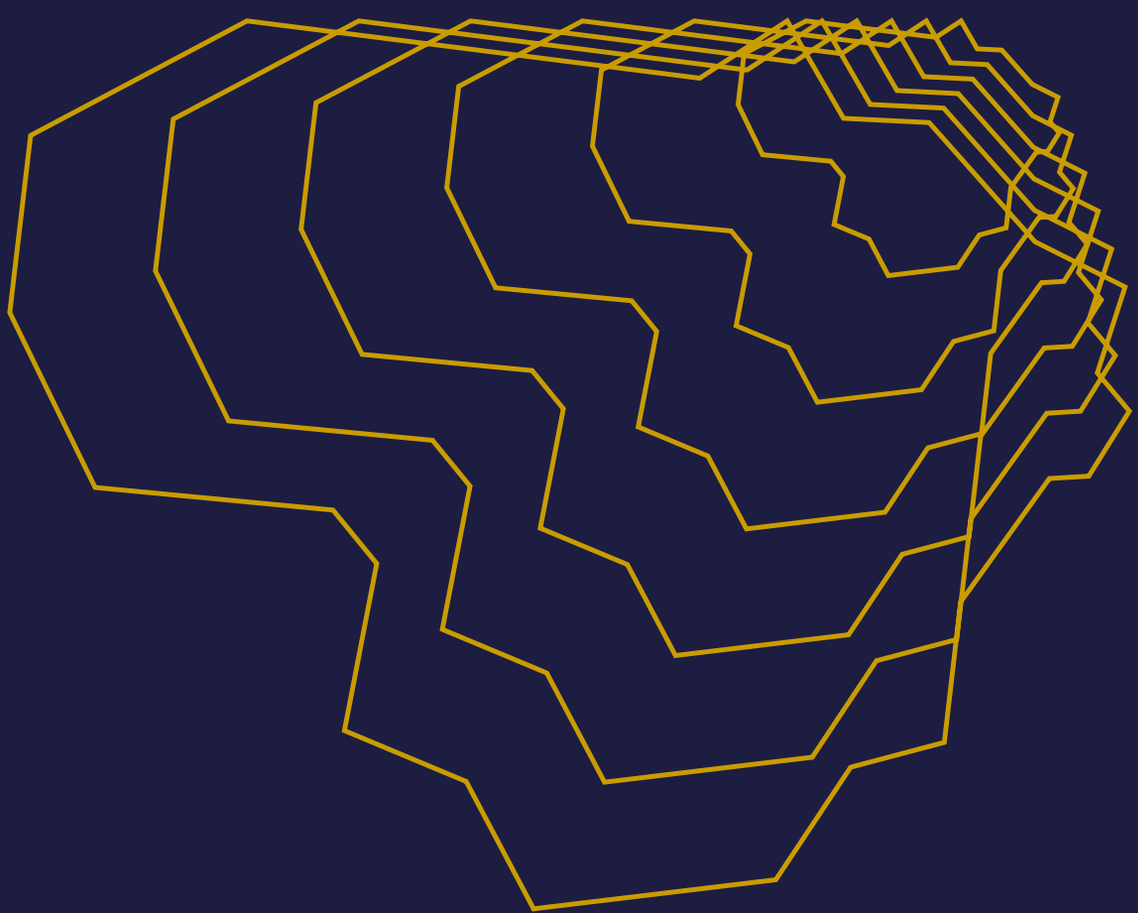
KRAŠTO APSAUGOS
MINISTERIJA

NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA



2025

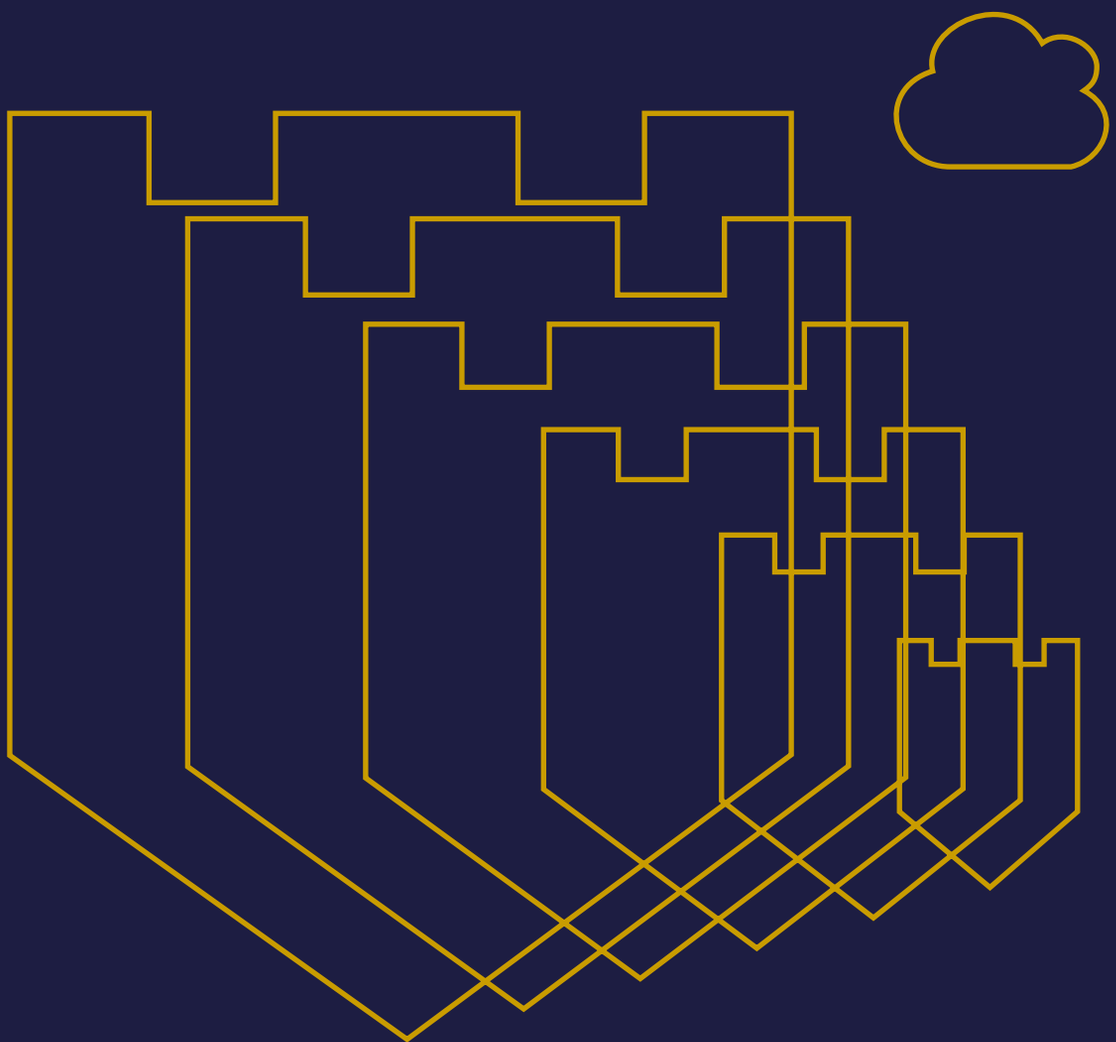
Turinys

Turinys

Turinys

Turinys

01



Įžanga

Robertas Kaunas,
Krašto apsaugos ministras

Įžanginis žodis

Turėdamas ilgametę patirtį IT versle, puikiai suprantu, kad kibernetinė erdvė yra kovos arena. Čia veikia priešiškų valstybių remiamos grupuotės, organizuoti nusikaltėliai ir oportunistiniai piktavaliai. Atakos prieš Lietuvą ir mūsų sąjungininkus nėra atsitiktinės – jos yra kryptingos, nuoseklios ir integruotos į platesnę hibridinio karo strategiją. Atakos prieš kritinę infrastruktūrą, institucijų diskreditavimas ir visuomenės skaldymas vyksta vienu metu skirtingais kanalais.

2025 m. užregistruoti 2 888 kibernetiniai incidentai – 25 proc. mažiau nei 2024 m. Nusikalstamų veikų elektroninėje erdvėje mažėjo 28 proc., jų ištyrimas išaugo 10,5 proc. Tai – teigiami ženklai. Tačiau registruoti skaičiai neatspindi viso vaizdo: dalis incidentų vis dar išlieka nežinomi dėl nesusiformavusios pranešimo kultūros.

