



KRAŠTO APSAUGOS
MINISTERIJA

NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA

2024




Viršelis sukurtas
naudojant dirbtinį
intelektą

**NACIONALINĖ
KIBERNETINIO
SAUGUMO BŪKLĖS
ATASKAITA
2024**



KRAŠTO APSAUGOS
MINISTERIJA

Turinys

 Dominančią temą galite pasiekti paspaudę ant jos pavadinimo



IŽANGA \04



SANTRAUKA \06



KIBERNETINIO SAUGUMO POLITIKOS FORMAVIMAS \14

KAM veikla stiprinant Lietuvos pasirengimą reaguoti į įvairias grėsmes ir didinant kibernetinės erdvės saugumą \15

Dalyvavimas formuojant ir įgyvendinant ES kibernetinio saugumo politiką \19

ES gynybos iniciatyvų naudojimas bendradarbiavimui ir projektų finansavimui \20

KAM veikla plėtojant tarptautinį bendradarbiavimą kibernetinio saugumo srityje \21

Kibernetinė gynyba - viena esminių NATO atgrasymo ir gynybos užduočių \24



LIETUVOS KIBERNETINIO SAUGUMO BŪKLĖS APŽVALGA \26

Kibernetinių incidentų dinamika Lietuvoje ir NKSC vykdomos prevencinės priemonės \27

Svarbiausi 2024 m. įvykiai ir tendencijos \28

Aktualios kibernetinio saugumo grėsmės ir rizikos bei kibernetinio saugumo incidentai \29

NKSC atliekama organizacijų atitikties priežiūra \36

Kibernetinių incidentų prevencija ir kitos kibernetinį saugumą stiprinančios priemonės \37

Elektroninių ryšių tinklų vientisumo ir vartotojų apsaugos užtikrinimas, draudžiamos viešai skleisti informacijos internete užkardymas \43

Svarbiausi 2024 m. įvykiai ir tendencijos \44

Viešųjų ryšių tinklų vientisumo užtikrinimas Lietuvoje \45

Radio ryšio užtikrinimas ir atsparumas \46

Vartotojų apsauga nuo žalingų interneto nuorodų, apsimestinių trumpųjų žinučių ir skambučių \47

Elektroninės atpažinties priemonių saugumo užtikrinimo lygio vertinimas \48

Skaitmeninių paslaugų priežiūra \48

Interneto karštosios linijos „Švarus internetas“ veikla ir žalingo turinio internete užkardymas \49

Viešųjų kompiuterių tinklų (internetu) prieigos vietose privalomų filtravimo priemonių naudojimo užtikrinimas \51

Visuomenės švietimo veikla \51

Nusikalstamų veikų kibernetinėje erdvėje mastas ir poveikis \52

Svarbiausi 2024 m. įvykiai ir tendencijos \53

Tarptautinė situacija \54

Nacionalinė situacija \55

Tarptautinis bendradarbiavimas \69

Prevencinė veikla siekiant užkirsti kelią sukčiavimui kibernetinėje erdvėje \69

Policijos kompetencijos kėlimas kibernetinių nusikaltimų užkardymo srityje \70

Asmens duomenų apsauga, saugumo užtikrinimas ir pažeidimų prevencija \72

Svarbiausi 2024 m. įvykiai ir tendencijos \73

ADSP Lietuvoje situacijos analizė \74

ADASL Lietuvoje \78

Mokymo ir švietimo veikla \78

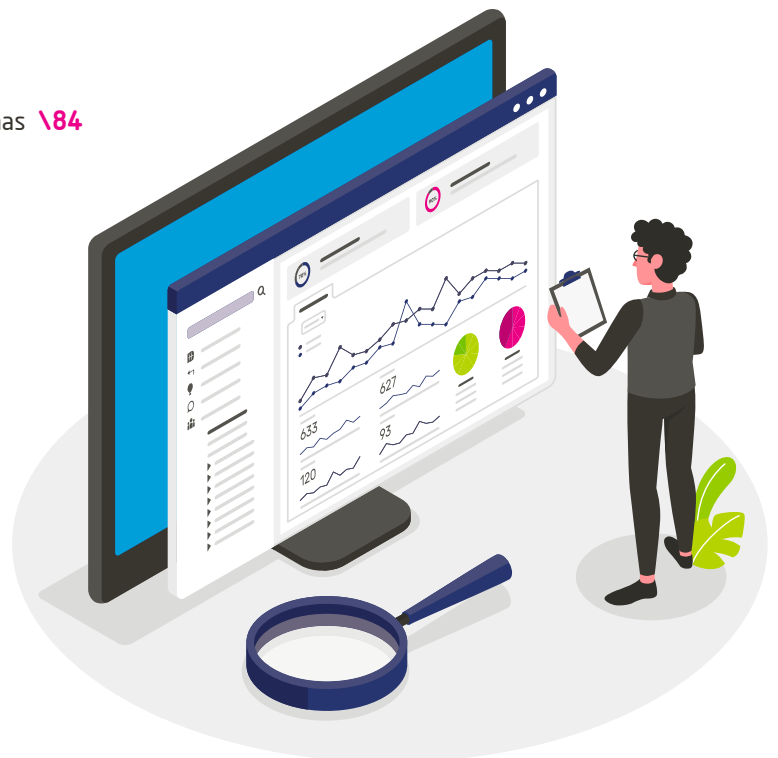
Priešiškos informacinės aplinkos vertinimas \80

Svarbiausi 2024 m. įvykiai ir tendencijos \81

Informacinės aplinkos grėsmių tendencijos \82

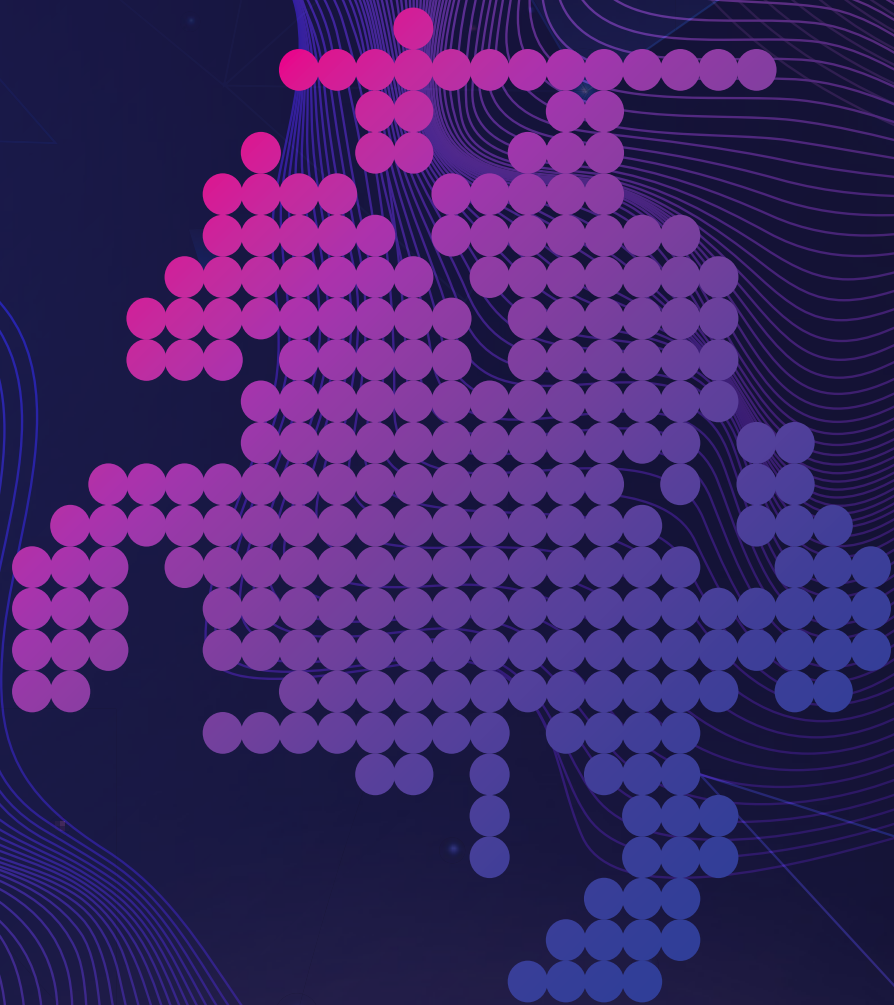
Bendradarbiavimas su partneriais ir visuomenės informavimas \84

Rezonansiniai atvejai \85



01

žanga





Dovilė Šakalienė,
krašto apsaugos ministrė

Pastarųjų metų įvykiai mums priminė – stabilumas ir taika nėra savaime suprantami. Geopolitinė įtampa, priešiškų valstybių remiamos kibernetinės ir hibridinės atakos, šnipinėjimas, povandeninės infrastruktūros pažeidimai Baltijos jūroje, manipuliavimas informacija – visa tai yra mūsų realybė. Priešiškos valstybės, nusikaltėliai, kiti piktavaliai vis dažniau naudoja ne tik įprastus ginklus, bet ir naujausias technologijas, pavyzdžiui, dirbtinį intelektą, socialinę inžineriją, dezinformaciją ir propagandą. Šie įrankiai skirti kritinei infrastruktūrai pažeisti, svarbioms paslaugoms sutrikdyti, pasitikėjimui institucijomis mažinti, visuomenei skaldyti ir nesaugumo jausmui kurti.

Gebėjimas apsisaugoti ne tik nuo fizinių, bet ir nuo nematomų kibernetinių grėsmių šiandien yra neatsiejama nacionalinio saugumo dalis. Priešiškos valstybėms vis aktyviau vykdant kibernetines atakas, mūsų valstybės kibernetinis atsparumas tampa ne pasirinkimu, o būtinybe.

2024 m. Lietuva susidūrė su išaugusiu kibernetinių incidentų skaičiumi, tačiau, Nacionalinio kibernetinio saugumo centro vertinimu, šis pokytis sietinas ne su padidėjusia grėsme, bet su augančiu visuomenės sąmoningumu. Patyrėme užsienio šalių remiamų grupuočių atakų, vis tik daugiau nei pusė Lietuvoje registruotų kibernetinių incidentų įvyko dėl piktavalių gebėjimo manipuluoti žmonių patiklumu. Tą pabrėžia ir Lietuvos policija – kibernetiniam nusikalstamumui didžiausią įtaką daro sukčiavimo elektroninėje erdvėje atvejai. Valstybinė duomenų apsaugos inspekcija atkreipia dėmesį, kad 2024 m. dėl kibernetinių incidentų reikšmingai išaugo Lietuvoje paveiktų subjektų skaičius. Šie faktai rodo, kad kibernetinės atakos prieš Lietuvą, kaip ir kitas demokratines valstybes, ne tik tobulėja, bet ir tampa dažnesnės. Didelių iššūkių nacionaliniam saugumui taip pat kelia tiekimo grandinėje dalyvaujančių subjektų nepakankamas dėmesys kibernetiniam saugumui. Apilaidus paslaugų teikėjų požiūris palieka atvirus kelius mūsų priešininkams įsiskverbti į mums kritiškai svarbių organizacijų sistemas ir jas galimai pažeisti.

Reaguodama į šias grėsmes, Krašto apsaugos ministerija formuoja kryptingą kibernetinio saugumo politiką, kuria siekia užtikrinti, kad Lietuva būtų atspari ir pasirengusi bet kokiai grėsmei kibernetinėje erdvėje. 2024 m. mūsų šalyje pradėjo galioti atnaujintas Kibernetinio saugumo įstatymas, kuriuo į nacionalinę teisę perkėlėme ES Tinklų ir informacinių sistemų direktyvą (NIS 2). Lietuva yra viena iš keturių Europos Sąjungos šalių, kurios šią direktyvą perkėlė laiku. Taigi organizacijos žino, ką daryti, o valstybė turi priemones tai koordinuoti ir vertinti.

Europos Sąjunga toliau vysto kitas iniciatyvas, stiprinančias valstybių kritinių sektorių kibernetinį atsparumą, o mes, kaip Krašto apsaugos ministerija, kartu su kitomis Lietuvos institucijomis siekiame, kad nacionalinis interesas būtų tinkamai atspindėtas ir laiku priimami nacionaliniai sprendimai. Vieni svarbiausių artimiausio laikotarpio sprendimų – perėjimas prie postkvantinės kriptografijos ir Lietuvos institucijų įsipareigojimų užtikrinti skaitmeninių produktų kibernetinio saugumo reikalavimus nustatymas.

Lietuva 2024 m. taip pat ėmėsi didinti savo indėlį į NATO kolektyvinį saugumą ir reagavimo į kibernetines atakas pajėgumus – įsteigta Lietuvos kariuomenės Kibernetinės gynybos valdyba.

Kibernetinis saugumas yra bendras darbas. Nuoširdžiai dėkoju Lietuvos institucijoms, prisidėjusioms prie šios ataskaitos rengimo, ir už jų profesionalumą, patikimumą ir atsakomybę kuriant tokią Lietuvą, kuri sugeba apsaugoti savo žmones, organizacijas ir savo vertybes, – tiek fizinėje, tiek kibernetinėje erdvėje. Tai apima ne tik techninių sprendimų tobulinimą, bet ir institucijų pasirengimo gerinimą, visuomenės budrumo skatinimą ir gebėjimą veikti išvien. Šia kryptimi ir kviečiame dirbti toliau.

02

Santrauka



Kibernetinio saugumo grėsmės, priešišky valstybių interesai ir visuomenės atsparumo įtaka Lietuvos kibernetinio saugumo būklei

1. Kibernetinio saugumo stiprinimas: nauji teisės aktai, gynybos pajėgumai ir tarptautinis bendradarbiavimas.



Krašto apsaugos ministerija (toliau - KAM) 2024 m. atliko svarbų vaidmenį formuodama Lietuvos kibernetinio saugumo politiką ir prisidėdama prie Europos Sąjungos (toliau - ES) kibernetinio saugumo ateities. Daugiausia dėmesio 2024 m. buvo skiriama:

- 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyvos (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148, (toliau - TIS 2 direktyva) perkėlimui į nacionalinę teisę;
- Lietuvos kariuomenės Kibernetinės gynybos valdybos (toliau - LK KGV) steigimo darbams;
- Nacionalinės kibernetinio saugumo plėtros programos, patvirtintos Lietuvos Respublikos Vyriausybės 2023 m. rugsėjo 20 d. nutarimu Nr. 746 „Dėl 2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos patvirtinimo“, (toliau - Kibernetinio saugumo plėtros programa) įgyvendinimui;
- nacionalinėms pozicijoms dėl ES teisėkūros iniciatyvų kibernetinio saugumo srityje rengti ir joms atstovauti ES Taryboje;
- JAV ir Lietuvos bendradarbiavimo kibernetinio saugumo ir gynybos srityje gairėms.

KAM koordinavo TIS 2 direktyvos perkėlimo į nacionalinę teisę veiksmus - buvo atnaujintas Kibernetinio saugumo įstatymas, patvirtinti įgyvendinamieji teisės aktai, o pokyčiai pristatyti viešojo ir privataus sektoriaus atstovams įvairiuose renginiuose ir leidiniuose. Lietuva buvo viena iš pirmųjų šalių, perkėlusių TIS 2 direktyvos nuostatas.

2024 m. buvo užbaigti visi LK KGV steigimo darbai, būtini Lietuvos kariuomenės gebėjimams kibernetinėje erdvėje stiprinti, ryšių ir informacinėms sistemoms (toliau - RIS) saugoti ir jų sąveikai su NATO užtikrinti. Naujos struktūros kariuomenė veiklą pradėjo 2025 m. sausio 1 d.

2024 m. pabaigoje KAM kartu su kitomis valstybės institucijomis pradėjo įgyvendinti priemones, skirtas Lietuvos kibernetiniam atsparumui didinti: stiprinti kibernetinio saugumo valdyseną, kurti stebėsenos ir reagavimo į kibernetinius incidentus pajėgumus, rengti specialistus, vystyti tyrimų infrastruktūrą ir stiprinti visuomenės atsparumą kibernetinėms grėsmėms.

KAM rengė Lietuvos pozicijas ir atstovavo šalies interesams derybose dėl naujų ES kibernetinio atsparumo, saugumo ir solidarumo aktų, pradėjo dalyvauti Europos Komisijos (toliau - EK) sudarytoje Postkvantinės kriptografijos ekspertų darbo grupėje, prisidėjo prie ES kibernetinės gynybos iniciatyvų vystymo.

2024 m. lapkritį patvirtintas JAV ir Lietuvos 2025–2029 m. bendradarbiavimo kibernetinio saugumo ir gynybos srityje planas. Šis planas ne tik sustiprino jau egzistuojantį transatlantinį bendradarbiavimą, bet ir atliepė globalias grėsmes, reikalaujančias tarpusavio veiksmų koordinavimo. Plano tikslas – stiprinti karinius kibernetinės gynybos pajėgumus, didinti visuomenės ir kritinės infrastruktūros atsparumą bei užtikrinti glaudesnę bendradarbiavimą su JAV ir kitais sąjungininkais bendrose pratybose ir mokymuose.

2. 2024 m. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC) užregistravo 63 proc. daugiau kibernetinių incidentų nei 2023 m., tačiau šis pokytis sietinas ne su padidėjusia grėsme, bet su augančiu visuomenės sąmoningumu ir būtinybės pranešti apie kibernetinius incidentus supratimu.



2024 m. NKSC iš viso užregistravo 3 874 kibernetinius incidentus, t. y. apie 63 proc. daugiau nei ankstesniais metais (2023 m. – 2 378). Dauguma jų buvo priskirti nereikšmingai ir vidutinei kategorijoms, o 3 kibernetiniai incidentai – didelei kategorijai (2023 m. tokių incidentų nebuvo). Pastarosios kategorijos incidentai siejami su užsienio šalių remiamomis grupuotėmis, kurios įsilaužusios į organizacijų tinklus siekia ilgalaikių tikslų – šnipinėjimas vienas jų. NKSC vertinimu, nors 2024 m. fiksuota incidentų skaičiaus dinamika daugiausia susijusi su gerėjančiais visuomenės pranešimo apie kibernetinius incidentus įpročiais, vis dėlto piktavalių socialinės inžinerijos metodų taikymas siekiant išvilioti jautrią informaciją yra pagrindinė kibernetinių incidentų Lietuvoje priežastis. Pažymėtina, kad 2024 m. šio tipo incidentai sudarė net 59 proc. visų NKSC registruotų incidentų (2023 m. – 38 proc.).

Daugiausia incidentų įvyko interneto prieglobos paslaugų infrastruktūroje (angl. *hosting*), užsienio subjektų sektoriuje ir interneto paslaugų teikėjų (toliau – IPT) infrastruktūroje. Tiek 2023 m., tiek ir 2024 m. interneto prieglobos paslaugų infrastruktūra ir toliau pirmauja pagal joje fiksuotų incidentų skaičių. Šiame sektoriuje matoma itin sparti incidentų skaičiaus didėjimo tendencija – incidentų padidėjo net 74 proc. Didžiausią žalą organizacijoms ir gyventojams darė incidentai, priskiriami socialinei inžinerijai, antroje vietoje fiksuota sparčiai didėjusi neteisėta įtaka RIS veiklai ir (ar) teikiamoms paslaugoms (2023 m. – 116; 2024 m. – 444), o trečioje vietoje – nepageidaujimų laiškų ir (ar) klaidinančios informacijos platinimas (2023 m. – 200; 2024 m. – 318). Daug metų buvę vienais dažniausių kibernetinių incidentų, susijusių su kenkimo programinės įrangos platinimu, 2024 m. šie incidentai atsidūrė penktoje vietoje (2023 m. – 554; 2024 m. – 223).

Nerimą kelia pastaraisiais metais pasaulio šalyse, įskaitant ir Lietuvą, 2024 m. smarkiai išaugęs nutekintų prisijungimo duomenų kiekis. Tam didelę įtaką daro kibernetinės atakos, tinklų ir informacinės sistemos spragos (toliau – spragos) ir slaptažodžių pakartotinis naudojimas skirtingose platformose.

Didėjančios spragos kėlė pavojų tiek valstybės institucijoms ir įstaigoms, tiek privataus sektoriaus organizacijoms, tačiau subjektų pranešimai apie aptiktas spragas pagal atsakingo atskleidimo tvarką (toliau – atsakingas atskleidimas) padeda užkardyti kibernetines grėsmes.

2024 m., palyginti su 2023 m., nustatytų potencialiai pažeidžiamų informacinių sistemų skaičius išaugo daugiau kaip 3 kartus (2023 m. – 1 963; 2024 m. – 6 700). Didžiausią riziką kėlė spragos Lietuvos viešojo ir privataus sektoriaus organizacijų plačiai naudojamuose *Fortinet*, *Palo Alto Networks*, *Cisco*, *VMware* produktuose ir tinklų infrastruktūroje.

NKSC taip pat daug dėmesio skyrė spragoms, susijusioms su *WordPress* turinio valdymo sistemos įskiepiams (angl. *plugin*), kurie dažnai tampa įsilaužėlių taikiniu dėl nepakankamos apsaugos ir laiku neatliekamų atnaujinimų.

NKSC pažymi, kad įsilaužėliai vis dažniau taikosi į informacinių technologijų (toliau – IT) tiekimo grandinės spragas – per paslaugų teikėją jie gali pasiekti daugiau aukų. 2024 m. NKSC dalį tokių grėsmių užkardė, apie nustatytas spragas informuodamas paslaugų teikėjus ir jų klientus. Tačiau tiekimo grandinės atakų pavojų dar labiau didina tai, kad jos gali likti nepastebėtos ilgą laiką ir dažnai tik duomenų vagystė, organizacijos veiklos sutrikdymas, atsiradę finansiniai nuostoliai leidžia organizacijai suprasti įvykusio incidento pobūdį.

2024 m. NKSC gavo 68 pranešimus apie aptiktas spragas pagal atsakingą atskleidimą (2023 m. – 74) tiek privataus, tiek viešojo sektoriaus organizacijose. Tai leido laiku informuoti paveiktas organizacijas ir suteikti joms galimybę ištaisyti spragas dar prieš jomis pasinaudojant kibernetiniams piktavaliams.

NKSC, bendradarbiaudamas su kitomis privataus ir viešojo sektoriaus organizacijomis, stiprino nacionalinę kibernetinių grėsmių analizę ir prevenciją.

Kovai su žaibiškais kibernetinėmis sukčiavimo atakomis NKSC 2024 m. toliau tobulino organizacijų ir gyventojų apsaugai skirtą domenų blokavimo įrankį „Vasaris“. 2024 m. pabaigoje šis įrankis buvo taikomas beveik 2,4 mln. mobiliojo ir 725 tūkst. fiksuoto interneto ryšio paslaugų vartotojų. Jis kasdien apsaugojo vidutiniškai apie 35 500 gyventojų. Šiuo įrankiu naudojasi ir 9 Lietuvos valstybės institucijos ir įstaigos.

NKSC 2024 m. aktyviai teikė paramą Vyriausiajai rinkimų komisijai (toliau – VRK) pasirengimo rinkimams ir jų metu. 2024 m. birželio mėn., rinkimų į Europos Parlamentą metu, NKSC specialistams talkino ir kartu Lietuvos kibernetinės erdvės saugumu rūpinosi Europos kibernetinio greitojo reagavimo komandos (angl. *Cyber Rapid Response Team* (CRRT)) nariai.

NKSC 2024 m. pradėjo vykdyti aktyvią nutekintų duomenų paiešką, siekdamas laiku identifikuoti grėsmes ir informuoti paveiktas organizacijas: 2 tūkst. kartų informavo įvairias organizacijas apie jų nutekintus duomenis, pateikė įmonėms ir institucijoms informaciją apie šimtus tūkstančių nutekintų įrašų ir pan. Tai leidžia NKSC greičiau reaguoti į kibernetinius incidentus, mažinti žalą ir stiprinti bendrą šalies kibernetinį atsparumą.

2024 m. NKSC sukūrė nemokamą nuotolinių mokymų platformą, skirtą tiek gyventojams, tiek organizacijoms. Per metus įvairius kursus sėkmingai baigė daugiau nei 46 tūkst. asmenų. Internetu patogiai pasiekiamų mokymų turinys pritaikytas skirtingoms visuomenės grupėms – darbuotojams, mokytojams, mokiniams ir kt. Iš pristatytų kursų paminėtini „Kibernetinė higiena namuose“, „Kibernetinis saugumas mokiniams“, „Kibernetinis saugumas mokytojams“ ir kiti.

NKSC 2024 m. toliau organizavo nacionalines kibernetinio saugumo pratybas, tobulino jų scenarijus ir vykdymo metodus, kurie leido viešojo sektoriaus ir ypatingos svarbos infrastruktūros valdytojams patikrinti savo darbuotojų atsparumą socialinės inžinerijos atakoms ir pačios organizacijos gebėjimus identifikuoti, valdyti ir komunikuoti apie kibernetinius incidentus. Per pratybas „Kibernetinis skydas PhishEx 2024“ išsiųsta 280 tūkst. imitacinių el. laiškų, juose atkartotos dažniausiai pasitaikančios programišių taktikos, o didžiausios nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas OpEx 2024“ pirmą kartą buvo vykdomos gyvai virtualiame kibernetinių pratybų poligone. Šiose pratybose dalyvavo 75 organizacijos, iš kurių 39 tobulino viešosios komunikacijos įgūdžius, mokydamosi efektyviai informuoti visuomenę apie incidentus.

3. Ryšių reguliavimo tarnybos (toliau – RRT) įtvirtintos sukčiavimo trumposiomis žinutėmis (SMS) ir skambučiais užkardymo priemonės, vykdyta žalingo turinio šalinimo iš interneto veikla darė svarbią ir teigiamą įtaką kibernetinės erdvės saugumui, vaikų ir nepilnamečių apsaugai internete.



RRT vertinimu, 2024 m. viešojo judriojo ir viešojo fiksuotojo ryšio tinklų sutrikimai ir gedimai buvo šalinami operatyviai, tačiau liepos mėnesį siautusi audra sukėlė didelių sunkumų viešojo mobiliojo ryšio tinklams, teikėjai susidūrė su žmogiškųjų išteklių stygiumi ir atsarginių maitinimo šaltinių trūkumu šalindami tinklo gedimus. Sutrikimų mastas paskatino sparčiau atnaujinti RRT tarybos nutarimu patvirtintas Viešųjų ryšių tinklų vientisumo užtikrinimo taisykles, kad kilus ekstremalioms situacijoms tinklai būtų atsparesni, o galimų sutrikimų mastas – mažesnis.

2024 m. lapkričio mėn. Baltijos jūroje buvo nutrauktas jūrinis ryšio kabelis, jungiantis Lietuvą ir Švediją. RRT kartu su kitomis institucijomis tyrė šį incidentą, taip pat fiksavo ir tyrė orlaivių globalinės padėties nustatymo sistemos (angl. *Global Positioning System (GPS)*) (toliau – GPS) sutrikimų, neteisėtų transliacijų iš Rusijos atvejus. RRT nustatė, kad GPS sutrikimus sukėlė Rusijos ir Baltarusijos teritorijose veikiantys ryšio slopintuvai, o dėl GPS klastojimo atvejų kreipėsi į Tarptautinę telekomunikacijų sąjungą (angl. *International Telecommunication Union (ITU)*) (toliau – ITU). Tokie saugumo incidentai yra kompleksiniai, todėl reikalingas atsakingų Lietuvos institucijų bendradarbiavimas, vieningas ES požiūris ir koordinuotas bendras atsakas.

Buvo dedamos didelės pastangos, kad vartotojai, ypač vaikai ir nepilnamečiai, būtų apsaugoti nuo žalingo turinio internete. 2024 m. RRT, kuri yra tarptautinės interneto karštųjų linijų asociacijos INHOPE narė, interneto karštąja linija (www.svarusinternetas.lt) gavo 2 177 pranešimus apie internete rastą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją; palyginti su 2023 m. (2 516), gautų pranešimų skaičius sumažėjo. Pasitvirtinusių pranešimų apie draudžiamą ir neigiamą poveikį nepilnamečiams darančią informaciją, dėl kurios pašalinimo galima imtis veiksmų, buvo 1 488, t. y., šiek tiek daugiau nei 2023 m. (1 475). Nerimą kelianti tendencija – didėjantis patyčių ir smurto kibernetinėje erdvėje atvejų skaičius.

RRT rūpinasi, kad visose prieigos prie viešųjų kompiuterių tinklų (internetu) vietose, kuriose gali lankytis ir naršyti internete nepilnamečiai, būtų įdiegtos privalomos, RRT aprobuotos, neigiamą poveikį nepilnamečių vystymuisi darančios informacijos filtravimo priemonės. 2024 m. RRT ir toliau vykdė patikrinimus Lietuvos mokyklose ir viešosiose bibliotekose, teikė ekspertines konsultacijas filtravimo priemonių pasirinkimo ir naudojimo klausimais.

Neabejotiną poveikį Lietuvos gyventojų saugumui kibernetinėje erdvėje nuo 2023 m. daro RRT priimti įpareigojimai operatoriams aptikti ir blokuoti apgaulingus skambučius. Kovai su apsimestinėmis trumpomis žinutėmis 2024 m. RRT tarybos patvirtintas Apsimestinių trumpųjų žinučių identifikavimo tvarkos aprašas, kuris įpareigojo mobiliojo ryšio paslaugų teikėjus identifikuoti apsimestines SMS ir jas užkardyti.

RRT aktyviai dalyvauja ES vystomo palydovinio ryšio projekto „Atsparumo, sujungiamumo ir saugumo palydoviniu ryšiu infrastruktūra“ (angl. *Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²)*) (toliau – IRIS²) techninėje ir vartotojų darbo grupių veikloje ir kitose tarptautinėse darbo grupėse, sprendžiančiose ryšio ir trukdžių problemas.

4. Policijos duomenimis, 2024 m. nusikalstamų veikų elektroninėje erdvėje grėsmės lygis nepakito, ypač sumažėjo nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui, tačiau esminė problema vis dar lieka sukčiavimas.



2024 m. Lietuvoje užregistruotos 3 966 nusikalstamos veikos elektroninėje erdvėje. Nors šis skaičius vos didesnis nei 2023 m. (3 912), šių nusikalstamų veikų grėsmės lygis išliko nepakitęs ir neturėjo įtakos 2024 m. registruoto nusikalstamumo augimui. Kaip ir pernai, ypač sumažėjo nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui, kurie kvalifikuojami pagal Lietuvos Respublikos baudžiamojo kodekso (toliau – LR BK) 196–198² str. Pavyzdžiui, neteisėto poveikio elektroniniams duomenims, informacinei sistemai, neteisėto prisijungimo prie informacinės sistemos atvejų sumažėjo beveik 10 proc. Šie policijos 2024 m. stebėsenos rezultatai sutampa su nepriklausomų ekspertų išvadomis. Kompanijos „Surfshark“ skaitmeninio gyvenimo kokybės indeksas (angl. *Digital Quality of Life Index* (DQL)) rodo, kad Lietuva pagal kibernetinį saugumą 2024 m., kaip ir anksčiau, išliko antrąja šalimi pasaulyje.

2024 m. policijos įstaigos užregistravo 4 atvejus, kai elektroniniai duomenys buvo užšifruoti iš-pirkos reikalaujančio kenkimo programinio kodo virusais (tai beveik 5 kartus mažiau nei 2023 m.). Pirmą kartą toks virusas panaudotas prieš Lietuvos finansų sektorių.

Esminė problema vis dar lieka sukčiavimo elektroninėje erdvėje atvejai. Jie 2024 m. sudarė didžiąją dalį – 53 proc. – visų elektroninėje erdvėje padarytų nusikalstamų veikų: išankstinio mokėjimo sukčiavimo, investicinio sukčiavimo, sukčiavimo apgaulingais telefoniniais skambučiais, el. laiškais ir žinutėmis. Apgaulingų telefoninių skambučių atvejų skaičius 2024 m., palyginti su 2023 m., išaugo 64 proc. Skambučiais siekta išvilioti grynuosius pinigus ir (ar) vertybes, naudojant išviliotus elektroninės bankininkystės vartotojų duomenis grobti lėšas iš banko sąskaitų. Policija daro prielaidą, kad tai galėjo lemti efektyvi apgaulingų SMS žinučių kontrolė – nusikaltėliai prisitaikė prie taikomų techninių priemonių ir grįžo prie apgaulingų skambučių.

Pagrindinė elektroninės bankininkystės duomenų išviliojimo ir (ar) provokavimo patvirtinti apgaulingą finansinę operaciją priemonė liko suklastotos svetainės nuorodos pateikimas interneto vartotojams. Naujas išskirtinis reiškinys – interneto vartotojų prisijungimas prie suklastotos svetainės esveikata.lt.

Finansų rinkos dalyvių duomenimis, iš Lietuvos gyventojų ir juridinių asmenų 2024 m. apgaule buvo kėsintasi išvilioti 35 mln. Eur, tačiau finansų įstaigoms pavyko apsaugoti 17,6 mln. Eur, t. y. dvigubai daugiau lėšų negu pernai (7,9 mln. Eur). Vis dėlto 2024 m. gyventojų patirti nuostoliai siekė 17,3 mln. Eur, t. y. yra 28 proc. daugiau negu 2023 m.

Socialiniai tinklai vis dar dominuoja kaip apgaulingų skelbimų platinimo vieta, pavyzdžiui, „Facebook“ 2024 m. paskelbtų apgaulingų skelbimų, palyginti su 2023 m., padaugėjo 27 proc.

2024 m. kibernetinės atakos siekiant sutrikdyti valstybės informacines sistemas ir (ar) išgauti valstybės ir tarnybos paslaptis neturėjo sistemingo nusikalstamumo požymių ir nekėlė kritinės žalos nacionaliniam saugumui. Iš viešųjų subjektų patyrusių kibernetinių atakų poveikį, dažniausios buvo švietimo sektoriaus, sveikatos paslaugų ir kultūros sektoriaus informacinės sistemos.

2024 m. Organizuoto nusikalstamumo internete grėsmių vertinimo ataskaitoje (angl. *Internet Organised Crime Threat Assessment* (IOCTA)) (toliau – IOCTA ataskaita) daroma išvada, kad dirbtiniu intelektu (toliau – DI) pagrįstos technologijos daro socialinę inžineriją dar efektyvesnę.

Susirūpinimą taip pat kelia ir giliųjų klautočių (angl. *deepfakes*) naudojimas, nes tai toks pat galingas įrankis, kaip ir balso atkartojimas ar klatojimas. Lietuvos policijos atliekamuose tyrimuose nėra nustatyta, kad progresuotų DI naudojimas nusikalstamoms veikoms vykdyti, tačiau kartu su kitomis valstybėmis nagrinėjama potenciali DI įtaka socialinei inžinerijai ir prevencinės priemonės.

5. Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) duomenimis, 2024 m. Lietuvoje paveiktų duomenų subjektų skaičius padidėjo beveik 3 kartus, palyginti su 2023 m., ir tai lėmė didesnis asmens duomenų saugumo pažeidimų (toliau – ADSP), įvykusių dėl kibernetinių incidentų, skaičius.



Iš 2024 m. pranešimų apie ADSP Lietuvoje statistikos matyti, kad VDAI gavo 273 pranešimus apie ADSP, t. y. 7 proc. daugiau negu 2023 m. (2023 m. – 254). VDAI pastebi, kad pokytis nėra didelis, todėl negalima daryti prielaidos, kad ADSP skaičius Lietuvoje išaugo. Tačiau 2024 m. beveik 3 kartus padidėjo Lietuvoje paveiktų duomenų subjektų skaičius – 1 467 368 (2023 m. – 571 833). Tai lėmė didesnis ADSP, įvykusių dėl kibernetinių incidentų, skaičius, buvo paveikta daug duomenų subjektų.

Pagal ADSP pobūdį Lietuvoje statistiškai vyrauja konfidencialumo pažeidimai, jie sudarė net 87 proc. visų atvejų. Tai šiek tiek daugiau, palyginti su 2023 m., kai konfidencialumo pažeidimai sudarė 76 proc. visų pažeidimų.

VDAI, išanalizavusi 2024 m. gautus pranešimus apie ADSP, nustatė, kad 90 (33 proc.) ADSP įvyko dėl kibernetinių incidentų: duomenų užšifravimo ir išpirkos reikalavimo atakų, neteisėtai gautos prieigos prie IT sistemų, socialinės inžinerijos metodais paremtų atakų, prisijungimo duomenų užpildymo kibernetinių atakų ir kt. 2023 m. VDAI gavo tik 37 pranešimus apie ADSP dėl kibernetinių incidentų, t. y. 15 proc. visų 2023 m. gautų pranešimų apie ADSP. Dažniausios kibernetinių incidentų priežastys: perimti naršyklėse išsaugoti prisijungimo duomenys – 27 proc., nepakankamai išmokytas personalas – 18 proc., kelių faktorių autentifikavimo nebuvimas – 10 proc.

Vienas išskirtinių atvejų – poveikio priemonių taikymas viešojo sektoriaus organizacijai. Atlikusi ADSP ir kibernetinio incidento tyrimą, VDAI priėmė sprendimą skirti 9 tūkst. Eur baudą viešojo sektoriaus organizacijai už nustatytus Bendorjo duomenų apsaugos reglamento (ES) 2016/679 (toliau – BDAR) nuostatų pažeidimus. Dėl netinkamai vykdomos prieigų kontrolės ir autentifikavimo nebuvimo prisijungta prie įstaigos serverių ir užšifruoti duomenys.

Lietuvos gyventojų sąmoningumą asmens duomenų apsaugos srityje rodo asmens duomenų apsaugos sąlygų lygis (toliau – ADASL). ADASL nustatomas pagal kasmet atliekamos reprezentatyvios Lietuvos gyventojų apklausos duomenis. 2024 m. ADASL siekė 63 proc. ir nuo 2021 m. faktiškai padidėjo 3 proc.

VDAI 2024 m. savo veiklą organizavo taip, kad būtų nuosekliai stiprinamos duomenų valdytojų, duomenų apsaugos pareigūnų ir duomenų subjektų žinios, ugdoma kompetencija ir jgūdžiai asmens duomenų apsaugos srityje:

- ✔ suteiktos 4 334 kasdienės konsultacijos gyventojams ir organizacijoms;
- ✔ aktyviai dalyvauta nacionalinėse kibernetinio saugumo pratybose „Kibernetinis skydas OpEx 2024“;
- ✔ surengti nuotoliniai mokymai ir šviečiamieji renginiai (dalyvavo daugiau nei 7 000 dalyvių);
- ✔ paskelbti 25 metodiniai dokumentai (juos galima rasti VDAI svetainėje).

