus nustatyta, kad nesudarytos sąlygos specializuotiems prokurorams ir pareigūnams kelti kvalifikaciją NEE srityje:

    - *Vis dar nėra parengta NEE mokymų programa NEE specializacijos pareigūnams.* 2017 m. Kriminalinės žvalgybos mokymo centrui atlikus struktūrinių kriminalinės policijos padalinių vadovų apklausą, nustatytos šešios privalomų kompetencijų kryptys, iš kurių viena – pareigūnų, tiriančių NEE, mokymai. 2018 m. patvirtinta ir šiuo metu įgyvendinama bendrosios kompetencijos specializuotų padalinių pareigūnų mokymų programa[193]. Pareigūnų, tiriančių NEE, mokymo programą planuojama parengti ir įgyvendinti II etape, suteikus būtinų žinių pagal bendrąją programą. LKPB duomenimis, mokymai specializuotiems pareigūnams vyksta pagal svarbiausius poreikius[194]. Auditorių vertinimu, tokia praktika netinkama ir sudaro sąlygas ugdymo poreikius realizuoti pavėluotai, neatsižvelgiant į greitus NEE pokyčius.
    - *Mokymų turinys nepakankamas.* Kriminalinės žvalgybos mokymo centro duomenimis, 2015–2019 m. vykdytus NEE srities mokymus išklausė

[188] Prieiga per internetą: http://lkpb.policija.lrv.lt/lt/lkpb-veiklos-sritys/kompetenciju-kelimas.

[189] Lietuvos kriminalinės policijos biuro 2019-07-22 pateikta informacija pagal auditorių klausimus.

[190] Prieiga per internetą: https://www.prokuraturos.lt/data/public/uploads/2017/08/2016-09-27-i-229-mokymu-skyriaus-nuostatai-aktuali-2017-07-24-i-262-nauja-redakcija.pdf.

[191] Generalinės prokuratūros 2020-01-10 informacija apie mokymų programas, dalyvių skaičių ir mokymų vertinimo rezultatus.

[192] Lietuvos kriminalinės policijos biuro 2019-12-19 ir 2019-12-23 informacija apie kvalifikacijos tobulinimą, mokymų programas ir dalyvius, vertinimo rezultatus.

[193] Lietuvos policijos generalinio komisaro 2018-04-16 įsakymas Nr. 5-V-370 „Dėl LKPB specialiųjų mokymo modulių programos „Specializuotų kriminalinės žvalgybos padalinių pareigūnų pagrindinių kompetencijų formavimas ir tobulinimas““.

[194] Lietuvos kriminalinės policijos biuro 2019-07-22 pateikta informacija pagal auditorių klausimus.

261 kriminalinę žvalgybą ir ikiteisminius tyrimus atliekantis pareigūnas (žr. pavyzdį).

NEE mokymų pareigūnams pavyzdžiai

- „Atvirų šaltinių žvalgyba internete ir slaptieji interneto tyrimai“, vykdyti 2016, 2017 ir 2019 m., dalyvavo 118 pareigūnų;
- „Nusikaltimų elektroninėje erdvėje tyrimo taktika ir naujoves/aktualijos“, vykdyti 2015 ir 2019 m., dalyvavo 93 pareigūnai;
- „Kriminalinės policijos pareigūnų gebėjimų stiprinimas kibernetinio saugumo, vaikų seksualinio išnaudojimo, nusikaltimų elektroninėje erdvėje tyrimo srityse“, vykdyti 2017 m., dalyvavo 17 pareigūnų ir 5 prokurorai;
- „Kova su teroristinio pobūdžio propaganda internete: instrumentai ir metodai“, vykdyti 2018 m., dalyvavo 28 pareigūnai.

LKPB SO5 minėtu laikotarpiu dalyvavo mokymuose užsienyje[195] ir vykdė mokymus AVPK veiklos ir KP NEE specializuotiems padaliniams: „Kova su nusikaltimais elektroninėje erdvėje Lietuvoje. Situacija šiandien.“; „Informacijos rinkimas iš atvirųjų interneto šaltinių“; „Tekstinių failų apdorojimas ir analizė *MS Excel* ir *Linux* pagalba“; vyko mokymai pagal Norvegijos projekto finansinį mechanizmą; „Įvykių žurnalų apžiūra“.

GP 2016–2019 m. vykdytus NEE srities prokurorų mokymus išklausė beveik 400 prokurorų (žr. pavyzdį).

NEE mokymų specializuotiems prokurorams pavyzdžiai

- „Sukčiavimas el. erdvėje“, 2016 m., 97 specializuoti prokurorai;
- „Vaikų seksualinis išnaudojimas elektroninėje erdvėje“, 2017 m., 29 specializuoti prokurorai;
- „Saugumo situacija regione ir užsienio politikos tendencijos. Užsienio valstybių tarnybų veikla. Grėsmės ir pavojai elektroninėje erdvėje“, 2017 m., 32 specializuoti prokurorai;
- „Elektroninių nusikaltimų tyrimas, įrodinėjimas ir teismų praktika šios kategorijos bylose. Elektroninių duomenų gavimo būdai ir tvarka iš užsienio paslaugų tiekėjų“, 2017–2018 m., 81 specializuotas prokuroras;
- „Kibernetiniai nusikaltimai. BDAR – nekonkuravimo susitarimai“, 2018 m., 8 specializuoti prokurorai;
- „Elektroniniai įrodymai“, 2019 m., 142 specializuoti prokurorai;
- „Nusikalstamos veikos elektroninėje erdvėje ir jų kvalifikavimas“, 2019 m., 8 specializuoti prokurorai.

2016–2019 m. 18 prokurorų žinias NEE srityje tobulino stažuotėse ir mokymuose užsienyje.

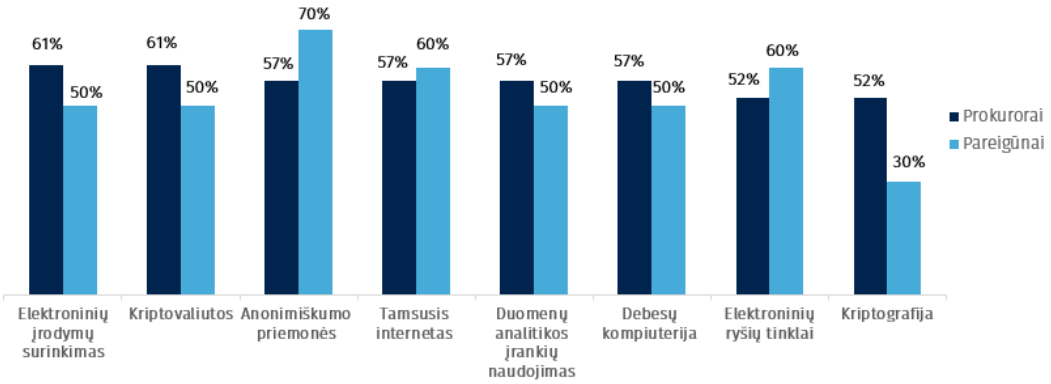
Įvertinus mokymų programų turinį nustatyta, kad Kriminalinės žvalgybos mokymo centro organizuojami mokymai NEE srityje yra bendrojo pobūdžio ir nepadengia IOCTA ataskaitose nurodytų mokymų krypčių, kurias identifikavo ekspertinis lygmuo – LKPB SO5[196]: kompiuterių atakos, siekiant išvesti sistemas iš normalaus darbo režimo „DDos atakos“ ir jų tyrimo ypatumai; virusinių programų, skirtų pavogti duomenis, tyrimo ypatumai; klastotų internetinių mokėjimo instrumentų tyrimo ypatumai; virtualių (kripto) valiutų neteisėtos apyvartos tyrimo ypatumai, jų vagysčių atskleidimo taktika; socialinė inžinerijos (įsiskverbimo į asmeninius failus ir susirašinėjimą) tyrimo taktika; anoniminių tinklų „Dark Net“ tyrimo ypatumai.

[195] 2018-2019 m. LKPB SO5 4 specializuoti pareigūnai dalyvavo mokymuose užsienyje pagal Erasmus+ programos projektą „Teisėsaugos tarnybų profesinės kvalifikacijos kėlimas kovos su kibernetiniais nusikaltimais srityje (angl. *Professional training of law enforcement services to combat cybercrime*)“.

[196] Lietuvos kriminalinės policijos biuro 2019-07-22 pateikta informacija pagal auditorių klausimus.

Siekiant nustatyti, ar vykdomų mokymų NEE srityje pakanka, buvo apklausti 38 prokurorai ir 37 pareigūnai[197]. Jie nurodo, kad reikia ugdyti kompetenciją įvairiose srityse (žr. 24 pav.). 70 proc. atsakiusiųjų prokurorų ir pareigūnų nurodė, kad ypač aktualūs NEE tyrimų atlikimo mokymai, bet vidutiniškai 50 proc. jų pažymėjo, kad aktualios ir bendrosios žinios, informacijos paieškos mokymai.

24 pav. Specializuotų pareigūnų ir prokurorų nurodytas NEE mokymų poreikis pagal sritis



Šaltinis – Valstybės kontrolė pagal prokurorų ir pareigūnų apklausą

- *Neorganizuojami bendri mokymai prokurorams ir pareigūnams, bendruose mokymuose nedalyvauja teisėjai.* ES Tarybos 2017 m. vertinimo ataskaitoje apie Lietuvą[198] rekomenduojama organizuoti bendrus prokurorų, ikiteisminio tyrimo pareigūnų ir teisėjų mokymus, stiprinant kompetenciją. Audituojamu laikotarpiu organizuoti vieni bendri pareigūnų ir prokurorų mokymai[199], o kartu su teisėjais bendrų mokymų nebuvo. Pažymėtina, kad tiek pareigūnų, tiek prokurorų mokymų temos susijusios ir aktualios abiem šalims, todėl tikslinga sudaryti sąlygas juos organizuoti dažniau. Bendrų mokymų poreikį nurodė Vilniaus, Kauno, Klaipėdos AVPK KP NEE specializuotų padalinių atstovai[200].
- *Mokymų organizuojama nepakankamai.* 70 proc. apklausoje dalyvavusių NEE specializuotų pareigūnų ir prokurorų nurodė, kad mokymų NEE srityje nepakanka. Atlikus Kriminalinės žvalgybos mokymo centro mokymų dalyvių sąrašų analizę nustatyta, kad 2015–2019 m. 30 proc.[201] specializuotų pareigūnų nė karto juose nedalyvavo, kiti tik fragmentiškai, nes mokymų organizuojama nepakankamai. Pažymėtina, kad šiuose mokymuose nedalyvavo 36 proc. pareigūnų, kurie pradėjo specializuotis 2019 m. Prokurorų mokymai 2015–2019 m. vyko kasmet, bet 61 proc. apklausoje dalyvavusių specializuotų prokurorų juose dalyvavo fragmentiškai.

[197] Apklausai atrinkta 115 (iš 148) prokurorų, arba 78 proc. 2019 m. dirbusių ir NEE tyrimus atlikusių prokurorų, 38 (33 proc.) į klausimyną atsakė, iš jų 23 specializuoti prokurorai. Apklausai atrinkti ir 95 (iš 203) pareigūnai, arba 47 proc. 2019 m. dirbusių ir NEE tyrimus atlikusių, 37 (39 proc.) į klausimyną atsakė, iš jų 10 specializuotų pareigūnų. Šios apklausos atliktos nuo 2020-01-06 iki 2020-01-17.

[198] Prieiga per internetą: http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf.

[199] 2017 m. mokymuose „Kriminalinės policijos pareigūnų gebėjimų stiprinimas kibernetinio saugumo, vaikų seksualinio išnaudojimo, nusikaltimų elektroninėje erdvėje tyrimo srityse“ dalyvavo 17 pareigūnų ir 5 prokurorai.

[200] Susitikimų protokolai: 2020-02-04 su Vilniaus AVPK KP NNTV atstovais, 2020-02-06 su Kauno AVPK KP NNTV atstovais, 2020-02-12 su Klaipėdos AVPK KP NNTV atstovais.

[201] Apskaičiavimo algoritmas: NEE specializuotų pareigūnų (pagal LKPB sąrašus) dalis iš visų dalyvių, kurie nurodyti Kriminalinės žvalgybos mokymo centro vykdytų mokymų dalyvių sąrašuose 2015-2019 m.

83. Siekiant užtikrinti pakankamą NEE specializuotų pareigūnų ugdymo procesą, reikia parengti ir patvirtinti specializuotiems pareigūnams skirtą NEE mokymų programą, atitinkančią pareigūnų ugdymo poreikius šioje srityje, ypač didelį dėmesį skiriant naujų specialiųjų kompetencijų ugdymui, ir ją įgyvendinti. Siekiant gerinti specializuotų pareigūnų ir prokurorų bendrą ugdymo procesą, reikia parengti bendrą NEE specializuotų pareigūnų ir prokurorų mokymų programą ir ją įgyvendinti. Be to, reikia didinti NEE mokymų specializuotiems prokurorams apimtis ir užtikrinti, kad šiuose mokymuose dalyvautų visi specializuoti prokurorai.