Grėsmės vis dažniau nukreiptos ne į pačias sistemas, o į žmones, kurie turi prieigą prie jų. Socialinės inžinerijos pagrindu įvykdyti incidentai sudarė didžiausią dalį visų užregistruotų atvejų. Sukčiavimas išlieka dominuojančiu kibernetiniu nusikaltimu – 44 proc. visų nusikalstamų veikų elektroninėje erdvėje, o finansiniai nuostoliai siekė dešimtis milijonų eurų.

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (NKSC) į grėsmes reaguoja sistemiškai ir dideliu mastu. 2025 m. DNS užkarda suveikdavo vidutiniškai po 50 tūkst. kartų per dieną – beveik penkis kartus daugiau nei 2024 m. Per metus sustabdyta apie 13 mln. apgaulingų skambučių ir beveik 6 mln. suklastotų SMS žinučių.

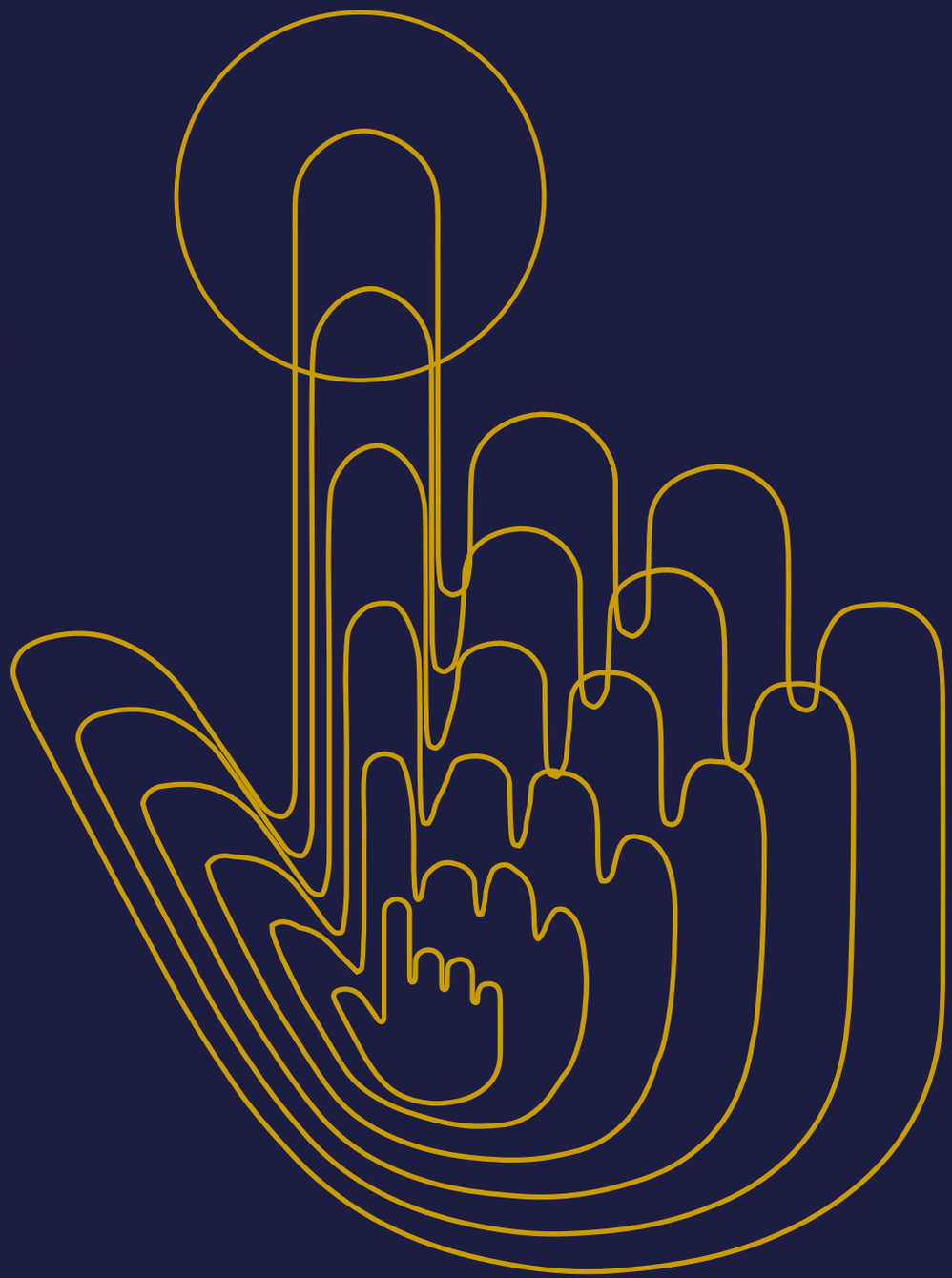
Subjektų, veikiančių ypatingos svarbos ir kituose itin svarbiuose sektoriuose, spragos išlieka rimtu pažeidžiamumo šaltiniu – aplaidus požiūris į saugumą atveria kelius į kritiškai svarbias sistemas. Iš 153 Nacionalinio kibernetinio saugumo centro vertintų informacinių sistemų 64 proc. nustatytos kaip pažeidžiamos. Tai reiškia, kad atsparumo didinimas turi tapti nenutrūkstamu procesu, o ne būti periodine patikra.