6. Lietuvos kariuomenės Strateginės komunikacijos departamento (toliau – LK SKD) duomenimis, 2024 m. informacinei veiklai prieš Lietuvą didžiausią įtaką turėjo besitęsianti Rusijos agresija prieš Ukrainą.



Didžiausias informacinių grėsmių prieš Lietuvą ir šalies strateginius interesus šaltinis – Rusijos ir Baltarusijos režimų pareigūnai, šių valstybių politinė ir karinė vadovybė ir režimo kontroliuojami žiniasklaidos atstovai. Tęsiantis Rusijos karinei invazijai Ukrainoje, ypač daug dėmesio skirta Lietuvos paramai Ukrainai.

2024 m. daugiausia vyravo įprasti naratyvai, pavyzdžiui, NATO yra agresyvus karinis blokas, o Lietuva – rusofobiška valstybė. Taip pat priešiški informaciniai veikėjai, susiję su Rusijos ar Baltarusijos režimais ir (arba) jų kontroliuojami, stengėsi sumenkinti Lietuvos pastangas stiprinti šalies gynybinius pajėgumus ir Vokietijos brigados dislokavimo reikšmę.

Atsižvelgiant į dabartinę geopolitinę situaciją, paminėtini nauji naratyvai, pavyzdžiui, Lietuvoje ir Lenkijoje rengiami diversantai perversmui Baltarusijoje sukelti ir Aliksandro Lukašenkos režimui nuversti, Lietuvos karinio pajėgumo stiprinimas yra pasirengimas Rusijos ir Baltarusijos puolimui, NATO šalys yra įsitraukusios į karinę operaciją Kurske.

2024 m. išryškėjo ir nauja tendencija – bauginimo ir grasinimo atvejai informacinėje erdvėje. Palyginti su 2023 m., padažnėjo pranešimų apie Trečiąjį pasaulinį arba branduolinį karą.

LK SKD vertinimu, tikėtina, kad 2025 m. informacinis spaudimas neatslūgs, o priešiškų valstybių kontroliuojami ar jų įtaką patiriantys informaciniai veikėjai toliau sieks diskredituoti Lietuvos kariuomenę ir NATO bei pateisinti savo veiksmus fizinėje erdvėje kaltindami „kolektyvinius Vakarus“.



03

Kibernetinio saugumo politikos formavimas



KAM 2024 m. atliko svarbų vaidmenį formuodama Lietuvos kibernetinio saugumo politiką ir prisidėdama prie ES kibernetinio saugumo ateities. Daugiausia dėmesio 2024 m. buvo skiriama TIS 2 direktyvai⁰¹ į nacionalinę teisę perkelti, LK KGV steigimo darbams, Kibernetinio saugumo plėtros programai įgyvendinti⁰², kartu su kitomis ES šalimis deryboms dėl svarbių ES teisės aktų kibernetinio saugumo srityje užbaigti, o svarbiausias bendradarbiavimo su strategine partnere JAV pasiekimas – patvirtintas JAV ir Lietuvos bendradarbiavimo kibernetinio saugumo ir gynybos srityje 2025–2029 m. planas.

1 KAM veikla stiprinant Lietuvos pasirengimą reaguoti į įvairias grėsmes ir didinant kibernetinės erdvės saugumą

Nacionalinių kibernetinio saugumo pajėgumų, valstybės informacinių išteklių ir kritinės infrastruktūros apsaugos stiprinimas

Kibernetinio saugumo plėtros programai įgyvendinti numatytos veiklos, kurios padėtų spręsti dėl pasikeitusių kibernetinių grėsmių pobūdžio ir augančio jų masto mažėjančio šalies kibernetinio atsparumo problemą. Krašto apsaugos ministro 2024 m. vasario 5 d. įsakymu Nr. V-98 buvo patvirtintas 2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos pažangos priemonės Nr. 06-007-10-05-07 „Stiprinti kibernetinį atsparumą“ aprašas, numatantis Kibernetinio saugumo plėtros programai įgyvendinti skirtas veiklas, jų vykdytojus ir siekiamus rezultatus. Pažangos priemonės Nr. 06-007-10-05-07 „Stiprinti kibernetinį atsparumą“ veiklų vykdytojai: KAM, NKSC, Kertinis valstybės telekomunikacijų centras (toliau – KVTC) ir Policijos departamentas prie Vidaus reikalų ministerijos (toliau – PD), 2024 m. rudenį pasirašė projektų vykdymo sutartis su VŠĮ Centrinė projektų valdymo agentūra ir pradėjo vykdyti Ekonomikos gaivinimo ir atsparumo didinimo priemonės lėšomis finansuojamus projektus:

✓ KAM vykdomas projektas – „Kibernetinio saugumo valdysenos Lietuvoje stiprinimas“.

✓ NKSC vykdomi projektai:

- „Nacionalinės kibernetinio saugumo stebėsenos sistemos sukūrimas“;
- „Nacionalinės SOC / CSIRT modulinės sistemos, suteikiančios galimybę SOC / CSIRT paslaugomis naudotis TIS2 direktyvoje nurodytų sektorių kibernetinio saugumo subjektams, sukūrimas“;
- „Nusikalstamų veikų elektroninėje erdvėje tyrimui ir mokymams skirtos laboratorijos sukūrimas ir instruktorių darbui šioje laboratorijoje parengimas“;
- „Kibernetinio saugumo subjektuose dirbančių darbuotojų, kibernetinio saugumo specialistų kompetencijų bei įgūdžių kibernetinio saugumo srityje stiprinimas bei pažeidžiamiausių visuomenės grupių kibernetinio saugumo brandos kėlimas“.



01

2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva). Prieiga per internetą <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>.

02

Lietuvos Respublikos Vyriausybės 2023 m. rugsėjo 20 d. nutarimas Nr. 746 „Dėl 2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos patvirtinimo“. Prieiga per internetą <https://e-seimas.lrs.lt/portal/legalAct/lt/TA/D/54521320591e11ee8e3cc6ee348ebf6d?fwid=-1a256e44a1>.

✓ KVTC vykdomas projektas – „Saugiajame tinkle esančių informacinių išteklių auditas ir kibernetinių saugos priemonių architektūros, užtikrinančios atsparumą ir tinkle esančių informacinių išteklių pasiekiamumą, sukūrimas“.

✓ PD vykdomas projektas – „Nusikalstamų veikų elektroninėje erdvėje prevencijai, užkardymui ir tyrimui reikalingos infrastruktūros sukūrimas ir šias veiklas vykdančių specialistų kompetencijų stiprinimas“.

NKSC taip pat vykdo ir projektus, finansuojamus 2021–2027 m. Skaitmeninės Europos programos bendrojo finansavimo ir 2021–2027 m. Skaitmeninės Europos programos lėšomis, skirtus finansinei paramai smulkaus ir vidutinio verslo subjektams suteikti, jų kibernetiniam atsparumui stiprinti ir aktyviai Lietuvos kibernetinio saugumo bendruomenei sukurti.

KAM 2024 m. koordinavo ir vykdė TIS 2 direktyvos perkėlimo į nacionalinę teisę darbus. KAM, rengdama tam skirtus teisės aktų projektus, organizavo susitikimus su viešojo ir privataus sektorių atstovais. Susitikimuose buvo diskutuojama apie tinkamiausią Lietuvai kibernetinio saugumo politikos formavimo ir įgyvendinimo modelį ir atnaujinamus kibernetinio saugumo reikalavimus. TIS 2 direktyvos nuostatos Lietuvoje buvo perkeltos patvirtinus šiuos teisės aktus:

✓ 2024 m. liepos 11 d. Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymą ir kitų susijusių įstatymų pakeitimo įstatymus;

✓ Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 6 d. nutarimą Nr. 945 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo“⁰³.

Viešojo ir privataus sektoriaus laukiantys pokyčiai, susiję su TIS 2 direktyvos nuostatų perkėlimu į nacionalinę teisę, buvo pristatyti 2024 m. įvairiuose viešuose renginiuose: Trijų jūrų iniciatyvos surengtame forume „Kritinės infrastruktūros kibernetinio saugumas ir atsparumas“, NKSC organizuojamuose „Kibernetinio saugumo pusryčiuose“ ir kituose kibernetinio saugumo temai skirtose konferencijose ir renginiuose. Papildoma informacija apie atnaujinto Kibernetinio saugumo įstatymo ir su juo susijusių kitų teisės aktų reikalavimus pateikiama KAM interneto svetainėje⁰⁴, viešinama KAM socialinės žiniasklaidos paskyrose ir įvairiose internetinės žiniasklaidos priemonėse. Taip pat parengti informaciniai leidiniai⁰⁵ apie atnaujinto Kibernetinio saugumo įstatymo svarbiausias nuostatas. Vienas iš leidinių skirtas organizacijų vadovams, kitas, išsamesnis, – organizacijų specialistams.

Europos kibernetinio saugumo organizacija (angl. *European Cyber Security Organisation* (ECSO)) Lietuvą nurodė kaip vieną iš keturių ES šalių, laiku perkėlusią TIS 2 direktyvą⁰⁶. 2025 m. KAM daug dėmesio skirs atnaujintam Kibernetinio saugumo įstatymui įgyvendinti – imsis priemonių Lietuvos organizacijų kibernetinį atsparumui didinti ir sektorių kibernetinio saugumo lygiui suvienodinti.

Atsižvelgiant į ES institucijų 2024 m. priimtus kitus teisės aktus kibernetinio saugumo srityje, 2025 m. į nacionalinę teisę bus integruojamas Kibernetinio atsparumo akto⁰⁷, Kibernetinio saugumo akto pakeitimo⁰⁸ nuostatos ir dalyvaujama kitų valstybės institucijų koordinuojamose nacionalinės teisėkūros iniciatyvose, iš kurių svarbesnės yra susijusios su Dirbtinio intelekto aktu⁰⁹ ir vadinamuoju pirmuoju ES tinklų kodeksu, skirtu kibernetiniam saugumui elektros energijos sektoriuje¹⁰.

Atsižvelgiant į NATO sprendimą kibernetinę erdvę pripažinti penktuoju kariavimo domenu ir 2022 m. Lietuvos Respublikos Seimo politinių partijų pasirašytą susitarimą „Dėl Lietuvos nacionalinio saugumo ir gynybos artimiausio laikotarpio stiprinimo“, nuosekliai stiprinami Lietuvos kibernetinės gynybos pajėgumai. 2024 m. liepos 19 d. Seimas pritarė KAM pasiūlytam kariuomenės struktūros pakeitimui¹¹ ir tai sudarė teisinį pagrindą įsteigti LK KGV. LK KGV tikslas – stiprinti Lietuvos kariuomenės kibernetinį

03

Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 6 d. nutarimu Nr. 945 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo“ patvirtintas Nacionalinis kibernetinių incidentų valdymo planas ir Kibernetinio saugumo reikalavimų aprašas, Kibernetinio saugumo subjektų identifikavimo pagal specialiuosius kriterijus metodika, Vykdyto užtikrinimo priemonių taikymo kibernetinio saugumo subjektams tvarkos aprašas ir kiti su kibernetinio saugumo politika susiję dokumentai.

04

KAM interneto svetainės skiltis „Kibernetinio saugumo įstatymas“. Prieiga per internetą <https://kam.lt/kibernetinio-saugumo-istatymas/>.

05

Informacinius leidinius galima rasti KAM interneto svetainės skiltyje „Kibernetinio saugumo įstatymas“. Prieiga per internetą <https://kam.lt/kibernetinio-saugumo-istatymas/>.

06

„ECSO Baltoji knyga – TIS 2 įgyvendinimas: iššūkiai ir prioritetai“ (angl. *ECSO White Paper — NIS2 Implementation: Challenges & Priorities*). Prieiga per internetą <https://ecso-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf>.

07

2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontalių kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas). Prieiga per internetą <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847>.

08

2024 m. gruodžio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2025/37, kuriuo iš dalies keičiamas Reglamentas (ES) 2019/881, kiek tai susiję su valdomomis saugumo paslaugomis. Prieiga per internetą <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0037>.

09

2024 m. birželio 13 d. priimtas Europos Parlamento ir Tarybos Reglamentas (ES) 2024/1689, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas). Prieiga per internetą https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=OJ:L_202401689.

saugumą, konsoliduojant Lietuvos kariuomenei skiriamoms užduotims įgyvendinti reikalingus pajėgumus, įgyvendinant valstybės ginkluotos gynybos planus. LK KGV buvo kuriama restruktūrizuojant atitinkamas krašto apsaugos sistemos institucijas, siekiant užtikrinti, kad LK KGV rūpinsis Lietuvos kariuomenės stacionaria ryšių ir informacine infrastruktūra, kariuomenei teiks būtinas informacinių technologijų paslaugas, užtikrins sąveiką su NATO, krašto apsaugos sistemos ir kitų institucijų bei organizacijų RIS. Naujas Lietuvos kariuomenės junginys pagal poreikį planuos ir vykdys kibernetinės erdvės operacijas, taip pat diegs strateginio ir operacinio lygmenų ryšių ir informacines sistemas. 2023–2024 m. krašto apsaugos sistemoje užbaigti visi suplanuoti LK KGV steigimo darbai. LK KGV veiklą pradėjo 2025 m. sausio 1 d.



Nuo 2022 m. balandžio mėn. įsigaliojus teisės aktams, užtikrinantiems, kad kritinėje infrastruktūroje, įskaitant 5G infrastruktūrą, būtų naudojama tik patikimų gamintojų įranga, 2024 m. KAM ir toliau glaudžiai bendradarbiavo su valstybės institucijomis ir organizacijomis, veikiančiomis nacionalinio saugumo požiūriu svarbiuose sektoriuose, ir ragino jas nuo 2025 m. sausio 1 d. nenaudoti nepatikimų gamintojų informacinių ir ryšių technologijų įrangos.

2024 m. KVTC toliau stiprino Saugiojo valstybinio duomenų perdavimo tinklo (toliau - Saugusis tinklas), vieno iš esminių Lietuvos nacionalinio saugumo užtikrinimo kibernetinėje erdvėje elementų, infrastruktūros kibernetinį atsparumą. KVTC praplėtė Saugiajame tinkle taikomų kolektyvinių kibernetinio saugumo priemonių sąrašą, įtraukdamas papildomų kolektyvinės apsaugos kibernetinio saugumo priemonių ir Saugumo operacijų centro (angl. *Security Operations Center (SOC)*) paslaugų. Šiuo laikotarpiu buvo ne tik atnaujinta Saugiojo tinklo įranga, bet ir pakeista kita, Saugiajame tinkle funkcionavusi, nepatikimų gamintojų įranga, atsižvelgiant į Kibernetinio saugumo įstatymą ir kitus galiojančius teisės aktus, užtikrinančius, kad kritinėje infrastruktūroje būtų naudojama tik patikimų gamintojų įranga.

Lietuvos pasirengimas įveikti iššūkius, susijusius su virsmo technologijų plėtra

2023–2024 m. įvykęs DI taikymo proveržis, ypač didelių kalbos modelių (angl. *large language models*) taikymo srityje, tapo galingu įrankiu tiek inovacijoms, tiek kibernetinėms grėsmėms. Naudojant DI galima greitai analizuoti didelius duomenų kiekius, kurti įtikinamą garsinį, vaizdinį ar tekstinį turinį ir suasmenintas žinutes. Tad augantis DI modelių pažangumas, autonomiškumas ir jų prieinamumas ėmė kelti vis didesnes socialinės inžinerijos ir ja paremtos dezinformacijos sklaidos bei kibernetinio šnipinėjimo grėsmes. Taip pat didėja piktavalių, neturinčių daug įgūdžių ir resursų, galimybės vykdyti kenkėjišką veiklą.

Pagrindinės problemos:

-  socialinės inžinerijos ir ja paremtos dezinformacijos sklaidos grėsmės – naudojant DI lengviau ir greičiau kuriamos itin įtikinamos apgaulingos žinutės, klastojamas balsas ir vaizdas. Tai leidžia kurti tikroviškas sukčiavimo schemas ir manipuluoti aukomis realiu laiku;
-  kibernetinio šnipinėjimo grėsmės – DI padeda greičiau ir tiksliau identifikuoti vertingus taikinius (aukas) ir nustatyti jų pažeidžiamumus. Naudojant DI daug greičiau nustatomos ir išnaudojamos neatnaujintos informacinės sistemos ir nežinomi („nulinės dienos“) pažeidžiamumai, sparčiau vykdoma pavogtų duomenų eksfiltracija ir analizė ir pan.;




10

2024 m. kovo 11 d. Komisijos deleguotasis reglamentas (ES) 2024/1366, kuriuo Europos Parlamento ir Tarybos reglamentas (ES) 2019/943 papildomas nustatant tinklo kodeksą dėl tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektų sektorinių taisyklių. Prieiga per internetą <https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:32024R1366>.

11

Lietuvos Respublikos principinės kariuomenės struktūros, karių ir Lietuvos kariuomenės darbuotojų, dirbančių pagal darbo sutartis ir gaunančių darbo užmokestį iš valstybės biudžeto ir valstybės pinigų fondų (išskyrus darbuotojus, gaunančius darbo užmokestį iš ES struktūrinės, kitos ES finansinės paramos ir tarptautinės finansinės paramos lėšų (išskyrus techninės paramos lėšas), ribinio skaičiaus patvirtinimo įstatymus. Prieiga per internetą <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/18d39e83232711eab86ff95170e24944/asr>.

 duomenų, naudojamų mašininio mokymosi ir DI modeliams kurti, saugumo grėsmės – piktaivaliai gali sąmoningai „užteršti“ mokymosi duomenis, todėl minėti modeliai gali pateikti netikslius rezultatus. Patys modeliai taip pat gali būti pavogti ir panaudoti blogiems tikslams, atskleisti jautrūs mokymosi duomenys.

Sparti DI pažanga suteikia daug galimybių, tačiau kelia naujų grėsmių. Stebint technologinį DI proveržį, galima konstatuoti, kad DI ir toliau bus sparčiai tobulinamas, didės jo panaudojimo galimybės, todėl DI turi būti kuriamas, diegiamas ir naudojamas saugiai ir atsakingai.

Lietuva, kaip ES narė, kartu su kitomis ES šalimis įsipareigoja stiprinti DI naudojimo saugumą ir etiką. Dirbtinio intelekto aktas, įsigaliojęs 2024 m. rugpjūčio 1 d., yra pirmasis ES reglamentas, nustatantis DI sistemų kūrimo, naudojimo ir platinimo reikalavimus, siekiant užtikrinti saugumą, skaidrumą ir žmogaus teisių apsaugą. Dirbtinio intelekto aktas apima įvairias DI sistemų kategorijas ir suskirsto jas pagal rizikos lygį: nuo mažiausios rizikos (minimaliai reguliuojamos) iki didelės rizikos (griežtai prižiūrimos) ir nepriimtinos rizikos (visiškai draudžiamos). Atkreiptinas dėmesys, kad nors Dirbtinio intelekto aktas reguliuoja DI sistemų panaudojimą, šis reguliavimas netaikomas su nacionaliniu saugumu susijusiose srityse. Lietuvoje už Dirbtinio intelekto akto reikalavimų įgyvendinimą atsakinga Lietuvos Respublikos ekonomikos ir inovacijų ministerija ir jai pavaldžios įstaigos.

Lietuva kartu su daugiau nei 50 pasaulio valstybių yra prisijungusi prie 2023 m. JAV iniciuotos politinės deklaracijos dėl DI atsakingo panaudojimo karinėms reikmėms ir autonomijos¹². Siekiant minimizuoti galimą DI sistemų žalą (pavojų) tretiesiems asmenims konflikto zonose, siūloma remtis atskaitomybės ir žmogaus kontrolės užtikrinimo, atitikties tarptautinei humanitarinei teisei, personalo, dirbančio su DI sistemomis, tinkamo mokymo ir nuolatinio rizikų valdymo principais. Įgyvendinant deklaracijos nuostatas sudarytos 3 darbo grupės, vienoje jų – Priežiūros darbo grupėje – dalyvauja ir Lietuva. Šios darbo grupės tikslas – dalytis geriausia DI teisinės priežiūros praktika ir teikti rekomendacijas, kaip turėtų būti teisiškai reguliuojamas DI panaudojimas karinėms reikmėms.

Kitų virsmo technologijų, pavyzdžiui, kvantinės technologijos, spartus vystymasis ir unikalus gebėjimas analizuoti milžiniškus duomenų kiekius ir atlikti itin sudėtingus skaičiavimus sukels ne tik didelį teigiamą proveržį įvairiose srityse, bet ir rimtą grėsmę kibernetiniam saugumui. Kvantiniai kompiuteriai gebės išspręsti sudėtingas matematinės problemas, kurios yra dabartinės asimetrinės kriptografijos pagrindas, per ypač trumpą laiką. Vadinasi, mūsų duomenų apsaugos priemonės taps neefektyvios ir pažeidžiamos. Prognozuojama, kad per artimiausius 5-10 metų gali būti sukurti tokie galingi kvantiniai kompiuteriai, kurie gebės šiuo metu plačiai naudojamus asimetrinio šifravimo algoritmus, pavyzdžiui, RSA (angl. *Rivest-Shamir-Adleman*), DSA (angl. *Digital Signature Algorithm*) ir ECC (angl. *Elliptic Curve Cryptography*), nulaužti ir šie duomenų saugumo užtikrinimo būdai taps nebeefektyvūs. Šio kriptografinės apsaugos problemos sprendimas – postkvantinė kriptografija (angl. *Post-Quantum Cryptography* (PQC)), t. y. kriptografijos metodai, sukurti taip, kad būtų atsparūs kvantinių kompiuterių galiai.

Nacionalinis standartų ir technologijos institutas (angl. *National Institute of Standards and Technology* (NIST)), pagrindinė JAV agentūra, kurianti technologijų ir matavimo standartus, 2024 m. rugpjūčio 13 d. pristatė naujus standartizuotus postkvantinės kriptografijos algoritmus. EK parengė Koordinuoto perėjimo prie postkvantinės kriptografijos veiksmų gaires, taip pat sudarė Postkvantinės kriptografijos ekspertų grupę.

2024 m. KAM ir NKSC kartu su kitų ES valstybių kompetentingomis institucijomis parengė ir išplatino bendrą pranešimą¹³. Pranešimu siekiama dar kartą atkreipti dėmesį į kvantinės kompiuterijos keliamas grėsmes dabartinei kriptografijai ir pabrėžti būtinybę pereiti prie postkvantinės kriptografijos kuo greičiau.

12

Politinė deklaracija dėl dirbtinio intelekto atsakingo panaudojimo karinėms reikmėms ir autonomijos (angl. *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*). Prieiga per internetą <https://www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy>.

13

Bendras KAM, NKSC prie KAM, kitų ES valstybių kompetentingų institucijų pranešimas „Dėl saugaus rytojaus šiandien – perėjimas prie postkvantinės kriptografijos“. Prieiga per internetą <https://kam.lt/wp-content/uploads/2024/12/ES-bendras-valstybiu-pranesimas-del-postkvantines-kriptografijos-1.pdf>.

2 Dalyvavimas formuojant ir įgyvendinant ES kibernetinio saugumo politiką

ES teisėkūros iniciatyvos

ES kibernetinė darbotvarkė 2024 m. iš esmės buvo skirta deryboms dėl ES teisės aktų projektų kibernetinio saugumo srityje užbaigti ir pagalbai ES narėms dėl siūlymų įgyvendinimo teikti.

2024 m. gruodžio 10 d. įsigaliojo Kibernetinio atsparumo aktas, nustatantis skaitmeninių produktų, tiekiamų ES rinkai, projektavimo, kūrimo, gamybos kibernetinio saugumo reikalavimus, taip pat šių produktų tiekimo į rinką taisykles ir kitų ekonominės veiklos vykdytojų (importuotojų, platintojų) pareigas. Kibernetinio atsparumo aktas įsigalios 2027 m. pabaigoje ir bus taikomas visose ES šalyse. Pasirengimą įgyvendinti teisės aktą Lietuvoje koordinuoja KAM.

2024 m. gruodžio 19 d. buvo pakeistas Kibernetinio saugumo aktas ir priimtas Kibernetinio solidarumo aktas¹⁴. Kibernetinio saugumo akto pakeitimu sudaromos sąlygos ES mastu sertifikuoti valdomas saugumo paslaugas, o Kibernetinio solidarumo aktu siekiama:

- ✓ sukurti visos Europos kibernetinio saugumo centrų tinklą;
- ✓ sukurti reagavimo į kibernetinio saugumo krizes mechanizmą;
- ✓ numatyti didelio masto kibernetinio saugumo incidentų peržiūros mechanizmą.

Įgyvendindama 2024 m. balandžio 11 d. priimtas EK rekomendacijas dėl Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairių¹⁵, KAM pradėjo dalyvauti EK sudarytoje Postkvantinės kriptografijos ekspertų darbo grupėje. Šios darbo grupės tikslas – parengti perėjimo prie postkvantinės kriptografijos veiksmų gaires ir užtikrinti koordinuotą visų ES valstybių narių perėjimą prie postkvantinės kriptografijos.

Naujoji EK darbą pradėjo 2024 m. pabaigoje. EK pirmininkė Ursula von der Leyen įgaliojamajame rašte vykdomajai pirmininko pavaduotojai Henni Virkkunen išklė tikslą pagerinti Europos kibernetinio saugumo sertifikavimo sistemų priėmimo procesą, t. y. peržiūrėti Kibernetinio saugumo aktą. Siūlymų dėl šio akto laukiama 2025 m. antroje pusėje. Taip pat H. Virkkunen pavesta prisidėti prie veiksmų plano, skirto ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetiniam saugumui stiprinti, parengimo. EK siūlymas dėl šio plano jau paskelbtas¹⁶. EK pirmininkės U. von der Leyen įgaliojamajame rašte ES gynybos ir kosmoso komisarui Andriui Kubiliui daug dėmesio skiriama ES kibernetinės gynybos stiprinimui ir susijusių iniciatyvų vystymui. Komisaras A. Kubilius taip pat prisidės prie darbo stiprinant ES kibernetinį atsparumą ir kovą su kibernetinėms ir hibridinėms atakomis. Komisarų užduotis – ne tik užtikrinti kibernetinės gynybos pajėgumų plėtrą ES, bet ir bendradarbiavimą su NATO.

EK, siekdama mažinti kibernetinio saugumo specialistų trūkumą Europoje ir tobulinti jų įgūdžius ir plėtodama Kibernetinio saugumo įgūdžių akademijos¹⁷ veiklą, 2024 m. gruodžio 4 d. inicijavo naujo Pramonės ir akademinės bendruomenės tinklo (angl. *Industry-Academia Network*; toliau – tinklas) kūrimą ir pakvietė prisijungti ES pramonės ir švietimo institucijas. Tikimasi, kad pramonės ir švietimo institucijų atstovai bendradarbiaudami vykdys įvairias konkrečias veiklas, pavyzdžiui, kurs ar atnau-



14

2024 m. gruodžio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2025/38, kuriuo nustatomas solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Kibernetinio solidarumo aktas). Prieiga per internetą <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0038>.

15

2024 m. balandžio 11 d. Europos Komisijos rekomendacijos (ES) 2024/1101 dėl Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairių. Prieiga per internetą https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=OJ:L_202401101.

16

2025 m. sausio 15 d. Europos Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei Regionų komitetui – Europos veiksmų planas dėl ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinio saugumo (COM(2025) 10 galutinis). Prieiga per internetą <https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers>.

17

2023 m. balandžio 18 d. Europos Komisijos komunikatas Europos Parlamentui ir Tarybai – Kibernetinio saugumo srities talentų trūkumo problemos sprendimas siekiant didinti ES konkurencingumą ir atsparumą bei skatinti jos augimą (Kibernetinio saugumo įgūdžių akademija) (COM(2023) 207 galutinis). Prieiga per internetą <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2023:207:FIN>.

jins bendras kibernetinio saugumo mokymo programos, ieškos bendrų sprendimų dėl prieigos prie kibernetinio saugumo praktinių įgūdžių laboratorijų (angl. *cyber ranges*) suteikimo, tobulins mikro-kredencialus kibernetinio saugumo srityje ir pan. Aukštojo mokslo institucijos, Europos universitetų aljansai ir profesinio mokymo programų teikėjai gali nuolat teikti paraiškas prisijungti prie tinklo¹⁸, o privataus sektoriaus organizacijos – savanoriškai įsipareigodamos dalyvauti Kibernetinio saugumo įgūdžių akademijos veikloje.

ES kibernetinė diplomatija

2024 m. ES aktyviai taikė ES kibernetinės diplomatijos priemonių mechanizmą, skatino bendradarbiavimą stiprinančias priemones, rengdama kibernetinius dialogus su partneriais. Kibernetiniai dialogai leidžia ES ir globaliems partneriams keistis nuomonėmis apie kibernetines grėsmes ir ieškoti bendradarbiavimo galimybių kibernetinio saugumo srityje. 2024 m. ES surengti kibernetiniai dialogai su bendramintėmis partnerėmis – Jungtine Karalyste, Ukraina ir Japonija.

ES ir ES valstybės narės kartu su bendraminčiais partneriais 2024 m. gegužės 3 d. deklaracijomis griežtai pasmerkė Rusijos vykdomą kenkėjišką kibernetinę veiklą prieš ES valstybių narių, įskaitant ir Lietuvos, demokratines institucijas ir rinkimų procesus. Solidarizuodamasi su Australija, ES ir ES valstybės narės 2024 m. sausio 29 d. pasmerkė Rusijos kibernetinių nusikaltėlių kenkėjišką veiklą prieš šalies sveikatos priežiūros sektorių. ES taip pat pareiškė solidarumą su Jungtine Karalyste dėl Kinijos kenkėjiškos kibernetinės veiklos poveikio Jungtinės Karalystės demokratiniams procesams.

Siekdama atgrasyti iš trečiųjų šalių kylančias ar nusikalstamų veikėjų keliamas kibernetines grėsmes ir atakas prieš ES ir ES valstybes nares, ES toliau taikė 2019 m. nustatytas kibernetinių grėsmių ribojamąsias priemones. ES taiko tikslines ribojamąsias priemones asmenims ar subjektams, susijusiems su kibernetiniais išpuoliais, kurie daro didelį poveikį ir kelia išorės grėsmę ES ar jos valstybėms narėms. 2024 m. į šį kibernetinių sankcijų sąrašą įtraukti dar 6 asmenys, tiesiogiai susiję su Rusijos Federaline saugumo tarnyba ir kibernetinėmis grupuotėmis. Šiuo metu kibernetinių sankcijų sąrašė yra 14 asmenų ir 4 juridiniai asmenys iš Rusijos, Kinijos ir Šiaurės Korėjos¹⁹.



3 ES gynybos iniciatyvų naudojimas bendradarbiavimui ir projektų finansavimui

ES Kibernetinių greitojo reagavimo pajėgų (angl. *Cyber Rapid Response Teams (CRRT)*) plėtra

Lietuva nuo 2018 m. vadovauja ES nuolatinio struktūrizuoto bendradarbiavimo projektui „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“ (toliau – PESCO CRRT projektas). PESCO CRRT projekto tikslas – užkirsti kelią kibernetinėms atakoms ir reaguoti į kibernetinius incidentus ES valstybėse narėse, bendros saugumo ir gynybos politikos karinėse misijose ir operacijose bei teikti paramą partneriams.

2024 m. prie PESCO CRRT projekte jau dalyvavusių šalių: Estijos, Kroatijos, Lenkijos, Lietuvos, Nyderlandų, Rumunijos, Belgijos, Slovėnijos, Danijos, prisijungė 3 naujos ES valstybės narės – Austrija,

18

Prieiga per internetą https://ec.europa.eu/eusurvey/runner/Industry_Academia_Network_2025.

19

2019 m. gegužės 17 d. ES Tarybos sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais. Prieiga per internetą <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019D0797-20240624>.

Latvija ir Italija. Taip buvo gerokai sustiprintos Kibernetinės greitojo reagavimo pajėgos, padidėjo galimybės reaguoti į daugiau kibernetinių incidentų vienu metu tiek ES valstybėse narėse, tiek ES institucijose, misijose ir operacijose bei partnerėse šalyse. Stebėtojo teisėmis PESCO CRRT projekte šiuo metu dalyvauja Graikija, Prancūzija, Ispanija ir Suomija.

2024-ieji buvo išskirtiniai Lietuvai metai PESCO CRRT veikloje – Lietuva ne tik koordinavo projektą, bet ir vadovavo reagavimo komandų operacinėms veikloms: organizavo pajėgų pratybas, mokymus, reagavimo į paramos prašymus veiksmus ir surengė metinį PESCO CRRT Tarybos susitikimą Vilniuje.

2024 m. PESCO CRRT projektas buvo taikytas 3 kartus – Kibernetinės greitojo reagavimo pajėgos dalyvavo kartu su NKSC užtikrinamos kibernetinį saugumą Europos Parlamento rinkimuose Lietuvoje, taip pat 2 kartus vyko į Moldovą atlikti Moldovos valstybės institucijų tinklų pažeidžiamumo vertinimo ir prisidėti prie Moldovos prezidento rinkimų ir ES referendumo kibernetinio saugumo užtikrinimo.

Prie Lietuvos vadovaujamo PESCO CRRT projekto prisijungiant vis daugiau narių ir daugėjant pajėgumo pasitelkimo atvejų, PESCO CRRT projektas susilaukia vis daugiau dėmesio iš kitų ES valstybių narių, taip pat ir iš ES institucijų. PESCO CRRT projektas įtraukiamas į įvairius ateities planavimo scenarijus, susijusius su ES kibernetine gynyba, kibernetinio saugumo užtikrinimu ir reagavimu į galimus incidentus ES šalyse, institucijose bei ES bendrosios saugumo ir gynybos politikos misijos ir operacijose.

4

KAM veikla plėtojant tarptautinį bendradarbiavimą kibernetinio saugumo srityje

Bendradarbiavimas su JAV

2024 m. lapkritį patvirtintas JAV ir Lietuvos 2025–2029 m. bendradarbiavimo kibernetinio saugumo ir gynybos srityje planas. Sutarta, kad Lietuva ir JAV stiprins bendradarbiavimą koncentruodamosi į 4 pagrindines kryptis:

- ✓ vystys kibernetinį pajėgumą ir stiprins koordinuotą atsaką į kibernetinius incidentus;
- ✓ stiprins karinį bendradarbiavimą kibernetinės gynybos srityje;
- ✓ gerins informacijos apie kibernetines grėsmes keitimosi procedūras ir bendradarbiaus kibernetinio saugumo tyrimų srityje;
- ✓ skatins dalyvauti bendrose pratybose ir mokymuose.

2024 m. buvo toliau stiprinamas bendradarbiavimas su JAV Pensilvanijos nacionaline gvardija (angl. *Pennsylvania National Guard* (PANG)) (toliau – PANG). PANG atstovai prisidėjo prie NKSC rengiamų studijų apie kibernetines grėsmes iš Kinijos bei kibernetines grėsmes kritinei infrastruktūrai Baltijos jūros regione²⁰. Taip pat PANG kartu su NKSC kibernetinių grėsmių analizės celės specialistais stebėjo Lietuvos Respublikos Prezidento rinkimus. 2024 m. pabaigoje PANG kartu su Kalifornijos nacionaline gvardija (angl. *California National Guard* (CalGuard)) (toliau – CalGuard) dalyvavo didžiausiose Lietuvos



20

Informacinis leidinys „Kaip atpažinti Kinijos kibernetines grėsmes“ (angl. *How To Recognize China Cyber Threats*). Prieiga per internetą <https://www.nksc.lt/doc/rkgc/How-To-Recognize-China-Cyber-Threats.pdf>. Informacinis leidinys „Kibernetinės grėsmės kritinei infrastruktūrai Baltijos jūros regione“ (angl. *Cyber Threats to Critical Infrastructure in the Baltic Sea*). Prieiga per internetą https://www.nksc.lt/doc/rkgc/2024_Cyber_Threats_to_Critical_Infrastructure_in_the_Baltic_Sea_region.pdf.

kariuomenės organizuojamose kibernetinio saugumo pratybos „Gintarinė migla“. Lietuvos kritinės infrastruktūros įmonių kibernetinių incidentų valdytojai sudarė komandą kartu su PANG, o į Lietuvą atvykę Ukrainos kariai pratybose treniravosi kartu su CalGuard.

2024 m. Lietuvos kariuomenės Gynybos štabo ir KAM ekspertai bendradarbiavo su JAV karinių pajėgų Europoje vadavieta (angl. *U.S. European Command (USEUCOM)*) ruošdamiesi LK KGV steigimui. 2024 m. vasarį organizuotos pirmosios stalo pratybos, skirtos LK KGV vizijai, pradiniam operaciniam pajėgumui aptarti ir abiem valstybėms apsikeisti gerąja praktika rengiant kibernetinio saugumo personalą.

JAV kibernetinės vadavietės (angl. *US Cyber Command (USCYBERCOM)*) atstovai 2024 m. gruodžio mėnesį baigė gynybinę kibernetinio saugumo operaciją Lietuvoje. JAV ir NKSC kibernetinio saugumo specialistai 2024 m. kartu stiprino praktinį sąveikumą ir didino vieno iš viešojo sektoriaus subjektų tinklų atsparumą kibernetinėms grėsmėms. Tai jau ketvirtoji Lietuvos įstaiga, kurioje vyko JAV ir Lietuvos kibernetinės gynybos operacija nuo bendradarbiavimo su USCYBERCOM ir PANG kibernetinės gynybos srityje pradžios.

Lietuva iniciatyvos „Iniciatyva prieš išpirkos reikalaujančias atakas“ viena iš lyderių



Lietuva dalyvauja tarptautinėje iniciatyvoje „Iniciatyva prieš išpirkos reikalaujančias atakas“ (angl. *Counter Ransomware Initiative (CRI)*) (toliau – CRI). Tai aukšto lygio JAV Baltųjų rūmų organizuojama iniciatyva, skirta 71 valstybės ir tarptautinės organizacijos pastangoms suvienyti kovojant su išpirkos reikalaujančiomis kibernetinėmis atakomis. Lietuvos atstovai iš KAM ir NKSC yra vieni iš 6 šios iniciatyvos lyderių ir yra atsakingi už informacijos valdyseną. Siekiant maksimalaus keitimosi informacija efektyvumo, Lietuvos iniciatyva 2024 m. pradėtos kurti aiškios taisyklės, kaip ir su kuo dalytis informacija apie išpirkos reikalaujančių kibernetinių atakų grėsmes. 2024 m. KAM ir NKSC atlikti darbai:

- ✓ 2023 m. sudaryta galimybė iniciatyvos šalims naudotis informacijos apsikeitimo platforma, skirta tarptautinių lygiu informacijai apie išpirkos reikalaujančių veikėjų grėsmes dalytis, o 2024 m. šia platforma aktyviai pradėjo naudotis vis daugiau iniciatyvos narių;
- ✓ kartu su Belgija organizuoti informacijos dalijimosi mokymai daugiau nei 100 CRI narių;
- ✓ pradėtos rengti standartinės vienodo dalijimosi informacija procedūros labai išaugus iniciatyvos narių skaičiui.

