



KRAŠTO APSAUGOS  
MINISTERIJA

# NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA **2023**



Viršelis sukurtas  
dirbtinio  
intelekto (DI)



# NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA **2023**



KRAŠTO APSAUGOS  
MINISTERIJA

# Turinys



ĮŽANGA \06



SANTRAUKA \08



KIBERNETINIO SAUGUMO POLITIKOS FORMAVIMAS \16


- KAM veikla stiprinant Lietuvos pasirengimą reaguoti į įvairias grėsmes ir kibernetinės erdvės saugumą \17
- ES gynybos iniciatyvų naudojimas bendradarbiavimui ir projektų finansavimui \19
- KAM veikla plėtojant tarptautinį bendradarbiavimą kibernetinio saugumo srityje \20
- Dalyvavimas formuojant ir įgyvendinant ES kibernetinio saugumo politiką \22
- Kibernetinė gynyba yra viena esminių NATO atgrasymo ir gynybos užduočių \24



LIETUVOS KIBERNETINIO SAUGUMO BŪKLĖS APŽVALGA \26

Lietuvos kibernetinės erdvės apžvalga: incidentų dinamika ir prevencinės priemonės, skirtos kibernetiniam atsparumui stiprinti \27

- Svarbiausi 2023 m. įvykiai ir tendencijos \28
- Kibernetinio saugumo grėsmės ir rizikos \29
  - Išorinės aplinkos vertinimas \29
  - Vidinės aplinkos vertinimas \29
- Kibernetinių incidentų dinamika \32
  - Elektroninius duomenis užšifruojantys ir išpirkos reikalaujantys kenkimo programinio kodo virusai \34
  - DDoS atakos \35
  - Tiekimo grandinių atakos \35
  - Socialinė inžinerija ir duomenų viliojimas \35

 Dominančią temą galite pasiekti paspaudę ant jos pavadinimo

- Kibernetinio saugumo stiprinimas \36
  - Kenkimo interneto svetainių užkardymas \36
  - Kibernetinio saugumo kompetencijų ugdymas \37
  - Išmoktos karo Ukrainoje pamokos \38
  - Nacionaliniam saugumui užtikrinti svarbių objektų apsauga \38
  - Atsakingas kibernetinio saugumo spragų atskleidimas \38
  - Kibernetinio saugumo patikrinimai \39
  - NATO viršūnių susitikimas Vilniuje \39
- NKSC 2024 m. prioritetai \39

Asmens duomenų apsauga, saugumo užtikrinimas ir pažeidimų prevencija \42

- Svarbiausi 2023 m. įvykiai ir tendencijos \43
- Asmens duomenų saugumo pažeidimų Lietuvoje situacijos analizė \44
- Asmens duomenų apsaugos sąlygų lygis \49
- Tarptautinio bendradarbiavimo iniciatyvos ir mokymo bei švietimo veiklos \51

Nusikalstamų veikų kibernetinėje erdvėje mastas ir poveikis \54

- Svarbiausi 2023 m. įvykiai ir tendencijos \55
- Tarptautinė situacija \56
- Nacionalinė situacija \57
  - Kibernetiniai nusikaltimai siaurąja prasme \59
  - Kibernetiniai nusikaltimai plačiąja prasme \67
- Tarptautinis bendradarbiavimas \72
- Prevencija \73
- Mokymai \73

Elektroninių ryšių tinklų vientisumo užtikrinimas ir draudžiamos viešai skleisti informacijos internete užkardymas \74

- Svarbiausi 2023 m. įvykiai ir tendencijos \75
- Viešųjų ryšių tinklų vientisumo užtikrinimas Lietuvoje \76
- Interneto karštosios linijos „Švarus internetas“ veikla \78
- RRT dalyvavimas tarptautiniame projekte „Arachnid“ \80
- Viešųjų kompiuterių tinklų (internetu) prieigos vietose privalomų filtravimo priemonių naudojimo užtikrinimas \80
- Vartotojų apsauga nuo žalingų interneto nuorodų, apsimestinių SMS žinučių ir skambučių \82

RRT paskirta kvalifikuotos elektroninės atpažinties paslaugos teikėjų priežiūros įstaiga \82

Edukacinė veikla \83

### Priešiškos informacinės aplinkos apžvalga ir Lietuvos informacinės aplinkos saugumo vertinimas \84

Informacinės aplinkos grėsmių tendencijos \85

Fiksuoti informaciniai incidentai gynybos srityje \86

Fiksuoti informaciniai incidentai užsienio politikos srityje \87

Fiksuoti informaciniai incidentai konstitucinių pagrindų apsaugos srityje \88



# 01

## Įžanga



**Laurynas Kasčiūnas,**  
krašto apsaugos  
ministras

2023-ieji – tai metai, kuriuos pasitikome stipresni, atsparesni ir jau išmokę dalį karo Ukrainoje pamokų. Nuo 2022-ųjų vasario 24 d. mes ne tik matėme Rusijos išpuolių Ukrainoje žiaurumą, ne tik teikėme karinę ir kitokią paramą besiginančiai nuo okupantų šaliai, bet ir stropiai mokėmės.

Mokėmės, kaip informacinė erdvė panaudojama dezinformacijai skleisti prieš prasidedant atviram kariniam įsiveržimui, kaip ir koku mastu pasitelkiamos šiuolaikinės technologijos ir programinė įranga puolimui kibernetinėje erdvėje.

Įsitikinome, kad šiuolaikiniai konfliktai peržengia fizinės valstybių sienas ir apima beribę kibernetinę erdvę. Drąsiai galime teigti, kad šiame – skaitmeniniame – amžiuje informacinės technologijos yra vienas iš pagrindinių įrankių, kuriuo įgyvendinamos priešiškos valstybių ir organizacijų politinės, ekonominės ir karinės ambicijos. Ne tik Ukrainoje, bet ir Izraelyje matėme įvairių grupuočių kibernetines atakas kaip sudedamąją kinetinio konflikto dalį, kaip dar vieną būdą siekti savo iškreiptos pasaulėžiūros tikslų ir trikdyti civilizuotų žmonių gyvenimą.

Didėjančios geopolitinės diktatoriškų ir teroristinių valstybių ambicijos, didėjančios kibernetinių incidentų skaičiai, priešiškos valstybių remiamos kibernetinės atakos, informaciniai karai kelia rimtą grėsmę ne tik mūsų informacinei infrastruktūrai, bet ir nacionaliniam saugumui. Sparti technologijų, tokių kaip dirbtinis intelektas, plėtra suteikia ne tik naujų galimybių, bet kartu tampa ir galingu įrankiu piktavalių rankose. Todėl būtina stiprinti kibernetinį saugumą, kurti geresnes kibernetinės gynybos strategijas ir bendradarbiauti tarptautiniu lygiu.

Dėl aktyvios paramos Ukrainai Lietuva išliko su Kremliumi siejamų grupuočių taikinyje. Todėl džiaugiuosi, kad 2023 m. Lietuvos kibernetinio saugumo būklės ataskaitoje atsispindi mūsų, kaip visuomenės ir kaip valstybės, kibernetinės brandos pokyčiai. Palyginti su ankstesniais metais ir nepaisant intensyvesnės nusikaltėlių veiklos, bendras registruotų incidentų skaičius sumažėjo 30 proc., nors pavojingesnių incidentų skaičius šiek tiek didėjo. Matome ir tai, kad didėja organizacijų atsparumas kibernetinėms grėsmėms, tačiau tikiu, kad dar turime kur pasitempti ir privalome judėti sparčiau stiprindami savo virtualios erdvės gynybą.

Todėl noriu palinkėti visiems, kas skaitys šią ataskaitą, išlikti budriems, kritiškai mąstantiems, savo šalį mylintiems ir puoselėjantiems piliečiams. Tikiu, kad kiekvienas iš mūsų, vadovaudamasis šiais principais savo kasdienėje veikloje, prisideda prie atsparesnės ir saugesnės Lietuvos tiek fizinėje, tiek ir virtualioje erdvėje.



**Greta Monika Tučkutė,**  
krašto apsaugos  
viceministrė

Pristatome jau aštuntąją Nacionalinės kibernetinio saugumo būklės ataskaitą. Metinėje apžvalgoje pateikiame praėjusių metų pagrindinius įvykius, pasiekimus ir kibernetinio saugumo būklės tendencijas. 2023 m. kibernetinės grėsmės Lietuvoje, kaip ir visame regione, kėlė Rusijos karas Ukrainoje, programišių grupuočių, siejamų su Rusija ir Kinija, kenkimo veikla bei virsmo technologijų, tokių kaip dirbtinis intelektas, kvantinės technologijos, sparti plėtra ir naudojimas.

2022-ųjų antrosios pusės dirbtinio intelekto sprendimus, tokius kaip didieji kalbos modeliai, žinome visi. Šis ir kiti dirbtinio intelekto įrankiai vis plačiau naudojami įvairiose srityse, ne išimtis ir kibernetinio saugumo ar gynybos sektoriai. Pavyzdžiui, dirbtinis intelektas gali labai padėti aptikti kibernetines atakas, tirti ir rūšiuoti incidentus, ypač greitai ir tiksliai nustatyti kenkimo el. laiškus ar kitas sukčiavimo priemones. Kita vertus, visais šiais dirbtinio intelekto privalumais naudojasi ir piktavaliai, remiami priešiškos valstybių, ir nusikaltėliai. Ir nors kol kas nėra fiksuota incidentų, kuriuos išskirtinai vykdytų dirbtinis intelektas, tačiau jo panaudojimas kuriant socialinės inžinerijos ir dezinformacijos atakas vis labiau auga – tampa labai sudėtinga pastebėti ir atskirti tikras žinutes nuo sukčių atakų.

2023 m. Lietuvoje fiksuota gerėjanti kibernetinio saugumo situacija įvairiose srityse, pavyzdžiui Valstybinė duomenų apsaugos inspekcija 2023 m. gavo mažiau pranešimų apie asmens duomenų saugumo pažeidimus nei 2022 m., registruotų nusikalstamų veikų elektroninėje erdvėje, palyginti su 2022 m., sumažėjo 26 proc., o Nacionalinis kibernetinio saugumo centras 2023 m. fiksavo beveik trečdaliu mažesnį registruotų incidentų skaičių nei 2022 m. Tačiau vis tik matome ir nerimą keliančių ženklų: didėja vidutinio rimtumo incidentų skaičius (12 proc. prieaugis, palyginti su 2022 m.), o dėl kibernetinių incidentų įvykę asmens duomenų saugumo pažeidimai paveikė didelę dalį (net 49 proc.) subjektų. Vadinas, atakos tampa subtilesnės ir efektyvesnės.

Kaip ir visoje Europoje, Lietuvoje 2023 m. didžiausią grėsmę kėlė elektroninius duomenis užšifruojančios ir išpirkos reikalaujančios programinio kodo atakos, taip pat paskirstytų paslaugų trikdymo atakos, tiekimo grandinės atakos bei socialinės inžinerijos atakos, kuriomis siekiama išvilioti jautrius duomenis.

Įvertindamos geopolitinę įtampą regione, virsmo technologijų naudojimo rizikas, valstybės institucijos imasi visų būtinų ir neatidėliotinių priemonių, siekdamos užkirsti kelią kibernetinėms grėsmėms. Priimta nacionalinė kibernetinio saugumo plėtros programa, stiprinami valstybės nacionaliniai kibernetinio saugumo pajėgumai įgyvendinant TIS2 direktyvą, plėtojamas tarptautinis bendradarbiavimas su bendramintėmis šalimis, Lietuvos kariuomenėje steigama Kibernetinės gynybos valdyba bei taikomos kitos Lietuvos kibernetinio atsparumo didinimo priemonės. Noriu padėkoti visoms institucijoms, kurios bendradarbiaudamos su Nacionaliniu kibernetinio saugumo centru prisideda prie saugesnės kibernetinės erdvės kūrimo ir šios ataskaitos rengimo.

Kviečiu visus neabejingus Lietuvos saugumui ir gerovei dirbti kartu, pagal savo galimybes prisidėti prie nacionalinio kibernetinio saugumo užtikrinimo ir visuomenės kibernetinės brandos stiprinimo. Tam tinka viskas – ir individualūs mokymai, kuriuose Jūs gilinate savo kibernetinio saugumo žinias, ir Jūsų darbas kuriant pažangias ir saugas technologijas ir remiant mūsų ir sąjungininkų pajėgumus, ir sąžiningai ir dėmesingai atliekamos pareigos bet kurioje kitoje srityje. Ir, žinoma, nepamirškime atnaujinti ne tik savo žinių, bet ir programinės įrangos!





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

### 1. Krašto apsaugos ministerijos (toliau – KAM) veikla kibernetinio saugumo politikos formavimo srityje buvo nukreipta į nacionalinių kibernetinio saugumo pajėgumų stiprinimą.



2023 m. KAM kartu su kitomis suinteresuotomis institucijomis siekė nustatyti konkrečias priemones, kuriomis tikslingai spręstų 2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinėje kibernetinio saugumo plėtros programoje (toliau – Plėtros programa) identifiкуotą problemą – didintų dėl pasikeitusių kibernetinių grėsmių pobūdžio ir augančio jų masto nepakankamą šalies kibernetinį atsparumą. Siekiant šio tikslo, 2023 m. rugsėjo 20 d. Lietuvos Respublikos Vyriausybės nutarimu buvo patvirtinta Plėtros programa. Pagrindinis Plėtros programos finansavimo šaltinis – Ekonomikos gaivinimo ir atsparumo didinimo planas „Naujos kartos Lietuva“. Plėtros programoje numatytais priemonėmis bus siekiama, atsižvelgiant į 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)<sup>01</sup>, reikalavimus, patobulinti Kibernetinio saugumo įstatyme dar nuo 2014 m. įtvirtintą kibernetinio saugumo modelį, atnaujinti kibernetinio saugumo reikalavimus ir sustiprinti jų įgyvendinimo stebėseną, vystyti kibernetinių nusikaltimų tyrimo infrastruktūrą ir ugdyti tyrėjų kompetencijas, daugiau dėmesio skirti visuomenės ir smulkaus bei vidutinio verslo atstovų kibernetinio saugumo žinių lygio kėlimui bei praktiniams įgūdžiams, stiprinti bendradarbiavimą tarp viešojo ir privataus sektoriaus.

2023 m. buvo pradėti intensyvūs TIS 2 direktyvos perkėlimo į nacionalinę teisę darbai: pradėtas rengti Lietuvos Respublikos kibernetinio saugumo įstatymo pakeitimo įstatymo projektas. TIS 2 direktyvą įgyvendinančius teisės aktus planuojama priimti iki 2024 m. spalio 17 d.

KAM 2023 m. priimtas sprendimas Lietuvos kariuomenėje įsteigti struktūrinį padalinį – Kibernetinės gynybos valdybą. Naujo vieneto Lietuvos kariuomenėje sukūrimas padės planuoti ir vykdyti krašto apsaugos sistemos kibernetinės erdvės gynybines operacijas. Tai leis vykdyti jungtinį visų operacinių domenų karinį planavimą ir koordinuoti užduočių vykdymą kibernetinėje erdvėje.

Nacionaliniam saugumui užtikrinti ypač svarbi kibernetinėms atakoms atspari ypatingos svarbos infrastruktūra. Dar nuo 2022 m. balandžio mėn. įsigaliojo teisės aktai, užtikrinantys, kad kritinėje infrastruktūroje, įskaitant 5G infrastruktūrą, būtų naudojama tik patikimų gamintojų įranga. 2023 m. KAM toliau tęsė darbus šioje srityje: atnaujino Viešojo pirkimo objektų, kuriuos įsigyjant būtų keliami su nacionalinio saugumo užtikrinimu susiję reikalavimai, sąrašą ir dar kartą paragino visas atsakingas institucijas, veikiančias nacionaliniam saugumui užtikrinti svarbiose srityse, organizuoti nepatikimų gamintojų įrangos pašalinimą ir pakeitimą patikima iki 2025 m. sausio 1 d.

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>.



## 2. Didėjant geopolitinei įtampai pasaulyje, KAM stiprina tarptautinį bendradarbiavimą kibernetinio saugumo ir gynybos srityse.

Kibernetinio saugumo iššūkių ir rizikų Europos bei Indijos ir Ramiojo vandenynų regionuose daugėja. Siekdama efektyviau reaguoti į regionines grėsmes, Lietuva aktyviai dalyvauja tarptautinių organizacijų iniciatyvose ir užmezga glaudžius ryšius su bendramintėmis valstybėmis.

KAM toliau glaudžiai bendradarbiavo su strategine partnere – JAV. 2023 m. gruodį pasirašytas JAV gynybos departamento ir KAM 2024–2028 m. bendradarbiavimo gynybos srityje planas. Vienas šio plano prioritetų – bendradarbiavimas kibernetinio saugumo ir gynybos srityje. Tad JAV Pensilvanijos nacionalinės gvardijos (angl. *Pennsylvania National Guard* (PANG)) specialistai drauge su Lietuvos atstovais iš Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) ne tik dalyvavo bendruose mokymuose ir pratybose, bet ir dalijosi informacija apie kibernetines grėsmes bei rengė jas analizuojančias studijas. KAM ir NKSC specialistai 2023 m. toliau dalyvavo JAV Baltųjų rūmų organizuojamoje tarptautinėje „Iniciatyvoje prieš išpirkos reikalaujančias atakas“ (angl. *Counter Ransomware Initiative* (CRI)), skirtoje valstybių ir tarptautinių organizacijų pastangoms suvienyti kovojant su išpirkos reikalaujančiomis kibernetinėmis atakomis.

KAM tęsia ES nuolatinio struktūrizuoto bendradarbiavimo projekto „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“ (toliau – PESCO CRRT projektas) koordinavimą: 2023 m. priimtos 3 naujos ES valstybės narės – Belgija, Slovėnija ir Danija, pirmą kartą dalyvauta remiant ES bendros saugumo ir gynybos politikos mokymo misiją Mozambike, kurioje Kibernetinės greitojo reagavimo pajėgos Europos išorės veiksmų tarnybos (EIVT) kvietimu atliko kibernetinio pažeidžiamumo vertinimą. Projektas jau vienija 9 ES valstybes nares ir tampa patirties bei praktinio bendradarbiavimo platforma.

2023 m. užmegztas glaudesnis bendradarbiavimas kibernetinio saugumo srityje su bendramintėmis Indijos ir Ramiojo vandenynų regiono šalimis – Japonija, Australija, Pietų Korėja, Singapūru, Taivanu – bus tęsiamas ir toliau. Paminėtinas ir pirmą kartą Lietuvoje surengtas aukšto lygio NATO, Indijos ir Ramiojo vandenynų regiono ir partnerių šalių kibernetinio saugumo forumas „Cyber Champions Summit“, tai buvo gretutinis NATO viršūnių susitikimo 2023 m. Vilniuje renginys. KAM kartu su NKSC surengtame forumo „Cyber Champions Summit“ NATO sąjungininkių ir stipriausių vienminčių partnerių aukšto lygio ekspertai diskutavo apie kibernetinio saugumo tendencijas ir bendradarbiavimo galimybes, dalijosi patirtimis, kaip atremti kibernetines atakas ir reaguoti į grėsmes kylančias iš Rusijos ir Kinijos.

2023 m. krašto apsaugos sistemos atstovai toliau efektyviai teikė įvairią pagalbą Ukrainos kibernetinio saugumo ir gynybos pajėgumams: tiekė techninę ir programinę įrangą, organizavo mokymus Ukrainos kibernetinio saugumo specialistams, kartu analizavo Rusijos karo prieš Ukrainą išmoktas pamokas. Taip pat Lietuva kartu su kitomis Ukrainos gynybos kontaktinės grupės (Ramšteino formatas) šalimis prisijungė prie informacinių technologijų (toliau – IT) koalicijos, kurios tikslas – teikti paramą ir stiprinti Ukrainos kibernetinės gynybos pajėgumus.



## 3. KAM atstovai aktyviai dalyvavo formuojant ir įgyvendinant ES kibernetinio saugumo politiką, formuodami Lietuvos pozicijas dėl Europos Sąjungos teisėkūros iniciatyvų.

Europos Sąjungos kibernetinio saugumo darbotvarkė 2023 m. koncentruota į ES teisėkūros pasiūlymų kibernetinio saugumo srityje derinimą su valstybėmis narėmis. Kibernetinio atsparumo aktas, Kibernetinio saugumo akto pakeitimas ir Kibernetinio solidarumo aktas – tai ES teisėkūros paketas, inicijuotas Europos Komisijos. Šiomis naujomis teisėkūros iniciatyvomis numatoma dar labiau sustiprinti ES ir jos valstybių narių kibernetinį saugumą.

Kibernetinio atsparumo aktas, kuriam buvo pritarta 2023 m. gruodžio mėn., įsigalios 2024 m. pirmoje pusėje. Remiantis reglamento nuostatomis, gamintojai (taip pat importuotojai ir platintojai) privalės užtikrinti, kad į ES rinką teikiami produktai su skaitmeniniais elementais būtų saugūs atitinkamą laikotarpį (ne mažiau kaip 5 metus), o atsiradus pažeidžiamumų – pranešti atitinkamoms ES institucijoms, nacionalinėms priežiūros įstaigoms ir reagavimo į kompiuterinius saugumo incidentus tarnyboms. Kiekvienas subjektas, teikiantis skaitmeninius produktus į ES rinką, bus atsakingas už įsipareigojimus, susijusius su jų kokybe, pavyzdžiui, už aptiktų pažeidžiamumų šalinimą, programinės įrangos atnaujinimą, produktų auditą ir sertifikavimą.

Kibernetinio saugumo akto pakeitimu siekiama į ES sertifikavimo sistemą įtraukti naują reguliavimo objektą – valdomas saugumo paslaugas, kurias sudaro reagavimas į kibernetinius incidentus, pažeidžiamumų skenavimas, kibernetinio saugumo auditai.

Kibernetinio solidarumo aktu siekiama skatinti ES valstybių narių bendradarbiavimą kibernetinėje srityje tiek pritaikant prevencines priemones, tiek ištikus didelio masto kibernetinėms krizėms, tiek atsikuriant po incidentų. Vienas šio akto tikslų – įsteigti ES masto saugumo operacijų centrų (angl. *security operation centre*, SOC) tinklą, ES kibernetinio saugumo rezervą (angl. *EU Cybersecurity Reserve*), kurį sudarytų patikimi privataus sektoriaus subjektai.

## 4. Didžiausią poveikį Lietuvos kibernetinio saugumo aplinkai darė geopolitiniai ir naujausių technologijų plėtros veiksniai.



NKSC vertinimu, 2023 m. didelę įtaką šalies kibernetinei aplinkai darė naujausių technologijų (dirbtinis intelektas (toliau – DI), generatyvusis dirbtinis intelektas (toliau – GDI) plėtra ir jų poveikis plačiajai visuomenei bei geopolitiniai veiksniai. Lietuva dėl aktyvios paramos Ukrainai išliko su Kremliumi siejamų pažangių ir tęstinių kibernetinių grėsmių grupuočių (angl. *Advanced Persistent Threat*, APT) taikinyje.

2023 m. NKSC registravo 2 378 kibernetinius incidentus. Palyginti su ankstesniais metais, bendras registruotų incidentų skaičius sumažėjo 30 proc., tačiau 12 proc. augo pavojingesnių – vidutinės kategorijos incidentų skaičius. Daugiausia kibernetinių incidentų buvo fiksuota 2023 m. liepos-rugsėjo mėn.

Sektoriai, kuriuose buvo fiksuota daugiausia incidentų, išlieka tie patys, kaip ir ankstesniais metais. 2023 m. daugiausia incidentų įvyko interneto prieglobos paslaugų infrastruktūroje (angl. *hosting*), antroje vietoje – viešojo administravimo sektoriuje, trečioje vietoje – interneto paslaugų teikėjų infrastruktūroje ir prie jos prijungtuose fizinių asmenų galiniuose įrenginiuose.



Didžiausią žalą pagal kibernetinių atakų tipus ir metodus, NKSC duomenimis, 2023 m. darė elektroninius duomenis užšifruojančių ir išpirkos reikalaujančių kenkimo programinio kodo virusai (angl. *ransomware*), paskirstytų paslaugų trikdymo atakos (angl. *Distributed Denial of Service*, DDoS) (toliau – DDoS), tiekimo grandinės<sup>02</sup> atakos (angl. *Supply Chain Attacks*) ir socialinės inžinerijos principais sukurtos atakos, kuriomis siekiama išvilioti įvairius jautrius duomenis (angl. *Social Engineering, phishing*).

## 5. NKSC mato teigiamą organizacinių ir techninių kibernetinio saugumo priemonių poveikį organizacijų kibernetiniam atsparumui, tačiau to nepakanka.

Siekdamas įvertinti organizacijų kibernetinio atsparumo lygį, NKSC periodiškai vertina organizacinių ir techninių priemonių taikymą ypatingos svarbos informacinę infrastruktūrą (toliau – YSII)<sup>03</sup> valdančiose organizacijose.

Organizacinių reikalavimų (pavyzdžiui, patvirtintina kibernetinio saugumo politika, ją įgyvendinantis standartai, procedūros ir kt.) įgyvendinimas YSII 2023 m. augo 10 proc., palyginti su 2022 m. duomenimis. Daugiau finansinių, žmogiškų resursų ir kompetencijų reikalaujančių techninių saugumo priemonių įgyvendinimas šiose organizacijose 2023 m. padidėjo 7 proc.

NKSC skatina visas organizacijas, net tik YSII, savanoriškai savo veikloje taikyti organizacines ir technines kibernetinio saugumo priemones, nes jos gerokai mažina riziką patirti kibernetines atakas, užtikrina organizacijos veiklos tęstinumą ir mažina kibernetinių incidentų sukeltą žalą.

Siekdamas surinkti objektyvią informaciją apie YSII būklę, 2023 m. NKSC atliko arba koordinavo 17 įvairaus tipo išsamių patikrinimų, iš jų 14 buvo vykdomi bendradarbiaujant su Europos Sąjungos kibernetinio saugumo agentūra (angl. *European Union Agency for Cybersecurity*) (toliau – ENISA) bei jos įgaliotais paslaugų teikėjais iš verslo sektoriaus. Dvylikoje organizacijų, kurios valdo YSII arba valstybės informacinius išteklius, buvo atliekamas informacinių sistemų, tinklo atsparumo įsilaužimams testavimas.

2023 m. NKSC Lietuvoje nustatė 1 963 potencialiai kritinių saugumo spragų turinčias ryšių ir informacines (toliau – RIS) sistemas. Atsakingi pranešėjai aptiko 74 kibernetinio saugumo spragas įvairiose Lietuvos informacinėse sistemose ir laikydamiesi atsakingo kibernetinių spragų atskleidimo proceso reikalavimų apie jas pranešė NKSC. Nors pažeidžiamų RIS savininkai operatyviai šalino pažeidžiamumus, NKSC mato, kad organizacijos vis dar neskiria pakankamai dėmesio savo valdomų RIS gyvavimo ciklo užtikrinti.

## 6. NKSC 2023 m. daug dėmesio skyrė organizacijų ir visuomenės kibernetinio saugumo kompetencijų stiprinimui bei taikė efektyvias Lietuvos kibernetinį atsparumą didinančias priemones.

Nuolatinis kibernetinių kompetencijų ugdymas yra viena iš svarbiausių valstybės atsparumo kibernetinėms grėsmėms didinimo priemonių. 2023 m. NKSC ypač daug dėmesio skyrė kibernetinio saugumo mokymams ir pratyboms. NKSC organizuotus įvairaus tipo teorinius mokymus baigė daugiau kaip 11,5 tūkst. asmenų. 2023 m. pabaigoje NKSC pradėjo rengti ir nuotolinius mokymus, skirtus tiek paprastiems naudotojams, tiek organizacijų vadovams susipažinti su pagrindinėmis kibernetinio saugumo rizikomis.

02

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

03

YSII – tai ryšių informacinė sistema ar jos dalis, ryšių informacinės sistemos grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams.

Įgytas teorines žinias organizacijos ir jų personalas galėjo patikrinti NKSC organizuotose nacionalinėse kibernetinio saugumo pratybose „Kibernetinis skydas“. Pratybų rezultatai rodo didėjančią dalyvių kibernetinę brandą, nes beveik trečdaliu išaugo skaičius organizacijų, kurios pratybose ne tik žinojo, kaip tinkamai reaguoti į kibernetinį incidentą, bet ir pateikė reikiamą informaciją NKSC. 2023 m. tokių organizacijų buvo 76 (2022 m. – 54).

Siekdamas padėti organizacijoms ir gyventojams apsaugoti nuo žaibiškų sukčiavimo atakų ir kitų kenkimo interneto svetainių poveikio, NKSC 2023 m. toliau tobulino jų apsaugai skirtus įrankius – interneto domenų vardų sistemos (angl. *Domain Name System* (DNS)) užkardą (toliau – DNS užkarda) ir blokuojamų domenų valdymo priemonę „Vasaris“. Visos šios priemonės, įteisinamos teisės aktais ir taikomos kartu su kompetentingomis kitomis Lietuvos institucijomis, leido reikšmingai sumažinti kibernetinio saugumo grėsmes.

## 7. Ryšių reguliavimo tarnybos (toliau – RRT) nustatytas įpareigojimas operatoriams taikyti NKSC žalingų nuorodų blokavimo užkardą, taip pat įtvirtintos sukčiavimo skambučiais ir vardinėmis SMS žinutėmis užkardymo priemonės, vykdyta žalingo turinio šalinimo iš interneto veikla darė didelę įtaką vaikų ir nepilnamečių apsaugai internete bei kibernetinės erdvės saugumui.



RRT vertinimu, 2023 m. viešųjų ryšių tinklų vientisumo pažeidimų skaičius ir mastas yra panašus kaip ir ankstesniais metais. Tad nors ir buvo fiksuoti gedimai viešojo mobiliojo ir viešojo fiksuotojo ryšio tinkluose, jie pašalinti operatyviai, o viešųjų ryšių tinklų vientisumo pažeidimų mastas nesukėlė ekstremalių įvykių, dėl kurių būtų reikėję imtis papildomų veiksmų ir (ar) informuoti kitas institucijas teisės aktų nustatyta tvarka.

RRT siekia, kad vartotojai, ypač vaikai ir nepilnamečiai, būtų apsaugoti nuo žalingo turinio internete.

2023 m. RRT interneto karštąją liniją ([www.svarusinternetas.lt](http://www.svarusinternetas.lt)) gavo 65 proc. daugiau pranešimų (tai sudarė 2 516 pranešimų) apie internete rastą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją nei 2022 m. Deja, didelę pasitvirtinusių pranešimų dalį (669 atvejai) sudarė informacija dėl vaikų seksualinio išnaudojimo, t. y. tokių atvejų buvo 2,5 karto daugiau nei 2022 m. (272). RRT vertinimu, šį skaičių nulėmė atsakingas asmenų požiūris į internete rastus vaikų seksualinio išnaudojimo vaizdus. Kita nerimą kelianti tendencija – didėjantis patyčių ir smurto kibernetinėje erdvėje (angl. *cyberbullying*) atvejų skaičius socialiniuose tinkluose.

RRT rūpinasi, kad visose prieigos prie viešųjų kompiuterių tinklų (internetu) vietose, kur gali lankytis ir naršyti internete nepilnamečiai, būtų įdiegtos privalomos, RRT aprobuotos, neigiamą poveikį nepilnamečių vystymuisi darančios informacijos filtravimo priemonės. 2023 m. RRT prioritetą teikė tiems viešųjų kompiuterių tinklų (internetu) taškams, kur gali lankytis ir internete naršyti išskirtinai didelis skaičius nepilnamečių, proaktyviai skatino tokias įstaigas diegti ir naudoti privalomas filtravimo priemones, dalijosi gerosios praktikos pavyzdžiais ir patarimais.

RRT 2023 m. antrą pusmetį priimti teisės aktai, kuriais operatoriai buvo įpareigoti taikyti NKSC žalingų interneto nuorodų blokavimo įrankį – DNS užkardą, mažino nusikalstamumą elektroninėje erdvėje. Taip pat didelį poveikį Lietuvos gyventojų saugumui kibernetinėje erdvėje turėjo operatorių įpareigojimas aptikti ir blokuoti apgaulingus skambučius ir vardines SMS žinutes.





## 8. Lietuvoje 2023 m. buvo fiksuotas sumažėjęs nusikalstamumas elektroninėje erdvėje, tačiau fiziniai asmenys ir toliau išlieka dažniausiai pažeidžiama grupė, kuri nukenčia nuo sukčių.

Nors pasaulinė situacija rodo, kad nusikaltimai elektroninėje erdvėje sparčiai tampa pelningu „verslu“ ir įvairiose pasaulio vietose kyla geopolitinė įtampa, Lietuvoje 2023 m. fiksuotas registruotų nusikalstamų veikų elektroninėje erdvėje mažėjimas: nusikalstamų veikų elektroninėje erdvėje, palyginti su 2022 m., sumažėjo 26 proc. ir jos neturėjo įtakos registruoto nusikalstamumo augimui šalyje. Lietuvos policija pažymi, kad 2023 m. antrą pusmetį Lietuvoje įgyvendinus tarpinstitucinio bendradarbiavimo priemones, skirtas žalingai veiklai internete ir apgaulingiems elektroninio komunikavimo būdams apriboti, buvo fiksuotas ryškus nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui (Lietuvos Respublikos baudžiamojo kodekso (toliau – LR BK) 196–198<sup>2</sup> str.) sumažėjimas. Lietuvos policijos 2023 m. stebėsenos vertinimas sutampa su viešuose šaltiniuose paskelbtomis nepriklausomų ekspertų išvadomis. Kompanijos „Surfshark“ 2023 m. atlikto skaitmeninio gyvenimo kokybės indekso (angl. *Digital Quality of Life Index* (DQL)) tyrimo duomenimis, Lietuva pagal kibernetinį saugumą 2023 m. buvo antra pasaulyje.

2023 m. ir toliau išliko situacija, kad nusikalstamumą elektroninėje erdvėje labiausiai lemia sukčiavimo atvejai (LR BK 182 str.). Jie 2023 m. sudarė didžiąją – 50 proc. – dalį visų elektroninėje erdvėje padarytų nusikalstamų veikų. Finansų rinkos dalyvių duomenimis<sup>04</sup>, iš Lietuvos gyventojų ir juridinių asmenų 2023 m. apgaule buvo išviliota apie 12,3 mln. eurų, t. y. 3,9 proc. daugiau negu 2022 m., tačiau finansų įstaigoms pavyko susigrąžinti beveik 900 tūkst. eurų, todėl realūs nuostoliai siekė 11,4 mln. eurų. Sukčiavimo būdai nesikeičia: vienas populiariausių sukčiavimo būdų – avansinis (išankstinio mokėjimo) sukčiavimas. Šių atvejų skaičius kasmet sparčiai didėja, nes nusikaltėliams vis dar puikiai pavyksta įtikinti aukas atlikti mokėjimus į sukčių nurodytas sąskaitas pagal internete paskelbtus apgaulingus skelbimus.

2023 m. išliko situacija, kad 2023 m. tarp visų subjektų, patiriančių kibernetinių nusikaltimų poveikį, dažniausiai nukenčia fiziniai asmenys. 2023 m. buvo fiksuojami pokyčiai, dominuojančia apgaulingų skelbimų vieta tampa socialiniai tinklai. 2023 m. didėjo ir kiti populiariūs sukčiavimo būdai, tokie kaip apgaulingų SMS žinučių siuntimas, investicinis sukčiavimas. Dėl pastarojo 2023 m. gerokai išaugo padaryta žala gyventojams – apie 4,8 mln. eurų (2022 m. – 1,9 mln. eurų).

## 9. Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) 2023 m. prioritetinė veikla duomenų valdytojų, duomenų apsaugos pareigūnų ir duomenų subjektų žinių, kompetencijų ir įgūdžių srityje davė teigiamų rezultatų – gauta mažiau pranešimų apie asmens duomenų saugumo pažeidimus (toliau – ADSP) negu 2022 m.

VDAI 2023 m. stiprinant duomenų valdytojų, duomenų apsaugos pareigūnų ir duomenų subjektų žinias, kompetenciją ir įgūdžius, taip pat didėjant organizacijų sąmoningumui, buvo pasiekti teigiami rezultatai asmens duomenų apsaugos srityje. Tą rodo ir statistika: 2023 m. VDAI gavo mažiau pranešimų apie ADSP negu 2022 m. (2022 m. – 304, 2023 m. – 254), taip pat Lietuvoje daugiau nei 3 kartus sumažėjo paveiktų duomenų subjektų skaičius (2022 m. – 1 955 382, 2023 m. – 571 833).

Tačiau VDAI pažymi, kad nors 2023 m. ADSP, kurie įvyko dėl kibernetinio incidento, fiksuota gerokai mažiau negu 2022 m., tačiau jų metu buvo paveikti net 49 proc. subjektų (nuo visų 2023 m. paveiktų subjektų skaičiaus). Tarp 2023 m. dėl kibernetinių incidentų įvykusių ADSP buvo tokių, kurių metu buvo ne tik užšifruoti serveriai, buhalterinės programos ir kitos sistemos, bet ir nukopi-

04

VšĮ Pinigų plovimo prevencijos kompetencijų centro duomenys. Prieiga per internetą <https://amlcenter.lt/2023-m-finansiniu-sukciu-aktyvumas-augo-trecdaliu-pasitelke-vartotoju-pandeminius-iprocus/>.

juoti juose esantys duomenys, reikalauja išpirkos už duomenų dešifravimą ir pateikti grasinantys pranešimai nukopijuotus asmens duomenis paskelbti tamsiojo interneto forumuose (angl. *Dark Web Forums*). Taip pat buvo vykdomos prisijungimo duomenų užpildymo (angl. *Credential Stuffing*) kibernetinės atakos, kurių metu piktaivaliai, pasinaudoję nutekėjusiais prisijungimo duomenimis, bandė prisijungti prie kitiems asmenims priklausančių paskyrų. Taip pat 2023 m. asmens duomenys buvo pažeisti DDoS atakų metu.

Lietuvos gyventojų sąmoningumą asmens duomenų apsaugos srityje rodo augantis asmensduomenų apsaugos sąlygų lygis (toliau – ADASL) (2021 ir 2022 m. ADASL siekė 60 proc., 2023 m. – 64 proc.) ir gyventojų žinios apie Bendrąjį duomenų apsaugos reglamentą<sup>05</sup> (toliau – BDAR) (2023 m. apie BDAR žinojo 82,4 proc., arba 7,4 proc. daugiau negu 2022 m.). VDAI kasmet atliekamos visuomenės apklausos rodo, kad visuomenė mato pokyčius ne tik organizacijoms tvarkant asmens duomenis, bet ir joms komunikuojant apie įvykčius kibernetinius incidentus ir (ar) ADSP. Be kita ko, VDAI ir kitos šioje srityje veikiančios institucijos, atsižvelgdamos į pasitaikiusias veiklos spragas organizacijose, dalijasi rekomendacijomis, padedančiomis mažinti rizikas. Atsižvelgdama į šiuos rezultatus, informuotumo didinimą VDAI laiko vienu iš veiklos prioritetų.

## 10. Lietuvos kariuomenės Strateginės komunikacijos departamento (toliau – LK SKD) analitikai 2023 m. informacinėje erdvėje fiksavo intensyvią veiklą prieš Lietuvą ir jos strateginius interesus.

2023 m. tęsiantis Rusijos karinei invazijai Ukrainoje prieš Lietuvą nukreiptos priešiškos informacijos atvejų skaičius nemažėjo. 2023 m. ir toliau fiksuota itin agresyvi Rusijos ir Baltarusijos retorika NATO atžvilgiu. 2023 m. aktyviau nei anksčiau buvo komunikuojama apie tai, kad NATO yra nepajėgi, silpna ir pralaimėtų karą su Rusija, kurstoma tautinė nesantaika tarp lietuvių ir ukrainiečių, menkinama parama Ukrainai. Rusijos informacinėje erdvėje buvo iškreipiami idėjų kalvių (angl. *Think Tank*), Vakarų analitinių centrų vertinimai – jie visuomenei būdavo pateikiami taip, tarsi akademinė Vakarų bendruomenė supranta Rusijos galią ir yra įsitikinusi, jog NATO nėra pasirengusi tiesioginiam karui.

