KRAŠTO APSAUGOS MINISTERIJA

# LIETUVOS KIBERNETINIO SAUGUMO BŪKLĖS APŽVALGA: SVARBIAUSIA INFORMACIJA

## 2024

Viršelis sukurtas naudojant dirbtinį intelektą

# LIETUVOS KIBERNETINIO SAUGUMO BŪKLĖS APŽVALGA: SVARBIAUSIA INFORMACIJA

2024

KRAŠTO APSAUGOS MINISTERIJA

# 01

# Įžanga

**Dovilė Šakalienė,**
**krašto apsaugos ministrė**

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

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

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

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

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

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

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

# 02

# Esminiai darbai, tendencijos ir statistika

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



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

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

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

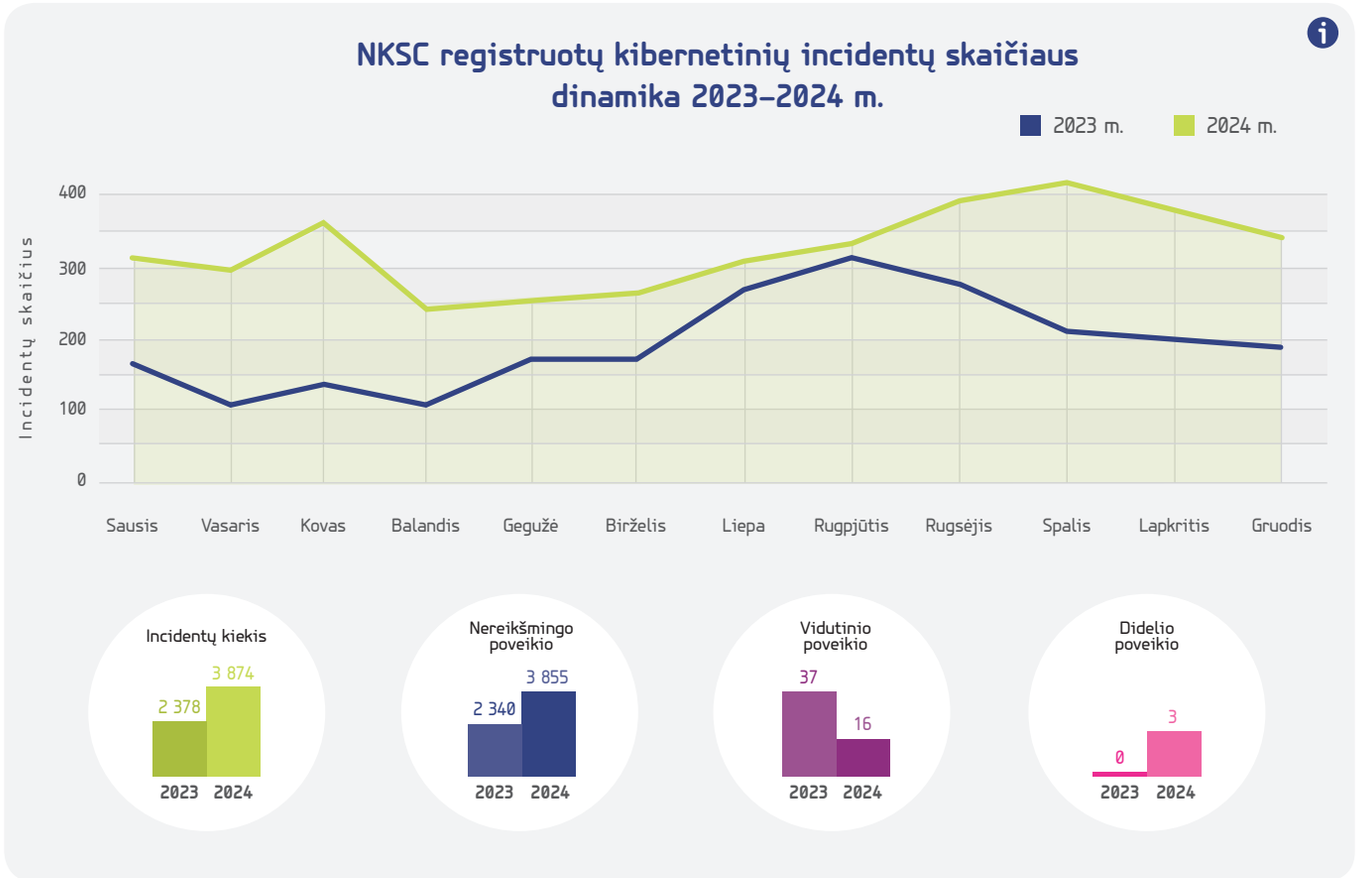
2024 m. buvo užbaigti visi LK KGV steigimo darbai, būtini Lietuvos kariuomenės gebėjimams kibernetinėje erdvėje stiprinti, ryšių ir informacinėms sistemoms (toliau – RIS) saugoti ir jų sąveikai su NATO užtikrinti. Naujos struktūros kariuomenė veiklą pradėjo 2025 m. sausio 1 d.