Parama Ukrainai kibernetinio saugumo ir gynybos pajėgumams



IT koalicija, skirta Ukrainai remti, įkurta 2023 m. rugsėjį Ukrainos gynybos kontaktinės grupės susitikime Ramšteine, Vokietijoje, tebevykstant Rusijos plataus masto invazijai Ukrainoje. IT koalicija daug dėmesio skiria paramos teikimui Ukrainos ginkluotosioms pajėgoms ir Gynybos ministerijai informacinių technologijų, ryšių ir kibernetinio saugumo srityse. 2024 m. pabaigoje IT koaliciją sudarė 17 šalių, dar 2 šalys išreiškė ketinimą prisijungti artimiausiu metu, o 11 šalių ir tarptautinių organizacijų turėjo stebėtojų statusą. 2024 m. IT koalicijai priklausančios valstybės, tarp jų ir Lietuva, Ukrainos ginkluotosioms pajėgoms ir Gynybos ministerijai perdavė informacinės ir ryšių technologijų įrangos už 422,9 mln. Eur, o bendroms viešųjų pirkimų iniciatyvoms įgyvendinti surinko 73,7 mln. Eur.

Dvišalio bendradarbiavimo pagrindais 2024 m. Lietuva ir toliau teikė kibernetinio saugumo paramą Ukrainai:

- ✓ sudarė sąlygas Ukrainos kibernetinio saugumo ekspertams rotaciniu principu tęsti darbus Regioniniame kibernetinės gynybos centre Kaune (NKSC filiale);
- ✓ bendradarbiavo su Ukrainos gynybos institucijomis tyrimų srityje;
- ✓ rengė kompiuterinių tinklų kibernetinio saugumo mokymus ir suteikė praktikos galimybes Ukrainos kibernetinio saugumo specialistams ir kadetams;
- ✓ kvietė Ukrainos gynybos institucijų kibernetinio saugumo ekspertus dalyvauti Lietuvos kariuomenės rengiamose tarptautinėse kibernetinės gynybos pratybose „Gintarinė migla“.

Bendradarbiavimas su Indijos ir Ramiojo vandenynų regiono šalimis

Lietuva, glaudžiai bendradarbiaudama kibernetinio saugumo srityje su bendramintėmis Indijos ir Ramiojo vandenynų regiono šalimis: Japonija, Australija, Pietų Korėja, Singapūru, Filipinais ir Taivanu, prisideda prie bendro ES, NATO ir bendraminčių Indijos ir Ramiojo vandenynų regiono valstybių kibernetinio saugumo stiprinimo reaguojant į vis didėjančios rizikas kibernetinėje erdvėje, kylančias iš Rusijos, Kinijos, Šiaurės Korėjos ir Irano.

2024 m. krašto apsaugos sistemos atstovai tęsė intensyvias aukšto lygio ir praktinio pobūdžio konsultacijas su bendramintėmis Indijos ir Ramiojo vandenynų regiono šalimis, taip pat dalyvavo bendrose kibernetinės gynybos pratybose. Vienas didžiausių pasiekimų – 2024 m. rugsėjį Vilniuje surengtas pirmasis Lietuvos ir Japonijos kibernetinio saugumo dialogas, kuriame dalyvavo abiejų šalių kibernetinių institucijų atstovai. Panašaus pobūdžio dialogai planuojami ir su kitomis regiono partnerėmis.

Lietuvos inicijuotas ir Vilniuje pirmą kartą 2023 m. surengtas aukšto lygio NATO, Indijos ir Ramiojo vandenynų regiono ir partnerių šalių kibernetinio saugumo forumas „Cyber Champions Summit“ 2024 m. tapo tęstiniu ir vienu svarbiausių (angl. flagship) NATO bendradarbiavimo su Indijos ir Ramiojo vandenynų regiono šalimis projektų. Šį forumą 2024 m. rugsėjį surengė Australija, o KAM kartu su NKSC prisidėjo prie bendrų NATO ir Australijos pastangų organizuojant „Cyber Champions Summit“ renginį.



5 Kibernetinė gynyba – viena esminių NATO atgrasymo ir gynybos užduočių

Atsižvelgiant į specifinius kibernetinės erdvės karinio planavimo ir operacijų vykdymo poreikius, atskirose NATO sąjungininkėse šalyse kuriamos kibernetinės pajėgos, tam tikri pokyčiai vykdomi ir NATO štabuose. 2024 m. NATO viršūnių susitikime Vašingtone buvo sutarta įkurti naują NATO integruotą kibernetinės gynybos centrą (*NATO Integrated Cyber Defence Centre*, NICC), siekiant pagerinti tinklų apsaugą, situacijos suvokimą ir kibernetinės erdvės, kaip vieno iš operacinių domenų, įgalinimą. Šis centras sujungs Aljanso kibernetines struktūras, karinius ir civilinius dėmenis, įtrauks sąjungininkių atstovus.

Siekdamos sustiprinti Aljanso atgrasymo politiką ir įrankius kibernetinėje erdvėje, NATO sąjungininkės Vašingtone patvirtino atnaujintas strateginių priemonių taikymo reaguojant į didelio masto kibernetinius išpuolius gaires.

Lietuva aktyviai prisideda prie Aljanso kibernetinės gynybos politikos formavimo, kibernetinių pajėgumų stiprinimo, taip pat dalyvauja kibernetinės gynybos pratybose ir iniciatyvose.

Lietuvos atstovai 2024 m. ir toliau dalyvavo NATO kibernetinės gynybos kompetencijos centro (angl. *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE)) (toliau - CCDCOE)²¹ veikloje. Tai suteikia krašto apsaugos sistemos atstovams galimybę susipažinti su NATO ir kitų šalių kibernetinės srities patirtimi, dalyvauti CCDCOE rengiamose kibernetinio saugumo pratybose, seminaruose, kursuose, konferencijose, gauti CCDCOE vykdomų tyrimų medžiagą, įtraukti į CCDCOE darbų programą nacionalinius kibernetinio saugumo poreikius.

KAM, NKSC ir Lietuvos kariuomenės atstovai kasmet dalyvauja CCDCOE organizuojamose pratybose „Suremti skydai“ (angl. *Locked Shields*). 2024 m. pratybose Lietuva ir Nyderlandų Karalystė sudarė bendrą kibernetinio saugumo ekspertų komandą (angl. *Blue Team*), kuri tobulino praktinius įgūdžius ginti nacionalines informacines sistemas ir kritinę infrastruktūrą nuo realiu laiku vykdomų kibernetinių atakų.

2024 m. pratybų „Suremti skydai“ strateginėje sesijoje „STRATEX“ dalyvavo KAM, NKSC, Lietuvos kariuomenės ir Nacionalinio krizių valdymo centro (toliau - NKVC) atstovai. Dalyvavimas sesijoje „STRATEX“ leidžia tobulinti nacionalines sprendimų priėmimo procedūras, priimti sprendimus reaguojant į kibernetines grėsmes ir incidentus, tobulinti sąveiką tarp NKSC ir paveiktų kritinės infrastruktūros valdytojų, subjektų, NKVC, kitų ministerijų ir suinteresuotų trečiųjų šalių.

21

NATO kibernetinės gynybos kompetencijos centras. Prieiga per internetą <https://ccdcoe.org/>.

Lietuva pagal pasaulinį kibernetinio saugumo indeksą



2024 m. rugsėjo 12 d. ITU 5 kartą paskelbė pasaulinį kibernetinio saugumo indeksą²² (angl. *Global Cybersecurity Index (GCI)*) (toliau – GCI). GCI rezultatas pagrįstas šalių kibernetinio saugumo įsipareigojimų vykdymu 5 srityse: teisinėje, techninėje, organizacinėje, gebėjimų ugdymo ir bendradarbiavimo. Nuo ankstesnių ITU paskelbtų GCI, paskutinis skiriasi tuo, kad šalys nebuvo reitinguojamos, o pagal surinktą balų skaičių suskirstytos į 5 kategorijas.

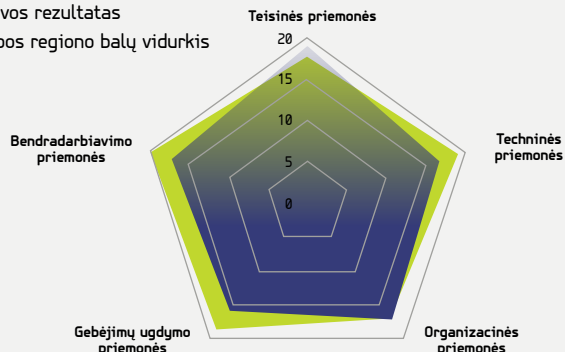
ITU ekspertai vertino, kaip Lietuva vykdo įsipareigojimus kibernetinio saugumo srityje nuo 2020 m. iki 2023 m. I pusmečio imtinai. Lietuva surinko 92,88 balo ir pagal tai priskiriama 2 kategorijai, t. y. prie pažangių šalių (žr. **1 pav.**). Šis rezultatas rodo, kad Lietuva nuolat stiprina kibernetinį saugumą 5 minėtose GCI srityse. Vis dėlto svarbu pažymėti, kad Lietuva pagal 2020 m. GCI užėmė aukštesnę vietą, palyginti su kitomis šalimis. Šis pokytis rodo ir stiprėjančią bendrą „konkurenciją“ pasauliniame kibernetinio saugumo kontekste, nes kitos šalys, ypač Europoje, ėmėsi didelių kibernetinio saugumo pokyčių. Taip pat būtina pabrėžti, kad šio GCI duomenys buvo renkami tuo metu, kai Lietuva dar tik pradėjo TIS 2 direktyvos perkėlimo į nacionalinę teisę darbus, o Kibernetinio saugumo plėtros programa dar nebuvo patvirtinta. Atkreiptinas dėmesys, kad GCI vertinti svarbūs rodikliai priklauso ne tik nuo KAM ir jai pavaldžių institucijų pastangų, bet ir nuo kitų Lietuvos valstybės institucijų kompetencijos, pavyzdžiui, Lietuvos policijos, VDAI, Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos, Lietuvos Respublikos užsienio reikalų ministerijos ir kitų.

▼ **1 pav.**

Lietuva pagal ITU indeksą
(šaltinis – GCI 5th Edition)

Lietuva

- Lietuvos rezultatas
- Europos regiono balų vidurkis



Šalies rezultatas
Šalies balas iš galimų 20

Teisinės priemonės	Techninės priemonės	Organizacinės priemonės	Gebėjimų ugdymo priemonės	Bendradarbiavimo priemonės
17,79	19,25	17,05	18,79	20

Santykinio stiprumo sritys

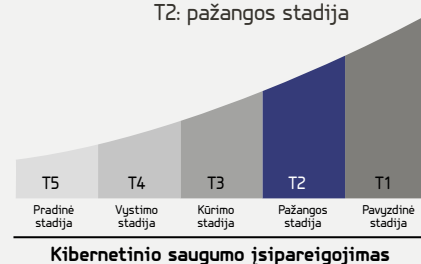
- Techninės priemonės
- Bendradarbiavimo priemonės

Potencialaus augimo sritys

- Teisinės priemonės
- Organizacinės priemonės
- Gebėjimų ugdymo priemonės

Kibernetinio saugumo brandos lygio įvertinimas

T2: pažangos stadija



22

5-oji GCI ataskaita. Prieiga per internetą <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>.

04

Lietuvos kibernetinio saugumo būklės apžvalga



Kibernetinių incidentų dinamika Lietuvoje ir NKSC vykdomos prevencinės priemonės

Vadovo žodis



Antanas Aleknavičius, laikinai einantis NKSC direktoriaus pareigas

2024-ieji buvo reikšmingi kibernetinio saugumo politikai Lietuvoje ir kitose Europos šalyse metai. Tapome viena iš pirmųjų šalių, perkėlusią TIS 2 direktyvą į nacionalinę teisę. Tai – tik pradžia, nes laukia praktinis įgyvendinimas. Nors iššūkių netrūks, stiprinsime atsparumą visais lygmenimis. Jau 2024 m. pradžioje atnaujinome NKSC viziją ir misiją, išgryninome vertybes, nustatėme strategines veiklos kryptis ir įgyvendinome organizacinius bei struktūrinius pokyčius. Pradėjome įgyvendinti 5 didelės apimties projektus, tarp kurių – inicijuotas 40-ies saugumo operacijų centrų steigimas viešajame sektoriuje. Taip pat organizavome specializuotus mokymus kibernetinio saugumo vadovams ir ekspertams, tobulinome kibernetinio saugumo subjektams skirtą Kibernetinio saugumo informacinę sistemą, kartu su kitomis institucijomis stiprinome kibernetinių grėsmių analizės ir prevencijos pajėgumus, ieškojome būdų, kaip spartinti keitimąsi informacija apie grėsmes ir efektyviai valdyti incidentus vieno langelio principu. Be to, vykdydami Skaitmeninės Europos programos lėšomis finansuojamą projektą, inicijavome projektus, stiprinančius kibernetinio saugumo bendruomenę.



KĄ SAUGO?

- ✓ Lietuvos kibernetinę erdvę ir kibernetinio saugumo subjektus.



NUO KO SAUGO?

- ✓ Nuo kibernetinių incidentų ir jų neigiamo poveikio.



KAIP SAUGO?

- ✓ Kontroliuodamas, kaip kritines paslaugas teikiančios organizacijos įgyvendina kibernetinio saugumo organizacinius ir techninius reikalavimus.
- ✓ Vykdydamas kibernetinių grėsmių bei tinklų ir informacinės sistemos spragų paiešką.
- ✓ Koordinuodamas reagavimą į kibernetinius incidentus ir atlikdamas jų tyrimus.
- ✓ Kurdamas ir plėtodamas prevencines nacionalines kibernetinio saugumo priemones.
- ✓ Ugdydamas kibernetinio saugumo kompetencijas.



NACIONALINIS
KIBERNETINIO SAUGUMO
CENTRAS

Svarbiausi 2024 m. įvykiai ir tendencijos



Didžiausią išorinį poveikį Lietuvos kibernetinio saugumo aplinkai 2024 m. darė geopolitinė situacija ir technologiniai veiksniai.



NKSC vertinimu, 2024 m. kibernetinio saugumo situacija Lietuvoje išliko stabili, o 63 proc. išaugęs NKSC fiksuotų incidentų skaičius daugiausia siejamas su gerėjančiais subjektų ir gyventojų raportavimo NKSC įpročiais.



Daugiausia incidentų įvyko interneto prieglobos paslaugų infrastruktūroje, užsienio subjektų sektoriuje, IPT infrastruktūroje.



Net 59 proc. visų NKSC per metus registruotų kibernetinių incidentų buvo susiję su socialinės inžinerijos metodais. Išaugo apgaulingų laiškų, DI sugeneruotų balso skambučių (angl. *vishing*) ir QR kodų sukčiavimo (angl. *qishing*) atakų skaičius.



2024 m. NKSC nustatė 6 784 potencialiai pažeidžiamas informacines sistemas ir apie rastas tinklų ir informacinės sistemos spragas informavo paveiktas organizacijas. Dauguma šių nustatytų spragų buvo susijusios su autentifikacijos neatlikimu, nuotolinio kodo naudojimu ir netinkama konfigūracijos prieiga prie jautrios informacijos.



Atsakingi pranešėjai pagal atsakingo atskleidimo principą 2024 m. NKSC pateikė 68 pranešimus apie tinklų ir informacinės sistemos spragas. Šie pranešimai leido laiku informuoti paveiktas organizacijas ir sumažinti galimą kibernetinių grėsmių poveikį.



2024 m. įvairius NKSC mokymus baigė daugiau nei 46 tūkst. asmenų, o kasmetinėse pratybose „Kibernetinio skydas“ dalyvavo daugiau nei 500 viešojo sektoriaus ir kritines paslaugas teikiančių organizacijų.



1 Aktualios kibernetinio saugumo grėsmės ir rizikos bei kibernetinio saugumo incidentai

Išorinės aplinkos vertinimas

Lietuvos kibernetinio saugumo būklę lemia daugybė išorinių veiksnių, iš kurių didžiausią įtaką daro geopolitiniai veiksniai. Ypač svarbi kaimynystė su Rusija ir Baltarusija – šios šalys didina riziką, nes jų remiamos kibernetinės grupuotės (angl. *state-sponsored groups*) vykdo atakas, susijusias su regioniais konfliktais, ir kelia įtampa NATO ir ES.

Pastaraisiais metais pasaulyje sparčiai populiarėjo elektroninius duomenis užšifruojančių ir išpirkos reikalaujančių kenkimo programinio kodo virusų kaip paslaugos (angl. *Ransomware-as-a-Service* (RaaS)) modelis⁰¹. 2024 m. išryškėjo tendencija, kad nusikaltėliai, siekdami priversti aukas sumokėti dvigubą išpirką, vis dažniau ne tik šifruoja duomenis, bet ir papildomai grasina pavišinti nutekintus duomenis (angl. *Data extortion*). ENISA duomenimis⁰², mažesnės įmonės tapo 4,2 karto pažeidžiamesnės šio tipo incidentams, nes dažnai neturi pakankamų saugumo priemonių ar išteklių tinkamai reaguoti į tokio pobūdžio grėsmes.

2024 m. visame pasaulyje fiksuotas reikšmingas paskirstytųjų paslaugos trikdymo (angl. *Distributed Denial of Service* (DDoS)) (toliau – DDoS) atakų augimas – jų skaičius išaugo 50 proc., palyginti su 2023 m. Remiantis ENISA duomenimis⁰³, iki šiol dažniausias šių atakų taikinytis – viešojo administravimo sektorius, o tokių atakų augimą daugiausia lėmė geopolitiniai konfliktai ir išaugęs haktivizmas⁰⁴. Lietuvoje dauguma DDoS atakų taip pat buvo vykdomos prieš valstybės valdymo, viešojo administravimo ir aplinkos sektorius. Tačiau, palyginti su ankstesniais metais, Lietuvoje registruotų DDoS incidentų skaičius 2024 m. sumažėjo, iš viso užregistruoti 74 atvejai (2023 m. – 89).

Taip pat kartu su technologijų pažanga kyla ir naujų grėsmių. DI, kvantinės kompiuterijos, daiktų interneto (angl. *Internet of Things* (IoT)) ir debesijos sprendimų plėtra suteikia verslui ir valstybei naujų galimybių, tačiau taip pat tampa patraukliu taikiniu kibernetinėms atakoms. Dėl spragų šios technologijos gali būti išnaudojamos ne tik informacijos vagystėms, bet ir plataus masto kibernetiniams išpuoliams.

Papildomą riziką kelia ir globalių tiekimo grandinių⁰⁵ sudėtingumas. Kadangi daugelis Lietuvos įmonių priklauso nuo tarptautinių IT paslaugų ir programinės įrangos tiekėjų, kibernetinės atakos gali jas paveikti netiesiogiai – per trečiąsias šalis. Tokiais atvejais net ir pažangiausia gynyba gali būti neveiksminga, jei pažeidžiamumas atsiranda tiekimo grandinės grandyse.



01

Paaiškinimas, kaip veikia elektroninius duomenis užšifruojančių ir išpirkos reikalaujančių kenkimo programinio kodo virusai kaip paslauga, ir pavyzdžiai (angl. *Ransomware as a Service (RaaS) Explained How It Works & Examples*). Prieiga per internetą <https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>.

02

ENISA grėsmių kraštovaizdis 2024 m. (angl. *ENISA Threat Landscape 2024*). Prieiga per internetą <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>.

03

Ten pat.

04

Haktivizmas (angl. *hacktivism*) – tai kibernetinių atakų forma, kai programiškai savo veiksmais siekia politinių, ideologinių ar socialinių tikslų, o ne finansinės naudos.

05

Tiekimo grandinė – tai organizacijų, žmonių, technologijų, veiklos, informacijos ir išteklių visuma, susijusi su tiekėjo prekės ar paslaugos suteikimu pirkėjui.

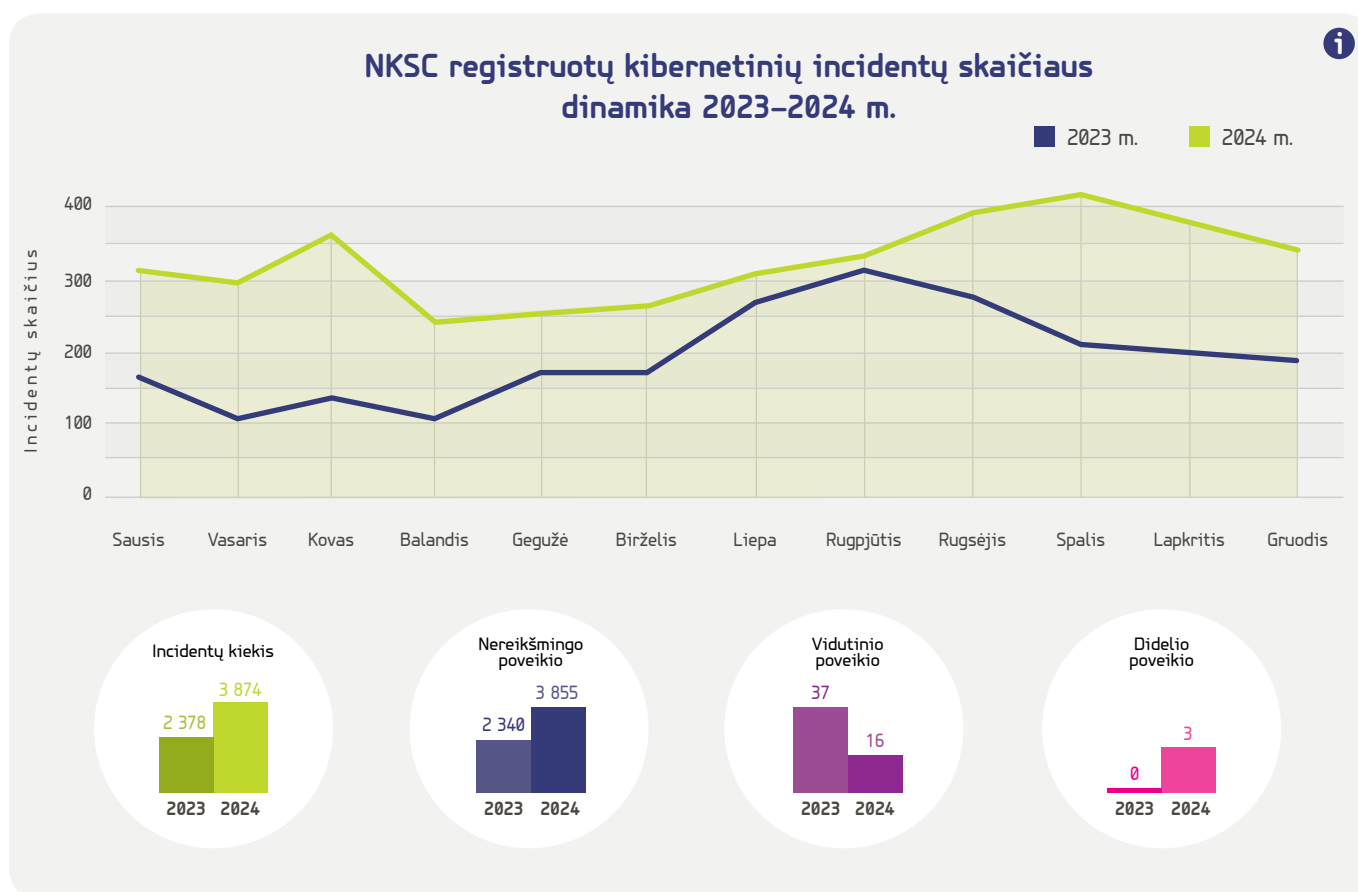
Vidinės aplinkos vertinimas

Didėja registruotų kibernetinių incidentų skaičius

2024 m. NKSC iš viso užregistravo 3 874 kibernetinius incidentus, t. y. apie 63 proc. daugiau nei ankstesniais metais (2023 m. - 2 378). Daugumą jų buvo priskirti nereikšmingai kategorijai, 16 - vidutinei (2023 m. - 37), 3 - didelei kategorijai (2023 m. tokių incidentų nebuvo) (žr. 1 pav.). Vidutinės kategorijos incidentai buvo susiję su įsilaužimais į RIS ir paslaugų trikdymu dėl DDoS atakų. Šias atakas, kaip nedaug resursų ir žinių reikalaujančią politinio spaudimo priemonę, ir toliau naudoja kibernetinių įsilaužėlių grupuotės. 3 didelės kategorijos incidentai siejami su užsienio remiamų grupuočių veikla. Svarbu paminėti, kad, pagal Kibernetinio saugumo įstatymą, Lietuvoje prievolė pranešti apie kibernetinį incidentą yra taikoma tik kibernetinio saugumo subjektams. Kitos organizacijos ir gyventojai tai gali padaryti savanoriškai, todėl tikrasis incidentų skaičius gali būti didesnis, nei nurodyta šioje ataskaitoje.



▼ 1 pav.
NKSC registruotų kibernetinių incidentų skaičiaus dinamika 2023–2024 m. (šaltinis – NKSC)



NKSC vertinimu, 2024 m. kibernetinio saugumo situacija Lietuvoje išliko stabili, o fiksuota incidentų skaičiaus dinamika daugiausia siejama su:

- gerėjančiais subjektų ir gyventojų raportavimo NKSC įpročiais. NKSC nuolat pabrėžia informavimo apie incidentus svarbą, nes tik tokiu būdu galima matyti sąryšius tarp incidentų, daryti apibendrinimus ir įžvalgas. Tikėtina, kad nuolatinis skatinimas pranešti apie incidentus duoda rezultatų - subjektai tampa aktyvesni informuodami NKSC, o Lietuvos gyventojai - sąmoningesni;

⚠ kibernetinių piktavalių vykdomomis kampanijomis prieš Lietuvos gyventojus ir institucijų darbuotojus. Siekiant išvilioti jautrią informaciją, taikomi socialinės inžinerijos metodai, naudojamosi žinomų institucijų ir įmonių vardais, pavyzdžiui, Lietuvos pašto, Valstybinės mokesčių inspekcijos (toliau - VMI), „Swedbank“ ir kt., todėl dalis gavėjų jų neatpažįsta ir patiria žalą.

Incidentų pasiskirstymas pagal sektorius

2024 m. daugiausia incidentų įvyko interneto prieglobos paslaugų infrastruktūroje, antroje vietoje - užsienio subjektų sektoriuje, trečioje vietoje - IPT infrastruktūroje (žr. 2 pav.).

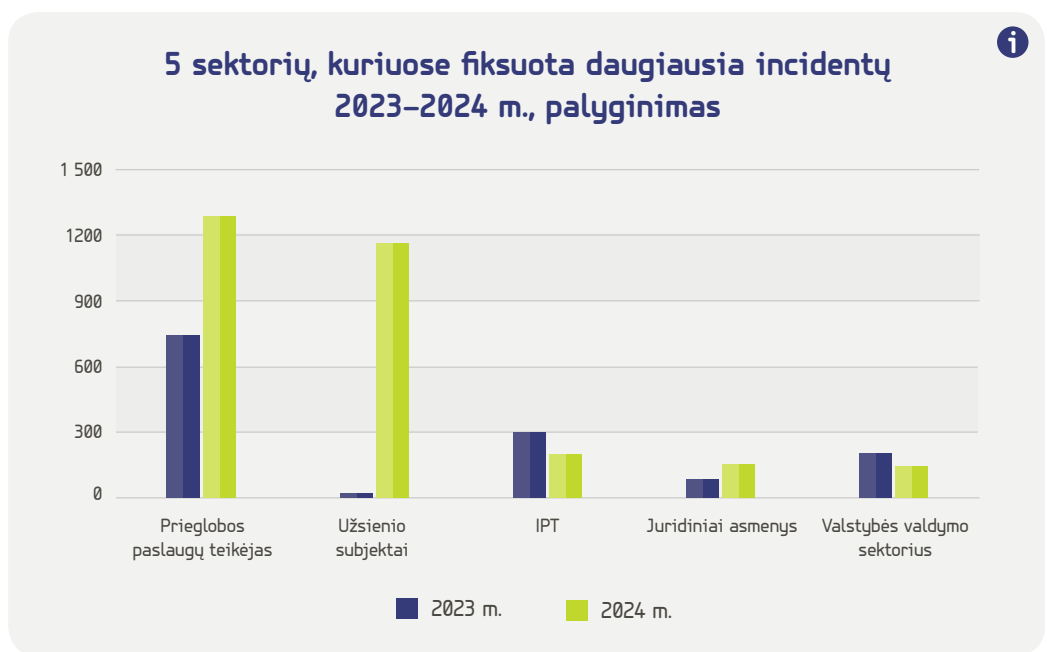
Nors tiek 2023 m., tiek ir 2024 m. interneto prieglobos paslaugų infrastruktūra pirmauja pagal fiksuotų incidentų skaičių, tačiau šiame sektoriuje matoma incidentų augimo tendencija (2023 m. - 742; 2024 m. - 1288).

Svarbu pažymėti, kad 2024 m. matyti itin išaugęs incidentų skaičius užsienio subjektų sektoriuje (2023 m. - 20; 2024 m. - 1165). Šį pokytį lėmė patikslintas incidentų priskyrimas sektoriams - nuo 2024 m. užsienio subjektų sektoriuje patiriami incidentai nebėra išskaidomi ir registruojami viename, o ne keliuose sektoriuose.

IPT sektoriuje incidentų sumažėjo (2023 m. - 301; 2024 m. - 200). Pažymėtina, kad 2023 m. šis sektorius buvo antroje vietoje, o 2024 m. - trečioje.

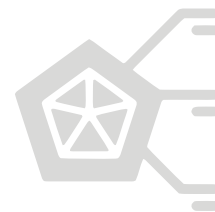
2024 m. ketvirtoje vietoje - juridinių asmenų sektorius, kuriame incidentų skaičius išaugo, palyginti su ankstesniais metais (2023 m. - 85; 2024 m. - 155).

2024 m. beveik 29 proc. sumažėjo incidentų valstybės valdymo sektoriuje (2023 m. - 203; 2024 m. - 145).



< 2 pav. 5 sektorių, kuriuose fiksuota daugiausia incidentų 2023–2024 m., palyginimas (šaltinis – NKSC)

Incidentų pasiskirstymas pagal incidentų grupes

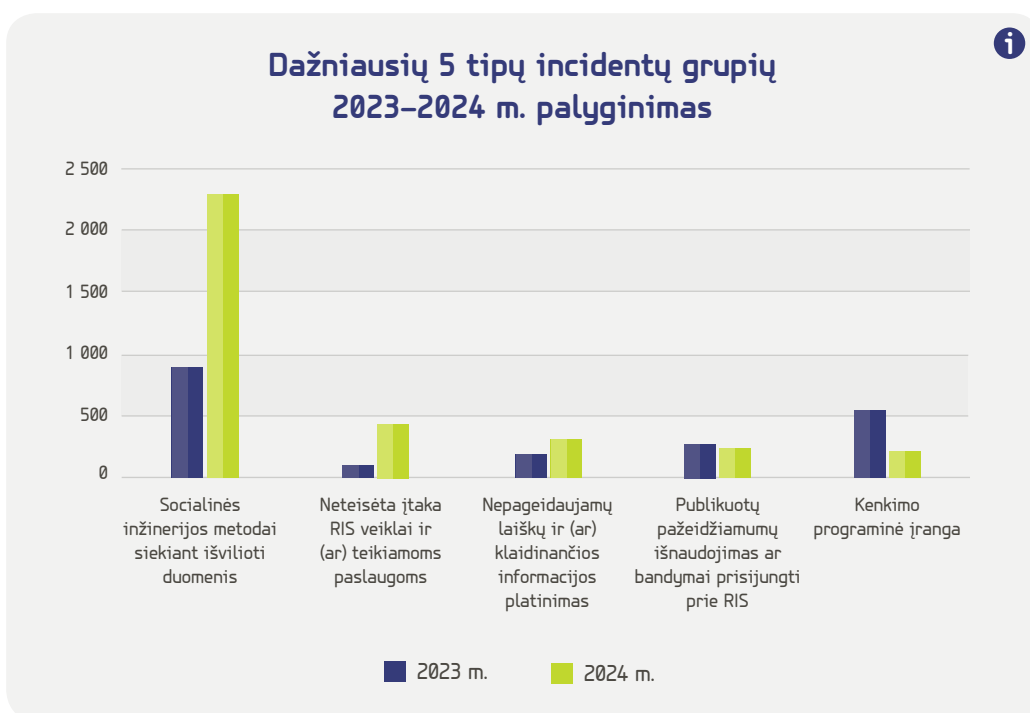


2024 m., kaip ir 2023 m., NKSC daugiausia registravo incidentų, priskiriamų socialinei inžinerijai, kai siekiama išvilioti jautrius duomenis (angl. *phishing*), pavyzdžiui, prisijungimo prie įvairių paskyrų duomenis ir pan. (žr. **3 pav.**). 2024 m. buvo matomas itin didelis šios grupės incidentų skaičiaus augimas (2023 m. - 897, 2024 m. - 2288). Pažymėtina, kad 2024 m. šio tipo incidentai sudarė net 59 proc. visų NKSC registruotų incidentų (2023 m. - 38 proc.).

Antroje vietoje pagal incidentų grupes buvo fiksuota auganti neteisėta įtaka RIS veiklai ir (ar) teikiamoms paslaugoms (2023 m. - 116; 2024 m. - 444). 2023 m. ši incidentų grupė buvo penktoje vietoje pagal incidentų skaičių.

Trečioje vietoje - nepageidaujamų laiškų ir (ar) klaidinančios informacijos platinimas (2023 m. - 200; 2024 m. - 318), o ketvirtoje - publikuotų pažeidžiamumų išnaudojimas ar bandymai prisijungti prie ryšių ir informacinių sistemų (šių atvejų skaičius išliko beveik stabilus: 2023 m. - 284, 2024 m. - 246).

Kenkimo programinės įrangos naudojimas 2024 m. buvo penktoje vietoje pagal incidentų grupes. Šioje grupėje matyti žymus incidentų skaičiaus mažėjimas, palyginti su ankstesniais metais (2023 m. - 554; 2024 m. - 223).



< 3 pav.

Dažniausių 5 tipų incidentų grupių 2023–2024 m. palyginimas (šaltinis – NKSC)

Socialinė inžinerija ir duomenų viliojimo tendencijos

Didėjant kibernetinės erdvės svarbai, vis daugiau jautrios informacijos perkeliama į internetą, o kritinės valstybės funkcijos tampa vis labiau priklausomos nuo skaitmeninių paslaugų. Priklausomybė neišvengiamai didina piktavalių motyvaciją vykdyti nusikalstamas veikas - nuo finansinių sukčiavimo iki valstybės veiklai kritinių paslaugų sutrikdymo.

ENISA duomenimis⁰⁶, 2024 m. sukčiavimo atakos sudarė 16 proc. visų kibernetinių incidentų, o Lietuvoje - net 59 proc. Pasaulio šalyse, įskaitant ir Lietuvą, ryškėja įprastų apsaugos priemonių veiksmingumą mažinantys sukčiavimo būdai, pavyzdžiui, QR kodų sukčiavimas (angl. *Qishing*) ir DI generuojami balso skambučiai. Šiais atvejais yra itin svarbu ugdyti kritinį mąstymą ir vertinti gaunamą informaciją.

Dažniausiai siunčiami įvairūs pranešimai ar laiškai, kuriuose imituojamos pašto ar kurjerių tarnybų paslaugos, taip pat VMI paslaugos, siekiant išvilioti pinigus iš gyventojų ir įmonių.

Socialinės inžinerijos atakų metu vis dažniau imituojamos populiaros IT paslaugos, pavyzdžiui, prisijungimo prie „Microsoft 365“ ar „Outlook“ paskyrų paslauga, nes vis daugiau organizacijų naudoja šias debesijos paslaugas kasdienėje veikloje, o vartotojai įpratę jomis naudotis intuityviai, dažnai nesusimąstydami apie galimą riziką. Taip piktavaliai siekia gauti prieigą prie organizacijų vidinių išteklių, konfidencialios informacijos arba apsimesti teisėtais vartotojais. Be to, šiomis atakomis dažnai paleidžiamas kenkimo kodas ar vykdomi destruktivūs veiksmai aukos infrastruktūroje, po jų gali būti reikalaujama išpirkos už informacijos grąžinimą.



Atsižvelgiant į tai, kad socialinės inžinerijos principais grįstų atakų artimiausiu metu nemažės, rekomenduojama:



stiprinti darbuotojų kibernetinio saugumo kompetencijas;



taikyti veiksmingas technines saugumo priemones;



nuosekliai laikytis kibernetinės higienos principų.

Auganti grėsmė – duomenų nutekinimas⁰⁷

Pastaraisiais metais pasaulio šalyse, įskaitant ir Lietuvą, smarkiai išaugo nutekintų prisijungimo duomenų kiekis. Tam didelę įtaką daro kibernetinės atakos, duomenų saugumo spragos ir slaptažodžių pakartotinis naudojimas skirtingose platformose. Toks duomenų nutekinimas sukelia didelę žalą - nuo finansinių nuostolių ir tapatybės vagysčių iki organizacijų reputacijos praradimo. Be to, pavogti duomenys dažnai panaudojami kibernetiniams nusikaltimams, įskaitant sukčiavimą ir šantažą, vykdyti.