2023 m. LK SKD fiksuotas bendras priešiškos informacinės veiklos atvejų skaičius sudarė daugiau nei 3 500 unikalių informacinių atvejų. Skleidžiamos priešiškos informacijos srautas išsiskyrė kaltinimais, kad Lietuva ir NATO provokuoja Rusiją ir Baltarusiją. Taip pat mūsų šalis su NATO buvo kaltinama siekiu pulti šias valstybes. Skleista dezinformacija apie NATO bei Lietuvos kariuomenės karinius pajėgumus, Vakarų ekonominę ir karinę paramą Ukrainai.

Per NATO viršūnių susitikimą Vilniuje buvo fiksuotas didžiausias informacinis spaudimas. Priešiška informacinė erdvė buvo intensyviai ruošiama dar iš anksto, o diena prieš bei antroji susitikimo diena pasižymėjo didžiausiu incidentų skaičiumi per visus 2023 m. – tada informacinis spaudimas išaugo 3–4 kartus, palyginti su vidutiniu atvejų skaičiumi per dieną.

LK SKD nuomone, dėl daugelyje pasaulio šalių vykstančių rinkimų 2024 m. pasižymės dar didesniu informaciniu spaudimu nei 2023 m.



05

2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). Prieiga per internetą <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679>.



# 05

## Kibernetinio saugumo politikos formavimas



KAM 2023 m. tęsė darbus kibernetinio saugumo politikos formavimo srityje, tačiau į savo darbotvarkę įtraukė ir naujų aspektų, pavyzdžiui: viename teisės akte išdėstyti techniniai kibernetinio saugumo reikalavimai ir priimtos aiškesnės nuostatos dėl keitimosi įslaptinta informacija, parengtas ir priimtas naujas kibernetinio saugumo srities programinis dokumentas, sustiprintas tarptautinis bendradarbiavimas kibernetinio saugumo srityje su Indijos ir Ramiojo vandenynų regiono šalimis, vertinamos naujos Europos Sąjungos teisėkūros iniciatyvos, turėsiančios didelį poveikį kibernetinio saugumo politikos formavimo srityje, ir kt. Visa tai tam, kad Lietuva neslūgstant geopolitinei įtampai būtų atspari kibernetinėms atakoms, gebėtų greitai atsikurti joms ištikus ir kartu su kitomis vienmintėmis šalimis efektyviau valdytų su kibernetiniu saugumu susijusias rizikas.

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

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



Plėtos programa buvo patvirtinta Lietuvos Respublikos Vyriausybės 2023 m. rugsėjo 20 d. nutarimu Nr. 746<sup>01</sup>. Plėtos programai įgyvendinti numatyta 40,15 mln. eurų Ekonomikos gavimo ir atsparumo didinimo priemonės (angl. *Recovery and Resilience Facility* (RRF)) lėšų ir 3,7 mln. – 2021-2027 m. Skaitmeninės Europos programos lėšų. Remdamasi Plėtos programa, KAM įgyvendins 2021-2030 metų nacionaliniame pažangos plane numatytą uždavinį – stiprinti kibernetinį saugumą ir gynybą.

#### Siekiant spręsti kibernetinio saugumo srityje kylančias problemas, Plėtos projekte planuojama:

- ✓ peržiūrėti nacionalinės kibernetinio saugumo politikos formavimo ir įgyvendinimo sistemą, į kibernetinio saugumo valdymą ir užtikrinimą įtraukiant vis daugiau institucijų;
- ✓ atnaujinti organizacinius ir techninius kibernetinio saugumo reikalavimus;
- ✓ modernizuoti kibernetinio saugumo ir elektroninių nusikaltimų tyrimo infrastruktūrą;
- ✓ stiprinti darbuotojų kibernetinio saugumo srityje ir elektroninių nusikaltimų tyrėjų kompetencijas;
- ✓ didinti visuomenės, ypač labiausiai pažeidžiamų visuomenės grupių, supratimą apie kibernetinį saugumą: suteikti bazinių kibernetinio saugumo žinių, padėti įgyti praktinių kibernetinės higienos įgūdžių, tokių kaip saugumo atnaujinimų įdiegimas naudojamuose įrenginiuose, slaptažodžių sudarymas ir naudojimas, atsarginių kopijų darymas, – visa tai padėtų išvengti dalies kibernetinių incidentų ir (ar) sumažintų jų poveikį;

#### 01

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





skatinti viešojo ir privataus sektoriaus bendradarbiavimą. Pagalba mažoms ir vidutinėms įmonėms, aktyvus viešojo ir privataus sektoriaus bendradarbiavimas kibernetinio saugumo srityje padėtų užtikrinti ne tik didesnį kibernetinį atsparumą, bet ir skatintų rasti ir pasiūlyti inovatyvių kibernetinio saugumo sprendimų visos valstybės mastu.

Daugiau informacijos apie programą KAM interneto svetainėje

<https://kam.lt/planavimo-dokumentai/>.

KAM koordinuoja TIS 2 direktyvos<sup>02</sup> perkėlimą į nacionalinę teisę. TIS 2 direktyva siekiama padidinti organizacijų, kurios įvairiuose sektoriuose atlieka itin svarbias funkcijas, kibernetinio atsparumo lygį, taip pat sumažinti kibernetinio atsparumo neatitikimus tarp sektorių ir sektoriuose bei pagerinti informacijos mainus ir kolektyvinius gebėjimus pasirengti incidentams ir į juos reaguoti. Viešojo ir privataus sektoriaus laukia dideli pokyčiai, susiję su esminių ir svarbių subjektų identifikavimu, kibernetinio saugumo rizikų valdymo priemonių įgyvendinimu, kibernetinių incidentų valdymu bei kibernetinio saugumo subjektams taikoma priežiūra. Šie ir kiti numatomi pokyčiai kibernetinio saugumo srityje 2023 m. buvo aptariami su susijusiomis institucijomis. 2023 m. siekiant į nacionalinę teisę perkelti TIS 2 direktyvą pradėtas rengti Lietuvos Respublikos kibernetinio saugumo įstatymo pakeitimo įstatymo projektas bei su juo susiję kitų teisės aktų pakeitimo projektai. TIS 2 direktyvą įgyvendinančius teisės aktus planuojama priimti iki 2024 m. spalio 17 d.

Daugiau informacijos apie TIS 2 direktyvos perkėlimo į nacionalinę teisę KAM interneto svetainėje <https://kam.lt/tinklu-ir-informaciniu-sistemu-direktyva/>.

Atsižvelgiant į NATO sprendimą kibernetinę erdvę pripažinti penktuoju kariavimo domenu ir 2022 m. Seimo politinių partijų pasirašytą susitarimą „Dėl Lietuvos nacionalinio saugumo ir gynybos artimiausio laikotarpio stiprinimo“<sup>03</sup>, numatoma nuosekliai stiprinti Lietuvos kibernetinės gynybos pajėgumus. 2023 m. KAM pradėti Lietuvos kariuomenės Kibernetinės gynybos valdybos (toliau – valdyba) steigimo darbai. Valdyba bus steigiama Lietuvos kariuomenės sudėtyje ir pradės veikti nuo 2025 m. sausio 1 d. Valdybos tikslas – stiprinti Lietuvos kariuomenės kibernetinį saugumą, konsoliduojant Lietuvos kariuomenei skiriamoms užduotims įgyvendinti reikalingus pajėgumus, įgyvendinant valstybės ginkluotos gynybos planus.

Nuo 2022 m. balandžio mėn. įsigaliojo teisės aktai, užtikrinantys, kad kritinėje infrastruktūroje, įskaitant 5G infrastruktūrą, būtų naudojama tik patikimų gamintojų įranga. 2023 m. KAM atnaujino Viešojo pirkimo objektų, kuriuos įsigyjant būtų keliami su nacionalinio saugumo užtikrinimu susiję reikalavimai, sąrašą<sup>04</sup> ir papildomai į sąrašą įtraukė įrangą ir kitus objektus (pavyzdžiui, laivų eismo valdymo įrangą, oro uostų stebėjimo sistemas, mikrokompiuterių centrinius procesorius, radijo imtuvus ir pan.).

Taip pat KAM, siekdama toliau užtikrinti, kad valstybės institucijose ir nacionalinio saugumo požiūriu svarbiuose sektoriuose, įskaitant 5G infrastruktūrą, nebūtų naudojamos nepatikimų gamintojų technologijos ir įranga, 2023 m. dar kartą paragino visas institucijas, veikiančias gynybos srityje, valdančias YSII, veikiančias srityse, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi ar yra įrašytos į Saugiojo valstybinio duomenų perdavimo tinklo naudotojų sąrašą, organizuoti nepatikimų gamintojų įrangos pašalinimą ir pakeitimą patikima iki 2025 m. sausio 1 d.

Kritines funkcijas vykdančios ir mobilizacinės užduotis atliekančios valstybės institucijos yra įtrauktos į Saugųjų tinklą ir gali efektyviai ir saugiai keistis informacija tarpusavyje ir su Europos Sąjungos institucijomis nepriklausomai nuo viešųjų elektroninių ryšių tinklų ir naudotis Kertinio valstybės telekomunikacijų centro (toliau – KVTC) teikiamomis kolektyvinėmis kibernetinio saugumo

priemonėmis. KAM kartu su NKSC ir KVTC 2023 m. užbaigė Europos Sąjungos struktūrinių fondų finansuojamą projektą „Saugiojo tinklo ir kibernetinių atakų prevencijos sistemos sukūrimas“. Vykdamas projektą buvo įsigyta nauja ir atnaujinta turima kibernetinės saugos techninė įranga, atnaujinti Saugiojo tinklo elementai, tai leido modernizuoti Saugųjų tinklą, padidinti valstybės informacinių išteklių kibernetinį saugumą ir pagerinti kibernetinių grėsmių aptikimo prevenciją. Saugiojo tinklo modernizavimas ir jo architektūros atnaujinimas suteikia galimybę prijungti prie šio tinklo dar daugiau svarbiausių valstybės institucijų.

Plečiant Vyriausybinių plačiajuosčių šifruotą duomenų ir balso perdavimo tinklą (toliau – Šifruotas tinklas) ir skatinant valstybės institucijas saugiai apdoroti ir perduoti įslaptintą informaciją, 2023 m. buvo atnaujintas ir viešai paskelbtas Prisijungimo prie Vyriausybinio plačiajuosčio šifruoto duomenų ir balso perdavimo tinklo tvarkos aprašas<sup>05</sup>. Aprašytas prisijungimo prie Šifruoto tinklo procesas sudaro galimybę valstybės institucijoms greitai ir saugiai perduoti įslaptintą informaciją ir užtikrinti jos slaptumą, vientisumą ir prieinamumą teisėtiems naudotojams bei leidžia sprendimus priimti laiku.

## 2 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 PESCO CRRT projektui. 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.

2023 m. prie PESCO CRRT projekte jau dalyvavusių Estijos, Kroatijos, Lenkijos, Lietuvos, Nyderlandų, Rumunijos prisijungė 3 naujos ES valstybės narės – Belgija, Slovėnija ir Danija. Taip buvo gerokai sustiprintos Kibernetinės greitojo reagavimo pajėgos, padidėjo galimybės reaguoti į kibernetinius incidentus visose ES valstybėse narėse, ES institucijose bei partnerėse šalyse. Stebėtojo teisėmis PESCO CRRT projekte šiuo metu dalyvauja Austrija, Graikija, Prancūzija, Italija, Ispanija ir Suomija.

Vienas tokių reagavimo ir rėmimo pavyzdžių – Kibernetinės greitojo reagavimo pajėgos dalyvavimas remiant ES bendros saugumo ir gynybos politikos mokymo misiją Mozambique 2023 m. Kibernetinės greitojo reagavimo pajėgos šalyje atliko kibernetinio pažeidžiamumo vertinimą.

Matydamos Lietuvos vadovaujamo PESCO CRRT projekto sėkmingumą ir efektyvumą, glaudesnio bendradarbiavimo siekia ir trečiosios šalys – Moldova, Ukraina, Juodkalnija. Šias šalis Lietuvos atstovai aktyviai konsultuoja dėl bendradarbiavimo galimybių.



02

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>.

03

Lietuvos Respublikos Seime atstovaujamų politinių partijų susitarimas „Dėl Lietuvos nacionalinio saugumo ir gynybos artimiausio laikotarpio stiprinimo“. Prieiga per internetą <https://www.lrs.lt/sip/getFile?guid=5adbb505-99d8-4b48-867c-90b5d584fff1>.

04

Viešojo pirkimo objektų, kuriuos įsigyjant būtų keliami su nacionalinio saugumo užtikrinimu susiję reikalavimai, sąrašas, patvirtintas Lietuvos Respublikos Vyriausybės 2022 m. kovo 30 d. nutarimu Nr. 280 „Dėl Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 13, 14 ir 15 dalių nuostatų įgyvendinimo“. Prieiga per internetą <https://e-seimasx.lrs.lt/portal/legalAct/lt-TAD/1a061730b0c711ecaf79c2120caf5094/asr>.

05

Prisijungimo prie Vyriausybinio plačiajuosčio šifruoto duomenų ir balso perdavimo tinklo tvarkos aprašas, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2023 m. rugpjūčio 21 d. įsakymu Nr. V-669 „Dėl Prisijungimo prie Vyriausybinio plačiajuosčio šifruoto duomenų ir balso perdavimo tinklo tvarkos aprašo patvirtinimo“. Prieiga per internetą <https://www.e-tar.lt/portal/lt/legalAct/a2db4d903ff611ee9de9e7e0fd363afc>.

06

Išmokyt kibernetinių pamokų karo Ukrainoje metu ataskaita. Prieiga per internetą <https://www.nksc.lt/rkgc/ataskaitos.html>.

### 3 KAM veikla plėtojant tarptautinį bendradarbiavimą kibernetinio saugumo srityje

#### Bendradarbiavimas su JAV

2023 m. gruodį pasirašytas JAV gynybos departamento ir KAM 2024–2028 m. bendradarbiavimo gynybos srityje planas. Sutarta, kad Lietuva ir JAV tęs bendradarbiavimą koncentruodamosi į kibernetinio pajėgumo vystymą, dalydamosi kibernetinių grėsmių informacija, dalyvaudamos bendrose pratybose ir mokymuose bei tęsdamos bendrus projektus Regioniniame kibernetinės gynybos centre (toliau – RKGC), kuris yra NKSC padalinys.

2023 m. toliau stiprinamas bendradarbiavimas su JAV Pensilvanijos nacionaline gvardija (angl. *Pennsylvania National Guard* (PANG)) (toliau – PANG). PANG specialistai Lietuvoje dalyvavo nacionalinėse strateginio lygio kibernetinio saugumo stalo pratybose (angl. *Cyber Shield Stratex*). PANG atstovai prisidėjo prie rengiamų studijų apie karo Ukrainoje metu išmoktas pamokas kibernetinio saugumo ir gynybos srityje.

JAV kibernetinės vadovietės (angl. *US Cyber Command*, USCYBERCOM) atstovai 2023 m. rugpjūčio mėnesį baigė antrąją gynybinę kibernetinio saugumo operaciją Lietuvoje. JAV ir NKSC kibernetinio saugumo specialistai kartu stiprino praktinį sąveikumą ir didino svarbiausių Vidaus reikalų ministerijos tinklų atsparumą kibernetinėms grėsmėms. Tai jau antroji tokia kibernetinio saugumo operacija, kuri įgyvendinta remiantis ankstesne patirtimi, įgyta krašto apsaugos sistemoje bei Užsienio reikalų ministerijoje.

Lietuva dalyvauja tarptautinėje „Iniciatyvoje prieš išpirkos reikalaujančias atakas“. Tai aukšto lygio JAV Baltųjų rūmų organizuojama iniciatyva, vienijanti 50 valstybių ir tarptautinių organizacijų kovai su išpirkos reikalaujančiomis kibernetinėmis atakomis. Lietuva yra viena šios iniciatyvos lyderių, vadovaujančių informacijos dalijimosi darbo grupei kartu su Indija bei Izraeliu. 2022–2023 m. KAM ir NKSC atlikti darbai:

- ✓ pradėta plėtoti informacijos apsiikeitimo platforma, skirta tarptautinių lygiu informacijai apie išpirkos reikalaujančių veikėjų grėsmes dalytis;
- ✓ organizuoti įvadiniai informacijos dalijimosi mokymai;
- ✓ parengtos 2 ataskaitos apie pagrindines tarptautines išpirkos reikalaujančias kibernetines grupuotes bei labiausiai nuo tokių atakų pažeidžiamus sektorius.



#### Bendradarbiavimas su Indijos ir Ramiojo vandenynų regiono šalimis

Daugėjant iššūkių bei didėjant rizikoms Europoje ir Indijos ir Ramiojo vandenynų regione, Lietuva, reaguodama į regionines grėsmes, kylančias iš Rusijos ir Kinijos veiksmų kibernetinėje erdvėje, stiprina bendradarbiavimą kibernetinio saugumo srityje su bendramintėmis regiono šalimis – Japonija, Australija, Pietų Korėja, Singapūru, Taivanu – kibernetinio saugumo srityje. Glaudesniu bendradarbiavimu su Indijos ir Ramiojo vandenynų regiono šalimis siekiama sustiprinti ES, NATO ir jų partnerių kibernetinį saugumą.

2023 m. vyko intensyvios aukšto lygio ir praktinio pobūdžio konsultacijos šalims svarbiais klausimais, buvo dalyvauta bendrose kibernetinės gynybos pratybose. Kitas glaudesnio bendradarbiavimo su Indijos ir Ramiojo vandenynų regiono šalimis pavyzdys – 2023 m. spalį Tokijuje pasirašytas Lietuvos ir Japonijos bendradarbiavimo gynybos srityje susitarimas, kuriame daug dėmesio skiriama kibernetiniam saugumui.

2023 m. pirmą kartą Lietuvoje surengtas aukšto lygio NATO, Indijos ir Ramiojo vandenynų regiono ir partnerių šalių kibernetinio saugumo forumas „Cyber Champions Summit“, tai buvo gretutinis NATO viršūnių susitikimo Vilniuje renginys. KAM kartu su NKSC surengtame forume „Cyber Champions Summit“ NATO sąjungininkių ir stipriausių vienminčių partnerių aukšto lygmens ekspertai diskutavo apie kibernetinio saugumo tendencijas ir bendradarbiavimo galimybes, dalijosi patirtimis, kaip atremti kibernetines atakas ir reaguoti į grėsmes kylančias iš Rusijos ir Kinijos.

#### Parama Ukrainai kibernetinio saugumo ir gynybos pajėgumams

Nenutrūkstant Lietuvos ir kitų partnerių šalių partnerių parama Ukrainai yra ne tik siekis visokeriopa paremti Rusijos agresiją patiriančią šalį, bet tai yra ir investicija į visos Europos saugumą. Lietuvos parama Ukrainai teikiama įvairiomis kryptimis, viena jų – parama kibernetinio saugumo ir gynybos pajėgumams tiek dvišaliu, tiek daugiašaliu lygiu.

Ukrainos rėmėjų kontaktinės grupės (Ramšteino formatas) kontekste 2023 m. rugsėjį Lietuva kartu su Liuksemburgu, Estija, Latvija, Danija, Belgija ir Ukraina įsteigė IT koaliciją Ukrainai remti. Šios koalicijos tikslas – teikti paramą ir stiprinti Ukrainos gynybos ministerijos ir Ukrainos gynybos pajėgų IT ir kibernetinio saugumo pajėgumus.

#### Dvišalio bendradarbiavimo pagrindais 2023 m. Lietuva ir toliau teikė kibernetinio saugumo paramą Ukrainai:

- ✓ tiekė techninę ir programinę įrangą;
- ✓ NKSC Ukrainos kibernetinio saugumo specialistai gilino žinias ir gerino kibernetinio saugumo įgūdžius;
- ✓ parengta išmokyti kibernetinių pamokų karo Ukrainoje metu ataskaita<sup>06</sup>.





## 4 Dalyvavimas formuojant ir įgyvendinant ES kibernetinio saugumo politiką

### NKSC perėmė Nacionalinio koordinavimo centro užduočių vykdymą

2023 m. pabaigoje NKSC iš KAM perėmė vykdyti Nacionalinio koordinavimo centro (toliau – Lietuvos NKC)<sup>07</sup> užduotis. Lietuvos NKC yra vienas iš 27 ES nacionalinių koordinavimo centrų<sup>08</sup>, kuris:

- ✓ yra viešojo sektoriaus subjektas;
- ✓ jo darbuotojai turi mokslinių tyrimų ir technologinių žinių kibernetinio saugumo srityje arba turi galimybę jomis naudotis;
- ✓ vienija Lietuvos kibernetinio saugumo bendruomenę ir veikia kaip bendruomenei skirtas informacinis centras nacionaliniu lygiu;
- ✓ gali gauti tiesiogines ES dotacijas savo veiklai;
- ✓ gali teikti finansinę paramą trečiosioms šalims;
- ✓ teikia techninę pagalbą suinteresuotiems subjektams – remia juos teikiant projektų, kuriuos valdo Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras (angl. *European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres* (ECCC)), paraiškas.

Siekdamas didinti Lietuvos kibernetinio saugumo bendruomenės kompetencijas, 2023 m. NKC su Europos Komisija pasirašė projekto „CyberUp“ finansavimo susitarimą. „CyberUp“ projektu, vykdomu iki 2025 m. pabaigos, bus siekiama visiškai įveiklinti Lietuvos NKC, suburti aktyvią Lietuvos kibernetinio saugumo bendruomenę bei finansuoti nedidelės vertės mažų ir vidutinių įmonių projektus kibernetinio saugumo srityje.

### ES teisėkūros iniciatyvos

Europos Sąjungos kibernetinė darbotvarkė 2023 m. koncentruota į Europos Sąjungos teisėkūros pasiūlymų kibernetinio saugumo srityje derinimą.

Po dvejus metus trukusių derybų 2023 m. gruodžio 13 d. buvo priimtas Reglamentas (ES, Euratomas) 2023/2841, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti<sup>09</sup>. Lietuva kartu su dauguma kitų Europos Sąjungos valstybių narių derybose siekė, kad Europos Sąjungos institucijoms būtų taikomi aukšti kibernetinio saugumo reikalavimai ir standartai, atitinkantys Europos Sąjungos valstybėms narėms taikomas nuostatas pagal TIS2 direktyvą.

2023 m. gruodžio 20 d. po trišalių Europos Parlamento, ES Tarybos ir Europos Komisijos derybų pritarta kompromisiniam Reglamento dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, kuriuo iš dalies keičiamas Reglamentas (ES) 2019/1020, tekstui (Kibernetinio atsparumo aktas)<sup>10</sup>. Akte bus numatytos sąlygos kurti saugius produktus su skaitmeniniais elementais bei nurodyti įpareigojimai aparatinės ir programinės įrangos produktų kūrėjams rinkai pateikti gaminius su mažiau pažeidžiamumu.

07

Prieiga per internetą <https://www.nksc.lt/nkc/>.

08

Prieiga per internetą [https://cybersecurity-centre.europa.eu/en/nccs\\_en](https://cybersecurity-centre.europa.eu/en/nccs_en).

09

Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2023/2841, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti. Prieiga per internetą <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32023R2841&qid=1706716098394>.

10

Europos Komisijos pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, kuriuo iš dalies keičiamas Reglamentas (ES) 2019/1020. Prieiga per internetą <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454>.

Daugiau informacijos apie Kibernetinio saugumo atsparumo aktą <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet>.

2023 m. ES Taryba pradėjo derybas su Europos Parlamentu dėl Europos Komisijos pasiūlyto Europos Parlamento ir Tarybos reglamento, kuriuo dėl valdomų saugumo paslaugų sertifikavimo keičiamas Reglamentas (ES) 2019/881 (Kibernetinio saugumo aktas)<sup>11</sup>. Šiuo Kibernetinio saugumo akto pakeitimu siekiama sudaryti teisinės sąlygas ne tik tvirtinti informacinių ir ryšių technologijų produktų, paslaugų ar procesų Europos kibernetinio saugumo sertifikavimo schemas, tačiau ir įtraukti naują reguliavimo objektą – valdomas saugumo paslaugas. Valdomos saugumo paslaugos pagal siūlomą pakeitimą yra apibrėžiamos kaip veikla, susijusi su kibernetinio saugumo rizikos valdymu, įskaitant atsaką į incidentus, skverbties bandymus (angl. *penetration testing*), saugumo auditus ir konsultacijas.

2023 m. balandžio 18 d. Europos Komisija pasiūlė naują Reglamentą, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės (Kibernetinio solidarumo aktas).<sup>12</sup> Šiuo teisės aktu siekiama sudaryti sąlygas Europos Sąjungos valstybėms narėms, Europos Sąjungos institucijoms bei Skaitmeninės Europos programoje dalyvaujančioms šalims, taip pat ir Ukrainai pasirengti, atsakyti ir greitai atsikurti, patyrus reikšmingus ir didelio masto kibernetinio saugumo incidentus.

Daugiau informacijos apie Kibernetinio solidarumo aktą <https://digital-strategy.ec.europa.eu/en/library/eu-cyber-solidarity-act-factsheet>.

Naujausios ES teisėkūros iniciatyvos kibernetinio saugumo srityje didina viešojo ir privataus sektoriaus subjektų poreikį turėti ir (ar) naudotis profesionaliomis kibernetinio saugumo specialistų paslaugomis. Įvairių tyrimų duomenimis, 2022 m. Europos Sąjungoje trūko nuo 260 000 iki 500 000 kibernetinio saugumo specialistų. Siekdama spręsti šias problemas, Europos Komisija 2023 m. balandžio 18 d., minėdama Europos įgūdžių metus, priėmė komunikatą dėl Kibernetinio saugumo įgūdžių akademijos<sup>13</sup>. Šio komunikato tikslas – numatyti pagrindines priemones, padėsiančias ugdyti ES kibernetinio saugumo specialistų įgūdžius. Numatomomis priemonėmis bus siekiama sumažinti kibernetinio saugumo įgūdžių trūkumą ir aprūpinti ES reikiama darbuotojais, kad ji galėtų reaguoti į nuolat kintančią grėsmių padėtį, o valstybės narės – įgyvendinti ES politiką, kuria siekiama apsaugoti ES nuo kibernetinių išpuolių, taip pat didinti verslo galimybes ir konkurencingumą.

### ES kibernetinė diplomatija

2023 m. birželio 8 d. Europos Sąjungos Taryba paskelbė atnaujintą Europos Sąjungos kibernetinės diplomatijos priemonių rinkinį (angl. *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox*)<sup>14</sup>. Lietuva kartu su vienmintėmis Europos Sąjungos valstybėmis narėmis pasisakė už kibernetinės diplomatijos priemonių, ypač kibernetinių sankcijų režimo, išplėtimą įtraukiant sektorines sankcijas, papildomų ribojamųjų priemonių įtraukimą. Europos Sąjungos kibernetinės diplomatijos sistema taip pat apima bendradarbiavimą stiprinančias priemones, pagal kurias 2023 m. surengti Europos Sąjungos ir JAV, Jungtinės Karalystės, Japonijos ir Indijos kibernetiniai dialogai.

Solidarizuodamosi su Jungtinės Karalystės ir kitų partnerių pareiškimais, 2023 m. gruodžio 7 d. Europos Sąjunga ir Europos Sąjungos valstybės narės deklaracijomis<sup>15</sup> griežtai pasmerkė kibernetinę kenkimo veiklą prieš demokratines institucijas ir rinkimų procesus.

Siekdama atgrasyti iš trečiųjų šalių kylančias ar nusikalstamų veikėjų keliamas kibernetines

11

Europos Komisijos pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo dėl valdomų saugumo paslaugų sertifikavimo keičiamas Reglamentas (ES) 2019/881. Prieiga per internetą <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52023PC0208>.

12

Europos Komisijos pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomas solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės. Prieiga per internetą <https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act>.

13

2023 m. balandžio 18 d. Europos Komisijos komunikatas Europos Parlamentui ir Tarybai (COM(2023) 207 final) „Kibernetinio saugumo srities talentų trūkumo problemos sprendimas siekiant didinti ES konkurencingumą ir atsparumą bei skatinti jos augimą (Kibernetinio saugumo įgūdžių akademija)“. Prieiga per internetą <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52023DC0207>.

14

Atnaujintas Europos Sąjungos kibernetinės diplomatijos priemonių rinkinys. Prieiga per internetą <https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf>.

15

ES vyriausiojo įgalotinio užsienio reikalams ir saugumo politikai pareiškimas ES vardu dėl demokratinių procesų apsaugos nuo kibernetinės kenkimo veiklos. Prieiga per internetą <https://www.consilium.europa.eu/en/press/press-releases/2023/12/07/cyber-statement-by-the-high-representative-on-behalf-of-the-european-union-on-the-protection-of-democratic-processes-against-malicious-cyber-activities/>.



grėsmes ir atakas prieš Europos Sąjungą ir Europos Sąjungos valstybes nares, Europos Sąjungos Taryba nuo 2019 m. taiko iki 2025 m. gegužės 18 d. galiojančią kibernetinių grėsmių ribojamųjų priemonių sistemą<sup>16</sup>. Pagal šią sistemą Europos Sąjungos taiko tikslines ribojamąsias priemones asmenims ar subjektams, susijusiems su kibernetiniais išpuoliais, kurie daro didelį poveikį ir kelia išorės grėsmę Europos Sąjungos ar jos valstybėms narėms. Šiuo metu kibernetinių sankcijų sąrašė yra aštuoni asmenys ir keturi subjektai iš Rusijos, Kinijos ir Šiaurės Korėjos<sup>17</sup>.

## ES kibernetinė gynyba

Lietuva aktyviai prisidėjo prie 2023 m. gegužės 22 d. priimtų Europos Sąjungos Tarybos išvadų dėl Europos Sąjungos kibernetinės gynybos politikos (angl. *Council Conclusions on the EU Policy on Cyber Defence*)<sup>18</sup> ir Europos Sąjungos kibernetinės gynybos politikos įgyvendinimo plano sudarymo. Derinimo procesuose buvo atsižvelgta į Lietuvos bei suburtų vienminčių Europos Sąjungos valstybių narių grupių pozicijas dėl Tarybos išvadų dėl Europos Sąjungos kibernetinės gynybos politikos teksto formuluočių, ypač dėl Lietuvos vadovaujamo PESCO CRRT projekto, valstybių narių išskirtinių kompetencijų nacionalinio saugumo, įskaitant kibernetinės gynybos, srityje ir tolesnio ES ir NATO bendradarbiavimo stiprinimo kibernetiniais klausimais.

## 5 Kibernetinė gynyba yra viena esminių NATO atgrasymo ir gynybos užduočių

NATO dar 2016 m. pripažino kibernetinę erdvę operacijų sritimi, kurioje Aljansas turi užtikrinti tinkamą gynybą. Rusijos karas prieš Ukrainą tik dar labiau išryškino, kad kibernetinė veikla yra integrali šiuolaikinių konfliktų dalis. Rusija taip pat suaktyvino hibridinius veiksmus prieš NATO sąjungininkes ir partnerius, įskaitant kibernetinę kenkimo veiklą. Lietuva, būdama neatsiejama NATO dalimi, aktyviai prisideda prie Aljanso kibernetinės gynybos politikos formavimo, kibernetinių pajėgumų stiprinimo, dalyvauja kibernetinės gynybos pratybose ir iniciatyvose.

Atsižvelgiant į specifinius kibernetinės erdvės karinio planavimo ir operacijų vykdymo poreikius, atskirose NATO sąjungininkėse šalyse kuriamos kibernetinės pajėgos, atitinkami pokyčiai vykdomi ir NATO štabuose. NATO viršūnių susitikime Vilniuje buvo patvirtintas ir sėkmingai išbandytas NATO virtualus reagavimo į kibernetinius incidentus pajėgumas (angl. *Virtual Cyber Incident Support Capability* (VCISC)) (toliau – NATO virtualus pajėgumas), skirtas nacionaliniams sąjungininkių pajėgumams paremti reaguojant į didelio masto kibernetinius incidentus.

NATO lyderiai Vilniuje taip pat sutarė stiprinti kibernetinės gynybos įsipareigojimus (angl. *Cyber Defence Pledge*) ir siekti naujų ambicingų tikslų stiprinant nacionalinę kibernetinę gynybą ir kritinės infrastruktūros kibernetinį saugumą.

Lietuvos atstovai dalyvauja NATO kibernetinės gynybos kompetencijos centro (NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE)) (toliau – CCDCOE)<sup>19</sup> veikloje. Tai suteikia 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.

NKSC ir Lietuvos kariuomenės atstovai kasmet dalyvauja CCDCOE organizuojamose pratybose „Suremti skydai“ (angl. *Locked Shields*)<sup>20</sup>. Pratybose kibernetinio saugumo ekspertai tobulina praktinius įgūdžius ginti nacionalines informacines sistemas ir kritinę infrastruktūrą nuo realiu laiku vykdomų kibernetinių atakų.

CCDCOE organizuoja tarptautines kibernetinių konfliktų konferencijas „CyCon“<sup>21</sup>. Jose kasmet dalyvauja viešojo, privataus sektoriaus ir akademinės bendruomenės pranešėjai ir dalyviai iš NATO sąjungininkių šalių, įskaitant Lietuvos, ir partneriai. Konferencijose aptariami techniniai, teisiniai, politiniai, strateginiai ir kariniai kibernetinės gynybos ir saugumo klausimai bei pristatomi naujausi kibernetinio saugumo moksliniai tyrimai.



<sup>20</sup> CCDCOE organizuojamos pratybos „Suremti skydai“. Prieiga per internetą <https://ccdcOE.org/exercises/locked-shields/>.

<sup>21</sup> Tarptautinė kibernetinių konfliktų konferencija „CyCon“. Prieiga per internetą <https://ccdcOE.org/cycon/>.

<sup>16</sup> Prieiga per internetą <https://www.consilium.europa.eu/lt/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/>.

<sup>17</sup> 2019 m. gegužės 17 d. 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/LT/TXT/PDF/?uri=CELEX:02019D0797-20201124>.

<sup>18</sup> 2023 m. gegužės 22 d. Europos Sąjungos Tarybos išvada dėl Europos Sąjungos kibernetinės gynybos politikos. Prieiga per internetą <https://www.consilium.europa.eu/media/64526/st09618-en23.pdf>.

<sup>19</sup> NATO kibernetinės gynybos kompetencijos centras. Prieiga per internetą <https://ccdcOE.org/>.



## 06

Lietuvos kibernetinio  
saugumo būklės apžvalgaLietuvos kibernetinės erdvės apžvalga:  
incidentų dinamika ir prevencinės priemonės,  
skirtos kibernetiniam atsparumui stiprintiLiudas Ališauskas,  
NKSC direktorius

## Vadovo žodis

2023 m. Nacionalinis kibernetinio saugumo centras tęsė savo misiją – didinti Lietuvos atsparumą kibernetinio saugumo grėsmėms, padėti šalies viešojo valdymo sektoriaus ir kritines paslaugas teikiančioms organizacijoms veikti be sutrikimų ir kurti saugią Lietuvos kibernetinę erdvę.

Šioje dalyje apžvelgiami svarbiausi 2023 m. įvykiai, kibernetinės grėsmės Lietuvoje, jų tendencijos, rizikos, aptariama kartu su partneriais bei saugumo bendruomene pasiekta pažanga šalies kibernetinio saugumo srityje.

NKSC, siekdamas stiprinti Lietuvos kibernetinį atsparumą, 2023 m. toliau kryptingai tęsė savo veiklą: ugdė saugumo kompetencijas, atliko kibernetinio saugumo rizikos vertinimus, vykdė kibernetinio saugumo subjektų patikrinimus, tobulino kibernetinio saugumo priemones. Kartu buvo pradėti įgyvendinti ir NKSC struktūriniai pokyčiai. Naujoji organizacijos struktūra ir didesni pajėgumai padės įveikti iššūkius, pasiekti strateginius tikslus ir įgyvendinti 2024 m. Lietuvoje įsigaliosiantį Europos Parlamento ir Tarybos priimtą TIS 2 direktyvos teisinį reglamentavimą.



## 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 ir pažeidžiamumų paiešką.
- ✓ Koordinuodamas reagavimą į kibernetinius incidentus ir atlikdamas jų tyrimus.
- ✓ Kurdamas ir plėtodamas prevencines nacionalines kibernetinio saugumo priemones.
- ✓ Ugdymas kibernetinio saugumo kompetencijas.



## Svarbiausi 2023 m. įvykiai ir tendencijos



Didžiausią išorinį poveikį Lietuvos kibernetinio saugumo aplinkai darė geopolitiniai ir technologiniai veiksniai.



2023 m. buvo tęsiami Lietuvos kibernetinę gynybą ir atsparumą stiprinantys veiksmai: įkurtos pirmosios sektorinės apsaugos kibernetinio saugumo informacija platformos, plėtojamas keitimasis aktualia informacija su tarptautiniais partneriais, vykdoma aktyvi kibernetinio saugumo kompetencijų ugdymo veikla.



Bendras nacionalinis kibernetinis atsparumas tiesiogiai priklauso nuo kiekvienos organizacijos tinkamo pasiruošimo savo kasdienėje veikloje taikyti organizacines ir technines saugos priemones. Šioje srityje NKSC mato teigiamą pokytį, situaciją dar galima gerinti.



Vykdydamas Lietuvos kibernetinės erdvės prevencinę priežiūrą, NKSC 2023 m. nustatė 1 963 potencialiai kritinių saugumo spragų turinčias ryšių ir informacines sistemas. Apie šias spragas valdytojai buvo informuoti tiesiogiai arba per interneto paslaugų teikėjus.



Atsakingi pranešėjai 2023 m. aptiko 74 kibernetinio saugumo spragas įvairiose Lietuvos informacinėse sistemose ir apie tai informavo NKSC laikydamiesi atsakingo kibernetinių spragų atskleidimo principų. Palyginti su ankstesniais metais, iš pranešėjų sulaukta 45 proc. daugiau pranešimų.



NKSC registravo 2 378 kibernetinius incidentus. Palyginti su ankstesniais metais, bendras registruotų incidentų skaičius sumažėjo 30 proc., tačiau 12 proc. augo pavojingesnių – vidutinės kategorijos incidentų skaičius.



Daugiausia incidentų įvyko interneto prieglobos paslaugų infrastruktūroje, antroje vietoje – viešajame administravimo sektoriuje, trečioje vietoje – interneto paslaugų teikėjų infrastruktūroje ir prie jos prijungtuose fizinių asmenų galiniuose įrenginiuose.



Didžiausią žalą darė elektroninius duomenis užšifruojančių ir išpirkos reikalaujančių kenkimo programinio kodo virusai, DDoS atakos, tiekimo grandinės atakos ir socialinės inžinerijos principais sukurtos atakos.



Kovai su žaibiškais kibernetinėmis sukčiavimo atakomis NKSC toliau tobulino organizacijų ir gyventojų apsaugai skirtą įrankį – DNS užkardą. Ši priemonė 2023 m. buvo taikoma beveik 4 mln. mobiliojo ir 775 tūkst. fiksuoto interneto ryšio paslaugų naudotojų ir per dieną vidutiniškai apsaugojo daugiau kaip 2 tūkst.



Kibernetinių kompetencijų ugdymas yra viena iš svarbiausių valstybės atsparumo didinimo priemonių nuolat keičiantis kibernetinėms grėsmėms. 2023 m. NKSC organizuotus įvairaus tipo teorinius mokymus baigė daugiau kaip 11,5 tūkst. asmenų.

## 1 Kibernetinio saugumo grėsmės ir rizikos

### Išorinės aplinkos vertinimas

2023 m. Lietuvos kibernetinio saugumo aplinkai didžiausią išorinį poveikį darė geopolitiniai ir technologiniai veiksniai.

Antrus metus besitęsiantis karas Ukrainoje išliko pagrindiniu įtaką darančiu geopolitiniu išorės veiksniu, nes dėl aktyvios paramos Ukrainai Lietuva liko su Kremliumi siejamų pažangių ir tęstinių kibernetinių grėsmių (angl. *Advanced Persistent Threat*, APT) (toliau – APT) grupuočių<sup>01</sup> taikinyje. Lietuvoje šio pobūdžio atakų ar jų bandymų daugėjo, nusikalstamos grupuotės elgėsi agresyviau nei anksčiau. Lietuvoje APT išskirtinai veikė prieš viešojo administravimo sektorių. Pagrindiniai tikslai, manoma, buvo šnipinėjimas, pasirengimas ir siekis vykdyti destruktines atakas, ekonominės naudos siekimas.