Būtent todėl plečiame atsakomybės lauką. Kibernetinio saugumo subjektų registre 2025 m. – 1 443 organizacijos, privalomų reikalavimų taikymo apimtis išaugo keliskart. Kritines paslaugas teikiančios organizacijos pradeda įgyvendinti konkrečius organizacinius ir techninius standartus – tai svarbus žingsnis kasdieniame procese, tačiau nėra savaiminis tikslas.

Dirbtinis intelektas keičia grėsmių matricą greičiau, nei spėjame prisitaikyti. Giliosios klastotės, automatizuotos atakos ir pažangios įsilaužimo priemonės tampa prieinamos visiems. Tai tik dar kartą patvirtina: investicijos į žmogų ir į technologijas yra gyvybiškai svarbios. Nuo šiandien priimamų sprendimų dėl sistemų architektūros, duomenų valdymo ir darbuotojų kompetencijų tiesiogiai priklausys, koks pažeidžiamumų žemėlapis bus rytoj.

Kibernetinis saugumas nėra tik IT klausimas – tai strateginis valstybės valdymo klausimas. Spręskime jį kartu.

02



Santrauka

Santrauka

Kibernetinių grėsmių mastas, greitis ir sudėtingumas šiais laikais keičiasi itin sparčiai – tradiciniai gynybos modeliai nespėja taip greitai prisitaikyti. Dėl technologijų pažangos, dirbtinio intelekto (toliau – DI) plėtros ir didėjančios priklausomybės nuo skaitmeninių paslaugų atsiranda ne tik naujų galimybių, bet ir plečiasi kibernetinių grėsmių atakos paviršius, trumpėja laikas incidentams aptikti ir suvaldyti, o jų poveikis didėja. Todėl nė viena organizacija ar valstybė negali veiksmingai užtikrinti saugumo be partnerių paramos. Kibernetinio atsparumo didinimo sąlyga – valstybės institucijų, verslo, akademinės bendruomenės ir tarptautinių partnerių bendradarbiavimas.

Nacionalinę kibernetinio saugumo būklės ataskaitą parengė Krašto apsaugos ministerija (toliau – KAM) remdamasi 2025 m. sausio 1 d. – gruodžio 31 d. duomenimis ir įžvalgomis, kurias pateikė kibernetinio saugumo ekosistemos partneriai – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), Lietuvos policija, Valstybinė duomenų apsaugos inspekcija (toliau – VDAI), Lietuvos Respublikos ryšių reguliavimo tarnyba (toliau – RRT) ir Lietuvos kariuomenės Strateginės komunikacijos departamentas (toliau – LK SKD). Ataskaitoje pristatomos išvardytų institucijų veiklos srityse nustatytos grėsmės, pagrindiniai rodikliai, svarbiausios tendencijos ir taikomos atsako priemonės – nuo incidentų valdymo ir nusikalstamų veikų elektroninėje erdvėje tyrimo iki elektroninių ryšių patikimumo, asmens duomenų apsaugos ir informacinių grėsmių stebėsenos. Iš ataskaitos galima susidaryti aiškų ir visapusišką Lietuvos kibernetinio saugumo būklės vaizdą.

Ataskaita skirta plačiajai visuomenei, organizacijų vadovams, ekspertams ir sprendimų priėmėjams, siekiantiems geriau suprasti rizikas, stiprinti atsparumą ir priimti pagrįstus sprendimus. Informacija, apimanti 2026 m. laikotarpį, pažymima išnašose.

KAM stiprino Lietuvos kibernetinį atsparumą ir pasirengimą naujos kartos grėsmėms

KAM, formuodama kibernetinio saugumo politiką, kartu su kitomis Lietuvos institucijomis stiprino tarpusavio bendradarbiavimą, siekiant didinti visuomenės sąmoningumą ir institucijų pasirengimą atpažinti ir užkardyti kibernetines grėsmes – pasirašyti bendradarbiavimo susitarimai su Vidaus reikalų ministerija, Švietimo, mokslo ir sporto ministerija, Kultūros ministerija ir Sveikatos ministerija. Įgyvendinant KAM nacionalinę kibernetinio saugumo plėtros programą buvo vykdomi kibernetinio saugumo infrastruktūros atnaujinimai, organizuojami mokymai, orientuoti į kompetencijų stiprinimą, įvairios komunikacinės veiklos

bei teisės aktų peržiūra ir atnaujinimas. Siekiant pasirengti kvantinei erai ir laiku pereiti prie kvantiškai atsparios – postkvantinės kriptografijos – parengti perėjimo prie postkvantinės kriptografijos proceso valdymo organizacijose gairių projektai.

KAM ir toliau aktyviai dalyvavo formuojant Europos Sąjungos (toliau – ES) kibernetinio saugumo politiką. 2025 m. intensyviai dalyvauta ES teisėkūros etapuose svarstant Europos Komisijos (toliau – EK) pasiūlymus dėl ES teisės aktų pakeitimų (tarp jų ir dėl TIS 2 direktyvos pakeitimo) bei naujų teisės aktų (pavyzdžiui, Skaitmeninio sektoriaus bendrojo rinkinio). Kartu su kitomis ES šalimis buvo ne tik aptartas naujasis ES krizių valdymo mechanizmas, bet ir sudalyvauta kibernetinių krizių valdymo pratybose.