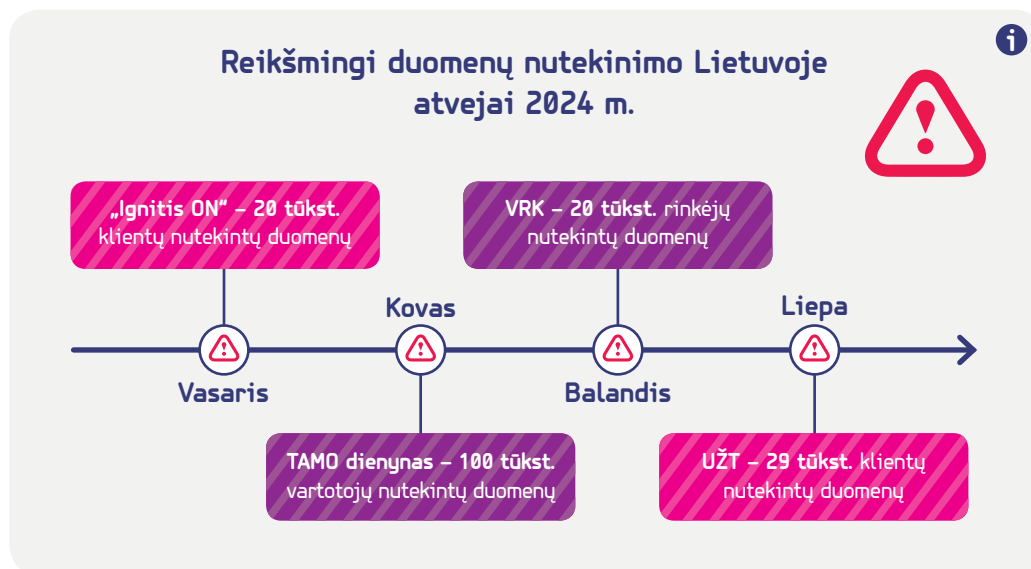
⁰⁶

ENISA grėsmių kraštovaizdis 2024 m. (angl. *ENISA Threat Landscape 2024*). Prieiga per internetą <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>.

⁰⁷

Asmens duomenų saugumo pažeidimus nagrinėja VDAI, o duomenų nutekinimo atvejus kibernetinio saugumo aspektu tiria ir apie rezultatus informuoja paveiktas institucijas NKSC.

2024 m. Lietuvoje įvyko keli reikšmingi duomenų nutekimo atvejai, dar kartą atkreipę dėmesį į asmens duomenų apsaugos svarbą (žr. 4 pav.). Paminėtinas „Ignitis ON“ incidentas, kai buvo paviešinti 20 tūkst. klientų duomenys, elektroninio dienyno TAMO pažeidimas, kai nutekinta 100 tūkst. vartotojų informacija, VRK duomenų pažeidimas, paveikęs 20 tūkst. rinkėjų, ir Užimtumo tarnybos (toliau - UŽT) atvejis, kai buvo atskleisti 29 tūkst. klientų duomenys. Šie incidentai pabrėžė būtinybę stiprinti duomenų apsaugą tiek viešajame, tiek privačiame sektoriuje.



< 4 pav. Reikšmingi duomenų nutekimo Lietuvoje atvejai 2024 m. (šaltinis – NKSC)

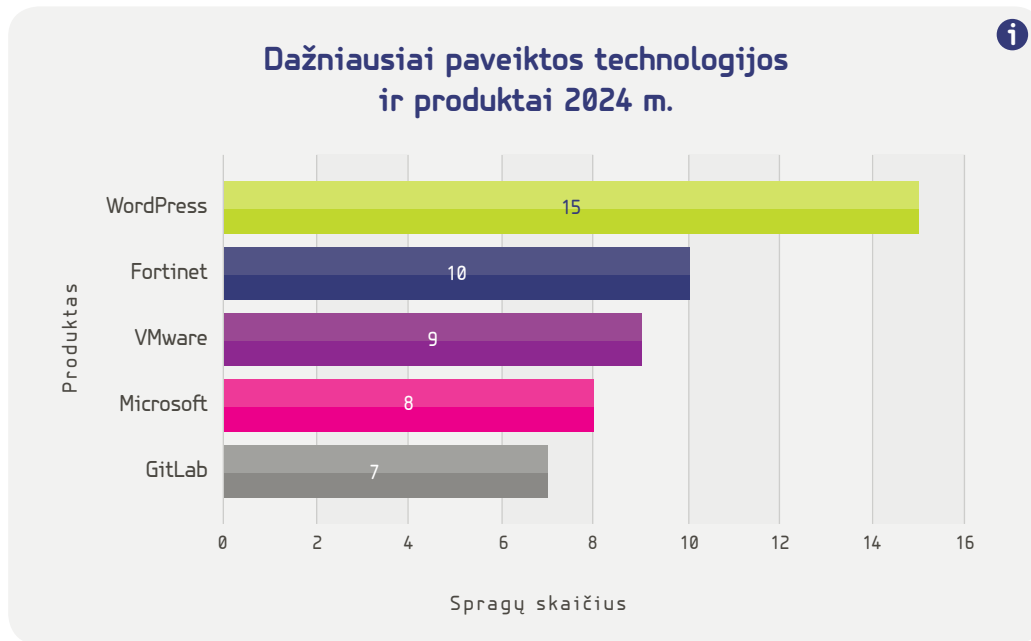
Didėjančios tinklų ir informacinės sistemos spragos

NKSC nuolat fiksuoja pranešimus apie naujai aptinkamas kritines spragas ir vykdo šių spragų Lietuvoje paiešką. 2024 m. NKSC užfiksavo didelį kritinių spragų skaičių, šie atvejai kėlė realų pavojų tiek valstybinėms institucijoms, tiek privataus sektoriaus organizacijoms. NKSC 2024 m. išsiuntė šioms organizacijoms saugumo įspėjimus dėl daugiau nei 6 700 potencialiai pažeidžiamų informacinių sistemų. Palyginti su ankstesniais metais, nustatytų potencialiai pažeidžiamų informacinių sistemų skaičius išaugo daugiau kaip 3 kartus (2023 m. – 1 963). Dauguma nustatytų spragų, apie kurias NKSC informavo paveiktus subjektus, buvo susijusios su autentifikacijos apėjimu, nuotolinio kodo naudojimu (angl. *remote code execution* (RCE)) ir netinkama konfigūracijos prieiga prie jautrios informacijos.



Lietuvoje, kaip ir visame pasaulyje, 2024 m. buvo fiksuoti kibernetiniai incidentai, susiję su kibernetinių spragų išnaudojimu dar iki jų oficialaus atskleidimo (angl. *zero-day*). Tai rodo, kad kibernetiniai piktavaliai tampa vis labiau organizuoti ir veikia strategiškai.

Didžiausią riziką 2024 m. kėlė spragos tinklų infrastruktūroje ir *Fortinet*, *Palo Alto Networks*, *Cisco*, *VMware* produktams, kurie plačiai naudojami tiek privataus, tiek viešojo sektoriaus organizacijose (žr. 5 pav.). NKSC daug dėmesio skyrė spragoms, susijusioms su *WordPress* įskiepiams, nes, remiantis ankstesnių metų patirtimi, jie dažnai tampa lengvu įsilaužėlių taikiniu dėl nepakankamos apsaugos ir atnaujinimų stokos.



< 5 pav.

Dažniausiai paveiktos technologijos ir produktai 2024 m. (Šaltinis – NKSC)

Kritinių spragų mastas ir jų išnaudojimo dinamika rodo, kad tiek privataus, tiek viešojo sektoriaus organizacijos turėtų skirti dar daugiau dėmesio saugumo priemonėms. Tendencijos aiškiai rodo, jog atakų pasinaudojant spragomis skaičius nuolat auga.

Įsilaužėliai vis dažniau taikosi į IT tiekimo grandinės spragas – per paslaugų teikėją jie gali pasiekti daugiau aukų. 2024 m. dalis tokių grėsmių buvo užkardyta apie nustatytas spragas informuojant pažeidžiamus paslaugų teikėjus ir jų klientus. Tiekimo grandinės atakų pavojų dar labiau didina tai, kad jos gali išlikti nepastebėtos ilgą laiką. Jų poveikis dažnai išryškėja tik tuomet, kai jau patiriama reali žala – prarandami duomenys, sutrinkdama veikla, patiriami reputaciniai ar finansiniai nuostoliai.

Siekdamos efektyviai sumažinti su spragomis susijusias grėsmes, organizacijos privalo taikyti nuoseklią šios rizikos valdymo politiką. Tai apima:

- ⚙️ nuolatinį spragų stebėjimą;
- ⚙️ jų vertinimą pagal rizikos lygį;
- ⚙️ laiku atliekamą pažeidžiamų sistemų atnaujinimą.

Reguliarus programinės įrangos atnaujinimas ir saugumo pataisų diegimas turėtų būti prioritetinga IT skyriaus užduotis. Uždelsus vos kelias dienas gali būti prarasti organizacijos duomenys.

Be techninių rizikos valdymo sprendimų, būtina įdiegti aiškią pokyčių valdymo (angl. *change management*) politiką, tai padėtų išvengti neapgalvotų konfigūracijos keitimų ir užtikrintų, kad naujos sistemos ir paslaugos būtų diegiamos saugiai. Organizacijos taip pat turėtų reguliariai atnaujinti IT infrastruktūros inventORIZACIJOS sąrašą – tai leistų greitai identifikuoti pažeidžiamus komponentus ir taikyti prevencines priemones. Kai įmanoma, rekomenduojama reguliariai vykdyti įsilaužimų testavimą (angl. *penetration testing*), siekiant nustatyti silpnąsias vietas ir užkirsti kelią galimoms atakoms. Kibernetinio saugumo užtikrinimas yra nuolatinis procesas, reikalaujantis ne tik technologinių sprendimų, bet ir aiškių organizacinių procedūrų įgyvendinimo.

2 NKSC atliekama organizacijų atitiktis priežiūra

Kibernetinis atsparumas prasideda nuo organizacijos pasirengimo. Kibernetinio saugumo subjektai iki įsigaliojant naujiems kibernetinio saugumo reikalavimams⁰⁸ 2024 m. turėjo įgyvendinti saugumo kontrolines priemones – organizacinius ir techninius kibernetinio saugumo reikalavimus (toliau – OTR). Atitiktis OTR kelia pasitikėjimą organizacijos teikiamomis paslaugomis, apsaugo jos reputaciją ir užtikrina efektyvesnę duomenų, tinklų ir informacinių sistemų apsaugą.

NKSC, vertindamas ypatingos svarbos informacinės infrastruktūros (toliau – YSII) būklę⁰⁹, 2024 m. atliko arba koordinavo 15 įvairaus tipo išsamių patikrinimų, iš jų 9 buvo vykdomi bendradarbiaujant su ENISA ir jos įgaliotais paslaugų teikėjais iš verslo sektoriaus. Taip pat buvo atlikti 6 išsamūs YSII subjektų atitiktis vertinimai, kurių metu buvo vykdomi tiek dokumentiniai ir darbo vietų patikrinimai, tiek išorės skenavimai ir įsilaužimo testavimai.

NKSC periodiškai vertino OTR taikymą YSII valdančiose organizacijose taikydamas vadinamąjį savideklaracijos principą, kai YSII organizacijos pačios deklaruoja savo duomenis apie atitiktį OTR. Kasmet atliekamas tokių duomenų surinkimas atskleidžia deklaruojamą YSII kibernetinio saugumo būklę.

2024 m. YSII savideklaracijos duomenys rodo, kad bendras OTR įgyvendinimo procentas padidėjo, tačiau vis dar yra nepakankamas. Palyginti su ankstesniais metais, sparčiau įgyvendinami techniniai reikalavimai organizacijose. Tačiau vien tik organizacinių reikalavimų įgyvendinimas pokyčio per metus beveik nepadarė. Pagal YSII savideklaracijos duomenis, organizacinius reikalavimus (pavyzdžiui, patvirtinta kibernetinio saugumo politika, incidentų valdymo procedūros, prieigos teisių valdymas, rizikos vertinimas ir kt.) 2024 m. visiškai buvo įgyvendinę 73 proc. YSII valdytojų, 2023 m. – 72 proc. (žr. 6 pav.).

08

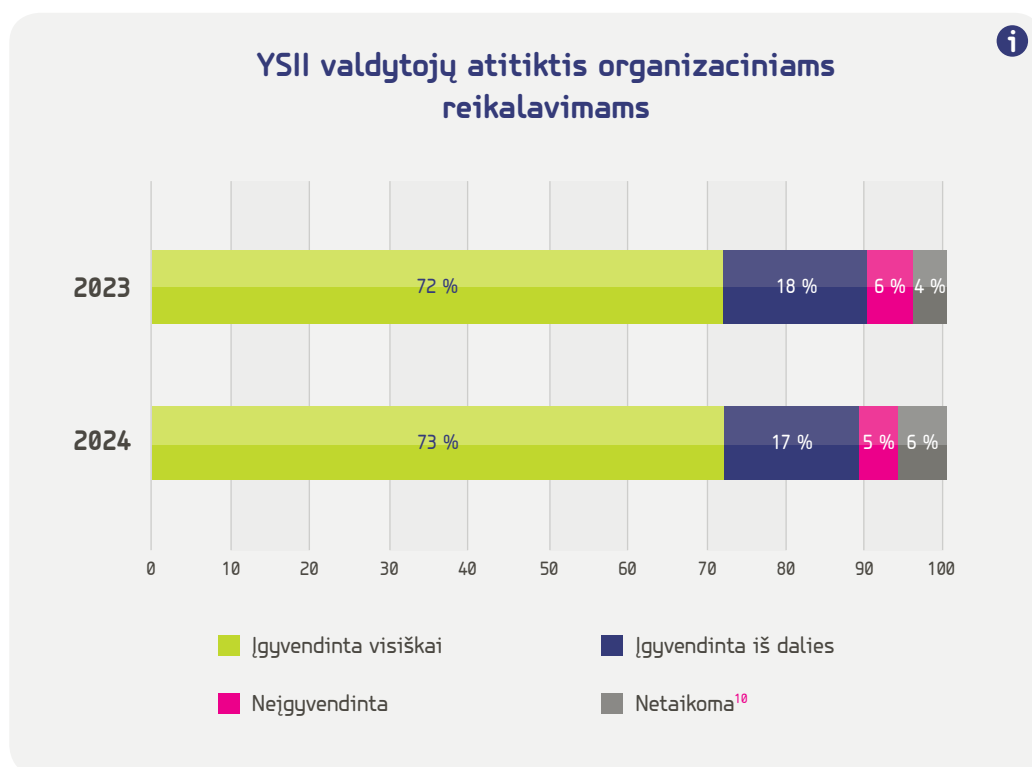
Pagal TIS 2 direktyvos reikalavimus atnaujintas Kibernetinio saugumo reikalavimų aprašas buvo patvirtintas 2024 m. lapkričio 11 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 945 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo“. Kibernetinio saugumo reikalavimų apraše nustatytiems kibernetinio saugumo reikalavimams įgyvendinti yra nustatytas ne trumpesnis kaip 12 mėn. pereinamasis laikotarpis (žr. Kibernetinio saugumo reikalavimų aprašo 71 ir 72 p.).

09

Ypatingos svarbos informacinės infrastruktūros valdytojų sąvoka Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatyme nebėra vartojama. Tačiau NKSC, vadovaudamasis minėto įstatymo 3 priedo nuostatomis, 2024 m. vertino ypatingos svarbos informacinės infrastruktūros valdytojų atitiktį tuo metu jiems galiojusiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams.

< 6 pav.

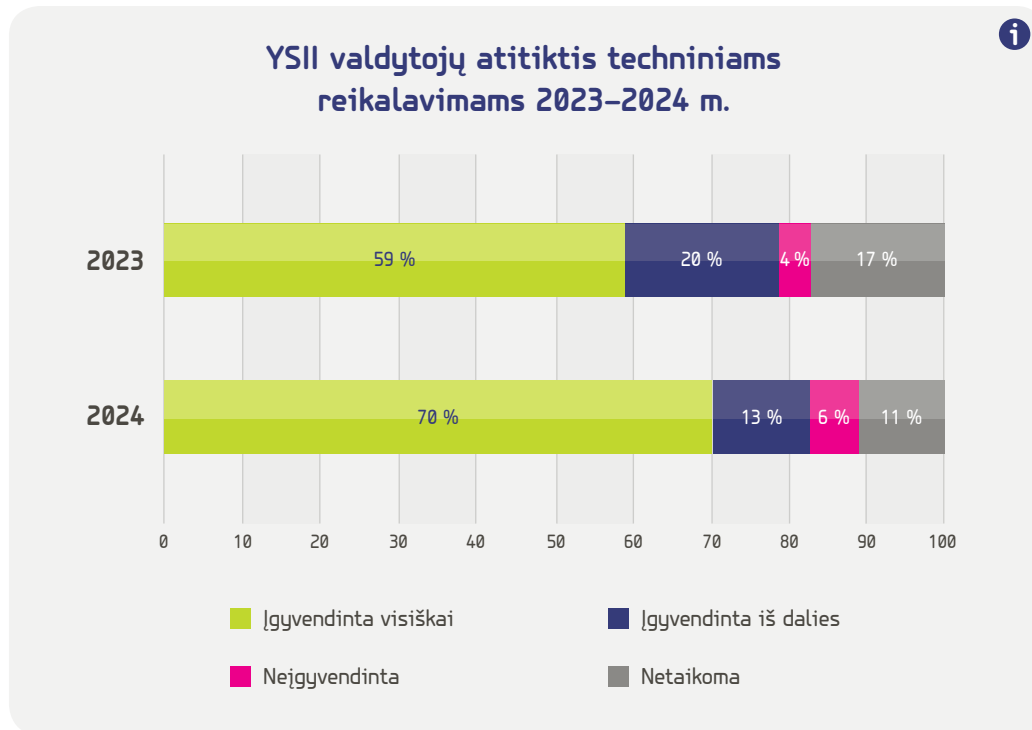
YSII valdytojų atitiktis organizaciniams reikalavimams (2023–2024 m.) (šaltinis – NKSC)



10

„Netaikoma“ – kai YSII valdytojo valdomai infrastruktūrai (technologinėms sistemoms) netaikomi informacinių sistemų reikalavimai.

Techninių reikalavimų, kuriems įgyvendinti reikia daugiau laiko, resursų (pavyzdžiui, priemonės, apimančios autentifikavimo, duomenų šifravimo, atsarginių kopijų darymo, tinklo segmentacijos ar kitus sprendimus) ir kompetentingų specialistų, per metus įvykdyta 11 proc. daugiau (žr. 7 pav.).



< 7 pav.

YSII valdytojų atitiktis techniniams reikalavimams 2023–2024 m. (šaltinis – NKSC)

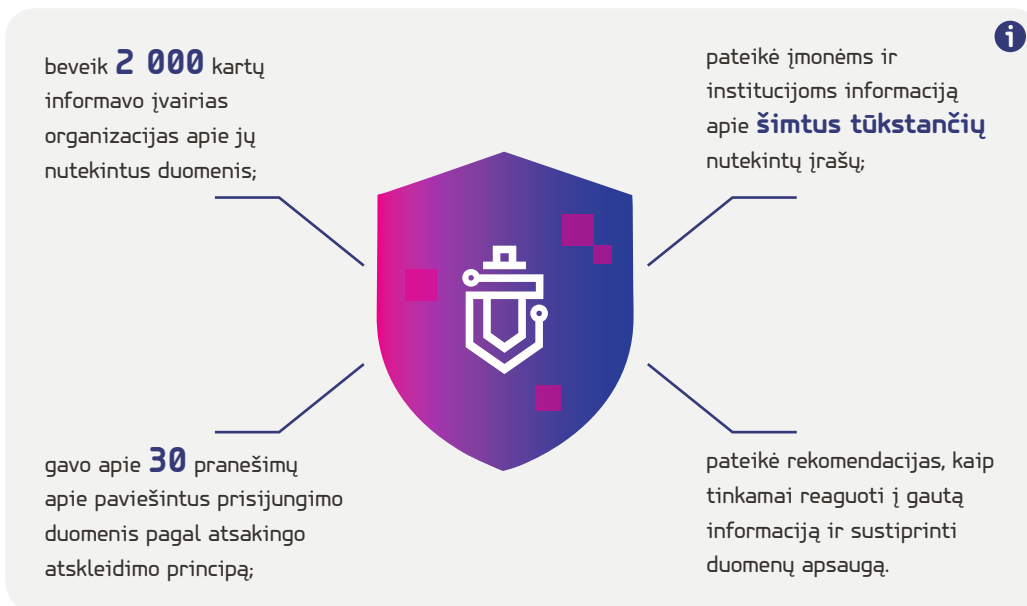
3 Kibernetinių incidentų prevencija ir kitos kibernetinį saugumą stiprinančios priemonės

Duomenų nutekimo prevencija

Didėjant duomenų nutekimo mastui, NKSC 2024 m. ėmėsi aktyvių veiksmų, siekdamas apsaugoti savo prižiūrimus subjektus. Pradėta sistemingai stebėti viešojoje erdvėje skelbiama informacija apie nutekintus duomenis, siekiant laiku identifikuoti grėsmes ir informuoti paveiktas organizacijas. Tai leidžia greičiau reaguoti į kibernetinius incidentus, mažinti žalą ir stiprinti bendrą šalies kibernetinį atsparumą.



2024 m. NKSC, vykdydamas aktyvią nutekintų duomenų paiešką, remdamasis partnerių ir atsakingo atskleidimo principu gauta informacija:



NKSC pažymi, kad prisijungimo duomenys dažniausiai nutekinami dėl:

- ⚠ socialinės inžinerijos atakų, kai vartotojai apgaule įtikinami pateikti savo duomenis;
- ⚠ kenkimo kodo (pvz. *Infostealer*¹¹), slapta renkančio duomenis iš vartotojų įrenginių;
- ⚠ trečiųjų šalių saugumo spragų, leidžiančių piktavaliams gauti prieigą prie jautrių duomenų.

Siekiant apsaugoti tinklus ir sistemas nuo galimo duomenų nutekimo, rekomenduojama:

- ⚙ naudoti daugiafunkcinį autentifikavimą;
- ⚙ reguliariai keisti slaptažodžius ir nenaudoti tų pačių slaptažodžių skirtingoms paskyroms;
- ⚙ nesaugoti slaptažodžių naršyklėse ar viešai prieinamuose įrenginiuose;
- ⚙ darbinį el. paštą naudoti tik darbo reikmėms, vengti asmeninių registracijų ar prenumeratų;
- ⚙ kontroliuoti nuotolinę prieigą ir ja naudotis tik iš patikimų, organizacijos prižiūrimų įrenginių;
- ⚙ organizuoti nuolatinį darbuotojų mokymus apie kibernetinio saugumo grėsmes ir saugaus elgesio principus.

11

Infostealer – tai kenkimo programinės įrangos (angl. *malware*) tipas vartotojų duomenims slapta rinkti ir perduoti kibernetiniams piktavaliams. Skirtingai nei kitų tipų kenkimo programinė įranga, *infostealer* dažniausiai neveikia destruktvyviai – ji skirta vertingai informacijai nepastebimai rinkti.

Kenkimo interneto svetainių užkardymas

Kovai su kibernetinėmis grėsmėmis, ypač su žaibiškais kibernetinėmis sukčiavimo atakomis, NKSC 2024 m. toliau tobulino organizacijų ir gyventojų apsaugai skirtą domenų blokavimo įrankį „Vasaris“¹². 2024 m. pabaigoje ši apsaugos priemonė buvo taikoma beveik 2,4 mln. mobiliojo ir 725 tūkst. fiksuoto interneto ryšio paslaugų vartotojų. Ji kasdien apsaugojo vidutiniškai apie 35 500 gyventojų, kurie, neatpažinę nusikaltėlių atsiųstos žinutės, bandė prisijungti prie svetainių, skirtų pinigams ar jautriems duomenims išvilioti. Iš viso per 2024 m. buvo apsaugota daugiau nei 3,5 mln. vartotojų.

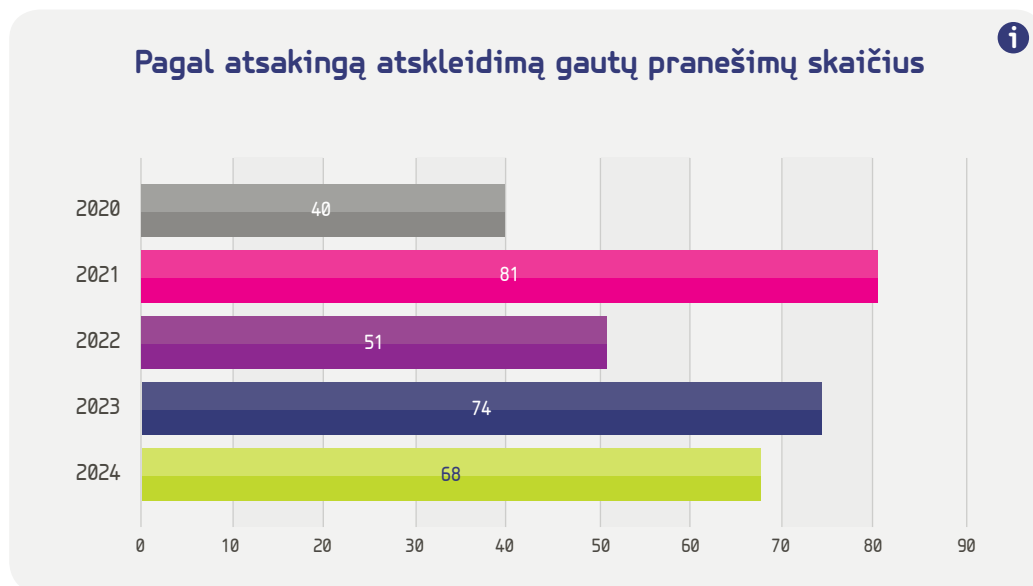
Šia blokuojamų domenų valdymo blokavimo sistema bendrai naudojasi 9 Lietuvos kompetentingos institucijos: Lietuvos bankas, Lošimų priežiūros tarnyba, PD, Lietuvos radijo ir televizijos komisija, Žurnalistų etikos inspektoriaus tarnyba (toliau – ŽEIT), Valstybinė vartotojų teisių apsaugos tarnyba, Narkotikų, tabako ir alkoholio kontrolės departamentas ir NKSC.

Lietuva yra viena iš nedaugelio Europos valstybių, efektyviai taikančių šią vartotojų apsaugos nuo kenksmingų interneto svetainių priemonę. 2025 m. NKSC sieks maksimaliai automatizuoti procesus, stiprinti tarpinstitucinį bendradarbiavimą ir dar geriau apsaugoti Lietuvos piliečius nuo žaibiškų sukčiavimo atakų bei kitų kibernetinių grėsmių.



Atsakingo atskleidimo principo įgyvendinimas

2024 m. NKSC gavo 68 pranešimus apie aptiktas spragas pagal atsakingą atskleidimą¹³ (2023 m. – 74 pranešimai) tiek privataus, tiek viešojo sektoriaus organizacijose (žr. 8 pav.). Tai leido laiku informuoti paveiktas organizacijas ir suteikti joms galimybę ištaisyti spragas dar prieš jomis pasinaudojant kibernetiniams piktavaliams.



< 8 pav.

Pagal atsakingą atskleidimą gautų pranešimų skaičius (2020–2024 m.) (šaltinis – NKSC)

Atsakingas atskleidimas ne tik padeda mažinti kibernetinių grėsmių poveikį, bet ir skatina organizacijas aktyviau taikyti prevencines priemones. Ši praktika stiprina pasitikėjimą tarp saugumo bendruomenės ir infrastruktūros valdytojų. Spragų užkardymas laiku ir informacinių sistemų apsauga parodo abipusę atsakingo atskleidimo naudą. NKSC dėkoja visiems pilietiškiems asmenims, kurie prisidėjo prie šalies kibernetinio saugumo stiprinimo, pranešdami apie spragas pagal atsakingo atskleidimo principą. Aktyvus visuomenės dalyvavimas šioje veikloje yra svarbus veiksnys užtikrinant kibernetinį atsparumą.

¹² Daugiau apie blokuojamų domenų valdymo sistemą „Vasaris“ galima rasti <https://www.nksc.lt/vasaris.html>.

¹³ Atsakingas spragų atskleidimas – kai informacija apie aptiktas spragas yra visų pirma pateikiama pačiai organizacijai, kurios informacinėse sistemose ar produktuose jos buvo aptiktos ir (ar) spragų atskleidimo procesą koordinuojančiai institucijai – NKSC.

NKSC parama užtikrinant rinkimų saugumą

NKSC 2024 m. aktyviai teikė paramą VRK pasirengimo rinkimams ir jų metu. 2024 m. birželio mėn., rinkimų į Europos Parlamentą metu, NKSC specialistams talkino ir kartu Lietuvos kibernetinės erdvės saugumu rūpinosi Europos kibernetinio greitojo reagavimo komandos (angl. *Cyber Rapid Response Team* (CRRT)) nariai. Į Lietuvą buvo atvykę 7 CRRT ekspertai iš 5 ES valstybių narių: Belgijos, Lenkijos, Kroatijos, Estijos ir Nyderlandų. Glaudžiai bendradarbiaudami su NKSC, ekspertai rinkimų laikotarpiu vykdė kibernetinių grėsmių paiešką, analizavo pažeidžiamas infrastruktūros vietas ir buvo pasirengę reaguoti į galimus kibernetinius incidentus.



Mokymai ir visuomenės švietimas

NKSC daug dėmesio skiria visuomenės švietimui kibernetinio saugumo temomis. 2024 m. NKSC sukūrė nemokamą nuotolinių mokymų platformą, skirtą tiek gyventojams, tiek organizacijoms. Per metus šioje platformoje įvairius kursus sėkmingai baigė daugiau nei 46 tūkst. asmenų.



Internetu patogiai pasiekiamų mokymų turinys pritaikytas skirtingoms visuomenės grupėms – darbuotojams, mokytojams, mokiniams ir kt. Iš 2024 m. pristatytų kursų paminėtini „Kibernetinė higiena namuose“, „Kibernetinis saugumas mokiniams“, „Kibernetinis saugumas mokytojams“ ir kt. Platforma pasiekama adresu <https://mokymai.nksc.lt>.

Siekdamas, kad ši iniciatyva taptų žinomesnė, 2024 m. spalį NKSC visoje Lietuvoje vykdė informacinę domėjimosi kibernetiniu saugumu skatinimo kampaniją.

Tarptautiniai mokymai ir partnerystės

Siekdamas glaudesnio tarptautinio bendradarbiavimo, NKSC įsitraukė ir į specializuotų mokymų organizavimą kartu su tarptautiniais partneriais. Vienas reikšmingiausių pavyzdžių – bendras kursas su JAV laivyno aukštąja mokykla (angl. *Naval Postgraduate School*). 2024 m. buvo surengtas kompiuterių tinklų kibernetinio saugumo kursas.



Kursą baigė beveik 40 specialistų iš Lietuvos ir Ukrainos kariuomenių, kritinės infrastruktūros ir akademinio sektoriaus. Šie mokymai ne tik suteikė dalyviams naujų žinių ir įgūdžių, bet ir sustiprino jų gebėjimus apsaugoti kritinę infrastruktūrą nuo kibernetinių grėsmių.

Teorinių žinių patikrinimas NKSC organizuotose pratybose

Sudėtingėjant ir intensyvėjant kibernetinėms grėsmėms, praktinis organizacijų pasirengimas atremti incidentus tampa kritiškai svarbus. Atsižvelgdamas į tai, NKSC 2024 m. toliau tobulino pratybų scenarijus ir vykdymo metodus, kurie leido viešojo sektoriaus ir ypatingos svarbos infrastruktūros valdytojams patikrinti savo darbuotojų atsparumą socialinės inžinerijos atakoms ir pačios organizacijos gebėjimus identifikuoti, valdyti ir komunikuoti apie kibernetinius incidentus.



Pratybos „Kibernetinis skydas phishex 2024“. Pratybos buvo skirtos viešojo sektoriaus ir ypatingos svarbos infrastruktūros objektuose dirbančių asmenų atsparumui socialinės inžinerijos principais grįstoms atakoms ugdyti. Per metus iš viso išsiųsta 280 tūkst. imitacinių el. laiškų, juose atkartotos dažniausiai pasitaikančios programišių taktikos. Pratybos buvo vykdomos 3 kartus per metus, kiekvieną kartą papildant naujais scenarijais.

Pratybos „Kibernetinis skydas OpEx 2024“. Didžiausios nacionalinės kibernetinio saugumo pratybos. 2024 m. pirmą kartą šios pratybos buvo vykdomos gyvai virtualiame kibernetinių pratybų poligone. Dalyvavusios organizacijos susidūrė su realiomis kibernetinėmis atakomis, jas reikėjo identifikuoti ir neutralizuoti realiu laiku. Iš viso pratybose dalyvavo 75 organizacijos, iš kurių 39 taip pat tobulino viešosios komunikacijos įgūdžius, mokydamosi efektyviai informuoti visuomenę apie incidentus.

NKSC dalyvavimas tarptautinėse pratybose

2024 m. NKSC atstovai aktyviai dalyvavo tarptautinėse kibernetinio saugumo pratybose, siekdami ugdyti savo kompetencijas, tobulinti reagavimo į incidentus gebėjimus ir stiprinti bendradarbiavimą su sąjungininkais.



NATO pratybos „Suremti skydai 2024“ (angl. *Locked Shields 2024*). NKSC kartu su KAM, Lietuvos kariuomenės, Lietuvos šaulių sąjungos, verslo ir akademinės bendruomenės atstovais sudarė bendrą ekspertų komandą (angl. *Blue Team*) ir dalyvavo didžiausiose pasaulyje kibernetinės gynybos pratybose. Tai leido keistis patirtimi, didinti sąveikumą ir tobulinti praktinius įgūdžius ginti nacionalines informacines sistemas ir kritinę infrastruktūrą nuo realiu laiku vykdomų kibernetinių atakų.

JAV pratybos „Kibernetinis skydas“ (angl. *Cyber Shield*). Šios pratybos, organizuojamos JAV Gynybos departamento, yra vienos svarbiausių pasaulyje. Lietuvos dalyvavimas jose tapo įmanomas dėl glaudaus bendradarbiavimo su Pensilvanijos nacionaline gvardija. Pratybose Lietuvos atstovai treniravosi įvairiose srityse, įskaitant grėsmių paiešką, kritinės infrastruktūros apsaugą ir kibernetinę žvalgybą. Tai sustiprino Lietuvos kibernetinės gynybos pajėgumus ir padėjo stiprinti integraciją į tarptautinius kibernetinio saugumo tinklus.

Lietuvos kariuomenės pratybos „Gintarinė migla 2024“ (angl. *Amber Mist*). 2024 m. šiose pratybose dalyvavo daugiau nei 300 kibernetinio saugumo specialistų iš įvairių pasaulio šalių – Belgijos, Japonijos, JAV, Lenkijos, Ukrainos ir Vokietijos. NKSC grėsmių paieškos ir analizės komandos kartu ir Mil-CERT atstovais pratybose testavo ir tobulino bendro atsako į kibernetines grėsmes strategijas, skirdami ypač daug dėmesio operaciniam bendradarbiavimui tarp sąjungininkų.

NATO pratybos „Purpurinis gynėjas 2024“ (angl. *Guardian Purple 2024*). Šiose operatyviam reagavimui į kibernetines atakas skirtose pratybose NKSC ekspertai stiprino savo žinias gynybinėse (angl. *Blue Team*), puolamosiose (angl. *Red Team*) komandose, siekdami praktiškai išbandyti ir apsaugos, ir įsilaužimo metodus. Pratybose įgyti įgūdžiai leidžia geriau suprasti realias kibernetinių atakų grėsmes ir efektyviau jas neutralizuoti.

Tarptautinis bendradarbiavimas

2024 m. NKSC ir toliau bendradarbiavo su pagrindiniais užsienio partneriais – JAV, Lenkija, Ukraina ir Sakartvelu. Dirbdami NKSC tarptautiniame kibernetinių grėsmių analizės padalinyje, šių valstybių atstovai kartu su NKSC specialistais analizavo regionines grėsmes. Padalinys, be periodinių grėsmių analizių, 2024 m. parengė ir specializuotą studiją, skirtą kibernetinėms grėsmėms prieš kritinę infrastruktūrą Baltijos jūros regione, apžvalgą¹⁴. Analizę atlikusių specialistų teigimu, priešiška nusiteikusių šalių veiksmai dažnėja, todėl būtinas didesnis regiono šalių įsitraukimas stiprinant kibernetinę gynybą.



NKSC telkė vis daugiau tarptautinių partnerių. 2024 m. rugsėjį buvo pasirašytas bendradarbiavimo susitarimas tarp NKSC ir Čekijos nacionalinio kibernetinio saugumo biuro (angl. *National Cyber and Information Security Agency* (NUKIB)). Čekijos prisijungimas stiprins Lietuvos kibernetinių grėsmių analizę, skatins specialistų bendradarbiavimą ir tobulins grėsmių atpažinimo sistemą.

NKSC ES projektinės veiklos

Nuo 2024 m. sausio 1 d. pradėtas įgyvendinti NKSC 2021–2027 m. Skaitmeninės Europos programos lėšomis finansuojamas „Kibernetinio saugumo bendruomenės kompetencijų stiprinimo“ projektas (projektas „CyberUP“). Projektas skirtas Lietuvos kibernetinio saugumo bendruomenei sukurti ir Nacionalinio koordinavimo centrui įveikinti.



NKSC kartu su VŠĮ Centrine projektų valdymo agentūra ir KAM išplatino kvietimą mažoms ir vidutinėms įmonėms pasinaudoti ES finansavimo galimybėmis ir teikti paraiškas, kad galėtų sustiprinti kibernetinį atsparumą ir kurti kibernetinio saugumo ugdymo turinį, skirtą neformaliajam švietimui. Į kvietimą atsiliepė daugiau nei 80 įmonių, o po vertinimo pasirašyta beveik 30 sutarčių, jų įgyvendinimas truks 9 mėn.

Inovacijų ir mokslo skatinimas yra viena iš projekto „CyberUP“ užduočių, todėl kartu su Latvijos ir Estijos nacionaliniais koordinavimo centrais buvo suorganizuotas pirmasis Baltijos šalių kibernetinio saugumo inovacijų forumas „CyberBazaar“ Rygoje, į renginį atvyko apie 650 dalyvių. Taip pat kartu su Estijos nacionalinio koordinavimo centru buvo suorganizuotas Lietuvos mergaičių komandos išvykimas į tarptautinę vasaros stovyklą „CyberWizards 2024“.

Siekdamas telkti kibernetinio saugumo bendruomenę, NKSC pradėjo organizuoti periodinius renginius „NKSC kibernetinio saugumo pusryčiai“, kurie buvo transliuojami ir socialinėje platformoje „YouTube“. Juose buvo išsamiai pristatomos atnaujinto Kibernetinio saugumo įstatymo nuostatos, diskutuojama kibernetinei bendruomenei aktualiomis temomis. 2024 m. iš viso suorganizuoti 4 tokie renginiai, juose dalyvavo daugiau nei 280 asmenų.