Didelę įtaką kibernetinei aplinkai darė ir naujausių technologijų plėtra. Ypač ryškūs pokyčiai yra susiję su DI ir GDI technologijų proveržiu ir šių technologijų prieinamumu plačiai naudotojų auditorijai. Kaip ir daugelyje veiklos sričių, šiomis technologijomis siekiama stiprinti kibernetinio saugumo pajėgumus, o nusikaltėliai tas pačias technologijas naudoja savo nusikalstamoms veikloms.

Pasaulinei saugumo bendruomenei kelia nerimą DI technologijų panaudojimo kibernetinėms atakoms potencialas, nors tiek Lietuvoje, tiek kitose šalyse, didžiųjų kibernetinio saugumo organizacijų duomenimis<sup>02</sup>, 2023 m. dar nebuvo fiksuota incidentų, kuriuos išskirtinai vykdytų DI. Vis tik matomas aktyvus didžiųjų kalbos modelių<sup>03</sup> (angl. *Large Language Models*, LLM) (toliau – LLM) naudojimas kuriant socialinės inžinerijos ir dezinformacijos žinutes įvairiomis kalbomis. Iki šiol kalbos klaidos žinutėse leisdavo lengviau pastebėti klastą, tačiau pritaikius LLM tai tapo kur kas sunkiau.

### Vidinės aplinkos vertinimas

Nacionalinis atsparumas kibernetinėms grėsmėms tiesiogiai priklauso nuo kiekvienos organizacijos tinkamo pasiruošimo savo kasdienėje veikloje taikyti organizacines ir technines saugos priemones. Šioje srityje NKSC mato teigiamą pokytį, tačiau situaciją dar reikėtų gerinti.

Organizacinių reikalavimų (pavyzdžiui, patvirtinta kibernetinio saugumo politika, ją įgyvendinantys standartai, procedūros ir kt.) įgyvendinimas YSII<sup>04</sup> 2023 m. augo 10 proc., palyginti su 2022 m. duomenimis (žr. 1 pav.).



<sup>01</sup> Pažangios ir tęstinės kibernetinės grėsmės (angl. *Advanced Persistent Threat*, APT) – tai tikslingos kibernetinės atakos, kuriomis grupuotės nepastebėtai įsilaužusios į tinklą siekia ilgalaikių tikslų.

<sup>02</sup> Vienu žingsniu priekyje priešininkų dirbtinio intelekto amžiuje (angl. *Staying ahead of threat actors in the age of AI*). Priega per internetą <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/>.

<sup>03</sup> Didieji kalbos modeliai – tai DI sistemos, skirtos panašiam į žmogaus sukurtą tekstui apdoroti, suprasti ir generuoti. Jie pagrįsti gilaus mokymosi metodais ir parengti naudojant didžiulius duomenų rinkinius, kuriuose paprastai yra milijardai žodžių iš įvairių šaltinių, pavyzdžiui, interneto svetainių, knygų, straipsnių.

<sup>04</sup> YSII – tai ryšių informacinė sistema ar jos dalis, ryšių informacinė sistemos grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams.

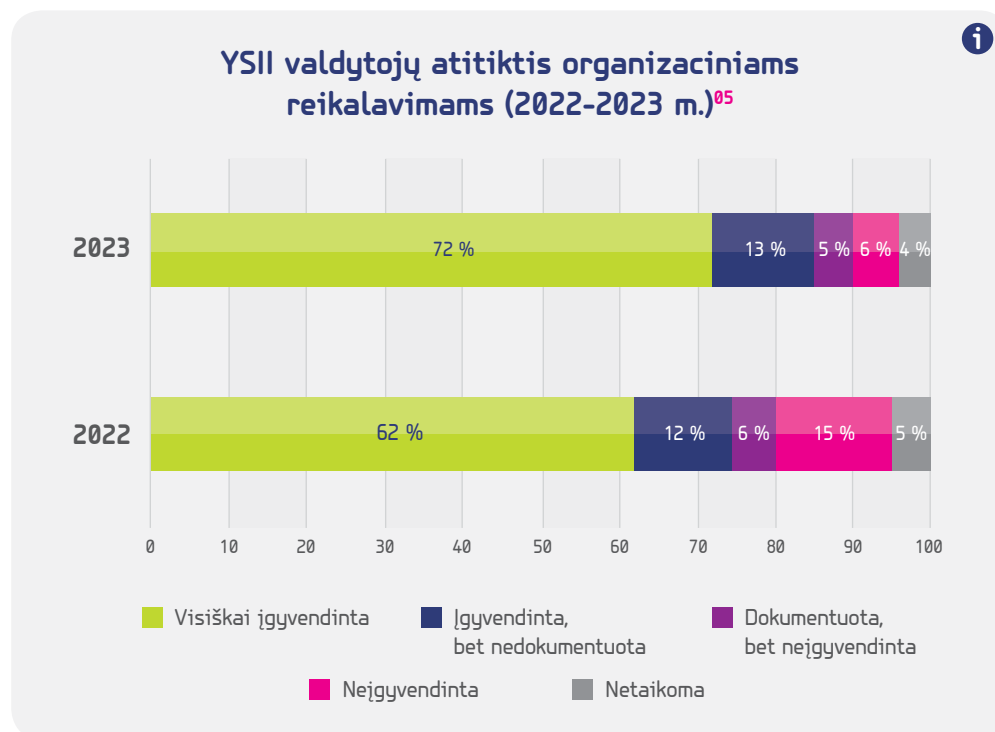
0100  
11011  
01011





**1 pav. >**

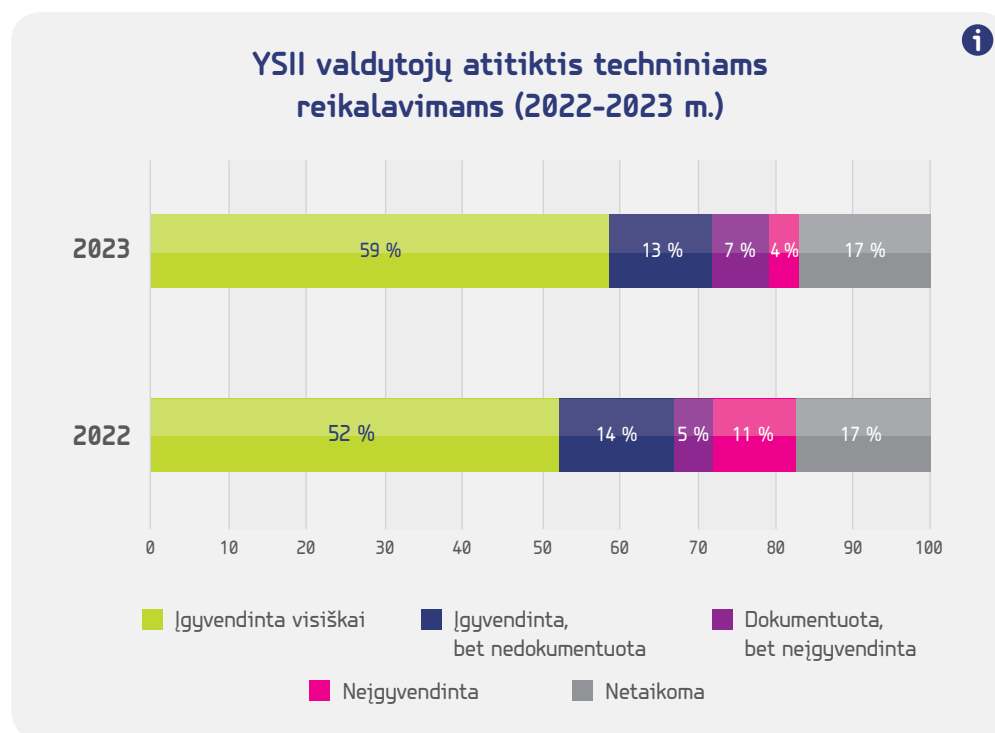
YSII valdytojų atitiktis organizaciniams reikalavimams (2022–2023 m.)  
(šaltinis – NKSC)



Daugiau finansinių ir žmogiškų resursų ir kompetencijų reikalaujančių techninių saugumo priemonių įgyvendinimas per metus padidėjo 7 proc. (žr. 2 pav.)

**2 pav. >**

YSII valdytojų atitiktis techniniams reikalavimams (2022–2023 m.)  
(šaltinis – NKSC)



Vykdydamas Lietuvos kibernetinės erdvės prevencinę priežiūrą, NKSC 2023 m. nustatė 1 963 potencialiai kritinių saugumo spragų turinčias RIS.

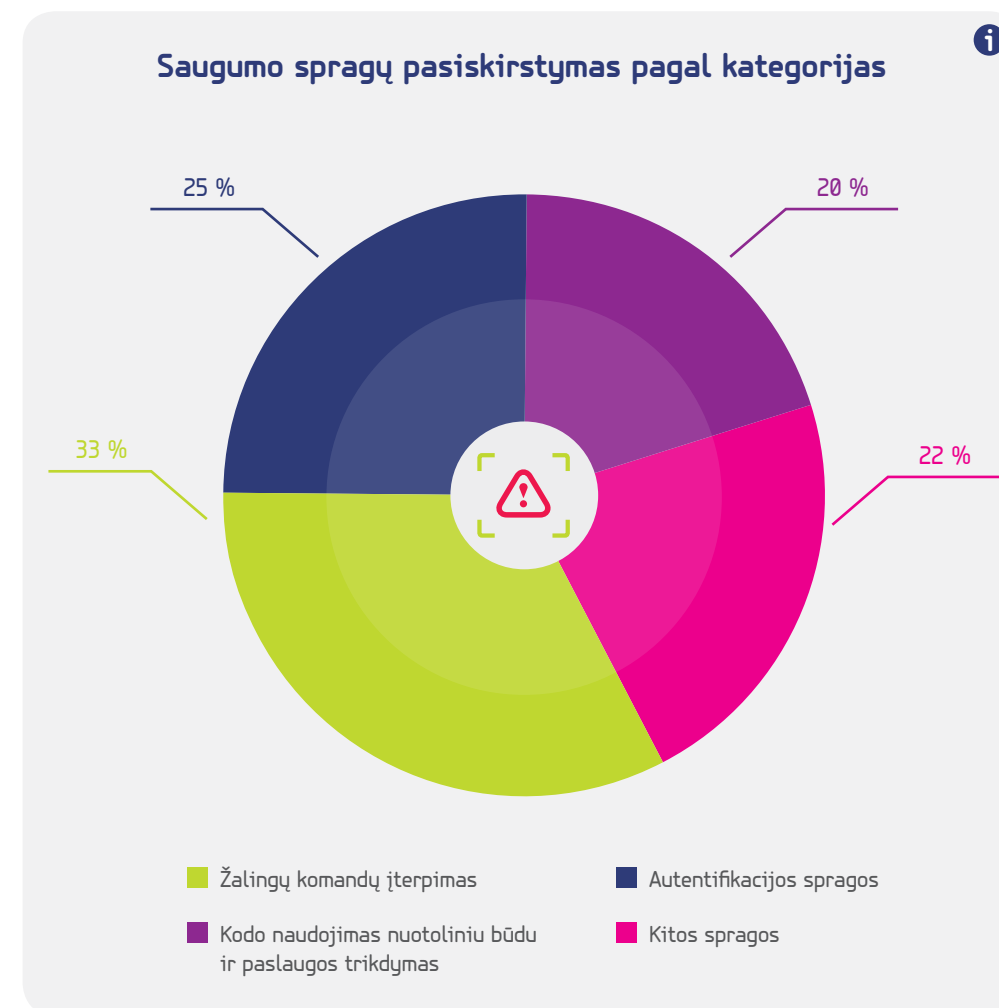
Didžioji dalis (24 proc.) kibernetinio saugumo spragų buvo susijusios su gamintojų paliktomis klaidomis ir (ar) spragomis: maršrutizatorių programiniame kode, virtualaus privataus tinklo (toliau – VPN) sprendimuose ir ugniasienėse. Kiti pažeidžiamumai (beveik 22 proc.) buvo susiję su

**05**

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

įrenginių programine įranga, kuri naudojama RIS stebėti, dokumentuoti, užduotims valdyti ir pan. Trečioji rastų spragų kategorija – internetinių platformų įskiepai, kurie dėl specifikos dažnai buvo nekokybiški, neatnaujinami ir todėl pažeidžiami.

Vertinant visų 2023 m. nustatytų kibernetinio saugumo spragų pobūdį, beveik 33 proc. šių spragų leido jas išnaudojant į RIS įterpti žalingas komandas arba kodą, 25 proc. – pasireiškė netinkamai įgyvendintu autentifikacijos mechanizmu, 20 proc. – suteikė galimybę nuotoliniu būdu vykdyti pasirinktiną kodą arba trikdyti paslaugos teikimą (žr. 3 pav.).

**< 3 pav.**

Saugumo spragų pasiskirstymas pagal kategorijas (šaltinis – NKSC)

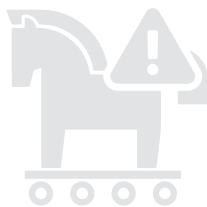
Nors pažeidžiamų RIS savininkai operatyviai šalino pažeidžiamumus, NKSC mato, kad organizacijos vis dar neskiria pakankamai dėmesio savo valdomų RIS gyvavimo ciklui užtikrinti.

2023 m. NKSC tobulino kibernetinių grėsmių aptikimo būdus ir juos taikė kibernetinio saugumo subjektų tinkluose. Iš viso 2023 m. nustatytos 248 grėsmės, jų skaičius, palyginti su 2022 m., padidėjo 35 proc.

Dažniausiai tinkluose aptinkamos grėsmės – įvairi kenkimo programinė įranga, skirta kriptovaliutoms generuoti nelegaliai išnaudojant kompiuterinius resursus. Kitos identifikuotos grėsmės susijusios su jautrių duomenų perdavimu atviru tekstu. Siunčiant duomenis nesaugiais kanalais ir netaikant jokio šifravimo, didelė tikimybė, kad jie gali būti perimti ir pasisavinti trečiųjų šalių.

## 06

Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 5 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo“. Prieiga per internetą <https://e-seimas.lrs.lt/portal/legAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr>.



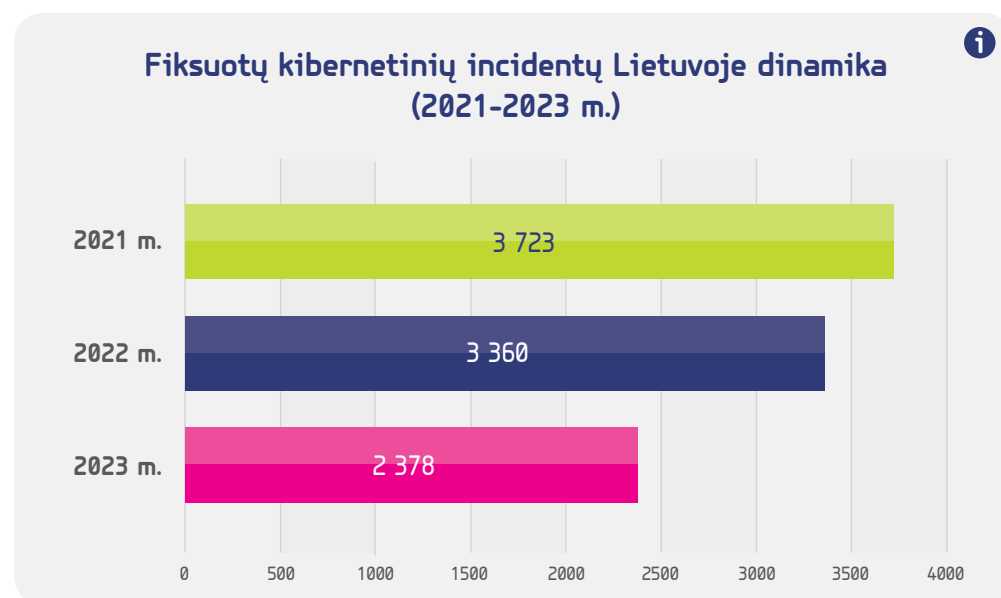
## 4 pav. &gt;

NKSC fiksuotų kibernetinių incidentų Lietuvoje dinamika (2021–2023 m.) (šaltinis – NKSC)

Kibernetinio saugumo užtikrinimas organizacijose yra tęstinis procesas, kuriam reikia nuolatinės RIS priežiūros ir atsakingo personalo kompetencijų. RIS turi būti nuolat stebimos, surandami nauji pažeidžiamumai ir sutvarkoma klaidinga konfigūracija. Nors organizacijoms, kurios valdo YSII, yra privaloma įsdiegti organizacines ir technines kibernetinio saugumo priemones, kaip numato galiojantys teisės aktai<sup>06</sup>, tačiau savanoriškas jų taikymas ir kitose tiek viešo administravimo, tiek privačiose organizacijose gerokai mažina riziką patirti kibernetines atakas, užtikrina organizacijos veiklos tęstinumą ir mažina žalą. Todėl NKSC skatina organizacijas ir jų vadovus ir toliau tinkamai rūpintis savo organizacijų atsparumu kibernetinėms grėsmėms.

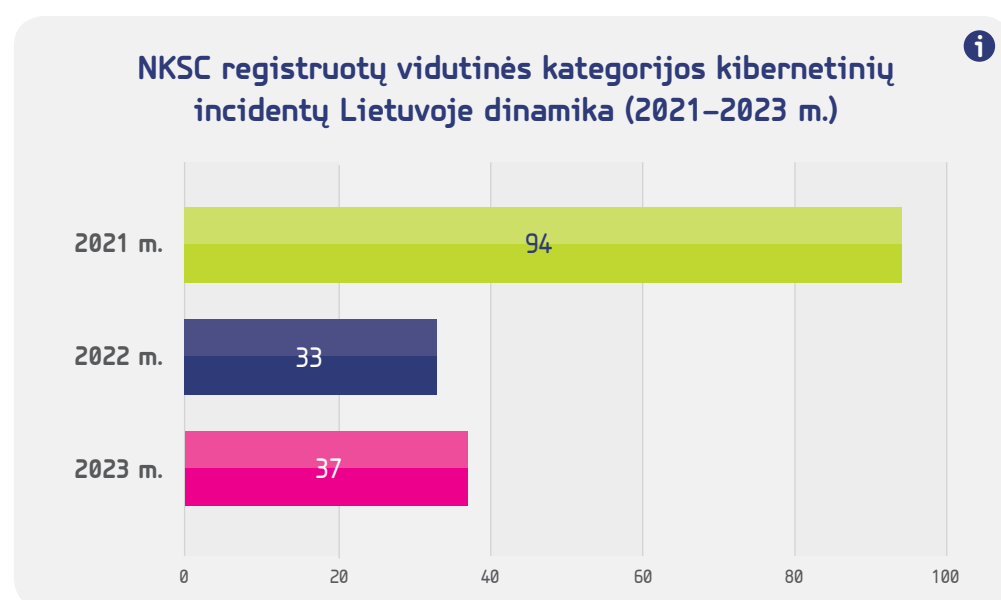
## Kibernetinių incidentų dinamika

2023 m. NKSC registravo 2 378 kibernetinius incidentus (žr. 4 pav.). Palyginti su ankstesniais metais, bendras registruotų incidentų skaičius sumažėjo 30 proc., tačiau 12 proc. augo pavojingesnių – vidutinės kategorijos incidentų skaičius (žr. 5 pav.).



## 5 pav. &gt;

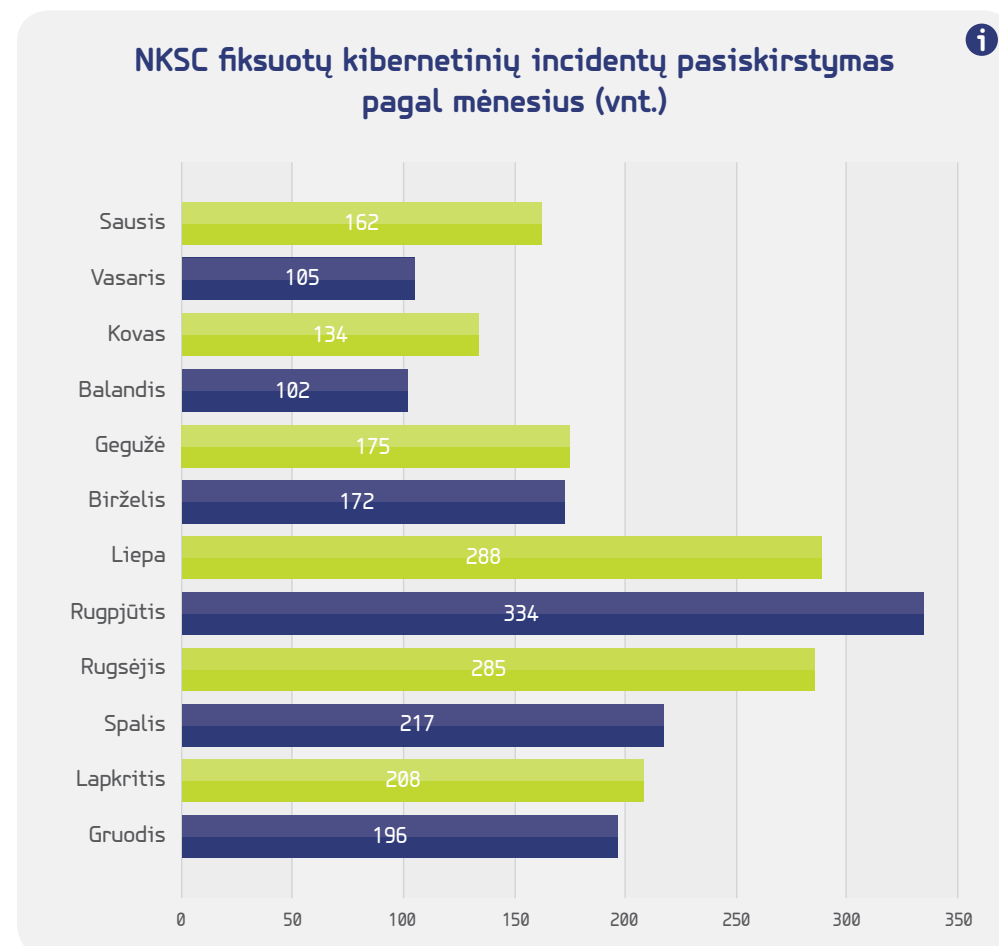
NKSC registruotų vidutinės kategorijos kibernetinių incidentų Lietuvoje dinamika (2021–2023 m.) (šaltinis – NKSC)



## 07

NKSC 2023 m. patikslino kibernetinių incidentų fiksavimo metodiką, todėl skaičiai lentelėje skiriasi nuo ankstesnėse nacionalinės kibernetinio saugumo būklės ataskaitose pateiktų duomenų.

Daugiausia kibernetinių incidentų buvo fiksuota liepos-rugsėjo mėn. (žr. 6 pav.). Tai siejama su liepos mėn. Vilniuje vykusiu NATO viršūnių susitikimu bei svarbiu pokyčiu kovoje su žaibiškomis kibernetinėmis sukčiavimo atakomis išplėtus NKSC sukurtą žalingų interneto nuorodų blokavimo įrankio – DNS užkardos taikymo apimtį (žr. 36 psl. „Kenkimo interneto svetainių užkardymas“).



## &lt; 6 pav.

2023 m. NKSC fiksuotų kibernetinių incidentų pasiskirstymas pagal mėnesius (vnt.) (šaltinis – NKSC)

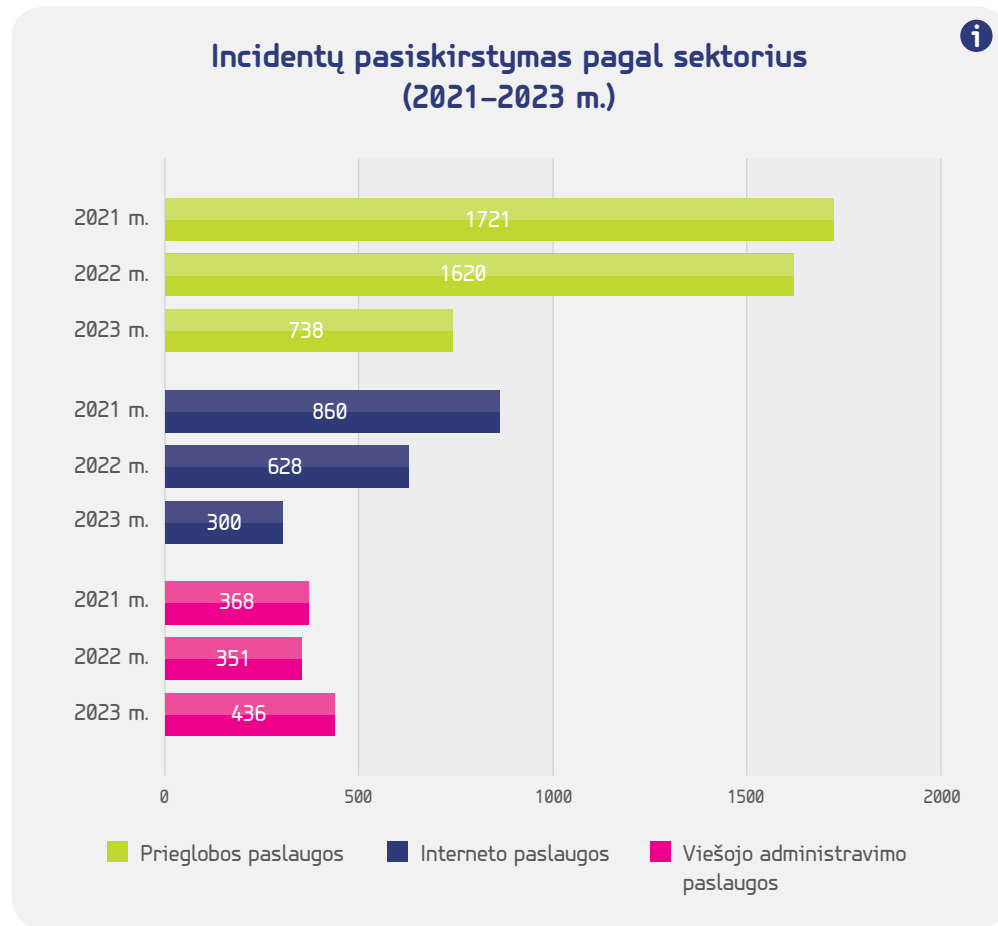
Apžvelgiamuose sektoriuose matomos tokios pat tendencijos kaip ir ankstesniais metais (žr. 7 pav.). Daugiausia incidentų įvyko interneto prieglobos paslaugų infrastruktūroje (angl. *hosting*), kurią kibernetiniai nusikaltėliai išnaudoja kibernetinėms atakoms vykdyti. Dalį paslaugų nusikaltėliai pasiekia įsilauždami į prastai apsaugotas organizacijų ar piliečių sistemas arba pasinaudodami suklastotomis tapatybėmis. Kadangi dalis Lietuvos prieglobos paslaugų teikėjų leidžia už paslaugas atsiskaityti kriptovaliuta, toks atsiskaitymo būdas sukuria papildomas galimybes nusikaltėliams pasislėpti, gerokai apsunkina jų atsekamumą arba padaro jį iš viso neįmanomą.

Antroje vietoje 2023 m. pagal fiksuojamų kibernetinių incidentų skaičių buvo viešasis administravimo sektorius. Šis sektorius nusikaltėlius domina dėl jautrios informacijos ir sektoriaus svarbos šalies valdymui. Į jį labiausiai taikosi APT grupuotės šnipinėdamos ir siekdamos sutrikdyti su valstybės valdymu susijusią veiklą.

Trečioje vietoje išlieka interneto paslaugų teikėjų (toliau – IPT) infrastruktūra ir prie jos prijungti fizinių asmenų galiniai įrenginiai, pavyzdžiui, kompiuteriai, išmanieji įrenginiai, internetinės vaizdo kameros, asmeniniai tinklo įrenginiai ir pan. Dėl prastos apsaugos, kai pamirštama laiku atnaujinti įrenginius, tinkamai juos sukonfigūruoti, šie įrenginiai dažnai tampa lengvu grobiu kibernetiniams nusikaltėliams, yra užvaldomi ir vėliau naudojami įvairioms kibernetinėms atakoms vykdyti.

7 pav. >

Incidentų pasiskirstymas pagal sektorius (2021–2023 m.) (šaltinis – NKSC)



Didžiausią žalą pagal kibernetinių atakų tipus ir metodus, NKSC duomenimis, 2023 m. darė elektroninius duomenis užšifruojančių ir išpirkos reikalaujančių kenkimo programinio kodo virusai, DDoS atakos, tiekimo grandinės<sup>08</sup> atakos, socialinės inžinerijos principais sukurtos atakos, kuriomis siekiama išvilioti įvairius jautrius duomenis.

### Elektroninius duomenis užšifruojantys ir išpirkos reikalaujantys kenkimo programinio kodo virusai

NKSC vertinimu, elektroninius duomenis užšifruojančių ir išpirkos reikalaujančių kenkimo programinio kodo virusų plitimo mastas 2023 m. tiek pasaulyje, tiek Lietuvoje toliau augo. Nuo 2022 m. išryškėjo dvigubo šantažo tendencija – kibernetiniai nusikaltėliai ne tik reikalauja išpirkos už duomenų iššifravimą, bet ir už pavogtų duomenų neišviešinimą.

Lietuvoje 2023 m. šių atakų taikiniais tapo tiek viešojo administravimo sektorius, tiek ir privačios įmonės. Vienas ryškesnių incidentų fiksuotas gruodžio mėn., kai buvo užšifruota dalis Vilniaus rajono savivaldybės duomenų ir dėl to sutriko savivaldybės veikla, vėlavo socialinės išmokos gyventojams<sup>09</sup>.

Kad būtų išvengta žalos, NKSC organizacijoms rekomenduoja<sup>10</sup> nuolat stebėti privilegijuotas teises, daryti jautrių duomenų ir informacinių sistemų atsargines kopijas bei testuoti atsarginių kopijų atstatymo procedūras.

08

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

09

„Gyventojų dėmesiui: visos socialinės išmokos bus išmokėtos.“ Prieiga per internetą <https://vrsa.lt/titulinio-naujienos/424/gyventoju-demesiui-visos-socialines-ismokos-bus-ismoketos:3677>.

10

Informacinis biuletenis. Duomenis šifruojantis ir išpirkos reikalaujantis kenkimo kodas. Prieiga per internetą [https://www.nksc.lt/doc/biuleteniai/2021-11-05\\_Ransomware.pdf](https://www.nksc.lt/doc/biuleteniai/2021-11-05_Ransomware.pdf).

### DDoS atakos

2023 m. visame pasaulyje buvo gausu DDoS atakų išpuolių prieš viešąjį administravimo sektorių. ENISA duomenimis<sup>11</sup>, maždaug 66 proc. atakų prieš viešųjų paslaugų sektorių buvo vykdomos dėl politinių tikslų, pusė visų analizuotų incidentų buvo susiję su Rusijos plataus masto agresija prieš Ukrainą. Visiškai paslaugas sutrikdė 56,8 proc. vykdytų atakų.

Analogiška tendencija 2023 m. buvo matoma ir Lietuvoje. DDoS atakos buvo intensyviai vykdomos siekiant daryti politinį ir informacinį spaudimą. Pačios atakos rimtų sutrikimų nesukėlė, nusikaltėliai dažnai jas vykdė siekdami atkreipti dėmesį į save ir padidinti savo žinomumą.

Siekiant tinkamai apsisaugoti nuo DDoS atakų, organizacijoms rekomenduojama savo iš interneto pasiekiamiems ištekliams taikyti DDoS apsaugos priemones. Daugelis didžiųjų pasaulinių DDoS apsaugos priemonių gamintojų mažoms ir vidutinėms organizacijoms savo priemones suteikia nemokamai.

### Tiekimo grandinių atakos

Tiekimo grandinių atakos tampa vis populiarsnės, nes puolamos silpnesnės tiekimo grandinės grandys gali suteikti nusikaltėliams prieigą prie didesnių ir atsparesnių organizacijų. Lietuvoje praeitais metais buvo registruoti incidentai, kai įsilaužus į informacinių ir ryšių technologijų (toliau – IRT) paslaugas teikiančias įmones buvo pasiekti tikrieji taikiniai – IRT paslaugas teikiančių įmonių klientai. Šių atakų sėkmė priklauso nuo to, kokie reikalavimai yra paslaugų teikimo sutartyse ir kaip užsakovai valdo savo rangovų prieigos teises.

ENISA duomenimis<sup>12</sup>, nuo tokio tipo atakų yra nukentėję nuo 39 proc. iki 62 proc. organizacijų. 2023 m. „Kurk Lietuvai“ komanda, bendradarbiaudama su NKSC, analizavo trečiųjų šalių valdymo Lietuvoje situaciją ir pateikė rekomendacijas<sup>13</sup>.

Siekdamas suvaldyti šią riziką, NKSC organizacijoms rekomenduoja peržiūrėti sutartis su IRT paslaugų teikėjais ir produktų tiekėjais ir jose numatyti papildomus reikalavimus teikėjams užtikrinti, kad jų infrastruktūra yra tinkamai saugoma ar veikla sertifikuota pagal tarptautinį saugumo standartą. Privalu griežtai kontroliuoti IRT paslaugų teikėjų prieigos teises prie organizacijos kritinių sistemų, registruoti ir analizuoti specialistų veiksmus prisijungimo metu, vertinti IRT pakeitimų saugumą prieš juos taikant produkcijai.

### Socialinė inžinerija ir duomenų viliojimas

2023 m. 38 proc. visų NKSC registruotų incidentų buvo paremti socialinės inžinerijos metodais. Šis metodas ne tik populiarėjo, bet ir gerėjo siunčiamų apgaulingų žinučių kokybė.

NKSC kartu su įvairiomis organizacijomis vykdytų iš anksto neskelbtų pratybų „Kibernetinis skydas PhishEx“ rezultatai rodo, kad nusikaltėlių žinučių neatpažintų ir potencialiai žalingus veiksmus atliktų apie 16 proc. darbuotojų. Aukų klaidos tikimybė tiesiogiai priklauso nuo žinučių kokybės, tam nusikaltėliai puikiai išnaudoja GDI technologijas, kurios žinutes padaro dar sunkiau atpažįstamas. Sparčiai plečiantis skaitmeninei erdvei, į ją perkeliama vis daugiau jautrios informacijos, taip pat eksponentiškai didėja kritinių valstybės funkcijų priklausomybė nuo skaitmeninių paslaugų. Neišvengiamai didėja ir piktavalių motyvacija vykdyti kibernetinius nusikaltimus, siekiant įvairių

11

„Europos Sąjungos kibernetinio saugumo agentūros DDoS atakų grėsmių vertinimas“ (angl. *ENISA Threat Landscape for DoS Attacks*). Prieiga per internetą <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks>.

12

„ENISA gerosios praktikos užtikrinti tiekimo grandinių kibernetinį saugumą“ (angl. *Good Practices for Supply Chain Cybersecurity*). Prieiga per internetą <https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity>.

13

Detalesnė informacija apie 2023 m. „Kurk Lietuvai“ komandos projektą „Kibernetinis saugumas: kaip valstybė galėtų padėti užtikrinti trečiųjų šalių (kontraktorių) valdymą?“ ir jo išvadas pateikta 40 p.



tikslių – nuo finansinių iki valstybei kritinių paslaugų sutrikdymo tikslių. Negalima tikėtis, kad kibernetinių nusikaltimų mažės, tačiau būtina tinkamai tam pasiruošti. Organizacijoms taikant tinkamas saugumo priemonės, nuolat ugdant reikalingas kompetencijas bei laikantis elementarios kibernetinės higienos, galima kur kas daugiau išvengti incidentų, finansinės ir reputacinės žalos bei greitai atnaujinti kritines paslaugas.

## Kibernetinio saugumo stiprinimas

### Kenkimo interneto svetainių užkardymas

Kovai su kibernetinėmis grėsmėmis, ypač su žaibiškomis kibernetinėmis sukčiavimo atakomis, NKSC toliau tobulino organizacijų ir gyventojų apsaugai skirtą įrankį – DNS užkardą<sup>14</sup> (**8 pav.**). 2023 m. pabaigoje ši apsaugos priemonė buvo taikoma beveik 4 mln. mobiliojo ir 775 tūkst. fiksuoto interneto ryšio paslaugų naudotojų ir per dieną vidutiniškai apsaugojo daugiau kaip 2 tūkst. gyventojų, kurie, neatpažinę nusikaltėlių atsiųstos žinutės, bandė prisijungti prie pinigams ar jautriems duomenims išvilioti skirtų svetainių.

#### 8 pav. >

DNS užkarda  
(šaltinis – NKSC)



Taip pat NKSC pradėjo plėtoti ir blokuojamų domenų valdymo priemonę<sup>15</sup>, kuri efektyviau įgalina 7 kompetingas Lietuvos institucijas (Lietuvos policija, Lošimų priežiūros tarnyba, Lietuvos bankas, Lietuvos radijo ir televizijos komisija, Žurnalistų etikos inspektoriaus tarnyba, Valstybinė vartotojų teisių apsaugos tarnyba bei Narkotikų, tabako ir alkoholio kontrolės departamentas) nurodyti IPT blokuoti kenkimo išteklius internete.

Lietuva yra viena iš vos kelių Europos valstybių efektyviai taikanti priemonę, kuri leidžia naudotojus apsaugoti nuo kenkimo interneto svetainių. 2024 m. NKSC sieks maksimaliai automatizuoti procesus, intensyvinti tarpinstitucinį bendradarbiavimą ir dar geriau apsaugoti Lietuvos piliečius nuo žaibiškų sukčiavimo atakų ir kitų kenkimo interneto svetainių.

#### 14

NKSC sukurtas įrankio – DNS užkardos pristatymas. Prieiga per internetą <https://www.nksc.lt/uzkarda.html>.

#### 15

NKSC sukurtos blokuojamų domenų valdymo sistemos „Vasaris“ pristatymas. Prieiga per internetą <https://www.nksc.lt/vasaris.html>.

### Kibernetinio saugumo kompetencijų ugdymas

Kibernetinių kompetencijų ugdymas yra viena iš svarbiausių valstybės atsparumo didinimo priemonių nuolat keičiantis kibernetinėms grėsmėms. 2023 m. NKSC ypač daug dėmesio skyrė mokymams ir pratyboms, taip siekdamas stiprinti kibernetinio saugumo subjektų gebėjimus tinkamai valdyti rizikas, aptikti kibernetinius incidentus ir tinkamai į juos reaguoti.

2023 m. NKSC organizuotus įvairaus tipo teorinius mokymus baigė daugiau kaip 11,5 tūkst. asmenų iš viešojo administravimo sektoriaus įstaigų, nevyriausybinių organizacijų, smulkaus ir vidutinio verslo įmonių.

Siekdamas stiprinti šalies kritinės infrastruktūros atsparumą kibernetinėms grėsmėms, NKSC, bendradarbiaudamas su JAV karinio laivyno aukštąja mokykla (angl. *Naval Postgraduate School*), pirmą kartą suorganizavo Industrinių valdymo sistemų kibernetinio saugumo kursą. Kursą baigė 39 dalyviai iš Lietuvos ir Ukrainos<sup>16</sup>. 2023 m. taip pat inicijuotas nacionalinis industrinių valdymo sistemų kibernetinio saugumo kompetencijų ugdymo pajėgumo sukūrimas.

Siekdamas stiprinti šalies aukščiausio lygio sprendimų priėmėjų kompetencijas, NKSC kartu su Nacionaliniu krizių valdymo centru ir JAV Pensilvanijos nacionalinės gvardijos atstovais gegužės mėn. organizavo Lietuvos Respublikos Vyriausybės kanceliarijos, visų ministerijų ir svarbiausių šalies energetikos bendrovių atstovų strategines kibernetinio saugumo stalo pratybas „Kibernetinis skydas StratEx 2023“<sup>17</sup>. Pratybose buvo tikrinami institucijų ir įstaigų gebėjimai tinkamai veikti, jeigu prieš vieną iš strateginių šalies sektorių būtų įvykdyta didelio masto kibernetinė ataka ir dėl to sutriktų dalies kritinių paslaugų teikimas.