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

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

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

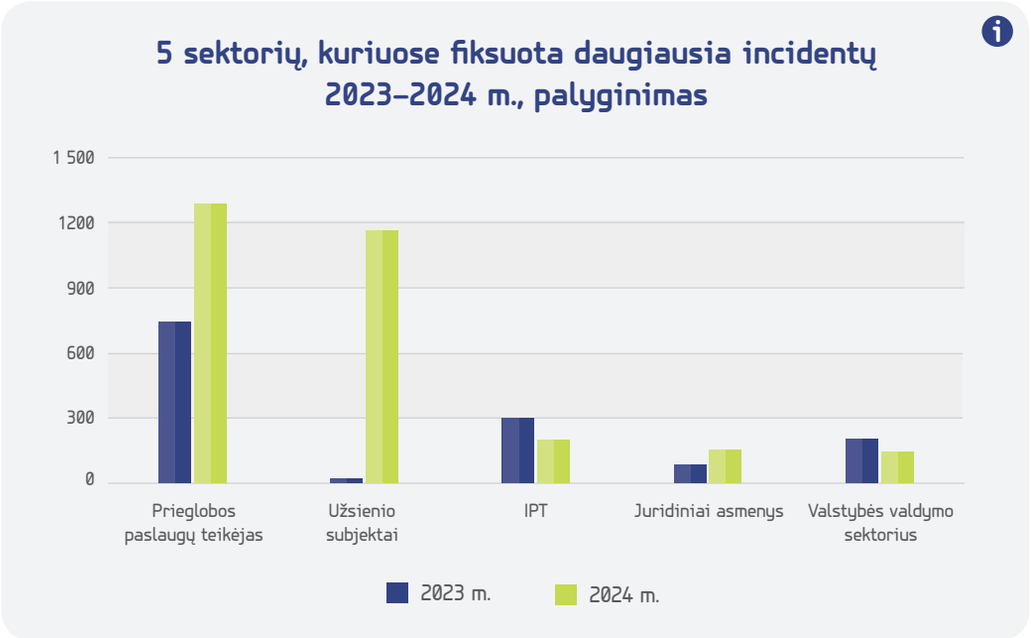
2024 m. NKSC iš viso užregistravo 3 874 kibernetinius incidentus, t. y. apie 63 proc. daugiau nei ankstesniais metais (2023 m. - 2 378). Dauguma jų buvo priskirti nereikšmingai ir vidutinei kategorijoms, o 3 kibernetiniai incidentai - didelei kategorijai (2023 m. tokių incidentų nebuvo).




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

Pastarosios kategorijos incidentai siejami su užsienio šalių remiamomis grupuotėmis, kurios įsilaužusios į organizacijų tinklus siekia ilgalaikių tikslų - šnipinėjimas vienas jų. NKSC vertinimu, nors 2024 m. fiksuota incidentų skaičiaus dinamika daugiausia susijusi su gerėjančiais visuomenės pranešimo apie kibernetinius incidentus įpročiais, vis dėlto piktavalių socialinės inžinerijos metodų taikymas siekiant išvilioti jautrią informaciją yra pagrindinė kibernetinių incidentų Lietuvoje priežastis. Pažymėtina, kad 2024 m. šio tipo incidentai sudarė net 59 proc. visų NKSC registruotų incidentų (2023 m. - 38 proc.).

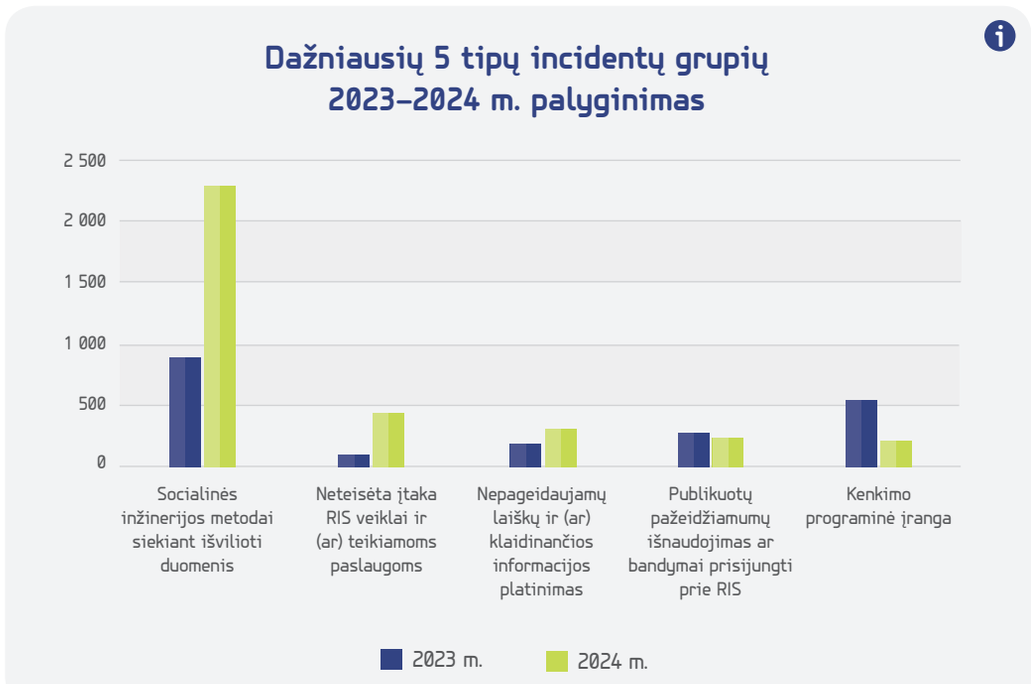
Daugiausia incidentų įvyko interneto prieglobos paslaugų infrastruktūroje (angl. *hosting*), užsienio subjektų sektoriuje ir interneto paslaugų teikėjų (toliau - IPT) infrastruktūroje. Tiek 2023 m., tiek ir 2024 m. interneto prieglobos paslaugų infrastruktūra ir toliau pirmauja pagal joje fiksuotų incidentų skaičių.