Projektas „Cyber Campus LT“ – tai nauja kibernetinio saugumo bendruomenės koncepcija, pristatyta programos „Kurk Lietuvai“ projekto „Kibernetinio saugumo bendruomenės būrimas: *Cyber Campus LT* koncepcija“¹⁵ (toliau – „Cyber Campus LT“) metu. Ši iniciatyva skirta kibernetinio saugumo specialistams iš verslo, viešojo sektoriaus ir akademinės bendruomenės suburti, siekiant stiprinti Lietuvos kibernetinį atsparumą. Tikimasi, kad „Cyber Campus LT“ ne tik skatins inovacijas ir mokymąsi, bet ir sudarys sąlygas glaudžiau bendradarbiauti įvairių sričių profesionalams.

Vienas pagrindinių projekto tikslų – sukurti erdvę, kurioje būtų identifikuojamos ir sprendžiamos aktualiausios kibernetinio saugumo problemos. Tam būtų įsteigtos specializuotos darbo grupės švietimo, inovacijų, tarptautinio bendradarbiavimo ir gynybos reikalams. Toks modelis leistų efektyviau pasirengti galimoms kibernetinėms grėsmėms tiek taikos, tiek krizės metu.

NKSC 2025 m. prioritetai:



pagalba ir parama vystant viešojo administravimo sektoriaus taktinius kibernetinės gynybos pajėgumus;



įvairių grupių kibernetinio saugumo kompetencijų ugdymo plėtra;



pasirengimas vykdyti organizacijų atitikties vertinimą pagal atnaujinto Kibernetinio saugumo įstatymo ir jo poįstatyminių teisės aktų reikalavimus, atitikties vertinimo ir audito metodikos trečiosioms šalims sukūrimas;



tarpinstitucinio bendradarbiavimo stiprinimo sprendimų paieška.

14

Kibernetinės grėsmės ypatingos svarbos infrastruktūrai Baltijos jūros regione (angl. *Cyber Threats to Critical Infrastructure in the Baltic Sea Region*). Prieiga per internetą https://www.nksc.lt/doc/rkgc/2024_Cyber_Threats_to_Critical_Infrastructure_in_the_Baltic_Sea_region.pdf.

15

Projektas „Kibernetinio saugumo bendruomenės būrimas: *Cyber Campus LT* koncepcija“ atliktas 2023–2024 m. NKSC. Prieiga per internetą https://data.kurk.lt/wp-content/uploads/2024/03/2024-09-05-Cyber-Campus-koncepcija_FINAL.pdf.

Elektroninių ryšių tinklų vientisumo ir vartotojų apsaugos užtikrinimas, draudžiamos viešai skleisti informacijos internete užkardymas

Vadovės žodis



Jūratė Šovienė,

RRT tarybos pirmininkė

2024-ieji buvo intensyvūs metai elektroninių ryšių rinkoje. RRT, nuosekliai stiprindama interneto ryšio tinklų atsparumą ir užtikrindama vartotojų saugumą, sprendė kibernetines problemas. Reaguodami į išorės grėsmes, dalyvavome tiriant kabelio nutraukimo incidentą Baltijos jūroje, nagrinėjome GPS signalų trikdžius ir neteisėtas radijo transliacijas iš Rusijos.

Vartotojų apsauga – vienas svarbiausių mūsų prioritetų. Kovą su elektroniniu sukčiavimu tęsiame glaudžiai bendradarbiaudami su atsakingomis institucijomis ir nuolat atnaujindami taikomas priemones.

Daug dėmesio skiriame skaitmeniniam raštingumui stiprinti. Prie projekto „Nė vienas nėra pamirštas“, skirto senjorų skaitmeninei atskirčiai mažinti, jau prisijungė daugiau kaip 150 organizacijų.



KAŲ SAUGO?

- ✓ Viešųjų elektroninių ryšių paslaugų vartotojų teisę į nepertraukiamą paslaugų teikimą.
- ✓ Radijo ryšio vartotojų galimybes naudotis kokybišku radijo ryšiu be trukdžių, mobiliojo ryšio operatorių tinklų, televizijos transliacijų, radijo ryšio navigacijos ir kitų sistemų saugų ir patikimą veikimą.
- ✓ Vaikų, nepilnamečių ir kitų asmenų teisę į šviesią ir saugią skaitmeninę erdvę.



NUO KO SAUGO?

- ✓ Nuo vientisumo pažeidimų, pavyzdžiui, nuo elektros energijos tiekimo sutrikimų, kabelių nutraukimo, tinklo įrangos gedimų ir pan.
- ✓ Nuo žalingų radijo trukdžių, trikdančių radijo ir navigacinius ryšius, televizijos ir radijo transliacijas, radijo ryšio sistemų veikimą.
- ✓ Nuo draudžiamos skleisti ar neigiamą poveikį nepilnamečiams darančios informacijos internete – nuo vaikų seksualinio išnaudojimo medžiagos, pornografijos, rasinės ir tautinės nesantaikos kurstyimo, smurto, patyčių, narkotikų ir kt.



KAIP SAUGO?

- ✓ Užtikrindama, kad viešųjų ryšių tinklų teikėjai įgyvendintų tinkamas technines ir organizacines priemones vientisumui užtikrinti.
- ✓ Vykdydama radijo spektro stebėseną ir identifikudama neteisėtus dažnių naudojimo atvejus bei juos šalindama.
- ✓ Vykdydama interneto karštosios linijos „Švarus internetas“ veiklą ir užtikrindama, kad draudžiama skleisti informacija būtų pašalinta arba būtų atitinkamai pažymėta ir apribota.
- ✓ Aprobudama turinio filtravimo priemones mokyklose ir bibliotekose.
- ✓ Edukuodama gyventojus skaitmeninio turinio klausimais.





Svarbiausi 2024 m. įvykiai ir tendencijos



Iš 4 paslaugų teikėjų gauti 6 pranešimai apie įvykusius viešųjų ryšių tinklų vientisumo pažeidimus. Užfiksuotas 31 įvairaus masto ir pobūdžio paslaugų sutrikimas iš 5 paslaugų teikėjų.



Pagrindinės viešųjų ryšių tinklų vientisumo pažeidimų priežastys – elektros energijos tiekimo sutrikimai, duomenų kabelių pažeidimai, tinklo įrangos gedimai ir valdymo sistemų sutrikimai.



Užfiksuoti 3 neteisėtų radijo stočių iš Rusijos teritorijos veikimo atvejai skirtingose Lietuvos pasienio vietovėse, taip pat nustatyti GPS sutrikimus sukeltantys ryšio slopintuvai Rusijos ir Baltarusijos teritorijose, stebėti GPS klastojimo atvejai.



Patvirtintas Apsimestinių trumpųjų žinučių identifikavimo tvarkos aprašas ir blokuota per 3,2 mln. apsimestinių SMS.



Operatoriai, vadovaudamiesi RRT priimtais teisės aktais, blokavo per 8,5 mln. apgaulingų skambučių iš užsienio.



Interneto karštąja linija gauti 2 177 pranešimai apie internete rastą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją. 68 proc. gautų pranešimų pasitvirtino.



RRT tyrėjai, dalyvaudami tarptautiniame projekte „Arachnid“, įvertino 54 840 potencialiai draudžiamo turinio vaizdų.



RRT vykdė švietėjišką veiklą: vedė mokiniams pamokas apie saugų elgesį internete, organizavo paskaitas ir praktinius skaitmeninių įgūdžių tobulinimo mokymus senjorams.



RRT pradėjo vykdyti skaitmeninių paslaugų koordinatoriaus funkcijas pagal ES Skaitmeninių paslaugų akto reikalavimus.



1 Viešųjų ryšių tinklų vientisumo užtikrinimas Lietuvoje

Svarbiausia 2024 m. RRT gautų pranešimų apie įvykusius viešųjų ryšių tinklų vientisumo pažeidimus priežastis - elektros tiekimo sutrikimas dėl liepos 28-29 d. visoje Lietuvoje siautusios audros. Šios audros padariniai buvo itin stipriai jaučiami Vilniaus regione - nuo visiško paslaugų nebuvimo keletą parų iki nežymaus sutrikimo (sulėtėjusios mobiliojo interneto greیتaveikos). Visoje Lietuvoje paveiktų vartotojų skaičius siekė beveik 350 000. Pažymėtina, kad paveiktų viešųjų ryšių tinklų vartotojų skaičius tolydžio mažėjo, o tinklų funkcionalumas buvo visiškai atkurtas per 4 dienas.

2024 m. RRT fiksavo ir 25 mažesnio masto viešųjų ryšių tinklų vientisumo pažeidimus, apie juos paslaugų teikėjai informavo teikdami ketvirčio ataskaitas. Pagrindinės šių gedimų priežastys: tinklo įrangos gedimai, duomenų kabelių nutraukimai, elektros tiekimo sutrikimai, konfigūracijų klaidos. Pagrindinės viešųjų ryšių tinklų vientisumo pažeidimų priežastys ir palyginimas su ankstesniais metais pateiktas lentelėje⁰¹ (žr. 1 pav.).

▼ 1 pav.

Pagrindinės viešųjų ryšių tinklų vientisumo pažeidimų priežastys (šaltinis – RRT).

VIEŠŪJŲ RYŠIŲ TINKLŲ VIENTISUMO PAŽEIDIMŲ PRIEŽASTYS	2022 m.		2023 m.		2024 m.	
	Pranešimų apie pažeidimus skaičius	Galutinių paslaugų gavėjų, kuriems turėjo įtakos vientisumo pažeidimai, skaičius	Pranešimų apie pažeidimus skaičius	Galutinių paslaugų gavėjų, kuriems turėjo įtakos vientisumo pažeidimai, skaičius	Pranešimų apie pažeidimus skaičius	Galutinių paslaugų gavėjų, kuriems turėjo įtakos vientisumo pažeidimai, skaičius
Elektros energijos tiekimo sutrikimai	2	32 946	2	28 000	4	433 601
Kabelio nutraukimas, remontas	-	-	1	381	1	5 233
Tarptinklinio ryšio paslaugų sutrikimai	-	-	-	-	-	-
Tinklo įrangos gedimai	3	1 000 000 <*	11	1 000 000 <*	-	-
Kita	2	40 000	3	100 000 <*	1	1000 000 <*
Iš viso	7		17		6	

01

Mažesnio masto pažeidimai, fiksuoti paslaugų teikėjų periodinėse ataskaitose, šioje lentelėje nepateikiami.

2024 m. lapkričio mėn. fiksuotas incidentas Baltijos jūroje, kai buvo nutrauktas jūrinis elektroninių ryšių kabelis, jungiantis Lietuvą su Švedija. Nors Lietuvos elektroninių ryšių tinklų operatoriai informavo, kad dėl šio incidento nenutrūko elektroninių ryšių paslaugų teikimas ir nepablogėjo kokybė, tarptautinio ryšio srautai buvo operatyviai subalansuoti kitomis jungtimis. RRT, atsižvelgdama į faktą, kad tarptautinio ryšio sutrikimas gali pabloginti Lietuvos Respublikos tarptautinį junglumą, kreipėsi į prokuratūrą, buvo pradėtas ikiteisminis tyrimas.

RRT, įvertinusi 2024 m. buvusių viešųjų ryšių tinklų vientisumo pažeidimus, jų priežastis ir mastą, atsižvelgdama į sutrikimų tendencijas, visuomenės įpročių pokyčius ir didėjančią elektroninių ryšių svarbą, skubiai inicijavo Viešųjų elektroninių ryšių paslaugų nepertraukiamo teikimo užtikrinimo taisyklių (toliau – taisyklės) projekto parengimą⁰² ir sugriežtino paslaugų teikėjams taikomus reikalavimus. Atsižvelgdami į numatomus taisyklių pokyčius, paslaugų teikėjai, įvykus elektros tiekimo sutrikimui, būtų įpareigoti užtikrinti paslaugų teikimą 24 valandas.

2 Radijo ryšio užtikrinimas ir atsparumas

RRT fiksavo 3 radijo stočius, veikiančius FM bangų ruože ir lokalizuotų Rusijos Federacijos Karaliaučiaus srityje, nesukoordinuotų⁰³ su Lietuvos Respublikos ryšių administracija, veikimą skirtingose Lietuvos pasienio vietovėse: 2023 m. nustatytas neteisėtas spinduliuotės šaltinis, veikiantis 87,9 MHz radijo dažniu (programos „Sputnik“ transliacija Klaipėdos regione), 2024 m. – 2 naujos veikiančios stotys. Nepaisant RRT pranešimų dėl interferencijos, siųstų ir ITU Radijo ryšio biurui, Rusijos Federacijos administracija tokios veiklos nenutraukė. 2023 m. RRT įgyvendino radijo programos 87,9 MHz radijo dažniu priėmimą Klaipėdos teritorijoje ir Nidos apylinkėse sunkinančias priemones, siekdama apriboti neteisėtos radijo programos transliavimą iš Karaliaučiaus srities, bet nesukelti žalingo poveikio radijo stočių veiklai tais pačiais ir gretimais radijo dažniais.

2024 m. Lietuvoje buvo fiksuojami GPS sutrikimai, darantys neigiamą poveikį orlaiviams. Nors skrydžių metu naudojama GPS nėra kritiškai svarbi saugumui užtikrinti, tačiau padaugėjus tokių trukdžių atvejų RRT, siekdama, kad incidentai būtų fiksuojami kuo operatyviau ir tiksliai nustatomas jų mastas ir periodiškumas, įdiegė orlaivių stebėsenos sistemą.

RRT nustatė GPS sutrikimus sukeliančius 2 ryšio slopintuvus Rusijos Federacijos Karaliaučiaus srityje ir 1 slopintuvą Baltarusijos teritorijoje. Taip pat RRT fiksavo ir GPS klastojimo (angl. *spoofing*) atvejų, kai buvo siekiama suklaidinti GPS imtuvą ir sutrikdyti GPS tinklo veikimą. Reaguodama į trukdžius, RRT kreipėsi į ITU dėl orlaivių navigacijos sistemų trukdžių iš Rusijos ir Baltarusijos teritorijų, taip pat išsiuntė raštus Baltarusijos ir Rusijos ryšių administracijoms, bendradarbiavo su atsakingomis Lietuvos institucijomis. Su didėjančių orlaivių GPS trukdžių atvejų skaičiumi susiduria ne tik Lietuva, bet ir kitos Baltijos jūros bei Europos šalys, todėl siekiant valstybių veiksmų koordinavimo ir bendrų efektyvių sprendimų šis klausimas nagrinėjamas atitinkamose EK darbo grupėse. Tuo tikslu RRT įsitraukė į EK Pasaulinės palydovinės navigacijos sistemos (angl. *Global Navigation Satellite System* (GNSS)) trukdžių darbo grupės veiklą.

02

Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos nutarimo „Dėl Lietuvos Respublikos elektroninių ryšių įstatymo 51 straipsnio 2 ir 4 dalių nuostatų įgyvendinimo“ projektas. Prieiga per internetą <https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/932503b0a00211ef9db2c9aaf9c67042?positionInSearchResults=0&searchModelUUID=9c9a21ef-2379-41f6-abe9-be50b4be09bc>.

03

Rusijos ryšių administracija nėra gavusi Lietuvos ryšių administracijos (t. y. RRT) sutikimo radijo dažnių priskyrimams pagal ITU pirmojo ir trečiojo regiono šalių susitarimą dėl 87,5–108 MHz radijo dažnių juostos naudojimo FM garso transliavimo sistemose (Ženeva, 1984 m.) ir šio susitarimo radijo dažnių plano. Be sutikimo dažnio naudojimas pagal ITU įstatus ir ITU radijo ryšio reglamentą laikomas neteisėtu.

Kadangi grėsmių ryšio infrastruktūrai ir ryšio sistemų veiklai nemažėja, ryšio atsparumą ir patikimumą galima sustiprinti numatant alternatyvias ryšio sistemas, pavyzdžiui, palydovinį ryšį. ES vystomo palydovinio ryšio projekto IRIS² tikslas – sukurti pažangią palydovinio ryšio infrastruktūrą, kuri užtikrintų saugų ir patikimą junglumą visoje Europoje ir leistų tapti nepriklausomais nuo komercinių tinklų paslaugų teikėjais iš ne ES narių. RRT pagal savo kompetenciją aktyviai dalyvauja IRIS² techninėje ir vartotojų darbo grupės veikloje, teikia pasiūlymus planuojant IRIS² ryšio komponentų struktūrą ir standartus. RRT vertinimu, šis projektas dabartinių geopolitinių išbandymų metais yra vertas didesnio atsakingų Lietuvos institucijų įsitraukimo.

RRT siekia sudaryti palankias sąlygas Lietuvoje išbandyti tradicinio antžeminio mobiliojo ryšio ir naujos kartos palydovinio ryšio tinklų hibridinį veikimą. 2024 birželio mėn. Vilniuje vykusiam tarptautiniame renginyje „EuroDIG“ RRT organizavo sesiją „Ateities ryšys: kas tas naujas žaidėjas?“ Sesijoje buvo pristatytos naujos technologijos, pavyzdžiui, sparčiai vystoma palydovinio ryšio technologija tiesioginiam ryšiui su įrenginiu palaikyti (angl. *direct to device*), ir hibridiniai palydovų ir antžeminių tinklų modeliai ryšio prieinamumui atokiose vietovėse ir atsparumui krizėms pagerinti. Renginyje inovatyvius sprendimus pristatė pranešėjai iš Pasaulinės palydovinio ryšio operatorių asociacijos, Europos kosmoso agentūros, tarptautinių palydovinio ryšio kompanijų SES, „SpaceX“, „Amazon“ ir kitų organizacijų.

3 Vartotojų apsauga nuo žalingų interneto nuorodų, apsimestinių trumpųjų žinučių ir skambučių

2024 m. RRT ir toliau vykdė sukčiavimo kibernetinėje erdvėje prevenciją. Patvirtinus Apsimestinių trumpųjų žinučių identifikavimo tvarkos aprašą⁰⁴, viešųjų elektroninių ryšių paslaugų teikėjai buvo įpareigoti iš viso SMS srauto identifikuoti žinutes su internetinėmis nuorodomis ir nustačius, kad jos įtrauktos į NKSC žalingų interneto resursų sąrašus, blokuoti tokių SMS žinučių siuntimą vartotojams. Iš viso blokuota per 3 mln. tokio tipo SMS žinučių, potencialiai kėlusią grėsmę, kad vartotojai atidarys netikrus interneto puslapius ir bus išvilioti jų asmens duomenys ar kita jautri informacija. Operatoriai taip pat buvo įpareigoti sudaryti sąlygas turinio siuntėjams⁰⁵ suderinti siunčiamų vardinių SMS žinučių identifikacinius požymius. Taikant šią priemonę, 2024 m. buvo blokuota 206 tūkst. SMS žinučių su suklustotais siuntėjų vardais, o įskaitant žinutes su žalingomis nuorodomis iš viso blokuota per 3,2 mln. SMS. Operatoriai, vykdydami RRT nustatytus reikalavimus, iš viso 2024 m. blokavo per 8,5 mln. apgaulingų skambučių iš užsienio.

2024 m. RRT sukčiavimo kibernetinėje erdvėje prevencijos ir užkardymo srityje glaudžiai bendradarbiavo su Lietuvos paštu, Lietuvos banku, Lietuvos kriminalinės policijos biuru, NKSC, Pinigų plovimo prevencijos kompetencijų centru, VMI, operatoriais. Sukčiavimo kibernetinėje erdvėje užkardymo klausimais buvo suorganizuoti 2 renginiai: balandžio 15 d. – apvaliojo stalo diskusija, spalio 24 d. – kibernetinio saugumo konferencija⁰⁶. Renginiuose aptartos sukčiavimą kibernetinėje erdvėje užkardančios priemonės bus įtrauktos į 2025 m. RRT rengiamus teisės aktų pakeitimų projektus.

Bendradarbiaudama su mobiliojo ryšio operatoriais, RRT nustatė geografines vietas, vadinamuosius SIM spiečius, kuriuose galimai nusikalstamai veikai vykdyti gali būti naudojamas didelis kiekis SIM kortelių. Surinkta informacija perduota Lietuvos policijai dėl galimai neteisėtų veiksmų tyrimo ir užkardymo.

04

Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos 2024 m. sausio 25 d. nutarimas Nr. TN-64 „Dėl Apsimestinių trumpųjų žinučių identifikavimo tvarkos aprašo patvirtinimo“. Prieiga per internetą <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/82399520bbc411ee9269b566387cfcb?jfwid=-136q3l51to>.

05

Komunalinių, finansinių ir draudimo, pašto, el. ryšių ir kitų paslaugų teikėjams.

06

Konferencijos pranešimų skaidres galima rasti <https://www.rrt.lt/pranesimu-skaidres/2024-m/>.

4 Elektroninės atpažinties priemonių saugumo užtikrinimo lygio vertinimas

RRT nuo 2024 m. buvo paskirta kvalifikuotos elektroninės atpažinties paslaugos teikėjų priežiūros įstaiga ir atlikdama naują pareigą pradėjo vertinti ir tvirtinti elektroninės atpažinties paslaugos teikėjų išduodamų elektroninės atpažinties priemonių saugumo užtikrinimo lygį. Priklausomai nuo elektroninės atpažinties priemonės išdavimo procedūrų, techninių ir saugumo aspektų, elektroninės atpažinties priemonei pagal ES teisinį reguliavimą gali būti priskirtas tam tikras saugumo užtikrinimo lygis: žemas, pakankamas arba aukštas. Aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonės bus visiškai patikimos ir turintys tokią priemonę fiziniai asmenys galės gauti ypač svarbias viešąsias ir (arba) administracines paslaugas, pavyzdžiui, naudotis europinės skaitmeninės tapatybės dėklės „eWallet“ aplikacija. 2024 m. įvertintos 3 elektroninės atpažinties priemonės ir joms priskirtas saugumo užtikrinimo lygis: valstybės įmonės Registrų centras išduodamai elektroninės atpažinties priemonei LT ID priskirtas pakankamas saugumo užtikrinimo lygis, o „SK ID Solutions AS“ Lietuvos filialo išduodamoms elektroninės atpažinties priemonėms „Mobile-ID“ ir „Smart-ID“ - aukštas saugumo užtikrinimo lygis. Elektroninės atpažinties paslaugos teikėjai siekia, kad jų išduodamos elektroninės atpažinties priemonės būtų patikimos ir saugios. RRT 2024 m. aktyviai teikė konsultacijas elektroninės atpažinties paslaugos teikėjams dėl galimybės priskirti saugumo užtikrinimo lygį jų išduodamoms elektroninės atpažinties priemonėms. Tikėtina, kad kvalifikuotos elektroninės atpažinties paslaugos teikėjų skaičius ateityje didės, o elektroninės atpažinties paslaugos vartotojai gaus kokybiškas paslaugas.

5 Skaitmeninių paslaugų priežiūra

2024 m. RRT pradėjo vykdyti skaitmeninių paslaugų koordinatoriaus funkcijas pagal Skaitmeninių paslaugų akto⁰⁷ reikalavimus: koordinavo atsakingų institucijų veiksmus dėl dezinformacijos, politinės reklamos skaidrumo interneto erdvėje bei neigiamo poveikio demokratiniais procesams ir pilietiniam diskursui užkardymo Seimo rinkimų laikotarpiu.

2024 m. rugsėjo 18 d. RRT surengė apvaliojo stalo diskusiją su VRK ir EK atstovais. Susitikime dalyvavo NKVC, ŽEIT, Lietuvos radijo ir televizijos komisijos bei Užsienio reikalų ministerijos, didžiųjų interneto platformų ir interneto paieškos sistemų „Google“, „X“, „Meta“, „TikTok“ ir „YouTube“ ekspertai. Socialinių tinklų atstovai pristatė EK gairių įgyvendinimo priemones ir pasidalijo informacija apie su rinkimais susijusius dezinformacijos ir žalingo turinio incidentų eskalavimo kanalus. Buvo aptarti įvykę incidentai ir jų priežastys.

2024 m. spalio 2 d. su VRK ir EK suorganizuotas susitikimas su nevyriausybinėmis organizacijomis („Debunk EU“, pilietinio atsparumo iniciatyva „Baltosios pirštinės“) atstovais, veikiančiais rinkimų ir žalingo turinio užkardymo srityje. Jame dalyvavo didžiųjų interneto platformų ir interneto paieškos sistemų atstovai. Susitikime pristatyti efektyvūs žalingo turinio pranešimų būdai ir bendradarbiavimo su nevyriausybinėmis organizacijomis gerieji pavyzdžiai kitose ES šalyse.

Seimo rinkimų laikotarpiu fiksuotas tik vienas incidentas, susijęs su autorinių teisių pažeidimu „YouTube“ platformoje. Šis incidentas buvo operatyviai išspręstas.

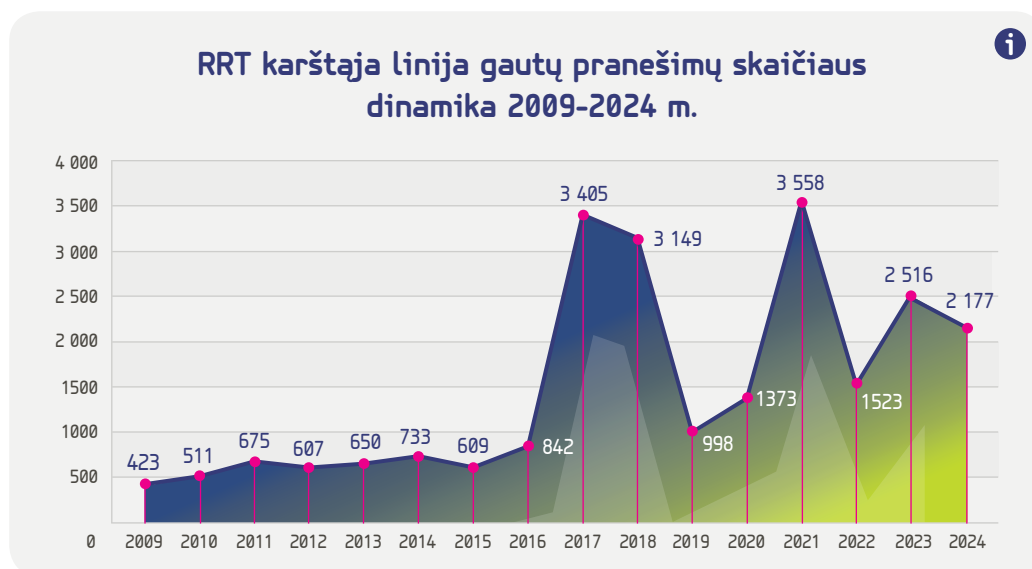
07

2022 m. spalio 19 d. Europos Parlamento ir Tarybos Reglamentas (ES) 2022/2065 dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB (Skaitmeninių paslaugų aktas). Prieiga per internetą <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32022R2065>.

6 Interneto karštosios linijos „Švarus internetas“ veikla ir žalingo turinio internete užkardymas

RRT siekia, kad interneto vartotojai, ypač vaikai ir nepilnamečiai, būtų apsaugoti nuo žalingo turinio. RRT administruojama interneto karštąja linija „Švarus internetas“ (<https://www.svarusinternetas.lt/>) visi interneto vartotojai gali pranešti apie rastą internete draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją, t. y. viešas patyčias kibernetinėje erdvėje panaudojus vaizdinę informaciją, pornografinio turinio informaciją (įskaitant informaciją, kurioje vaizduojamas vaikų seksualinis išnaudojimas (pedofilija)), informaciją, kuria tyčiojamosi, niekinama, skatinama neapykanta ar kurstoma diskriminacija ir kt. RRT nuo 2008 m. yra tarptautinės interneto karštųjų linijų asociacijos INHOPE narė.

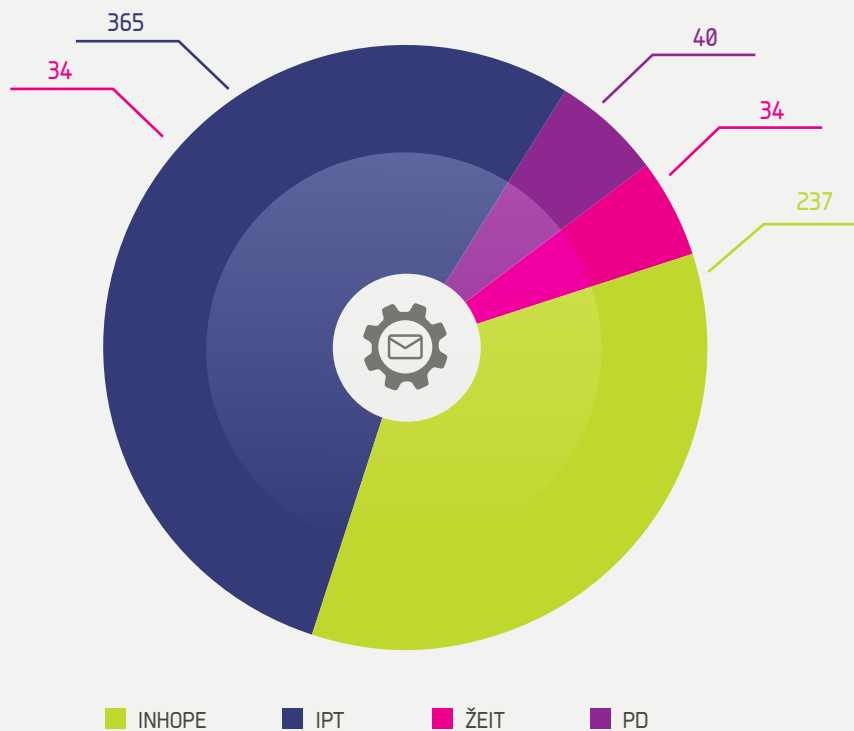
2024 m. RRT interneto karštąja linija „Švarus internetas“ gautų pranešimų (2 177) apie internete rastą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją, palyginti su 2023 m., skaičius sumažėjo 13 proc. (žr. 2 pav.).



< 2 pav. RRT karštąja linija gautų pranešimų dinamika 2009–2024 m. (šaltinis – RRT)

Pasitvirtinusių pranešimų (angl. *actionable reports*), t. y. pranešimų apie draudžiamą ir neigiamą poveikį nepilnamečiams darančią informaciją, dėl kurios pašalinimo galima imtis veiksmų, buvo 1 488 (tai sudaro 68 proc. visų gautų pranešimų) (2023 m. tokių pasitvirtinusių pranešimų buvo 1 475). RRT atlikti veiksmai su pasitvirtinusiaisiais pranešimais, gautais karštąja linija (žr. 3 pav.):

Veiksmai, atlikti su pranešimais



- 237** pranešimai apie vaikų seksualinio išnaudojimo vaizdus persiųsti kitoms šalims, tarptautinės interneto karštųjų linijų asociacijos INHOPE narėms.
- 365** pranešimai persiųsti įvairių šalių IPT, svetainių savininkams, socialinių tinklų valdytojams su atitinkama žyma ir nurodyta kuo skubiau pašalinti jų svetainėse ar tinkluose esantį draudžiamą skleisti interneto turinį;
- 40** pranešimų persiųsta tolesniam tyrimui PD, nes įtariamas draudžiamas turinys Lietuvos tarnybinėse stotyse. 34 pranešimai buvo apie vaikų seksualinio išnaudojimo vaizdus;
- 34** pranešimai, įtarus neigiamą poveikį nepilnamečiams darančią informaciją, persiųsti tolesniam tyrimui ŽEIT.
- 812** gautų pranešimų, kuriais buvo pranešta apie draudžiamą turinį, buvo pasikartojantys, t. y. apie tą patį turinį, dėl kurio buvo imtasi aukščiau nurodytų veiksmų.

Svarbu paminėti, kad iš 110 gautų pranešimų apie patyčias ir smurtą kibernetinėje erdvėje 47 atvejais informacija pasitvirtino ir buvo imtasi atitinkamų veiksmų, kad turinys būtų kuo skubiau pašalintas (2023 m. buvo fiksuoti 27 tokie pasitvirtinę pranešimai).

RRT, bendradarbiaudama su Kanados nevyriausybine organizacija „Canadian Centre for Child Protection“, dalyvauja tarptautiniame projekte „Arachnid“⁰⁸. RRT vertina iš interneto surinktus galimai draudžiamus vaizdus ir identifikuoja vaikų seksualinio išnaudojimo medžiagą (angl. *Child Sexual Abuse Material (CSAM)*). RRT, dalyvaudama šiame projekte, prisideda prie tokių vaizdų duomenų bazės papildymo ir jų pašalinimo iš interneto. 2024 m. RRT specialistai įvertino 54 840 potencialiai draudžiamo turinio vaizdų.

< 3 pav.

Veiksmai, atlikti su 2024 m. gautais pranešimais apie internete rastą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją (šaltinis – RRT)

08

Kanados nevyriausybės organizacijos „Canadian Centre for Child Protection“ (C3P) vykdomas „Arachnid“ projektas. Prieiga per internetą <https://projectarachnid.org/en/>.

7 Viešųjų kompiuterių tinklų (interneto) prieigos vietose privalomų filtravimo priemonių naudojimo užtikrinimas

RRT apibūna nepilnamečiams skirtą turinio filtravimo priemones ir jas skelbia RRT interneto svetainėje⁰⁹.

Vykdydama pavestas priežiūros funkcijas ir siekdama paskatinti kuo daugiau mokyklų ir viešųjų bibliotekų įsidiesti ir naudoti apibūnatas filtravimo priemones nepilnamečiams nuo žalingo interneto turinio apsaugoti, RRT tiesiogiai ir netiesiogiai susisiekė su visomis Lietuvos mokyklomis ir bibliotekomis, ragino vykdyti prievolę įsidiesti ir naudoti turinio filtravimo priemones bei priminė atsakomybę už prievolės nevykdymą¹⁰, patikrino 45 mokyklas ir viešąsias bibliotekas, organizavo susitikimus su mokyklų ir viešųjų bibliotekų steigėjais, supažindino viešųjų bibliotekų IT specialistus su RRT apibūnotomis filtravimo priemonėmis ir pabrėžė reikalavimą jomis naudotis, suteikė 193 ekspertines konsultacijas filtravimo priemonių pasirinkimo ir naudojimo klausimais, vertino turinio filtravimo priemones.

8 Visuomenės švietimo veikla

RRT, siekdama stiprinti interneto vartotojų sąmoningumą, 2024 m. vykdė švietėjišką veiklą: organizavo mokymus Lietuvos senjorams, vedė mokiniams pamokas apie saugų elgesį internete.

Nuo 2023 m. RRT vykdo projektą „Nė vienas nėra pamirštas“, skirtą senjorų skaitmeninei atskirčiai mažinti. Projektą globoja Lietuvos Respublikos Prezidentas. RRT ekspertai susitinka su visos Lietuvos bendruomenėmis ir, bendradarbiaudami su viešojo ir privataus sektoriaus atstovais, edukuoja senjorus, kaip patogiai naudotis skaitmeninėmis paslaugomis, apsisaugoti nuo sukčiavimo atvejų, kokios yra jų, kaip vartotojų, teisės. 2024 m. surengti 46 mokymai senjorams ir moksleiviams, juose dalyvavo 6 098 dalyviai. Šiuo metu prie projekto „Nė vienas nėra pamirštas“ yra prisijungę daugiau nei 150 organizacijų iš viešojo ir privataus sektoriaus, Lietuvos savivaldybės, bibliotekos, regioniniai informaciniai partneriai.

RRT nuo 2023 m. aktyviai dalyvauja projekte „Vilnius yra mokykla“, už tai yra gavusi Vilniaus mero padėką. 2024 m. dalyvaudami šiame projekte, RRT darbuotojai pravedė moksleiviams 19 pamokų apie saugų elgesį internete, ryšio technologijas. Pamokose dalyvavo 400 Vilniaus moksleivių.

RRT taip pat administruoja interneto svetainę www.esaugumas.lt. Joje interneto vartotojams teikiama aktuali ir nuolat atnaujinama informacija, kaip saugiai elgtis socialiniuose tinkluose, tinkamai pasirinkti antivirusinę programą, saugiai naudotis viešuoju belaidžiu internetu, elektronine bankininkyste, elektroninės prekybos galimybėmis ar apsaugoti savo privatumą internete.

2024 m. RRT specialistai socialinių tinklų vartotojams suteikė 306 konsultacijas. Interneto vartotojai dažniausiai susidūrė su socialinių tinklų paskyrų užgrobimu, paskyrų užblokavimu pažeidus socialinių tinklų taisykles, prisijungimo prie paskyros duomenų praradimu.

09

Aprobūotų filtravimo priemonių sąrašas pateiktas RRT interneto svetainėje <https://www.rrt.lt/saugenis-internetas/turinio-filtravimo-priemones/>.

10

Lietuvos Respublikos administracinių nusižengimų kodekso 496 str. 3 d. Prieiga per internetą <https://www.e-tar.lt/portal/lt/legalAct/4ebe66c0262311e5bf92d6af3f6a2e8b/asr>.

Nusikalstamų veikų kibernetinėje erdvėje mastas ir poveikis

Vadovo žodis



Arūnas Paulauskas,
Lietuvos policijos
generalinis komisaras

Kibernetinis saugumas yra neatsiejama šiuolaikinės valstybės ir visuomenės saugumo dalis. Nusikaltimų elektroninėje erdvėje dinamika ir kompleksiskumas kelia nemažai iššūkių teisėsaugai, tačiau Lietuvos policija yra pasirengusi profesionaliai kovoti su šiuo reiškiniu. Nuolat investuojame į pareigūnų kompetencijų tobulinimą ir technologinių priemonių, skirtų kovai su nusikaltimais elektroninėje erdvėje, vystymą ir diegimą. Įvertinus hibridines ir kitokio pobūdžio grėsmes, šiandien kylančias Lietuvai, itin svarbiu komponentu kibernetiniam saugumui užtikrinti tampa teisėsaugos ir kitų kibernetinio saugumo sektoriuje veikiančių institucijų ir privataus verslo struktūrų bendradarbiavimas. Dirbdami išvien galime nuveikti daug svarbių darbų kibernetinio saugumo stiprinimo srityje.



KAŲ SAUGO?

- ✓ Lietuvos žmonių teises ir laisves, visuomenę ir valstybę.



NUO KO SAUGO?

- ✓ Nuo nusikalstamų veikų ir jų neigiamo poveikio.



KAIP SAUGO?

- ✓ Tirdama, atskleisdama ir užkardydama nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui.
- ✓ Apribodama viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikimą paslaugų gavėjui ir (arba) nurodydama taikyti priemones, kuriomis šalinamos nusikalstamų veikų kibernetinėje erdvėje priežastys, kai paslaugų gavėjas galimai dalyvauja nusikalstamoje veikoje ar jo RIS įranga galimai naudojama nusikalstamai veikai.
- ✓ Inicijuodama kibernetinių incidentų tyrimus ir teikdama nurodymus interneto vartotojams kartu su NKSC.
- ✓ Perspėdama visuomenę dėl grėsmių kibernetinėje erdvėje, <https://policija.lrv.lt/lt/policija-pataria>.