2025 m. buvo aktyviai plėtojamas tarptautinis bendradarbiavimas kibernetinio saugumo srityje. Tęsiamos konsultacijos su Lenkija, Latvija, Moldova, JAV bei Indijos ir Ramiojo vandenynų regiono šalimis. Taip pat pradėtas bendradarbiavimas su Suomija ir Kanada.

2026 m. bus siekiama toliau vykdyti veiksmus, susijusius su organizacijų sklandžiu perėjimu prie postkvantinės kriptografijos, ES nuolatinio struktūrizuoto bendradarbiavimo (angl. *Permanent Structured Cooperation*, PESCO) (toliau – PESCO) projekto „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“ (toliau – PESCO projektas) valdymu ir PESCO projektu suburtų Kibernetinių greitojo reagavimo pajėgų (toliau – Kibernetinės greitojo reagavimo pajėgos) dalyvavimu ES bendros saugumo ir gynybos politikos karinėse misijose ir operacijose bei misijose ES šalyse partnerėse. Taip pat 2026 m. bus itin daug dėmesio skiriama Lietuvos pirmininkavimo ES Tarybai pasiruošimui.

NKSC vertinimu, 25 proc. mažiau kibernetinių incidentų rodo pažangą, tačiau organizacijų branda dar netolygi

2025 m. Lietuvoje užregistruoti 2 888 kibernetiniai incidentai – 25 proc. mažiau nei 2024 m. Tai lėmė tiek efektyviau taikomos NKSC prevencinės priemonės, įskaitant daugiau nei 70 tūkst. žalingų domenų blokavimą, tiek augantis organizacijų kibernetinio saugumo sąmoningumas. Kita vertus, apie dalį incidentų galėjo būti nepranešta dėl skirtingo teisinio reguliavimo interpretavimo ar dėl kompetencijų trūkumo identifikuojant kibernetinius incidentus.

Didžiąją incidentų dalį sudarė nedideli arba vos neįvykę incidentai. Didelių incidentų registruota nedaug – 19. Tai rodo stiprėjančius NKSC ir organizacijų incidentų valdymo pajėgumus ir kartu patvirtina, kad kibernetinės grėsmės nuolat plečiasi.

Skaitmeninė infrastruktūra (pvz.: debesijos, prieglobos, ryšių ir informacinių technologijų (toliau – IRT) paslaugų teikėjų sistemos) tampa ne tik atakų taikiniu, bet ir platforma, per kurią gali būti vykdomos tolesnės kibernetinės atakos. Daugiausia kibernetinių incidentų (2 118) susiję su užsienio subjektų prieglobos paslaugų infrastruktūra, naudojama kenkėjiškam turiniui skelbti ir platinti.

2025 m. išryškėjo dar viena tendencija – Lietuvos juridinių asmenų informacinėse sistemose įvyko beveik dvigubai daugiau kibernetinių incidentų (nuo 155 incidentų 2024 m. iki 280 incidentų 2025 m.). Tai reiškia, kad didžiausia rizika kyla organizacijų viduje. Šie incidentai dažniausiai įvyksta dėl žmogiškojo faktoriaus: darbuotojų budrumo stokos ir saugumo žinių trūkumo.

2025 m. fiksuotas didėjantis kibernetinių incidentų skaičius (267) ir Lietuvos skaitmeninėje infrastruktūroje. Šie incidentai susiję su paslaugų trikdymu, bandymais įsilaužti ir įvairiais veiklos sutrikimais.

Atkreiptinas dėmesys, kad kibernetinių grėsmių struktūra iš esmės nesikeičia – daugiau nei 54 proc. visų incidentų susiję su socialine inžinerija. Kita vertus, tokių incidentų skaičius 2025 m. buvo beveik trečdaliu mažesnis nei 2024 m. Net ir augant technologiniam atsparumui, didžiausia rizika išlieka susijusi su žmogaus elgsena, budrumu ir gebėjimu atpažinti apgaulės schemas.

Naudotojų paskyrų (angl. *Account*) užvaldymas išlieka pagrindinis įsilaužimo būdas. NKSC nustatė daugiau nei 106 tūkst. nutekintų prisijungimo duomenų, identifikuotų viešuosiuose ir uždaruose informacijos šaltiniuose, ir apie tai informavo 221 organizaciją – išsiuntė beveik 3000 pranešimų (2024 m. – 2000). Tai rodo, kad duomenų nutekėjimai ir toliau sudaro pagrindą tolimesnėms atakoms, ir pagrindinės duomenų nutekinimo priežastys yra kenkimo programinės įrangos (angl. *Malware*) tipas naudotojų duomenims slapta rinkti ir perduoti piktavaliams bei žmogiškasis faktorius. Reaguodamas į vis didėjančią grėsmę, NKSC automatizavo informavimą apie nutekėjusius prisijungimo duomenis ir pradėjo rengti atskirų sektorių kibernetinių grėsmių ataskaitas.

Išlieka aktuali NKSC aptinkamų tinklų ir informacinės sistemos (toliau – TIS) spragų problema. Interneto svetainės, žiniatinklio programos ir tinklo įrenginiai išlieka vienais dažniausių kibernetinių grėsmių taikinių, o nustatomi pažeidžiamumai rodo, kad dalis organizacijų vis dar nepakankamai užtikrina viešai prieinamų sistemų apsaugą ir laiku nešalina žinomų spragų.

2025 m. kibernetinio saugumo ekosistemos pokyčiai: į Kibernetinio saugumo subjektų registrą (toliau – Registras) įtrauktos 1 443 organizacijos, NKSC priežiūros apimtis išaugo beveik 5 kartus. Pradėta kurti nacionalinė saugumo operacijų centrų (angl. *Security Operations Center*, SOC) (toliau – SOC) modulinė sistema, sudaranti prielaidas greitesniam ir koordinuotam reagavimui į incidentus valstybiniu mastu, rengiamos praktinės rekomendacijos svarbiausiose kibernetinio saugumo srityse, įskaitant atsakingą DI naudojimą, trečiųjų šalių valdymą bei kibernetinių rizikų valdymą, plėtojamas tarpinstitucinis bendradarbiavimas su finansų sektoriumi ir teisėsaugos institucijomis, siekiant greitesnio informacijos apsikeitimo ir efektyvesnio reagavimo į grėsmes. Žvelgiant į 2026 m., tikėtina, kad pagrindinės grėsmių kryptys nesikeis, tačiau jų mastas ir sudėtingumas toliau augs. Dėl DI naudojimo kibernetinės atakos taps greitesnės ir įtikinamesnės, priklausomybė nuo tiekimo grandinių išliks vienu iš pagrindinių sisteminių pažeidžiamumų.