Mokymuose įgytas teorines žinias viešojo sektoriaus ir ypatingos svarbos informacinių išteklių personalas galėjo patikrinti NKSC organizuojamose didžiausiose nacionalinėse kibernetinio saugumo pratybose „Kibernetinis skydas“. 2023 m. pratybos buvo vykdomos trimis kryptimis. Be minėtų strateginio lygio pratybų „Kibernetinis skydas StratEx“, visus metus buvo rengiamos imitacinės socialinės inžinerijos pratybos „Kibernetinis skydas PhishEx“. Jose savo praktines žinias atpažinti kibernetinių nusikaltėlių žinutes patikrino 154 organizacijos. Organizacijų darbuotojams iš viso buvo išsiųsta daugiau kaip 200 tūkst. imitacinių piktavalių el. laiškų<sup>18</sup>. Pratybų rezultatai rodo, kad vidutiniškai duomenų viliojimo žinučių neatpažįsta ir potencialiai žalingus veiksmus atlieka apie 16 proc. darbuotojų. Kadangi duomenų viliojimo atakomis ne tik vykdomos asmens duomenų vagystės, bet ir daug sudėtingesnių įsilaužimų į vidinius organizacijos tinklus ir sistemas, organizacijos turi gerokai daugiau skirti dėmesio darbuotojų mokymams ir kibernetinio atsparumo stiprinimui.

#### 16

„Lietuvos ir Ukrainos atstovai sėkmingai baigė pirmą kartą surengtą pramoninių technologijų kibernetinio saugumo kursą.“ Prieiga per internetą [https://www.nksc.lt/naujienos/lietuvos\\_ir\\_ukrainos\\_atstovai\\_sekingai\\_baige\\_pirm.html](https://www.nksc.lt/naujienos/lietuvos_ir_ukrainos_atstovai_sekingai_baige_pirm.html).

#### 17

„Pratybose „Kibernetinis skydas STRATEX 2023“ tikrinti valstybės institucijų ir energetikos įmonių gebėjimai ir sąveika didelio masto kibernetinio incidento akivaizdoje.“ Prieiga per internetą <https://lrv.lt/lt/naujienos/pratybose-kibernetinis-skydas-stratex-2023-tikrinti-valstybes-instituciju-ir-energetikos-imoniu-gebėjimai-bei-saveika-didelio-masto-kibernetinio-incidento-akivaizdoje/>.

#### 18

„Pašto tarnybomis apsietančių internetinių sukčių neatpažintų kas septintas darbuotojas.“ Prieiga per internetą [https://www.nksc.lt/naujienos/pasto\\_tarnybotomis\\_apsietanciu\\_internetiniu\\_sukciu\\_.html](https://www.nksc.lt/naujienos/pasto_tarnybotomis_apsietanciu_internetiniu_sukciu_.html).

Pagrindinės pratybos „Kibernetinis skydas OpEx“, kaip ir kasmet, buvo organizuojamos spalio mėn. Jose 82 organizacijos (iš kurių 77 dalyvės yra valstybės informacinių išteklių (toliau – VII) ir YSII valdytojos) tikrino kibernetinių incidentų valdymo gebėjimus ir procesus, įsivertino savo organizacijos saugumo būklę. Pratybų rezultatai rodo didėjančią dalyvių kibernetinę brandą, nes beveik trečdaliu išaugo skaičius organizacijų, kurios pratybose ne tik tinkamai reagavo į kibernetinį incidentą, bet ir pateikė informaciją apie incidentą NKSC. 2023 m. tokių organizacijų buvo 76 (2022 m. – 54). Šiose pratybose dalyviai taip pat galėjo patikrinti savo gebėjimus tinkamai informuoti visuomenę apie patirtą kibernetinį incidentą. 2023 m. šia galimybe pasinaudojo apie 50 organizacijų ir tai yra beveik dvigubai daugiau nei ankstesniais metais.

Taip pat šalies kibernetinio saugumo specialistai savo praktinius įgūdžius aptikti ir užkardyti kibernetinius incidentus galėjo stiprinti NKSC virtualiame pratybų poligone (angl. *Cyber Range*). 2023 m. šia galimybe pasinaudojo 356 asmenys (2022 m. – 221), buvo įvykdytos 373 mokymo sesijos (2022 m – 223). NKSC virtualus pratybų poligonas 2023 m. pirmą kartą panaudotas ir Lietuvos šaulių sąjungos organizuotame hakatone „Ugninis skydas 2023“<sup>19</sup>.

NKSC 2023 m. sukūrė nuotolinių mokymų sistemą, kurioje kibernetinio saugumo subjektų personalas ir atskiri asmenys gali susipažinti su kibernetinio saugumo pagrindais. Be to, sistemoje prieinami ir vadovams skirti mokymai, kuriuose atkreipiamas dėmesys į kibernetinio saugumo rizikas. Kursų pabaigoje dalyviai turi išlaikyti testą ir gauti kursų baigimą patvirtinantį sertifikatą. NKSC nuotolinių mokymų sistema pasiekama <https://mokymai.nksc.lt>.

## Išmoktos karo Ukrainoje pamokos

Jau dvejus metus vykstantis plataus masto karas Ukrainoje ir toliau veikė bendrą regiono kibernetinio saugumo aplinką. 2023 m. NKSC, bendradarbiaudamas su ekspertais iš Ukrainos, Lenkijos, Sakartvelo ir JAV, parengė studiją apie kibernetines pamokas, išmoktas karo Ukrainoje metu (angl. *Report on Cyber Lessons Learned during the War in Ukraine*)<sup>20</sup>.

Identifikavus pagrindines karo Ukrainoje kibernetinio saugumo pamokas, 2023 m. buvo pradėti pokyčiai, kurie padės stiprinti Lietuvos kibernetinę gynybą ir atsparumą: įkurtos pirmosios sektorinės apsaugos kibernetinio saugumo informacija platformos, plėtojamas keitimasis aktualia informacija su tarptautiniais partneriais, pradėti parengiamieji Lietuvos kariuomenės Kibernetinio saugumo valdybos kūrimo darbai, vykdoma aktyvi kibernetinio saugumo kompetencijų ugdymo veikla.

## Nacionaliniam saugumui užtikrinti svarbių objektų apsauga

NKSC prisidėjo stiprinant perkančiųjų organizacijų tiekimo grandinės saugumą, vykdamas nacionaliniam saugumui užtikrinti svarbių įmonių ir YSII valdytojų pirkimų priežiūrą. NKSC šią funkciją iš KAM perėmė 2023 m. viduryje ir per tą laikotarpį iš viso svarstė 27 medžiagos paketus, atliko 434 vertinimus. Vertinimai ir rekomendacijos buvo pateikti Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo komisijai galutiniams sprendimams.

## Atsakingas kibernetinio saugumo spragų atskleidimas

2023 m. atsakingi pranešėjai aptiko 74 kibernetinio saugumo spragas įvairiose Lietuvos informacinėse sistemose ir apie tai informavo NKSC laikydamiesi atsakingo kibernetinių spragų atskleidimo principų<sup>21</sup>.

19 „Saugumo inovacijų hakatonas baigėsi: tarp prizininkų – minų ieškantis DI, dronai kamikadzės bei kosminis ryšys.“ Prieiga per internetą <https://www.sauliusajunga.lt/saugumo-inovaciju-hakatonas-baigesi-tarp-prizininku-minu-ieskantis-di-dronai-kamikadzės-bei-kosminis-rysys/>.

20 „Studija apie kibernetines pamokas, išmoktas karo Ukrainoje metu“ (angl. *Report on Cyber Lessons Learned during the War in Ukraine*). Prieiga per internetą [https://www.nksc.lt/doc/rkgc/report\\_on\\_cyber\\_lessons\\_learned\\_during\\_the\\_war\\_in\\_ukraine.pdf](https://www.nksc.lt/doc/rkgc/report_on_cyber_lessons_learned_during_the_war_in_ukraine.pdf).

21 Lietuvos Respublikos Seimas įteisino atsakingą kibernetinių spragų atskleidimą. Prieiga per internetą [https://www.nksc.lt/naujienos/lr\\_seimas\\_iteisino\\_atsakinga\\_kibernetiniu\\_spragu\\_a.html](https://www.nksc.lt/naujienos/lr_seimas_iteisino_atsakinga_kibernetiniu_spragu_a.html).

Buvo pranešta apie spragas, kuriomis pasinaudojant iš sistemų (neretai valstybės informacinės sistemos ar registry, kuriuose kaupiama Lietuvos gyventojų informacija) buvo galima nutekinti jautrius duomenis.

Palyginti su ankstesniais metais, iš pranešėjų sulaukta 45 proc. daugiau pranešimų. NKSC dėkoja visiems kompetentingiems ir sąmoningiems piliečiams bei skatina ir toliau tai daryti.

## Kibernetinio saugumo patikrinimai

Siekdamas surinkti objektyvią informaciją apie YSII būklę, 2023 m. NKSC atliko arba koordinavo 17 įvairaus tipo išsamių patikrinimų, iš jų 14 buvo vykdomi bendradarbiaujant su ENISA bei jos įgaliojais paslaugų teikėjais (atstovais iš verslo sektoriaus). Dvylikoje organizacijų, kurios valdo YSII arba VII, buvo atliekamas informacinių sistemų, tinklo atsparumo įsilaužimams testavimas. Bendradarbiaujant su ENISA ir jos įgaliojais paslaugų teikėjais, papildomai dviejose organizacijose buvo surengtos socialinės inžinerijos pratybos, o vienoje organizacijoje atliktas atitikties kibernetinio saugumo teisės aktų reikalavimams ir rizikų vertinimas, tinklo skenavimas, atitikties tarptautiniams teisės aktams vertinimas.

## NATO viršūnių susitikimas Vilniuje

NKSC aktyviai prisidėjo užtikrinant kibernetinį saugumą per NATO viršūnių susitikimą Vilniuje. Pasirengimo laikotarpiu NKSC atliko 25 organizacijų, kurios buvo įtrauktos į renginio organizatorių sąrašą, plataus masto kibernetinio saugumo rizikos vertinimą, pateikė rekomendacijas dėl rizikų mažinimo priemonių taikymo<sup>22</sup>. Paties NATO viršūnių susitikimo Vilniuje metu liepos mėn. NKSC įsteigtame specialiaame Saugumo operacijų centre nuolatinį budėjimą vykdė NKSC, policijos ir kitų institucijų atstovai ir tarptautiniai partneriai.

Renginyje kibernetinių incidentų išvengti nepavyko, tačiau jie didelės žalos nepadarė, renginys vyko be sutrikimų, visos kritinės paslaugos buvo teikiamos tinkamai. Buvo fiksuoti keli hibridiniai incidentai, DDoS atakos<sup>23</sup>, identifiukuoti ir užkardyti bandymai sukurti su NATO viršūnių susitikimu susijusių tinklapių kopijas. Renginio pabaigoje, labai tikėtina, kad su Rusija siejama kibernetinė grupuotė paviešino perimtą viešai neprieinamą su susitikimu susijusią informaciją, siekdama diskredituoti Lietuvą tarptautinėje arenoje<sup>24</sup>.

### NKSC 2024 m. prioritetai



Pagalba ir parama vystant viešojo administravimo sektoriaus taktinius kibernetinės gynybos pajėgumus.



Kibernetinio saugumo kompetencijų ugdymo portfelio įvairioms grupėms plėtra.



Pasiruošimas vykdyti naujas funkcijas pagal rudenį Lietuvoje įsigaliosiantį TIS 2 direktyvos teisinį reglamentavimą.



Tolesnis sprendimų, padedančių stiprinti ir siekti glaudesnio tarpinstitucinio bendradarbiavimo, vystymas.

22 NKSC rekomendacijos viešbučiams dėl bevielio tinklo kibernetinio saugumo stiprinimo. Prieiga per internetą [https://www.nksc.lt/doc/biuleteniai/2023\\_06\\_15\\_bevielio\\_tinklo\\_rekomendacijos\\_viesbučiams.pdf](https://www.nksc.lt/doc/biuleteniai/2023_06_15_bevielio_tinklo_rekomendacijos_viesbučiams.pdf).

23 „Prieš žiniasklaidos portalus – kibernetinės atakos: stebimi pasiekiamumo sutrikimai.“ Prieiga per internetą <https://www.delfi.lt/m360/naujausi-straipsniai/pries-ziniasklaidos-portalus-kibernetines-atakos-stebimi-pasiekiamumo-sutrikimai-93906999>.

24 2023 m. grėsmių nacionaliniam saugumui vertinimas. Prieiga per internetą <https://www.aotd.lt/gresmiu-vertinimas>.

## Projektas „Kibernetinis saugumas: kaip valstybė galėtų padėti užtikrinti trečiųjų šalių (kontraktorių) valdymą?“

Su trečiosiomis šalimis susiję kibernetiniai incidentai yra pasaulinio masto problema. ENISA duomenimis<sup>25</sup>, grėsmės, susijusios su tiekimo grandinėmis, ir informacinių ryšių paslaugų teikėjų pažeidžiamumas taps viena iš dešimties opiausių problemų visame pasaulyje.

Lietuvoje šiuo metu nėra aiškių reguliavimo struktūrų ir procedūrų, kurios leistų efektyviai valdyti trečiųjų šalių kibernetinį saugumą. Dalinę kontrolę vykdo NKSC ir teikia sandorių vertinimus Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo komisijai, tačiau tai apima tik tas organizacijas, kurios priklauso YSII arba yra svarbios nacionaliniam saugumui. Kiti subjektai lieka pažeidžiami dėl trečiųjų šalių saugumo spragų ir grėsmių, nes labai dažnai šiai sričiai ir su ja susijusioms rizikoms valdyti neskiria pakankamai dėmesio. NKSC beveik kasmet fiksuoja kibernetinius incidentus, kurie įvyksta dėl netinkamai valdomų trečiųjų šalių ir jų teikiamų paslaugų<sup>26</sup>.

2023 m. „Kurk Lietuvai“ komanda bendradarbiaudama su NKSC parengė studiją<sup>27</sup>. Joje nagrinėjama trečiųjų šalių rizikos valdymo problemos Lietuvoje ir užsienio šalių gerieji pavyzdžiai, kurie buvo naudojami kaip pagrindas trečiųjų šalių valdymo Lietuvoje gairėms parengti.

Užsienio šalių patirties pavyzdžiai atskleidžia, kad tiekimo grandinės saugumui užtikrinti būtinas sąmoningumas kibernetinio saugumo srityje turi būti stiprinamas kompleksiskai, t. y. naudojant įvairias priemones: sertifikatus, mokymus, minimalius kibernetinio saugumo standartus, įrankius, platformas, savęs vertinimo klausimynus ir vadovus su rekomendacijomis. Trečiosioms šalims valdyti naudojami skirtingi standartai (NIST, ISO27002, CIS, „Zero Trust“), taip pat nacionaliniai modeliai (Ispanijos IMC ir C4V), tačiau jie nėra privalomi.

Lietuvoje kibernetinio saugumo paslaugų teikėjams (trečiosioms šalims) privalomi organizaciniai ar techniniai reikalavimai nėra taikomi, jie taip pat nėra įpareigoti informuoti apie patirtus kibernetinius incidentus, trečiosios šalys nėra įtraukiamos į rizikos kategoriją ir nėra laikomos kontroliuojama tiekimo grandinės rizika (išskyrus Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo apibrėžiama apimtimi<sup>28</sup>).

25

„ENISA gerosios praktikos užtikrinti tiekimo grandinių kibernetinį saugumą“ (angl. *Good Practices for Supply Chain Cybersecurity*). Prieiga per internetą <https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity>.

26

„Galimai išnaudojant vieno svetainių gamintojo pažeidžiamumą buvo įsilaužta į maždaug 10 Lietuvos interneto svetainių.“ Prieiga per internetą [https://www.nksc.lt/naujienos/isnaudojant\\_vieno\\_svetainiu\\_gamintojo\\_pazeidziamum.html](https://www.nksc.lt/naujienos/isnaudojant_vieno_svetainiu_gamintojo_pazeidziamum.html).

27

2023 m. „Kurk Lietuvai“ projektas „Kibernetinis saugumas: kaip valstybė galėtų padėti užtikrinti trečiųjų šalių (kontraktorių) valdymą?“ Prieiga per internetą <https://kurk.lt/projekta/kibernetinis-saugumas-kaip-valstybe-galetu-padeti-uztikrinti-treciuju-saliu-kontraktoriu-valdyma>.

28

Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas numato, kad nacionaliniam saugumui užtikrinti svarbių objektų (įmonės, įrenginiai ir turtas bei ūkio sektoriai) ir nacionaliniam saugumui užtikrinti svarbių įmonių, įrenginių ir turto apsaugos zonose esantis turtas ir teritorija bei YSII valdytojų sandoriai turi būtų apsaugoti nuo visų galinčių kelti grėsmę nacionalinio saugumo interesams rizikos veiksmų, ir šalinti tokių veiksmų atsiradimo priežastis ir sąlygas.

0100  
11011  
01011

## Rekomendacijos sprendimams Lietuvoje:

- ✓ Struktūruoti kibernetinio saugumo santykius su tiekėjais. Pavyzdžiui, remdamasi Danijos pavyzdžiu Lietuva galėtų parengti kibernetinių saugumo santykių su tiekėjais valdymo gaires arba numatyti proceso etapus.
- ✓ Atlikti trečiųjų šalių vertinimus ir suteikti įvairaus tipo sertifikatus. Pavyzdžiui, pasinaudodama Austrijos pavyzdžiu Lietuva galėtų sukurti „Cyber Trust“<sup>29</sup> sertifikavimo lygį, kurie padėtų įvertinti tiekimo grandinės dalyvių kibernetinio saugumo būklę. Tai galėtų padėti organizacijoms lengviau pasirinkti saugius ir patikimus tiekėjus.
- ✓ Sudaryti tiekimo grandinės žemėlapi. Pavyzdžiui, remdamasi Didžiosios Britanijos pavyzdžiu Lietuva galėtų taikyti tiekimo grandinės žemėlapių sudarymo principą, kad identifikuotų potencialias rizikas ir sužinotų, kaip organizacijos procesus gali paveikti jų valdymo trečiosioms šalims.
- ✓ Sukurti standartus. Pavyzdžiui, remtis Prancūzijos modeliu ir skatinti organizacijas atitikti kibernetinio saugumo standartus.
- ✓ Palengvinti viešųjų pirkimų procesą. Pavyzdžiui, sukurti skirtingas preliminaras sutartis (sutarčių šablonus) su paslaugų teikėjais.
- ✓ Dalytis informacija. Pavyzdžiui, remiantis ENISA pavyzdžiu skatinti tiekėjus informuoti ir viešai skelbti apie informaciją apie kibernetinius incidentus, susijusius su tiekimo grandinės atakomis.



29

„Cyber Trust Austria“ – tai Austrijos kibernetinio saugumo sertifikavimo sistema ir kokybės ženklas. Prieiga per internetą <https://www.cyber-trust.at/en/labeloverview>.



# Asmens duomenų apsauga, saugumo užtikrinimas ir pažeidimų prevencija



Dijana Šinkūnienė,  
VDAI direktorė

## Vadovo žodis

Valstybinė duomenų apsaugos inspekcija, būdama viena iš institucijų, įgyvendinančių kibernetinio saugumo politiką Lietuvoje, 2023 m. prisidėjo prie šios sistemos užtikrinimo dalyvaudama Kibernetinio saugumo tarybos veikloje, kibernetinio saugumo pratybose, bendradarbiaudama tiriant kibernetinius incidentus ir vykdydama prevencinę veiklą. Valstybinės duomenų apsaugos inspekcijos patirtis tiriant asmens duomenų saugumo pažeidimus rodo, kad dėmesys tinkamam saugumo užtikrinimui organizacijose vis dar nėra pakankamas. Suprasdama organizacijų lūkesčius Valstybinė duomenų apsaugos inspekcija 2023 m. ir toliau nuosekliai siekė vieno iš veiklos prioritetų „didinti duomenų valdytojų, duomenų apsaugos pareigūnų ir duomenų subjektų žinias, kompetenciją ir įgūdžius asmens duomenų apsaugos srityje“.

Atsižvelgiant į 2023 m. organizacijų patirtus iššūkius dėl įvairių kibernetinių incidentų, kurių metu buvo pažeisti ir asmens duomenys, ateityje turės būti skiriama daugiau dėmesio tinkamų saugumo priemonių užtikrinimui bei šviečiamosios veiklos vykdymui.



## KĄ SAUGO?

- ✓ Žmogaus teisę į asmens duomenų apsaugą.



## NUO KO SAUGO?

- ✓ VDAI prižiūri, ar viešojo ir privataus sektoriaus organizacijos tinkamai įgyvendina teisės į asmens duomenų apsaugą reikalavimus ir, tvarkydamos asmens duomenis, užtikrina, kad jie būtų tinkamai apsaugoti nuo praradimo, sunaikinimo ar sugadinimo.



## KAIP SAUGO?

- ✓ Vykdydama organizacijų asmens duomenų tvarkymo ir saugumo užtikrinimo stebėseną ir patikrinimus.
- ✓ Nagrinėdama pranešimus apie ADSP ir atlikdama tyrimus.
- ✓ Teikdama organizacijoms išankstines konsultacijas, susijusias su naujų technologinių sprendimų vertinimu dėl organizacinių ir techninių priemonių tinkamumo ir duomenų tvarkymo saugumo.
- ✓ Atlikdama asmens duomenų tvarkymo auditus valstybės informacinėse sistemose, kai tai numato ES teisės aktai.



VALSTYBINĖ  
DUOMENŲ  
APSAUGOS  
INSPJEKCIJA

## Svarbiausi 2023 m. įvykiai ir tendencijos



2023 m. VDAI gavo mažiau pranešimų apie ADSP negu 2022 m.



2023 m. Lietuvoje paveiktų duomenų subjektų skaičius sumažėjo daugiau kaip 3 kartus.



Palyginti su 2022 m. duomenimis, ADSP dėl žmogiškosios klaidos daugėja.

76%

Pagal ADSP pobūdį Lietuvoje statistiškai vyrauja konfidencialumo pažeidimai, jų skaičius per 2023 m. sudarė net 76 proc. visų atvejų.



2023 m. įvykusių ADSP dėl kibernetinio incidento yra 20 proc. mažiau negu 2022 m.

49%

Nors kibernetiniai incidentai sudarė tik 15 proc. visų 2023 m. įvykusių ADSP, bet jų metu buvo paveikti net 49 proc. (iš visų 2023 m. paveiktų subjektų) subjektų duomenys.



Duomenų valdytojai 2023 m. pranešė apie įvykdytas duomenų užšifravimo ir išpirkos reikalavimo atakas, taip pat buvo vykdomos prisijungimo duomenų užpildymo (angl. *Credential Stuffing*) atakos.



2023 m. kovo mėn. VDAI, atlikusi ADSP tyrimą, priėmė sprendimą privačiai bendrovei skirti 20 tūkst. eurų baudą už nustatytus BDAR nuostatų pažeidimus.



2023 m. VDAI organizuoti šviečiamieji renginiai sulaukė 14 731 dalyvių.

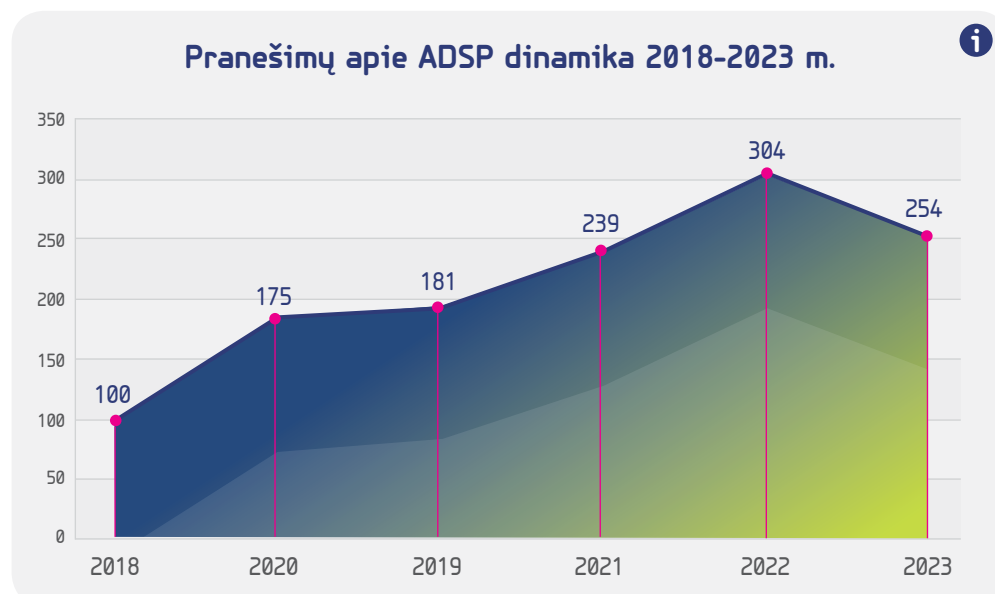


## 1 Asmens duomenų saugumo pažeidimų Lietuvoje situacijos analizė

2023 m. VDAI gavo 254 pranešimus apie ADSP, tais metais Lietuvoje paveiktų duomenų subjektų skaičius – 571 833 (žr. **1 pav.**). Palyginti su ankstesnių metų duomenimis, VDAI gavo mažiau pranešimų apie ADSP negu 2022 m. (2022 m. – 304), taip pat Lietuvoje paveiktų duomenų subjektų skaičius sumažėjo daugiau negu 3 kartus (2022 m. – 1 955 382) (žr. **2 pav.**). Tai rodo teigiamą tendenciją, didėjantį organizacijų sąmoningumą ir efektyvesnių apsaugos priemonių diegimą ir naudojimą Lietuvoje per praėjusius metus. Sustiprėjęs organizacijų rūpinimasis duomenų saugumu taip pat yra griežtesnės priežiūros ir šviečiamosios veiklos rezultatas. Tai svarbus žingsnis siekiant didesnio asmens duomenų saugumo užtikrinimo Lietuvoje.

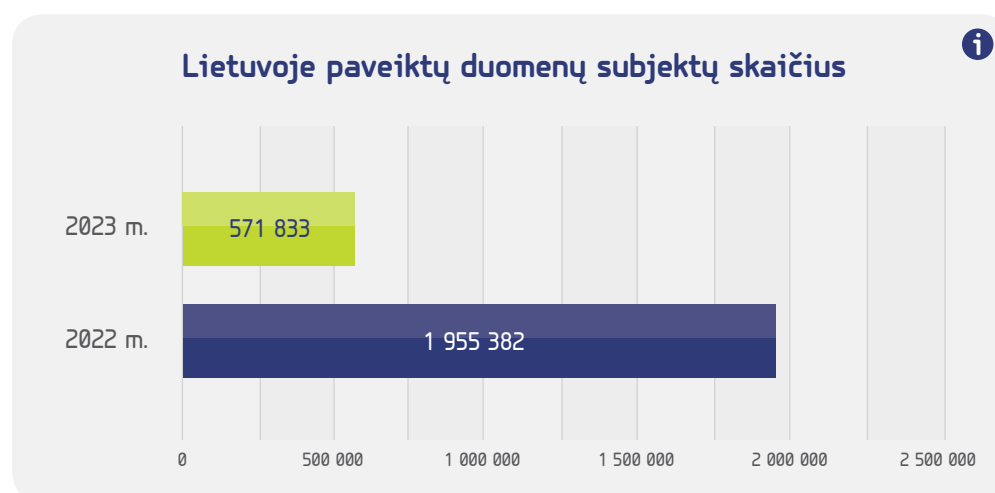
### 1 pav. >

1 pav. 2018–2023 m. gautų pranešimų apie ADSP dinamika (šaltinis – VDAI).



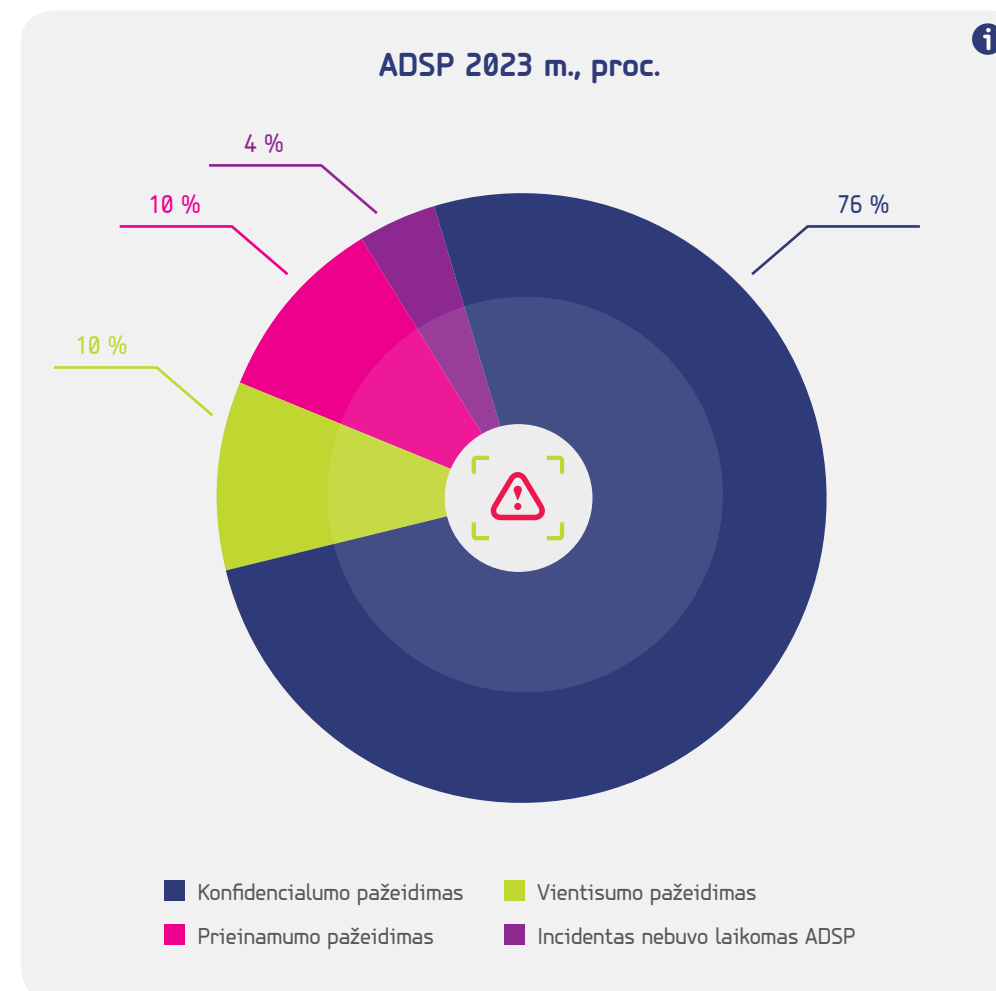
### 2 pav. >

Lietuvoje paveiktų duomenų subjektų skaičius (šaltinis – VDAI).



### < 3 pav.

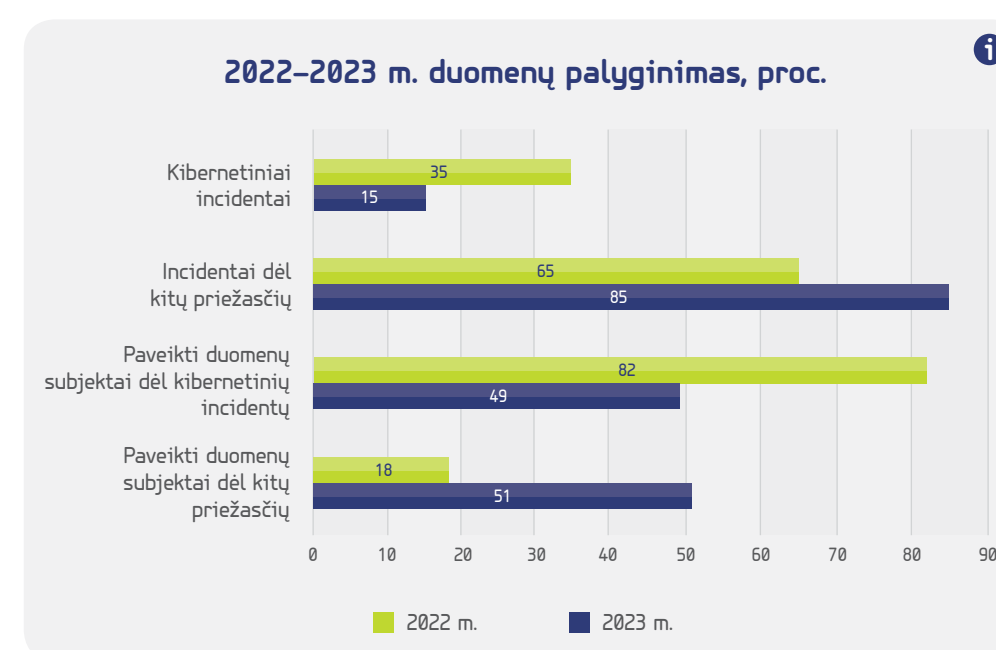
ADSP 2023 m., proc.  
(šaltinis – VDAI).



Pagal ADSP pobūdį Lietuvoje statistiškai vyrauja konfidencialumo pažeidimai (žr. **3 pav.**). Šių pažeidimų skaičius per 2023 m. sudarė net 76 proc. visų pažeidimų, 10 proc. atvejų – vientisumo pažeidimai, 10 proc. – prieinamumo pažeidimai ir 4 proc. atvejų incidentas nebuvo laikomas ADSP (neatitiko sąvokos).

### < 4 pav.

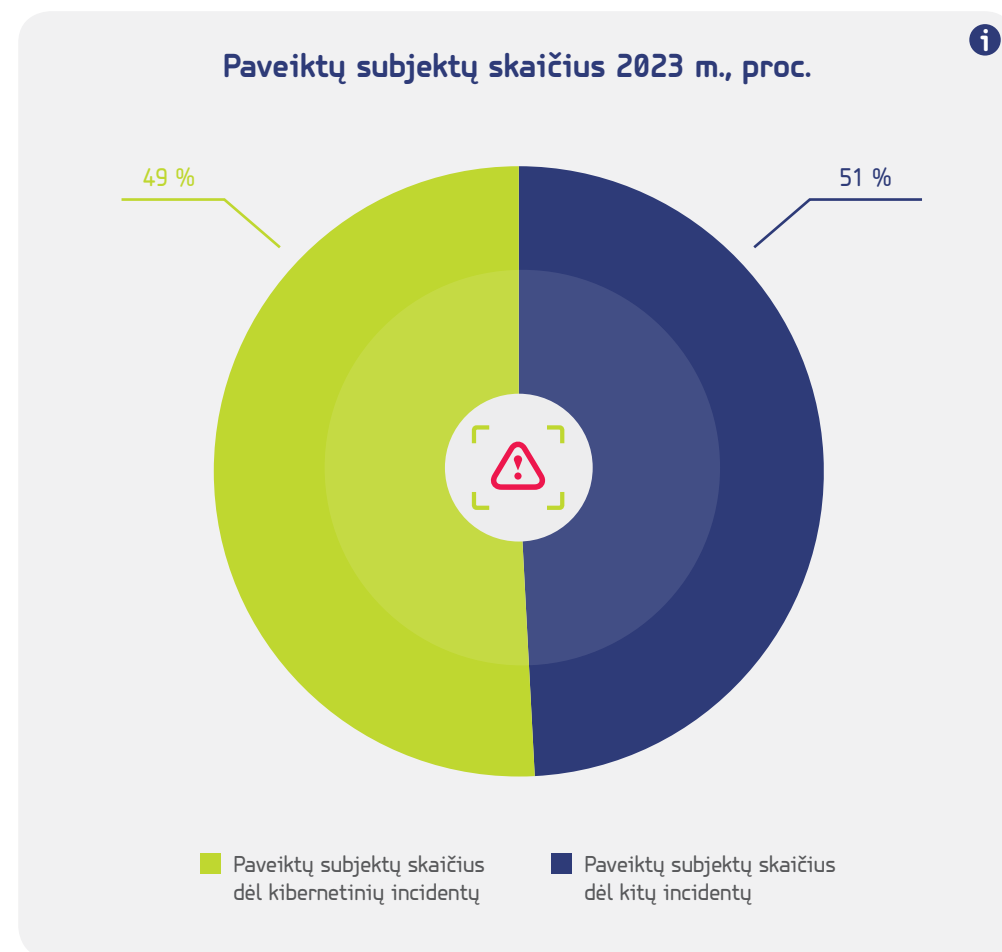
2022–2023 m. duomenų palyginimas, proc.  
(šaltinis – VDAI).



Palyginti su praėjusių metų duomenimis, pažymėtina, kad ADSP dėl kibernetinio incidento įvyko mažiau negu 2022 m. (2022 m. – 35 proc.) (žr. **4 pav.**).

### 5 pav. >

Paveiktų subjektų skaičius 2023 m., proc. (šaltinis – VDAI).



Svarbu paminėti, kad nors kibernetiniai incidentai sudarė tik 15 proc. visų 2023 m. įvykusių ADSP, bet jų metu buvo paveikti net 49 proc. (iš visų 2023 m. paveiktų subjektų) subjektų duomenys, dėl kitų priežasčių buvo paveikti 51 proc. subjektų duomenys (žr. **5 pav.**). Palyginti su praėjusių metų duomenimis, pažymėtina, kad dėl 2022 m. įvykusių kibernetinių incidentų buvo paveikta 82 proc. duomenų subjektų (iš visų 2022 m. paveiktų duomenų subjektų skaičiaus), o dėl kitų priežasčių – 18 proc. duomenų subjektų.

VDAI 2023 m. gavo 37 pranešimus apie kibernetinius incidentus, iš kurių 24 kibernetinių incidentų tyrimas baigtas 2023 m., o 13 nagrinėjimas bus tęsiamas 2024 m. 2023 m. duomenų valdytojai pranešė apie įvykdytas duomenų užšifravimo ir išpirkos reikalavimo atakas<sup>01</sup>, kurių metu buvo ne tik užšifruoti serveriai, buhalterinės programos ir kitos sistemos, bet ir nukopijuoti juose esantys duomenys, reikalauja išpirkos už duomenų dešifravimą ir pateikti grasinantys pranešimai nukopijuotus asmens duomenis paskelbti tamsiojo interneto forumuose (angl. *Dark Web Forums*). VDAI dėl šių ADSP pradėjo tyrimą savo iniciatyva. Taip pat buvo vykdomos prisijungimo duomenų užpildymo (angl. *Credential Stuffing*) kibernetinės atakos, kurių metu piktaivaliai, pasinaudoję nutekėjusiais prisijungimo duomenimis, bandė prisijungti prie kitiems asmenims priklausančių paskyrų. 2023 m. ADSP metu buvo užfiksuotos ir DDoS atakos.

<sup>01</sup>

2023 m. buvo gauta 12 pranešimų apie ADSP, kurie įvyko dėl šifruojamojo kenkimo programinio kodo atakų. Piktavaliai, vykdydami įvairias socialinės inžinerijos atakas, pasitelkdami gerai apgalvotus scenarijus, siekė gauti įvairius prisijungimo duomenis.

VDAI atkreipia dėmesį, kad 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) nustato pranešimo VDAI ir duomenų subjektui apie įvykusį ADSP turinį. Dažniausios pranešimo VDAI apie įvykusį ADSP klaidos susijusios su tuo, kad:

- ⚠ nepakankamai išsamiai aprašomos įvykusio ADSP aplinkybės;
- ⚠ duomenų subjektai netinkamai informuojami apie įvykusį ADSP (pavyzdžiui, nenurodoma kokių priemonių jie galėtų imtis galimoms neigiamoms pasekmėms sumažinti ar į ką organizacijoje, kurioje įvyko ADSP, galėtų kreiptis dėl papildomos informacijos);
- ⚠ neaprašomos priemonės, kurių ėmėsi arba ketina imtis duomenų valdytojas, kad būtų pašalintas ADSP bei sumažintas pavojus duomenų subjektų teisėms ir laisvėms ir kad ADSP ateityje nepasikartotų.