Trūksta metodinių dokumentų, kurie palengvintų praktinį nusikaltimų elektroninėje erdvėje tyrimą

84. NEE yra specifinė sritis, kuri dėl greitų technologinių pokyčių nuolatos keičiasi, todėl ikiteisminius tyrimus atliekantys pareigūnai praktikoje gali susidurti su įvairiais sunkumais, kaip tinkamai tirti NEE ir atlikti tam tikrus procesinius veiksmus, kurie neatsiejami nuo elektroninės erdvės, todėl svarbu turėti pakankamai metodinių praktinio NEE ištyrimo priemonių, kuriose būtų pateikti techniniai aspektai, palengvinantys ir pagreitinantys NEE ištyrimą.

85. GP yra parengusi ir patvirtinusi tiesiogiai su NEE susijusias 2 metodines rekomendacijas dėl:

    - nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tyrimo atlikimo ir kvalifikavimo ypatumų[202];
    - elektroninėje erdvėje vykdomų sukčiavimų (telefoninio sukčiavimo) tyrimo ir nusikalstamų veikų kvalifikavimo[203].

86. Siekdami įvertinti parengtų NEE srities rekomendacijų pakankamumą, atlikome šiuos tyrimus atliekančių pareigūnų[204] ir jiems vadovaujančių prokurorų[205] apklausą. Didžioji dalis prokurorų (74 proc.) ir pareigūnų (73 proc.) nurodė, kad rekomendacijos yra pakankamos[206].

87. Beveik du trečdaliai prokurorų (apie 68 proc.) ir pareigūnų (apie 62 proc.) teigia, jog reikia naujų metodinių dokumentų, skirtų NEE tyrimui, pvz., 83 proc. prokurorų ir 87 proc. pareigūnų nurodė, kad trūksta rekomendacijų dėl NEE elektroninių įrodymų surinkimo ir išsaugojimo. 87 proc. prokurorų ir 69 proc. pareigūnų nurodė, kad reikia ir specifinių kibernetinių nusikaltimų tyrimo metodinių rekomendacijų (pvz.: botnetai, kibernetinis terorizmas ir kt.).

---

[202] Generalinio prokuroro 2017-06-20 įsakymu Nr. I-223 patvirtintos Metodinės rekomendacijos dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui tyrimo atlikimo ir kvalifikavimo ypatumų.

[203] Generalinio prokuroro 2014-02-10 įsakymu Nr. I-37 patvirtintos Metodinės rekomendacijos dėl elektroninėje erdvėje vykdomų sukčiavimų (telefoninio sukčiavimo) tyrimo ir nusikalstamų veikų kvalifikavimo.

[204] Apklausai atrinkti 95 (iš 203) pareigūnai, arba 47 proc. 2019 m. dirbusių ir NEE tyrimus atlikusių, kuriems buvo pateiktas klausimynas. 37 (39 proc.) į klausimyną atsakė, iš jų 10 specializuotų pareigūnų.

[205] Apklausai atrinkta 115 (iš 148) prokurorų, arba 78 proc. 2019 m. dirbusių ir NEE tyrimus atlikusių prokurorų, 38 (33 proc.) į klausimyną atsakė, iš jų 23 specializuoti.

[206] Prokurorų ir pareigūnų apklausos atliktos nuo 2020-01-06 iki 2020-01-17. Respondentai teikė pavienes pastabas, kad metodikose ne viskas aptariama, bet nepateikė kritinių pastabų dėl jų netinkamumo.

88. Siekiant palengvinti NEE ikiteisminių tyrimų atlikimą, kartu gerinant NEE ištyrimą, siūloma įvertinti metodinių rekomendacijų NEE srityje poreikį ir jas parengti. Pažymėtina, kad GP parengė ir audito metu patvirtino metodines rekomendacijas dėl kriptovaliutų[207].

Vis dar visu pajėgumu neveikia nusikaltimų elektroninėje erdvėje specializuotų prokurorų tinklas, o pareigūnai jo neturi

89. Europos Sąjungos Tarybos 2017 m. vertinimo ataskaitoje apie Lietuvą [208] nurodyta, kad valstybės narės turėtų apsvarstyti galimybes sukurti pareigūnų, kurie specializuojasi kibernetinio nusikalstamumo srityje nacionaliniu lygmeniu, tinklą, kuriame sistemos dalyviai galėtų keistis gerąja praktika bei patirtimi.

90. 2019 m. rugpjūčio mėn. įsteigtas[209] prokurorų, besispecializuojančių NEE tyrimuose, tinklas „Cyberpro“. Į šio tinklo veiklą įtraukti 15 apygardų prokuratūrų bei GP NEE srityje besispecializuojantys prokurorai. GP duomenimis, tinklas pradės veikti visu pajėgumu 2020 m. ir turėtų sudaryti sąlygas keistis žiniomis NEE srityje tarp prokurorų, o informaciją apie tinklo narius planuojama viešinti, kad būtų galima prireikus pasikonsultuoti ar suteikti pagalbą sunkesnėse bylose [210]. Pažymėtina, kad NEE besispecializuojantys pareigūnai tokio tinklo neturi.

91. Siekiant gerinti ir stiprinti pareigūnų kompetenciją, gebėjimus ir tyrimų rezultatyvumą, reikia sukurti NEE besispecializuojančių pareigūnų tinklą ir užtikrinti jo aktyvią veiklą.

[207] Lietuvos Respublikos generalinio prokuroro 2020-03-09 įsakymas Nr. I-64 „Dėl Proceso veiksmų su virtualiosiomis valiutomis atlikimo metodinių rekomendacijų patvirtinimo“.

[208] Prieiga per internetą: http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/lt/pdf.

[209] Tinklo koordinatoriaus, Generalinės prokuratūros Baudžiamojo persekiojimo departamento vyriausiojo prokuroro pavaduotojo 2019-09-17 patvirtintas Prokurorų, besispecializuojančių nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui baudžiamojo persekiojimo srityje, tinklo „CYBERPRO“ narių sąrašas Nr. 17.9.-11920.

[210] 2020-01-30 susitikimo su GP atstovais protokolas.

4. KOVAI SU ELEKTRONINIAIS NUSIKALTIMAIS REIKIA SKIRTI DIDESNĮ DĖMESĮ

92. 2015 m. Europos Sąjungos Tarybos išvadose dėl atnaujintos 2015–2020 m. ES Vidaus saugumo strategijos[211] paskelbta, kad kova su NEE yra vienas iš trijų pagrindinių saugumo prioritetų. NEE viena greičiausiai augančių ir besikeičiančių nusikalstamumo formų, todėl svarbu žinoti, kokia yra NEE srities būklė, pokyčiai, ir laiku reaguoti į juos[212].

93. Laikytasi nuostatos, kad NEE užkardymo ir ištyrimo gerinimui sudarytos sąlygos, kai:

- nacionaliniuose strateginiuose dokumentuose numatytos priemonės sprendžia aktualias NEE srities problemas[213];
- nuolatos atliekama NEE tiriančių institucijų ir padalinių veiklos kontrolė, kuri prisideda prie veiklos gerinimo[214];
- nustatytas NEE klasifikatorius, kuris sudaro sąlygas bendrai rinkti informaciją apie visus NEE[215].

4.1. Strateginio planavimo ir vidaus kontrolės priemonės nepakankamos nusikaltimų elektroninėje erdvėje užkardymo ir ištyrimo gerinimui

94. Lietuvos siekis mažinti NEE ir plėtoti gebėjimus kovoti su jais numatytas Viešojo saugumo plėtros 2015–2025 m. programoje[216] ir Nacionalinėje kibernetinio saugumo strategijoje[217]. Įgyvendinant tikslą, šių strateginių dokumentų įgyvendinimo tarpinstituciniuose veiklos planuose nustatyti uždaviniai ir priemonės NEE srityje[218] (žr. 25 pav.).

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

[212] CobiT 4.1 metodika – ME1 „IT veiklos stebėsena ir vertinimas“, ME2 „Vidaus kontrolės stebėsena ir vertinimas“, ME4 „IT valdymo užtikrinimas“.

[213] ENISA gairės dėl ES kibernetinio saugumo strategijų, prieiga per internetą: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

[214] 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.

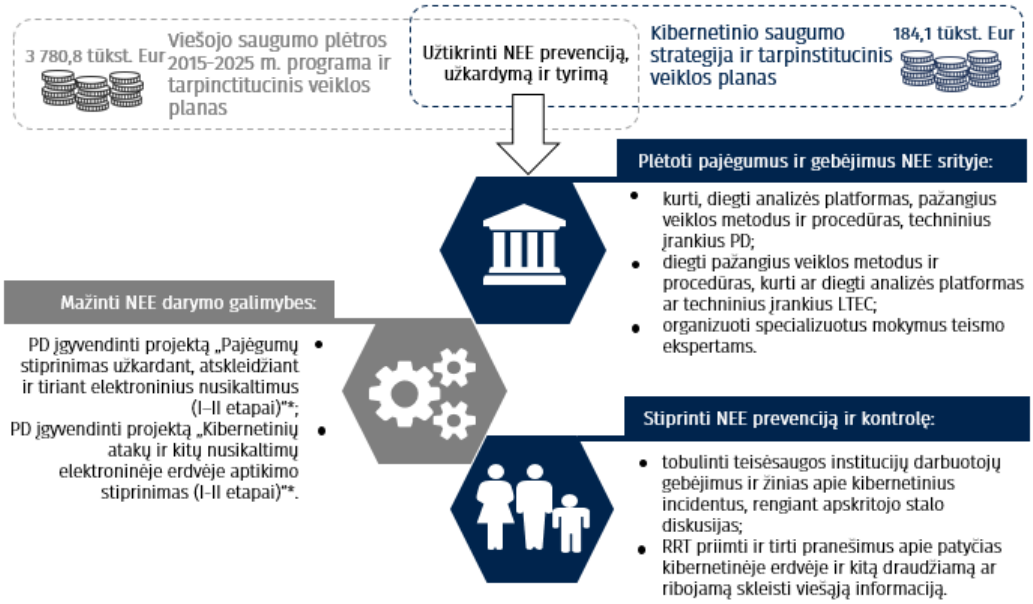
[215] Prieiga per internetą: http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/lt/pdf.

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

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

[218] Vyriausybės 2016-04-13 nutarimu Nr. 370 patvirtintas Viešojo saugumo plėtros 2015–2025 m. programos įgyvendinimo tarpinstitucinis veiklos planas; Vyriausybės 2019-07-03 nutarimu Nr. 709 patvirtintas Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas.

25 pav. Strateginiuose dokumentuose numatyti tikslai, uždaviniai ir priemonės NEE srityje



* Įsigyta specializuota programinė įranga

Šaltinis – Valstybės kontrolė pagal strateginio planavimo dokumentus

95. Įvertinus minėtuose strateginiuose dokumentuose numatytus uždavinius ir priemones, auditorių nuomone, jos prisideda prie NEE tiriančių padalinių veiklos gerinimo, bet nėra pakankamos, nes nesprendžia prevencinės veiklos (1.1 poskyris, 18 psl.), neteisėto ir žalingo turinio internete pašalinimo (1.2 poskyrius, 22 psl.), kibernetinių incidentų, kurie galimai yra NEE, valdymo (2 skyrius, 26 psl.), sisteminių NEE identifikavimo (3.1.1 poskyris, 39 psl.), specializuotų kompetencijų ugdymo (3.1.3 poskyrius, 45 psl.), ilgų IT objektų tyrimų eilių (3.1.4 poskyrius, 47 psl.), nepakankamo NEE profiliavimo (4 skyrius, 55 psl.) problemų. Tai rodo, kad NEE tyrimo tobulinimui ir vystymui skiriamas nepakankamas dėmesys.

96. Siekiant gerinti darbo organizavimo efektyvumą ir produktyvumą užkardant, atskleidžiant ir tiriant NEE, LKPB Veiklos koordinavimo ir kontrolės valdyba 2018–2019 m. atliko KP NEE specializuotų padalinių nuotolinę stebėseną ir tikrinimus septyniose AVPK KP NNTV ir NTS[219]. Buvo vertinamas etatų pokytis, funkcijų ir darbo krūvių paskirstymas, veiklos rezultatyvumas ir intensyvumas, darbo organizavimas, atliekamų proceso veiksmų kokybė, padalinio procesinės veiklos kontrolė, kt. Ataskaitose pateikiamos išvados dėl pastebėtų veiklos trūkumų ir teikiami AVPK pasiūlymai dėl veiklos gerinimo (žr. pavyzdį).

LKPB VKKV po atliktų tikrinimų teiktų siūlymų AVPK dėl veiklos gerinimo pavyzdžiai[220]

- Padalinio struktūros išgrynimui: suvienodinti pareigybes, padidinti vyriausiųjų tyrėjų santykinę dalį, atsisakyti tyrėjų pareigybių, specialistus, atliekančius įvykio vietos objektų apžiūras ar tyrimus, perkelti į kriminalistinių tyrimų padalinį, atsisakyti pareigybių, kurioms pavestos pagalbinės funkcijos.

[219] Lietuvos kriminalinės policijos biuro VKKV veiklos patikrinimo ataskaitos: Vilniaus AVPK KP NNTV 2019-04-12, Kauno AVPK KP NNTV 2019-11-05, Klaipėdos AVPK KP NNTV 2018-10-30, Šiaulių AVPK KP NNTV 2020-02-03, Tauragės AVPK KP NTS 2018-11-27, Utenos AVPK KP NTS 2018-04-23, Marijampolės AVPK KP NTS 2018-05-11.