Policijos duomenimis, 2025 m. nusikalstamų veikų elektroninėje erdvėje sumažėjo, tačiau sukčiavimas, įgaunantis naujas formas, išlieka pagrindine grėsme

2025 m. Lietuvoje registruotų nusikalstamų veikų fizinėje erdvėje skaičius kiek sumažėjo (7 proc.), o elektroninėje erdvėje jų sumažėjo 28 proc., palyginti su 2024 m. Per pastaruosius penkerius metus nusikalstamumo lygis išlieka stabilus, rizikos augimo nenustatyta.

Elektroninėje erdvėje nusikalstamumą ir toliau daugiausia lemia sukčiavimas (44 proc.) ir nusikaltimai, nukreipti prieš informacines sistemas (21 proc.). Nors sukčiavimo atvejų skaičius 2025 m. stabilizavosi – pirmą kartą po tokių nusikalstamų veikų progresavimo pastaruosius 5 metus, fiksuota 7 proc. mažiau šių nusikalstamų veikų, sukčiavimo sukelta finansinė žala išlieka didelė. Finansų rinkos dalyvių duomenimis siekta išvilioti 58,8 mln. eurų, iš jų daugiau nei pusė sustabdyta, tačiau gyventojų nuostoliai sudarė apie 20,5 mln. eurų, tai yra nežymiai daugiau (apie 0,5 mln. eurų) lyginant su 2024 m. Tai lėmė tikslinis pažeidžiamų visuomenės grupių išnaudojimas ir prekyba nutekintais duomenimis, kelianti reikšmingą grėsmę tarptautiniu mastu.

Išlieka tendencija, kad sukčiavimo atvejai daugiausiai orientuoti į turtinės naudos gavimą (81 proc., arba 16 proc. daugiau nei 2024 m.) ir elektroninės bankininkystės vartotojus (76 proc., arba 16 proc. daugiau nei 2024 m.). Didėja rizika, kad aukos gali būti išnaudojamos ir kaip netyčiniai nusikaltimų bendrininkai ir kitiems tikslams, pavyzdžiui, hibridinėms atakoms vykdyti.

2025 m. reikšmingai išaugo apgaulingų skambučių ir svetainių klastojimo internete mastas. Nors apgaulingų skambučių 2025 m. antroje pusėje sumažėjo dėl taikytų užkardymo ir prevencinių priemonių, jų grėsmės rizika išlieka aukšta dėl organizuoto, tarptautinio nusikalstamumo ir agresyvėjančių nusikaltėlių veikimo metodų. Svetainių klastojimas, pradėjęs sistemingai plisti 2024 m. pabaigoje, išlieka dinamiškas ir gali tapti vienu dominuojančių sukčiavimo būdų, nes nusikaltėliai prisitaiko prie prevencinių priemonių ir ieško naujų būdų pasiekti aukas, apeiti taikomas apsaugas ir užvaldyti jų paskyras ar finansinius duomenis, siekiant pasisavinti lėšas.

2025 m. nusikalstamų veikų, nukreiptų prieš elektroninių duomenų ir informacinių sistemų saugumą, skaičius padidėjo apie 9,2 proc., tačiau jų pavojingumas išlieka žemas. Didžiausią nusikalstamumo elektroninėje erdvėje riziką kelia neteisėto prisijungimo prie informacinių sistemų atvejai, tačiau jų dinamika išlieka stabili.

Lietuvoje, priešingai nei kitose ES šalyse, kibernetinių atakų, susijusių su elektroninius duomenis užšifruojančiais išpirkos reikalaujančio kenkimo programinio kodo virusais (angl. *Ransomware*) ir paskirstytųjų paslaugos trikdymo (angl. *Distributed Denial of Service* (DDoS)) (toliau – DDoS) atvejai Lietuvoje nepasireiškė sistemingai ir sudarė mažiau nei 1 proc. visų nusikalstamų veikų elektroninėje erdvėje.

Nors DI panaudojimo nusikalstamose veikose policija dar plačiai nefiksuoja, jo panaudojimas nusikaltimams vykdyti auga ir kelia ilgalaikius iššūkius teisėsaugai. Kartu policija stiprina savo technologinius pajėgumus, diegdama pažangų analitinį įrankį, skirtą analizuoti duomenis ir tirti sudėtingas nusikalstamas veikas.

Išliekant sukčiavimo, DI ir ideologiškai motyvuotų kibernetinių atakų tendencijoms, ypač susijusioms su geopolitine situacija ir hibridinėmis grėsmėmis, lemiamą reikšmę turės teisėsaugos gebėjimas stiprinti pajėgumus ir užtikrinti veiksmingą bendradarbiavimą bei sisteminiai sprendimai, susiję su teisės aktų pritaikymu sparčiai kintančiai technologinei aplinkai.

VDAI duomenimis, 2025 m. Lietuvoje 29 proc. asmens duomenų saugumo pažeidimų (toliau – ADSP) įvyko dėl kibernetinių incidentų

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

2025 m. VDAI gavo 223 pranešimus apie ADSP, 18 proc. mažiau negu 2024 m. VDAI teigimu, teigiamą įtaką tam galėjo turėti įsigaliojusi nauja Kibernetinio saugumo įstatymo (toliau – KSĮ) redakcija, taip pat praplėstas kibernetinio saugumo subjektų sąrašas, aiškiai reglamentuotos techninės ir organizacinės priemonės, taip pat reguliariai VDAI vykdoma švietimo veikla.

2025 m. 29 proc. ADSP įvyko dėl kibernetinių incidentų, tačiau jų metu buvo paveikti net 57 proc. duomenų subjektų (iš viso 713 644), t. y. daugiau nei pusė iš visų 2025 m. paveiktų asmenų, duomenys.