**< 2 pav.**

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

Šiame sektoriuje matoma itin sparti incidentų skaičiaus didėjimo tendencija – incidentų padidėjo net 74 proc. Didžiausią žalą organizacijoms ir gyventojams darė incidentai, priskiriami socialinei inžinerijai, antroje vietoje fiksuota sparčiai didėjusi neteisėta įtaka RIS veiklai ir (ar) teikiamoms paslaugoms (2023 m. – 116; 2024 m. – 444), o trečioje vietoje – nepageidaujamų laiškų ir (ar) klaidinančios informacijos platinimas (2023 m. – 200; 2024 m. – 318). Daug metų buvę vienais dažniausių kibernetinių incidentų, susijusių su kenkimo programinės įrangos platinimu, 2024 m. šie incidentai atsidūrė penktoje vietoje (2023 m. – 554; 2024 m. – 223).




**< 3 pav.**

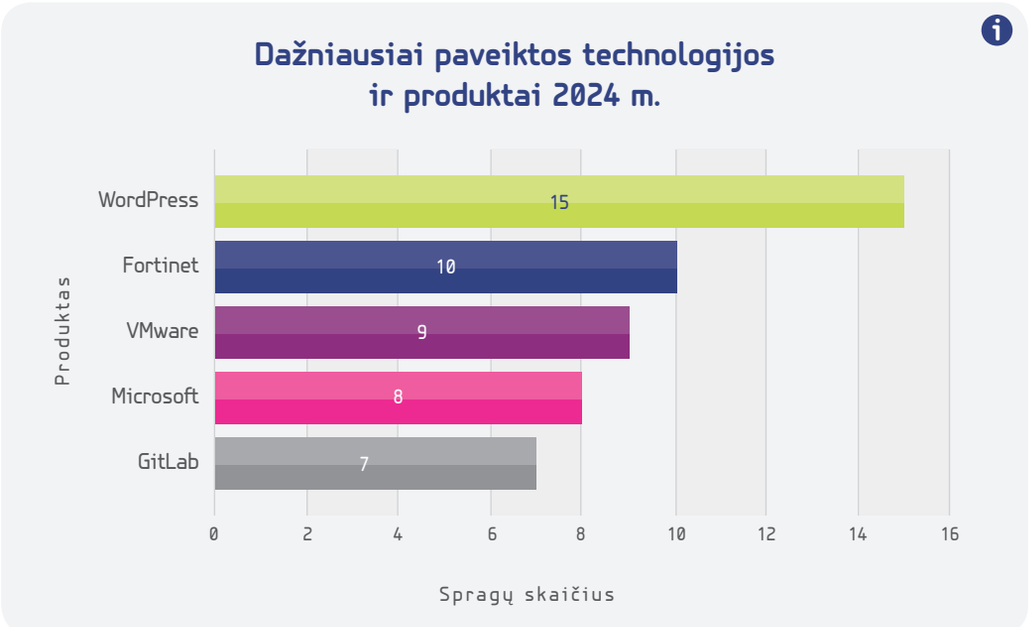
Dažniausių 5 tipų incidentų grupių 2023–2024 m. palyginimas (*šaltinis – NKSC*)