[220] Lietuvos kriminalinės policijos biuro VKKV veiklos patikrinimo ataskaitos: Vilniaus AVPK KP NNTV 2019-04-12, Kauno AVPK KP NNTV 2019-11-05, Klaipėdos AVPK KP NNTV 2018-10-30, Šiaulių AVPK KP NNTV 2020-02-03, Tauragės AVPK KP NTS 2018-11-27, Utenos AVPK KP NTS 2018-04-23, Marijampolės AVPK KP NTS 2018-05-11.

- Ikiteisminio tyrimo pareigūnų darbo krūvio mažinimui: komplektuoti neužimtas pareigybes, atlikti ikiteisminius tyrimus, kurie reikalauja ypatingų specifinių žinių ar tyrimo priemonių panaudojimo.
- Ikiteisminių tyrimų atlikimo trukmės mažinimui: specialistų kompiuterinės technikos pažiūrai bei tyrimams skaičiaus didinimas kriminalistinių tyrimų padalinyje.
- Sisteminių nusikaltimų užkardymui, atskleidimui ir tyrimui: periodiškai keistis informacija apie šiuos nusikaltimus, nuolatos vykdyti sisteminių nusikalstamų veikų, vykdomų aptarnaujamoje teritorijoje, stebėseną ir spręsti dėl ikiteisminių tyrimų perėmimo iniciavimo.
- Kompetencijų gerinimui: skatinti pareigūnus maksimaliai išnaudoti ES teisėsaugos mokymo agentūros CEPOL teisėsaugos pareigūnams skirtus nuotolinius mokymus.
- Kriminalinės žvalgybos stiprinimui: atriboti šią žvalgybą vykdančių ir ikiteisminį tyrimą atliekančių pareigūnų funkcijas.

97. NEE besispecializuojantys prokurorai, atlikdami NEE sustabdytų, nutrauktų ikiteisminių tyrimų ir atsisakymų pradėti ikiteisminį tyrimą tikrinimus (per 2017–2019 m. patikrintas 191 procesinis sprendimas), nustato besikartojančias neatitiktis dėl procesinių veiksmų (pvz., dėl netinkamo vietos nustatymo, nusikalstamų veikų kvalifikavimo, įrodymų surinkimo, pakankamo visų reikiamų aplinkybių įvertinimo). Atsižvelgę į tai, prokurorai teikia siūlymus dėl veiklos tobulinimo (žr. pavyzdį). Taip pat nustatomos problemos dėl sisteminių nusikaltimų identifikavimo.

GP po atliktų tikrinimų teiktų siūlymų dėl veiklos gerinimo pavyzdžiai[221]

- Organizuoti mokymus ikiteisminio tyrimo pareigūnams bei prokurorams dėl nusikaltimų elektroninėje erdvėje tyrimo ir kvalifikavimo ypatumų.
- Sustiprinti teritorinių prokuratūrų aukštesniųjų prokurorų atliekamą pavaldžių prokurorų priimamų proceso sprendimų kontrolę ikiteisminiuose tyrimuose, užtikrinant priimamų procesinių sprendimų teisėtumą ir pagrįstumą.
- Veiksmingos praktikos formavimui, sėkmingai komunikacijai, pasidalinimui gerąja praktika bei konkrečių klausimų aptarimui tikslinga sukurti vidinį specializuotų prokurorų tinklą, organizuoti periodinius susitikimus aktualiais klausimais.
- Nustačius pažeidimus, spręsti klausimą dėl reagavimo raštų apygardų vyriausiesiems prokurorams parengimo.

98. Įvertinę minėtų GP ir LKPB atliktų tikrinimų ataskaitas ir juose teiktus siūlymus dėl veiklos gerinimo, nustatėme, kad šios priemonės taip pat nesprendžia sisteminių problemų NEE srityje, nes jos vis dar nėra išspręstos.

99. Siekiant gerinti NEE užkardymą ir tyrimą, svarbu nacionaliniuose strateginiuose planavimo dokumentuose numatyti uždavinius ir priemones, kurie būtų nukreipti spręsti aktualias NEE srities problemas ir užtikrintų reikiamų pokyčių įgyvendinimą.

4.2. Nepakankamas nusikaltimų elektroninėje erdvėje profiliavimas

100. Pagal ES Tarybą, siekiant įvertinti įvairių rūšių NEE keliamą grėsmę, padėti efektyviau atlikti tyrimus, o politikos formuotojui – priimti strateginius sprendimus, ypač svarbu

[221] GP Baudžiamojo persekiojimo departamento patikrinimų pažymos dėl BK XXX sk. numatytų nusikalstamų veikų: 2020-02-28 Nr. 17.9.-3057, 2019-05-27 Nr. 17.9.-7497, 2019-06-13 Nr. 17.9-8352, 2019-06-27 Nr. 17.9.-8780, 2018-08-03 Nr. 17.9.-11140, 2017-07-07 Nr. 17.9.-3949.

rinkti patikimą ir išsamią statistiką apie NEE[222]. Ji turėtų apimti ikiteisminį tyrimą ir teismą, pvz., nusikalstamos veikos rūšį ir konkrečią tyrimo priemonę, nusikaltimų, apie kuriuos pranešta, skaičių, atliktų tyrimų skaičių ir sprendimus netirti tam tikrų rūšių NEE, nukentėjusiųjų ir jų skundų skaičių, asmenų, kurie buvo patraukti baudžiamojon atsakomybėn ir nuteisti už įvairių rūšių NEE, bei tarpvalstybinių bylų skaičių, savitarpio teisinės pagalbos prašymų rezultatus ir procedūros trukmę[223].

101. Lietuvoje duomenys apie nusikalstamas veikas, kartu ir apie NEE yra kaupiami Nusikalstamų veikų žinybiniame registre. Jis duomenis apie užregistruotas, ištirtas nusikalstamas veikas gauna iš Integruotos baudžiamojo proceso informacinės sistemos[224]. Šie duomenys naudojami policijos įstaigose atliekant nacionalinį sunkaus ir organizuoto nusikalstamumo grėsmių vertinimą, kurio metu analizuojamos nusikalstamumo tendencijos, galimos jų raidos prognozės. Atsižvelgiant į tai, teikiamos rekomendacijos dėl prioritetinių nusikalstamų veikų tyrimo krypčių ir reikiamų atlikti prevencinių darbų.

102. Peržiūrėję 2019 m. teritorinio, nacionalinio sunkaus ir organizuoto nusikalstamumo grėsmių vertinimo ataskaitas nustatėme, kad NEE profilis apima nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui (BK XXX sk.) ir nusikaltimus, susijusius su vaikų seksualiniu išnaudojimu elektroninėje erdvėje, tačiau neapima kitų nusikalstamų veikų (tradicinių), kurios padarytos šioje erdvėje ir nurodytos Konvencijoje dėl elektroninių nusikaltimų[225] (kompiuterinių sukčiavimų, nusikaltimų susijusių su autorių teisių ir gretutinių teisių pažeidimais, rasistinio ir ksenofobinio pobūdžio nusikaltimų).

103. Kadangi NEE profilis neapima visų nusikalstamų veikų NEE srityje, policijos registruose nėra renkama, sisteminama ir analizuojama visa informacija apie NEE, todėl gali būti neanalizuojama faktinė jų grėsmių apimtis ir tendencijos. Susipažinus su GP[226] ir PD[227] strateginiais planavimo dokumentais nustatyta, kad pagal juose numatytą vertinimo kriterijų, kuris skirtas matuoti NEE srities ištyrimo rezultatus[228], apskaičiuojami tik nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui (BK XXX sk.) ištyrimo rezultatai. Todėl GP[229] ir LKPB[230] veiklos ataskaitose skelbiami nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui ištyrimo rezultatai (2017 m.: GP

[222] 2017-10-02 galutinė ataskaita dėl Europos kibernetinio nusikalstamumo prevencijos ir kovos su tokiu nusikalstamumu politikos praktinio įgyvendinimo ir veikimo septintojo tarpusavio vertinimo etapo, prieiga per internetą: http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/lt/pdf.

[223] Ten pat, 20 psl.

[224] Vidaus reikalų ministro 2015-08-27 įsakymu Nr. 1V-667 patvirtinti Nusikalstamų veikų žinybinio registro nuostatai, Vidaus reikalų ministerijos 2020-06-23 raštas Nr. 1D-3189.

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

[226] Generalinio prokuroro 2020-02-21 įsakymu Nr. I-56 patvirtintas Generalinės prokuratūros 2020–2022 m. strateginis veiklos planas.

[227] Vidaus reikalų ministro 2019-02-06 įsakymu Nr. 1V-126 patvirtintas Policijos departamento 2019–2021 m. strateginis veiklos planas.

[228] NEE Ištyrimo rodiklis skaičiuotas pagal formulę X = (A / B) × 100 proc. A – per ataskaitinį laikotarpį policijos įstaigose ištirtų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui (BK 196– 198[2] str.) skaičius. B – ataskaitiniu laikotarpiu užregistruotų nusikalstamų veikų (BK XXX sk. 196–198[2] str.) skaičius.

[229] Prieiga per internetą: https://www.prokuraturos.lt/lt/administracine-informacija/planavimo-dokumentai-ataskaitos/ataskaitos/138.

[230] Prieiga per internetą: http://lkpb.policija.lrv.lt/lt/administracine-informacija/ataskaitos; https://www.ird.lt/lt/paslaugos/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos/nusikalstamu-veiku-zinybinio-registro-nvzr-atviri-duomenys-paslaugos/ataskaitos-1/nusikalstamumo-ir-ikiteisminiu-tyrimu-statistika-1/view_item_datasource?id=8175&datasource=40985.

– 81 proc., LKPB – 112,6 proc.; 2018 m.: GP – 76 proc., LKPB – 81,8 proc.; 2019 m.: GP – 55 proc., LKPB – 50,3 proc.). Tokie rezultatai neparodo visos NEE ištyrimo būklės. Visos informacijos apie NEE neturėjimas gali neigiamai veikti priimamus strateginius sprendimus ir tinkamą reagavimą į vykstančius pokyčius šioje srityje.

104. Minėto vertinimo kriterijaus reikšmė 2015–2019 m. PD[231] ir GP[232] strateginiuose planavimo dokumentuose skyrėsi 26 proc. (GP 70 proc., PD 96 proc.). Nuo 2020 m. numatytas vienodas 50 proc. NEE ištyrimo kriterijus. Tačiau Viešojo saugumo plėtros 2015–2025 m. programos įgyvendinimo tarpinstituciniame veiklos plane lieka 96 proc. NEE ištyrimas[233]. Auditorių vertinimu, svarbu nustatyti tyrimų praktiką atitinkančius ambicingus rodiklius, kurie turi būti suvienodinti visų lygių strateginiuose planavimo dokumentuose, kitaip išlieka neaiškumas dėl siektinų veiklos rezultatų ir jų įgyvendinimo būklės.

105. Siekiant rinkti, sisteminti ir analizuoti informaciją apie visus NEE, reikia peržiūrėti ir įvertinti NEE profilio apimtį, užtikrinant visų nusikalstamų veikų, turinčių NEE požymių, rinkimą, sisteminimą ir panaudojimą grėsmių analizei ir strateginiams sprendimams priimti. Be to, siūloma tobulinti NEE srities vertinimo kriterijus, suvienodinti juos visuose strateginio planavimo dokumentuose ir sudaryti sąlygas matuoti visų NEE ištyrimo būklę.

[231] Vidaus reikalų ministro 2020-02-17 įsakymu Nr. 1V-137 patvirtintas vidaus reikalų ministrui pavestų valdymo sričių 2020–2022 m. strateginis veiklos planas.

[232] Generalinio prokuroro 2020-02-21 įsakymu Nr. I-56 patvirtintas Generalinės prokuratūros 2020–2022 m. strateginis veiklos planas.

[233] Vyriausybės 2016-04-13 nutarimu Nr. 370 patvirtintas Viešojo saugumo plėtros 2015–2025 metų programos įgyvendinimo tarpinstitucinio veiklos planas, vertinimo kriterijaus kodas P-2-2-1.

REKOMENDACIJŲ ĮGYVENDINIMO PLANAS

Laukiamas audito poveikis: didės visuomenės saugumas elektroninėje erdvėje ir gerės elektroninių nusikaltimų ištyrimas.