Vertinant 2025 m. gautus ADSP pranešimus, kurie įvyko dėl kibernetinio incidento, nustatyta, kad 45 proc. ADSP įvyko piktavaliui neteisėtai gavus prieigą prie IT sistemų, 26 proc. dėl socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) atakų, 16 proc. dėl duomenų užšifravimo ir išpirkos reikalavimo (angl. *Ransomware*) atakų. 6 proc. iš visų 2025 m. gautų ADSP pranešimų priežastys nenustatytos. Darytina išvada, kad, įvykus kibernetiniam incidentui, duomenų valdytojai neįstengia tinkamai atlikti kibernetinio incidento tyrimo ir nustatyti priežasčių, kurių išaiškinimas galėtų ateityje padėti išvengti tokio pobūdžio atakų.

VDAI praktika 2025 m. parodė, kad Lietuvoje ir Europoje įvykę ADSP, dėl kurių nukentėjo Lietuvos gyventojai, atskleidė sistemines silpnąsias vietas: žmogiškąjį faktorių, tiekimo grandinių pažeidžiamumą ir nepakankamą trečiųjų šalių kontrolę. Tai patvirtino poreikį stiprinti darbuotojų kompetencijas, vidaus kontrolę, rizikos ir incidentų valdymo brandą bei griežčiau vertinti naudojamus DI įrankius.

VDAI įvertinus 2025 m. duomenis ir Lietuvoje bei pasaulyje vyraujančias tendencijas, darytina išvada, kad socialinės inžinerijos ir duomenų viliojimo atakos sėkmingos dėl vis dar nepakankamo darbuotojų gebėjimo atpažinti socialinės inžinerijos požymius, papildomų tapatybės autentifikavimo priemonių netaikymo, įgalinančio pasinaudoti išviliotais prisijungimo duomenimis, tiekimo grandinių pažeidžiamumą ir nepakankamą trečiųjų šalių kontrolę.

Remiantis 2025 m. VDAI patirtimi, vertinant gautus ADSP pranešimus, galima pagrįstai prognozuoti, kad 2026 m. DI naudojimo iššūkiai, susiję su asmens duomenų apsauga, išliks aktualūs ir pareikalaus nuoseklaus priežiūros institucijų bei organizacijų dėmesio. 2026 m. VDAI įsipareigoja ir toliau aktyviai vykdyti visuomenės švietimą bei stiprinti gyventojų informuotumą apie kibernetinio sukčiavimo atvejus, siekdama padėti jiems laiku atpažinti grėsmes ir veiksmingai nuo jų apsisaugoti.

RRT priemonės mažinant sukčiavimą ir žalingą turinį internete stiprino kibernetinės erdvės saugumą, tačiau išryškėjo naujos rizikos

2025 m. Lietuvos elektroninių ryšių infrastruktūra išliko stabiliai veikianti – nebuvo fiksuota didelių sutrikimų, o paslaugų teikimas dažniausiai buvo atkuriamas per maždaug 2 valandas. Tačiau išryškėjo naujos rizikos: žalingi radijo trukdžiai iš Kaliningrado teritorijos paveikė orlaivių, laivų valdymo sistemas, mobiliojo ryšio bazines stotis ir pasienio teritorijas. Žalingųjų radijo trukdžių intensyvėjimas 2025 m. pabaigoje parodė, kad trukdžiai Baltijos regione tampa ilgalaike ir sistemine problema, kuri turi būti eskaluojama ES ir tarptautiniu lygiu.

Telefoninio sukčiavimo mastas 2025 m. toliau sparčiai augo – nors buvo blokuoti milijonai apgaulingų skambučių (63 proc. daugiau nei 2024 m.) ir apsimestinių SMS (beveik 80 proc. daugiau nei 2024 m.), tai rodo ne tik taikomą efektyvesnę apsaugą, bet ir didėjantį pačios grėsmės intensyvumą. Sukčiavimo schemos tampa vis adaptyvesnės, daugėja suklastotų lietuviškų numerių, pritaikomi vis nauji socialinės inžinerijos metodai, todėl būtina stiprinti reguliacinį ir operacinį atsaką taip, kad taikomos priemonės veiktų ne tik reaguojant, bet ir užkertant tam kelią.

Elektroninės atpažinties ir kvalifikuoto elektroninio parašo naudojimas Lietuvoje tapo plačiai paplitęs, o šių priemonių patikimumas tiesiogiai susijęs su pasitikėjimu skaitmenine aplinka. 2025 m. RRT priimti sprendimai šioje srityje didino tokių paslaugų prieinamumą ir pasirinkimo galimybes rinkoje.

Įgyvendinant Skaitmeninių paslaugų aktą (toliau – SPA) ir jo nuostatas nacionalinėje teisėje, Lietuva iš kitų ES šalių išsiskyrė aktyviu neteisėto turinio šalinimo mechanizmų taikymu. Per 2025 m. pirmąjį pusmetį Lietuvos institucijos labai didelėms interneto platformoms pateikė 480 pranešimų (ES – 2 700), o Lietuvos patikimų pranešėjų iniciatyva pašalinta apie 6 mln. neteisėto turinio nuorodų, taip mažinant vartotojų susidūrimą su žalingu turiniu internete.

Užkardant draudžiamą ir neigiamą poveikį nepilnamečiams darančios informacijos plitimą elektroninėje erdvėje, 2025 m. išryškėjo augančios rizikos: interneto karštoji linija „Švarus internetas“ gavo daugiau kaip 3,5 tūkst. pranešimų (beveik 62 proc. daugiau nei 2024 m.), iš kurių daugiau kaip 2,2 tūkst. pasitvirtino. Ypač sparčiai augo kibernetinių patyčių mastas – 2025 m. pasitvirtinusių atvejų skaičius palyginti su 2024 m. išaugo apie tris kartus, o per trejus metus – daugiau nei penkis kartus. Taip pat 18 proc. padaugėjo pranešimų apie vaikų seksualinio išnaudojimo turinį internete, kurio didžioji dalis laikoma kitų šalių serveriuose. Žalingo turinio užkardymo internete veiksmingumas tiesiogiai priklauso nuo operatyvaus Lietuvos institucijų ir tarptautinių partnerių bendradarbiavimo.