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

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

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

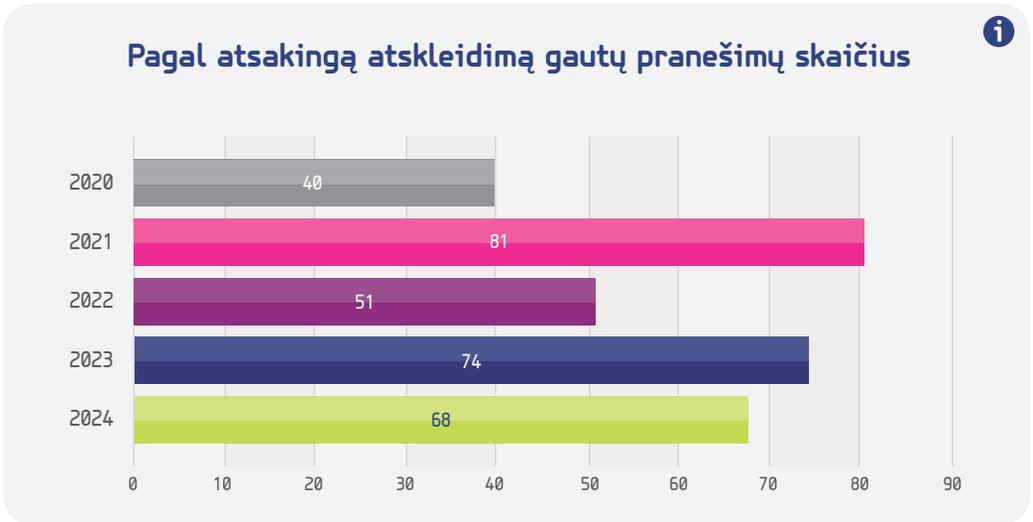
**4 pav. >**
Dažniausiai paveiktos technologijos ir produktai 2024 m. *(šaltinis – NKSC)*




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

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

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




**< 5 pav.**

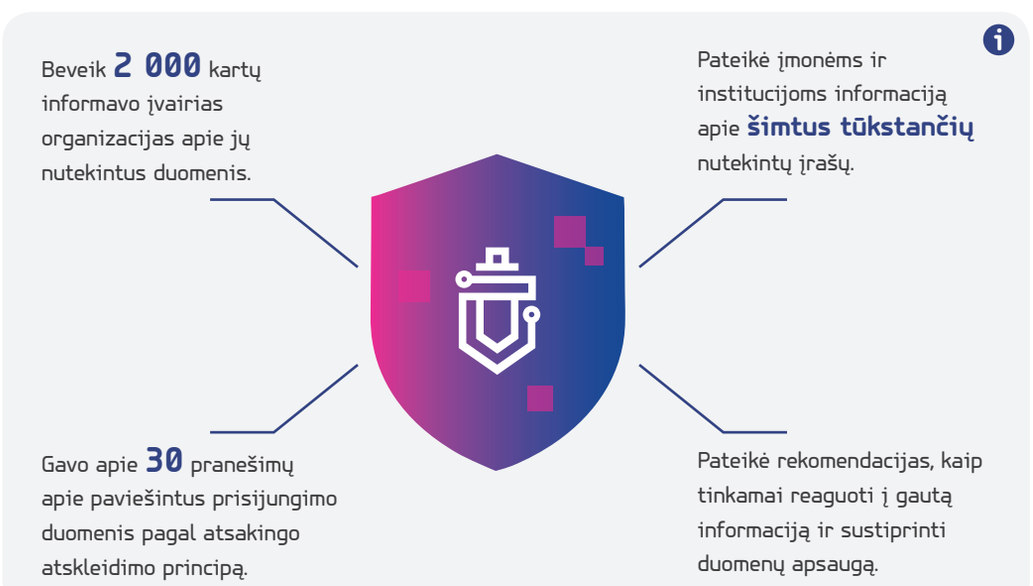
Pagal atsakingą atskleidimą gautų pranešimų skaičius (2020–2024 m.)
(*šaltinis – NKSC*)