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama)	Pokyčio vertinimo rodikliai ir jų reikšmės*			Pokyčio rodiklio matavimo data ir periodiškumas pagal poreikį**	Atsakingas (-i) subjektas (-ai)	Rekomendacijos (-ų) įgyvendinimo terminas (pokyčio pasiekimo terminas)**
		rodiklis	pradinė reikšmė	siektina reikšmė			
1-asis pagrindinis audito rezultatas Prevencinė veikla neužtikrina visuomenės saugumo elektroninėje erdvėje, nes: • šalies mastu nesukurta tarpinstitucinė prevencinės veiklos planavimo, koordinavimo ir poveikio matavimo sistema; • nesudarytos sąlygos šalinti neteisėtą ir žalingą turinį elektroninėje erdvėje.	**Didelės svarbos** 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. **Vidutinės svarbos** 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; 2.2. užtikrinti bendrą blokavimo įgaliojimų įgyvendinimo tvarką.	Gyventojų, žinančių apie oficialius kanalus [234], kuriais galima pranešti apie elektroninius nusikaltimus ar kitą neteisėtą veiką internete, dalis	17 proc.	30 proc.	2021, 2022, 2023, 2024 m.	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Policijos departamentas	2024 m.
		Gyventojų, kurie mano, kad nėra gerai informuoti arba yra visiškai neinformuoti apie elektroninių nusikaltimų grėsmes, dalis	42 proc.	35 proc.	2021, 2022, 2023, 2024 m.	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Policijos departamentas	2024 m.
		Gyventojų, kurie mano, kad yra pajėgūs veiksmingai apsisaugoti nuo elektroninių nusikaltimų, dalis	40 proc.	55 proc.	2021, 2022, 2023, 2024 m.	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Policijos departamentas	2024 m.
		Priemonės**				**Subjektas, įgyvendinantis priemones**	**Priemonių įgyvendinimo ir informavimo apie jį terminas*** **
		1. Sukurti ir įgyvendinti tarpinstitucinio bendradarbiavimo mechanizmą, užtikrinantį tarpinstitucinį prevencinės veiklos nusikaltimų elektroninėje erdvėje srityje planavimą, koordinavimą ir poveikio matavimą. 2.1. Parengti ir pateikti Vyriausybei teisės aktų projektus, sudarančius teisines prielaidas veiksmingiau šalinti neteisėtą ir žalingą turinį internete. 2.2. Parengti ir pateikti Vyriausybei pasiūlymus, prireikus – teisės aktų projektus dėl blokavimo įgaliojimų įgyvendinimo tvarkos suvienodinimo.					Vidaus reikalų ministerija	1. 2022 m. II ketvirtis**** 2.1. 2023 m. II ketvirtis**** 2.2. 2023 m. II ketvirtis****

[234] Interneto svetainė, el. pašto adresas, internetinė forma ar telefono numeris.

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama)	Pokyčio vertinimo rodikliai ir jų reikšmės*			Pokyčio rodiklio matavimo data ir periodiškumas pagal poreikį**	Atsakingas (-i) subjektas (-ai)	Rekomendacijos (-ų) įgyvendinimo terminas (pokyčio pasiekimo terminas)**
		rodiklis	pradinė reikšmė	siektina reikšmė			
2-asis pagrindinis audito rezultatas Kibernetinių incidentų valdymas nesudaro sąlygų identifikuoti galimai nusikalstamas veikas: • nėra kriterijų (bendros taksonomijos), pagal kuriuos būtų galima identifikuoti, kurie kibernetiniai incidentai galimai yra nusikaltimai elektroninėje erdvėje; • nesudarytos sąlygos kibernetinius incidentus, kurie galimai yra nusikaltimai elektroninėje erdvėje, valdyti taikant vieno langelio principą; • neaiškus informavimo apie kibernetinius incidentus reglamentavimas; • trūksta metodinio vadovavimo, konsultacijų ir mokymų, kurie stiprintų kibernetinio saugumo subjektų gebėjimus atpažinti ir reaguoti į nusikalstamas veikas; • Lietuvos kriminalinės policijos biuras neskiria pakankamai žmogiškųjų išteklių vykdyti incidentų, kurie galimai yra nusikaltimai elektroninėje erdvėje, stebėsenai ir analizei.	**Didelės svarbos** 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; 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. **Vidutinės svarbos** 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; 4.2. parengti metodinius dokumentus dėl incidento žalos / nuostolio įvertinimo, elektroninių įrodymų rinkimo ir išsaugojimo.	Rezultatyviais kriminalinės žvalgybos tyrimais užbaigtų bylų dalis tiriant kibernetinius incidentus	0 proc.	60 proc.	2023 m.	Policijos departamentas, Krašto apsaugos ministerija, Generalinė prokuratūra	2025 m.
		Priemonės**				**Subjektas, įgyvendinantis priemones**	**Priemonių įgyvendinimo ir informavimo apie jį terminas*** **
		3.1. Įgyvendinant 3.1 rekomendaciją, parengti rekomendacijas, nustatančias kriterijus, kuriais remiantis kibernetiniai incidentai galėtų būti identifikuojami kaip galimos nusikalstamos veikos ir suderinti jas su Generaline prokuratūra.				3.1. Policijos departamentas	3.1. 2021-12-31
		3.2. Įgyvendinant 3.2 rekomendaciją: 3.2.1. Parengti Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo projektą, papildant Nacionalinį kibernetinių incidentų valdymo planą reikalingomis nuostatomis dėl visų Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos teikiamų pranešimų apie kibernetinius incidentus, kurie galimai yra nusikaltimai elektroninėje erdvėje, privalomo pateikimo vieno langelio principu kibernetinius incidentus valdančioms ir (ar) tiriančioms institucijoms; 3.2.2. Esant poreikiui, bendradarbiaujant su Policijos departamentu, įdiegti reikalingus techninius sprendimus vieno langelio principo įgyvendinimui.				3.2. Krašto apsaugos ministerija, Policijos departamentas	3.2.1. 2022-12-31 3.2.2. 2023-06-30
		4.1. Įgyvendinant 4.1 rekomendaciją, į planavimo dokumentus, rengiamus Nacionalinės pažangos planui įgyvendinti, įtraukti priemonę dėl periodiškai (ne rečiau kaip 2 kartus per metus), bendradarbiaujant su Lietuvos policija ir Generaline prokuratūra, kibernetinio saugumo subjektams organizuojamų kibernetinio saugumo mokymų, kurių metu būtų suteikiamos reikiamos teisinės bei techninės žinios apie nusikaltimus elektroninėje erdvėje bei užtikrinti šios priemonės įgyvendinimą.				4.1. Krašto apsaugos ministerija, Generalinė prokuratūra	4.1. 2022-12-31
		4.2. Įgyvendinant 4.2 rekomendaciją, parengti rekomendacijas dėl incidento žalos / nuostolio įvertinimo, elektroninių įrodymų rinkimo ir išsaugojimo.				4.2. Policijos departamentas	4.2. 2021-12-31
2-asis pagrindinis audito rezultatas	**Didelės svarbos** 5. Siekiant didinti nusikaltimų elektroninėje erdvėje tyrimų rezultatyvumą:	Specializuotų padalinių veiklos rezultatyvumas	29 proc.	40 proc.	2023 m.	Policijos departamentas,	2025 m.

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama)	Pokyčio vertinimo rodikliai ir jų reikšmės*			Pokyčio rodiklio matavimo data ir periodiškumas pagal poreikį**	Atsakingas (-i) subjektas (-ai)	Rekomendacijos (-ų) įgyvendinimo terminas (pokyčio pasiekimo terminas)**
		rodiklis	pradinė reikšmė	siekiama reikšmė			
Kibernetinių incidentų valdymas nesudaro sąlygų identifikuoti galimai nusikalstamas veikas, nes Lietuvos kriminalinės policijos biuras neskiria pakankamai žmogiškųjų išteklių vykdyti incidentų, kurie galimai yra nusikaltimai elektroninėje erdvėje, stebėsenai ir analizei. **3-iasis pagrindinis audito rezultatas** Nusikaltimų elektroninėje erdvėje tyrimas nepakankamai rezultatyvus, nes: • šalies mastu neužtikrinamas sisteminių nusikaltimų elektroninėje erdvėje identifikavimas; • trūksta specializuotų pajėgumų tirti nusikaltimus elektroninėje erdvėje ir ikiteisminių tyrimų paskirstymo mechanizmas neužtikrina privalomos kompetencijos specializuotiems pareigūnams ir prokurorams; • nepakankamai veiksmingas specializuotų pareigūnų ir prokurorų ugdymo organizavimas; • ilgai trunka informacinių technologijų objektų tyrimai.	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; 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; 5.3. sukurti nusikaltimų elektroninėje erdvėje besispecializuojančių pareigūnų tinklą ir užtikrinti jo aktyvią veiklą.					Generalinė prokuratūra, Kalėjimų departamentas, Vidaus reikalų ministerija Krašto apsaugos ministerija	
		Prokurorų panaikintų sprendimų sustabdyti, nutraukti arba atsisakyti pradėti nusikaltimų elektroninėje erdvėje ikiteisminį tyrimą dalis nuo visų tikrintų	11 proc.	5 proc.	2023 m.	Policijos departamentas, Generalinė prokuratūra	2025 m.
		Priemonės**				**Subjektas, įgyvendinantis priemones**	**Priemonių įgyvendinimo ir informavimo apie jį terminas*** **
		5.1. Įgyvendinant 5.1 rekomendaciją: 5.1.1. Peržiūrėti nusikaltimų elektroninėje erdvėje specializuotų padalinių veiklos modelį, parengti efektyvios šių padalinių veiklos koncepciją bei ją įgyvendinti. 5.1.2. Atlikti išsamią šios srities specializuotiems pareigūnams būtinų įrankių poreikių analizę, teikti siūlymus dėl jų įsigijimo, diegimo. 5.1.3. Užtikrinti efektyvesnį kriminalistinių tyrimų veiklos modelį teritorinėse policijos įstaigose, įgyvendinti veiksmingą šios srities veiklos bei koordinavimo politiką, mažinant NEE ekspertinių tyrimų trukmę ir eiles. 5.1.4. Vykdyti tęstines kontrolės priemones informacijos apie identifikuotus sisteminius nusikaltimus valdymo srityje. 5.2. Įgyvendinant 5.2 rekomendaciją: 5.2.1. Parengti ir patvirtinti kriminalinės policijos specializuotiems pareigūnams skirtą nusikaltimų elektroninėje erdvėje mokymų programą, atitinkančią pareigūnų ugdymo poreikius šioje srityje. 5.2.2. Pagal parengtą programą apmokyti visus NEE besispecializuojančius pareigūnus. 5.3. Įgyvendinant 5.3 rekomendaciją: 5.3.1. Sukurti nusikaltimų elektroninėje erdvėje besispecializuojančių pareigūnų tinklą į jo veiklą įtraukiant visus NEE specializuotus pareigūnus.				Policijos departamentas	5.1. 2025-12-31 5.2. 2023-12-31 5.3. 2021-12-31

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama)	Pokyčio vertinimo rodikliai ir jų reikšmės*			Pokyčio rodiklio matavimo data ir periodiškumas pagal poreikį**	Atsakingas (-i) subjektas (-ai)	Rekomendacijos (-ų) įgyvendinimo terminas (pokyčio pasiekimo terminas)**
		rodiklis	pradinė reikšmė	siektina reikšmė			
4-asis pagrindinis audito rezultatas Neskiriamas pakankamas dėmesys nusikaltimų elektroninėje erdvėje srities prevencijos ir ištyrimo gerinimui, nes nusikaltimų elektroninėje erdvėje profilis neapima visų nusikalstamų veikų, kurios padarytos elektroninėje erdvėje.	**Vidutinės svarbos** 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.	Gyventojų, žinančių apie oficialius kanalus [235], kuriais galima pranešti apie elektroninius nusikaltimus ar kitą neteisėtą veiklą internete, dalis	17 proc.	30 proc.	2021, 2022, 2023, 2024 m.	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Policijos departamentas	2024 m.
		Gyventojų, kurie mano, kad nėra gerai informuoti arba yra visiškai neinformuoti apie elektroninių nusikaltimų grėsmes, dalis	42 proc.	35 proc.	2021, 2022, 2023, 2024 m.	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Policijos departamentas	2024 m.
		Gyventojų, kurie mano, kad yra pajėgūs veiksmingai apsisaugoti nuo elektroninių nusikaltimų, dalis	40 proc.	55 proc.	2021, 2022, 2023, 2024 m.	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Policijos departamentas	2024 m.
		Rezultatyviais kriminalinės žvalgybos tyrimais užbaigtų bylų dalis tiriant kibernetinius incidentus	0 proc.	60 proc.	2023 m.	Policijos departamentas, Krašto apsaugos ministerija, Generalinė prokuratūra	2025 m.
		Specializuotų padalinių veiklos rezultatyvumas	29 proc.	40 proc.	2023 m.	Policijos departamentas, Generalinė prokuratūra, Kalėjimų departamentas, Vidaus reikalų ministerija Krašto apsaugos ministerija	2025 m.
		Prokurorų panaikintų sprendimų sustabdyti, nutraukti arba atsisakyti pradėti nusikaltimų	11 proc.	5 proc.	2023 m.	Policijos departamentas, Generalinė prokuratūra	2025 m.

[235] Interneto svetainė, el. pašto adresas, internetinė forma ar telefono numeris.