Stiprinant visuomenės gebėjimą atpažinti kibernetines grėsmes ir saugiai naudotis skaitmeninėmis paslaugomis, 2025 m. RRT tęsė projektą „Nė vienas nėra pamirštas“. Projektas subūrė šimtus partnerių visoje Lietuvoje, o skaitmeninio raštingumo mokymai pasiekė dešimtis tūkstančių gyventojų, ypač vyresnio amžiaus žmones.

Žvelgdama į 2026 m., RRT sieks nuosekliai stiprinti elektroninių ryšių tinklų ir skaitmeninių paslaugų saugumą ir patikimumą, daugiausia dėmesio skirdama kovai su sukčiavimu elektroninėje erdvėje bei saugesnės skaitmeninės aplinkos kūrimui.

LK SKD duomenimis, 2025 m. Lietuvoje, kaip ir visoje Europoje, išaugo informacinių incidentų skaičius

2025 m. LK SKD identifikavo 3 707 informacinius incidentus, kai buvo skleista priešiška, klaidinanti ar melaginga informacija apie Lietuvą ar jos partnerius (NATO, ES). Tai siejama su aktyvėjančiu priešišku Baltarusijos veikimu informacinėje erdvėje ir nuosekliu Rusijos veikimu prieš NATO ir ES.

Gynybos ir saugumo tematika ne vienerius metus išlieka dominuojanti priešiškoje informacinėje aplinkoje. 2025 m. ji sudarė 70 proc. visų identifikuotų informacinių incidentų, nukreiptų prieš Lietuvą ar jos partnerius. 2025 m. ypatingai didelis dėmesys skirtas Baltijos jūros regionui ir Kaliningrado sričiai. Priešiškų valstybių taikiniu buvo Lietuvos gynybos politikos sprendimai, ypatingai išnaudota pasienio su Rusija ir Baltarusija gynybos stiprinimo tema.

2025 m. stebėtas augantis Baltarusijos režimo vykdomas informacinis spaudimas prieš Lietuvą, siekiant įtikinti tiek vidaus, tiek išorės auditorijas, kad Lietuvos vykdoma užsienio politika yra neracionali, agresyvi Baltarusijos atžvilgiu ir kenksminga Lietuvos piliečiams. Aktyviausiais propagandos sklaidos kanalais išliko valstybinės ir režimų kontroliuojamos žiniasklaidos priemonės, taip pat socialiniai tinklai, daugiausiai – „Telegram“.

2025 m. DI tapo grėsme ir LK SKD veiklos srityje – jis naudojamas kibernetinėse atakose, socialinės inžinerijos ir sukčiavimo schemose, informacinėse bei psichologinėse operacijose. DI įgalina kur kas didesnį priešiškų kampanijų mastą, greitesnį naratyvų adaptavimą ir aukštesnį personalizacijos bei maskavimo lygį. 2026 m., siekiant prisidėti prie visuomenės atsparumo informacinėms grėsmėms stiprinimo, LK SKD ir toliau vykdys šviečiamąsias veiklas, dalinsis įžvalgomis su žiniasklaida ir visuomene.

Sustiprintas tarpinstitucinis bendradarbiavimas kaip atsakas į kibernetines grėsmes

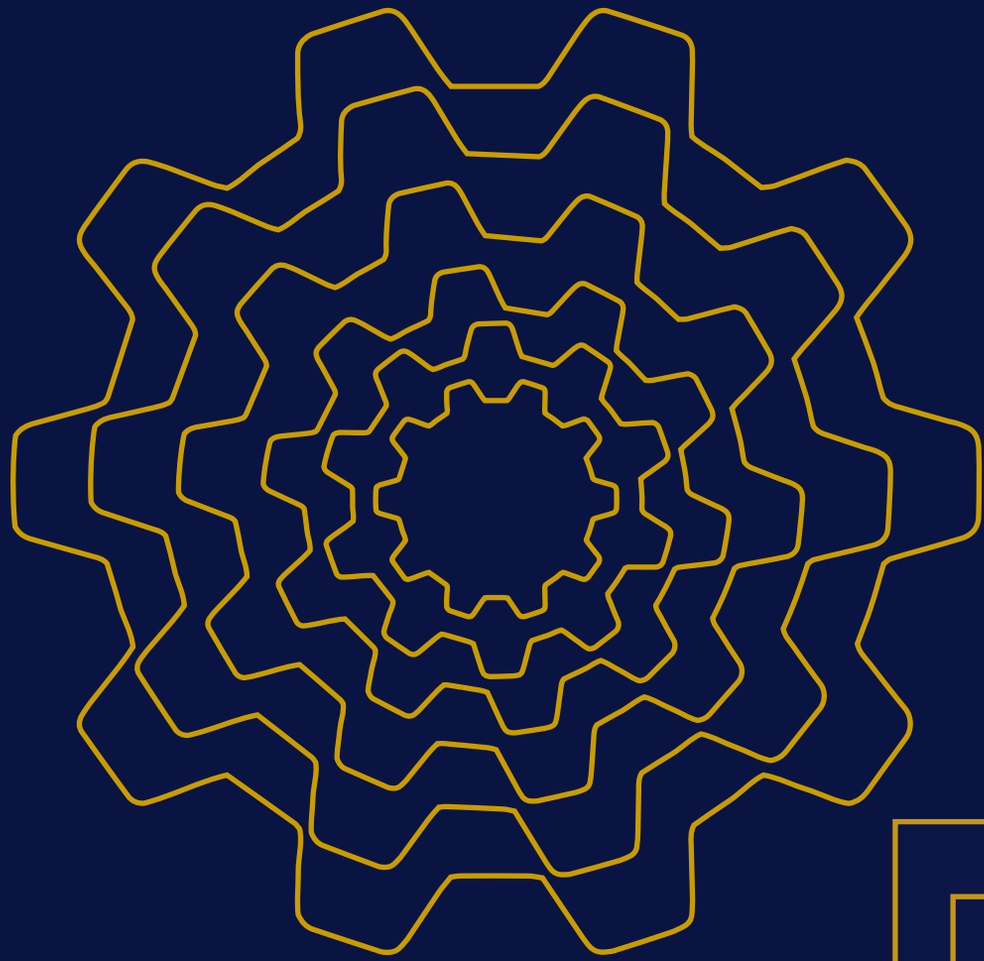
Vis labiau ryškėja tendencija, kad kai kurios kibernetinės grėsmės, ypač socialinės inžinerijos principais grindžiamas sukčiavimas, apima keletą sričių vienu metu ir nebegali būti veiksmingai valdomos pavienių institucijų pastangomis. Tokios grėsmės tuo pačiu metu daro įtaką teisėsaugos, finansų, elektroninių ryšių bei kibernetinio saugumo sritims, įskaitant fizinių asmenų ir organizacijų interesus. Todėl didžiausią vertę kuria operatyvūs informacijos mainai, koordinuoti veiksmai ir suderintos prevencinės priemonės. Atsižvelgdami į tai, Lietuvos bankas, Lietuvos policija, Lietuvos Respublikos generalinė prokuratūra, NKSC, RRT ir Pinigų plovimo prevencijos kompetencijų centras 2025 m. kovo 27 d. pasirašė memorandumą dėl bendradarbiavimo mažinant sukčiavimą skaitmeninėje erdvėje. Memorandumu siekiama sutelkti institucijų pajėgumus bendrai kovai su sukčiavimu skaitmeninėje erdvėje, užtikrinant spartų informacijos apsikeitimą, koordinuotą reagavimą, bendras prevencines priemones ir veiksmingesnį visuomenės perspėjimą apie grėsmes.