Atsižvelgdama į tai, VDAI rekomenduoja naudoti VDAI patvirtintą pranešimo apie ADSP formą<sup>02</sup> ir joje pateikti išsamią informaciją apie įvykusį ADSP. Taip pat VDAI, susipažinusi su pranešimų apie ADSP turiniu, dažnai nustato, kad pavojus asmens teisėms ir laisvėms dėl įvykusio ADSP yra vertintas formaliai, t. y. nurodoma, kad pavojus kilo arba nekilo, tačiau nepateikiama argumentų, dėl kokių priežasčių daromos tokios išvados. VDAI atkreipia dėmesį, kad atlikdamas pavojaus duomenų subjektų teisėms ir laisvėms vertinimą duomenų valdytojas turėtų vadovautis BDAR preambulės 75 konstatuojamąja dalimi, rekomendacija<sup>03</sup> bei gairėmis<sup>04</sup>.

VDAI atkreipia dėmesį į didėjančią naudojamos programinės ir techninės įrangos gamintojų ar debesijos paslaugų teikėjų patikimumo, reputacijos ir kilmės šalies įvertinimo ir potencialių rizikų duomenų saugumui nustatymo svarbą. Organizacijos, duomenims tvarkyti pasirinkdamos įrangą ir paslaugų teikėjus, turėtų įvertinti, ar asmens duomenys nebus perduodami į trečiąsias valstybes, neužtikrinančias tinkamo asmens duomenų apsaugos lygio.

2023 m. ADSP atvejais išryškėjo prieigos kontrolės valdymo organizacijų kompiuterių tinkluose spragos – suteikiant prieigą netaikyti apribojimai ir tinklo segmentavimas, nesilaikyta „mažiausių teisių privilegijos“ ir „būtina žinoti“ principų, netaikytas dviejų veiksmų autentifikavimas (angl. *2 factor authentication* (2FA)) aukštesnes teises turintiems, nuotoliniu būdu besijungiantiems ar virtualų privatų tinklą naudojančiams asmenims. Taip pat įvykus duomenų užšifravimo ir išpirkos reikalavimo atakoms, piktaivaliai dažnai pašalina duomenų atsargines kopijas ir įvykių žurnalinius įrašus, kurie buvo saugomi toje pačioje vietoje, kaip ir užšifruoti duomenys, dėl to duomenų valdytojai nebegali lengvai atkurti duomenų prieinamumo ir tinkamai atlikti kibernetinio incidento ir ADSP tyrimo.

VDAI pažymi, kad organizacijoms būtina metodinė pagalba, kaip atpažinti ADSP, nes pasitaikė nemažai atvejų, kai VDAI buvo pranešama apie ADSP, nors incidentai neatitiko ADSP sąvokos. Atsižvelgdama į tai, 2023 m. VDAI parengė metodinį dokumentą, kuris turėtų padėti organizacijoms vertinti įvykusius incidentus ir poreikį apie juos pranešti VDAI.<sup>05</sup>

### Detalesnė informacija apie kiekvieną nusikaltimą elektroninių duomenų ir informacinių išteklių saugumui pagal LR BK 196-198<sup>2</sup> str.:

- ⚠ 2023 m. VDAI skyrė 2 administracines baudas dėl bendrovėje ir viešojo sektoriaus įstaigoje įvykusių ADSP. Per incidentą buvo pažeistas apie 55 tūkst. duomenų subjektų (vartotojų) asmens duomenų konfidencialumas. VDAI nustatė, kad dėl netinkamai vykdomos prieigų kontrolės ir autentifikavimo buvo prisijungta prie bendrovės duomenų bazės ir nutekinti bendrovės klientų duomenys (nustatyti BDAR 5 straipsnio 1 dalies e ir f punktų, 32 straipsnio 1 dalies b ir d punktų pažeidimai).

<sup>02</sup>

Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. rugpjūčio 29 d. įsakymas Nr. 1T-82(1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“. Prieiga per internetą <https://www.e-tar.lt/portal/lt/legalAct/ce581900ab7a11e88f64a5ecc703f89b>.

<sup>03</sup>

2018 m. liepos 2 d. VDAI rekomendacija dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo, pranešimo apie juos ir dokumentavimo tvarkos. Prieiga per internetą [https://vdoi.lrv.lt/uploads/vdoi/documents/files/Rekomend\\_ADSP\\_2018.pdf](https://vdoi.lrv.lt/uploads/vdoi/documents/files/Rekomend_ADSP_2018.pdf).

<sup>04</sup>

2017 m. spalio 3 d. 29 straipsnio duomenų apsaugos darbo grupės gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679 (nauja redakcija nuo 2023 m. kovo 28 d.) bei 2021 m. gruodžio 14 d. Europos duomenų apsaugos valdybos gairės 01/2014 dėl pranešimo apie asmens duomenų saugumo pažeidimą pavyzdžių. Prieiga per internetą <https://ec.europa.eu/newsroom/article29/items/612052>.

<sup>05</sup>

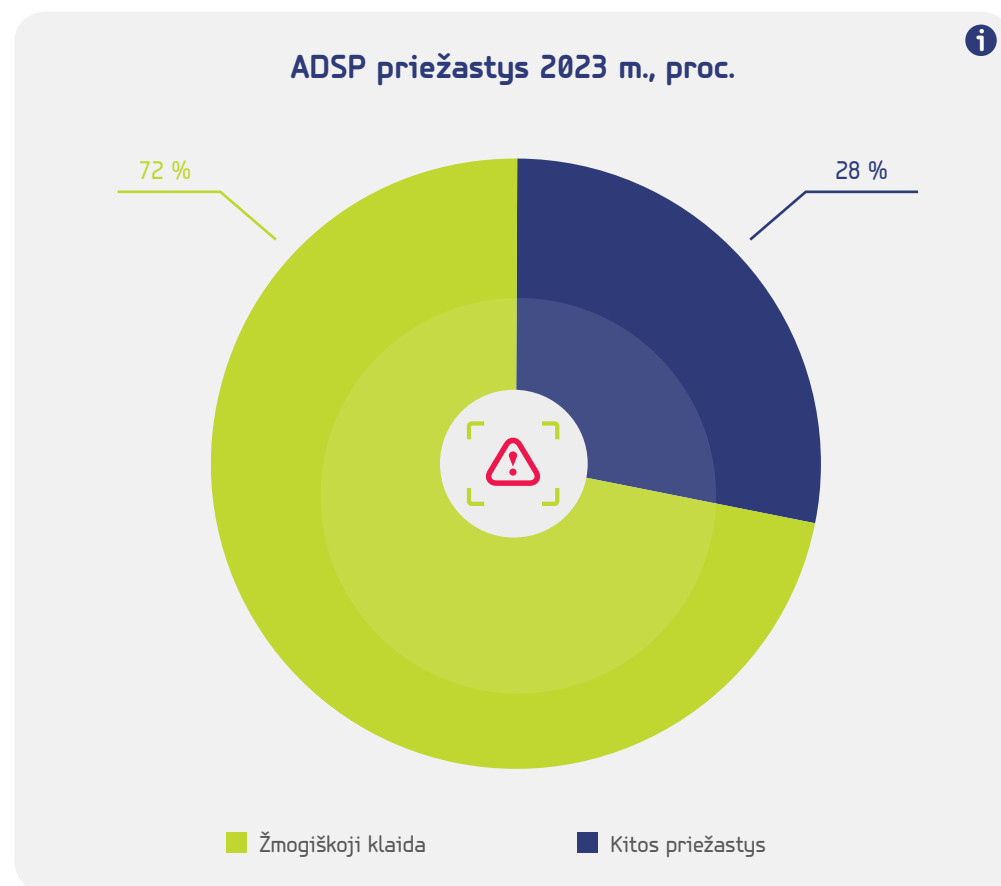
VDAI patarimai dėl pasitaikančių atvejų, kai pranešama apie įvykusius incidentus, kurie nėra laikomi ADSP. Prieiga per internetą <https://vdoi.lrv.lt/lt/naujienos/vdai-pataria-dėl-pasitaikančių-atvejų-kai-pranesama-apie-ivykusius-incidentus-kurie-nera-laikomi-asmens-duomeniu-saugumo-pazeidimais/>.



⚠️ 2023 m. kovo mėn. VDAI, atlikusi ADSP tyrimą, priėmė sprendimą viešojo sektoriaus įstai-  
gai skirti 6 600 eurų baudą už nustatytus BDAR nuostatų pažeidimus. Per incidentą buvo  
pažeistas 13 525 duomenų subjektų (vartotojų) asmens duomenų konfidencialumas. VDAI  
nustatė, kad dėl neatnaujinamos programinės įrangos ir galimybės prie valdymo panelės  
prisijungti iš išorinio tinklo nenaudojant dviejų veiksmų autentifikavimo sukčiai prisijungė  
prie interneto svetainės, nukopijavo vartotojų duomenų bazę ir paskelbė duomenis tamsiojo  
internetu forume (nustatyti BDAR 5 straipsnio 1 dalies c, e, f punktų, 24, 25 ir 32 straipsnių  
pažeidimai).

Palyginti su praėjusių metų duomenimis, ADSP dėl žmogiškosios klaidos daugėja (žr. **6 pav.**).  
2023 m. 72 proc. ADSP įvyko dėl žmogiškosios klaidos (2022 m. tokių ADSP buvo 60 proc.). ADSP  
įvyksta dėl neapdairumo, nežinojimo, kad tam tikras elgesys gali sukelti ADSP, taip pat dėl veiksmų,  
nuo kurių negali apsaugoti įprastai taikomos techninės ir organizacinės priemonės, pavyzdžiui,  
el. pašto adresų įrašymas į „Kopiją“ (angl. *Carbon Copy* (CC)), o ne į „Nematomą kopiją“ (angl. *Blind  
Carbon Copy* (BCC)), dokumentų su asmens duomenimis išsiuntimas netinkamiems gavėjams,  
netinkamai nuasmeninto dokumento paviešinimas ir kt. Dėl kitų priežasčių įvykę ADSP sudaro  
28 proc. (2022 m. tokių ADSP buvo 40 proc.). Tai buvo įvairūs kibernetiniai incidentai, IT sistemų  
trikdžiai ir kt., pavyzdžiui, piktavaliui pasinaudojus sistemų pažeidžiamumu ir įsilažus į serverį,  
jame esantys duomenys buvo užšifruojami, dėl IT sistemos klaidos atnaujinti duomenys nebuvo  
laiku perduodami, todėl duomenų valdytojas negalėjo laiku suteikti paslaugų ir kt.

**6 pav. >**  
ADSP priežastys 2023 m.,  
proc. (Šaltinis – VDAI).



VDAI, atsižvelgdama į tai, kad ADSP vis dažniau įvyksta dėl žmogiškosios klaidos, atkreipia dėmesį,  
kad labai svarbi priemonė siekiant minimizuoti žmogiškąsias klaidas ir išvengti kibernetinių incidentų  
(socialinės inžinerijos atakų ir kt.) yra darbuotojų mokymai. Duomenų apsaugos ir saugumo procedūrų  
(pavyzdžiui, slaptažodžių naudojimas ir prieiga prie konkrečių IT sistemų) mokymai ir įvairios duomenų  
viliojimo metodais paremtų atakų simuliacijos yra svarbūs tinkamam organizacinių ir techninių saugumo

priemonių įgyvendinimui užtikrinti ir netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atsklei-  
dimo be leidimo ar neteisėtos prieigos prie jų prevencijai. Žinios apie asmens duomenų tvarkymui  
keliamus reikalavimus bei atsakomybę yra ypač svarbios tiems asmenims, kurie atlieka didelės  
rizikos asmens duomenų tvarkymo operacijas, pavyzdžiui, specialiųjų kategorijų duomenų tvarkymą.

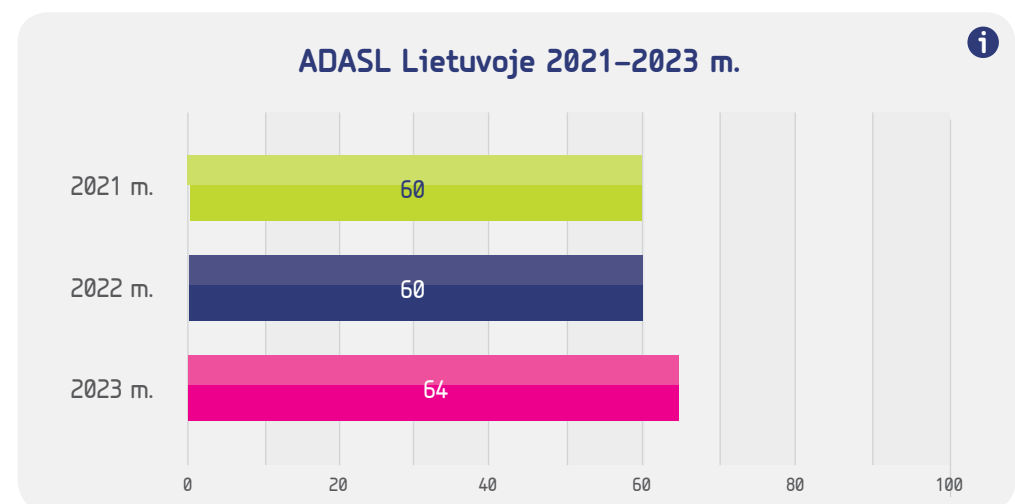
Ateities technologijos<sup>06</sup>, viską jungiantis internetas<sup>07</sup> (angl. *Internet of Everything* (IoE)), DI ir  
didieji duomenys<sup>08</sup> (angl. *Big Data*) suteikia naujų galimybių inovacijas pritaikyti žmonijai, tačiau  
taip pat kelia iššūkių duomenų subjektų teisių srityje. Visos šios technologijos turi potencialą  
užtikrinti asmens duomenų saugumą, tačiau tuo pat metu reikalauja nuolatinio rizikos vertinimo,  
bendradarbiavimo tarp verslo, viešojo sektoriaus institucijų ir mokslo bendruomenių, siekiant rasti  
efektyvius ir saugius duomenų panaudojimo sprendimus.

## 2 Asmens duomenų apsaugos sąlygų lygis

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 keturias sritis: gyventojų žinias, pasitikėjimą įmonėmis ir įstaigomis dėl  
asmens duomenų tvarkymo, elgesį, susidūrus su pažeidimais, ir pasitikėjimą priežiūros sistema.

Lietuvoje 2023 m. ADASL<sup>09</sup> siekė 64 proc. (2021 ir 2022 m. ADASL siekė 60 proc.) (ADASL siektina  
vertė yra 100 proc.) (žr. **7 pav.**). Palankiausiai asmens duomenų apsaugos sąlygas (ADASL) Lietuvoje  
vertina specialistai ir tarnautojai (ADASL – 69 proc.), o prasčiausiai – pensininkai (ADASL – 58 proc.).  
Be to, apklausa rodo, kad gaunantys didesnes pajamas ir turintys aukštesnį išsilavinimą gyventojai  
asmens duomenų apsaugos sąlygas vertina palankiau: geriau žino savo teises, labiau pasitiki  
duomenų valdytojais ir duomenų tvarkytojais ir asmens duomenų apsaugos priežiūros institucijomis.

ADASL augimas rodo, kad visuomenė pastebi pokyčius ne tik organizacijoms tvarkant asmens duo-  
menis, bet ir joms komunikuojant apie įvykusius kibernetinius incidentus ir (ar) asmens duomenų  
saugumo pažeidimus. Be kita ko, VDAI ir kitos šioje srityje veikiančios institucijos, atsižvelgdamos  
į pasitaikiusias veiklos spragas organizacijose, deda pastangas dalytis rekomendacijomis, pade-  
dančiomis mažinti galinčias kilti rizikas.



**6**  
Išradimai ar inovacijos, kuriomis galima  
lengviau ir patogiau atlikti kasdieninius  
darbus, vystyti mokslinę veiklą, pavyzdžiui,  
skaitmeniniai pinigai, kvantiniai  
kompiuteriai.

**7**  
Į vieną sistemą sujungiami įrenginiai,  
procesai ir internetą naudojantys žmonės.

**8**  
Žmonių ar mašinų sukuriama dideli  
duomenų kiekiai, kaip antai pirkimo  
sandorių duomenys, naudojimosi  
socialiniais tinklais įpročiai, interesai ir  
pomėgiai, padėties nustatymo sistemų  
(pavyzdžiui, GPS) signalai, jutiklių  
registruojama klimato informacija ir kt.

**9**  
ADASL 2023 m. apžvalga. Prieiga per  
internetą [https://vdai.lrv.lt/media/viesa/  
saugykla/2024/1/8MRMatvN9FA.pdf](https://vdai.lrv.lt/media/viesa/saugykla/2024/1/8MRMatvN9FA.pdf).

**< 7 pav.**  
2022–2023 m. duomenų  
palyginimas, proc.  
(Šaltinis – VDAI).

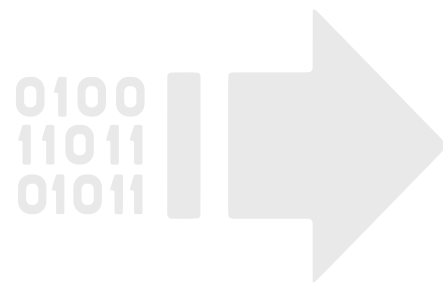
## Ką Lietuvos gyventojai mano apie asmens duomenų apsaugą

Remiantis minėtos apklausos duomenimis, 2023 m. 82,4 proc., arba 7,4 proc. daugiau negu 2022 m., respondentų buvo girdėję apie BDAR. 4 proc. padaugėjo respondentų, teisingai nurodžiusių institucijos (be teismų), kuri padėtų apginti jų teises asmens duomenų apsaugos srityje, pavadinimą (24 proc. nurodė VDAI). Nepaisant to, pasitikėjimas savo žiniomis apie asmens duomenų apsaugos teises išliko panašus – pusė apklaustų gyventojų teigia, kad jie žino šias savo teises.

2023 m. gyventojai daug rečiau patyrė asmens duomenų apsaugos pažeidimus. Net 88 proc. (15 proc. mažiau negu 2022 m.) gyventojų teigia, kad per pastaruosius metus nesusidūrė su jokių neteisėtų jų asmens duomenų tvarkymu. Visuomenės sąmoningumo didėjimą asmens duomenų apsaugos srityje rodo ir tai, kad tuo atveju, jei susidurtų su galimu asmens duomenų apsaugos pažeidimu, net 93 proc. gyventojų imtųsi kokių nors veiksmų – ieškotų daugiau informacijos, kreiptųsi į įmonę ar įstaigą, kuri netinkamai tvarkė duomenis, arba teiktų skundą atsakingai priežiūros institucijai.

Remiantis apklausos duomenimis, gyventojai labiausiai pasitiki savo darbdaviais – 65 proc. apklaustų gyventojų teigia, kad jų darbdaviai laikosi asmens duomenų apsaugos reikalavimų. 60 proc. gyventojų mano, kad apskritai įmonės ir įstaigos užtikrina teisę į duomenų apsaugą (6 proc. daugiau negu praėjusiais metais). Respondentai gerokai mažiau pasitiki smulkiais ir vidutinėmis įmonėmis. Tik 47 proc. gyventojų mano, kad jos laikosi asmens duomenų apsaugos reikalavimų. 50 proc. gyventojų mano, kad įmonės ir įstaigos, kurios neužtikrina tinkamos asmens duomenų apsaugos, bus nustatytos. Taip pat lygiai pusė respondentų mano, kad įmonės ir įstaigos, kurios neužtikrina tinkamos asmens duomenų apsaugos, bus nubaustos. Labiausiai asmens duomenų apsaugos priežiūra Lietuvoje pasitiki jaunimas, o mažiausiai – pensininkai.






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



## 4 Tarptautinio bendradarbiavimo iniciatyvos ir mokymo bei švietimo veiklos

2023 m. Europos duomenų apsaugos valdyba (angl. *the European Data Protection Board*) (toliau – EDAV), Europos Sąjungos (ES) valstybių narių asmens duomenų apsaugos priežiūros institucijas vienijanti Europos Sąjungos institucija, 2023 m. gruodžio 15 d. vykusiame plenariniame posėdyje patvirtino BDAR penkerių metų taikymo apžvalgą. Apžvalga sudarys dalį Europos Komisijos rengiamos BDAR įgyvendinimo ataskaitos.

### EDAV pasidalijo tokiomis įžvalgomis:

-  BDAR taikymas pirmuosius penkerius su puse metų buvo sėkmingas;
-  šiuo metu per anksti persvarstyti BDAR;
-  ES teisės aktų leidėjai raginami skubiau priimti naują reglamentą, kuriuo būtų nustatytos papildomos procedūrinės taisyklės, susijusios su tarpvalstybiniu BDAR vykdymo užtikrinimu;
-  EDAV ragina ES teisės aktų leidėjus ir Europos Komisiją siekti didesnio naujų funkcijų ir įgaliojimų, patikėtų asmens duomenų priežiūros institucijoms ir EDAV pagal naujus teisės aktus, aiškumo ir vienodumo;
-  duomenų apsaugos institucijoms ir EDAV būtini pakankami ištekliai, kad jos galėtų vykdyti savo užduotis.

2023 m. lapkričio mėn. EDAV parengė ataskaitą<sup>10</sup>. Joje analizuojami priežiūros institucijų sprendimai, priimti pagal BDAR 60 straipsnį dėl asmens duomenų tvarkymo saugumo ir saugumo pažeidimų. Ataskaitoje dėmesys atkreipiamas į BDAR 32, 33 ir 34 straipsnius. Akcentuojama, kad daugiausia asmens duomenų tvarkymo ir saugumo pažeidimų įvyksta dėl kibernetinių atakų, žmogiškųjų klaidų ir dėl to, kad nesiimama tinkamų techninių organizacinių priemonių.

2023 m. pradžioje VDAI su visuomene pasidalijo dvejus metus vykdyto informuotumo skatinimo projekto „SolPriPa 2 WORK“<sup>11</sup> rezultatais, rodančiais asmens duomenų apsaugos padėtį darbo santykiuose. Parengtose 3 gairėse darbuotojams ir viešojo bei privataus sektoriaus darbdaviams, be kita ko, pateikta informacijos ir apie ADSP.

2023 m. VDAI užtikrino kasdieninį gyventojams ir organizacijoms reikalingų konsultacijų teikimą. Iš viso suteiktos 4 163 konsultacijos, dalis jų – dėl organizacinių ir techninių duomenų saugumo priemonių. Taip pat surengta keletas nuotolinių mokymų, įrašai sulaukė itin daug peržiūrų. Iš viso VDAI šviečiamuosiuose renginiuose dalyvavo 14 731 dalyvis.

10




Duomenų tvarkymo saugumo ir pranešimo apie duomenų saugumo pažeidimus suvestinė vieno langelio principu (angl. *One-Stop-Shop case digest on Security of Processing and Data Breach Notification*). Prieiga per internetą [https://edpb.europa.eu/our-work-tools/our-documents/other/one-stop-shop-case-digest-security-processing-and-data-breach\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/one-stop-shop-case-digest-security-processing-and-data-breach_en).

11

„SolPriPa 2 WORK“ projektas. Prieiga per internetą <https://vdai.lrv.lt/lt/naudinga-informacija/solpripa-2-work-projektas/>.

2023 m. spalio mėn. VDAI kartu su NKSC, atsižvelgdami į pastebėtus praktikoje kylančius su teisės aktų reikalavimų įgyvendinimu susijusius sunkumus dėl asmens duomenų saugumo užtikrinimo ir kibernetinio saugumo, surengė nuotolinius mokymus ir atsakė į suinteresuotų asmenų pateiktus klausimus.




Keletą mėnesių viešai prieinami pranešimų įrašai sulaukė 1 665 peržiūrų šiomis temomis:

-  organizacinių priemonių taikymas asmens duomenų saugumui užtikrinti;
-  techninių priemonių taikymas asmens duomenų saugumui užtikrinti;
-  kibernetinio saugumo rizikos ir atitiktis organizaciniams techniniams reikalavimams.

2023 m. lapkričio mėn. VDAI surengė nuotolinius duomenų apsaugos pareigūnų mokymus. Stebėti mokymų buvo pakviesti tiek privataus sektoriaus, tiek viešojo sektoriaus duomenų apsaugos pareigūnai. Apie pareigūnų paskyrimą buvo pranešta VDAI. Kelias savaites mokymų įrašas buvo skelbiamas viešai. Taip suteikta galimybė susipažinti su mokymų medžiaga platesnei auditorijai. Mokymai sulaukė 4 500 peržiūrų.

2023 m. gruodžio mėn. VDAI, atsižvelgdama į metų pradžioje surinktą informaciją apie institucijų poreikį dėl trūkstamų žinių apie asmens duomenų apsaugą, surengė mokymus viešajam sektoriui. Viena iš mokymų temų skirta ir asmens duomenų saugumo klausimams, buvo pateikta patarimų dėl praktikoje organizacijų daromų klaidų įvykus ADSP ir juos valdant. Mokymų įrašai buvo prieinami viešai ir sulaukė 3 300 peržiūrų.

### 2023 m. VDAI parengti metodiniai dokumentai, kurie naudingi asmens duomenų užtikrinimo srityje:

-  rekomendacija dėl saugaus mobiliųjų aplikacijų naudojimo mobiliuosiuose įrenginiuose<sup>12</sup>;
-  20 žingsnių vaikams ir paaugliams, kaip apsaugoti savo asmens duomenis internete (saugaus elgesio internete gairės)<sup>13</sup>;
-  dažniausiai pasitaikančių atvejų, kai pranešama dėl įvykusių incidentų, kurie nėra laikomi asmens duomenų saugumo pažeidimais, apibendrinimas<sup>14</sup>.



12

VDAI 2023 m. birželio 16 d. rekomendacija dėl saugaus mobiliųjų aplikacijų naudojimo mobiliuosiuose įrenginiuose. Prieiga per internetą <https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomendacija%20del%20saugaus%20aplikaciju%20naudojimo%20mobiliuosiuose%20irenginiuose%202023-06.pdf>.

13

20 žingsnių vaikams ir paaugliams, kaip apsaugoti savo asmens duomenis internete. Prieiga per internetą [https://vdai.lrv.lt/uploads/vdai/documents/files/20\\_zingsniu\\_gaires%20vaikams%20ir%20paaugliams%202023\(1\).pdf](https://vdai.lrv.lt/uploads/vdai/documents/files/20_zingsniu_gaires%20vaikams%20ir%20paaugliams%202023(1).pdf).

14

Dažniausiai pasitaikančių atvejų, kai pranešama dėl įvykusių incidentų, kurie nėra laikomi asmens duomenų saugumo pažeidimais, apibendrinimas. Prieiga per internetą <https://vdai.lrv.lt/lt/naujienos/vdai-pataria-del-pasitaikanciu-atveju-kai-pranesama-apie-ivykusius-incidentus-kurie-nera-laikomi-asmens-duomenu-saugumo-pazeidimais/>.





# Nusikalstamų veikų kibernetinėje erdvėje mastas ir poveikis



Renatas Požėla,  
Lietuvos policijos  
generalinis komisaras

## Vadovo žodis

Interneto amžius atvėrė visuomenei naujas galimybes paprastai ir greitai atlikti kasdienes užduotis, dirbti ir tobulėti, todėl kibernetinio saugumo stiprinimo klausimas šiandien yra itin aktualus. Kibernetinis saugumas ir kova su nusikaltimais elektroninėje erdvėje – vienas pagrindinių Lietuvos policijos veiklos prioritetų. Nuolat stebime nusikalstamumo pokyčius ir nustatome kriminogenines rizikas, siekdami kurti saugią aplinką, užkirsti kelią galimiems nusikaltimams ir sėkmingai tirti nusikalstamas veikas. Turime kompetentingų ir profesionalių pareigūnų, modernių įrankių, žinių ir įgūdžių, tad esame pasiruošę iššūkiams ir reikšmingiems darbams.



### KA 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, kuriais šalinamos nusikalstamų veikų kibernetinėje erdvėje priežastys, kai paslaugų gavėjas galimai dalyvauja nusikalstamoje veikoje ar jo naudojama RIS įranga galimai naudojama nusikalstamai veikai.
- ✓ Inicijuodama kibernetinių incidentų tyrimus ir teikdama nurodymus interneto naudotojams kartu su NKSC.
- ✓ Perspėdama visuomenę dėl grėsmių kibernetinėje erdvėje, <https://policija.lrv.lt/lt/policija-pataria>.



LIETUVOS POLICIJA  
Ginti. Saugoti. Padėti.



[www.epolicija.lt](http://www.epolicija.lt)



[info@policija.lt](mailto:info@policija.lt)



112

## Svarbiausi 2023 m. įvykiai ir tendencijos



Nuolatinė grėsmė išliko valstybių remiami kibernetinių nusikaltimų vykdytojai ir jų gebėjimas įsiskverbti į taikinių informacines sistemas ir jas užvaldyti. Kibernetinės atakos, pirmiausia DDoS atakos, gali būti nutaikytos į kritinę infrastruktūrą.



Pastarųjų dvejų metų pasaulinės krizės suteikė sukčiams galimybę kurti apgaulingas schemas, susijusias su aktualiais įvykiais (pavyzdžiui, Rusijos invazija į Ukrainą, žemės drebėjimai Turkijoje ir Sirijoje).



Kompanijos „Surfshark“ skaitmeninio gyvenimo kokybės indeksas (angl. *Digital Quality of Life Index*) rodo, kad Lietuva pagal kibernetinį saugumą 2023 m. buvo antra pasaulyje.



2023 m. užregistruotos nusikalstamos veikos elektroninėje erdvėje (3 912 nusikalstamos veikos) neturėjo įtakos registruoto nusikalstamumo augimui ir jų grėsmės lygis gerokai nukrito, palyginti su 2022 m. (5 309 nusikalstamos veikos elektroninėje erdvėje).



2023 m. antrą pusmetį, kai Lietuvoje buvo pritaikytos svarbios tarpinstitucinio bendradarbiavimo priemonės, skirtos žalingos veiklos internete ir elektroninio komunikavimo priemonėmis prevencijai, gerokai sumažėjo kibernetinių nusikaltimų siaurąją prasme (t. y. pagal LR BK 196–198<sup>2</sup> str.).



2023 m. šalyje buvo užregistruoti 638 nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui pagal LR BK 196–198<sup>2</sup> str. (2022 m. – 919).



2023 m. išliko tendencija, kad nusikalstamumą elektroninėje erdvėje labiausiai lėmė sukčiavimai (LR BK 182 str.), jie sudarė dominuojančią 50 proc. dalį visų elektroninėje erdvėje padarytų nusikalstamų veikų.



2023 m. Lietuvoje išryškėjo tendencija, kad dominuojančia apgaulingų skelbimų vieta tampa socialiniai tinklai (62 proc., tai yra 45 proc. daugiau, palyginti su 2022 m.).





01001  
10101


Tiek 2023 m., tiek per pastaruosius kelerius metus kibernetinės atakos žalingų padarinių valstybės ir tarnybos paslaptims nesukėlė.


## 1 Tarptautinė situacija


Nusikaltimai elektroninėje erdvėje paskutiniu metu tapo pelningu „verslu“, kuriame dalyvauja nusikalstamų paslaugų teikėjai ir verbuotojai. Teisėsaugos institucijoms vis sunkiau tirti kibernetinius nusikaltimus, nes šioje srityje veikia daug įvairaus profilio nusikaltėlių iš viso pasaulio, o kibernetiniai nusikaltėliai ir toliau demonstruoja gebėjimą greitai prisitaikyti prie naujų technologijų. 2023 m. Organizuoto nusikalstamumo internete grėsmių vertinimo ataskaitoje (angl. *Internet Organised Crime Threat Assessment* (IOCTA)) (toliau – IOCTA ataskaita)<sup>01</sup>, kuri kasmet rengiama Europos Sąjungos teisėsaugos bendradarbiavimo agentūros (angl. *European Union Agency for Law Enforcement Cooperation*) (toliau – Europol), apžvelgiama kibernetinių nusikaltimų ekosistema ES ir analizuojami tokių nusikalstamų veikų padariniai, vykdytojai ir aukos. Pagrindinės IOCTA ataskaitos išvados:


 Nusikaltimai kaip plačiai paplitusios ir dažnai parduodamos arba reklamuojamos tamsiojo interneto<sup>02</sup> forumuose (angl. *Dark web forums*) ir prekyvietėse paslaugos (angl. *crime-as-a-service*). Šias paslaugas siūlantys asmenys specializuojasi atskirų nusikalstamų veikų srityse ir glaudžiai bendradarbiauja tarpusavyje. Visiems šių paslaugų teikėjams reikalinga atitinkama infrastruktūra, kuria pasinaudodami galėtų pasislėpti nuo teisėsaugos institucijų. Daugelis interneto paslaugų teikėjų, kurių paslaugomis dažnai naudojasi nusikaltėliai, netaiko plataus masto klientų stebėsenos procedūrų (pavyzdžiui, „Pažink savo klientą“) ir kliento bei metaduomenų (pavyzdžiui, IP adreso) saugojimo praktikos, todėl neišsaugo svarbių elektroninių pėdsakų ir apsunkina nusikalstamų veikų tyrimą – anonimizuoja savo klientą.


 Socialinė inžinerija, ypač duomenų viliojimo atakos, kuriomis siekiama iš aukos išgauti prisijungimo ar kredito kortelių duomenis. Apgaulė gali pasireikšti išgalvotu tekstu ar netikro, suklastoto siuntėjo vardu el. laiškuose ar SMS trumposios žinutės. Duomenų viliojimo atakos išlieka populiarios ir jomis naudojasi visų tipų kibernetiniai nusikaltėliai. Pasikeitus ES reguliavimui<sup>03</sup> ir apsunkinus sukčiavimo schemų su mokėjimo kortelėmis galimybes, nusikaltėliai daugiau dėmesio ėmė skirti kortelių naudotojams, o ne manipuliavimui skaitmeninėmis sistemomis. Duomenų viliojimas yra pagrindinė priemonė, kurią naudoja sukčiai savo internetinio sukčiavimo schemose ir kenkimo atakų atvejais, kai siekia įsilaužti į sistemas, pavogti duomenis arba išvilioti pinigus.


 Pažymėtina, kad kibernetiniai nusikaltėliai nusikalstamoms veikoms vykdyti išnaudoja įvairias krizes: pirmiausia COVID-19 pandemiją, o pastaruoju metu – su nestabilia geopolitine situacija Europoje susijusius įvykius ar žemės drebėjimą Turkijoje ir Sirijoje. 2023 m. padaugėjo sukčiavimui skirtų interneto svetainių, kuriose buvo renkamos lėšos ar telkiama pagalba Ukrainai, taip pat iš netikrų anketų siustų el. laiškus su raginiu teikti humanitarinę pagalbą ir prisidėti prie neva Ukrainos ar Rusijos pagalbai skirtų kampanijų ir fondų veiklų.

 Apsimetinėjimas kitu asmeniu – tai metodas, kurį plačiai taiko nusikaltėliai, veikiantys vaikų seksualinio išnaudojimo srityje ir vykdančys sukčiavimus internete. Su vaikų seksualiniu išnaudojimu susijusiose nusikalstamose veikose nusikaltėliai plačiai naudoja socialiniais tinklais, kad užmegztų ryšius su savo aukomis, dažnai su jomis bendrauja prisidengdami netikra tapatybe. 2023 m. ir toliau augo vaikų pornografijos plitimo grėsmė. Nusikaltėliai, platindami vaikų pornografiją internete, naudojo įvairias priemones tapatybei slėpti (pavyzdžiui, virtualius privačius ryšio tinklus). Vaikų pornografija buvo platinama tiek mažose interneto bendruomenėse, tiek dideliuose forumuose. Duomenų vagystė yra pagrindinė nusikaltimų internete ekosistemos sudedamoji dalis, nes pavogti duomenys gali būti panaudoti įvairiose nusikalstamose veikose, įskaitant nelegalią

 prekybą, neteisėtą prieigą prie sistemų, šnipinėjimą, šantažą ir socialinę inžineriją. Nelegaliose rinkose prekiaujama pavogtais prisijungimo duomenimis ir aukų asmens duomenimis, gautais iš programišių ir sukčių, kurie duomenis gauna įsilauždami į duomenų bazes ar taikydami socialinės inžinerijos metodus.

 Nusikaltimai elektroninėje erdvėje dažnai yra tarpusavyje susiję, todėl daugeliu atvejų ta pati auka tampa kelių nusikaltėlių taikiniu. Tai ypač akivaizdu vaikų seksualinio išnaudojimo nusikaltimuose, kenkimo programų atakų atvejais ir internetinėse sukčiavimo schemose. Nukentėjusių asmenų duomenys gali būti parduoti keliems pirkėjams, vadinas, auka gali tapti sukčių ir kenkimo programų platintojų taikiniu.

 Kibernetiniai nusikaltėliai, vykdančys kibernetines atakas ir teikiantys susijusias paslaugas, taip pat vykdančys prekybą tamsiojo interneto prekyvietėse ar jas administruojantys, savo finansinės veiklos sandorius sudaro beveik išimtinai kriptovaliuta. Siekdami paslėpti nusikalstamą būdą įgyto turto kilmę, prieš išgrynindami neteisėtą pelną nusikaltėliai taiko įvairius virtualiosios valiutos operacijų maskavimo metodus (pavyzdžiui, decentralizuotas keityklas, virtualiosios valiutos maišymą (angl. *mixers*)).

 Kibernetiniai nusikaltėliai ir grupuotės aktyviai naudoja tamsiojo interneto forumais, svetainėmis, kuriuose ne tik galima dalytis nusikalstamos veikos rezultatais, bet ir lengvai bendrauti, aptarinėti nusikaltimų detales ir burtis į komandas. Tamsiajame internete taip pat parduodama įvairi neteisėtu būdu gauta informacija, reklamuojami nusikalstamų veikų vykdymo techniniai įrankiai, dalijamasi patarimais, kaip naudotis tamsiuoju internetu. 2021 m. atlikto tyrimo duomenimis, paaiškėjo, kad jauni žmonės, nesusiję su nusikalstamų veikų vykdymu, taip pat lankosi tamsiojo interneto forumuose, interneto bendruomenių puslapiuose, dažnai įsitraukia ir į rizikingos veiklos vykdymą. 51 proc. apklausos dalyvių teigė, kad lankosi internetiniuose forumuose ir naudoja pasikalbėjimo platformomis, iš jų 12 proc. – tamsiojo interneto forumuose, 11 proc. – tamsiojo interneto apsipirkimo puslapiuose.

## 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.

Susirūpinimą keliančių tarptautinių grėsmių ir prognozių kontekste visiškai netikėtas 2023 m. Lietuvoje buvo reikšmingas registruotų kibernetinių nusikaltimų siaurąja prasme sumažėjimas ir matomas retrospektyvinis regresas. Taip pat matomas aiškus sutapimas (žr. **1 pav.**), kad kibernetinių nusikaltimų siaurąja prasme gerokai sumažėjo per 2023 m. antrąjį pusmetį, kai šalyje buvo pritaikytos svarbios tarpinstitucinio bendradarbiavimo priemonės, skirtos žalingos veiklos internete ir elektroninio komunikavimo priemonėmis prevencijai.

01

2023 m. Organizuoto nusikalstamumo internete grėsmių vertinimo ataskaita (angl. *Internet Organised Crime Threat Assessment* (IOCTA)). Prieiga per internetą <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023>.