LIETUVOS POLICIJA
Ginti. Saugoti. Padėti.

Svarbiausi 2024 m. įvykiai ir tendencijos



Kompanijos „Surfshark“ skaitmeninio gyvenimo kokybės indeksas rodo, kad Lietuva pagal kibernetinį saugumą 2024 m., kaip ir anksčiau, išliko antrąja šalimi pasaulyje.



Užregistruotų nusikalstamų veikų elektroninėje erdvėje (3 966 nusikalstamos veikos) skaičiaus didėjimas nebuvo kritinis (2023 m. – 3 912). Jų grėsmės lygis išliko nepakitęs ir neturėjo įtakos registruoto nusikalstamumo augimui.



Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui (LR BK 196–198² str.) sumažėjo beveik 10 proc.



Ypač sumažėjo kibernetinių nusikaltimų, susijusių su neteisėtu poveikiu elektroniniams duomenims (LR BK 196 str., palyginti su 2023 m., sumažėjo 71 proc.), neteisėtu poveikiu informacinei sistemai (LR BK 197 str., palyginti su 2023 m., sumažėjo 80 proc.), neteisėtu prisijungimu prie informacinės sistemos (LR BK 198¹ str., palyginti su 2023 m., sumažėjo 13 proc.).



2024 m. išliko teigiama tendencija, kad kibernetinės atakos prieš valstybės informacines sistemas ir (ar) valstybės ir tarnybos paslaptis neturėjo sistemingo nusikalstamumo požymių ir nekėlė kritinės žalos nacionaliniam saugumui.



2024 m. išliko tendencija, kad daugiausia nusikaltimų elektroninėje erdvėje sudaro įvairiais socialinės inžinerijos būdais vykdomas sukčiavimas (LR BK 182 str.). Tokių nusikaltimų kasmet daugėja.



Pagrindinis lėšų išviliojimo būdas liko avansinis (išankstinio mokėjimo) sukčiavimas, jo atvejų kasmet sparčiai daugėja. Didžiausios rizikos nukentėti nuo apgaulingų skelbimų vieta yra socialinis tinklas „Facebook“.



2024 m. ypač padaugėjo apgaulingų telefoninių skambučių. Vėl pradėta aktyviai naudoti pinigų viliojimo būdą skambinant dėl tariamai artimiesiems įvykusios nelaimės.



01001
10101

2024 m. išliko tendencija, kad suklastotos svetainės nuorodos pateikimas yra pagrindinė priemonė siekiant išviloti elektroninės bankininkystės duomenis ir (ar) išprovokuoti patvirtinti apgaulingą finansinę operaciją. Naujas išskirtinis reiškinys – interneto vartotojų prisijungimas prie suklastotos svetainės esveikata.lt.



Vienas iš sparčiausiai progresuojančių nusikaltimų – investicinis sukčiavimas, pasižymintis ypač didele finansine žala ir nusikaltėlių gaunama nauda.

1 Tarptautinė situacija

2024 m. IOCTA ataskaitoje⁰¹, kuri kasmet rengiama Europos Sąjungos teisėsaugos bendradarbiavimo agentūros (angl. *European Union Agency for Law Enforcement Cooperation (EUROPOL)*) (toliau – Europol), apžvelgiama kibernetinių nusikaltimų ekosistema ES ir analizuojami tokių nusikaltimų veikų padariniai, vykdytojai ir nukentėjusieji. Pagrindinės IOCTA ataskaitos išvados:

- įmonių el. pašto kompromitavimas ir romantinis sukčiavimas (angl. *romance fraud*) išlieka labiausiai paplitę kibernetinio sukčiavimo būdai ES, ypač vykdant duomenų viliojimo (angl. *phishing*) atakas, kuriomis siekiama iš aukos išvilioti prisijungimo ar kredito kortelių duomenis;
- sukčiai, naudojantys elektroninius duomenis užšifruojančių ir išpirkos reikalaujančių kenkimo programinio kodo virusus (angl. *ransomware*), vis dažniau atakuoja smulkaus ir vidutinio verslo įmones, nes jų žemesnis kibernetinio atsparumo lygis. El. prekybininkai ir bankai taip pat yra sukčių taikiny;
- prekyba vogtais duomenimis tampa vis didesne grėsme, susijusia su nusikaltimais kaip paslauga (angl. *crime-as-a-service*);
- kibernetiniai nusikaltėliai ir grupuotės ir toliau aktyviai naudojami tamsiojo interneto⁰² (angl. *Dark web*) forumais, svetainėmis, kuriuose ne tik galima dalytis nusikalstamos veikos rezultatais, bet ir lengvai bendrauti, aptarinėti nusikaltimų detales ir burtis į komandas. „Tor“ tinklas (angl. *the Tor network*) išlieka populiariausia platforma, skirta kibernetiniams nusikaltėliams pasiekti tamsųjį internetą;
- iki šiol kriminaliniame pasaulyje veikia tiek pavieniai sukčiai, turintys įvairių gebėjimų, tiek kuriami ištiesi nusikaltėlių tinklai. Į ES nusitaikiusių kibernetinių nusikaltėlių veikimo vieta taip pat įvairi: vieni veikia pačioje ES, kiti – užsienyje, nusišėdami savo neteisėtas operacijas ir lėšas trečiojoje šalyse;
- DI pagrįstos technologijos daro socialinę inžineriją dar efektyvesnę. Susirūpinimą taip pat kelia ir giliųjų klastočių naudojimas, nes tai toks pat galingas įrankis, kaip ir balso atkartojimas ar klatojimas.

01

IOCTA ataskaita. Prieiga per internetą <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024#downloads>.

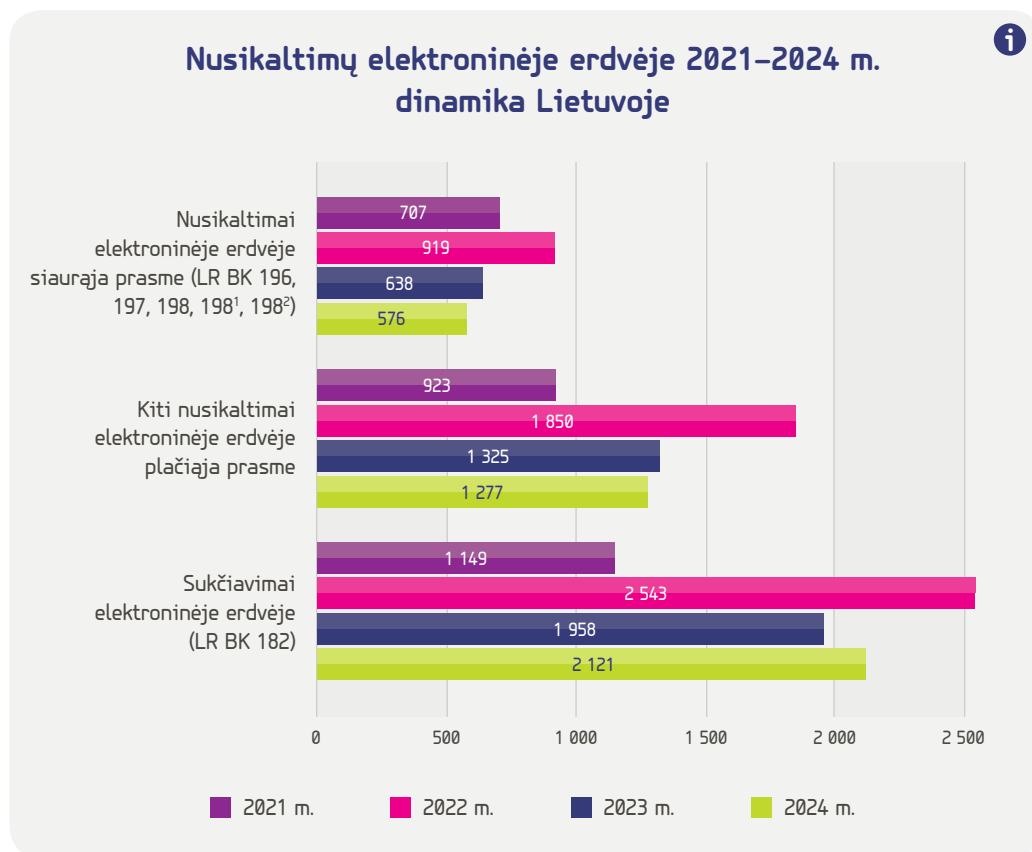
02

Tamsusis internetas – interneto dalis, kurią galima pasiekti tik naudojant tam tikrą programinę įrangą, konfigūracijas ar leidimą bei unikalių ryšio protokolą.

2 Nacionalinė situacija

Nusikaltimai elektroninėje erdvėje plačiąja prasme apibrėžiami kaip bet kokie nusikaltimai, kuriems įvykdyti vienaip ar kitaip buvo naudojamos kompiuterinės technologijos, o nusikaltimo faktui įrodyti turi būti taikomos specifinės nusikaltimų elektroninėje erdvėje tyrimo priemonės. **Nusikaltimai elektroninėje erdvėje siaurąja prasme** – tai nusikaltimai, tiesiogiai darantys įtaką elektroninių duomenų ir informacinių sistemų saugumui, kitaip tariant, pati kompiuterinė sistema yra nusikaltimo tikslas.

2024 m., kaip ir pernai, Lietuvoje ypač sumažėjo kibernetinių nusikaltimų siaurąja prasme. Tai liudija valstybės atsparumą kibernetinėms atakoms, žemą nusikaltimų elektroninėje erdvėje būklės lygį, nepavojingą dinamikos raidą ir mažą įtaką bendrai nusikalstamumo situacijai šalyje. Tačiau esminė problema vis dar lieka sukčiavimas elektroninėje erdvėje (žr. 1 pav.).

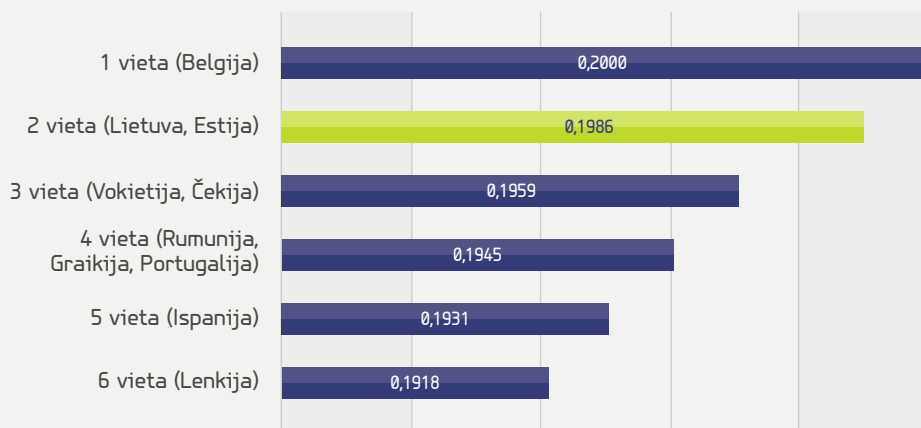


< 1 pav.

Nusikaltimų elektroninėje erdvėje 2021–2024 m. dinamika Lietuvoje (šaltinis – Lietuvos policija)

Lietuvos policijos 2024 m. stebėsenos vertinimas sutampa su nepriklausomų ekspertų išvadomis. Kompanijos „Surfshark“ 2024 m. atlikto skaitmeninio gyvenimo kokybės indekso tyrimo duomenimis, Lietuva pagal kibernetinį saugumą 2024 m. trečius metus iš eilės buvo paskelbta antrąja šalimi pasaulyje (žr. 2 pav.).

Šalių dešimtukas pagal kibernetinį saugumą 2024 m.



< 2 pav.

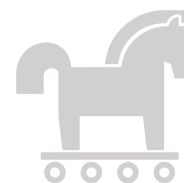
Kompanijos „Surfshark“ 2024 m. skaitmeninio gyvenimo kokybės indekso tyrimo rezultatai

Kibernetiniai nusikaltimai siaurąja prasme

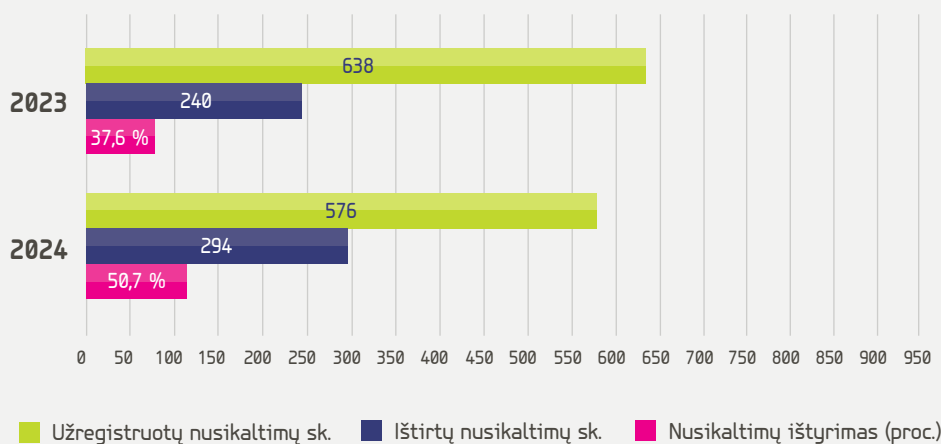
Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – IRD VRM) duomenimis, 2024 m. šalyje užregistruoti 576 nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui (LR BK 196-198² str.), tai 62 nusikalstamomis veikomis, arba 9,7 proc., mažiau nei 2023 m.

Bendroje nusikalstamumo struktūroje nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui 2024 m., kaip ir 2023 m., sudarė apie 1 proc. visų užregistruotų nusikalstamų veikų.

2024 m. šių nusikaltimų ištyrimas sudarė 50,7 proc. Palyginti su 2023 m., ištyrimas 13,1 proc. punktu didesnis (žr. 3 pav.).








2023-2024 m. įstaigose, atliekančiose ikiteisminius tyrimus, užregistruota nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui (LR BK 196-198² str.) (IRD prie LR VRM duomenys)



< 3 pav.

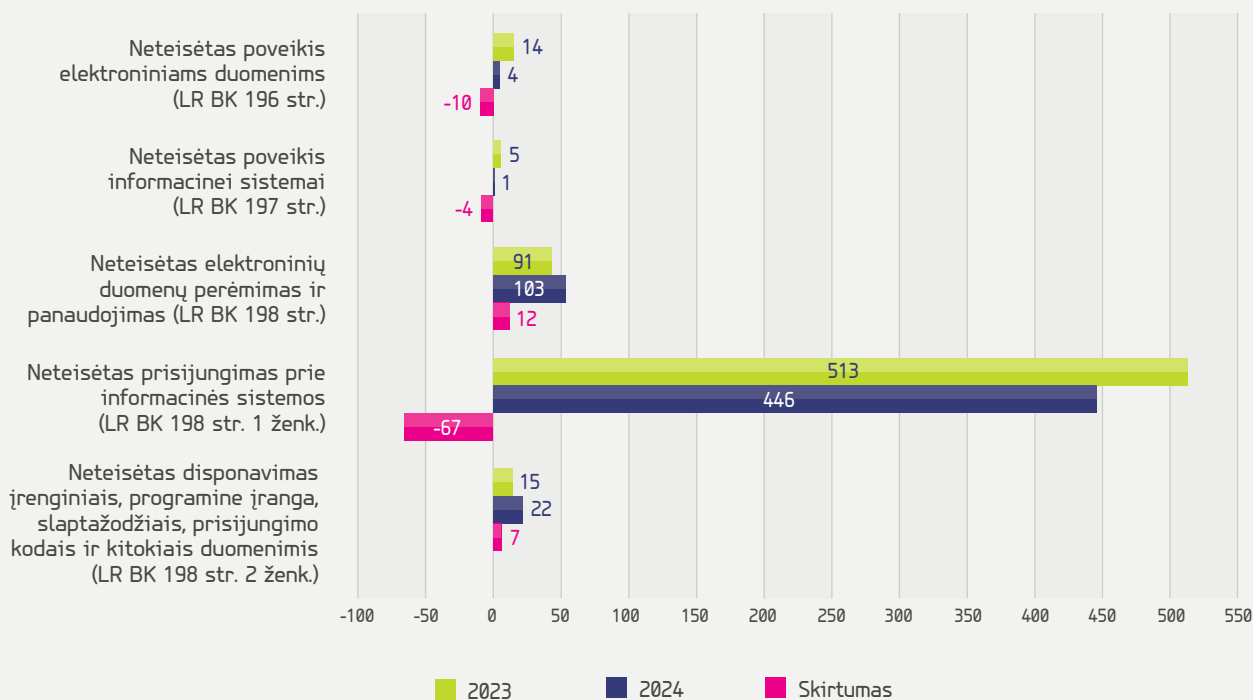
2023–2024 m. įstaigose, atliekančiose ikiteisminius tyrimus, nusikaltimų ištyrimas (šaltinis – Lietuvos policija)

Detalesnė informacija apie kiekvieną elektroninių duomenų ir informacinių išteklių saugumo nusikaltimą pagal LR BK 196-198² str. (žr. 4 pav.):

-  LR BK 196 str. „Neteisėtas poveikis elektroniniams duomenims“ – 2024 m. užregistruoti 4 nusikaltimai (2023 m. – 14). Palyginti su 2023 m., šių nusikaltimų užregistruota 71,4 proc. mažiau.
-  LR BK 197 str. „Neteisėtas poveikis informacinei sistemai“ – 2024 m. užregistruotas 1 nusikaltimas (2023 m. – 5). Palyginti su 2023 m., šių nusikaltimų užregistruota 80 proc. mažiau.
-  LR BK 198 str. „Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“ – 2024 m. užregistruoti 103 nusikaltimai (2023 m. – 91). Palyginti su 2023 m., šių nusikaltimų užregistruota 13,2 proc. daugiau.
-  LR BK 198¹ str. „Neteisėtas prisijungimas prie informacinės sistemos“ – 2024 m. užregistruoti 446 nusikaltimai (2023 m. – 513). Palyginti su 2023 m., šių nusikaltimų užregistruota 13,1 proc. mažiau.
-  LR BK 198² str. „Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis“ – 2024 m. užregistruoti 22 nusikaltimai (2023 m. – 15). Palyginti su 2023 m., šių nusikaltimų užregistruota 46,7 proc. daugiau.

▼ 4 pav.
2023–2024 m. įstaigose, atliekančiose ikiteisminius tyrimus, užregistruoti nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui atvejai (šaltinis – Lietuvos policija)





2023–2024 m. įstaigose, atliekančiose ikiteisminius tyrimus, užregistruota nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui (LR BK 196–198² str.) (IRD prie LR VRM duomenys)



Remiantis policijos ikiteisminių tyrimų duomenimis, 2024 m. atvejų, kai buvo naudojamosi elektroninius duomenis užšifruojančiais išpirkos reikalaujančio kenkimo programinio kodo virusais ar DDoS atakomis, dalis nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui struktūroje buvo 1 proc. (2023 m. – 5 proc.)

Dominuojančių tikslų, dėl kurių 2024 m. buvo daromi kibernetiniai nusikaltimai siaurąja prasme, struktūra kokybiškai nesikeičia, tačiau šios struktūros kiekybiniai rodikliai yra labai sumažėję. Iki šiol didžiausią kibernetinių nusikaltimų dalį sudaro turtinės naudos siekimo atvejai. 2024 m. tokie nusikaltimai sudarė 79 proc. (palyginti su 2023 m., atvejų sumažėjo 25 proc. punktais).

Kita vis dar dominuojančių kibernetinių nusikaltimų dalis 2024 m. yra beveik 4 kartus mažesnė ir kol kas susijusi su retesniais atvejais:

-  kibernetiniai nusikaltimai, kurių tikslas buvo duomenų apie informacinių sistemų pažeidžiamumą ieškojimas ir (ar) elektroninių duomenų grobimas, sudarė 7 proc. (palyginti su 2023 m., atvejų sumažėjo 13 proc. punktu);
-  kibernetinio chuliganizmo apraiškos, kurias, kaip ir anksčiau, dėl platinamo neetiško turinio ir (ar) pamokų trikdymo dažniausiai lėmė akademinio jaunimo kenkimas ugdymo informacinėms sistemoms, sudarė 6 proc. (palyginti su 2023 m., atvejų sumažėjo 26 proc. punktais);
-  kibernetiniai nusikaltimai dėl buitinių konfliktų, kuriuos, kaip ir anksčiau, labiausiai lėmė santykiai darbovietėse, artimojoje ir bendravimo aplinkoje, sudarė 3 proc. (palyginti su 2023 m., atvejų skaičius panašus);
-  žmonių bauginimas ir (ar) terorizavimas kibernetiniais būdais sudarė 2 proc. (palyginti su 2023 m., atvejų skaičius sumažėjo 56 proc. punktais). Šie atvejai nepasižymėjo kaip sistemingai organizuota veikla, kai siekiama pakenkti valstybės geopolitiniams interesams, žmonių ir (ar) jų grupių įsitikinimams ar dėl kitokios neapykantos asmenims.

Elektroninius duomenis užšifruojantys išpirkos reikalaujančio kenkimo programinio kodo virusai

2024 m. policijos įstaigos užregistravo 4 atvejus, kai elektroniniai duomenys buvo užšifruoti išpirkos reikalaujančio kenkimo programinio kodo virusais. Palyginti su 2023 m., tai beveik 5 kartus mažiau. Staigus ir išskirtinis tokių kibernetinių atakų skaičiaus mažėjimas vertinamas kaip ypač teigiamas situacijos pokytis (2020–2023 m. – 16 atvejų per metus).

2024 m. išpirkos už elektroninių duomenų iškodavimą prievartavimo metodai nesikeitė⁰³. 2024 m. reikalautų išpirkų dydis buvo nuo 9 999 USD (9 708 Eur) iki 2 BTC (111 826 Eur), o 2023 m. didžiausia prašyta išpirkos suma buvo 900 000 USD (832 254 Eur). 2024 m. nustatyta, kad elektroniniams duomenims užšifruoti buvo naudojami 2 šeimų elektroninius duomenis užšifruojantys išpirkos reikalaujančio kenkimo programinio kodo virusai⁰⁴.

2024 m. pirmą kartą elektroninius duomenis užšifruojantis išpirkos reikalaujančio kenkimo programinio kodo virusas buvo panaudotas prieš Lietuvos finansų sektorių. Nukentėjusi elektroninių pinigų įmonė patyrė kombinuotą elektroninių duomenų grobimo ir užšifravimo ataką. Šiuo atveju buvo sutrikdyta elektroninės bankininkystės sistema, todėl klientai negalėjo pasiekti savo paskyrų ir sąskaitų.

03

Virusais užkrėstose informacinėse sistemose buvo palikti raštai su išpirkos mokėjimo nurodymais ir komunikavimo kontaktais (angl. *ransom note*). Naudotos priegigos prie interneto maskavimo ir anoniminio komunikavimo priemonės (tamsiojo interneto anoniminė naršyklė „Tor“ (angl. *The Onion Router*), anoniminio el. pašto teikėjų paslaugos, 2024 m. nustatyta nauja priemonė – greito ir anoniminio bendravimo programėlė „TOX messenger“). Programišiai derino ir duomenų grobimo, ir duomenų užšifravimo atakas, todėl išpirkos reikalavimas apėmė grasinimą tiek duomenis sunaikinti, tiek juos paviešinti. Dažniausiai buvo reikalaujama išpirką sumokėti kriptovaliuta.

04

LOCKBIT (1 atvejis, virusas žinomas nuo 2021 m.), PHOBOS/EJECT VIRUS (1 atvejis, virusas žinomas nuo 2024 m.).

DDoS atakos

2024 m. pradėtas 1 ikiteisminis tyrimas (arba 1 mažiau nei 2023 m.) dėl informacinių sistemų trikdymo DDoS atakomis. Nuo 2020 m. policijos tyrimų dėl DDoS atakų skaičius išlieka stabilus – iki 3 atvejų per metus. Lietuvos informacinių sistemų atsparumas DDoS atakoms, valstybei išgyvenant daugiamečių ir stiprėjančių hibridinį karą, vertintinas labai teigiamai. 2024 m. nustatytos DDoS atakos priešastis buvo įmonės turto prievartavimas. Piktavaliai, trikdydami prekybos dovanų kuponais interneto svetainės veiklą, siekė priversti įmonę derėtis dėl nutekintų duomenų.






Kibernetinius nusikaltimus lėmusios aplinkybės ir kibernetinių nusikaltimų poveikio vertinimas

Kibernetinių nusikaltimų būdai

2024 m. pagrindinės kibernetinių nusikaltimų siaurąja prasme technologijos, kuriomis buvo užvaldyti informacinių sistemų vartotojų duomenys ir (ar) gauta prieiga prie informacinių sistemų, kaip ir anksčiau, daugiausia rėmėsi socialine inžinerija. Dažniausiai naudotos priemonės:








-  apgaulingos žinutės;
-  apgaulingi telefoniniai skambučiai;
-  apgaulingi el. pašto laiškai.

Naujas reiškinys – interneto vartotojų prisijungimas per naršyklę ar per apgaulingą skelbimo nuorodą prie suklastotų svetainių. Šių atvejų ypač padaugėjo 2024 m. pabaigoje, todėl jų tikrasis mastas ir dinamika paaiškės 2025 m. Suklastotos interneto svetainės buvo pritaikytos lėšoms iš banko sąskaitų grobti. Dažniausiai buvo prisijungiama per interneto naršyklėje pateiktas nuorodas į svetainės **esveikata.lt** klastotes. Taip pat atrodo dėsningi keli pirmieji atvejai, kai į bankų SEB ir „Swedbank“ svetainių klastotes buvo nukreipta per apgaulingų skelbimų internete nuorodas.

Kibernetinių nusikaltimų padariniai

2024 m. dažniausi kibernetinių nusikaltimų siaurąja prasme padariniai, palyginti su 2023 m., išliko tie patys:







-  neteisėtos finansinės operacijos;
-  duomenų stebėjimas ir (ar) pasisavinimas;
-  paskyrų perėmimas;
-  neteisėtas duomenų paskelbimas;
-  duomenų užšifravimas, sugadinimas, pakeitimas ar sunaikinimas; prekyba nutekintais duomenimis.



Atakuotos informacinės sistemos



2024 m. dažniausi kibernetinių nusikaltimų siaurąja prasme taikiniai, palyginti su 2023 m., išliko tie patys:








-  elektroninės bankininkystės paskyros;
-  socialinių tinklų paskyros;
-  interneto paslaugų vartotojų paskyros;
-  informacinių sistemų tinklai ir (ar) galiniai įrenginiai;
-  informacinių sistemų vartotojų paskyros;
-  el. pašto paskyros.

Atakuoti ar neteisėti (neteisėtai paskelbti) elektroniniai duomenys



2024 m. išliko ilgametė teigiama tendencija, susijusi su sąlyginai maža kibernetinių nusikaltimų rizika valstybės ir tarnybos paslaptims. Tiek 2024 m., tiek per pastaruosius kelerius metus kibernetinės atakos žalingų padarinių valstybės ir tarnybos paslaptims nesukėlė.

2024 m. dažniausiai buvo kėsinamasi į finansinius instrumentus. 6 kartus mažesnę dalį sudarė atvejai, susiję su kėsinimusi į konfidencialią (neviešą) informaciją:

-  informacinių sistemų vartotojų autentifikavimosi duomenis;
-  finansinius, ūkinius, komercinius duomenis;
-  privataus gyvenimo duomenis;
-  BDAR apibrėžtus asmens duomenis;
-  intymaus turinio duomenis;
-  informacinių sistemų operacinius duomenis;
-  tarnybinius, profesinius duomenis.

2024 m., priešingai nei 2023 m., nebuvo poveikio valstybės tvarkomiems informaciniams ištekliams. 2024 m. kibernetinių atakų, susijusių su apgaulingų ar žalingų elektroninių duomenų platinimu, buvo mažiau nei 2023 m. Didžiausią dalį sudarė neetiško ar bauginamo turinio informacija (2 kartus mažiau nei 2023 m.). 2024 m. taip pat sumažėjo atvejų, kai buvo platinami apgaulingi prašymai, apgaulingi komerciniai skelbimai internete, kenkimo programinė įranga ir (ar) jos jaukas.

2024 m. padaugėjo apgaulingų komercinių užsakymų internete, tačiau augimas nėra rizikingas.

Kibernetinių nusikaltimų poveikis fiziniams asmenims



2024 m., kaip ir 2023 m., iš visų subjektų, patiriančių kibernetinių nusikaltimų poveikį, dažniausiai nukentėjo fiziniai asmenys.

2024 m. išliko tendencija, kad, be socialine inžinerija paremtu sukčiavimo, fiziniai asmenys taip pat nukentėjo dėl poveikio socialinių tinklų paskyroms, paskyroms interneto svetainėse, mobiliųjų programėlių paskyroms, informacinių sistemų vartotojų paskyroms, el. pašto paskyroms, informacinių sistemų tinklams ir (ar) galiniams įrenginiams.

Dažniausi kibernetinių nusikaltimų padariniai fiziniams asmenims 2024 m. buvo paskyrų perėmimas, elektroninių duomenų stebėjimas ir (ar) pasisavinimas, neteisėtas elektroninių duomenų paskelbimas, neteisėtų finansinių operacijų, užvaldžius paskyras ir (ar) elektroninės bankininkystės duomenis, inicijavimas. 2024 m. naujas reiškinys – prekyba duomenimis, nutekintais iš fizinių asmenų informacinių sistemų. Tai lėmė staigus dovanų kuponų ir bilietų į renginius nutekinimas iš paskyrų, kurias fiziniai asmenys valdė platinimo paslaugas teikiančiose svetainėse, ir šių elektroninių duomenų perpardavimas internete.

2024 m. kibernetinėmis atakomis prieš fizinių asmenų informacines sistemas dažniausiai buvo kėsiamasi į konfidencialią (neviešą) informaciją, finansinius elektroninius instrumentus, apgaulingos ir (ar) žalingos informacijos svetimo asmens vardu platinimą.

2024 m. daugiausia kibernetinių atakų buvo taikyta į informacinių sistemų vartotojų autentifikavimosi duomenis. Kita kibernetinių atakų dalis buvo susijusi su fizinių asmenų privataus gyvenimo duomenimis, intymaus turinio duomenimis ir BDAR apibrėžtais asmens duomenimis.

2024 m. fizinių asmenų informacinėse sistemose platintą apgaulingą ar žalingą informaciją sudarė neetiško ar bauginamo turinio informacija, apgaulingi komerciniai užsakymai svetimo asmens vardu, apgaulingi prašymai, apgaulingi komerciniai skelbimai internete, kenkimo programinė įranga ir (ar) jos jaukas.

Kibernetinių nusikaltimų poveikis juridiniams asmenims



2024 m. kibernetinių nusikaltimų poveikio ir žalos juridiniams asmenims kokybinių požymių struktūra iš esmės nesikeitė.

2024 m. iš visų subjektų, patyrusių kibernetinių nusikaltimų poveikį, juridiniai asmenys sudarė 6 proc. arba mažiau. 2024 m. išliko tendencija, kad iš juridinių asmenų, patyrusių kibernetinių atakų poveikį, dažniausi buvo prekybos subjektai. Kitos ryškesnės kibernetinės atakos buvo prieš informatikos ar telekomunikacijų paslaugų, transportavimo paslaugų, buhalterinių paslaugų subjektus.

2024 m. juridiniai asmenys dažniausiai nukentėjo dėl poveikio interneto svetainėms, informacinių sistemų tinklams ir (ar) galiniams įrenginiams (atvejų sumažėjo), informacinių sistemų vartotojų paskyroms. Kitos atakuotos juridinių asmenų informacinės sistemos buvo el. pašto paskyros, socialinių tinklų paskyros, paskyros interneto svetainėse.

Dažniausi kibernetinių nusikaltimų padariniai juridiniams asmenims 2024 m. buvo elektroninių duomenų neteisėtas stebėjimas, pasisavinimas, elektroninių duomenų užšifravimas, sugadinimas, pakeitimas ar sunaikinimas, el. pašto adresų imitavimas ir (ar) elektroninio susirašinėjimo perėmimas, prekyba nutekintais duomenimis, neteisėtas elektroninių duomenų paskelbimas, prieigos prie informacinių sistemų ir (ar) elektroninių duomenų apribojimas, paskyrų perėmimas.

2024 m. daugiausia kibernetinių atakų buvo taikytą į finansinius, ūkinius, komercinius duomenis. Kitos kibernetinės atakos buvo susijusios su juridinių asmenų informacinių sistemų vartotojų autentifikavimosi duomenimis, valdomais asmens duomenimis, kuriuos apibrėžia BDAR, informacinių sistemų operaciniais duomenimis, privataus gyvenimo duomenimis.

2024 m. juridinių asmenų informacinėse sistemose platinta apgaulinga ar žalinga elektroninė informacija pasižymėjo tik apgaulingai vartotojų internete pateiktais komerciniais užsakymais.

Kibernetinių nusikaltimų poveikis viešųjų paslaugų subjektams

2024 m. kibernetinių nusikaltimų poveikio ir žalos viešiesiems subjektams kokybinių požymių struktūra iš esmės nesikeitė.

2024 m. iš visų subjektų, patyrusių kibernetinių nusikaltimų poveikį, viešieji subjektai sudarė 5 proc., arba mažiau. Išliko tendencija, kad iš viešųjų subjektų, patyrusių kibernetinių atakų poveikį, dažniausios buvo švietimo sektoriaus informacinės sistemos. Kitos akivaizdesnį poveikį viešiesiems subjektams turėjusios kibernetinės atakos taikytos prieš sveikatos paslaugų ir kultūros sektorių.

Viešieji subjektai dažniausiai nukentėjo dėl poveikio informacinių sistemų vartotojų paskyroms. Kitos atakuotos viešųjų subjektų informacinės sistemos buvo socialinių tinklų paskyros, interneto svetainės, informacinių sistemų duomenų registrai ar duomenų bazės.

Dažniausi kibernetinių nusikaltimų padariniai viešiesiems subjektams buvo elektroninių duomenų užšifravimas, sugadinimas, pakeitimas ar sunaikinimas, neteisėtas elektroninių duomenų paskelbimas, elektroninių duomenų stebėjimas, pasisavinimas, paskyrų perėmimas.

Kibernetinėmis atakomis prieš viešųjų subjektų informacines sistemas dažniausiai buvo siekiama platinti apgaulingą ir (ar) žalingą informaciją svetimo asmens vardu ir konfidencialią (neviešą) informaciją.

Iš viešųjų subjektų konfidencialios (neviešos) informacijos, į kurią buvo taikytos kibernetinės atakos, dažniausia buvo finansiniai, ūkiniai, komerciniai elektroniniai duomenys ir informacinių sistemų vartotojų autentifikavimosi duomenys. Kitos kibernetinės atakos buvo susijusios su viešųjų subjektų valdomais asmens duomenimis, kuriuos apibrėžia BDAR, ir tarnybiniais, profesiniais duomenimis.

2024 m. viešųjų subjektų informacinėse sistemose platintą apgaulingą ar žalingą elektroninę informaciją daugiausia sudarė neetiško ar bauginamo turinio informacija.

Kibernetinių nusikaltimų poveikis valstybės įmonėms

2024 m., priešingai nei 2023 m., kibernetinių atakų prieš valstybės įmones policija nenustatė.



Kibernetinių nusikaltimų poveikis valstybės institucijoms



2024 m. kibernetinės atakos prieš valstybės institucijų informacines sistemas nebuvo sistemingas ir masiškai organizuojamo kenkimo požymius atitinkantis reiškinys.

2024 m. pradėtas ikiteisminis tyrimas dėl 1 kibernetinės atakos prieš valstybės institucijos informacinę sistemą (2023 m. - 3). Tai sudaro iki 1 proc. visų subjektų, patyrusių kibernetinių atakų poveikį (panašiai kaip ir 2023 m.).

2024 m. nuo kibernetinės atakos nukentėjo Lietuvos Respublikos užsienio reikalų ministerija - buvo įsilaužta į informacinės sistemos vartotojo paskyrą ir nutekinti tarnybiniai, profesiniai duomenys. Pradėtas ikiteisminis tyrimas pagal LR BK 198 str. dėl neteisėto elektroninių duomenų perėmimo ir panaudojimo ir LR BK 198¹ str. dėl neteisėto prisijungimo prie informacinės sistemos. Nors kibernetinių atakų prieš valstybės institucijų informacines sistemas skaičius nėra didelis, tačiau Užsienio reikalų ministerijos valdomi tarnybiniai, profesiniai duomenys pradėti nutekinti nuo 2023 m.

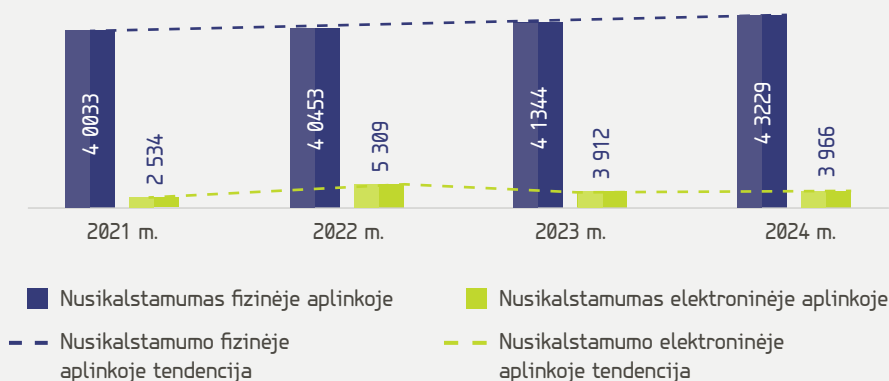
Kibernetinių nusikaltimų siaurąją prasme situacijos vertinimas liudija valstybės institucijų ir jų informacinių sistemų atsparumą kibernetinėms grėsmėms. Valstybei pavojingiausios kibernetinės atakos, sukeliančios ypač nuostolingų padarinių, nelaikomos sistemingais nusikaltimo atvejais, pasitaiko tik pavienių bandymų pakenkti.