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama)	Pokyčio vertinimo rodikliai ir jų reikšmės*			Pokyčio rodiklio matavimo data ir periodiškumas pagal poreikį**	Atsakingas (-i) subjektas (-ai)	Rekomendacijos (-ų) įgyvendinimo terminas (pokyčio pasiekimo terminas)**
		rodiklis	pradinė reikšmė	siektina reikšmė			
		elektroninėje erdvėje ikiteisminį tyrimą dalis nuo visų tikrintų					
		Priemonės**				**Subjektas, įgyvendinantis priemones**	**Priemonių įgyvendinimo ir informavimo apie jį terminas*****
		6. Įgyvendinant 6 rekomendaciją: 6.1. Įtraukti į NEE profilį aktualius nusikaltimus. 6.2. Naudoti juos grėsmių analizei ir strateginių sprendimų priėmimui.				Policijos departamentas	2023-12-31
3-iasis pagrindinis audito rezultatas Nusikaltimų elektroninėje erdvėje tyrimas nepakankamai rezultatyvus, nes: • ikiteisminių tyrimų paskirstymo mechanizmas neužtikrina privalomos kompetencijos specializuotiems pareigūnams ir prokurorams; • nepakankamai veiksmingai organizuojamas specializuotų pareigūnų ir prokurorų ugdymas.	**Vidutinės svarbos** 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; 7.2. didinti nusikaltimų elektroninėje erdvėje mokymų specializuotiems prokurorams apimtis ir užtikrinti, kad šiose mokymuose dalyvautų visi specializuoti prokurorai; 7.3. parengti bendrą nusikaltimų elektroninėje erdvėje specializuotų pareigūnų ir prokurorų mokymų programą ir ją įgyvendinti; 7.4. įvertinti metodinių rekomendacijų, skirtų nusikaltimų elektroninėje erdvėje tyrimui, poreikį ir jas parengti.	Specializuotų padalinių veiklos rezultatyvumas	29 proc.	40 proc.	2023 m.	Policijos departamentas, Generalinė prokuratūra, Kalėjimų departamentas, Vidaus reikalų ministerija Krašto apsaugos ministerija	2025 m.
		Prokurorų panaikintų sprendimų sustabdyti, nutraukti arba atsisakyti pradėti nusikaltimų elektroninėje erdvėje ikiteisminį tyrimą dalis nuo visų tikrintų	11 proc.	5 proc.	2023 m.	Policijos departamentas, Generalinė prokuratūra	2025 m.
		Priemonės**				**Subjektas, įgyvendinantis priemones**	**Priemonių įgyvendinimo ir informavimo apie jį terminas*****
		7.1. Įvertinus esamą prokurorų specializacijos reglamentavimą, parengti atitinkamų teisės aktų pakeitimų projektus. 7.2. Ne rečiau kaip kartą per metus organizuoti mokymus, kurių metu būtų apmokyti visi prokurorai, kurių tiesioginės funkcijos susijusios su NEE kontrole ir vadovavimu. Mokintinų specializuotų prokurorų skaičius bus nustatytas įgyvendinus 7.1. rekomendaciją, o mokymai bus surengti remiantis 2020 m. parengta bazinių žinių, reikalingų atliekant					Generalinė prokuratūra	7.1. 2021-12-31 7.2. 2021-12-31, 2022-12-31, 2023-12-31 7.3.1. 2020-12-31 7.3.2. 2023-12-31 7.4. 2022-12-31

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama)	Pokyčio vertinimo rodikliai ir jų reikšmės*			Pokyčio rodiklio matavimo data ir periodiškumas pagal poreikį**	Atsakingas (-i) subjektas (-ai)	Rekomendacijos (-ų) įgyvendinimo terminas (pokyčio pasiekimo terminas)**
		rodiklis	pradinė reikšmė	siektina reikšmė			
		NEE tyrimą, ir specializuotų pareigūnų ir prokurorų mokymų programa (7.3.1 priemonė). 7.3.1. Parengti atliekant NEE tyrimą prokurorams reikalingų bazinių žinių ir bendrą nusikaltimų elektroninėje erdvėje specializuotų pareigūnų ir prokurorų mokymų programą. 7.3.2. Įgyvendinti specializuotų pareigūnų ir prokurorų mokymų programą. 7.4. Apklausiant ikiteisminio tyrimo pareigūnus ir prokurorus, nustatyti metodinių rekomendacijų, skirtų nusikaltimų elektroninėje erdvėje tyrimui atlikti, poreikį ir prireikus jas parengti ar papildyti esamas.					
3-iasis pagrindinis audito rezultatas Specializuotų nusikaltimų elektroninėje erdvėje padalinių veiklos rezultatyvumas yra nepakankamas, nes trūksta specializuotų pajėgumų tirti nusikaltimus elektroninėje erdvėje.	**Didelės svarbos** 8. Siekiant sustabdyti elektroninius nusikaltimus, vykdomus iš laisvės atėmimo vietų, numatyti ir įgyvendinti priemones, kurios užkardytų šiuos nusikaltimus.	Specializuotų padalinių veiklos rezultatyvumas	29 proc.	40 proc.	2023 m.	Policijos departamentas, Generalinė prokuratūra, Kalėjimų departamentas, Vidaus reikalų ministerija, Krašto apsaugos ministerija	2025 m.
		Priemonės**				**Subjektas, įgyvendinantis priemones**	**Priemonių įgyvendinimo ir informavimo apie jį terminas*** **
		8.1. Nuteistųjų, kaip įtariama, organizuojančių nusikalstamas veikas (sukčiavimus), perkėlimas ir koncentravimas atskiruose sektoriuose, kuriuose taikoma sustiprinta priežiūra ar blokuojamas mobilusis ryšys: 8.1.1. Nuteistųjų, kaip įtariama, organizuojančių nusikalstamas veikas (sukčiavimus), identifikavimas ir sąrašo sudarymas. 8.1.2. Nuteistųjų, kaip įtariama, organizuojančių nusikalstamas veikas (sukčiavimus), perkėlimo procedūrų įgyvendinimas. 8.2. Įkalinimo įstaigų techninių, perimetro apsaugos ir vaizdo sistemų modernizavimas, kuriuo siekiama efektyviau užkardyti mobiliųjų telefonų permetimus, įnešimus, įvežimus į įstaigų teritoriją: 8.2.1. Modernizuoti apsaugos ir vaizdo sistemas Alytaus PN, Marijampolės PN, Pravieniškių PN-AK.2 sektoriuje. 8.2.2. Įdiegti papildomas technines priemones daiktų patikrai Vilniaus PN atlikti. 8.3. Nuteistųjų priežiūros sustiprinimas, atsisakant fizinės apsaugos ir nukreipiant daugiau darbuotojų nuteistųjų priežiūrai (užimtumui) užtikrinti:				Kalėjimų departamentas	8.1.1. 2020-08-01 8.1.2. 2020-12-31 8.2.1. 2021-07-01 8.2.2. 2021-12-31 8.3.1. 2021-12-01 8.3.2. 2021-12-30 8.4.1. 2021-07-07 8.4.2. 2021-05-01 8.4.3. 2022-12-01 8.4.4. 2020-12-31 8.5.1. 2020-12-31 8.5.2. 2021-12-31

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama)	Pokyčio vertinimo rodikliai ir jų reikšmės*			Pokyčio rodiklio matavimo data ir periodiškumas pagal poreikį**	Atsakingas (-i) subjektas (-ai)	Rekomendacijos (-ų) įgyvendinimo terminas (pokyčio pasiekimo terminas)**
		rodiklis	pradinė reikšmė	siektina reikšmė			
		8.3.1. Modernizavus įstaigų perimetro apsaugos ir vaizdo sistemas, atsisakyta fizinės apsaugos Alytaus PN – 8-iuose postuose (bokšteliuose), Marijampolės PN – 11-oje postų, Pravieniškių PN-AK – 6-iuose postuose. 8.3.2. Pakeisti Alytaus PN, Marijampolės PN ir Pravieniškių PN-AK apsaugos ir priežiūros postų planus, numatyti papildomus postus nuteistųjų priežiūrai užtikrinti, prioritetą skiriant nuteistųjų, kurie linkę vykdyti nusikalstamas veikas, priežiūrai. 8.4. Nuteistųjų gyvenamųjų patalpų renovavimas iš bendrabutinio į kamerinį tipą. Mobiliojo ryšio detektavimo sistemų diegimas renovuojant ir pertvarkant nuteistųjų gyvenamuosius bendrabučius į kamerinio tipo patalpas: 8.4.1. Alytaus PN nuteistųjų bendrabučio Nr. 2 rekonstrukcija (pertvarkant į kamerinio tipo patalpas). 8.4.2. Pravieniškių PN-AK 1-jo sektoriaus nuteistųjų bendrabučio kapitalinis remontas (pertvarkant į kamerinio tipo patalpas). 8.4.3. Pravieniškių PN-AK 2-jo sektoriaus nuteistųjų bendrabučio kapitalinis remontas (pertvarkant į kamerinio tipo patalpas). 8.4.4. Modulinių konteinerių įrengimas Marijampolės PN, Alytaus PN, Pravieniškių PN-AK. 8.5. Kriminalinės žvalgybos vykdymas ir ikiteisminio tyrimo efektyvumo gerinimas: 8.5.1. Neužimtų pareigybių komplektavimas. 8.5.2. Esamų ir naujai priimtų darbuotojų mokymai.					
4-asis pagrindinis audito rezultatas Neskiriamas pakankamas dėmesys nusikaltimų elektroninėje erdvėje srities prevencijos ir ištyrimo gerinimui, nes: • strateginiuose dokumentuose numatytos priemonės nesprendžia audito metu nustatytas problemas; • strateginiuose planavimo dokumentuose nustatytos	**Didelės svarbos** 9. Siekiant gerinti nusikaltimų elektroninėje erdvėje užkardymą ir tyrimą: 9.1. nacionaliniuose strateginiuose planavimo dokumentuose numatyti priemones, kurios padėtų spręsti aktualias nusikaltimų elektroninėje erdvėje srities problemas; 9.2. tobulinti nusikaltimų elektroninėje erdvėje vertinimo kriterijus, suvienodinant juos visuose strateginio planavimo dokumentuose ir sudarant sąlygas matuoti visų šių nusikaltimų ištyrimo būklę.	Gyventojų, žinančių apie oficialius kanalus [236], kuriais galima pranešti apie elektroninius nusikaltimus ar kitą neteisėtą veiką internete, dalis	17 proc.	30 proc.	2021, 2022, 2023, 2024 m.	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Policijos departamentas	2024 m.
		Gyventojų, kurie mano, kad nėra gerai informuoti arba yra visiškai neinformuoti apie elektroninių nusikaltimų grėsmes, dalis	42 proc.	35 proc.	2021, 2022, 2023, 2024 m.	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Policijos departamentas	2024 m.

[236] Interneto svetainė, el. pašto adresas, internetinė forma ar telefono numeris.

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama)	Pokyčio vertinimo rodikliai ir jų reikšmės*			Pokyčio rodiklio matavimo data ir periodiškumas pagal poreikį**	Atsakingas (-i) subjektas (-ai)	Rekomendacijos (-ų) įgyvendinimo terminas (pokyčio pasiekimo terminas)**
		rodiklis	pradinė reikšmė	siektina reikšmė			
skirtingos nusikaltimų elektroninėje erdvėje ištyrimo reikšmės.		Gyventojų, kurie mano, kad yra pajėgūs veiksmingai apsisaugoti nuo elektroninių nusikaltimų, dalis	40 proc.	55 proc.	2021, 2022, 2023, 2024 m.	Vidaus reikalų ministerija, Krašto apsaugos ministerija, Policijos departamentas	2024 m.
		Specializuotų padalinių veiklos rezultatyvumas	29 proc.	40 proc.	2023 m.	Policijos departamentas, Generalinė prokuratūra, Kalėjimų departamentas, Vidaus reikalų ministerija, Krašto apsaugos ministerija	2025 m.
		Priemonės**				Subjektas, įgyvendinantis priemones	Priemonių įgyvendinimo ir informavimo apie jį terminas***
		9.1. Į planavimo dokumentus, rengiamus Nacionalinės pažangos planui įgyvendinti, įtraukti priemones ir veiksmus aktualioms nusikalstamų veikų elektroninėje erdvėje srities problemoms spręsti.				9.1. Vidaus reikalų ir Krašto apsaugos ministerijos	9.1. 2021 m. IV ketvirtis
		9.2. Parengti rodiklius visų nusikalstamų veikų elektroninėje erdvėje tyrimo rezultatams įvertinti ir juos suderinti visuose atitinkamuose planavimo dokumentuose.				9.2. Vidaus reikalų ministerija	9.2. 2021 m. IV ketvirtis

* Detalūs pokyčių rodyklių duomenys pateikti 2 priede „Pokyčių rodiklių duomenys“.

** Priemones ir terminus joms įgyvendinti, pokyčiui pasiekti ir rodikliams pamatuoti pateikė X subjektas (-ai).

*** Rekomendacijų įgyvendinimo stebėsenos metu gali būti tikslinamos arba keičiamos rekomendacijų įgyvendinimo plane nurodytos priemonės ar pokyčių vertinimo rodikliai Valstybinio audito rekomendacijų įgyvendinimo stebėsenos tvarkos aprašo nustatyta tvarka. Aktualus priemonių ir pokyčių vertinimo rodiklių sąrašas yra pateikiamas Valstybės kontrolės atviruose duomenyse adresu www.vkontrole.lt.

**** Terminas apima atitinkamų teisės aktų priėmimą.

Atstovas ryšiams, atsakingas už Valstybės kontrolės informavimą apie priemonių įgyvendinimą ir kai kurių rodiklių reikšmes plane nustatytais terminais:

Vidaus reikalų ministerijos Viešojo saugumo politikos grupės patarėja Lina Bartaševičiūtė,. el. p. lina.bartaseviciute@vrm.lt, tel. (8 5) 271 8778

Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų politikos grupės patarėja Aušra Pipirienė, el. p. Ausra.Pipiriene@kam.lt, tel. 8 706 80800

Generalinės prokuratūros Baudžiamojo persekiojimo departamento vyriausiojo prokuroro pavaduotojas Zenonas Burokas, el. p. Zenonas.Burokas@prokuraturos.lt, tel. (8 5) 266 2320

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama)	Pokyčio vertinimo rodikliai ir jų reikšmės*			Pokyčio rodiklio matavimo data ir periodiškumas pagal poreikį**	Atsakingas (-i) subjektas (-ai)	Rekomendacijos (-ų) įgyvendinimo terminas (pokyčio pasiekimo terminas)**
		rodiklis	pradinė reikšmė	siektina reikšmė			

Lietuvos kriminalinės policijos biuro Veiklos koordinavimo ir kontrolės valdybos viršininkė Eglė Maziliauskienė, el. p. egle.maziliauskiene@policija.lt, tel. (8 5) 271 9875

Kalėjimo departamento prie Lietuvos Respublikos teisingumo ministerijos Saugumo valdymo skyriaus viršininkas Evaldas Gasparavičius, el. p. evaldas.gasparavicius@kaldep.lt, tel. (8 5) 271 9035

Valdymo audito departamento direktorė Jurgita Grebenkovienė

Vyresnysis valstybinis auditorius Gytis Tamulevičius

PRIEDAI

Valstybinio audito ataskaitos
„Ar veiksmingai kovojama su elektroniniais nusikaltimais“
1 priedas

Santrumpos ir sąvokos

AVPK – apskrities vyriausiasis policijos komisariatas

BK – Lietuvos Respublikos baudžiamasis kodeksas

BPK – Lietuvos Respublikos baudžiamojo proceso kodeksas

CSIRT – Reagavimo į kompiuterinio saugumo incidentus grupė (angl. *Computer Security Incident Response Team*)

Elektroniniai nusikaltimai – nusikalstamos veikos, padarytos elektroninėje erdvėje, nusikalstamos veikos elektroninėje erdvėje, nusikaltimai elektroninėje erdvėje.