02

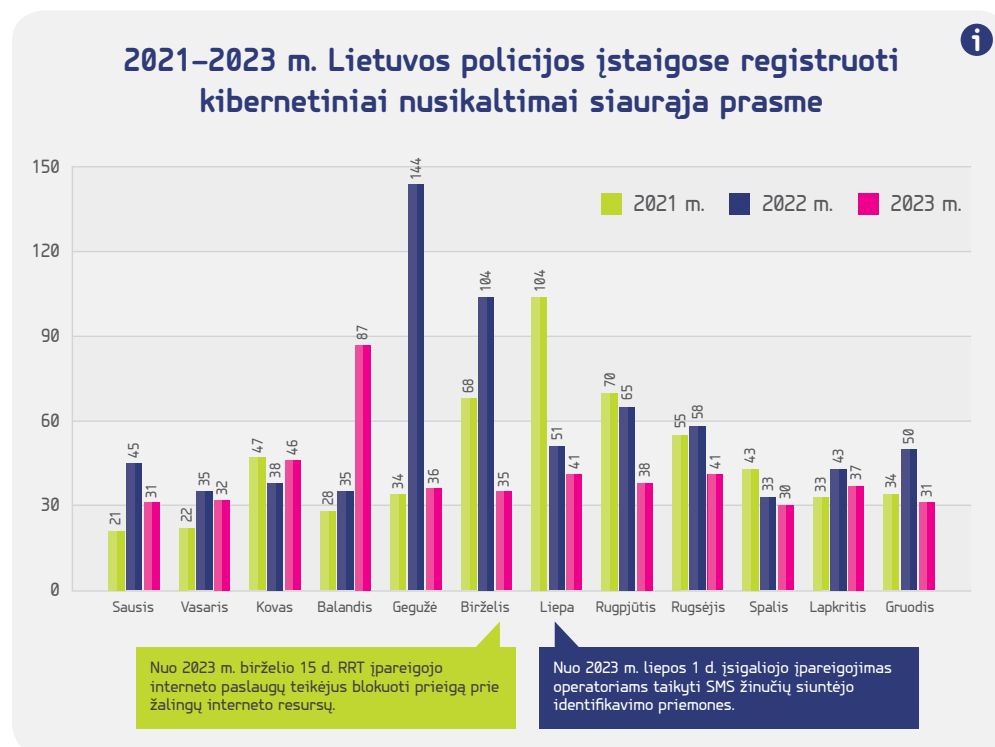
Tamsusis internetas – interneto dalis, kurią galima pasiekti tik naudojant tam tikrą programinę įrangą, konfigūracijas ar leidimą bei unikalų ryšio protokolą.

03

2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB. Šia direktyva nustatomos išsamios mokėjimo paslaugų taisyklės siekiant užtikrinti suderintą mokėjimo paslaugų teikimo taisyklės ES ir aukštą vartotojų apsaugos lygį. Prieiga per internetą <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L2366-20151223&qid=1707339672877>.

**1 pav. >**

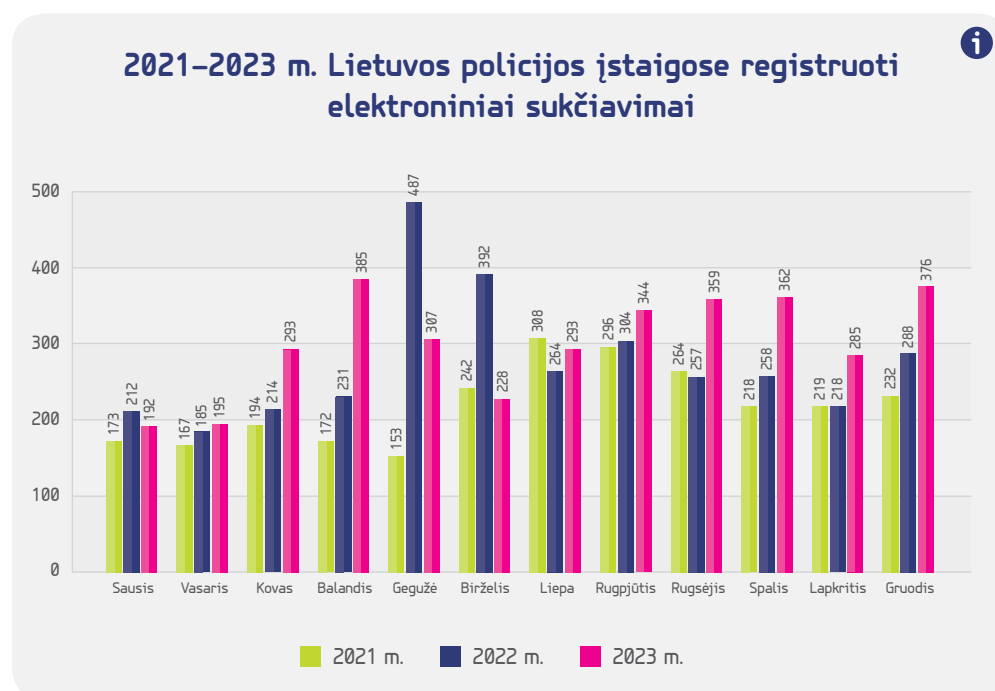
2021–2023 m. Lietuvos policijos įstaigose registruoti kibernetiniai nusikaltimai siaurąja prasme  
(šaltinis – Lietuvos policija)



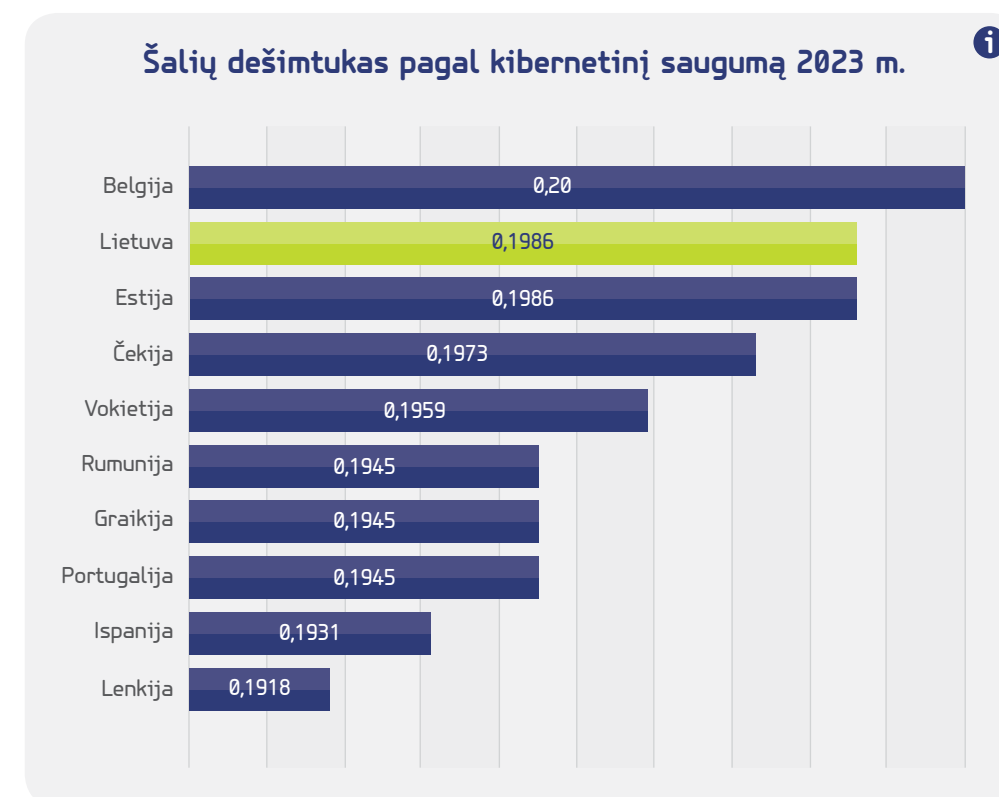
Atsižvelgus į ilgalaikę sukčiavimų elektroninėje erdvėje spartaus augimo tendenciją (žr. **2 pav.**), galima daryti išvadą, kad 2023 m. Lietuvoje buvo dažnesni socialinės inžinerijos metodai, kurie neturėjo poveikio informacinėms sistemoms ir (ar) jų duomenims. Ši situacija rodo, kad vyravo atvejai, kai kibernetiniai nusikaltėliai ne tik išprovokavo nukentėjusiuosius atskleisti elektroninius duomenis, bet ir savo informacinėse sistemose inicijuodavo operacijas, todėl šios sukčiavimo schemos, anksčiau labiausiai lėmusios kibernetinių nusikaltimų siaurąja prasme augimą, dabar nebesuteikia pagrindo, būtino šiems nusikaltimams tirti.

**2 pav. >**

2021–2023 m. Lietuvos policijos įstaigose registruoti elektroniniai sukčiavimai  
(šaltinis – Lietuvos policija)



Lietuvos policijos 2023 m. stebėsenos vertinimas sutampa su viešuose šaltiniuose paskelbtomis nepriklausomų ekspertų išvadomis. Kompanijos „Surfshark“ 2023 m. atlikto skaitmeninio gyvenimo kokybės indekso (angl. *Digital Quality of Life Index (DQL)*) tyrimo duomenimis (žr. **3 pav.**), Lietuva pagal kibernetinį saugumą 2023 m. buvo antra pasaulyje<sup>04</sup>.

**< 3 pav.**

Kompanijos „Surfshark“ 2023 m. skaitmeninio gyvenimo kokybės indekso tyrimo rezultatai (šaltinis – kompanija „Surfshark“)

**Kibernetiniai nusikaltimai siaurąja prasme**

Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos duomenimis, 2023 m. šalyje buvo užregistruoti 638 nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui (LR BK 196–198<sup>2</sup> str.). 2023 m. šių nusikaltimų užregistruota 281 nusikalstama veika mažiau nei 2022 m. (30,6 proc., mažiau nei 2022 m.) (žr. **4 pav.**).

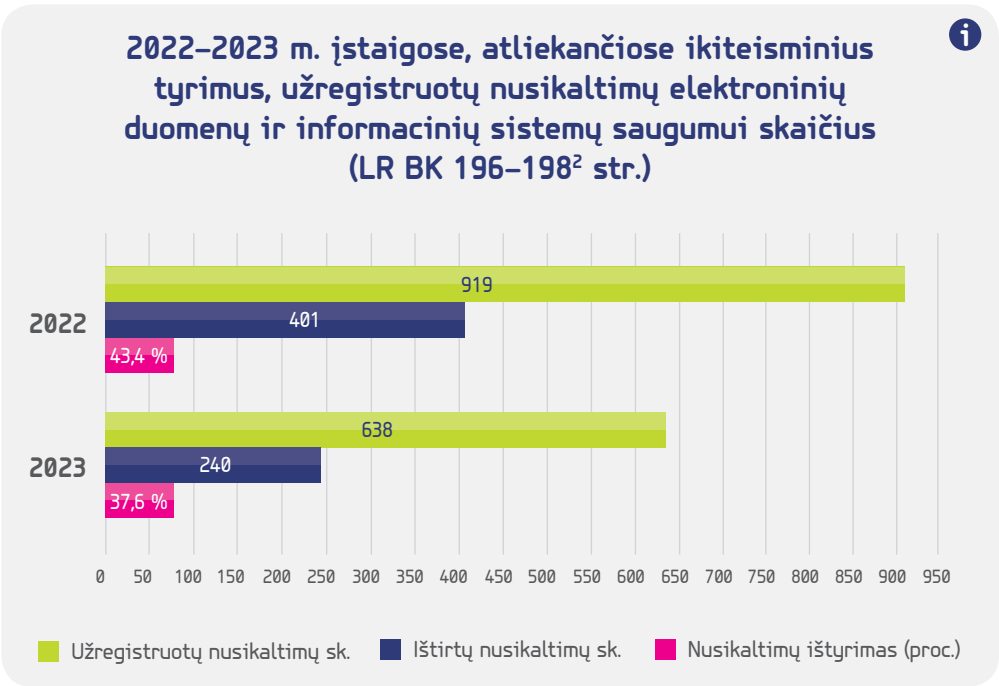
<sup>04</sup>

Kompanijos „Surfshark“ 2023 m. nustatytas skaitmeninio gyvenimo kokybės indeksas. Prieiga per internetą <https://surfshark.com/dql2023/insights>.



4 pav. >

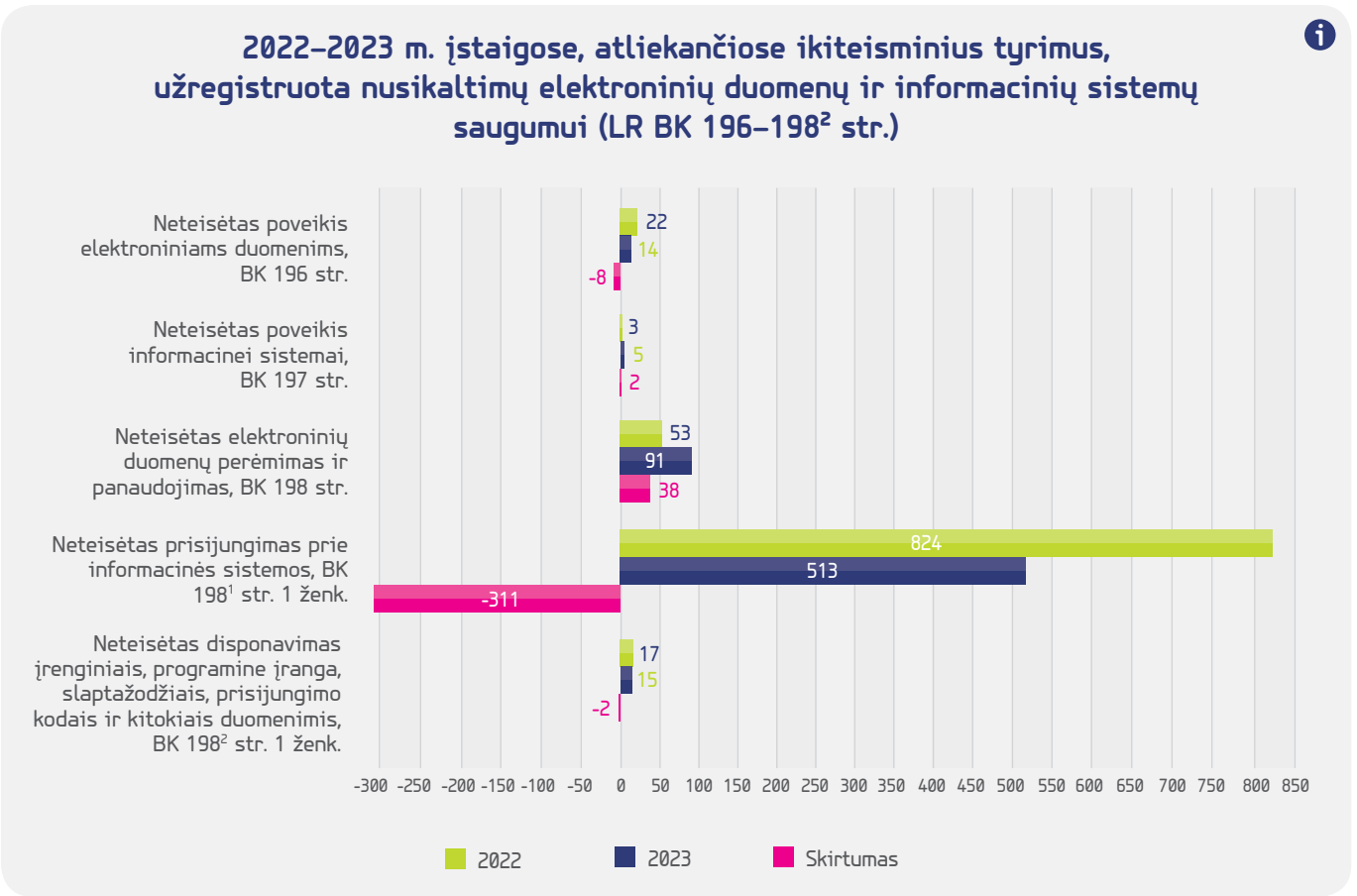
2022–2023 m. įstaigose, atliekančiose ikiteisminius tyrimus, užregistruotų nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui skaičius (LR BK 196–198<sup>2</sup> str.)



Bendroje nusikalstamumo struktūroje nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui 2023 m. sudarė apie 1 proc. visų užregistruotų nusikalstamų veikų (2021 ir 2022 m. šie nusikaltimai sudarė 2 proc. visų užregistruotų nusikalstamų veikų). 2023 m. šių nusikaltimų ištyrimas sudarė 37,6 proc.

Detalesnė informacija apie kiekvieną elektroninių duomenų ir informacinių išteklių saugumo nusikaltimą pagal LR BK 196–198<sup>2</sup> str. (žr. 5 pav.):

- ⚠ **LR BK 196 str. „Neteisėtas poveikis elektroniniams duomenims“ – 2023 m. užregistruota 14 nusikaltimų (2022 m. – 22). 2023 m., palyginti su 2022 m., šių nusikaltimų užregistruota 8 atvejai, arba 36,4 proc., mažiau.**
- ⚠ **LR BK 197 str. „Neteisėtas poveikis informacinei sistemai“ – 2023 m. užregistruoti 5 nusikaltimai (2022 m. – 3). 2023 m., palyginti su 2022 m., šių nusikaltimų užregistruota 2 atvejai, arba 66,7 proc., daugiau.**
- ⚠ **LR BK 198 str. „Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“ – 2023 m. užregistruotas 91 nusikaltimas (2022 m. – 53). 2023 m., palyginti su 2022 m., šių nusikaltimų užregistruota 38 atvejai, arba 71,7 proc., daugiau.**
- ⚠ **LR BK 198<sup>1</sup> str. „Neteisėtas prisijungimas prie informacinės sistemos“ – 2023 m. užregistruota 513 nusikaltimų (2022 m. – 824). 2023 m., palyginti su 2022 m., šių nusikaltimų užregistruota 311 atvejų, arba 37,7 proc., mažiau.**
- ⚠ **LR BK 198<sup>2</sup> str. „Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis“ – 2023 m. užregistruota 15 nusikaltimų (2022 m. – 17). 2023 m., palyginti su 2022 m., šių nusikaltimų užregistruota 2 atvejai, arba 11,8 proc., mažiau.**



Pagal policijoje vykdytus ikiteisminius tyrimus, 2023 m. atvejų, kai buvo naudojamosi elektroninius duomenis užšifruojančiais ir išpirkos reikalaujančiais kenkimo programinio kodo virusais ar DDoS atakomis, dalis nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui struktūroje buvo iki 5 proc.

2023 m., palyginti su 2022 m., šiek tiek padaugėjo tik kibernetinių nusikaltimų, kurių motyvai buvo duomenų apie informacinių sistemų pažeidžiamumą ieškojimas ir (ar) elektroninių duomenų grobimas.

2023 m. beveik panašus išliko žmonių bauginimo ir (ar) terorizavimo kibernetiniais būdais atvejų skaičius. Pagrindinės priežastys buvo terorizavimas dėl turtinės naudos, informacinės atakos, kenkimas valstybei ir (ar) viešiesiems subjektams. 2023 m. nusikaltimų skaičiumi nedaug skyrėsi nuo praėjusių, tačiau kaip nauji ir labai grėsmingi nusikaltimai buvo grasinimai žudyti sprogdinant ir (ar) šaudant (2 nauji atvejai mokyklų informacinėse sistemose) ir platintos ekstremistinės nuostatos (1 naujas atvejis informacinėse sistemose, skirtose viešose erdvėse informacijai transliuoti).

2023 m. kibernetinių nusikaltimų siaurąja prasme, kurių motyvai buvo kibernetinis chuliganizmas ir buitiniai konfliktai, mažėjo.

2023 m. kibernetinio chuliganizmo priežastys nesikeitė. Dažniausiai tai buvo akademinio jaunimo kibernetinis chuliganizmas, siekiant ugdymo informacinėse sistemose platinti neetišką turinį ir (ar) trikdyti pamokas. 2023 m. šiek tiek sumažėjo atvejų, kai poveikis informacinėms sistemoms ir (ar) jų duomenims buvo padarytas be konkrečių motyvų.

^ 5 pav.

2022–2023 m. įstaigose, atliekančiose ikiteisminius tyrimus, užregistruotų nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui skaičius (LR BK 196–198<sup>2</sup> str.)



## Elektroninius duomenis užšifruojantys ir išpirkos reikalaujantys kenkimo programinio kodo virusai

2023 m. registruota kiek daugiau atvejų nei 2022 m., kai elektroninius duomenis užšifruojančiais ir išpirkos reikalaujančiais kenkimo programinio kodo virusais buvo užšifruoti duomenys. 2023 m. buvo taikomi tokie patys išpirkos už elektroninių duomenų iškodavimą prievartavimo metodai: arba virusais užkrėstose informacinėse sistemose buvo paliekami raštai su išpirkos mokėjimo nurodymais (angl. *ransom note*), arba buvo nurodomi kontaktiniai el. pašto adresai, taip pat programišiai dažnai derino ir duomenų grobimo, ir duomenų užšifravimo atakas, todėl, reikalaudami išpirkos, grasino paviėšinti duomenis, o negavę išpirkos juos paviėšindavo. Komunikacijai dažniausiai buvo naudojamosi arba anoniminiu tinklu „Tor“<sup>05</sup>, arba anoniminio el. pašto teikėjų paslaugomis. Išpirkos dydis buvo nurodomas arba iš karto (*ransom note* raštuose), arba išpirkos sumą pasakydavo programišiai, jei nukentėjusieji su jais pradėdavo derybas. Reikalaudami išpirkos, programišiai dažnai nurodydavo, kad kaina priklausys nuo to, kaip greitai bus pradėta derėtis ir įvykdytas susitarimas sumokėti pinigus. 2023 m. sumokėti išpirką buvo prašoma tiek valiuta, tiek konvertuojant ją į kriptovaliutą ir pervedant į nurodytą piniginės adresą. 2023 m. reikalaučių išpirkų dydis buvo nuo 186,8 ETH (400 Eur) iki 900 000 USD (832 254 Eur), o didžiausia 2022 m. prašyta išpirkos suma buvo 1000 BTC (22 529 000 Eur). 2023 m. nustatyta, kad elektroniniams duomenims užšifruoti buvo naudojami 11 šeimų elektroninius duomenis užšifruojantys ir išpirkos reikalaujantys kenkimo programinio kodo virusai<sup>06</sup>.



## DDoS atakos

2023 m. pradėti 2 ikiteisminiai tyrimai (arba 1 mažiau nei 2022 m.) dėl informacinių sistemų trikdymo DDoS atakomis. Nuo 2020 m. Lietuvos policijos tyrimų, pradėtų dėl DDoS atakų, skaičius išlieka stabilus (2020–2023 m. laikotarpio vidurkis – iki 3 atvejų per metus).

Vienas iš ikiteisminių tyrimų buvo pradėtas dėl masinių DDoS atakų prieš Lietuvos valstybės institucijų ir verslo interneto svetaines nuo 2023 m. gegužės 6 d. iki 2023 m. birželio 4 d. (ne mažiau kaip 40 svetainių) ir nuo 2023 m. liepos 10 d. iki 2023 m. liepos 13 d. (ne mažiau kaip 21 svetainė). Šioms DDoS atakoms, kuriomis buvo reaguojama į Lietuvos valstybės paramą, skirtą padėti Ukrainai atremti Rusijos karinę agresiją, taip pat į NATO viršūnių susitikimą 2023 m. liepos mėnesį Vilniuje, organizuoti susivienijo ne mažiau kaip 17 Rusijos programišių grupių. Tarp jų buvo ir 2022 m. prieš Lietuvą veikusi Rusijos programišių grupė „Killnet“. Atakuotų Lietuvos svetainių sąrašus ir poveikio joms rezultatus Rusijos programišių grupė „Noname05716“ viešino „Telegram“ kanale.

Kita 2023 m. DDoS ataka buvo taikomasi į vieną iš meno kūrinų aukciono interneto svetainę. Aukciono organizatoriai įtarė konkurentus.

05

Tamsusis internetas pasiekiamas naudojant anoniminę naršyklę „Tor“ (angl. *The Onion Router* (TOR)).

06

CUBA (5 atvejai), ESXIArgs (2 atvejai), PHOBOS/FAUST (2 atvejai), ALPHV/BlackCat (1 atvejis), AVADDON (1 atvejis), GLOBEIMPOSTER 2.0 (1 atvejis), MEDUSALOCKER/LOCKFILESKR (1 atvejis, virusas žinomas iš anksčiau), NESHITA (1 atvejis), PHOBOS/DEVOS (1 atvejis), VENUS (1 atvejis), Win32/Filecoder.OOQ Trojan (1 atvejis).

0100  
11011  
01011



## Kibernetinius nusikaltimus lėmusios aplinkybės ir kibernetinių nusikaltimų poveikio vertinimas

### Kibernetinių nusikaltimų būdai

2023 m. pagrindinės kibernetinių nusikaltimų siaurąja prasme technologijos, kuriomis buvo užvaldyti informacinių sistemų vartotojų duomenys ir (ar) gauta prieiga prie informacinių sistemų, kaip ir anksčiau, rėmėsi socialine inžinerija, ir tai buvo priemonės, susijusios su apgaulingomis SMS žinutėmis, internetinio bendravimo programų pranešimais, telefoniniais skambučiais, el. pašto laiškais.



### Kibernetinių nusikaltimų padariniai

2023 m. dažniausi kibernetinių nusikaltimų siaurąja prasme padariniai, palyginti su 2022 m., išliko tie patys:



**duomenų stebėjimas ir (ar) pasisavinimas;**



**paskyrų perėmimas;**



**neteisėtas duomenų paskelbimas;**



**duomenų užšifravimas, sugadinimas, pakeitimas ar sunaikinimas.**



### Atakuotos informacinės sistemos

2023 m. dažniausi kibernetinių nusikaltimų siaurąja prasme taikiniai:



**socialinių tinklų paskyros;**



**internetu paslaugų vartotojų paskyros;**



**informacinių sistemų tinklai ir (ar) galiniai įrenginiai;**



**informacinių sistemų vartotojų paskyros;**



**el. pašto paskyros.**



2023 m. išryškėjo nauja kibernetinių atakų forma – įsilaužimas į informacines sistemas, skirtas informacijai viešose erdvėse transliuoti.

### Atakuoti ar neteisėti (neteisėtai paskelbti) elektroniniai duomenys

2023 m. išliko ilgametė teigiama tendencija, susijusi su maža kibernetinių nusikaltimų siaurąja prasme rizika valstybės ir tarnybos paslaptims. Tiek 2023 m., tiek per pastaruosius kelerius metus kibernetinės atakos žalingų padarinių valstybės ir tarnybos paslaptims nesukėlė.





2023 m. kibernetinėmis atakomis dažniausiai buvo kėsiniama į konfidencialią (neviešą) informaciją:

- ⚠ **informacinių sistemų vartotojų autentifikavimosi duomenis;**
- ⚠ **finansinius, ūkinius, komercinius duomenis;**
- ⚠ **BDAR apibrėžtus asmens duomenis;**
- ⚠ **informacinių sistemų operacinius duomenis;**
- ⚠ **privataus gyvenimo duomenis;**
- ⚠ **tarnybinius, profesinius duomenis;**
- ⚠ **valstybės tvarkomus informacinius išteklius.**

2023 m. kibernetinių atakų, susijusių su apgaulingų ar žalingų elektroninių duomenų platinimu, buvo daugiau nei 2022 m. Didžiausią jų dalį sudarė neetiško ar bauginančio turinio informacija. Kiti neteisėti elektroniniai duomenys buvo apgaulingi prašymai, fiktyvaus autentifikavimosi, siekiant apgaulingai gauti informacinių sistemų paslaugas, duomenys, apgaulingi komerciniai skelbimai internete, kenkimo programinė įranga ir (ar) jos jaukas, informacinėse sistemose apgaulingai įregistruoti duomenys, apgaulingi komerciniai užsakymai internete.

### Kibernetinių nusikaltimų poveikis fiziniams asmenims

Išliko tendencija, kad 2023 m. tarp visų subjektų, patiriančių kibernetinių nusikaltimų poveikį, dažniausiai nukentčia fiziniai asmenys.

2023 m., be socialine inžinerija paremto sukčiavimo, fiziniai asmenys taip pat nukentėjo dėl poveikio socialinių tinklų paskyroms, mobiliųjų programėlių paskyroms, paskyroms interneto svetainėse, el. pašto paskyroms, informacinių sistemų tinklams ir (ar) galiniams įrenginiams.

Dažniausi kibernetinių nusikaltimų padariniai fiziniams asmenims 2023 m. buvo paskyrų perėmimas, elektroninių duomenų stebėjimas ir (ar) pasisavinimas, neteisėtų finansinių operacijų, užvaldžius paskyras ir (ar) elektroninės bankininkystės duomenis, inicijavimas, neteisėtas elektroninių duomenų paskelbimas.

2023 m. kibernetinės atakos prieš fizinių asmenų informacines sistemas dažniausiai buvo orientuotos į konfidencialią (neviešą) informaciją, finansinius elektroninius instrumentus, apgaulingos ir (ar) žalingos informacijos svetimo asmens vardu platinimą.

2023 m. daugiausia kibernetinių atakų buvo taikyta į informacinių sistemų vartotojų autentifikavimosi duomenis. Kita kibernetinių atakų dalis buvo susijusi su fizinių asmenų privataus gyvenimo duomenimis ir BDAR apibrėžtais asmens duomenimis.

2023 m. fizinių asmenų informacinėse sistemose platintą apgaulingą ar žalingą informaciją sudarė apgaulingi prašymai, pavedimai, neetiško ar bauginančio turinio informacija, apgaulingi komerciniai skelbimai internete, kenkimo programinė įranga ir (ar) jos jaukas, fiktyvaus autentifikavimosi, siekiant apgaulingai gauti informacinių sistemų paslaugas, duomenys.



### Kibernetinių nusikaltimų poveikis juridiniams asmenims

2023 m. tarp visų subjektų, patyrusių kibernetinių nusikaltimų poveikį, juridiniai asmenys sudarė 7 proc., arba gerokai mažiau. 2023 m. išliko tendencija, kad tarp juridinių asmenų, patyrusių kibernetinių atakų poveikį, dominavo prekybos subjektai. Kitos 2023 m. ryškesnės kibernetinės atakos buvo prieš informatikos ar telekomunikacijų paslaugų subjektus, statybų pramonės subjektus, transportavimo paslaugų subjektus, apdirbamosios pramonės subjektus, teisinių paslaugų subjektus, renginių organizavimo subjektus.

2023 m. juridiniai asmenys dažniausiai nukentėjo dėl poveikio informacinių sistemų tinklams ir (ar) galiniams įrenginiams. Kitos 2023 m. atakuotos juridinių asmenų informacinės sistemos buvo el. pašto paskyros, interneto svetainės, paskyros interneto svetainėse, informacinių sistemų vartotojų paskyros, socialinių tinklų paskyros.

Dažniausi kibernetinių nusikaltimų padariniai juridiniams asmenims 2023 m. buvo elektroninių duomenų neteisėtas stebėjimas, pasisavinimas, elektroninių duomenų užšifravimas, sugadinimas, pakeitimas ar sunaikinimas, el. pašto adresų imitavimas ir (ar) elektroninio susirašinėjimo perėmimas, neteisėtas elektroninių duomenų paskelbimas.

2023 m. daugiausia kibernetinių atakų buvo taikyta į finansinius, ūkinius, komercinius duomenis. Kitos kibernetinės atakos buvo susijusios su juridinių asmenų valdomais asmens duomenimis, kuriuos apibrėžia BDAR, informacinių sistemų vartotojų autentifikavimosi duomenimis, informacinių sistemų operaciniais duomenimis, privataus gyvenimo duomenimis.

2023 m. juridinių asmenų informacinėse sistemose platintą apgaulingą ar žalingą elektroninę informaciją daugiausia sudarė fiktyvaus autentifikavimosi, siekiant apgaulingai gauti informacinių sistemų paslaugas, duomenys.

### Kibernetinių nusikaltimų poveikis viešųjų paslaugų subjektams

2023 m. tarp visų subjektų, patyrusių kibernetinių nusikaltimų poveikį, viešieji subjektai sudarė 7 proc., arba šiek tiek daugiau nei 2022 m. 2023 m. išliko tendencija, kad tarp viešųjų subjektų, patyrusių kibernetinių atakų poveikį, dominavo švietimo sektoriaus informacinės sistemos. Kitos 2023 m. akivaizdesnį poveikį viešiesiems subjektams turėjusios kibernetinės atakos taikytos prieš sveikatos paslaugų sektorių, žiniasklaidos sektorių, kultūros sektorių, susisiekiimo sektorių, aukštojo mokslo sektorių, turizmo sektorių, gatvių apšvietimo sektorių.




2023 m. viešieji subjektai dažniausiai nukentėjo dėl poveikio informacinių sistemų vartotojų paskyroms. Kitos 2023 m. atakuotos viešųjų subjektų informacinės sistemos:

- ⚠ **informacinių sistemų tinklai ir (ar) galiniai įrenginiai;**
- ⚠ **socialinių tinklų paskyros;**
- ⚠ **internetu svetainės;**
- ⚠ **informacinių sistemų duomenų registrai ar duomenų bazės;**
- ⚠ **el. pašto paskyros.**





Dažniausi kibernetinių nusikaltimų padariniai viešiesiems subjektams 2023 m.:

-  **neteisėtas elektroninių duomenų paskelbimas;**
-  **elektroninių duomenų užšifravimas, sugadinimas, pakeitimas ar sunaikinimas;**
-  **elektroninių duomenų stebėjimas, pasisavinimas.**

2023 m. kibernetinės atakos prieš viešųjų subjektų informacines sistemas dažniausiai buvo orientuotos į apgaulingos ir (ar) žalingos informacijos svetimo asmens vardu platinimą ir konfidencialią (neviešą) informaciją.

2023 m. tarp viešųjų subjektų konfidencialios (neviešos) informacijos, į kurią buvo taikytos kibernetinės atakos, dominavo finansiniai, ūkiniai, komerciniai elektroniniai duomenys, informacinių sistemų operaciniai duomenys, viešųjų subjektų valdomi asmens duomenys, kuriuos apibrėžia BDAR. Kitos kibernetinės atakos buvo susijusios su informacinių sistemų vartotojų autentifikavimosi duomenimis, privataus gyvenimo duomenimis, tarnybiniais, profesiniais duomenimis, valstybės tvarkomais informaciniais ištekliais.

2023 m. viešųjų subjektų informacinėse sistemose platintą apgaulingą ar žalingą elektroninę informaciją daugiausia sudarė neetiško ar bauginančio turinio informacija.

### Kibernetinių nusikaltimų poveikis valstybės įmonėms

2023 m. tarp visų subjektų, patyrusių kibernetinių nusikaltimų poveikį, valstybės įmonės sudarė iki 1 proc., arba šiek tiek mažiau nei 2022 m. 2023 m. kibernetinių atakų poveikį patyrė 2 valstybės įmonės – 1 veikianti energetikos sektoriuje (kaip ir 2022 m.) ir 1 susisiekimo sektoriuje (kaip ir 2022 m.).

2023 m. valstybės įmonės nukentėjo dėl poveikio interneto svetainėms.

Kibernetinių nusikaltimų padariniai valstybės įmonėms 2023 m. buvo prieigos prie informacinių sistemų ir (ar) elektroninių duomenų apribojimas.

### Kibernetinių nusikaltimų poveikis valstybės institucijoms

2023 m. išliko tendencija, kad kibernetinės atakos prieš valstybės institucijų informacines sistemas nėra sistemingas reiškinys. 2023 m. registruotos 3 kibernetinės atakos prieš valstybės institucijų informacines sistemas (iki 1 proc., arba panašiai kaip ir 2022 m.).

2023 m. kibernetines atakas patyrė 7 valstybės sektoriai. Po 2 kibernetines atakas patyrė informacinės sistemos, kurias valdo centrinės valdžios ir savivaldybių subjektai, po 1 kibernetinę ataką patyrė ministerijų, nacionalinio saugumo ir teisėsaugos, kariuomenės subjektai. 2023 m. po 1 kibernetinę ataką patyrė šių centrinės valdžios subjektų informacinės sistemos: Lietuvos Respublikos Vyriausybės, Lietuvos Respublikos Seimo.

2023 m. 1 kibernetinę ataką patyrė Lietuvos Respublikos užsienio reikalų ministerijos informacinė sistema. 2023 m. 1 kibernetinę ataką patyrė Lietuvos kariuomenės subjektų informacinė sistema. 2023 m. po 1 kibernetinę ataką patyrė šių 2 nacionalinio saugumo ir teisėsaugos subjektų informacinės sistemos: policijos, Lietuvos Respublikos vadovybės apsaugos tarnybos (1 naujas atvejis).

2023 m. valstybės institucijos nukentėjo dėl poveikio interneto svetainėms, informacinių sistemų tinklams ir (ar) galiniams įrenginiams, el. pašto paskyroms.

Kibernetinių nusikaltimų padariniai valstybės institucijoms 2023 m. buvo prieigos prie informacinių sistemų ir (ar) elektroninių duomenų apribojimas, neteisėtas elektroninių duomenų paskelbimas, el. pašto adresų imitavimas ir (ar) elektroninio susirašinėjimo perėmimas, elektroninių duomenų užšifravimas, sugadinimas, pakeitimas ar sunaikinimas.






Kibernetinės atakos prieš valstybės informacines sistemas 2023 m. taip pat nepadarė žalos valstybės ir tarnybos paslaptims. 2023 m. kibernetinėmis atakomis prieš viešųjų subjektų informacines sistemas buvo taikytasi į konfidencialią (neviešą) informaciją (2 atvejai, arba panašiai kaip 2022 m.).

2023 m. tarp valstybės institucijų konfidencialios (neviešos) informacijos, į kurią buvo taikytos kibernetinės atakos, buvo tarnybiniai, profesiniai duomenys (1 naujas atvejis) ir informacinių sistemų operaciniai duomenys.

## 3 Kibernetiniai nusikaltimai plačiąja prasme

2023 m. šalies policijos įstaigose užregistruotos 42 452<sup>07</sup> nusikalstamos veikos, iš kurių 3 912<sup>08</sup> nusikalstamų veikų, arba 9 proc., buvo padarytos elektroninėje erdvėje. 2023 m. nusikalstamų veikų elektroninėje erdvėje, palyginti su 2022 m., sumažėjo 26 proc., arba 1 397 nusikalstamomis veikomis. Bendroje nusikalstamumo struktūroje nusikalstamų veikų, padarytų elektroninėje erdvėje, dalis 2023 m. sumažėjo 3 proc. punktais. 2023 m. nusikalstamų veikų, padarytų fizinėje aplinkoje, padaugėjo 2 proc., arba 861 nusikalstama veika. Tai rodo, kad 2023 m. nusikalstamos veikos elektroninėje erdvėje neturėjo įtakos registruoto nusikalstamumo augimui ir jų grėsmės lygis gerokai nukrito.

Kaip ir pastaraisiais metais, 2023 m. išliko tendencija, kad nusikalstamumą elektroninėje erdvėje labiausiai lemia:

-  **sukčiavimo (LR BK 182 str.) atvejai – 50 proc.;**
-  **nusikaltimai elektroninėje erdvėje siaurąja prasme – 16 proc.;**
-  **neteisėto elektroninės mokėjimo priemonės ar jos duomenų panaudojimo atvejai (LR BK 215 str.) – 14 proc.;**
-  **netikros elektroninės mokėjimo priemonės gaminimo, tikros elektroninės mokėjimo priemonės klastojimo ar neteisėto disponavimo elektronine mokėjimo priemone arba jos duomenimis atvejai (LR BK 214 str.) – 7 proc.;**
-  **disponavimo pornografinio turinio dalykais atvejai (LR BK 309 str.) – 6 proc.;**  
**jaunesnio negu šešiolikos metų asmens tvirkinio atvejai (LR BK 153 str.)**

<sup>07</sup> Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos duomenys apie ikiteisminio tyrimo įstaigose užregistruotas nusikalstamas veikas (Forma\_EK-ITJ).

<sup>08</sup> Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos duomenys apie užregistruotas nusikalstamas veikas, padarytas elektroninėje erdvėje (Forma\_EL-ERDVĖ-ITJ).

⚠ – 1 proc.;

⚠ šmeižimo atvejai (LR BK 154 str.) – 1 proc.;

⚠ kurstymo prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę atvejai (LR BK 170 str.) – 1 proc.;

⚠ turto prievartavimo atvejai (LR BK 181 str.) – 1 proc.;

⚠ dokumento suklastojimo ar disponavimo suklastotu dokumentu atvejai (LR BK 300 str.) – 1 proc.;

⚠ grasinimo nužudyti ar sunkiai sutrikdyti žmogaus sveikatą arba žmogaus terorizavimo atvejai (LR BK 145 str.) – iki 1 proc.

2023 m. dominuojantys sukčiavimo elektroninėje erdvėje būdai nesikeitė.