Kibernetiniai nusikaltimai plačiąja prasme



2024 m. policija užregistravo 44 531⁰⁵ nusikalstamą veiką, iš jų 3 966⁰⁶ nusikalstamos veikos, arba 9 proc., padarytos elektroninėje erdvėje. Tokių nusikalstamų veikų, palyginti su 2023 m., padaugėjo 1 proc., arba 54 nusikalstamomis veikomis. 2024 m. nusikalstamų veikų, padarytų fizinėje aplinkoje, padaugėjo 5 proc., arba 2 025 nusikalstamomis veikomis. Tai rodo, kad 2024 m. nusikalstamos veikos elektroninėje erdvėje neturėjo įtakos registruoto nusikalstamumo augimui ir jų grėsmės lygis išliko nepakitęs. Bendroje nusikalstamumo struktūroje santykis tarp nusikalstamų veikų, padarytų elektroninėje erdvėje, ir nusikalstamų veikų, padarytų fizinėje aplinkoje, išliko toks pat kaip ir 2023 m. (žr. 5 pav.).

2021-2024 m. registruotas nusikalstamumas pagal padarymo vietos požymį (elektroninė erdvė ir fizinė aplinka) (IRD prie LR VRM duomenys)



< 5 pav.

2021–2024 m. registruotas nusikalstamumas pagal padarymo vietos požymį (šaltinis – IRD prie LR VRM)

⁰⁵

IRD VRM duomenys apie ikiteisminio tyrimo įstaigose užregistruotas nusikalstamas veikas (Forma_EK-ITJ).

⁰⁶

IRD VRM duomenys apie užregistruotas nusikalstamas veikas, padarytas elektroninėje erdvėje (Forma_EL-ERDVĖ-ITJ).

2024 m. išliko tendencija, kad nusikalstamą elektroninę erdvę ypač lemia:

-  sukčiavimo (LR BK 182 str.) atvejai – 53 proc. (palyginti su 2023 m., 3 proc. punktais daugiau);
-  nusikaltimai elektroninėje erdvėje siaurąja prasme – 14 proc. (palyginti su 2023 m., 2 proc. punktais mažiau);
-  neteisėto elektroninės mokėjimo priemonės ar jos duomenų panaudojimo atvejai (LR BK 215 str.) – 12 proc. (palyginti su 2023 m., 2 proc. punktais mažiau);
-  disponavimo pornografinio turinio dalykais atvejai (LR BK 309 str.) – 8 proc. (palyginti su 2023 m., 2 proc. punktais daugiau),
-  netikros elektroninės mokėjimo priemonės gaminimo, tikros elektroninės mokėjimo priemonės klastojimo ar neteisėto disponavimo elektronine mokėjimo priemone arba jos duomenimis atvejai (LR BK 214 str.) – 6 proc. (palyginti su 2023 m., 1 proc. punktu mažiau);
-  jaunesnio negu šešiolikos metų asmens tvirkimo atvejai (LR BK 153 str.) – 2 proc. (palyginti su 2023 m., 1 proc. punktu daugiau);
-  dokumento suklastojimo ar disponavimo suklastotu dokumentu atvejai (LR BK 300 str.) – 2 proc. (palyginti su 2023 m., 1 proc. punktu daugiau);
-  kurstymo prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę atvejai (LR BK 170 str.) – 1 proc. (arba tiek pat kaip 2023 m.);
-  šmeižimo atvejai (LR BK 154 str.) – 1 proc. (arba tiek pat kaip 2023 m.);
-  turto prievartavimo atvejai (LR BK 181 str.) – 1 proc. (arba panašiai kaip 2023 m.);
-  grasinimo nužudyti ar sunkiai sutrikdyti žmogaus sveikatą arba žmogaus terorizavimo atvejai (LR BK 145 str.) – iki 1 proc. (arba panašiai kaip 2023 m.).

Dominuojantys sukčiavimo elektroninėje erdvėje būdai nesikeitė ir 2024 m.

Sukčiavimo būdu padaryta žala

Finansų rinkos dalyvių duomenimis, iš Lietuvos gyventojų ir juridinių asmenų 2024 m. apgaule buvo kėsintasi išvilioti 35 mln. Eur, tačiau finansų įstaigoms pavyko apsaugoti 17,6 mln. Eur, t. y. dvigubai daugiau lėšų negu pernai, 2023 m. ši suma siekė 7,9 mln. Eur. 2024 m. gyventojų patirti nuostoliai siekė 17,3 mln. Eur, t. y. 28 proc. daugiau negu 2023 m. 2024 m. finansų įstaigos fiksavo daugiau kaip 13 tūkst. sukčiavimo atvejų⁰⁷.

2024 m. išliko tendencija, kad dažniausiai išviliotų pinigų sumos buvo iki 1 tūkst. Eur dydžio. Tačiau didžiausios žalos, kai lėšos viršijo 10 tūkst. Eur, atvejų 2024 m. padaugėjo 36 proc., šis rodiklis daugiau nei 2 kartus didesnis už metinį tokio sukčiavimo atvejų 2020–2023 m. vidurkį.



07

VsĮ Pinigų plovimo prevencijos kompetencijų centro duomenys. Prieiga per internetą <https://amlcenter.lt/naujausia-analize-atskleide-apsaugoti-milijonai-bet-nuostoliai-vis-dar-milziniski/>.

Avansinis (išankstinio mokėjimo) sukčiavimas



2024 m. avansinio (išankstinio mokėjimo) sukčiavimo atvejų padaugėjo. Šių nusikaltimų skaičius kasmet sparčiai didėja. Pagrindinis šio sukčiavimo būdas yra apgaulingų skelbimų platinimas internete ir išprovokavimas virtualiai susitarti ir atlikti mokėjimą į sukčiaus nurodytą sąskaitą. Iš apgaulingų skelbimų dažniausi buvo pasiūlymai pirkti elektronikos techniką, transporto priemonių dalis, buitinę techniką, transporto priemones, išsinuomoti nekilnojamąjį turtą. Socialiniai tinklai vis dar dominuoja kaip apgaulingų skelbimų platinimo vieta, pavyzdžiui, „Facebook“ 2024 m. paskelbtų apgaulingų skelbimų, palyginti su 2023 m., padaugėjo 27 proc. Nacionaliniuose reklamos ir (ar) naudotų dalykų komercijos portaluose, dažniausiai skelbiu.lt, autoplus.lt, autogidas.lt, platintų apgaulingų skelbimų dalis 2024 m. sudarė 10 proc. (palyginti su 2023 m., 23 proc. punktais mažiau). Nukentėjusiųjų dėl apgaulingų skelbimų platinimo tarptautinėse reklamos platformose dalis ir toliau liko nedidelė. Lietuvos gyventojai su didžiausia tarptautinio sukčiavimo rizika susiduria Vokietijos reklamos svetainėje mobile.de.

Svarbiausios avansinio (išankstinio mokėjimo) komunikavimo priemonės 2024 m. nekito – dažniausiai buvo naudojamos mobiliosios bendravimo programos „Facebook“ programėle „Messenger“ (palyginti su 2023 m., naudojimasis išaugo 28 proc.) ir nacionaliniu telefoniniu ryšiu (palyginti su 2023 m., naudojimasis sumažėjo 25 proc.).

Sukčiavimas apgaulingais telefoniniais skambučiais



2023 m. staiga sumažėjęs naudojimosi apgaulingais telefoniniais skambučiais rodiklis 2024 m. išaugo 64 proc. Nustatyta, kad apgaulingų skambučių skaičius daugiau nei 2 kartus didesnis už metinį vidurkį 2020–2023 m. Apgaulingais telefoniniais skambučiais buvo siekiama išvilioti grynuosius pinigus ir (ar) vertybes (palyginti su 2023 m., atvejų padaugėjo 69 proc.), naudojant išviliotus elektroninės bankininkystės vartotojų duomenis grobti lėšas iš banko sąskaitų (palyginti su 2023 m., atvejų padaugėjo 59 proc.).

2024 m. telefoniniai sukčiai dažniausiai apsimetinėjo informacinių sistemų specialistais (palyginti su 2023 m., atvejų padaugėjo 98 proc.), policijos pareigūnais (palyginti su 2023 m., atvejų padaugėjo 21 proc.), bankų darbuotojais (palyginti su 2023 m., atvejų padaugėjo 66 proc.), artimaisiais (palyginti su 2023 m., atvejų padaugėjo 89 proc.), advokatais (palyginti su 2023 m., atvejų padaugėjo 95 proc.).

Sukčiai dažniausiai melavo apie elektroninės bankininkystės sistemos problemas (palyginti su 2023 m., atvejų padaugėjo 72 proc.), artimųjų nelaimę (palyginti su 2023 m., atvejų padaugėjo 87 proc.), namuose laikomus netikrus pinigus (palyginti su 2023 m., atvejų sumažėjo 10 proc.), būtinumą suteikti pagalbą tyrėjams (palyginti su 2023 m., atvejų padaugėjo 38 proc.), organizuojamą loteriją (palyginti su 2023 m., atvejų padaugėjo 93 proc.).

Staigiam apgaulingų skambučių šuoliui 2024 m. įtakos galėjo turėti rusakalbiai sukčiai, nes jie vieni aktyviausių virtualaus sukčiavimo organizatorių, o pastaruoju metu galimai pradėta plėtoti migruojančių tarptautinių nusikalstamų grupių veikla. Anksčiau tokio sukčiavimo organizatoriai būdavo siejami su laisvės atėmimo bausmes kalėjimuose atliekančiais nuteistaisiais.

Nuo 2024 m. balandžio mėn. itin suaktyvėjo telefoniniai sukčiai. Siekdami išvilioti elektroninės bankininkystės vartotojų duomenis ir (ar) fizines bankų mokėjimo korteles su PIN kodais, sukčiai melavo tiek apie interneto tinklo galinių įrenginių, tiek apie elektroninės bankininkystės vartotojų sistemos problemas, kiekvienu atveju apsimesdami kartu veikiančiais internetinės „Google“ platformos specialistais, banko darbuotojais ir policijos pareigūnais. Sukčiai pasiimti banko mokėjimo kortelių atvykdavo

į namus arba nurodydavo jas atsiųsti paštu. Šie atvejai padarė įtaką kitam nusikaltimui elektroninėje erdvėje – 2024 m. pradėjo didėti sukčiavimo svetimomis banko mokėjimo kortelėmis atvejų.

2024 m. išaiškintos kelios telefoninių sukčių organizuotos nusikalstamos grupės, kurios meluodavo apie artimųjų nelaimę, o paimti grynųjų pinigų atvykdavo į nukentėjusiųjų gyvenamąją vietą. Šios organizuotos nusikalstamos grupės į Lietuvą atvyko iš užsienio ir bendrininkavo su Rusijos, Ukrainos, Estijos, Čekijos piliečiais.

Sukčiavimas apgaulingomis žinutėmis



Sukčiavimų naudojant apgaulingas SMS žinutes kasmet daugėjo iki 2023 m., o 2024 m. tokių atvejų skaičius staiga sumažėjo 50 proc. Viena iš spartaus apgaulingų SMS žinučių skaičiaus mažėjimo priežasčių – nusikaltėlių grupės pradėjo aktyviau naudoti skambučius telefonu. Tai galėjo lemti veiksminga žalingos veiklos internete ir veikimo elektroninio komunikavimo priemonėmis tarpinstitucinė prevencija, kuri apima ir nuo 2023 m. liepos mėn. nustatytą operatoriams įpareigojimą techniniais metodais identifikuoti SMS siuntėjus. Išaugęs pastarųjų metų prevencijos efektyvumas leidžia prognozuoti teigiamą apgaulingų SMS žinučių problemos pokytį. SMS žinučių, kaip vieno iš anoniminio bendravimo būdų, populiarumą tarp sukčiavimo organizatorių mažins ir nuo 2025 m. pradžios įsigaliojęs reikalavimas visiems išankstinio mokėjimo paslaugas teikiantiems mobiliojo ryšio tiekėjams registruoti SIM kortelių pirkėjus. Pastarųjų metų prevencijos būdų proveržis leidžia prognozuoti ryškų teigiamą apgaulingų SMS žinučių skaičiaus pokytį.

Tačiau apgaulingos žinutės 2024 m. buvo ir toliau siunčiamos internetinio bendravimo programomis. Šis anoniminio komunikavimo būdas nuo 2020 m. sparčiai populiarėjo. Apgaulingų internetinio bendravimo programų žinučių, palyginti su 2023 m., padaugėjo 20 proc. Svarbiausias sukčiavimo apgaulingomis žinutėmis tikslas išliko toks pat – grobstymas iš svetimų sąskaitų. Dažniausiai apgaulingose žinutėse teikiamos nuorodos į suklastotas svetaines ir išprovokuojama įvesti elektroninės bankininkystės duomenis ir (ar) patvirtinti apgaulingai inicijuotą pavedimą iš sąskaitos. 2024 m. apgaulingų nuorodų ir (ar) suklastotų svetainių padaugėjo 9 proc. Didelė dalis apgaulingų žinučių siejosi su dangstymusi pirkėjais internetinėse svetainėse, siuntų tarnybų vardu ir tariamu būtinumu sumokėti siuntos mokesť ar patikslinti adresato duomenis, VMI vardu ir tariama prievole sumokėti baudą, „Facebook“ draugu ir pranešimu apie tariamą laimėjimą loterijoje, finansų įstaigų ir (ar) jų informacinių sistemų vardu ir tariamomis problemomis elektroninės bankininkystės vartotojų paskyrose. Svarbiausia komunikavimo priemonė, platinant apgaulingas žinutes, yra socialinio tinklo „Facebook“ programėlė „Messenger“ (palyginti su 2023 m., naudojimasis išaugo 9 proc., o 2024 m. nustatytas atvejų skaičius yra daugiau nei 4 kartus didesnis už metinį 2020–2023 m. vidurkį). Žinutėmis dažniausiai buvo platinamos nuorodos į šias suklastotas interneto svetaines: DPD, „Omniva“, „LP Express“, skelbiu.lt, „Vinted“.

Investicinis sukčiavimas

Finansų sektoriaus dalyvių duomenimis, investicinis sukčiavimas 2024 m. išliko viena daugiausia nuostolių padariusių sukčiavimo formų. Bendra per metus prarasta suma siekė 5,57 mln. Eur, t. y. beveik 800 tūkst. Eur daugiau negu 2023 m.⁰⁸.



Investicinis sukčiavimas – vienas iš sparčiausiai progresuojančių nusikaltimų. 2024 m. šio nusikaltimo atvejų padaugėjo 17 proc., šis rodiklis daugiau nei 2 kartus didesnis už metinį tokio sukčiavimo atvejų 2020–2023 m. vidurkį. Kaip ir anksčiau, didžiąją dalį investicinio sukčiavimo atvejų sudarė apgaulingų investavimo platformų reklamos platinimas internete, išprovokavimas reklamos anketose užregistruoti kontaktinius duomenis ir skatinimas, komunikuojant telefonu ir (ar) internetu, pervesti lėšas į tariamai

08

VšĮ Pinigų plovimo prevencijos kompetencijų centro duomenys. Prieiga per internetą <https://amlcenter.lt/naujausia-analize-atskleide-apsaugoti-milijonai-bet-nuostoliai-vis-dar-milziniski/>.

investuoti skirtas sąskaitas, kurias sukčiai kontroliuoja, iš jų persiveda ir pasisavina lėšas. Kitas vis dar populiarus investicinio sukčiavimo būdas – telefoninių sukčių atakos ar apgaulingos reklamos platinimas internete, kai anksčiau nuo investicinio sukčiavimo nukentėjusiems asmenims pasiūloma tariama pagalba susigrąžinti prarastas lėšas. 2024 m. taip pat pasitaikydavo investicinio sukčiavimo atvejų, kai telefoniniai sukčiai išprovokuodavo nukentėjusiuosius melagingu reikalavimu uždaryti investicines sąskaitas, baugindami tuo, kad šias sąskaitas perėmė nusikalstamos struktūros ir naudoja neteisėtiems tikslams. Išliko tendencija, kad trečdajį investicinio sukčiavimo atvejų sudaro įrenginių, programinės įrangos valdymo ir teisės atlikti finansines operacijas sukčiams perleidimas. Sparčiai daugėja atvejų, kai sukčiai derina investicinį ir kreditinį sukčiavimą. 2024 m. atvejų, kai nukentėjusieji tariamai investavo paimtas paskolas ar tai nukentėjusiųjų vardu atliko sukčiai, padaugėjo 42 proc., šis rodiklis daugiau nei 4 kartus didesnis už metinį tokio sukčiavimo atvejų 2020–2023 m. vidurkį.

Sukčiavimas apgaulingais el. laiškais



2024 m. apgaulingų el. pašto laiškų padaugėjo 38 proc., šis rodiklis daugiau nei 2 kartus didesnis už metinį tokio sukčiavimo atvejų 2020–2023 m. vidurkį.

Apgaulingų el. pašto laiškų tikslas išliko toks pat – išprovokuoti elektroninės bankininkystės vartotojus, komercinio sandorio šalis ir darbuočių personalą.

2024 m. elektroninės bankininkystės vartotojų išprovokavimas apgaulingais el. laiškais padidėjo 43 proc., šis rodiklis daugiau nei 3 kartus didesnis už metinį tokio sukčiavimo atvejų 2020–2023 m. vidurkį. Šis sukčiavimo būdas išliko toks pats ir buvo susijęs su nuorodų platinimu, išprovokavimu suklastotose svetainėse prisijungti prie elektroninės bankininkystės paskyros ir patvirtinti apgaulingai inicijuotą pavedimą. 2024 m. apgaulingus el. laiškus platinę sukčiai dangstėsi labai skirtingų subjektų statusu: apsimetinėjo pirkėjais (palyginti su 2023 m., atvejų padaugėjo 40 proc.), VMI (palyginti su 2023 m., atvejų padaugėjo 40 proc.), bankų darbuotojais ir (ar) jų informacinių sistemų specialistais (palyginti su 2023 m., atvejų padaugėjo 22 proc.), siuntų tarnybų darbuotojais (palyginti su 2023 m., atvejų padaugėjo 84 proc.), pardavėjais ar paslaugų teikėjais (palyginti su 2023 m., atvejų padaugėjo 71 proc.), interneto paslaugų teikėjais (palyginti su 2023 m., atvejų padaugėjo 62 proc.).

Įsiterpimo į sandorio šalių elektroninį susirašinėjimą atvejų siekiant pakeisti el. laiško turinį ir mokėjimą atlikti į sukčių sąskaitą, palyginti su 2023 m., padaugėjo 8 proc. Apgaulingų el. laiškų, kai apsimetus darbovietės administracijos specialistais, finansų personalui nurodoma atlikti įstaigos lėšų pervedimą į sukčių sąskaitą, palyginti su 2023 m., padaugėjo 60 proc. Ši nusikalstama veika kelia susirūpinimą, nes pasižymi ypač didele finansine žala ir nusikaltėlių gaunama nauda.

2024 m. Lietuvos Respublikos vidaus reikalų ministerija, RRT ir Lietuvos bankas priėmė sprendimą kurti 24/7 veikiantį centrą, kuris operatyviai reaguos ir sieks užkardyti elektroninį ir telefoninį sukčiavimą. Šios institucijos taip pat sutarė, kad stiprinant viešojo ir privataus sektorių bendradarbiavimą bus kuriama bendra informavimo platforma, kurią koordinuos Lietuvos policija.

Prekės ar paslaugos įgijimas sukčiavimo būdu

2024 m. atvejų, kai sukčiavimo būdu buvo įgytos prekės ar paslaugos, padaugėjo 17 proc., tačiau šis rezultatas yra žemesnis už 2020-2023 m. metinį vidurkį, todėl situacija nepasižymi rizikingu vystymusi. Vyravo tie patys dažniausi šio sukčiavimo būdai, susiję arba su daiktų internete pardavėjų išprovokavimu išsiųsti prekę, prieš tai atsiuntus pardavėjui pranešimą apie atliktą mokėjimą ir suklastoto pavidimo kopiją, arba nuotoliniu būdu, panaudojus vogtus svetimos tapatybės duomenis, oficialiai su telekomunikacijos paslaugų operatoriais sudarytomis pirkimo išsimokėtinai sutartis. 2024 m. sukčiavimo būdu įgytos elektroninės technikos skaičiaus augimas buvo 37 proc., telekomunikacijos paslaugų - 40 proc.



Socialinės inžinerijos metodai, kuriems mažiausiai atsparūs Lietuvos gyventojai

Sukčiavimo atvejų stebėseną rodo, kad 2024 m. nusikaltėlių taikomi socialinės inžinerijos metodai nuolat kito. Siekiami sustiprinti apgaulės poveikį, nusikaltėliai stengėsi pasinaudoti įvairiais įvykiais, pavyzdžiui, rinkimais, deklaravimo periodu, nelaimėmis, paskyrų duomenų saugumo pažeidimo, duomenų nutekėjimo atvejais. 2024 m. pradžioje duomenys buvo viliojami naudojant suklastotas trumpąsias žinutes, vėliau - telefoniniais skambučiais, nes buvo pritaikytos prevencinės priemonės ir vykdoma plati informacijos sklaida. Pastebima, kad prieš sukurdami ryšį su auka nusikaltėliai išanalizuoja prieinamą informaciją, nutekina asmens duomenis, taip greičiau paveikiama gyventojų sąmonė ir pelnomas pasitikėjimas. Itin paveikus ir duomenų viliojimo būdas yra suklastotų nuorodų siuntimas el. paštu ar socialinių tinklų programėlėmis, nes gyventojai atlikdami finansines operacijas yra per daug neatidūs.



3 Tarptautinis bendradarbiavimas

Lietuvos kriminalinės policijos biuras toliau aktyviai dalyvavo Europos kovos su nusikalstamumo grėsmėmis tarpdisciplininės platformos ir Europolo analitinių projektų, susijusių su kova su nusikaltimais elektroninėje erdvėje ir sukčiavimais, veikloje. Bendradarbiaujant daug dėmesio skirta nusikaltimų elektroninėje erdvėje techninėms prevencinėms priemonėms, nes būtent jos yra labiausiai paveikios siekiant nusikaltimų prevencijos. Lietuvos policija kartu su kitų ES valstybių teisėsaugos institucijomis vystė dialogą su ES veikiančių platformų atstovais, siekdami užtikrinti vartotojų saugumą. Kartu su privataus sektoriaus partneriais sėkmingai įdiegtos papildomos apsaugos priemonės bendrose platformose, tai gerokai sumažino sukčiavimo viliojant duomenis atvejų.

Lietuvos policijos atliekamuose tyrimuose nėra nustatyta, kad progresuotų DI naudojimas nusikalstamoms veikoms vykdyti, tačiau kartu su kitomis valstybėmis nagrinėjama potenciali DI įtaka socialinei inžinerijai ir prevencinės priemonės. Kovoiant su tarptautiniu organizuotu nusikalstamumu kartu su kitų valstybių teisėsaugos institucijomis įvykdytos sėkmingos tarptautinės operacijos:

- ✓ 2024 m. gegužės mėn. Lietuvos kriminalinės policijos biuras dalyvavo Europolo koordinuojamoje operacijoje „Endgame“, skirtoje sistemoms „IcedID“, „SystemBC“, „Pikabot“, „Smokeloder“, „Bumblebee“ ir „Trickbot“ užkardyti. Per operaciją buvo sunaikinta išpirkos reikalaujančių programų ir kitos kenkimo programinės įrangos atakas palengvinusi kenkimo programinės įrangos infrastruktūra.
- ✓ 2024 m. gruodžio mėn. jungtinė Prancūzijos, Nyderlandų, Italijos, Vokietijos, Lietuvos ir Ispanijos teisėsaugos institucijų tyrimo grupė išaiškino sudėtingą šifruotos komunikacijos platformą „Matrix“. Platformoje buvo susirašinėjama ir siunčiami šifruoti pranešimai, susiję su sunkių ir labai sunkių nusikaltimų organizavimu ir darymu: tarptautine prekyba narkotikais, prekyba ginklais, pinigų plovimu ir kita organizuotų nusikalstamų grupuočių neteisėta veikla.

4 Prevencinė veikla siekiant užkirsti kelią sukčiavimui kibernetinėje erdvėje

Atsižvelgdama į didėjančius sukčiavimo mastus, 2024 m. policija aktyviai ir sistemingai vykdė įvairias priemones sukčiavimų prevencijai. Siekiant pasiekti tikslines grupes, organizuoti susitikimai su prižiūrimų teritorijų bendruomene. Informacija, kaip apsisaugoti nuo sukčiavimo elektroninėje erdvėje, kaip saugiai pirkti elektroninėje erdvėje, kaip apsisaugoti (ir išvengti) sukčiavimų, susijusių su lengvu uždabiu ir investavimu elektroninėje erdvėje, viešinta socialiniuose tinkluose ir (ar) visuomenės informavimo priemonėse. Atskira tema skirta ir vyresnio amžiaus asmenims (senjorams), kaip apsisaugoti ir netapti sukčiavimo aukomis. Organizuota daugiau kaip 1 840 informacinių susitikimų, juose dalyvavo per 96 tūkst. gyventojų.

Policija 2024 m. išleido ir socialiniams partneriams (Maltos ordino pagalbos tarnybai, Lietuvos „Caritui“, Lietuvos Raudonojo Kryžiaus draugijai, Vilniaus Švč. Mergelės Marijos Ramintojos bažnyčiai, apskričių vyriausiųjų policijos komisariatų kapelionams) perdavė dalyti visuomenei prevencinius šviečiamojo pobūdžio lankstinukus „Susisiekė sukčiai?“ (iš viso 20 tūkst. vnt., iš jų 15 tūkst. lietuvių k., po 2 500 – lenkų ir rusų kalbomis).

Informacijos sklaidą vykdė ir policijos virtualus patrulis. Siekdamas įspėti interneto vartotojus apie gresiančius pavojus dėl galimų sukčiavimų bei svarbių asmens ir kitų duomenų vagysčių elektroninėje erdvėje, policijos virtualus patrulis savo „Facebook“ paskyroje paskelbė 69 prevencinius pranešimus. Per 2024 m. virtualus policijos patrulis nustatė ir užregistravo 505 galimus teisės pažeidimus (2023 m. – 445), iš kurių dėl 26 pradėti ikiteisminiai tyrimai, dėl 355 – administracinio nusižengimo bylų teisenos, dėl 50 – asmenims buvo surengti prevenciniai pokalbiai, jie oficialiai įspėti. Virtualus policijos patrulis socialiniame tinkle „Facebook“ dėl galimų neapykantos kurstymo atvejų, viešosios tvarkos pažeidimų bei sukčiavimų viešai įspėjo 233 vartotojus. Virtualaus policijos patrulio iniciatyva užblokuotos 285 „Facebook“ paskyros ir kiti puslapiai.

Siekdama užtikrinti veiksmingą techninių prevencinių priemonių įgyvendinimą, policija toliau bendradarbiavo su privataus sektoriaus atstovais, keitėsi informacija apie tendencijas, tikslines aukų grupes, rizikas VŠĮ Pinigų plovimo prevencijos kompetencijų centro sukčiavimo prevencijos grupės veikloje bei RRT koordinuojamame formate kartu su mobiliojo ryšio operatoriais. Taip pat organizuoti susitikimai su finansinių technologijų kompanijas vienijančia asociacija „Fintech Hub LT“.

5 Policijos kompetencijos kėlimas kibernetinių nusikaltimų užkardymo srityje

Didėjant žinių, kaip atskleisti elektroninėje erdvėje įvykdytas nusikalstamas veikas, poreikiui, policija nuolat ieško būdų, kaip tobulėti ir kelti pareigūnų kvalifikaciją. Atsižvelgiant į šio pobūdžio nusikalstamų veikų daugialypiškumą, orientuojamasi tiek į bazinius pareigūnų įgūdžius atskleidžiant ir užkardant nusikalstamas veikas, tiek ir į specifines žinias. Stebint nuolatinę nusikalstamų veikimo būdų kaitą, laiku atnaujinamos programos, įtraukiama aktuali informacija, pavyzdžiui, informacija, susijusi su virtualiosios valiutos analize, DI naudojimu vykdant nusikalstamas veikas. Ypač daug dėmesio mokymuose skiriama ir tarpvalstybiniam įrodymų surinkimui, nes nemaža dalis šio tipo nusikalstamų veikų sietinos su keliomis valstybėmis. Kuriant mokymų programas bendradarbiaujama ir su Europolu. Analizuojant užsienio valstybių praktiką kvalifikacijos kėlimo srityje, nuolat vertinamos galimybės pareigūnams gilinti žinias ir tobulinti praktinius įgūdžius užsienio valstybių vykdomuose mokymuose.

Tarptautinio bendradarbiavimo atvejo, susijusio su sukčiavimu, analizė

Šiaulių apskrities vyriausiojo policijos komisariato Kriminalinės policijos nusikaltimų nuosavybei tyrimo valdyba nuo 2021 m. atlieka tyrimą, kuriame sujungti 186 ikiteisminiai tyrimai iš visos Lietuvos, apimantys 377 nusikalstamas veikas. Ikiteisminio tyrimo metu nustatytas 181 nukentėjusysis, jų patirta turtinė žala viršija 17 tūkst. Eur. Apgaulingomis SMS žinutėmis apie neva bankų sąskaitose „užšaldytus“ pinigus išprovokuota aktyvuoti nuorodą ir netikrame interneto banko puslapyje suvesti banko prisijungimo duomenis. Juos įvedus imituota operacijos klaida ir netikras interneto banko puslapis užsidarydavo. Sukčius, panaudojęs užvaldytus prisijungimo duomenis, prisijungdavo prie sąskaitos ir atlikdavo neteisėtą pinigų pervedimo operaciją. Vėliau pradėtos platinti apgaulingos SMS žinutės su pasiūlymu atšaukti tariamai neteisėtai pradėtą pavidimą iš sąskaitos aktyvuojant pridėtą nuorodą. Paspaudus nuorodą, atsidarydavo netikras banko ar VMI tinklapis. Naudodami nukentėjusiųjų banko kortelių duomenis, sukčiai perveddavo nukentėjusiųjų lėšas į kriptovaliutų platformas. Prie nukentėjusiųjų sąskaitų buvo prisijungiama iš skirtingų IP adresų, skirtingų įrenginių ir naudojantis virtualiu privačiu tinklu (VPN). Neteisėti pavidimai iš nukentėjusiųjų sąskaitų buvo atliekami į Latvijos, Lietuvos, Vengrijos piliečių vardais atidarytas „Revolut Payments“ (dabar – „Revolut Bank“) sąskaitas, „Wise“ banko belgiškas sąskaitas, „Bunq“ banko olandiškas sąskaitas, „Solaris“ banko vokiškas sąskaitas, „Pocopay“ estiškas sąskaitas, „Swedbank AS“ latviškas sąskaitas ir kriptovaliutų platformas. Tyrimo duomenys atskleidė, kad veikė didelis tarptautinis sukčių elektroninėje erdvėje tinklas, organizuojamas Lietuvoje, Latvijoje ir Suomijoje. Daugiau nei 2 metus trukęs tyrimas 2024 m. pasibaigė bendra Lietuvos, Latvijos ir Suomijos pareigūnų, taip pat koordinacinio centro „Eurojust“ operacija. Iš viso sulaikyti 8 asmenys (Lietuvoje ir Suomijoje – po 3, Latvijoje – 2). Nusikalstamos veikos organizatorius – Latvijos įkalinimo įstaigoje laisvės atėmimo bausmę atliekantis šios šalies pilietis A. S. A. S. taip pat organizavo nusikalstamu būdu gautų lėšų išgryninimą, pavidimą į įvairias sąskaitas, kriptovaliutų įgijimą, o šias finansines operacijas atliko bendrininkai Latvijos piliečiai. Atlikus pinigų pervedimo operacijas, pinigai atsidurdavo keliose sąskaitose, iš kurių jie buvo gryninami Latvijoje arba konvertuojami į kriptovaliutas. Pagrindinis techninių operacijų vykdytojas – suklastotų nuorodų kūrėjas ir siuntėjas Lietuvos pilietis D. E. Nukentėjusiųjų telefonų numerių sąrašus jis gaudavo iš tamsiojo interneto arba iš Latvijos piliečio A. S. Apgaulingas žinutes D. E. platino naudodamasis interneto programėlėmis, skirtomis masiškai SMS siųsti. D. E. visus neteisėtus veiksmus atliko naudodamasis virtualiąja mašina, todėl jo kompiuteryje neišliko jokių nusikalstamos veiklos pėdsakų. Iš Lietuvos piliečio D. E. per poėmį policijos žinion perimta įvairios kriptovaliutos, jos vertė siekia 185 tūkst. Eur. Lietuvoje sulaikytiems 3 asmenims pareikšti įtarimai dėl 377 nusikalstamų veikų įvykdymo.



Asmens duomenų apsauga, saugumo užtikrinimas ir pažeidimų prevencija

Vadovės žodis



Dijana Šinkūnienė,
VDAI direktorė

Asmens duomenų apsauga, saugumo užtikrinimas ir pažeidimų prevencija yra svarbiausi VDAI prioritetai, siekiant užtikrinti ne tik teisėtą, bet ir etišką duomenų naudojimą. Organizacijos vis dažniau naudoja naujas technologijas, todėl ypač svarbu išlaikyti aukštą saugumo lygį ir prisitaikyti prie besikeičiančių reikalavimų.

Pažeidimų prevencija yra svarbi ir būtina, nes grėsmės tampa vis kompleksiškesnės. Periodinis su saugumu susijusių rizikų vertinimas, nuolatinis darbuotojų švietimas padeda išvengti klaidų ir užtikrina, kad organizacijos veiktų pagal aukščiausius saugumo ir teisėtumo standartus.

Suprasdama organizacijų lūkesčius, VDAI 2024 m. savo veiklą organizavo taip, kad būtų nuosekliai stiprinamos duomenų valdytojų, duomenų apsaugos pareigūnų ir duomenų subjektų žinios, ugdoma kompetencija ir įgūdžiai asmens duomenų apsaugos srityje.



KĄ SAUGO?

- ✓ Žmogaus teisę į asmens duomenų apsaugą.

VDAI veikla orientuojama į:

fizinius asmenis – siekiama užtikrinti kiekvieno žmogaus teisę į asmens duomenų ir privatumo apsaugą;

viešojo ir privataus sektoriaus organizacijas – teikiamos konsultacijos ir prižiūrima, kaip organizacijos tvarko asmens duomenis, siekdamas užtikrinti teisės aktų laikymąsi.



NUO KO SAUGO?

- ✓ Nuo su duomenų apsauga susijusių grėsmių ir neteisėtų piktavalių veiksmų.

Piktavaliai:

- kibernetiniai nusikaltėliai (programišiai, įsilaužėliai ir sukčiai, vykdytys duomenų vagystes, atliekantys kitus kenkėjiškus veiksmus);
- asmens duomenų vagys ir sukčiai (asmens, neteisėtai renkantys, naudojantys ar parduodantys asmens duomenis).



KAIP SAUGO?

- ✓ Atlikdama organizacijų asmens duomenų tvarkymo ir saugumo užtikrinimo stebėseną ir patikrą.
- ✓ Nagrinėdama pranešimus apie ADSP ir atlikdama tyrimus.
- ✓ Teikdama organizacijoms išankstines konsultacijas, kai tvarkant duomenis galėtų kilti didelis pavojus, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti.
- ✓ Atlikdama asmens duomenų tvarkymo auditus valstybės informacinėse sistemose, kai tai numato ES teisės aktai.
- ✓ Atlikdama asmens duomenų tvarkymo auditus valstybės informacinėse sistemose, kai tai numato ES teisės aktai.
- ✓ Skatindama sąmoningumą teikiant metodinę pagalbą.



VALSTYBINĖ
DUOMENŲ
APSAUGOS
INŠPEKCIJA



Svarbiausi 2024 m. įvykiai ir tendencijos



2024 m. VDAI gavo 7 proc. daugiau pranešimų apie ADSP negu 2023 m. (2024 m. – 273, 2023 m.– 254).



Lietuvoje paveiktų duomenų subjektų skaičius – 1 467 368. Šis skaičius padidėjo beveik 3 kartus (2023 m. – 571 833), tai lėmė didesnis ADSP, įvykusių dėl kibernetinių incidentų, skaičius, buvo paveikta daug duomenų subjektų.



Pagal ADSP pobūdį Lietuvoje statistiškai vyrauja konfidencialumo pažeidimai, jie sudarė net 87 proc. visų atvejų.



2024 m. ADSP dėl kibernetinių incidentų įvyko 18 proc. daugiau negu 2023 m. (2024 m. – 33 proc., 2023 m. – 15 proc.).



33 proc. visų ADSP įvyko dėl kibernetinių incidentų, buvo paveikti 49 proc. duomenų subjektų (iš visų paveiktų subjektų) duomenys.



Dažniausios kibernetinių incidentų priežastys: perimti naršyklėse išsaugoti prisijungimo duomenys – 27 proc., nepakankamai išmokytas personalas – 18 proc., kelių veiksnių autentifikavimo metodo netaikymas – 10 proc.



Duomenų valdytojai VDAI pranešė apie duomenų užšifravimo ir išpirkos reikalavimo atakas, neteisėtas prieigas prie IT sistemų, socialinės inžinerijos ir duomenų viliojimo bei prisijungimo duomenų užpildymo (angl. *Credential Stuffing*) atakas.



Duomenų valdytojams dėl ADSP taikytos poveikio priemonės: 1 administracinė bauda (9 tūkst. Eur), 18 nurodymų ir 38 rekomendacijos.



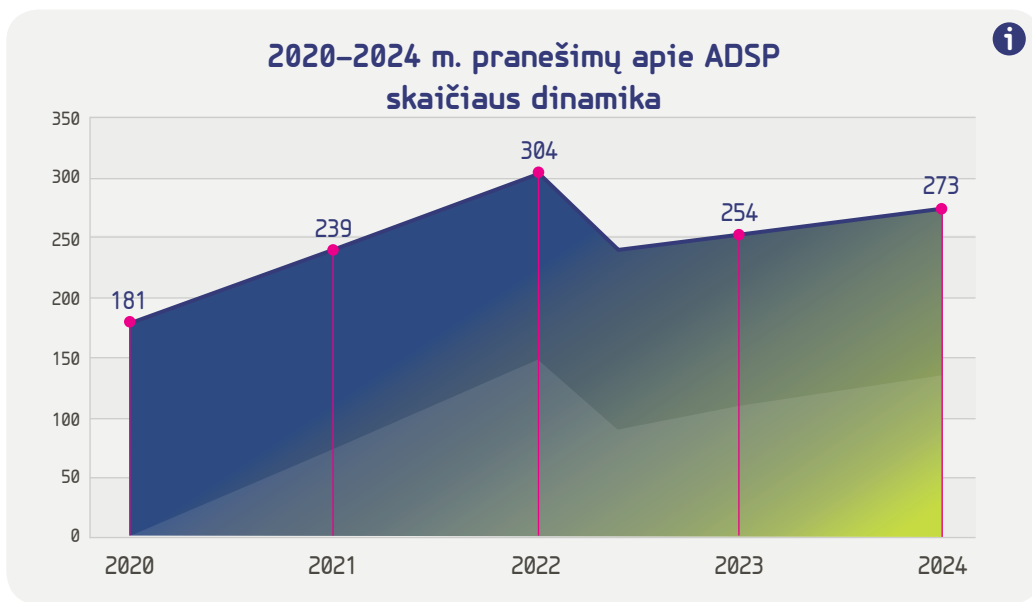
ADASL Lietuvoje siekė 63 proc.