ENISA – Europos Sąjungos Kibernetinio saugumo agentūra

ES – Europos Sąjunga

GP – Generalinė prokuratūra

IBPS – Integruota baudžiamojo proceso informacinė sistema

IOCTA – Europolo Sunkaus ir organizuoto nusikalstamumo grėsmių internete vertinimo ataskaita

IT – ikiteisminis tyrimas

IVPK – Informacinės visuomenės plėtros komitetas

KAM – Lietuvos Respublikos krašto apsaugos ministerija

KI – Kibernetinis incidentas

KIVT – kibernetinius incidentus valdanti ir (ar) tirianti institucija (NKSC, VDAI ir policija)[237]

KM – Lietuvos Respublikos krašto apsaugos ministerija

KP – Kriminalinė policija

KP NNTV – Kriminalinės policijos nusikaltimų nuosavybei tyrimo valdyba

KP NTS – Kriminalinės policijos Nusikaltimų tyrimų skyrius

KSS – Kibernetinio saugumo subjektas

[237] Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e16e7761fc4b11e89b04a534c5aaf5ce.

KTC – Kriminalistinių tyrimų centras

KTS – Kriminalistinių tyrimų skyrius

LITEKO – Lietuvos teismų informacinė sistema

LKPB – Lietuvos kriminalinės policijos biuras

LRVK – Lietuvos Respublikos Vyriausybės kanceliarija

LTEC – Lietuvos teismo ekspertizės centras

NEE – nusikaltimai elektroninėje erdvėje pagal Budapešto konvenciją dėl elektroninių nusikaltimų

NEE specializuotas padalinys – Apskrities vyriausiojo policijos komisariato Kriminalinės policijos Nusikaltimų nuosavybei tyrimų vadyba ir Nusikaltimų tyrimų skyrius, Lietuvos kriminalinės policijos biuro Sunkaus ir organizuotos nusikalstamumo tyrimo 5-oji valdyba (SO5)

NKSC – Nacionalinis kibernetinio saugumo centras prie Lietuvos Respublikos krašto apsaugos ministerijos

NPLC – Nusikalstamumo prevencijos Lietuvoje centras

NTA – Nacionalinė teismų administracija

NVŽR – Nusikalstamų veikų žinybinis registras

PD – Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos

PĮ – programinė įranga

RRT – Lietuvos Respublikos ryšių reguliavimo tarnyba

TM – Lietuvos Respublikos teisingumo ministerija

VDAI – Valstybinė duomenų apsaugos inspekcija

VKKV – Lietuvos kriminalinės policijos biuro Veiklos koordinavimo ir kontrolės valdyba

VRM – Lietuvos Respublikos vidaus reikalų ministerija

VšĮ – viešoji įstaiga

VVTAT – Valstybinė vartotojų teisių apsaugos tarnyba

ŽEIT – Žurnalistų etikos inspektoriaus tarnyba

Valstybinio audito ataskaitos
„Ar veiksmingai kovojama su elektroniniais nusikaltimais“
2 priedas

Audito apimtis ir metodai

Audito apimtis

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

Pagrindiniai audito klausimai:

- ar prevencinė veikla planuojama ir įgyvendina taip, kad užtikrintų NEE prevencinė veiklos tikslų pasiekimą;
- ar užtikrinamas NEE ištyrimas;
- ar sudarytos sąlygos tyrimų NEE srityje tobulinimui.

Audituojami subjektai – Krašto apsaugos ministerija, Teisingumo ministerija, Generalinė prokuratūra, Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos.

Audituojamas laikotarpis – 2015–2019 m.

Apribojimai – tikrindami, ar užtikrinamas nusikaltimų elektroninėje erdvėje ištyrimas, nevertinome ikiteisminio procesinių sprendimų teisėtumo ir pagrįstumo, nes pagal Prokuratūros įstatymą prokurorų proceso veiklą kontroliuoja aukštesnysis prokuroras ir teismas[238].

Auditas atliktas pagal Valstybinio audito reikalavimus[239] ir tarptautinius aukščiausiųjų audito institucijų standartus[240].

Audito duomenų rinkimo ir vertinimo metodai

Audito ataskaitos skyrius	**Taikyti duomenų rinkimo ir vertinimo metodai**	**Tikslas**
1. NEE grėsmių lygį reikia mažinti ir labiau didinti visuomenės saugumą elektroninėje erdvėje	<u>Dokumentų peržiūra</u> Nagrinėjome: ● Lietuvos Respublikos teisės aktus; ● nacionalinį kibernetinių incidentų valdymo planą; ● informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetinių incidentų tyrimo tvarkos aprašą; ● kriterijų, kuriais vadovaujantis kibernetiniai incidentai	Įvertinti, ar: ● sukurta veiksminga NEE prevencinių priemonių planavimo ir įgyvendinimo sistema; ● vykdomas kryptingas NEE prevencinių priemonių planavimas; ● rezultatyviai įgyvendinama NEE prevencinė veikla; ● atliekamas NEE prevencinių priemonių poveikio vertinimas; ● kibernetinių incidentų valdymo procesas užtikrina, kad visi kibernetiniai

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

[239] Valstybės kontrolieriaus 2002-02-21 įsakymas Nr. V-26 „Dėl Valstybinio audito reikalavimų patvirtinimo“.

[240] 3000-asis TAAIS „Veiklos audito standartas“, prieiga per internetą: http://www.vkontrole.lt/page.aspx?id=350.

Audito ataskaitos skyrius	Taikyti duomenų rinkimo ir vertinimo metodai	Tikslas
	priskiriami kibernetinių incidentų kategorijoms, sąrašą; • 2019 m. institucijų (PD, LKPB, AVPK, NKSC, VDAI, RRT, ŽEIT, IVPK, LRVK, KM, VVTAT, NPLC) nuostatus, metinius planus, metines darbo ataskaitas; • EUROPOL 2015–2019 m. ataskaitos; • 2019 m. Lietuvos policijos bendruomenės pareigūnų privalomų įgyvendinti bendrosios prevencijos veiklų kalendorių; • 215–2019 m. kibernetinio saugomo tarybos protokolus; • viešojo saugumo plėtros 2015–2025 metų programos įgyvendinimo tarpinstitucinius veiklos planus; • ENISA tyrimus, rekomendacijas ir gerąją praktiką NEE srityje; • 2015–2019 m. LKPB kibernetinių incidentų tyrimų bylas; • ES Tarybos ataskaitas; • BK, BPK, NVŽR, LITEKO nuostatus.	incidentai, galimai turintys NEE požymių, būtų identifikuojami; • nustatyta kibernetinių incidentų, galimai turinčių NEE požymių, identifikavimo tvarka; • atliekami kibernetinių incidentų vertinimai, siekiant identifikuoti NEE požymius; • policijai perduodama informacija apie kibernetinius incidentus, galimai turinčius nusikalstamos veikos požymių; • policija atlieka kibernetinių incidentų, galimai turinčių NEE požymių, vertinimą savo iniciatyva; • sudarytos sąlygos rinkti bendrą informaciją apie NEE.
	Duomenų analizė Analizavome: • institucijų (PD, LKPB, AVPK, NKSC, VDAI, RRT, ŽEIT, IVPK, LRVK, KM, VVTAT, NPLC) pateiktą informaciją apie įgyvendintas prevencines priemones 2015–2019 m.; • policijos įstaigų ir kitų institucijų įgyvendinančių projektinę veiklą NEE srityje pateiktą informaciją, susijusią su prevencinių priemonių poveikio matavimu; • LKPB pateiktą informaciją apie tarptautines prevencines priemones, prie kurių buvo prisijungta; • prevencinius projektus; • 2015–2019 m. IOCTA ataskaitas; • 2018 m. ir 2019 m. Eurobarometro apklausas; • 2019 m. Swedbank gyventojų elgsenos susidūrus su telefoniniais ar elektroniniais sukčiais tyrimą; • 2019 m. kriminogeninės situacijos apžvalgas; • mokslinius darbus NEE srityje; • blokavimo teises turinčių institucijų informaciją, pateikiamą internete; • 2019 m. VRM apklausas dėl „Gyventojų nuomonė apie teisėsaugos institucijas ir	

Audito ataskaitos skyrius	**Taikyti duomenų rinkimo ir vertinimo metodai**	**Tikslas**
	viešojo saugumo situacijos vertinimas“; • KSS papildomai po apklausos pateiktus duomenis (vertinimo tvarkas, atliktų vertinimų paaiškinimus, informacijos pateikimo policijai įrodymus); • 2015–2018 m. NKSC pateiktą kibernetinių incidentų statistiką; • 2015–2019 m. nacionalinio kibernetinio saugumo būklės ataskaitas; • NVŽR statistinius duomenis apie nusikalstamas veikas elektroninėje erdvėje 2015–2019 m.; • 2019 m. nacionalinio sunkaus ir organizuoto nusikalstamumo grėsmių ataskaitą ribota apimtimi.	
	<u>Pokalbiai su:</u> • Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos atstovais; • Lietuvos kriminalinės policijos biuro atstovais; • Lietuvos Respublikos krašto apsaugos ministerijos atstovais; • Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos atstovais; • Valstybinės duomenų apsaugos inspekcijos atstovais; • Informacinės visuomenės plėtros komiteto atstovais; • Lietuvos Respublikos kultūros ministerijos atstovais; • Lietuvos Respublikos Vyriausybės kanceliarijos atstovais; • Lietuvos Respublikos Ryšių reguliavimo tarnybos atstovais; • Valstybinės vartotojų teisių apsaugos tarnybos atstovais; • Žurnalistų etikos inspektoriaus tarnybos atstovais; • Nusikalstamumo prevencijos Lietuvoje centro atstovais; • AB „Telia Lietuva“ atstovais; • saugumo ekspertais ir advokatais.	
	<u>Apklausos</u> • Nuo 2019-11-22 iki 2019-12-16 vykdyta KSS, kurie valdo ir tvarko valstybės informacinius išteklius, apklausa apie kibernetinių incidentų, galimai turinčių nusikalstamos veikos požymių, identifikavimą,	

Audito ataskaitos skyrius	**Taikyti duomenų rinkimo ir vertinimo metodai**	**Tikslas**
	reagavimą ir informacijos perdavimą policijai. Apklausti visi 165 www.registrai.lt duomenimis valstybės informacinių sistemų, registrų valdytojais ir/ar tvarkytojai. Į apklausą iš viso atsakė 143 (86,67 proc.) apklaustų KSS; • nuo 2020-01-06 iki 2020-01-17 vykdyta pareigūnų ir prokurorų apklausa. Viso apklausai atrinkti 115 prokurorai, kas sudaro 78 proc. (115 iš 148) nuo 2019 m. dirbusių ir NEE tyrimus atlikusių prokurorų, kuriems buvo pateiktas klausimynas. 38 prokurorai (33 proc.) į klausimyną atsakė, iš kurių buvo 23 specializuoti prokurorai. Taip pat viso apklausai atrinki 95 pareigūnai, kas sudaro 47 proc. (95 iš 203) nuo 2019 m. dirbusių ir NEE tyrimus atlikusių pareigūnų, kuriems buvo pateiktas klausimynas. 37 pareigūnai (39 proc.) į klausimyną atsakė, iš kurių buvo 10 specializuotų pareigūnų.	
2. NEE tyrimas turi būti rezultatyvesnis ir labiau orientuotas į sisteminių NEE atskleidimą	<u>Dokumentų peržiūra</u> Nagrinėjome: • Lietuvos Respublikos teisės aktus; • nacionalinę kibernetinio saugumo strategiją ir jos tarpžinybinį veiklos planą; • 2015–2019 m. policijos pareigūnų mokymų sąrašus; • tyrėjų bei teisėjų specializacijos tvarkas; • rekomendacijas dėl prokurorų specializacijos; • 2015–2019 m. GP pateiktus įsakymus dėl specializacijos; • 2017-10-02 Europos Sąjungos Tarybos ataskaitą; • viešojo saugumo plėtros 2015–2025 metų programą ir jos tarpinstitucinį veiklos planą; • 2015–2019 m. prokurorų specializacijos įgyvendinimo ataskaitas; • 2018–2019 m. LKPB VKKV specializuotų padalinių veiklos patikrinimo ataskaitas; • Europos kibernetinio saugumo strategiją; • 2015–2019 m. IOCTA ataskaitos; • Pasaulio Ekonomikos Forumo 2020 m. Visuotinės rizikos ataskaitą. <u>Duomenų analizė</u> Analizavome:	Įvertinti, ar: • sudarytos sąlygos rezultatyviai atlikti NEE ikiteisminius tyrimus; • ikiteisminius tyrimus atliekantiems subjektams pakanka metodinių dokumentų, reglamentuojančių NEE tyrimą; • užtikrinama NEE srities specializacija; • NEE srityje rezultatyviai valdomi žmogiškieji ištekliai; • pakanka žmogiškųjų išteklių NEE tyrimams atlikti; • teisėsaugos pareigūnai bei prokurorai turi reikiamą kompetenciją tyrimus atlikti NEE srityje; • NEE ikiteisminių tyrimų metu vykdomas bendradarbiavimas su suinteresuotomis šalimis.