### Avansinis (išankstinio mokėjimo) sukčiavimas

2023 m. avansinio (išankstinio mokėjimo) sukčiavimo atvejų padaugėjo. Šių nusikaltimų skaičius kasmet sparčiai didėja. Pagrindinis avansinio (išankstinio mokėjimo) sukčiavimo būdas yra apgaulingų skelbimų platinimas internete ir išprovokavimas virtualiai susitarti ir atlikti mokėjimą į sukčiaus nurodytą sąskaitą. 2023 m. tarp apgaulingų skelbimų dominavo pasiūlymai pirkti mobiliuosius telefonus ir (ar) kompiuterių techniką, transporto priemones, transporto priemonių dalis, buitinę techniką, išsinuomoti nekilnojamąjį turtą. 2023 m. išryškėjo nauja tendencija, kad dominuojančia apgaulingų skelbimų vieta tampa socialiniai tinklai. 2023 m. socialiniame tinkle „Facebook“ buvo platinta apgaulingų skelbimų daugiau nei 2022 m. Nacionaliniuose reklamos ir (ar) naudotų daiktų komercijos portaluose, dažniausiai **skelbiu.lt**, **autoplus.lt**, **autogidas.lt**, **vinted.lt**, platintų apgaulingų skelbimų dalis 2023 m. sudarė 33 proc. 2023 m. nukentėjusiųjų dėl apgaulingų skelbimų platinimo tarptautinėse reklamos platformose dalis ir toliau liko nedidelė. 2023 m. tirti atvejai taip pat patvirtino, kad Lietuvos gyventojai su didžiausia tarptautinio sukčiavimo rizika susiduria Vokietijos reklamos svetainėje **mobile.de**. Svarbiausios avansinio (išankstinio mokėjimo) komunikavimo priemonės 2023 m. nekito – dažniausiai buvo naudojamos nacionaliniu telefoniniu ryšiu ir mobiliosios bendravimo programos „Facebook“ programėle „Messenger“.

### Sukčiavimas naudojant apgaulingas SMS žinutes

Sukčiavimų naudojant apgaulingas SMS žinutes kasmet daugėja. Svarbiausias sukčiavimo, kai siunčiamos apgaulingos telefoninės SMS žinutės, motyvas 2023 m. išliko toks pat – grobstymas iš svetimų sąskaitų. SMS žinutėse teikiamos nuorodos į suklastotas svetaines ir išprovokuojama įvesti elektroninės bankininkystės duomenis ir (ar) patvirtinti apgaulingai inicijuotą pavedimą iš sąskaitos. 2023 m. apgaulingų telefoninių SMS žinučių buvo išplatinta dangstantis Valstybinės mokesčių inspekcijos vardu ir tariama prievole sumokėti baudą, taip pat dangstantis siuntų tarnybų vardu ir tariamu būtinumu sumokėti siuntos mokestį ar patikslinti adresato duomenis. Kita vertus, 2023 m. gerokai sumažėjo atvejų, kai buvo dangstomasi finansų įstaigų ir (ar) jų informacinių sistemų vardu ir tariamomis problemomis elektroninės bankininkystės vartotojų paskyrose.

### Investicinis sukčiavimas

Finansų sektoriaus dalyvių duomenimis, 2023 m. gerokai išaugo investicinio sukčiavimo būdu padaryta žala gyventojams: 2023 m. – apie 4,8 mln. eurų, o 2022 m. – 1,9 mln. eurų. Pažymėtina, kad finansų įstaigų pastangomis išvengta dar didesnių nuostolių – proaktyviai sustabdytas apie 1 mln. apgaule išviliotų lėšų pervedimas<sup>09</sup>.

2023 m. investicinio sukčiavimo atvejų gerokai padaugėjo nei 2022 m. Šių nusikaltimų skaičius kasmet sparčiai didėja. 2023 m. didžiąją dalį investicinio sukčiavimo atvejų sudarė apgaulingų investavimo platformų reklamos platinimas internete, išprovokavimas reklamos anketose užregistruoti kontaktinius duomenis ir, komunikuojant telefonu ir (ar) internetu, skatinimas daryti pavedimus į tariamai investuoti skirtas sąskaitas, kurias sukčiai kontroliuoja, iš jų persiveda ir pasisavina lėšas. Kita dažniausia investicinio sukčiavimo schema 2023 m. buvo telefoninių sukčių atakos ar apgaulingos reklamos platinimas internete, kai anksčiau nuo investicinio sukčiavimo nukentėjusiems asmenims pasiūloma tariama pagalba susigrąžinti prarastas lėšas. 2023 m. taip pat padaugėjo investicinio sukčiavimo atvejų, kai telefoniniai sukčiai išprovokuodavo nukentėjusiuosius melagingu reikalavimu uždaryti investicines sąskaitas, bauginami tuo, kad šias sąskaitas perėmė nusikalstamos struktūros ir naudoja neteisėtiems tikslams.

### Sukčiavimas naudojant apgaulingas internetinio bendravimo programėlių žinutes

2023 m. naudojimosi apgaulingomis internetinio bendravimo programų žinutėmis dinamika stabilizavosi. Svarbiausias sukčiavimo, kai siunčiamos apgaulingos internetinio bendravimo programų žinutės, motyvas 2023 m. išliko toks pat – grobstymas iš svetimų sąskaitų.

2023 m. didžiąją dalį apgaulingų internetinio bendravimo programų žinučių gavo daiktus internete parduodantys asmenys iš apsimetėlių pirkėjų. Nauja 2023 m. apgaulingų internetinio bendravimo programų žinučių tendencija buvo žinutės, kuriose dangstytasi tariamai Valstybinės mokesčių inspekcijos ir „Facebook“ draugo pranešimais. 2023 m. gerokai mažiau apgaulingų internetinio bendravimo programų žinučių gavo elektroninės bankininkystės vartotojai tariamai iš elektroninės bankininkystės informacinių sistemų.

2023 m. apgaulingomis internetinio bendravimo programų žinutėmis dažniausiai buvo platinamos nuorodos į šias 4 suklastotas interneto svetaines: „Omviva“, „Vinted“, DPD, Valstybinės mokesčių inspekcijos.

### Prekės ar paslaugos įgijimas sukčiavimo būdu

2023 m. atvejų, kai sukčiavimo būdu buvo įgytos prekės ar paslaugos, gerokai sumažėjo. Ilgą laiką matomas ryškus šių nusikaltimų skaičiaus mažėjimas. 2023 m. šiuos nusikaltimus dažniau lėmė atvejai, susiję su prekių ar paslaugų užvaldymu sudarant oficialius sandorius. Mažiau nei 2022 m. sudarė apgavystės, kai internete daiktus parduodantis asmuo būdavo išprovokuojamas išsiųsti prekę, prieš tai pateikęs jam pranešimą apie atliktą mokėjimą ir suklastoto pavedimo kopiją. Nauja forma buvo transporto priemonių įsigijimas sukčiavimo būdu. Kitos pasikėsinimo tendencijos liko panašios, tačiau reikšmingai sumažėjo pasikėsinimo į elektroninę techniką, laisvalaikio ir pramogų priemones, buitinę techniką atvejų.

09

VšĮ Pinigų plovimo prevencijos kompetencijų centro duomenys. Prieiga per internetą <https://amlcenter.lt/2023-m-finansiniu-sukciu-aktyvumas-augo-trecdaliu-pasitelke-vartotoju-pandeminius-iprocus/>.





### Sukčiavimas naudojant apgaulingus el. laiškus

2023 m. apgaulingų el. pašto laiškų atvejų gerokai sumažėjo. Šių nusikaltimų rizikingas augimo tempas sulėtėjo.

Svarbiausias apgaulingų el. pašto laiškų motyvas 2023 m. išliko toks pat – išprovokuoti elektroninės bankininkystės vartotojus.

2023 m. išryškėjo nauja forma – Valstybinės mokesčių inspekcijos vardu siunčiami apgaulingi el. laiškai su pranešimu apie prievolę sumokėti baudą. El. laiškais buvo siunčiamos nuorodos į suklastotas svetaines ir išprovokuojama suvesti elektroninės bankininkystės duomenis ir (ar) patvirtinti apgaulingai inicijuotą pavedimą iš sąskaitos.

2023 m. apgaulingi el. laiškai dažniausiai buvo platinami daiktų interneto platformos „Vinted“ ir kitų reklamos portalų pardavėjams. Jiems apsimetėliai pirkėjai siuntė nuorodas ir išprovokuodavo suklastotose svetainėse suvesti elektroninės bankininkystės duomenis ir (ar) patvirtinti apgaulingai inicijuotą pavedimą iš sąskaitos.

Ilgalaikės tendencijos stebėsena rodo, kad kasmet išlieka panašus atvejų skaičius, kai sukčiai įsiterpia į verslo subjektų elektroninį susirašinėjimą, kuriuo derinamas komercinis sandoris, ir mokėjimą nukreipia į apgaulingai nurodytą banko sąskaitą.

### Sukčiavimo būdu padaryta žala

Finansų rinkos dalyvių duomenimis, iš Lietuvos gyventojų ir juridinių asmenų 2023 m. apgaule buvo išviliota apie 12,3 mln. eurų, t. y. 3,9 proc. daugiau negu 2022 m., tačiau finansų įstaigoms pavyko susigrąžinti beveik 900 tūkst. eurų. Praėjusiais metais finansų įstaigos fiksavo per 10 tūkst. sukčiavimo atvejų<sup>10</sup>. Lietuvos kriminalinės policijos biuro duomenimis, 2023 m. išliko tendencija, kad dažniausiai išviliotų pinigų sumos buvo iki 1 000 eurų dydžio. Didžiausių žalų, kai lėšos viršijo 10 000 eurų sumas, atvejai 2023 m. sudarė 9 proc. (arba 19 proc. daugiau nei 2022 m.).

### Socialinės inžinerijos metodai, kuriems mažiausiai atsparūs Lietuvos gyventojai

Sukčiavimo atvejų stebėsena rodo, kad slaptažodžių išviliojimas suklastotomis žinutėmis ar duomenų viliojimo kampanijomis yra dažniausiai naudojamas ir ypač paveikus lėšų išviliojimo apgaule būdas. Tiek žinutės, tiek el. laiškai sukuriama taip, kad sukeltų pasitikėjimą, baimę, verstų skubėti, todėl dažnu atveju neatkreipiama dėmesio į tai, kad žinutė gali būti apgaulinga. Nors šioje srityje itin svarbi informacijos sklaida laiku bei visuomenės atsparumas sukčiavimams<sup>11</sup>, tačiau, vertinant sukčiavimų skaičiaus pokytį, pažymėtina ir kitų prevencinių priemonių svarba (pavyzdžiui, aktyvus privatus sektorius bei gyventojų bendradarbiavimas su NKSC blokuojant žalingus šaltinius).

10

VšĮ Pinigų plovimo prevencijos kompetencijų centro duomenys. Prieiga per internetą <https://amlcenter.lt/2023-m-finansiniu-sukciu-aktyvumas-augo-trecdaliu-pasitelke-vartotoju-pandeminius-iprocus/>.

11

Naudingų patarimų, kaip išvengti sukčiavimo, pateikiama Lietuvos policijos interneto svetainės rubrikoje „Sukčiavimo būdai“. Prieiga per internetą <https://policija.lrv.lt/lt/policija-pataria>.

## Incidentų analizė

2023 m. liepos mėnesį pradėti du ikiteisminiai tyrimai dėl poveikio NATO viršūnių susitikimui Vilniuje. Vienas tyrimas pradėtas dėl įsilaužimo į policijos tarnybinio el. pašto paskyrą Vidaus reikalų telekomunikaciniame tinkle ir dėl darbo grupės NATO viršūnių susitikimui Vilniuje organizuoti dalies susirašinėjimo perėmimo. Programišių grupuotė „From Russia with Love“ nutekintus tarnybinius dokumentus, kurie buvo rengti Lietuvos Respublikos Vyriausybėje, Lietuvos Respublikos užsienio reikalų ministerijoje, Lietuvos Respublikos vadovybės apsaugos tarnyboje, policijoje, paskelbė „Telegram“ kanale „Colonelcassad“. Kitas ikiteisminis tyrimas buvo pradėtas dėl masinių DDoS atakų prieš Lietuvos valstybės institucijų ir verslo interneto svetaines nuo 2023 m. gegužės 6 d. iki 2023 m. birželio 4 d. (ne mažiau kaip 40 svetainių) ir nuo 2023 m. liepos 10 d. iki 2023 m. liepos 13 d. (ne mažiau kaip 21 svetainė). Šioms DDoS atakoms, kuriomis buvo reaguojama į Lietuvos valstybės paramą, skirtą Ukrainai atremti Rusijos karinę agresiją, taip pat į NATO viršūnių susitikimą 2023 m. liepos mėnesį Vilniuje, organizuoti susivienijo ne mažiau kaip 17 Rusijos programišių grupių. Tarp jų buvo ir 2022 m. prieš Lietuvą veikusi Rusijos programišių grupė „Killnet“. Atakuotų Lietuvos svetainių sąrašus ir poveikio joms rezultatus Rusijos programišių grupė „Noname05716“ viešino „Telegram“ kanale. 2023 m. rugsėjo mėnesį ši Rusijos programišių grupė įsilaužė į dar septynių Lietuvos viešųjų subjektų interneto svetaines ir jose paskelbė žalingo turinio informaciją – agresyvią Rusijos politikos propagandą.

2023 m. spalio mėnesį pradėtas ikiteisminis tyrimas dėl koncentruotos informacinės atakos, kuria siekta sukelti ažiotažą, sumaištį visuomenėje ir sutrikdyti Lietuvos institucijų veiklą. Nustatyta, kad nuo 2023 m. spalio 11 d. iki 2023 m. spalio 24 d. iš skirtingų „Gmail“ elektroninio pašto adresų buvo išplatinta daugiau kaip 3 800 melagingų pranešimų rusų kalba apie galimai mokyklų ir kitų valdžios institucijų bei visuomeninių organizacijų pastatuose padėtus sprogmenis su nurodytu detonacijos laiku. Dėl šių grasinimų mokyklose buvo sutrikdytas ugdymo procesas, kai kurios iš jų organizavo evakuaciją, nutraukė pamokas, perėjo prie nuotolinio mokymo. Grasintojai veikė skirtingų prorusiškų „Baltijos“ teroristų grupių vardu, apie savo veiklą ir melagingų grasinimų sprogdinti informacinę kampaniją skelbė socialinio tinklo „Telegram“ kanale @prbfront.



## 4 Tarptautinis bendradarbiavimas

Stebint nusikalstamų veikų elektroninėje erdvėje dinamiką, kartu matomas ir tarptautinių nusikalstamų skaičiaus didėjimas. Tokio pobūdžio nusikalstamų veikų identifikavimas ir užkardymas yra komplikuoatas ne tik dėl technologinių priemonių sudėtingumo, tačiau ir dėl to, kad šio pobūdžio nusikalstamos veikos vis dažniau sietinos su keliomis valstybėmis. Todėl šiuo atveju ypač svarbus tarptautinis bendradarbiavimas.

Lietuvos policija, o būtent Lietuvos kriminalinės policijos biuras, aktyviai dalyvauja Europos kovos su nusikalstamumo grėsmėmis tarpdisciplininės platformos (EMPACT) ir Europolo analitinių projektų, susijusių su kova su nusikaltimais elektroninėje erdvėje ir sukčiavimais, veikloje. Tarptautiniu bendradarbiavimu siekiama kovoti su organizuotais ir sunkiais tarptautiniais nusikaltimais, naudojantis valstybių narių patirtimi bei Europos Sąjungos institucijų pagalba. Tarpusavio bendradarbiavimas grindžiamas integruotu požiūriu į Europos Sąjungos vidaus saugumą, apimančiu informacijos valdymo, inovacijų, mokymo, prevencijos, viešojo ir privataus sektoriaus partnerystės aspektus. Identifikavus didžiausias grėsmes kryptingai ir nuosekliai dirbama tiek strateginiu, tiek taktiniu lygiu siekiant jas užkardyti.

Bendradarbiaujant keičiamasi informacija tarp valstybių apie aktualias tendencijas, užsienio valstybių gerąją praktiką nusikalstamų užkardymo ir atskleidimo srityje, identifikuojamos sisteminės nusikalstamos veikos, darančios poveikį valstybių narių gyventojams. Užkardant nusikaltimus elektroninėje erdvėje akcentuojama viešojo ir privataus sektoriaus partnerystės svarba, aktyvus techninių prevencinių priemonių taikymas, informacijos sklaida laiku.

Paminėtina, kad, atsižvelgdamas į nusikalstamumo elektroninėje erdvėje tendencijas, Europolas aktyviai plėtoja bendradarbiavimą su trečiosiomis šalimis.

Siekdamas užkardyti tarptautinį nusikalstamumą elektroninėje erdvėje, 2023 m. Lietuvos kriminalinės policijos biuras bendradarbiavo su 15 užsienio valstybių. Per sėkmingas tarptautines operacijas kartu su Europos Sąjungos ir kitų užsienio valstybių partneriais atskleisti ir sulaikyti elektroninėje erdvėje nusikalstamas veikas vykdė asmenys.

**Kaip sėkmingo tarptautinio bendradarbiavimo pavyzdžius galima paminėti šias išskirtines operacijas:**

✓ 2023 m. rugsėjo mėnesį per Europole veikiančio Europos kibernetinių nusikaltimų centro koordinuotą Suomijos muitinės tarnybos, Lietuvos kriminalinės policijos biuro, Vokietijos federalinės kriminalinės tarnybos ir Eurojusto operaciją buvo atskleistas ir uždarytas tamsiojo interneto tinklas „Tor“ (nuo 2022 m. gegužės mėnesio suomių kalba veikusiame tinklalapyje „Piilopuoti“ buvo dideliais kiekiais prekiaujama narkotinėmis medžiagomis ir kitomis nelegaliomis prekėmis<sup>12</sup>).

✓ 2023 m. rugsėjo mėnesį atlikus Kauno apskrities vyriausiojo policijos komisariato Kriminalinės policijos nusikaltimų nuosavybei tyrimų padalinio inicijuotą tyrimą Graikijoje buvo uždaryta nelegali sintetinių narkotikų laboratorija, kurios produkcija, įskaitant ir tarp jaunimo itin populiarius „Smile“ psichotropinius skysčius, per slaptą interneto prekyvietę buvo tiekiami ne tik į Lietuvą ir kitas Europos valstybes, bet ir JAV bei Australiją<sup>13</sup>.

12

„Per tarptautinę teisėsaugos operaciją uždarytas tamsiojo interneto tinklalapis“. Prieiga per internetą <https://www.delfi.lt/news/daily/crime/per-tarptautine-teisesaugos-operacija-uzdarytas-tamsiojo-interneto-tinklalapis.d?id=94656235>.

13

„Kauno pareigūnai prisikasė iki slaptos laboratorijos užsienyje: narkotikai iš čia keliavo po visą pasaulį“. Prieiga per internetą <https://www.delfi.lt/news/daily/crime/kauno-pareigunai-prisikase-iki-slaptos-laboratorijos-uzsienyje-narkotikai-is-cia-keliavo-po-visa-pasauli.d?id=94656715>.

## 5 Prevencija

2023 m. policija ir toliau sistemingai taikė prevencines priemones, kuriomis visuomenę informavo, kaip netapti sukčiavimo auka. Lietuvos policijos įstaigos savo prižiūrimos teritorijos gyventojus nuolat informavo apie dažniausius sukčiavimo būdus, teikė bendrą informaciją apie sukčiavimą, supažindino su naujausiomis kibernetinėmis grėsmėmis, mokė atpažinti socialinės inžinerijos atakas. Stebint nusikalstamumo dinamiką išryškėjo aktyvių ir prevencinių priemonių vykdymo laiku nauda. Siekdami užtikrinti visuomenės atsparumą šio pobūdžio nusikalstamoms veikoms, 2023 m. bendruomenės pareigūnai organizavo 2 477 šviečiamuosius susitikimus su visuomene, kaip saugiai pirkti elektroninėje erdvėje, kaip apsisaugoti nuo sukčiavimo elektroninėje erdvėje, taip pat lengvo uždarbio ir investavimo pavojų elektroninėje erdvėje prevencijos temomis. Susitikimuose dalyvavo 50 713 prižiūrimos teritorijos gyventojų. 2023 m. bendruomenės pareigūnai prevencinę informaciją apie nusikaltimus socialiniuose tinkluose viešino 827 kartus.

2023 m. aktyvią veiklą tęsė ir virtualus policijos patrulis. Siekdamas įspėti interneto naudotojus apie gresiančius pavojus dėl galimo sukčiavimo bei svarbių asmens bei kitų duomenų vagysčių elektroninėje erdvėje, virtualus policijos patrulis savo „Facebook“ paskyroje skelbė prevencinius pranešimus (33 pranešimai).

Paminėtina, kad virtualaus patrulio efektyvumas ir aktyvumas vis didėja. Per 2023 m. policijos virtualus patrulis nustatė ir užregistravo 445 galimus teisės pažeidimus, iš kurių dėl 28 pradėti ikiteisminiai tyrimai, dėl 303 – administracinio nusižengimo bylų teisenos, dėl 31 – asmenims buvo surengti prevenciniai pokalbiai, jie oficialiai įspėti.

Itin svarbus policijos bendradarbiavimas su privataus sektoriaus atstovais, nes operatyviau apsiikeičiama informacija, identifikuojamos rizikos, efektyviau taikomos prevencinės priemonės. Paminėtinas ir tęstinis bendradarbiavimas VŠĮ Pinigų plovimo prevencijos kompetencijų centro sukčiavimo prevencijos grupės veikloje. Taip pat svarbus Pinigų plovimo prevencijos kompetencijų centro indėlis rengiant mokymus sukčiavimo prevenciją užtikrinantiems specialistams ir teisėsaugos pareigūnams.

## 6 Mokymai

Didėjant žinių, kaip atskleisti elektroninėje erdvėje įvykdytas nusikalstamas veikas, poreikiui Lietuvos policija nuolat ieško būdų tobulėti bei 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 pasitelkimu vykdant nusikalstamas veikas. Ypač daug dėmesio skiriama ir tarpvalstybiniam įrodymų surinkimui, nes nemaža dalis šio tipo nusikalstamų veikų sietinos su keliomis valstybėmis. Kuriant mokymų programas bendradarbiaujama ir su Europolu. 2023 m. mokymuose, susijusiuose su nusikalstamų veikų elektroninėje erdvėje atskleidimu, dalyvavo daugiau kaip 300 policijos pareigūnų.

Analizuojant užsienio valstybių praktiką kvalifikacijos kėlimo srityje, nuolat vertinamos galimybės pareigūnams gilinti žinias ir tobulinti praktinius įgūdžius užsienio valstybių vykdomuose mokymuose.

# Elektroninių ryšių tinklų vientisumo užtikrinimas ir draudžiamos viešai skleisti informacijos internete užkardymas



Jūratė Šovienė,  
RRT tarybos pirmininkė

## Vadovo žodis

Ryšių reguliavimo tarnybos tikslas – saugūs elektroninių ryšių rinkos vartotojai, saugūs paslaugų teikėjai ir saugūs tinklai. Deja, dažnai susikoncentravę į infrastruktūros saugumą, pamirštame pasirūpinti silpnąja grandimi – vartotojais.

Vienas reikšmingesnių praėjusių metų Ryšių reguliavimo tarnybos pasiekimų – nustatytas įpareigojimas interneto paslaugų teikėjams taikyti NKSC žalingų nuorodų blokavimo užkardą, taip pat įtvirtintos sukčiavimo skambučiai ir SMS žinutėmis užkardymo priemonės.

Inicijavome ilgalaikį projektą „Nė vienas nėra pamirštas“, kurio tikslas – bendradarbiaujant su verslo ir kitomis organizacijomis edukuoti ir konsultuoti Lietuvos moksleivius ir senjorus skaitmeninėje visuomenėje aktualiais klausimais.

Saugumas – kompleksinis klausimas, dėl to šioje srityje rezultatų galime pasiekti tik bendradarbiaudami visi nacionaliniu ir tarptautiniu lygiu.



## KĄ SAUGO?

- ✓ Viešųjų elektroninių ryšių paslaugų naudotojų teisę į nepertraukiamą paslaugų teikimą.
- ✓ Nepilnamečių ir kitų asmenų teisę į švarią skaitmeninę erdvę.



## NUO KO SAUGO?

- ✓ Nuo elektroninių ryšių tinklų vientisumo pažeidimų.
- ✓ Nuo draudžiamos skleisti ar neigiamą poveikį nepilnamečiams darančios informacijos internete.



## KAIP SAUGO?

- ✓ Užtikrindama, kad viešųjų ryšių tinklų teikėjai įgyvendintų tinkamas technines ir organizacines savo viešųjų ryšių tinklų vientisumo priemones.
- ✓ Vykdydama interneto karštosios linijos „Svarus internetas“ veiklą ir užtikrindama, kad patyčios ir kita draudžiama skleisti informacija būtų pašalinta arba būtų atitinkamai pažymėta ir apribota.
- ✓ Aprobudama ir prižiūrėdama turinio filtravimo priemones, kuriomis viešųjų kompiuterių tinklų (internetu) prieigos vietose ribojama neigiamą poveikį nepilnamečiams daranti viešoji informacija.
- ✓ Edukuodama gyventojus skaitmeninio turinio klausimais bei konsultuodama interneto naudotojus, kaip saugiai elgtis internete ir socialiniuose tinkluose.



## Svarbiausi 2023 m. įvykiai ir tendencijos



2023 m. RRT iš penkių paslaugų teikėjų gavo 17 pranešimų apie viešųjų ryšių tinklų vientisumo pažeidimus.



Pagrindinės viešųjų ryšių tinklų vientisumo pažeidimų priežastys – elektros energijos tiekimo sutrikimai, kabelio nutraukimas, tinklo įrangos gedimai.



2023 m. RRT interneto karštąją liniją ([www.svarusinternetas.lt](http://www.svarusinternetas.lt)) gavo 2 516 pranešimų apie internete rastą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją. Daugiau nei pusė atvejų (59 proc. visų gautų pranešimų) pasitvirtino.



2023 m. RRT specialistai socialinių tinklų naudotojams suteikė 17 proc. daugiau konsultacijų apie saugų elgesį internete nei 2022 m.



RRT, siekdama didesnio interneto naudotojų sąmoningumo, 2023 m. vykdė papildomą interneto naudotojų švietėjišką veiklą, vedė pamokas mokiniams apie saugų elgesį internete, organizavo paskaitas, susitikimus ir praktines dirbtuves Lietuvos pensininkams.



RRT 2023 m. pasirašė ilgalaikę sutartį su Kanados nevyriausybine organizacija „Canadian Centre for Child Protection“ (C3P) dėl dalyvavimo jos vykdomame projekte „Arachnid“, skirtame kovai su vaikų seksualinio išnaudojimo medžiagos sklaida internete.



2023m. RRT tyrėjai dalyvaudami projekte „Arachnid“ įvertino 68 348 potencialiai draudžiamą turinio vaizdus, iš jų 35 114 pripažino kaip vaikų seksualinio išnaudojimo medžiagą (angl. Child Sexual Abuse Material (CSAM)).



RRT atliktos kasmetinės apklausos duomenimis, 25 proc. įstaigų, dalyvavusių apklausoje, naudoja netinkamas turinio filtravimo priemones, t. y. 16 proc. įstaigų naudoja kitas RRT neapčiuotus turinio filtravimo priemones, o 9 proc. nenaudoja jokių turinio filtravimo priemonių.



RRT įpareigojo interneto paslaugų tiekėjus taikyti NKSC žalingų interneto nuorodų blokavimo įrangą – DNS užkardą.



Priimdama naujas ir tobulindama ankstesnes teisinės normas, RRT įtvirtino sukčiavimo apgaulingais skambučiais ir SMS žinutėmis užkardymo priemones.



**01**

Pranešimo ir keitimosi informacija apie įvykį, ekstremaliųjų įvykį, ypatingą įvykį, ekstremaliąją situaciją ar krizę tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2022 m. gruodžio 29 d. nutarimu Nr. 1317 „Dėl Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymo įgyvendinimo“. Prieiga per internetą <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/044f60e1875e11edbdcabd68a7a0df7e/asr>.

**02**

Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos 2023 m. spalio 19 d. nutarimas Nr. TN-519 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. balandžio 25 d. įsakymo Nr. 1V-394 „Dėl Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklių patvirtinimo“ pakeitimo“. Prieiga per internetą <https://www.e-tar.lt/portal/lt/legalAct/1983ff806e8911ee8f3bca2fb16d96d>.

**1 pav.**

Pagrindinės viešųjų ryšių tinklų vientisumo pažeidimų priežastys ir palyginimas suankstesniais metais (šaltinis – RRT).

# 1 Viešųjų ryšių tinklų vientisumo užtikrinimas Lietuvoje

Vadovaujantis Lietuvos Respublikos elektroninių ryšių įstatymo (toliau – ERĮ) 51 straipsnio 1 dalimi, viešųjų ryšių tinklų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų viešųjų ryšių tinklų vientisumui užtikrinti, kad šiais tinklais būtų nepertraukiamai teikiamos viešosios elektroninių ryšių paslaugos. Be to, ERĮ 51 straipsnio 4 dalyje numatyta, kad įvykus vientisumo pažeidimui, kuris turėjo didelę įtaką viešojo ryšių tinklo veikimui arba viešųjų elektroninių ryšių paslaugų teikimui, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas (toliau – paslaugų teikėjas) privalo nedelsdamas apie šį vientisumo pažeidimą informuoti RRT.

Atkreiptinas dėmesys, kad RRT, atsižvelgdama į Lietuvos Respublikos Vyriausybės 2022 m. gruodžio 29 d. nutarimu Nr. 1317 patvirtinto Pranešimo ir keitimosi informacija apie įvykį, ekstremaliųjų įvykį, ypatingą įvykį, ekstremaliąją situaciją ar krizę tvarkos aprašo (toliau – Pranešimo aprašas) nuostatas<sup>01</sup>, 2023 m. spalio 19 d. priėmė nutarimo „Dėl Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklių patvirtinimo“ pakeitimą (toliau – Taisyklės)<sup>02</sup>. Vadovaujantis Taisyklėse nustatyta tvarka, buvo atsisakyta reikalavimo teikėjams apie vientisumo pažeidimus informuoti RRT telefono ryšio numeriu ir paliktas reikalavimas informuoti el. paštu vientisumas@rrt.lt. Taip optimizuotas RRT darbo organizavimas, žmoniškųjų resursų paskirstymas.

2023 m. RRT iš penkių paslaugų teikėjų gavo 17 pranešimų apie viešųjų ryšių tinklų vientisumo pažeidimus. Pagrindinės viešųjų ryšių tinklų vientisumo pažeidimų priežastys ir palyginimas su ankstesniais metais pateiktas lentelėje (žr. **1 pav.**).

	2021 m.		2022 m.		2023 m.	
Viešųjų ryšių tinklų vientisumo pažeidimų priežastys	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
Kabelio nutraukimas, remontas	3	62 000	-	-	1	381
Tarptinklinio ryšio paslaugų sutrikimai	–	–	–	–	–	–
Tinklo įrangos gedimai	5	1 000 000 <	3	1 000 000 <*	11	1 000 000 <*
Kita	–	–	2	40 000	3	100 000 <*
Iš viso	8		7		17	

Pažymėtina, kad 4 kartus apie ta patį paslaugų teikimo sutrikimą informacija buvo gauta iš 2 paslaugų teikėjų. To priežastis – naudojimasis tais pačiais duomenų perdavimo resursais, todėl, įvykus gedimui vieno iš paslaugų teikėjų duomenų perdavimo centre, tam tikram laikui sutrikdavo duomenų perdavimas ir kito paslaugų teikėjų tinkle. Buvo gauti 2 pranešimai apie mobiliojo ryšio tinklo pažeidimus, 1 pranešimas apie mobiliojo ir fiksotojo ryšio tinklų pažeidimus bei 2 pranešimai apie nacionalinės televizijos transliacijos sutrikimą ir nutrūkimą, tačiau pažeidimai buvo ypač trumpos trukmės (5–9 min.). Vienas paslaugų teikėjų iš anksto informavo RRT apie planinius darbus, dėl kurių viename iš mažų miestelių nebuvo transliuojami 2 nacionalinės televizijos kanalai.

2023 m. viename iš viešųjų ryšių tinklų vientisumo pažeidimo pranešimų buvo nurodyta, kad, atliekant tinklo įrangos programinės konfigūracijos keitimo darbus, daliai klientų galėjo sutrikti duomenų perdavimo paslaugos, todėl jiems reikėjo perkrauti mobiliuosius telefonus arba išjungti ir vėl įjungti interneto duomenis. Pažymėtina, kad per šį incidentą galėjo būti paveikta net iki 260 tūkst. mobiliojo interneto paslaugų gavėjų bei šis sutrikimas užtruko 10 val. 6 min. Tačiau taip pat pripažintina, kad atsižvelgiant į tai, jog incidentas įvyko naktį, realus (faktinis) paveiktų klientų skaičius galėjo būti mažesnis. Taip pat buvo gautas pranešimas apie paveiktus 100 tūkst. kalbinio ryšio naudotojus, kurie paslaugas gauna „VoLTE“ technologija<sup>03</sup>. Pažeidimas truko 2 val. ir 5 min. ir per incidentą 75 proc. kalbinio ryšio naudotojų, kurie paslaugas gauna „VoLTE“ technologija, galėjo patirti ryšio trikdžių. Ir nors šie viešųjų ryšių tinklų vientisumo pažeidimai iš kitų išsiskyrė didesniu poveikiu galutiniams paslaugų gavėjams, tačiau vis tik nei paskutiniai paminėti, nei kiti 2023 m. pažeidimai neatitiko Pranešimo aprašo 2 priedo „Ekstremaliųjų įvykių kriterijų sąrašas“ 4.14–4.17 papunkčiuose nustatytų ekstremaliųjų įvykių trukmės kriterijų, dėl kurių apie pažeidimą reikėtų pranešti Lietuvos Respublikos Vyriausybės kanceliarijai, Priešgaisrinės apsaugos ir gelbėjimo departamentui prie Vidaus reikalų ministerijos, Lietuvos Respublikos valstybės saugumo departamentui ir NKSC.

Taigi, vertinant pateiktą informaciją ir apibendrintą viešųjų ryšių tinklų vientisumo situaciją, pažymėtina, kad 2023 m. viešųjų ryšių tinklų vientisumo pažeidimų skaičius ir mastas yra panašus kaip ir ankstesniaisiais metais. Viešojo mobiliojo ir viešojo fiksotojo ryšio tinkluose 2023 m. fiksuoti gedimai pašalinti operatyviai, o viešųjų ryšių tinklų vientisumo pažeidimų mastas nesukėlė ekstremalių įvykių, dėl kurių būtų reikėtų imtis papildomų veiksmų ir (ar) informuoti kitas institucijas teisės aktų nustatyta tvarka.

## Incidentų analizė



2023 m. vienas paslaugų viešųjų elektroninių ryšių paslaugų teikėjas informavo RRT apie skirtingais IP adresais vykdomas DDoS atakas<sup>04</sup>. Pažymėtina, kad DDoS atakas automatiškai fiksavo paslaugų teikėjas, jis pats sėkmingai užblokavo atitinkamus DDoS atakų srautus. Dėl šių atakų paslaugų teikimas vartotojams nesutriko, visos paslaugos buvo teikiamos.

Taip pat 2023 m. buvo gautas pranešimas apie gamtos stichijos padarytą žalą elektroninių ryšių paslaugų teikimui. Tuomet dėl vėtros siautusios Vilniuje vieno paslaugų teikėjo visos sistemos be elektros buvo 20 min., tačiau įjungus elektrą ne visa įranga pradėjo veikti tinkamai, todėl kai kurios paslaugos buvo atnaujintos iškart, tačiau dalies paslaugų atnaujinimas užtruko net iki 9 val.

**03**

„VoLTE“ (angl. *Voice over LTE*) – didelės spartos belaidžio ryšio standartas, skirtas balso skambučiams naudojant mobiliuosius telefonus ir duomenų terminalus.

**04**

DDoS ataka taikomasi į svetaines ir serverius, sutrikdomos tinklo paslaugos ir bandoma išnaudoti programos ištekliai. DDoS atakų srautu užtvindyta svetainė veikia prastai arba ji visiškai atjungiama.



svarus  
internetas



## Interneto karštosios linijos „Švarus internetas“ veikla

RRT siekia, kad vartotojai, ypač vaikai ir nepilnamečiai, būtų apsaugoti nuo žalingo turinio internete. Vadovaujantis Lietuvos Respublikos švietimo įstatymo 23<sup>2</sup> straipsniu, RRT nustatyta pareiga imtis veiksmų, kad draudžiama skleisti informacija būtų kuo greičiau pašalinta iš interneto, suteikta teisė duoti, o paslaugų teikėjams - vykdyti privalomus nurodymus (angl. *Notice and Take Down* (NTD)) Lietuvos elektroninės informacijos prieglobos ar viešųjų ryšių tinklų paslaugų teikėjams dėl draudžiamos skleisti informacijos pašalinimo iš jų tarnybinių stočių arba prieigos prie jos panaikinimo. Taip pat RRT aktyviai vykdo neteisėto ir žalingo turinio internete prevenciją.

RRT nuo 2007 m. yra įsteigusi ir administruoja interneto karštąją liniją „Švarus internetas“ ([www.svarusinternetas.lt](http://www.svarusinternetas.lt)). Šia interneto karštąja linija visi interneto naudotojai 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 tyčiojama, niekinama, skatinama neapykanta ar kurstoma diskriminuoti žmonių grupę ar jai priklausančią asmenį dėl lyties, seksualinės orientacijos, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų.

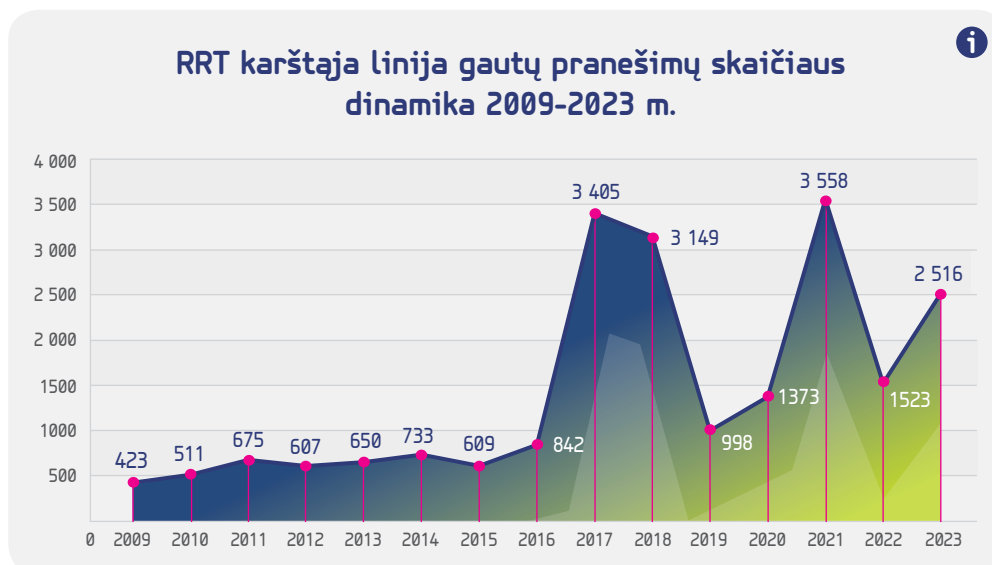
Kiekvienas gautas pranešimas, laikantis nustatytų procedūrų, ištiriamas RRT specialistų, o pasitvirtinus, jog turinys išties draudžiamas pagal Lietuvos teisės aktus ir saugomas Lietuvoje esančiose tarnybinėse stotyse, perduodamas tolesniam tyrimui Policijos departamentui bei kreipiamasi į informacijos prieglobos paslaugų teikėją, kad šis turinys būtų kuo greičiau pašalintas arba būtų nutraukta prieiga prie jo. Jei Lietuvoje draudžiamas turinys skelbiamas užsienio tarnybinėse stotyse ir tas turinys galimai draudžiamas ir pagal kitos šalies įstatymus, tada pranešimas persiunčiamas tolesniam tyrimui atitinkamos šalies interneto karštąjai linijai. Tuo atveju, jei turinys nėra draudžiamas, bet galimai darantis neigiamą poveikį nepilnamečiams, pranešimas persiunčiamas Žurnalistų etikos inspektoriatui tarnybai.