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

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

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

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



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

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

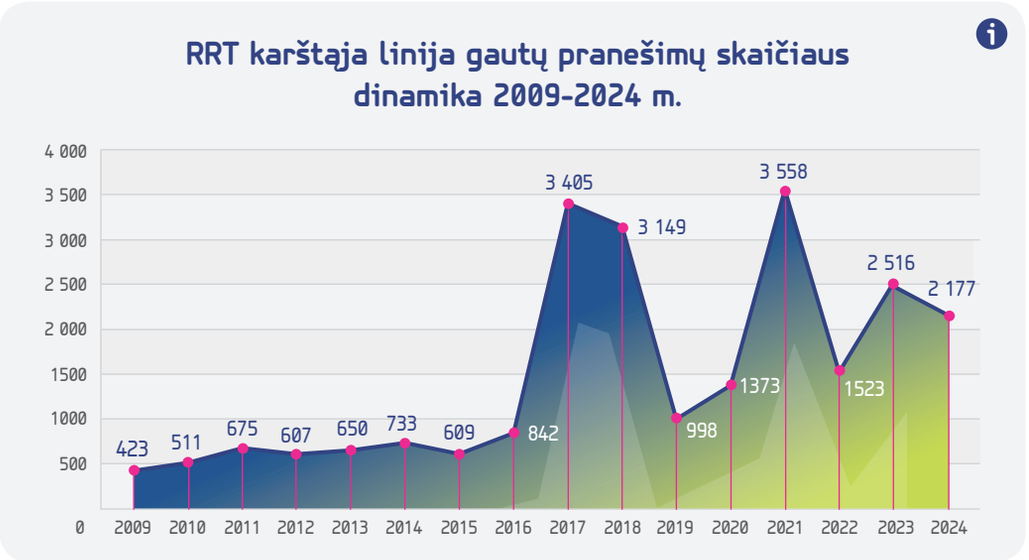
RRT

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

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

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

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




**< 6 pav.**

RRT karštąja linija gautų pranešimų dinamika 2009–2024 m. (*šaltinis – RRT*)

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

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

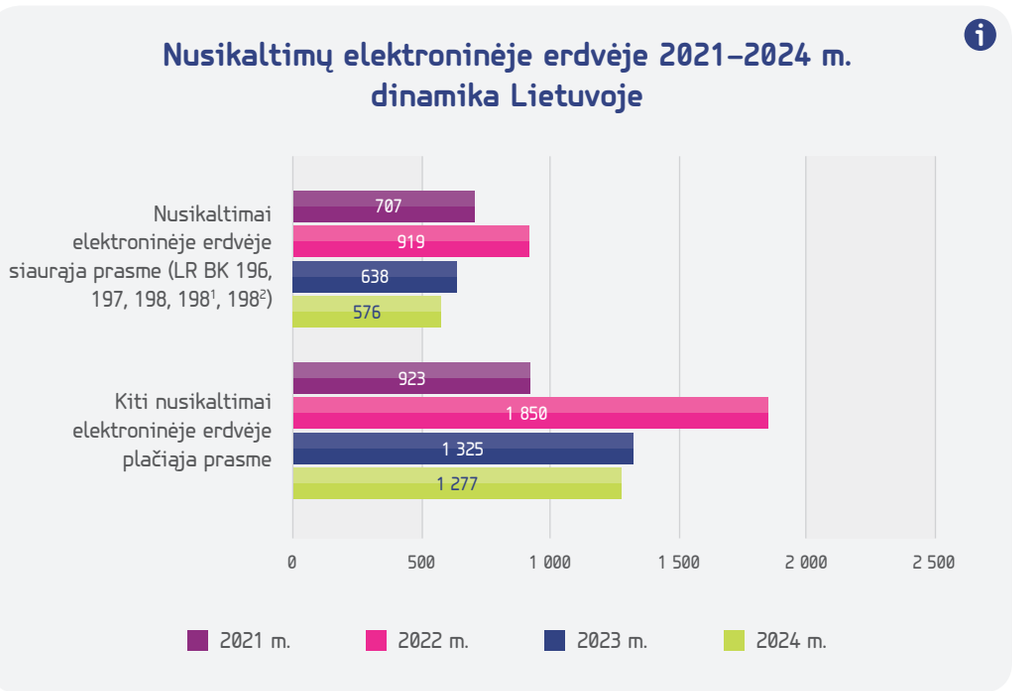
RRT aktyviai dalyvauja ES vystomo palydovinio ryšio projekto „Atsparumo, sujungiamumo ir saugumo palydoviniu ryšiu infrastruktūra“ (angl. *Infrastructure for Resilience, Interconnectivity and Security by Satellite* (IRIS²)) (toliau – IRIS²) techninėje ir vartotojų darbo grupių veikloje ir kitų tarptautinių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

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

2024 m. Lietuvoje užregistruotos 3 966 nusikalstamos veikos elektroninėje erdvėje. Nors šis skaičius vos didesnis nei 2023 m. (3 912), šių nusikalstamų veikų grėsmės lygis išliko nepakitęs ir neturėjo įtakos 2024 m. registruoto nusikalstamumo augimui. Kaip ir pernai, ypač sumažėjo nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui, kurie kvalifikuojami pagal Lietuvos Respublikos baudžiamojo kodekso (toliau – LR BK) 196-198[2] str. Pavyzdžiui, neteisėto poveikio elektroniniams duomenims, informacinei sistemai, neteisėto prisijungimo prie informacinės sistemos atvejų sumažėjo beveik 10 proc.