Audito ataskaitos skyrius	**Taikyti duomenų rinkimo ir vertinimo metodai**	**Tikslas**
	• LKPB pateiktą informaciją apie 2015–2019 m. specializuotus pareigūnus, ikiteisminius tyrimus; • 2015–2019 m. pareigūnų ir prokurorų sąrašus; • specializuotų prokurorų tinklo dokumentaciją; • Vilniaus, Kauno, Klaipėdos AVPK NNTV specializacijos padalinių informaciją apie teiktus pasiūlymus dėl kompetencijų aprašo tobulinimo, krūvių ir darbuotojų poreikio ir priėmimo; • NTA pateiktą informaciją dėl teisėjų specializacijos; • iš Kalėjimų departamento gautą informaciją apie blokavimo įrangą ir lėšas šiai įrangai; • 2017–2019 m. prokurorų atliktų NEE IT tikrinimų pažymas; • 8 (iš 120 (7 proc.)) atrinktus procesinius sprendimus atsisakyti pradėti ikiteisminį tyrimą, sustabdyti ikiteisminį tyrimą, nutraukti ikiteisminį tyrimą už 2019 m.; • viešai prieinamą informaciją apie kitų šalių NEE tyrimo praktiką; • 2018 m., 2019 m. Eurobarometro apklausas.	
	<u>Pokalbiai su:</u> • Lietuvos Respublikos Generalinės prokuratūros atstovais; • Lietuvos kriminalinės policijos biuro atstovais; • Lietuvos policijos kriminalistinių tyrimų centro atstovais; • Vilniaus, Kauno, Klaipėdos AVPK veiklos padalinių atstovais.	
	<u>Apklausos</u> • Pareigūnų ir prokurorų vykdyta apklausa (žr. aukščiau nurodytą informaciją apie tai).	
3. Strateginio planavimo ir vidaus kontrolės priemonės turi užtikrinti NEE prevencijos ir ištyrimo gerinimą	<u>Dokumentų peržiūra</u> Nagrinėjome: • Lietuvos Respublikos teisės aktus; • Nacionalinę kibernetinio saugumo strategiją; • Viešojo saugumo programą, tarpinstitucinius veiklos planus; • kitų šalių gerąją praktiką dėl teisinio reguliavimo NEE srityje;	Įvertinti, ar: • strateginis planavimas užtikrina nustatytų NEE srities problemų sprendimą; • užtikrinama NEE srities stebėsena; • užtikrinamas teisinio reguliavimo atnaujinimas, atsižvelgiant į besikeičiančius NEE;

Audito ataskaitos skyrius	**Taikyti duomenų rinkimo ir vertinimo metodai**	**Tikslas**
	• 2015–2019 m. BK priežiūros komiteto protokolus; • BK priežiūros komiteto darbo reglamentą; • Integruotos baudžiamojo proceso informacinės sistemos nuostatus ir kitą dokumentaciją; • PD kontrolės tvarkos aprašą; • LKPB kontrolės tvarkos aprašą; • 2015–2019 m. GP specializuotų prokurorų ataskaitas; • 2015–2019 m. GP Baudžiamojo persekiojimo departamento metinius veiklos planus. <u>Duomenų analizė</u> Analizavome: • policijos įstaigų ir GP strateginius dokumentus, juose numatytus NEE rodiklius ir jų faktinės reikšmes už 2015–2019 m.; • LKPB pateiktą informaciją apie lėšas už 2015–2019 m.; • ENISA tyrimų ataskaitos, kurios susijusios su NEE sritimi; • TM pateiktą informaciją apie teisinio reguliavimo NEE stebėseną; • TM gautus siūlymus dėl teisinio reguliavimo tobulinimo; • Informacinės prokuratūros sistemos, Lietuvos teismų informacinės sistemos, Nusikalstamų veikų žinybinio registro, Lietuvos kriminalinės policijos biuro, Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos pateiktą nusikalstamumo statistinę informaciją už 2015–2019 m.; • 2015–2019 m. LKPB stebėsenos ataskaitas, kontrolės ataskaitas / tarnybinius pranešimus. <u>Pokalbiai su:</u> • Lietuvos Respublikos Generalinės prokuratūros atstovais; • Lietuvos kriminalinės policijos biuro atstovais; • Mokslo bendruomenės atstovais; • Vilniaus, Kauno, Klaipėdos KP NEE specializuotų padalinių, kurie tiria NEE, atstovais.	• turimi įrankiai užtikrina informacijos, reikalingos NEE srities stebėsenai, surinkimą; • efektyviai atliekama NEE tiriančių institucijų ir padalinių veiklos kontrolė.

Valstybinio audito ataskaitos
„Ar veiksmingai kovojama su elektroniniais nusikaltimais“
3 priedas

Pokyčių rodiklių duomenys

1 lentelė. Visuomenės saugumo elektroninėje erdvėje pokyčio rodikliai

Rodiklis		Gyventojų, žinančių apie oficialius kanalus[241], kuriais galima pranešti apie elektroninius nusikaltimus ar kitą neteisėtą veiką internete, dalis	Gyventojų, kurie mano, kad nėra gerai informuoti arba yra visiškai neinformuoti apie elektroninių nusikaltimų grėsmes, dalis	Gyventojų, kurie mano, kad yra pajėgūs veiksmingai apsisaugoti nuo elektroninių nusikaltimų, dalis
Matavimo vienetas		Proc.	Proc.	Proc.
Pradinė reikšmė		17 proc.	42 proc.	40 proc.
Pradinės reikšmės fiksavimo data		2019 m.	2019 m.	2019 m.
Siektina reikšmė		30 proc.	35 proc.	55 proc.
Tolerancijos ribos	Gerai	27–30	35–36	51–55
	Vidutiniškai	22–26	37–39	46–50
	Blogai	17–21	40–42	40–45
Siektinos reikšmės fiksavimo data		2023 m.	2023 m.	2023 m.
Duomenų šaltinis rodikliui skaičiuoti		Eurobarometro tyrimai	Eurobarometro tyrimai	Eurobarometro tyrimai
Duomenų pateikimo periodiškumas		2021 m., 2022, 2023 m.	2021 m., 2022, 2023 m.	2021 m., 2022, 2023 m.
Detalus skaičiavimo aprašymas		Eurobarometro vykdoma visuomenės apklausa	Eurobarometro vykdoma visuomenės apklausa	Eurobarometro vykdoma visuomenės apklausa

2 lentelė. Elektroninių nusikaltimų ištyrimo pokyčio rodikliai

Rodiklis		Rezultatyviais kriminalinės žvalgybos tyrimais užbaigtų bylų dalis tiriant kibernetinius incidentus	Specializuotų padalinių veiklos rezultatyvumas	Prokurorų panaikintų sprendimų sustabdyti, nutraukti ar atsisakyti pradėti NEE ikiteisminį tyrimą dalis nuo visų tikrintų
Matavimo vienetas		Proc.	Proc.	Proc.
Pradinė reikšmė		0 proc.	29 proc.	11 proc.
Pradinės reikšmės fiksavimo data		2019 m.	2020 m.	2020 m.
Siektina reikšmė		60 proc.	40 proc.	5 proc.
Tolerancijos ribos	Gerai	Daugiau kaip 60 proc.	38–40	5–6
	Vidutiniškai	50–59 proc.	35–37	7–8

[241] Interneto svetainė, el. pašto adresas, internetinė forma ar telefono numeris.

Rodiklis	Rezultatyviais kriminalinės žvalgybos tyrimais užbaigtų bylų dalis tiriant kibernetinius incidentus	Specializuotų padalinių veiklos rezultatyvumas	Prokurorų panaikintų sprendimų sustabdyti, nutraukti ar atsisakyti pradėti NEE ikiteisminį tyrimą dalis nuo visų tikrintų
Blogai	Mažiau kaip 49 proc.	29–34	9–11
Siektinos reikšmės fiksavimo data	2023 m.	2023 m.	2023 m.
Duomenų šaltinis rodikliui skaičiuoti	LKPB pateikta informacija apie nuotolinės stebėsenos rezultatus dėl elektroninių nusikaltimų užregistravimo	LKPB pateikta informacija apie nuotolinės stebėsenos rezultatus dėl elektroninių nusikaltimų	GP pateiktos ikiteisminio tyrimo nutarimų patikrinimų pažymos dėl NEE
Duomenų pateikimo periodiškumas	2023 m.	2023 m.	2023 m.
Detalus skaičiavimo aprašymas	LKPB apskaičiuoja KŽ rezultatyvumą, proc.: dalis KŽ tyrimų, kuriu pagrindu pradėtas ikiteisminis tyrimas, nuo visų atliktų KŽ tyrimų.	LKPB apskaičiuoja kiekvieno AVPK KP NNTV ir NTS padalinių veiklos rezultatyvumo proc. (bylos perduotos į teismą nuo visų baigtų). Iš šių duomenų paskaičiuojamas visų minėtų padalinių rezultatyvumo vidurkis.	Apskaičiuojama, kiek per 2021–2022 metus buvo tikrintų NEE ikiteisminių tyrimų nutarimų ir iš šio skaičiaus padalinama, kiek sprendimų buvo panaikinta.

Valstybinio audito ataskaitos
„Ar veiksmingai kovojama su elektroniniais nusikaltimais“
4 priedas

Lietuvoje prevencinę veiklą NEE srityje vykdančios institucijos

Institucija	Įgyvendinta prevencinė veikla
Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos	Policijos įstaigose išskiriamos trys prevencinės veiklos kryptys: nusikalstamų veikų ir kitų teisės pažeidimų bendroji, individualioji ir situacijų prevencija. NEE prevencija policijos įstaigose išskirta nėra, ji yra bendrosios prevencijos dalis. Prevencinę veiklą policijos įstaigose įgyvendina AVPK ir bendruomenės pareigūnai, o jų veiklą organizuoja, koordinuoja ir kontroliuoja Viešoji policijos valdyba. AVPK ir bendruomenės pareigūnai per 2015–2019 m. įgyvendino per 1,5 tūkst. įvairių prevencinių priemonių (įvairūs renginiai, straipsniai žiniasklaidoje, internete, vaizdo medžiagos ir skrajučių platinimas, kt.). Šios priemonės buvo orientuotos į IOCTA ataskaitose numatytas pagrindines grėsmes: kibernetinis nusikalstamumas, vaikų išnaudojimas internete, el. sukčiavimas ir kt. Didžiausias dėmesys įgyvendinant prevencines priemones 2015–2019 m. policijos įstaigose buvo skiriamas bendroms saugumo temoms, pvz., kaip būti saugiam internete (43%), taip pat daug dėmesio buvo skiriama sukčiavimui (24%) ir patyčioms (17%) elektroninėje erdvėje. Įgyvendinant prevencinę veiklą, prevencinės priemonės buvo išskirtinai orientuotos į dvi jautrias visuomenės grupes – vaikus ir senjorus. Su vaikais dalintasi informacija apie saugumą ir patyčias bei vaikų išnaudojimą (prekyba žmonėmis, vaikų pornografija) elektroninėje erdvėje. Su senjorais dalintasi informacija sukčiavimo elektroninėje erdvėje ir bendromis saugumo temomis.
Lietuvos kriminalinės policijos biuras	Institucija vykdo visuomenės informavimo priemonėse skleidžiamos viešosios informacijos stebėseną ir kitas funkcijas, daugiau susijusias su individualiąja ir situacijų prevencija. Institucija nuolat vykdo interneto stebėjimą techninėmis priemonėmis. Interneto stebėjimo sistemoje sukurti įvairūs nuolatiniai ir teminiai stebėjimo profiliai. 2019 m. buvo atlikta 13 stebėsenų pagal šias temas: nusikaltimai elektroninėje erdvėje, vaikų seksualinis išnaudojimas internete, kova su terorizmu, kova su korupcinio pobūdžio nusikaltimais policijoje, neteisėto praturtėjimo ir turto susigrąžinimo srityse, publikacijų apie Lietuvos kriminalinės policijos biurą, Policijos departamentą stebėsena, stebėsenos rinkimų, nacionalinių egzaminų laikymo, rezonansinių bylų teisminio nagrinėjimo, Laisvojo Rusijos forumo, „Baltic Pride“ eitynių metu, dėl įkalinimo įstaigose galimų pažeidimų, informacijos apie organizuojamus renginius stebėsena. Institucija nuolat dalyvauja Europolo organizuojamuose renginiuose: EUCTF, EMPACT, Europolo FP Twins, Europolo FP Cyborg. Europole vyksta aukų identifikacijos darbiniai susitikimai, siekiant nustatyti nusikaltimų, susijusių su seksualinių vaikų išnaudojimu internete. Institucija tai pat prisideda prie Europolo prevencinių iniciatyvų rengiant ir platinant video medžiagą ir lankstinukus, didinančius visuomenės informuotumą apie kibernetines grėsmes išmaniesiems įrenginiams bei skatinančius informacines technologijas išmanantį jaunimą rinktis programuotojų bei kibernetinio saugumo specialistų, o ne programišių ir nusikaltėlių kelią (nuo 2016 m. prisidėjo prie 6 Europolo organizuotų iniciatyvų).
Nusikalstamumo prevencijos Lietuvoje centras	Institucija turi inicijuoti, organizuoti ir koordinuoti nusikalstamumo prevencijos programas bei priemones, derinant jas su šalyje vykdomais teisinės sistemos, socialine, ekonomine ir kitomis reformomis. Taip pat sukurti ir įgyvendinti veiksmingą nusikalstamumo prevencijos Lietuvoje sistemą, galinčią prognozuoti ir stabdyti nusikalstamumą mažinant jo lygį, gerinant šalies gyventojų, jų teisių bei interesų apsaugą ir kt. Nuo 2009 m. centras nebegauna finansavimo iš valstybės biudžeto, o nuo 2012 m. nevykdo jokios aktyvios veiklos, tačiau sprendimas dėl jos likvidavimo nėra priimtas.
Nacionalinis kibernetinio saugumo centras prie Lietuvos Respublikos krašto apsaugos ministerijos	Institucija analizuoja nacionalinę kibernetinio saugumo situaciją ir rengia nacionalinio kibernetinio saugumo būklės ataskaitas, teikia konsultacijas ir rekomendacijas valstybės informacinių išteklių valdytojams ir ypatingos svarbos infrastruktūros valdytojams kibernetinio saugumo klausimais, vykdo informacijos sklaidą kibernetinio saugumo klausimais, kartu su mokslo ir studijų institucijomis ir kibernetinio saugumo dalyviais plėtoja įvairius kibernetinio saugumo projektus – kasmet organizuoja kibernetinio saugumo pratybas „Kibernetinis skydas“. Institucijos veikla yra orientuota į darbą su kibernetinio saugumo subjektais, o ne visuomene, todėl institucijos vykdyta prevencinė veikla audito metu detaliai nenagrinėta.
Ryšių reguliavimo tarnyba	Institucija užtikrina neskelbtinos informacijos ir ribojamos viešosios informacijos platinimo priežiūrą viešo naudojimo kompiuterių tinkluose. Institucija taip pat aprobuoja žalingo interneto turinio, darančio neigiamą poveikį nepilnamečiams, filtravimo priemones. Bendradarbiaudama su privačiomis įmonėmis, policija ir VRM, sukūrė internetinę svetainę https://www.esaugumas.lt/lt, skirtą didinti supratimą apie saugų elgesį elektroninėje erdvėje. Joje pateikiama informacija apie kenkėjiškas