RRT administruojama interneto karštoji linija jau nuo 2008 m. yra tarptautinės interneto karštųjų linijų asociacijos INHOPE (<https://www.inhope.org/>), vienijančios 54 interneto karštąsias linijas iš 50 šalių, narė. RRT, kaip ir kitų INHOPE asociacijos vienijamų interneto karštųjų linijų, pagrindinis tikslas - kuo greičiau pašalinti draudžiamą skleisti turinį iš interneto. Ypač aktyviai INHOPE kovoja su vaikų seksualinio išnaudojimo vaizdų platinimu.

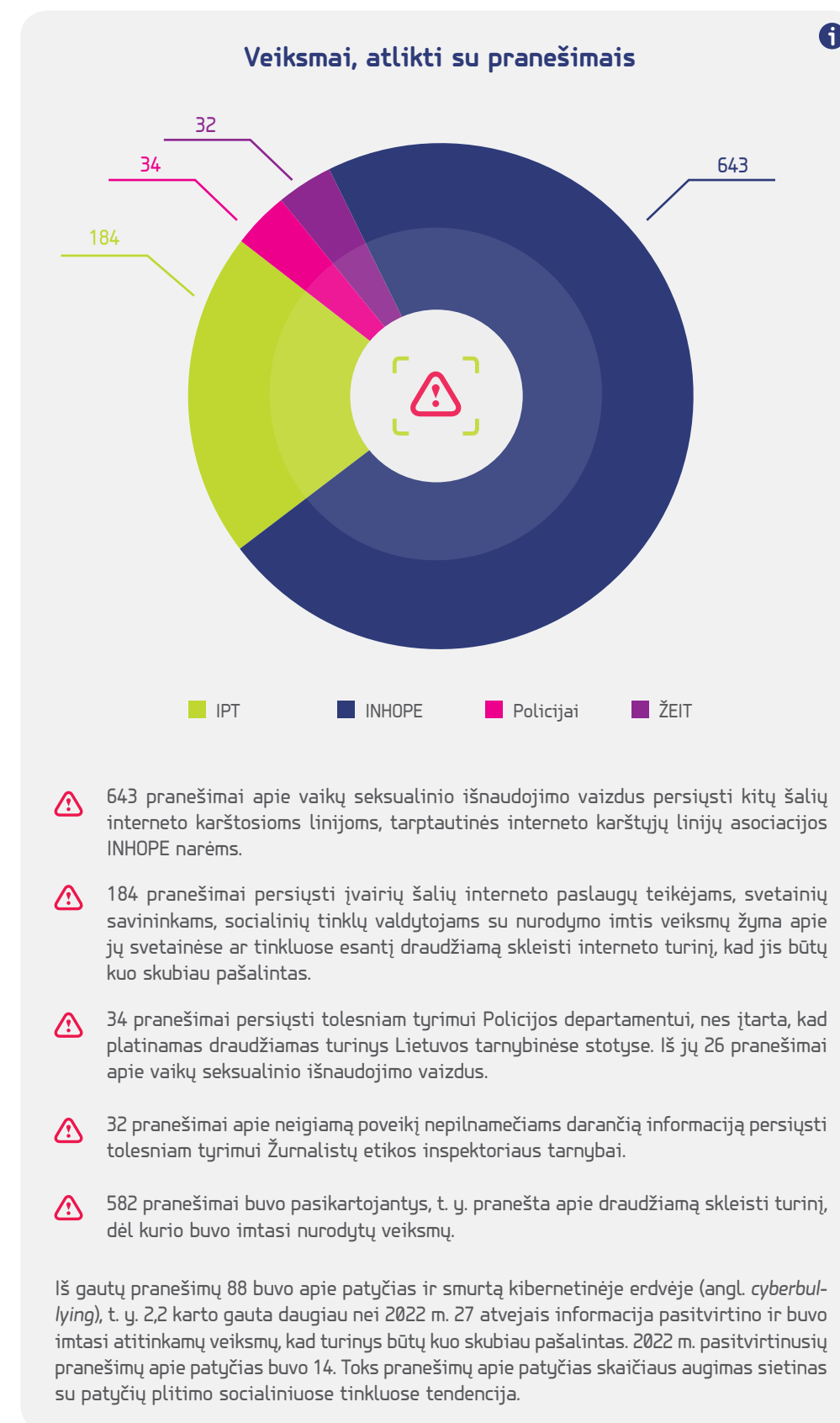
2023 m. RRT interneto karštąja linija gavo 2 516 pranešimų apie internete rastą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją. Palyginti su 2022 m. (1 523 pranešimai), pranešimų skaičius padidėjo 65 proc. (žr. 2 pav.)

### 2 pav. >

RRT karštąja linija gautų pranešimų dinamika 2009–2023 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 1 475 (tai sudaro 59 proc. visų gautų pranešimų). Svarbu paminėti, kad didelę pasitvirtinusių pranešimų dalį (669 atvejais) sudarė informacija dėl vaikų seksualinio išnaudojimo, t. y. tokių atvejų buvo 2,5 karto daugiau nei 2022 m. (272). 2023 m. RRT 893 atvejais dėl pasitvirtinusių pranešimų ėmėsi veiksmų (žr. 3 pav.).



### < 3 pav.

Veiksmai, atlikti su 2023 m. gautais pranešimais apie internete rastą galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją (šaltinis – RRT)



## 05

2021 m. balandžio 29 d. Europos Parlamento ir Tarybos Reglamentas (ES) 2021/784 dėl teroristinio turinio sklaidos internete klausimo sprendimo.<sup>05</sup> Prieiga per internetą <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32021R0784>.

## 06

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>.

## 07

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

## 08

Aprobuotų filtravimo priemonių sąrašas RRT interneto svetainėje <https://www.rtt.lt/saugesnis-internetas/turinio-filtravimo-priemones/>.

RRT nuo 2023 m. balandžio 28 d. vykdo vienos iš kompetentingų institucijų pagal 2021 m. balandžio 29 d. Europos Parlamento ir Tarybos Reglamentą (ES) 2021/784 dėl teroristinio turinio sklaidos internete klausimo sprendimo<sup>05</sup> funkcijas (vykdo prieglobos paslaugų teikėjų priežiūrą, t. y. kontroliuoja, ar jų veikla atitinka Reglamente nustatytus reikalavimus), taip pat buvo rengiamasi RRT vykdyti Skaitmeninių paslaugų koordinatoriaus funkcijas pagal 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)<sup>06</sup>, reikalavimus. Šis teisės aktas yra Europos iniciatyva užtikrinti „švaresnį“ internetą Europos Sąjungos gyventojams, o numatytus uždavinius šalys narės įgyvendins pasitelkdamos tiek nacionalines priemones, tiek europinį bendradarbiavimą.

## RRT dalyvavimas tarptautiniame projekte „Arachnid“

RRT ieškodama inovatyvių ir sėkmingai veikiančių įrankių, kurie padidintų galimybes aptikti ir padėtų kuo greičiau pašalinti draudžiamą interneto turinį, nuo 2022 m. rugsėjo bendradarbiauja su Kanados nevyriausybine organizacija „Canadian Centre for Child Protection“ (toliau – C3P) ir dalyvauja jų vykdomame „Arachnid“ projekte<sup>07</sup>. Šio projekto tikslas – vaikų seksualinio išnaudojimo medžiagos aptikimas ir pašalinimas iš interneto erdvės.

Šiuo metu prie projekto yra prisijungusios 15 interneto karštųjų linijų iš 14 šalių (Kanados, JAV, Kolumbijos, Švedijos, Suomijos, Estijos, Lietuvos, Belgijos, Vokietijos, Kroatijos, Albanijos, Kambodžos, Australijos ir Naujosios Zelandijos). RRT užduotis – vertinti „Arachnid“ klasifikavimo sistemoje robotų iš interneto surinktą medžiagą apie galimą vaikų seksualinį išnaudojimą (angl. *Child Sexual Abuse Material* (CSAM)) ir tuo prisidėti prie „Arachnid“ identifikuotų CSAM vaizdų duomenų bazės papildymo. Jau šeštus metus vystomo projekto „Arachnid“ dalyviai ir partneriai sėkmingai kovoja su visame pasaulyje draudžiamu turiniu, susijusiu su vaikų seksualinio išnaudojimu, aptikdami šį turinį „Arachnid“ sistema ir siųsdami pranešimus su nurodymo imtis veiksmų žyma informacijos prieglobos paslaugų teikėjams visame pasaulyje, kad jie pašalintų draudžiamą turinį iš savo serverių.

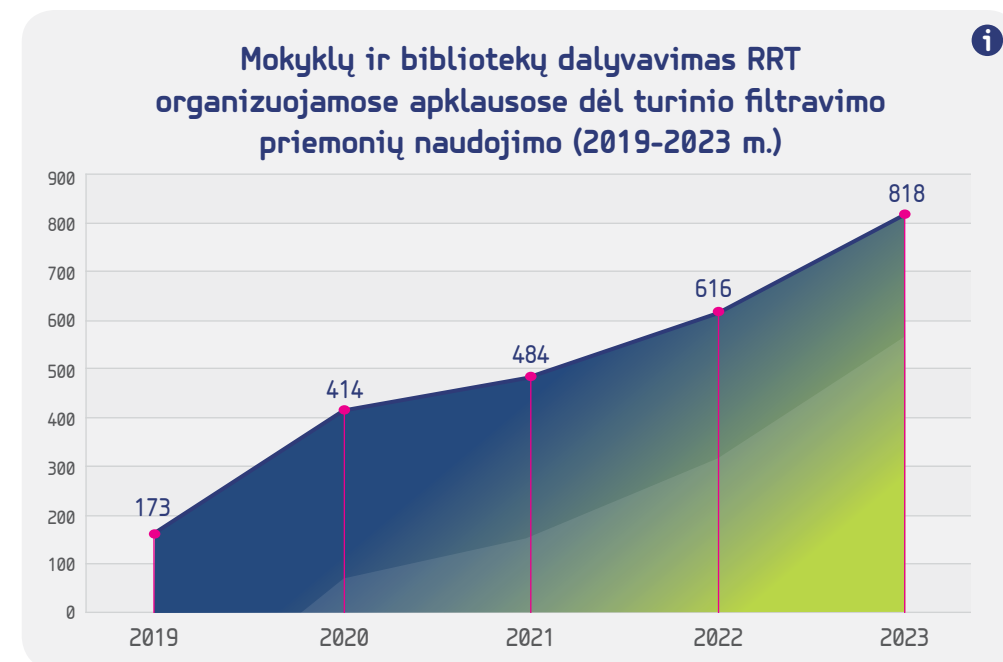
Atkreiptinas dėmesys, kad, RRT sėkmingai užbaigus pilotinio dalyvavimo projekte etapą ir C3P pripažinus RRT patikimu partneriu, 2023 m. pabaigoje buvo pasirašyta ilgalaikė projekto „Arachnid“ bendradarbiavimo sutartis.

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

RRT siekia, kad visose prieigos prie viešųjų kompiuterių tinklų (internetu) vietose, kur gali lankytis ir naršyti internete nepilnamečiai, būtų įdiegtos privalomos, RRT aprobuotos, neigiamą poveikį nepilnamečių vystymuisi darančios informacijos filtravimo priemonės<sup>08</sup>. RRT, įvertinusi prieigos paslaugų teikėjų rizikingumą ir poveikį, prioritetą skiria tiems viešųjų kompiuterių tinklų (internetu) taškams (nepilnamečių ugdymo įstaigų bibliotekoms, informacinių technologijų kabinetams, viešųjų bibliotekų skaitykloms ir kt.), kur gali lankytis ir internete naršyti išskirtinai didelis skaičius nepilnamečių.

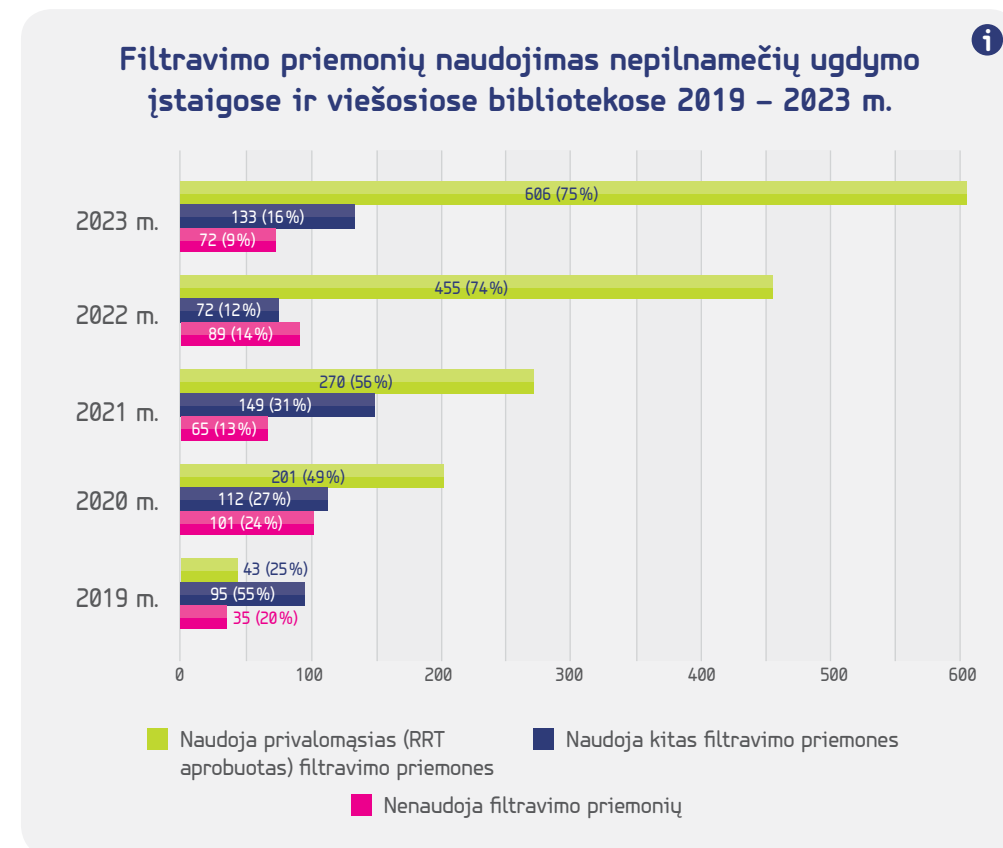
2023 m. RRT, įgyvendindama minėtais teisės aktais pavestas priežiūros funkcijas, apėmė 11 mokyklų, įvertino naudojamas turinio filtravimo priemones, o jų neturinčias skatino diegti ir naudoti privalomas filtravimo priemones. Taip pat atliko kasmetinę apklausą apie privalomų filtravimo priemonių (toliau – aprobuotos filtravimo priemonės) naudojimą nepilnamečių ugdymo įstaigose ir viešosiose bibliotekose (toliau – apklausa). Norėdama gauti kuo tikslesnę informaciją apie kie-

kvienos nepilnamečių ugdymo įstaigos ir viešosios bibliotekos (toliau kartu – įstaigos) naudojamas filtravimo priemones, 2023 m. sudarė įstaigų adresų žemėlapi bei komunikavo su kiekviena iš jų tiesiogiai. Tai lėmė, kad 2023 m. gauta 811 atsakymų, t. y. 24 proc. atsakymų daugiau nei 2022 m. – 616 (žr. **4 pav.**). Pažymėtina, kad aprobuotas filtravimo priemones naudojančių įstaigų, dalyvavusių apklausoje, dalis išlieka stabili – 75 proc. (2022 m. – 74 proc.), nenaudojančių jokių filtravimo priemonių dalis 2023 m. sumažėjo 5 proc. punktais ir sudarė 9 proc. (2022 m. – 14 proc.), o 16 proc. įstaigų naudojo netinkamas (RRT nepatiktintas) turinio filtravimo priemones, jų dalis padidėjo 4 proc. punktais (2022 m. – 12 proc.) (žr. **5 pav.**).



## &lt; 4 pav.

Mokyklų ir bibliotekų dalyvavimas RRT apklausose dėl turinio filtravimo priemonių naudojimo 2019–2023 m. (šaltinis – RRT)



## &lt; 5 pav.

Filtravimo priemonių naudojimas nepilnamečių ugdymo įstaigose ir viešosiose bibliotekose 2019–2023 m. (šaltinis – RRT)

RRT, siekdama paspartinti nepilnamečių ugdymo įstaigų įsitraukimą į nepilnamečių apsaugą nuo žalingo interneto turinio bei įsidięti ir naudoti aprobuotas filtravimo priemones, pasitelkė ir naujas priemones – edukacinius vizitus-patikrinimus. 2023 m. aplankė 11 mokyklų Vilniaus ir Alytaus apskrityse. Susitikimuose RRT specialistai akcentavo aprobuotų filtravimo priemonių naudojimo svarbą bei priminė apie pareigą jas įsidięti ir naudoti, vertino, ar nepilnamečių ugdymo įstaigos tinkamai ir tinkamomis priemonėmis saugo ugdytinius nuo žalingo interneto turinio, dalijosi realiais aplankyty nepilnamečių ugdymo įstaigų gerosios praktikos pavyzdžiais ir patarimais.

## Vartotojų apsauga nuo žalingų interneto nuorodų, apsimestinių SMS žinučių ir skambučių

RRT 2023 m. įpareigojo<sup>09</sup> interneto paslaugų teikėjus taikyti NKSC sukurtą žalingų interneto nuorodų blokavimo įrankį – DNS užkardą. DNS užkarda blokuoja NKSC žinomus žalingus interneto resursus: interneto svetaines, skirtas duomenims vilioti, nesąžiningai prekybai, kenkimo programiniam kodui platinti, užvaldytas svetaines ir teismo sprendimu blokuojamas svetaines. Vadinas, net ir paspaudęs ant sukčių atsiųstos nuorodos, naudotojas nepatirs žalos, nes kenkimo adresas bus blokuojamas, o naudotojas bus apie tai informuotas.

Priimdama naujas ir tobulindama kitas galiojančias teisinės normas, RRT 2023 m. įteisino sukčiavimo apgaulingais skambučiais ir SMS žinutėmis užkardymo priemones. RRT įpareigojo<sup>10</sup> operatorius aptikti ir blokuoti skambučius iš užsienio su lietuviškais numeriais.

## RRT paskirta kvalifikuotos elektroninės atpažinties paslaugos teikėjų priežiūros įstaiga

2023 m. gegužę priėmus Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo pakeitimus<sup>11</sup>, RRT nuo 2024 m. paskiriama kvalifikuotos elektroninės atpažinties paslaugos teikėjų priežiūros įstaiga. Įstatymu nustatytas elektroninės atpažinties paslaugos teikėjų priežiūros modelis ir įpareigojimas RRT priimti atitinkamus teisės aktus. RRT 2023 m. gruodį patvirtino Kvalifikuotos elektroninės atpažinties priemonės išdavimo paslaugos teikimo priežiūros tvarkos aprašą ir Elektroninės atpažinties priemonių, naudojamų teikiant elektronines paslaugas, saugumo užtikrinimo lygio pasirinkimo gaires<sup>12</sup> ir Pranešimų apie patikimumo užtikrinimo paslaugų ir prižiūrimų elektroninės atpažinties priemonių saugumo ir (ar) vientisumo pažeidimus pateikimo tvarkos aprašą<sup>13</sup>. Priklausomai nuo elektroninės atpažinties priemonės išdavimo procedūrų, techninių ir saugumo aspektų, elektroninės atpažinties priemonei pagal Europos Sąjungos teisinį reguliavimą galės būti priskirtas tam tikras saugumo užtikrinimo lygis: žemas, pakankamas arba aukštas. Aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonės bus visiškai patikimos ir su tokia priemone fiziniai asmenys galės gauti ypač svarbias viešąsias ir (arba) administracines paslaugas, pavyzdžiui, naudotis europinės skaitmeninės tapatybės deklės *eWallet* aplikacija. Siekiant aukšto saugumo ir patikimumo lygio, europinės skaitmeninės tapatybės deklės turės atitikti joms taikomus kibernetinio saugumo reikalavimus, kad būtų užtikrinta saugi palengvinta prieiga prie viešųjų ir privačiųjų paslaugų.

09

Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos 2023 m. birželio 2 d. nutarimas Nr. TN-249, „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. spalio 10 d. įsakymo Nr. 1V-960 „Dėl Prieigos, įskaitant tinklų sujungimą, suteikimo ir teikimo taisyklių patvirtinimo“ pakeitimo“. Prieiga per internetą <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/4d314b42017d11eebc0bd16e3a4d3b97?jfwid=exao1xgmp>.

10

Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos 2023 m. liepos 27 d. nutarimas Nr. TN-347 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos 2011 m. spalio 10 d. nutarimo Nr. 1V-960 „Dėl Prieigos, įskaitant tinklų sujungimą, suteikimo ir teikimo taisyklių patvirtinimo“ pakeitimo“. Prieiga per internetą <https://www.e-tar.lt/portal/lt/legalAct/37d1cd002c7b11ee9de9e7e0fd363afc>.

11

Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo Nr. XIII-1120 1, 2, 3, 12, 13, 16, 17, 18 straipsnių ir priedo pakeitimo ir įstatymo papildymo 4-1, 4-2 straipsniais, V-1, V-2 skyriais įstatymas. Prieiga per internetą <https://www.e-tar.lt/portal/lt/legalAct/e45846b0f96f11ed9978886e85107ab2>.

12

Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos 2023 m. gruodžio 21 d. nutarimas Nr. TN-709 „Dėl Kvalifikuotos elektroninės atpažinties priemonės išdavimo paslaugos teikimo priežiūros tvarkos aprašo ir Elektroninės atpažinties priemonių, naudojamų teikiant elektronines paslaugas, saugumo užtikrinimo lygio pasirinkimo gairių patvirtinimo“. Prieiga per internetą <https://www.e-tar.lt/portal/lt/legalAct/eabf89d0a0b511eea5a28c81c82193a8>.

13

Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos 2023 m. gruodžio 21 d. nutarimas Nr. TN-708 „Dėl Pranešimų apie patikimumo užtikrinimo paslaugų ir prižiūrimų elektroninės atpažinties priemonių saugumo ir (ar) vientisumo pažeidimus pateikimo tvarkos aprašo patvirtinimo“. Prieiga per internetą <https://e-tar.lt/portal/lt/legalAct/cb09dcd0a0b511eea5a28c81c82193a8>.

## Edukacinė veikla

RRT, siekdama didesnio interneto naudotojų sąmoningumo, 2023 m. vykdė papildomą interneto naudotojų švietėjišką veiklą, vedė pamokas mokiniams apie saugų elgesį socialiniuose tinkluose, organizavo susitikimus ir praktines dirbtuves Lietuvos pensininkams.

### RRT:

- ✓ dalyvavo projekte „Vilnius yra mokykla“ – vedė 10 pamokų moksleiviams apie saugų internetą ir telekomunikacijas (daugiau nei 300 mokinių);
- ✓ inicijavo projektą „Nė vienas nėra pamirštas“ – gruodį Klaipėdoje pensininkams surengė dirbtuves, kuriose buvo supažindinama su saugiu elgesiu internete, elektroniniu parašu ir vartotojų teisėmis (150 dalyvių). Projektas bus vykdomas ir 2024 m. Iš viso planuojama surengti 20 dirbtuvių Trečiojo amžiaus universiteto klausytojams visoje Lietuvoje.
- ✓ su projekto „Saugesnis internetas“ partneriais<sup>14</sup> surengė konferenciją „VAIKAS+EKRA-NAS+MOKYKLA=?“, skirtą EK inicijuotai ir remiamai, jau 20-metį skaičiuojančiai Saugesnio interneto diena paminėti. Ši diena įvairiais renginiais pažymima visame pasaulyje, siekiant atkreipti visuomenės dėmesį į aktualius skaitmeninius iššūkius, skatinant saugesnį, ypač vaikų ir jaunuolių, naudojimąsi internetu ir skaitmeninėmis technologijomis.



- ✓ RRT taip pat administruoja interneto svetainę ([www.esaugumas.lt](http://www.esaugumas.lt)), kurioje interneto naudotojams teikia aktualią ir nuolat atnaujinamą informaciją, kaip saugiai elgtis socialiniuose tinkluose, pataria, kaip tinkamai pasirinkti antivirusinę programą, saugiai naudotis viešuoju belaidžiu internetu, elektronine bankininkyste, elektronine prekyba ar apsaugoti savo privatumą internete ir t. t. 2023 m. RRT specialistai socialinių tinklų naudotojams suteikė 401 konsultaciją, t. y. 17 proc. daugiau nei 2022 m. (343). 2023 m. interneto naudotojai dažniausiai susidūrė su socialinių tinklų paskyrų užgrobimu, paskyrų užblokavimu pažeidus socialinių tinklų taisykles, prisijungimo prie paskyros duomenų praradimu. Dažniausias sukčiavimo būdas – kai sukčiai, pasinaudodami interneto tinklo naudotojų patiklumu, iš užgrobto socialinio tinklo draugo paskyros atsiunčia asmeninę žinutę su prašymu atsiųsti savo mobiliojo telefono numerį ir į telefoną gautą skaičių derinį (patvirtinimo kodą). Tada sukčiai nedelsdami pakeičia prisijungimo prie paskyros telefono numerį, el. pašto adresą, slaptažodį ir užgrobia asmeninę paskyrą. Atskirti sukčių žinutes nuo tikrų socialinių tinklų draugų sudėtinga, todėl RRT specialistai pataria socialinių tinklų naudotojams kritiškai mąstyti ir ignoruoti tokio pobūdžio asmenines žinutes, kuriose prašoma atsiųsti asmeninę informaciją ar duomenis.

14

2023 m. RRT toliau dalyvavo 24 mėn. trukmės Europos Komisijos koordinuojamame projekte „Saugesnis internetas“ (angl. *Safer Internet Centre Lithuania: draugiskasinternetas.lt V*). Šis projektas įgyvendinamas kartu su partneriais – Lietuvos mokinių neformaliojo švietimo centru, asociacija „Lengvas į ateitį“ ir VŠĮ „Vaikų linija“.





# Priešiškos informacinės aplinkos apžvalga ir Lietuvos informacinės aplinkos saugumo vertinimas



Kmd. Giedrius Valintėlis,  
LK SKD direktorius

## Vadovo žodis

Informacinis karas vyksta jau 13 metų. Lietuvos kariuomenės Strateginės komunikacijos departamentas kovoja su informacinėmis atakomis iš nedraugiškų šalių ir galima konstatuoti, kad šiame mūšio lauke operacijos vyksta kiekvieną dieną. Mūšio lauke Rusija savo galią stiprina informacinėmis ir psichologinėmis kovos priemonėmis. Jomis siekiama palaužti Lietuvos piliečių tikėjimą savo valstybe, valią gintis, pasitikėjimą NATO ir sumenkinti paramą Ukrainai. Informaciniame kare pasinaudojama visomis mūsų visuomenės silpnosiomis vietomis, siekiama mums primesti priešininko norimus veiksmus ar sprendimus. Tikėtina, kad kiti metai pasižymės dar didesniu informaciniu spaudimu.



### KĄ SAUGO?

- Nacionalinę ir NATO informacinę aplinką.



### NUO KO SAUGO?

- Nuo priešiškų organizacijų ir valstybių vykdomų informacinių operacijų.



### KAIP SAUGO?

- Stebėdama ir vertindama informacinę aplinką.
- Informuodama Lietuvos visuomenę apie priešiškų veikėjų veiksmus.



LIETUVOS KARIUOMENĖS  
STRATEGINĖS KOMUNIKACIJOS  
DEPARTAMENTAS

## 1 Informacinės aplinkos grėsmių tendencijos

Informacinis karas tapo įprastu reiškiniu įvairių krizių laikotarpiu. Priešiškai nusiteikusios valstybės ir nevalstybiniai subjektai naudoja visuomenei nerimą keliančiomis situacijomis ir informaciniu karu savo nacionaliniams ar geopolitiniais interesams ir strateginiam pranašumui įgyti.

2023 m. tęsiantis Rusijos karinei invazijai Ukrainoje, pavojų skaičius Lietuvos informacinėje erdvėje nesumažėjo. 2023 m. ir toliau fiksuota itin agresyvi Rusijos ir Baltarusijos retorika NATO atžvilgiu. Nuolat buvo palaikoma komunikacinė linija, jog pati NATO didina įtampą santykiuose su Rusija, o Aljanso vykdoma politika gali привести prie tiesioginės konfrontacijos. Atkreiptinas dėmesys, kad buvo aktyviau komunuikuota apie tai, kad NATO yra nepajėgi, silpna ir pralaimėtų prieš Rusiją kilus karui. 2023 m. išsiskyrė aktyviu idėjų kalvių. Vakarų analitinių centrų vertinimų pertransliavimu Rusijos informacinėje erdvėje. Visais atvejais šie vertinimai būdavo pateikiami iškreipiant kontekstą, jais stipriai manipuluota. Pavyzdžiui, kurtas įspūdis, kad akademinė Vakarų bendruomenė supranta Rusijos galią ir yra įsitikinusi, jog NATO nėra pasirengusi tiesioginiam karui.

Pažymėtina, kad Kinijos propagandinės informacijos prieš Lietuvą sklaida, kaip ir 2022 m., 2023 m. nepakito. Šalį valdantis komunistų režimas labiau orientavosi į informacinę konfrontaciją su NATO.

Vykdam 2023 m. Lietuvos informacinės aplinkos vertinimą, LK SKD stebėseną buvo perorientuota išskirtinai į gynybos srities stebėjimą. Suvokiant Rusijos informacinio karo principus, stebėtos atakos gynybos temomis per kitas – **užsienio politikos** bei **konstitucinių šalies pagrindų** – temas.

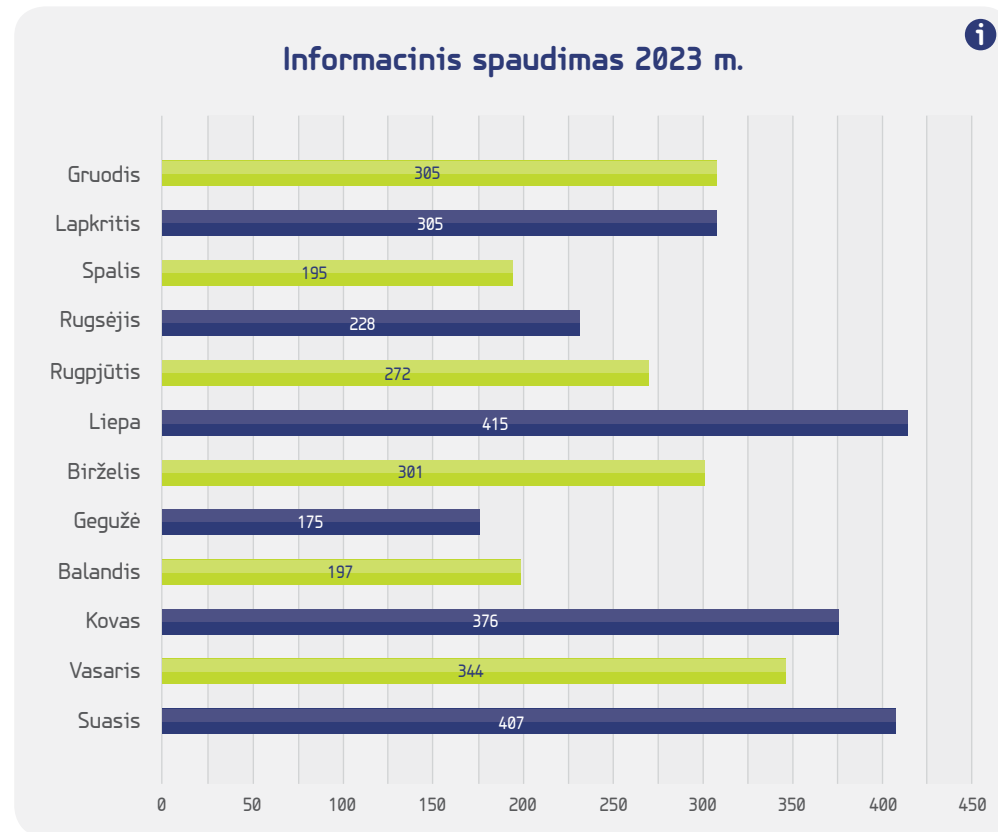
2023 m. fiksuotas bendras priešiškos informacinės veiklos atvejų skaičius sudarė daugiau nei 3 500 unikalių informacinių atvejų. Informacinis spaudimas Lietuvai svyravo tarp vidutinio ir didelio (žr. **1 pav.**). Rusijai naudojant informacines priemones savo galios įvaizdžiui Vakaruose stiprinti, Kremlius ir jo remiami informaciniai kanalai suintensyvindavo manipuliacinių bei grasinamojo pobūdžio žinučių Vakarams skleidimą po ryškesnių 2023 m. politikos įvykių: po V. Putino pranešimo apie branduolinio ginklo dislokavimą Baltarusijoje kovo mėnesį, Ukrainos Kachovkos užtvankos susprogdinimo birželį, Krymo tilto susprogdinimo liepą ir per Ribentropo-Molotovo pakto metinės rugpjūtį. Per NATO viršūnių susitikimą Vilniuje buvo fiksuotas didžiausias informacinis spaudimas. Priešiška informacinė erdvė buvo intensyviai ruošiamą dar iš anksto, o diena prieš bei antroji susitikimo diena pasižymėjo didžiausiu incidentų skaičiumi per visus 2023 m. – tada informacinis spaudimas išaugo 3-4 kartus, palyginti su vidutiniu atvejų skaičiumi per dieną.

0100  
11011  
01011



1 pav. >

Informacinis spaudimas  
2023 m. (šaltinis – LK SKD)



## Fiksuoti informaciniai incidentai gynybos srityje

2022 m. Rusijai pradėjus invaziją į Ukrainą, gynybos sričiai buvo skirtas didžiausias Rusijos ir Baltarusijos režimų valdomos žiniasklaidos dėmesys nuo 2017 m. 2023 m. gynybos srities pagrindiniai dezinformacijos taikiniai Lietuvoje:

- ⚠ NATO;
- ⚠ NATO pajėgumų stiprinimas;
- ⚠ Lietuvos narystė NATO;
- ⚠ Lietuvos kariuomenė;
- ⚠ Lietuvos kariniai pajėgumai;
- ⚠ Lietuvos kariuomenės modernizacija;
- ⚠ Lietuvos kariuomenės finansavimas;
- ⚠ Vokietijos brigada Lietuvoje;
- ⚠ parama Ukrainai;
- ⚠ Didžiojo etmono Konstantino Ostrogiškio brigada (toliau – LITPOLUKRBRIG)<sup>01</sup>.

Rusijos ir Baltarusijos skleidžiamos karinės propagandos retorika buvo agresyvi, tikslingai siekta formuoti Rusijos ir Baltarusijos, Baltijos šalių ir Vakarų tikslinių auditorijų nuomonę bei ją manipuluoti. Išskirtinis dėmesys 2023 m. priešiškoje informacinėje erdvėje skirtas Lietuvos kariuomenės modernizavimui ir infrastruktūros plėtrai. Skleista dezinformacija, kad perkamos ginkluotės ir technikos nepakaks apsiginti nuo Rusijos, o pinigai yra tiesiog švaistomi.

01

LITPOLUKRBRIG – Lietuvos, Lenkijos ir Ukrainos bendras karinis mokomasis vienetas, įsteigtas 2014 m. rugsėjo 19 d. Varšuvoje. Fiksuota nuo 2023 m. balandžio mėnesio iki liepos 21 d. vykdyta informacinė operacija prieš LITPOLUKRBRIG. Skleista dezinformacija, kad NATO viršūnių susitikime bus nuspręsta siųsti LITPOLUKRBRIG į Ukrainą, o šios idėjos sumanytojos – Lietuva ir Lenkija – yra agresyvios, į karą įsitraukti siekiančios valstybės.



## Populiariausi Rusijos ir Baltarusijos naratyvai gynybos srityje 2023 m.:

- ⚠ Lietuvos kariuomenė nepajėgi pasipriešinti Rusijai;
- ⚠ Lietuva ir NATO provokuoja Rusiją ir Baltarusiją pratybomis savo teritorijoje;
- ⚠ NATO karo atveju negins Lietuvos;
- ⚠ NATO pasinaudos Lietuva karui prieš Rusiją;
- ⚠ NATO yra agresyvus, puolantis karinis blokas;
- ⚠ NATO kariauja su Rusija Ukrainos rankomis;
- ⚠ NATO yra nepasiruošusi karui su Rusija;
- ⚠ NATO yra žlunganti organizacija;
- ⚠ Vokietijos brigada Lietuvoje kelia grėsmę Rusijai;
- ⚠ Lietuva yra okupuota Vokietijos ir Amerikos karių;
- ⚠ NATO viršūnių susitikimas yra nepavykęs.

Skleidžiamos priešiškos informacijos srautas 2023 m. išsiskyrė kaltinimais neva Lietuva bei NATO provokuoja Rusiją ir Baltarusiją, taip pat mūsų šalis su NATO buvo kaltinama siekiu pulti šias valstybes.

## Fiksuoti informaciniai incidentai užsienio politikos srityje

2023 m. užsienio politikos sektorius išliko vienas iš pagrindinių priešiškų informacinių veikėjų taikinių, tačiau informacinis spaudimas šiam sektoriui santykinai sumažėjo 2023 m., šoktelėjus gynybos atvejų skaičiui. 2023 m. užsienio politikos srities pagrindiniai dezinformacijos taikiniai Lietuvoje:

- ⚠ Lietuvos ir Rusijos santykiai;
- ⚠ Lietuvos ir Baltarusijos santykiai;
- ⚠ ES;
- ⚠ Lietuvos narystė ES;
- ⚠ Lietuvos ir JAV santykiai;
- ⚠ Lietuvos ir Ukrainos santykiai;
- ⚠ Baltijos šalių tarpusavio santykiai.

Priešiški informaciniai veikėjai itin aktyviai išnaudojo Lietuvos kaip NATO ir Europos Sąjungos „vasalės“ temą, t. y. siekta pavaizduoti Lietuvą kaip valstybę, neturinčią veikimo ir apsisprendimo teisės, teigiant, kad bet kokie sprendimai yra ne pačios Lietuvos, o „Vakarų šeimininkų“.





## Fiksuoti informaciniai incidentai konstitucinių pagrindų apsaugos srityje

2023 m. priešiškoje informacinėje erdvėje bandyta kurstyti tautinę nesantaiką tarp lietuvių ir ukrainiečių, didinti įtampą per Lietuvos visuomenės rengiamas Ukrainos palaikymo akcijas. Rusijos režimas žiniasklaidoje Lietuvą siekė vaizduoti kaip antirusišką valstybę.

## Išvados

2024 m. pasižymės didesniu informaciniu spaudimu nei 2023 m. 2024 m. rekordiška daug pasaulio šalių piliečių rinks savo atstovus valdžioje<sup>02</sup>, todėl galima tikėtis dar agresyvesnių dezinformacijos skleidimo akcijų.

Bus ir toliau ypač domimasi pratybomis „Steadfast Defender’24“<sup>03</sup>. Taip pat daug dėmesio bus skiriama visoms NATO šalių pratyboms ir (ar) NATO pajėgumų stiprinimui rytiniame Aljanso flange. Bus nusitaikyta į Vokietijos brigados dislokavimą Lietuvoje, paramą Ukrainai.

02

Nacionaliniai rinkimai 2024 m. vyks Jungtinėse Amerikos Valstijose, Jungtinėje Karalystėje ir Indijoje – trijose didžiausių ekonomikos potencialą turinčiose šalyse, taip pat keliuose šalyse, kurios anksčiau buvo tapusios užsienio kišimosi taikiniu, įskaitant Taivaną ir Moldovą.

03

„Steadfast Defender’24“ yra didžiausios NATO karinės pratybos nuo Šaltojo karo laikų. Prieiga per internetą <https://www.nato.int/cps/en/atohq/222847.htm>.







Išleido Lietuvos Respublikos krašto apsaugos ministerija,  
Totorių g. 25, LT-01121 Vilnius, [www.kam.lt](http://www.kam.lt)  
2024-05-21. Užsakymas Nr. GL-310

Dizaineris Andrej Garbar  
Kalbos redaktorė Inga Šorienė  
Naudotos iliustracijos iš [Freepik.com](http://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.



**NACIONALINĖ  
KIBERNETINIO  
SAUGUMO BŪKLĖS  
ATASKAITA**

**2023**