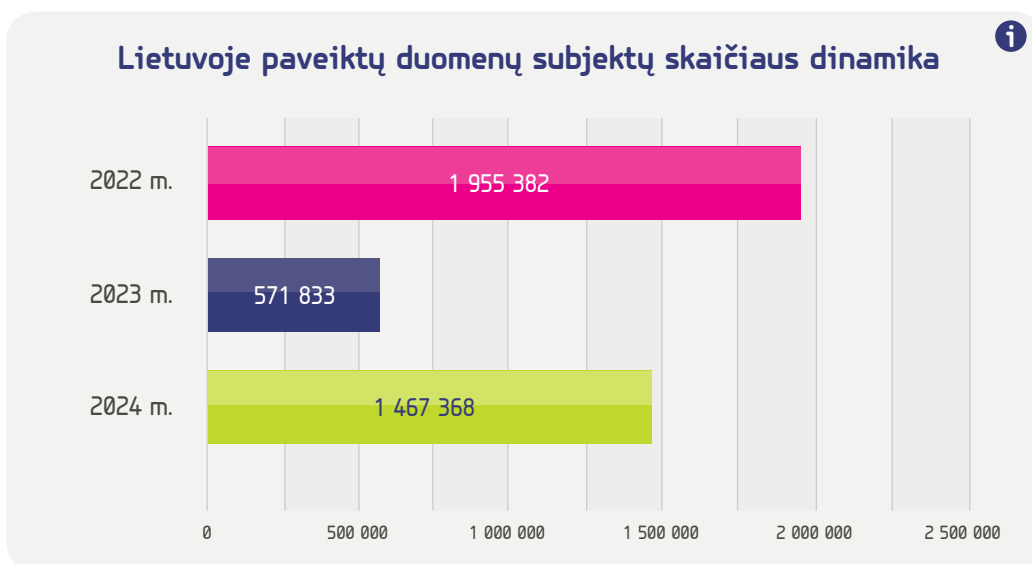
VDAI organizuojamuose šviečiamuosiuose renginiuose dalyvavo daugiau nei 7 000 dalyvių, parengti 25 metodiniai dokumentai.

1 ADSP Lietuvoje situacijos analizė

Apžvelgiant 2024 m. pranešimų apie ADSP Lietuvoje statistiką, paminėtina, kad gauti 273 pranešimai apie ADSP, Lietuvoje paveiktų duomenų subjektų skaičius – 1 467 368 (žr. 1 pav.) Palyginti su ankstesnių metų duomenimis, 2024 m. VDAI gavo 7 proc. daugiau pranešimų apie ADSP (2023 m. – 254). Lietuvoje paveiktų duomenų subjektų skaičius padidėjo beveik 3 kartus, palyginti su 2023 m. (2023 m. – 571 833), tai lėmė didesnis ADSP, įvykusių dėl kibernetinių incidentų, skaičius, buvo paveikta daug duomenų subjektų (žr. 2 pav.).

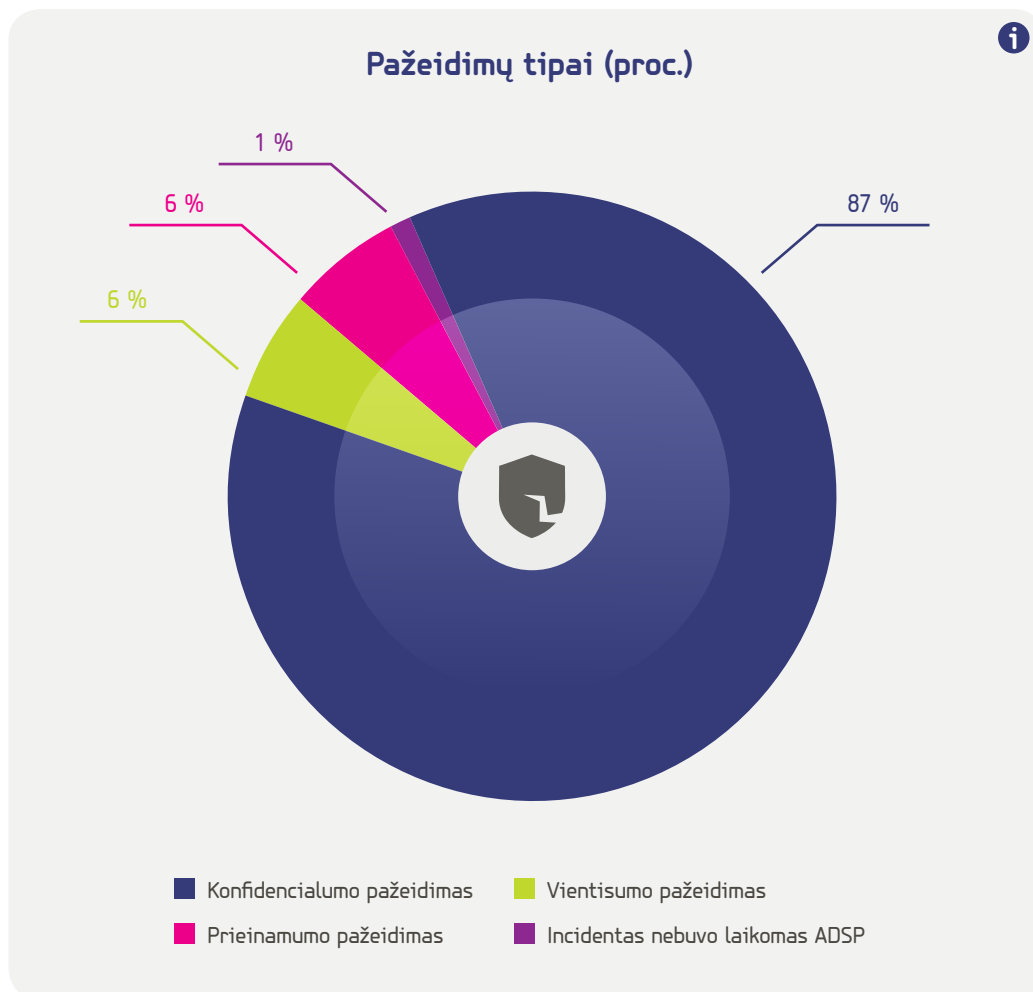


< 1 pav. 2020–2024 m. pranešimų apie ADSP skaičiaus dinamika (šaltinis – VDAI)



< 2 pav. Lietuvoje paveiktų duomenų subjektų skaičiaus dinamika (šaltinis – VDAI)

Pagal ADSP pobūdį Lietuvoje statistiškai vyrauja konfidencialumo pažeidimai, jie sudarė net 87 proc. visų atvejų, 6 proc. atvejų sudarė vientisumo pažeidimai, dar 6 proc. atvejų – prieinamumo pažeidimai ir 1 proc. atvejų nebuvo laikomi ADSP (neatitiko sąvokos) (žr. 3 pav.).



< 3 pav.

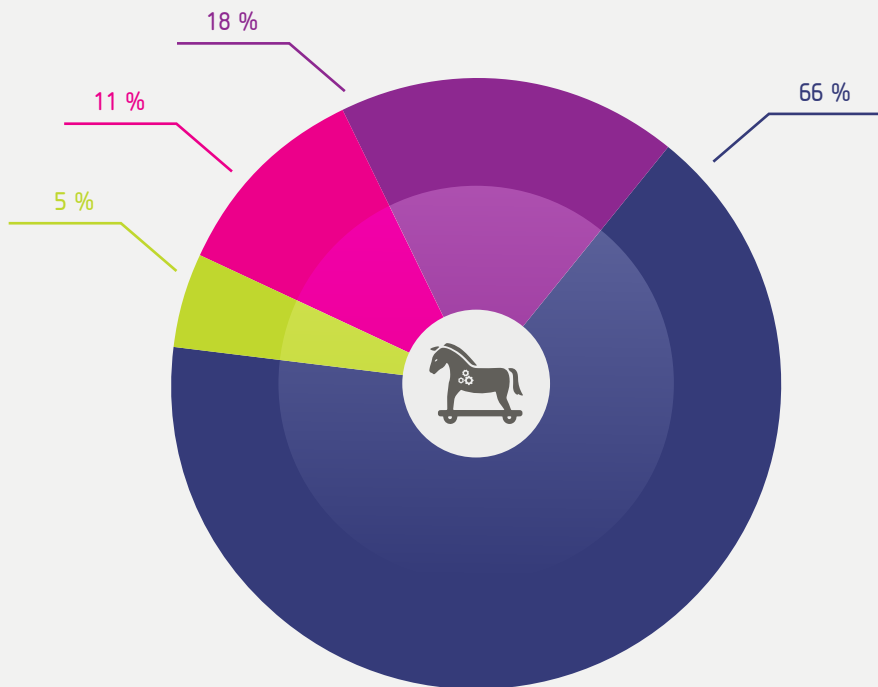
Pažeidimų tipai (proc.)
(Šaltinis – VDAI)

VDAI, išanalizavusi 2024 m. gautus pranešimus apie ADSP, nustatė, kad 33 proc. ADSP įvyko dėl kibernetinių incidentų (iš jų 11 proc. – dėl duomenų užšifravimo ir išpirkos reikalavimo atakų, 66 proc. – dėl neteisėtai gautos prieigos prie IT sistemų, 18 proc. – dėl socialinės inžinerijos metodais paremtų atakų ir 5 proc. – dėl prisijungimo duomenų užpildymo kibernetinių atakų (žr. 4 pav.)). 52 proc. ADSP įvyko dėl žmogiškosios klaidos⁰¹, 15 proc. – dėl kitų priežasčių (žr. 5 pav.).

01

ADSP įvyksta dėl žmogaus neapdairumo, nežinojimo, kad veiksmai gali sukelti ADSP, taip pat dėl veiksmų, nuo kurių įprastai apsaugoti negali taikomos techninės ir organizacinės priemonės, pavyzdžiui, el. pašto adresų įrašymas į eilutę „Kopija“ (angl. *Carbon Copy*, CC), o ne į „Nematoma kopija“ (angl. *Blind Carbon Copy*, BCC), dokumentų su asmens duomenimis siuntimas netinkamiems adresatams, netinkamai nuasmeninto dokumento paviešinimas ir kt.

Kibernetinių incidentų tipai (proc.)

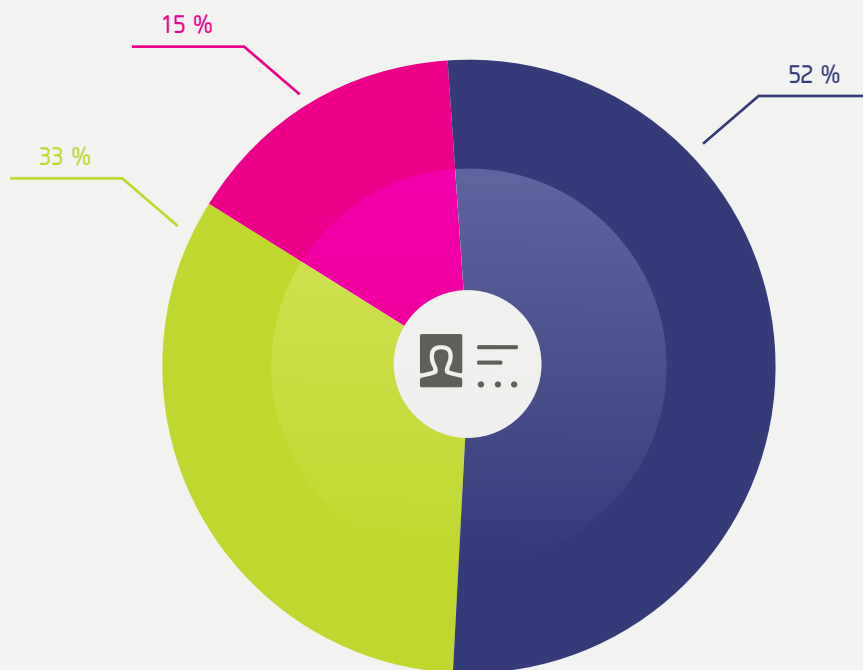


- Neteisėtos prieigos prie IT sistemų
- Socialinės inžinerijos metodais paremtos atakos
- Prisijungimo duomenų užpildymo atakos
- Duomenų užšifravimo ir išpirkos reikalavimo atakos

< 4 pav.

Kibernetinių incidentų tipai (proc.) (šaltinis – VDAI)

ADSP priežastys (proc.)



- Žmogiškoji klaida
- Kibernetinis incidentas
- Kitos priežastys

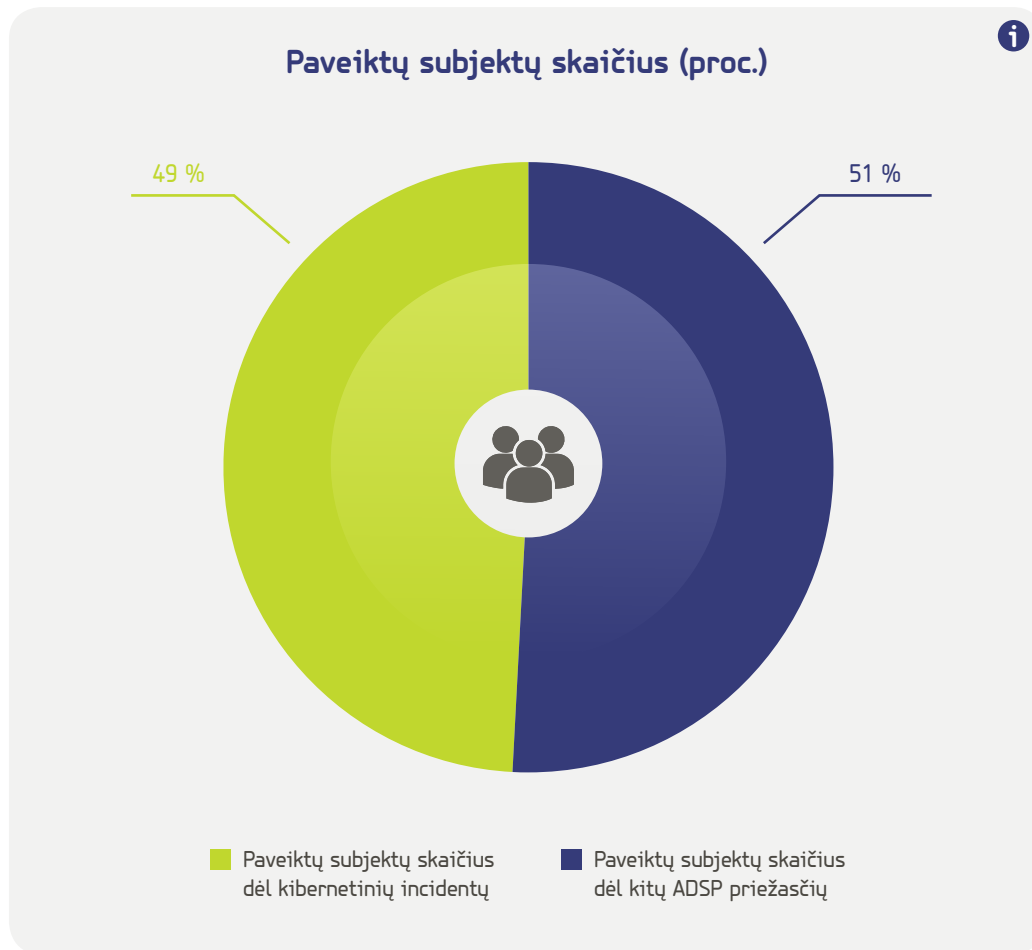
< 5 pav.

ADSP priežastys (proc.) (šaltinis – VDAI)

Pažymėtina, kad VDAI vis daugiau gauna pranešimų apie ADSP dėl įvykusių kibernetinių incidentų. Taikydami socialinės inžinerijos ir duomenų viliojimo metodus, piktavaliai išvengia kelių veiksmų autentifikavimo. Priežastys – darbuotojai nėra tinkamai išmokyti atpažinti kenkimo laiškus, paspaudžiamos gautos kenkimo nuorodos, atsisiunčiami priedai, suvedami ne tik prisijungimo duomenys, bet ir papildomas autentifikatorius, pavyzdžiui, telefono slaptažodis.

Duomenų valdytojai turi užtikrinti, kad būtų taikomos ne tik tinkamos techninės priemonės, kurios padėtų apsaugoti duomenų subjektų asmens duomenis, bet ir organizacinės⁰², pavyzdžiui, nuolatinis darbuotojų švietimas (mokymai, pratybos), kad darbuotojai, gavę kenkimo laiškus, juos atpažintų ir neatidarinėtų kenkimo nuorodų ar kitų priedų.

Svarbu paminėti, kad dėl kibernetinių incidentų buvo paveikti 49 proc. (712 881) duomenų subjektų (iš visų 2024 m. paveiktų subjektų) duomenys, dėl kitų priežasčių – 51 proc. (754 487) duomenų subjektų duomenys (žr. pav. 6).



< 6 pav.

Paveiktų subjektų skaičius (proc.) (šaltinis – VDAI)

02

Kibernetinio saugumo reikalavimų aprašas, standartas ISO/IEC 27002:2022 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“, Valstybinės duomenų apsaugos inspekcijos 2024 m. rugpjūčio 13 d. Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams.



Duomenų valdytojams taikytos poveikio priemonės

2024 m. VDAI, atlikusi ADSP ir kibernetinio incidento tyrimą, priėmė sprendimą skirti 9 tūkst. Eur. baudą viešojo sektoriaus organizacijai už nustatytus BDAR nuostatų pažeidimus. Dėl netinkamai vykdomos prieigų kontrolės ir autentifikavimo nebuvimo prisijungta prie įstaigos serverių ir užšifruoti duomenys. Kadangi nebuvo daromos serverių atsarginės kopijos, įstaigai vykdyti veiklą tapo sunkiau.

Įvertinusi gautus pranešimus apie ADSP ir nustačiusi, kad netinkamai užtikrinamas duomenų subjektų asmens duomenų saugumas, VDAI, vadovaudamasi teisės aktų nuostatomis, pateikė duomenų valdytojams arba duomenų tvarkytojams 18 nurodymų suderinti duomenų tvarkymo operacijas su BDAR nuostatomis. Taip pat pateiktos 38 rekomendacijos, kurios konkrečiais atvejais padės užtikrinti atitiktį BDAR reikalavimams.

2 ADASL Lietuvoje

Nuo 2021 m. VDAI, remdamasi reprezentatyvios Lietuvos gyventojų apklausos duomenimis, skaičiuoja ADASL Lietuvoje. ADASL yra sudėtinis rodiklis, nustatomas iš atsakymų į 10 apklausos klausimų. Klausimai apima 4 sritis: gyventojų žinias, pasitikėjimą įmonėmis ir įstaigomis dėl asmens duomenų tvarkymo, elgesį susidūrus su pažeidimais ir pasitikėjimą priežiūros sistema.

Lietuvoje 2024 m. ADASL siekė 63 proc. (2022 m. – 60 proc., 2023 m. – 64 proc.) (ADASL siektina reikšmė 2030 m. yra 70 proc.).

Asmens duomenų apsaugos reikalavimus geriau išmananti visuomenė deda daugiau pastangų ir gali tinkamai rūpintis savo asmens duomenų apsauga ir to paties reikalauti iš organizacijų. Atsižvelgdama į tai, informuotumo didinimą VDAI laiko vienu iš veiklos prioritetų.

3 Mokymo ir švietimo veikla

2024 m. VDAI užtikrino kasdieninių konsultacijų gyventojams ir organizacijoms poreikį. Iš viso suteiktos 4 334 konsultacijos, daugiausia dėl BDAR ir kitų asmens duomenų apsaugos teisės aktų taikymo, VDAI kompetencijos, taip pat dėl asmens duomenų tvarkymo teisėtumo ir duomenų subjektų teisių įgyvendinimo.

2024 m. VDAI, bendradarbiaudama su NKSC ir Lietuvos policija, aktyviai dalyvavo nacionalinėse kibernetinio saugumo pratybose „Kibernetinis skydas OpEx 2024“. VDAI, kaip priežiūros institucija, duomenų valdytojams teikė pastabas ir rekomendacijas dėl pranešimų apie ADSP, kad ateityje įvykus tikriems ADSP duomenų valdytojais gebėtų imtis tinkamų taisomųjų veiksmų.

Taip pat duomenų apsaugos pareigūnams, organizacijoms ir visuomenei, bendradarbiaujant su NKSC, surengti nuotoliniai mokymai įvairiomis asmens duomenų apsaugos ir kibernetinio saugumo temomis. Mokymų įrašų nuorodas galima rasti VDAI svetainėje. VDAI organizuojamuose šviečiamuosiuose renginiuose dalyvavo daugiau nei 7 000 dalyvių.

VDAI, siekdama didinti visuomenės švietimą asmens duomenų apsaugos temomis, 2024 m. paskelbė 25 metodinius dokumentus (juos galima rasti VDAI svetainėje). Paminėtini šie svarbiausi su asmens duomenų saugumo užtikrinimu susiję metodiniai dokumentai:

- ✓ Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams⁰³ (atnaujinta);
- ✓ Patarimai, kaip elgtis, jei paviešinti vartotojų prisijungimo duomenys⁰⁴;
- ✓ Rekomendacija dėl saugių ir stiprių slaptažodžių naudojimo svarbos (duomenų valdytojams)⁰⁵;
- ✓ DUK. Įsilaužimai į interneto svetaines – kaip reikėtų elgtis⁰⁶ (atnaujinta);
- ✓ Rekomendacija dėl asmens duomenų ir privatumo apsaugos naudojantis belaidžiais tinklais⁰⁷ (atnaujinta).

Tikimasi, kad šios iniciatyvos prisidės prie asmens duomenų apsaugos ir kibernetinio saugumo stiprinimo, visuomenės ir organizacijų sąmoningumo didinimo ir sudarys sąlygas efektyviau spręsti su duomenų apsauga susijusias problemas.



03

<https://vdai.lrv.lt/lt/naujienos/valstybine-duomenu-apsaugos-inspekcija-atnaujino-tvarkomu-asmens-duomenu-saugumo-priemoniu-ir-rizikos-ivertinimo-gaires-duomenu-valdytojams-ir-duomenu-tvarkytojams/>.

04

<https://vdai.lrv.lt/lt/naujienos/vdai-pataria-paviesinti-vartotoju-prisijungimo-duomenys-kaip-elgtis/>.

05

https://vdai.lrv.lt/public/canonical/1734937137/678/Rekomendacija_del_slaptazodziu_2024.pdf.

06

https://vdai.lrv.lt/public/canonical/1734955549/687/12_23_Isilauzimai_i_svetaines_DUK.pdf.

07

https://vdai.lrv.lt/public/canonical/1734950980/686/ASMENS%20DUOMENU%20IR%20PRIVATUMO%20APSAUGA%20NAUDOJANTIS%20WIFI_2024.pdf.

Priešiškos informacinės aplinkos vertinimas



Vadovo žodis

Šiuolaikiniai konfliktai nebeapsiriboja tik kariniais veiksmais, jais taip pat siekiama paveikti žmonių mąstymą, nuostatas ir elgesį. 2024 m. Rusijai tęsiant karą prieš Ukrainą, ir toliau darytas informacinis spaudimas Lietuvai ir NATO. Nedraugiškos valstybės siekia mus priversti pasiduoti dar neišaušus dienai X, pateikdamos Lietuvą kaip žlugusią valstybę, kurios neverta ginti, sukelti abejonę sąjungininkų patikimumu, o šiuos veiksmus savo auditorijai teisina menama grėsme iš Lietuvos ir kitų Baltijos šalių ar Aljanso. LK SKD stebi ir analizuoja tokią informacinę veiklą, deda pastangas stiprinti visuomenės atsparumą priešišky šalių propagandai.

Kmd. Giedrius Valintėlis,
LK SKD direktorius



KAŲ SAUGO?

- ✓ Nacionalinę ir NATO informacinę erdvę gynybos tema.



NUO KO SAUGO?

- ✓ Nuo priešišky valstybių ir organizacijų vykdomų informacinių operacijų.



KAIP SAUGO?

- ✓ Stebėdamas ir analizuodamas informacinę erdvę, rengdamas ataskaitas, pranešimus spaudai, bendradarbiaudamas su žiniasklaida, taip pat su kitomis nacionalinėmis institucijomis (NKVC) ir tarptautiniais partneriais (NATO), įskaitant ir dvišalį bendradarbiavimą.



LIETUVOS KARIUOMENĖS
STRATEGINĖS KOMUNIKACIJOS
DEPARTAMENTAS



kariuomene.lt



info@mil.lt



+370 618 26 857



Svarbiausi 2024 m. įvykiai ir tendencijos



Didžiausias informacinių grėsmių prieš Lietuvą ir šalies strateginius interesus šaltinis – Rusijos ir Baltarusijos režimų pareigūnai, šių valstybių politinė ir karinė vadovybė ir režimo kontroliuojami žiniasklaidos atstovai.



Rusija ir Baltarusija tęsia informacinį spaudimą Lietuvai ir kitoms Baltijos šalims ir NATO. Daug dėmesio skiriama Rusijos karui prieš Ukrainą, NATO ir Rusijos santykiams, paramai Ukrainai ir Lietuvos pastangoms stiprinti šalies karinius pajėgumus.



Priešiški informaciniai veikėjai dažniausiai melagingą informaciją skleidė gynybos temomis.



Priešiškoje informacinėje aplinkoje 2024 m. daug dėmesio skirta įvykiams, susijusiems su parama Ukrainai.



Daug dėmesio susilaukė Lietuvos pastangos stiprinti šalies gynybinius pajėgumus. Priešiški informaciniai veikėjai itin jautriai reagavo į kontrmobilumo priemonių parkų atidarymą ir Rūdninkų karinio miestelio statybų pradžią.



NATO ir Lietuvos kariuomenės pratybos buvo itin daug dėmesio sulaukusi tema. Tam įtakos turėjo didžiausios nuo Šaltojo karo laikų NATO pratybos „Steadfast Defender“ ir Lietuvoje vykusios pratybos, pavyzdžiui, „Geležinis Vilkas 2024“.



Priešiškuose informaciniuose kanaluose (angl. *Hostile information channels*) nevengota Baltijos šalis ar NATO apkaltinti dėl kai kurių Ukrainos veiksmų.



2024 m. fiksuoti propagandininkų bandymai pasitelkti ir mažų, ir didesnių resursų reikalaujančias priemones.



1 Informacinės aplinkos grėsmių tendencijos

Nors priešiška informacinė veikla prieš Lietuvą vykdoma ne vienerius metus, ji itin suintensyvėjo 2024 m. dėl besitęsiančios Rusijos agresijos Ukrainoje ir dezinformacijos taikinyje atsidūrė Lietuvos parama Ukrainai.

2024 m. daugiausia vyravo įprasti naratyvai, pavyzdžiui, NATO yra agresyvus karinis blokas, o Lietuva – rusofobiška valstybė. Taip pat priešiški informaciniai veikėjai, susiję su Rusijos ar Baltarusijos režimais ir (arba) jų kontroliuojami, stengėsi sumenkinti Lietuvos pastangas stiprinti šalies gynybinius pajėgumus ir Vokietijos brigados dislokavimo reikšmę.

Atsižvelgiant į dabartinę geopolitinę situaciją, paminėtini nauji naratyvai, pavyzdžiui:



- ⚠ NATO parama Ukrainai, įskaitant naikintuvų F-16 perdavimą, neturės įtakos karo eigai;
- ⚠ Lietuvoje ir Lenkijoje rengiami diversantai perversmui Baltarusijoje sukelti ir A. Lukašenkos režimui nuversti;
- ⚠ NATO šalys siekia atidaryti antrąjį frontą Baltarusijoje ir (ar) Kaliningrade;
- ⚠ NATO šalys yra įsitraukusios į karinę operaciją Kurske;
- ⚠ Lietuvos kariuomenės ir NATO pratybos yra puolamojo pobūdžio;
- ⚠ Lietuvos karinio pajėgumo stiprinimas – tai rengimasis sąjungininkų valstybių (Rusijos ir Baltarusijos) puolimui.

2024 m. išryškėjo nauja tendencija – bauginimo ir grasinimo atvejai informacinėje erdvėje. Palyginti su 2023 m., padažnėjo pranešimų apie Trečiąjį pasaulinį arba branduolinį karą.

2024 m. Seimas pratęsė draudimą retransliuoti ir platinti internete Rusijoje ar Baltarusijoje įsteigtų, tiesiogiai ar netiesiogiai valdomų, kontroliuojamų ar finansuojamų įmonių radijo ir televizijos programas. Tačiau priešiškos valstybės randa spragų ir kitų būdų transliuoti propagandinį turinį.

Socialiniuose tinkluose platinti suklastoti dokumentai (pavyzdžiui, krašto apsaugos ministro įsakymas), kuriuose neva kalbama apie Lietuvos karių siuntimą į Ukrainą. Taip pat propagandiniuose kanaluose bandyta sukurti neigiamą požiūrį į Lietuvą, Baltarusijos naujienuose kanaluose transliuoti „dokumentiniai“ filmai. Paminėtinas buvusios Baltarusijos opozicijos atstovės O. Tiškevič interviu naujienu kanalui ONT, kuriame ji teigė, kad Lietuvoje rengiami diversantai A. Lukašenkos režimui nuversti.

Šiai dezinformacijai įtaką taip pat darė virsmo technologijos. Jos leidžia imituoti Lietuvos institucijų dokumentus ir skleisti įtikinamo turinio melagienas socialiniuose tinkluose.

Rusijos dezinformacija vykdoma trimis kryptimis – ji skirta Vakarų, Rusijos ir Lietuvos auditorijoms:



Vakarams bandoma įteigti, kad Lietuvos neverta ginti, kad Lietuva nėra vakarietiška šalis ir neturi demokratiškas vertybių, o yra artima Rusijai;



savo auditorijai bandoma įteigti, kad Lietuva yra priešiška valstybė Rusijai, Lietuvos kariuomenė nepakankamai gera, joje vyrauja revanšistinės nuotaikos;



Lietuvos auditorijai bandoma įteigti, kad Lietuva nėra verta, kad ją gintų NATO, taip bandoma silpninti visuomenės valią gintis.

2024 m. priešiškų režimų kontroliuojamuose kanaluose ypač daug dėmesio skirta gynybos sektoriaus temoms. Propagandininkai ir priešiškų režimų pareigūnai pabrėžtinai rodė Lietuvą ir (ar) NATO kaip agresores, kurių veiksmai nukreipti prieš Rusiją ir (arba) Baltarusiją, o Lietuvos ir (arba) Aljanso siekis stiprinti savo saugumą buvo pateikiamas kaip rengiamasis kariniams veiksams prieš sąjunginę valstybę. Ypač suaktyvėjo informacinis spaudimas, susijęs su Lietuvos gynybinių pajėgumų stiprinimu (Rūdninkų karinio miestelio statybų pradžia, kontrmobilumo priemonių parkų atidarymu), NATO ir (ar) Lietuvos kariuomenės pratybomis („Steadfast Defender“, „Narsus Grifonas 2024-II“), parama Ukrainai (diskusijos dėl karių siuntimo į Ukrainą, naikintuvų F-16 perdavimas, leidimas Ukrainai ilgojo nuotolio raketomis smogti Rusijos gilumoje).

Pagrindinis Rusijos ir Baltarusijos siunčiamų pranešimų apie Lietuvą ir NATO tikslas – skatinti nepasitikėjimą savo valstybe, jos institucijomis ir vieni kitais, poliarizuoti visuomenę. Taip bandoma paveikti ir Vakarų demokratiškas valstybių stabilumą, ir piliečių gebėjimą priimti sprendimus. Šiam tikslui pasiekti Rusija Vakaruose naudoja visas įmanomas priemones ir tam skiria daug lėšų. Atviruose šaltiniuose minima, kad 2025 m. šiam tikslui planuojama skirti bent 1,5 mlrd. dolerių oficialių išlaidų, neįtraukiant slaptųjų tarnybų ir slaptų operacijų kaštų. Pagrindinis Rusijos propagandos uždavinys – sukurti neišvengiamai blogos baigties atmosferą.

Tikėtina, kad 2025 m. informacinis spaudimas neatslūgs, o priešiškų valstybių kontroliuojami ar jų įtaką patiriantys informaciniai veikėjai toliau sieks diskredituoti Lietuvos kariuomenę ir NATO bei pateisinti savo veiksmus fiziniame erdvėje kaltindami „kolektyvinius Vakarus“. Tam tikro Rusijos propagandos suaktyvėjimo galima tikėtis prieš šiais metais rudenį prasidedant pratyboms „Zapad“.

2 Bendradarbiavimas su partneriais ir visuomenės informavimas

LK SKD itin sėkmingai bendradarbiavo su kitomis informacinės erdvės stebėseną vykdančiomis krašto apsaugos sistemos institucijomis ir NKVC. Šis bendradarbiavimas suteikė galimybę greitai ir efektyviai keistis informacija apie priešišką informacinę veiklą, pavyzdžiui, apie dezinformacinio pobūdžio pranešimus ir informacines operacijas prieš Lietuvą ir šalies strateginius interesus.

LK SKD nuolat informuoja visuomenę, nacionalines institucijas ir sąjungininkus apie priešišką informacinę veiklą. Kiekvieną mėnesį leidžiamos mėnesinės apžvalgos, o naujų metų pradžioje skelbiama informacinės aplinkos vertinimo ataskaita. Joje pristatomos pagrindinės priešiškos informacinės veiklos prieš Lietuvą ir šalies strateginius interesus tendencijos.

Užsienio partneriai taip pat dalijasi tyrimais, ataskaitomis, susijusiomis su dezinformacijos analize. Paminėtinas NATO Strateginės komunikacijos kompetencijų centras (angl. *NATO Strategic Communications Centre of excellence* (NATO StratCom CoE))⁰¹ ir 2024 m. jo publikuoti itin aktualių tyrimų, pavyzdžiui, „Rusijos informacinės įtakos operacijos Šiaurės ir Baltijos šalių regione“⁰², „(Ne)šauti pranešėjo: psichologinė reakcija į Kremliaus naratyvus Šiaurės ir Baltijos šalių auditorijose“⁰³, „Socialinės žiniasklaidos manipuliavimas pardavimui: eksperimentas apie platformų gebėjimus atpažinti ir kovoti su neautentišku socialinės žiniasklaidos įsitraukimu“⁰⁴, rezultatai.

2024 m. LK SKD organizavo įvairius informacinius mokymus švietimo institucijose (mokyklose, universitetuose), valstybės ir savivaldybių institucijose, nevyriausybines organizacijose, verslo organizacijose. Pagrindinės mokymų temos: „Propaganda, dezinformacija ir priešiškos informacinės operacijos Lietuvoje. Kaip išlikti budriems?“, „Istorinė atmintis – informacinio karo taikiklyje“.



01

Prieiga per internetą
<https://stratcomcoe.org/>.

02

„Rusijos informacinės įtakos operacijos Šiaurės ir Baltijos šalių regione“. Prieiga per internetą <https://stratcomcoe.org/publications/russia-information-influence-operations-in-the-nordic-baltic-region/314>.

03

„(Ne)šauti pranešėjo: psichologinė reakcija į Kremliaus naratyvus Šiaurės ir Baltijos šalių auditorijose“. Prieiga per internetą <https://stratcomcoe.org/publications/dont-shoot-the-messenger-psychological-responses-to-kremlin-narratives-in-nordic-baltic-audiences/315>.

04

„Socialinės žiniasklaidos manipuliavimas pardavimui: eksperimentas apie platformų gebėjimus atpažinti ir kovoti su neautentišku socialinės žiniasklaidos įsitraukimu“. Prieiga per internetą <https://stratcomcoe.org/publications/social-media-manipulation-for-sale-experiment-on-platform-capabilities-to-detect-and-counter-inauthentic-social-media-engagement/311>.

Rezonansiniai atvejai

Baltarusijos KGB vadovo pareiškimas dėl Minską atakavusių dronų iš Lietuvos

2024 m. balandžio 25 d. Baltarusijos KGB vadovas Ivanas Tertelis visuotiniame Baltarusijos liaudies susirinkime pareiškė, kad buvo užkirstas kelias dronų atakai iš Lietuvos, kurios pagrindinis taikinys – Minskas. I. Tertelis taip pat pabrėžė, kad Lietuvoje ir Lenkijoje yra globojami radikalai, kurie gamina dronus planuojamoms atakoms prieš objektus Baltarusijoje.

Melagingi pranešimai apie Lietuvos karių siuntimą į Ukrainą socialiniuose tinkluose

Nuo gegužės 23 d. iki gegužės 26 d. socialiniuose tinkluose išplatinta netikra apklausa dėl pozicijos Lietuvos karių dalyvavimo kariniuose konfliktuose kitų valstybių teritorijoje klausimu. Sufabikuotas ir krašto apsaugos ministro įsakymas dėl karių siuntimo į Ukrainą. Oficialioje Ukrainos prezidento interneto svetainėje buvo paskelbta melaginga peticija, kad Vakarų šalių kariai yra kviečiami į Ukrainą priešintis Rusijos agresijai. Melagingai teigta, kad iškart po šios peticijos paskelbimo Lietuvos karių artimi giminaičiai pradėjo gauti pranešimus su reikalavimu paremti karių siuntimą į Ukrainą.



NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA 2024

Išleido Lietuvos Respublikos krašto apsaugos ministerija,
Totorių g. 25, LT-01121 Vilnius, www.kam.lt
2025-05-27. Užsakymas Nr. GL-264

Dizaineris Andrej Garbar
Kalbos redaktorė Inga Šorienė
Naudotos iliustracijos iš Freepik.com grafinio archyvo

Maketavo Krašto apsaugos ministerijos bendrųjų reikalų departamento
Vaizdinės informacijos skyrius, Totorių g. 25, LT-01121 Vilnius

Leidinio bibliografinė informacija pateikiama
Lietuvos nacionalinės Martyno Mažvydo bibliotekos
Nacionalinės bibliografijos duomenų banke (NBDB).

ISSN 2783-7009

© Lietuvos Respublikos krašto apsaugos ministerija
Atgaminti leidžiama nurodžius šaltinį.