Institucija	Įgyvendinta prevencinė veikla
	programas, nepageidaujamus elektroninius laiškus (šlamštą), sukčiavimą ir kitus vartotojų saugumo grėsmių internete būdus. Institucija taip pat vykdo interneto karštosios linijos veiklą. Ši veikla Lietuvoje vykdoma nuo 2007 m. pagal Europos Komisijos finansuojamą „Saugesnio interneto“ projektą. Karštoji linija sudaro sąlygas visuomenei pranešti apie žalingą, nepageidaujamą turinį internete. Tai galima padaryti adresu http://www.drauginskasinternetas.lt arba https://svarusinternetas.lt/.
Valstybinė duomenų apsaugos inspekcija	Institucija informuoja visuomenę asmens duomenų ir privatumo apsaugos klausimais, tame tarpe ir dėl asmens duomenų apsaugos elektroninėje erdvėje. 2015–2019 m. dalyvavo 8 renginiuose, kuriuose dalinosi informacija apie asmens duomenų apsaugą socialiniuose tinkluose, tapatybės vagystes ir kitomis susijusiomis temomis. Institucija taip pat dalinosi susijusia informacija savo interneto puslapyje bei kitose visuomenės informavimo priemonėse – spaudos konferencijos, interviu.
Valstybinė vartotojų teisių apsaugos tarnyba	Institucija vykdo vartotojų švietimą vartotojų teisių apsaugos srityje, taip pat įgyvendina prevencines priemones, padedančias užtikrinti vartotojų teisių apsaugą elektroninėje erdvėje. Institucija kasmet dalyvauja Tarptautinio vartotojų apsaugos ir gynimo tinklo (angl. *ICPEN*) organizuojamų švietimo bei informavimo kampanijų cikle – 2019 m. nuspręsta susitelkti į apgavysčių prevenciją renkantis prekes ir paslaugas internetu bei šviesti vartotojus tokiomis temomis kaip apgaulingos ir agresyvios mažmeninės prekybos taktikos, klaidinanti reklama, elektroninė prekyba, su sveikata susijęs sukčiavimas. Institucija audituojamu laikotarpiu dalinosi informacija savo interneto svetainėje, Facebook paskyroje ir kitose žiniasklaidos priemonėse – televizijoje, radijuje spaudoje. Taip pat organizavo per 300 renginių ir seminarų, kuriuose buvo pristatomi ir su nuotoline (elektronine) prekyba susiję klausimai, kylantys pavojai.
Žurnalistų etikos inspektoriaus tarnyba	Institucija vykdo aktyvią veiklą kovojant su nesantaikos kurstymu socialinių medijų erdvėje, taip užtikrinama pažeidžiamiausių socialinių grupių teisių apsauga visuomenės informavimo priemonėse, nes nesantaikos turinys yra operatyviai pašalinamas iš viešosios erdvės, prieiga prie jo panaikinama. Institucija kartu su VRM ir GP 2018 m. pradėjo vykdyti Europos Sąjungos pagal 2014–2020 m. Teisių, lygybės ir pilietybės programą finansuojamą projektą „Atsako į neapykantos nusikaltimus ir neapykantą kurstančias kalbas Lietuvoje stiprinimas“. Šio projekto tikslas – mažinti toleranciją internete ir kasdieniame gyvenime reiškiamai neapykantai, išmokti ją atpažinti ir efektyviai su ja kovoti.
Informacinės visuomenės plėtros komitetas	Vienas pagrindinių institucijos tikslų – įgyvendinti valstybės informacinės visuomenės plėtros politiką ir aptarnauti šios politikos formavimą ir įgyvendinimą. Institucija kartu su partneriais šiuo metu įgyvendina projektą „Prisijungusi Lietuva“, kurio tikslas – padėti gyventojams išmokti efektyviai, saugiai, atsakingai naudotis informacinėmis technologijomis bei internetu ir jo teikiamomis galimybėmis. Projektas yra nukreiptas į skaitmeninių įgūdžių formavimą ir ugdymą, tik dalis projekto veikų yra nukreipta į saugų elgesį internete. Vykdant projektą, institucija kartu su projekto partneriais organizavo vaizdo siužetų ir kt. priemonių, skirtų skatinti išmaniai ir saugiai naudotis internetu, sukūrimą. Taip pat 2018 m. lapkričio 5–9 d. akcijos „Akcija „Senjorų dienos internete“ metu ir 2019 m. vasario 4–9 d. „Saugesnio interneto savaitė“ metu, organizavo renginius vyresnio amžiaus asmenims ir mokyklų bendruomenėms apie saugų elgesį internete, kuriuose dalyvavo apie 24 tūkst. asmenų. Taip pat teikė informaciją projekto puslapyje https://www.prisijungusi.lt/ įvairiomis temomis, susijusiomis su saugiu elgesiu internete.
Lietuvos Respublikos kultūros ministerija	Nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais pagal Budapešto konvenciją yra laikomi NEE. Už šią sritį Lietuvoje yra atsakinga Kultūros ministerija, kuri aktyviai prisideda prie autorių teisių ir gretutinių teisių pažeidimų prevencijai skirtų projektų organizavimo ir įgyvendinimo. Kultūros ministerija 2014–2017 m. administravo Kūrybinės veiklos, autorių teisių ir gretutinių teisių apsaugos programą, pagal kurią galėjo būti finansuojami autorių teisių ir gretutinių teisių pažeidimų prevencijai skirti projektai. Projektai apėmė autorių teisių pažeidimus ir elektroninėje erdvėje, tačiau specifiškai šios srities neišskyrė. Pagal Kultūros ministerijos pateiktą informaciją nustatyta, kad iš viso 2014–2017 m. buvo finansuota 20 projektų. Nuo 2018 m. programų įgyvendinimas buvo perkeltas į Kultūros ministerijai pavaldžią įstaigą – Lietuvos kultūros tarybą.
Lietuvos Respublikos Vyriausybės kanceliarija	Institucija 2018–2019 m. organizavo kampaniją „Sustiprink imunit@ą!“, kurios tikslas – kibernetinio ir informacinio saugumo didinimas. Kampanijai skirtame interneto puslapyje https://sustiprinkimuniteta.lt/ pateikiama informacija apie tai, kaip apsaugoti vaikus internete, išvengti e-sukčių bei saugiai naudotis internetu. 2019 m. kampanijos metu buvo parengti 128 tekstai, internetinės žiniasklaidos priemonėms bei vietinei ir regioninei spaudai, pagaminti 52 vaizdo reportažai internetinės žiniasklaidos priemonėms bei regioniniams televizijos kanalams, pagaminti 18 reklaminių skydelių internetinės žiniasklaidos priemonėms.

Šaltinis – Valstybės kontrolė pagal institucijų pateiktus duomenis ir kitą viešai prieinamą informaciją

Valstybinio audito ataskaitos
„Ar veiksmingai kovojama su
elektroniniais nusikaltimais“
5 priedas

Kibernetiniai įvykiai 2015–2019 m.

Kibernetinių įvykių tipas	2015 m.	2016 m.	2017 m.	2018 m.	2019 m.
Kenkimo PĮ	10 928	11 212	10 839	10 822	68 562
Įsilaužimas (RIS užvaldymas)	6 975	10 673	10 951	10 059	–
RIS trikdymas (DoS)	50	61	50	31	355
Elektroninių duomenų klastojimas	559	555	1 237	872	–
Vientisumo pažeidimai	10	21	15	24	–
Įrenginių saugumo spragos	18 427	20 490	24 612	29 747	–
Įvairaus pobūdžio	4 613	6 450	6 710	1 628	–
Ryšių ir informacinių sistemų kibernetinės grėsmės	–	–	–	–	199 828
Informacijos rinkimas	–	–	–	–	37 363
Badymai įsibrauti	–	–	–	–	2 987
Iš viso:	**41 562**	**49 462**	**54 414**	**53 183**	**309 095**

Šaltinis – Valstybės kontrolė pagal Nacionalinio kibernetinio saugumo būklės ataskaitas

Valstybinio audito ataskaitos
„Ar veiksmingai kovojama su
elektroniniais nusikaltimais “
6 priedas

Nusikaltimų elektroninėje erdvėje specializuotų padalinių veikimo ribos (kompetencija)

Baudžiamojo kodekso straipsnis	Baudžiamojo kodekso straipsnio pavadinimas
154 str.	Šmeižimas
162 str.	Vaiko išnaudojimas pornografijai
166 str.	Asmens susižinojimo neliečiamumo pažeidimas
167 str.	Neteisėtas informacijos apie privatų asmens gyvenimą rinkimas
168 str.	Neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas
169 str.	Diskriminavimas dėl tautybės, rasės, lyties, kilmės, religijos ar kitos grupinės priklausomybės
170 str.	Kurstymas prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę
170[1] str.	Grupių ir organizacijų, turinčių tikslą diskriminuoti žmonių grupę arba kurstyti prieš ją, kūrimas ir veikla
170[2] str.	Viešas pritarimas tarptautiniams nusikaltimams, SSRS ar nacistinės Vokietijos nusikaltimams Lietuvos Respublikai ar jos gyventojams, jų neigimas ar šiurkštus menkinimas
171 str.	Trukdymas atlikti religines apeigas ar religines iškilmes
191 str.	Autorystės pasisavinimas
192 str.	Literatūros, mokslo, meno kūrinio ar gretutinių teisių objekto neteisėtas atgaminimas, neteisėtų kopijų platinimas, gabenimas ar laikymas
193 str.	Informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimas arba pakeitimas
194 str.	Neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas
195 str.	Pramoninės nuosavybės teisių pažeidimas
196 str.	Neteisėtas poveikis elektroniniams duomenims
197 str.	Neteisėtas poveikis informacinei sistemai
198 str.	Neteisėtas elektroninių duomenų perėmimas ir panaudojimas
198[1] str.	Neteisėtas prisijungimas prie informacinės sistemos
198[2] str.	Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis
213 str.	Netikrų pinigų ar vertybinių popierių gaminimas, laikymas arba realizavimas
214 str.	Netikros elektroninės mokėjimo priemonės gaminimas, tikros elektroninės mokėjimo priemonės klastojimas ar neteisėtas disponavimas elektronine mokėjimo priemone arba jos duomenimis
215 str.	Neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas
309 str.	Disponavimas pornografinio turinio dalykais

Šaltinis – Policijos įstaigų padalinių kompetencijų atlikti ikiteisminių tyrimus aprašas

NAUDINGI • VERTINAMI • ATPAŽĮSTAMI