**7 pav. >**

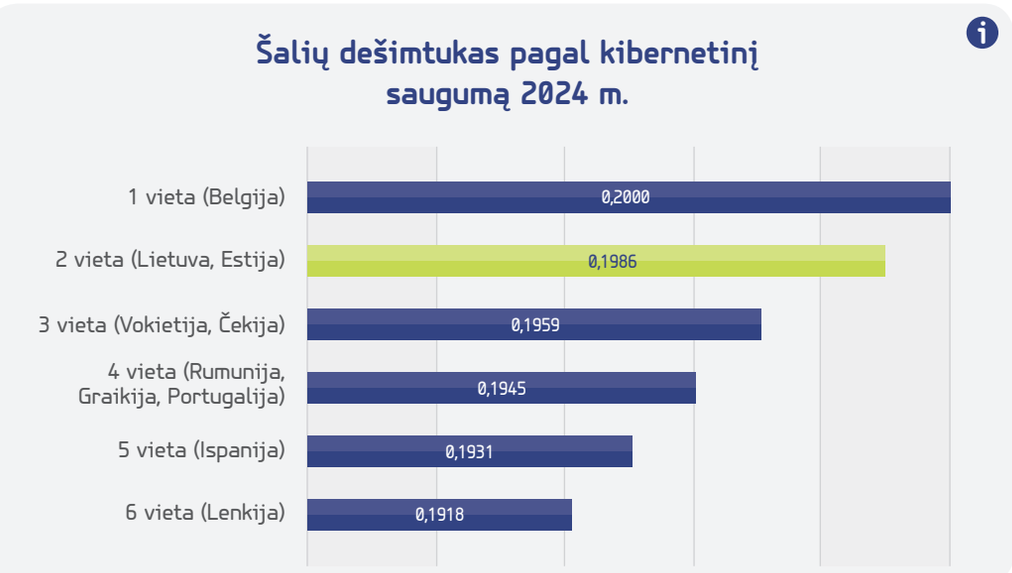
Nusikaltimų elektroninėje erdvėje 2021–2024 m. dinamika Lietuvoje *(šaltinis – Lietuvos policija)*




Šie policijos 2024 m. stebėsenos rezultatai sutampa su nepriklausomų ekspertų išvadomis. Kompanijos „Surfshark" skaitmeninio gyvenimo kokybės indeksas (angl. *Digital Quality of Life Index* (DQL)) rodo, kad Lietuva pagal kibernetinį saugumą 2024 m., kaip ir anksčiau, išliko antrąja šalimi pasaulyje.

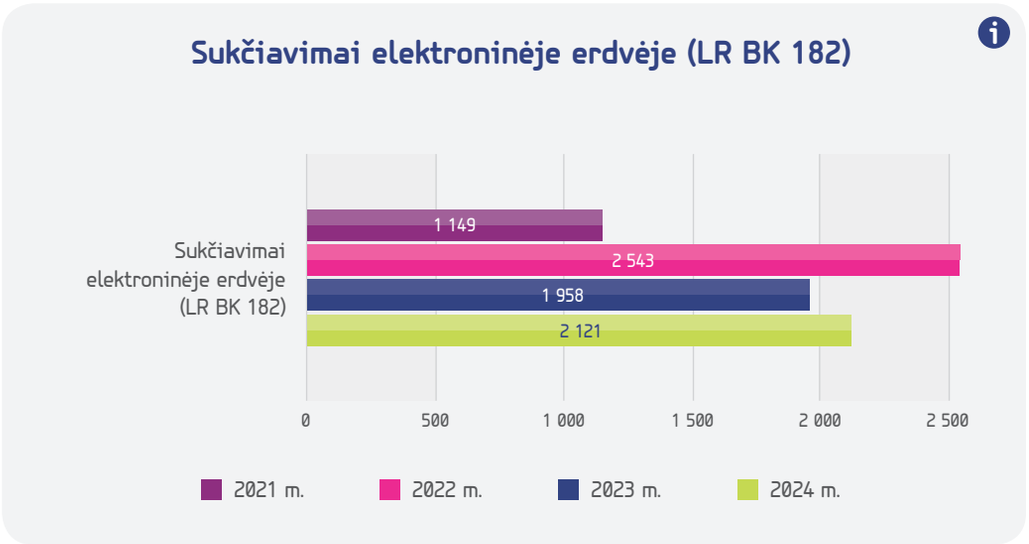
**8 pav. >**

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




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

Esminė problema vis dar lieka sukčiavimo elektroninėje erdvėje atvejai. Jie 2024 m. sudarė didžiąją dalį – 53 proc. – visų elektroninėje erdvėje padarytų nusikalstamų veikų: išankstinio mokėjimo sukčiavimo, investicinio sukčiavimo, sukčiavimo apgaulingais telefoniniais skambučiais, el. laiškais ir žinutėmis.




**< 9 pav.**
Sukčiavimai elektroninėje erdvėje (LR BK 182)
*(šaltinis – Lietuvos policija)*

Apgaulingų telefoninių skambučių atvejų skaičius 2024 m., palyginti su 2023 m., išaugo 64 proc. Skambučiais siekta išvilioti grynuosius pinigus ir (ar) vertybes, naudojant išviliotus elektroninės bankininkystės vartotojų duomenis grobti lėšas iš banko sąskaitų. Policija daro prielaidą, kad tai galėjo lemti efektyvi apgaulingų SMS žinučių kontrolė - nusikaltėliai prisitaikė prie taikomų techninių priemonių ir grįžo prie apgaulingų skambučių.

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

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

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

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

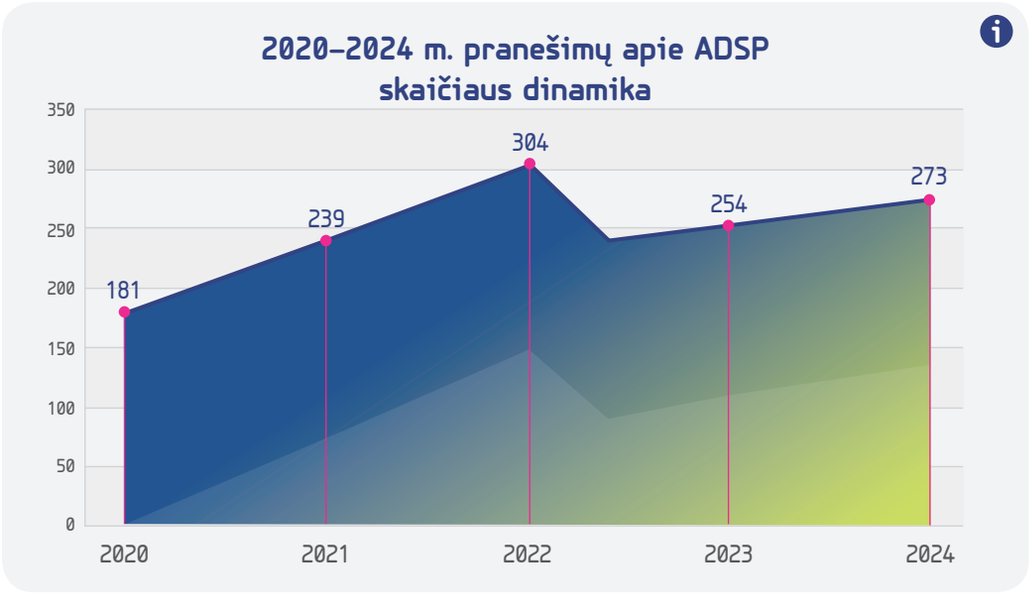
2024 m. Organizuoto nusikalstamumo internete grėsmių vertinimo ataskaitoje (angl. *Internet Organised Crime Threat Assessment* (IOCTA)) (toliau - IOCTA ataskaita) daroma išvada, kad dirbtiniu intelektu (toliau - DI) pagrįstos technologijos daro socialinę inžineriją dar efektyvesnę. Susirūpinimą taip pat kelia ir giliųjų klastočių (angl. *deepfakes*) naudojimas, nes tai toks pat galingas įrankis, kaip ir balso atkartojimas ar klastojimas. Lietuvos policijos atliekamuose tyrimuose nėra nustatyta, kad progresuotų DI naudojimas nusikalstamoms veikoms vykdyti, tačiau kartu su kitomis valstybėmis nagrinėjama potenciali DI įtaka socialinei inžinerijai ir prevencinės priemonės.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

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

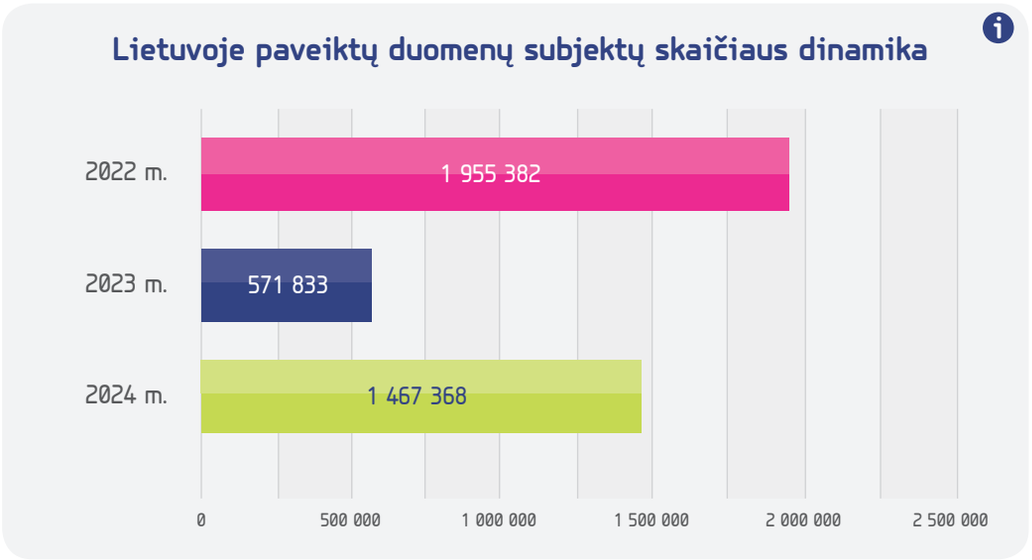
Iš 2024 m. pranešimų apie ADSP Lietuvoje statistikos matyti, kad VDAI gavo 273 pranešimus apie ADSP, t. y. 7 proc. daugiau negu 2023 m. (2023 m. – 254). VDAI pastebi, kad pokytis nėra didelis, todėl negalima daryti prielaidos, kad ADSP skaičius Lietuvoje išaugo.

**10 pav. >**
2020–2024 m. pranešimų apie ADSP skaičiaus dinamika *(šaltinis – VDAI)*



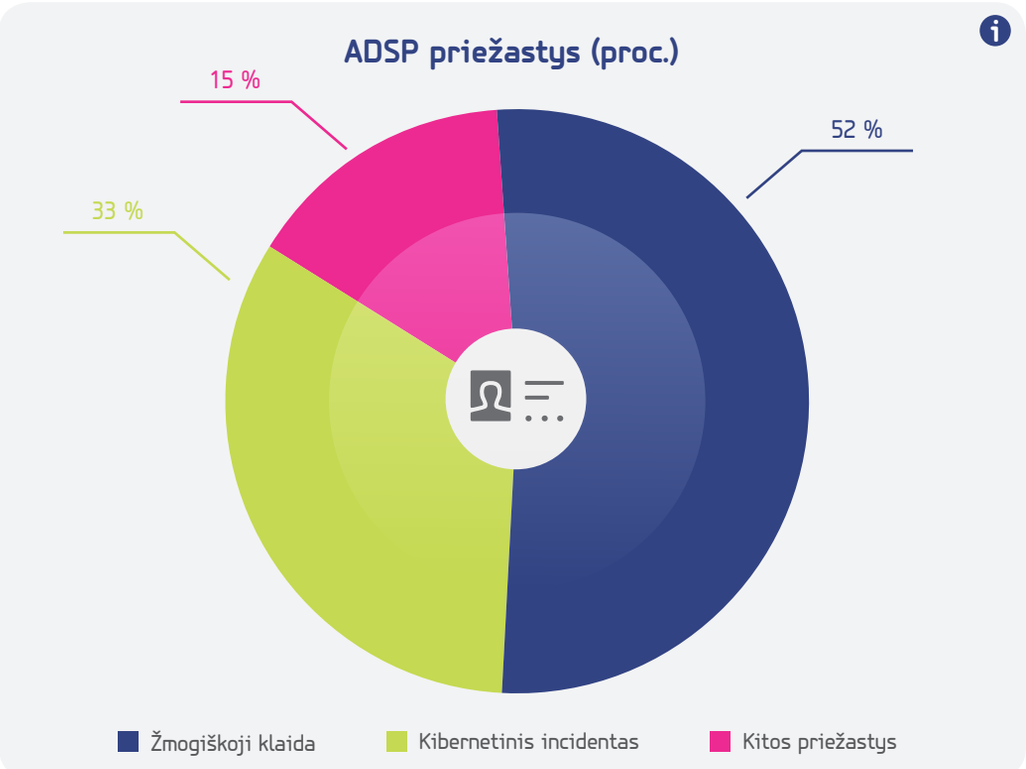

Tačiau 2024 m. beveik 3 kartus padidėjo Lietuvoje paveiktų duomenų subjektų skaičius – 1 467 368 (2023 m. – 571 833). Tai lėmė didesnis ADSP, įvykusių dėl kibernetinių incidentų, skaičius, buvo paveikta daug duomenų subjektų.

**11 pav. >**
Lietuvoje paveiktų duomenų subjektų skaičiaus dinamika *(šaltinis – VDAI)*




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

VDAI, išanalizavusi 2024 m. gautus pranešimus apie ADSP, nustatė, kad 90 (33 proc.) ADSP įvyko dėl kibernetinių incidentų: duomenų užšifravimo ir išpirkos reikalavimo atakų, neteisėtai gautos prieigos prie IT sistemų, socialinės inžinerijos metodais paremtų atakų, prisijungimo duomenų užpildymo kibernetinių atakų ir kt.




**< 12 pav.**
ADSP priežastys (proc.)
*(šaltinis – VDAI)*

2023 m. VDAI gavo tik 37 pranešimus apie ADSP dėl kibernetinių incidentų, t. y. 15 proc. visų 2023 m. gautų pranešimų apie ADSP. Dažniausios kibernetinių incidentų priežastys: perimti naršyklėse išsaugoti prisijungimo duomenys - 27 proc., nepakankamai išmokytas personalas - 18 proc., kelių faktorių autentifikavimo nebuvimas - 10 proc.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# LIETUVOS KIBERNETINIO SAUGUMO BŪKLĖS APŽVALGA: SVARBIAUSIA INFORMACIJA

## 2024

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

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

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

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

ISSN 2783-7009