Papildomai 2025 m. liepos 28 d. NKSC ir Lietuvos bankas pasirašė bendradarbiavimo susitarimą dėl keitimosi informacija apie kibernetinius incidentus finansų sektoriuje. Lietuvos bankui kaip finansų rinkos reguliuotojui, pirmajam prisijungus prie NKSC Nacionalinės kibernetinių incidentų valdymo platformos, sudarytos sąlygos automatizuotai keistis informacija apie incidentus ir kibernetines grėsmes realiuoju laiku, greičiau reaguoti į grėsmes ir plėtoti glaudesnį skirtingų sektorių bendradarbiavimą.

2025 m. praktika parodė, kad efektyviausias atsakas į skaitmenines grėsmes yra ne pavieniai sprendimai, o nenutrūkstamas valstybės institucijų, reguliuotojų, teisėsaugos ir svarbių sektorių bendradarbiavimas. Tada greitėja ne tik reagavimas į incidentus, bet ir bendrasis Lietuvos kibernetinis atsparumas.

03

Kibernetinio saugumo politikos formavimo kryptys



Kibernetinio saugumo politikos formavimo kryptys

Dabartinėje geopolitinio neapibrėžtumo aplinkoje visuomenės gebėjimas atpažinti grėsmes ir veikti atsakingai tampa svarbia nacionalinio saugumo dalimi. Kibernetinę erdvę priešiškos valstybės ir nusikalstamos grupuotės naudoja politiniams, kariniams ir ekonominiams tikslams, išnaudodamos organizacijų priklausomybę nuo tiekimo grandinių ir jų pažeidžiamumus. Papildomų iššūkių kelia sparčiai besivystančios technologijos – generatyvinis DI, didinantis kibernetinių atakų mastą ir greitį, bei kvantinių technologijų plėtra, ateityje galinti paveikti šiandien taikomas duomenų apsaugos priemones.

Todėl KAM siekia stiprinti institucijų bei verslo atsparumą, užtikrinti svarbiausių paslaugų tęstinumą ir didinti naudotojų pasitikėjimą kibernetine erdve. Organizacijų pasirengimas ir kibernetinio saugumo reikalavimų įgyvendinimas prisideda prie bendro Lietuvos ir ES kibernetinio atsparumo. Tarptautinis bendradarbiavimas, aktyvus dalyvavimas formuojant ES kibernetinio saugumo politiką ir įsipareigojimų NATO vykdymas išlieka svarbiais KAM prioritetais.

Stiprinamas kibernetinis atsparumas nacionaliniu ir ES lygiu

KAM, formuodama kibernetinio saugumo politiką, kartu su kitomis institucijomis 2025 m. ypatingą dėmesį skyrė koordinuotiems veiksmams stiprinant visuomenės sąmoningumą ir institucijų pasirengimą atpažinti kibernetines grėsmes. Ataskaitiniais metais pasirašyti **bendradarbiavimo susitarimai su Vidaus reikalų ministerija, Švietimo, mokslo ir sporto ministerija, Kultūros ministerija ir Sveikatos ministerija** sudarė prielaidas sistemingai plėtoti kibernetinio saugumo pratybas, gerinti keitimąsi informacija apie grėsmes ir incidentus, stiprinti incidentų tyrimo kompetencijas, ugdyti mokinių ir jaunimo pilietiškumą bei kibernetinio saugumo žinias, stiprinti ministerijų ir sveikatos priežiūros institucijų kibernetinį atsparumą, taip pat didinti visuomenės atsparumą, kritinį mąstymą, medijų raštingumą ir kovą su dezinformacija. Tokia tarpžinybinė partnerystė leidžia kryptingai stiprinti visuotinę gynybą ir kurti tvarią saugumo ekosistemą nacionaliniu mastu.

2025 m. buvo intensyvūs metai valstybės institucijoms įgyvendinant projektus, vykdomus siekiant spręsti problemą, identifikuotą **2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinėje kibernetinio saugumo plėtros programoje**[01], t. y. mažėjantį šalies kibernetinį atsparumą, kurį lemia pasikeitęs

01
Lietuvos Respublikos Vyriausybės 2023 m. rugsėjo 20 d. nutarimas Nr. 746 „Dėl 2023–2030 metų plėtros programos valdytojos Lietuvos Respublikos krašto apsaugos ministerijos nacionalinės kibernetinio saugumo plėtros programos patvirtinimo“.

kibernetinių grėsmių pobūdis ir augantis jų mastas. Ekonomikos gaivinimo ir atsparumo didinimo priemonės lėšomis finansuojamus projektus įgyvendina KAM, NKSC, Kertinis valstybės telekomunikacijų centras (toliau – KVTC) ir Policijos departamentas prie Vidaus reikalų ministerijos.

Šių valstybės institucijų 2024–2025 m. vykdyti projektai apėmė kibernetinio saugumo infrastruktūros atnaujinimą, mokymus, kompetencijų stiprinimą, komunikacines veiklas bei teisės aktų peržiūrą ir atnaujinimą, siekiant nuosekliai stiprinti nacionalinį kibernetinį atsparumą. 2025 m. KAM vykdė projekto **„Kibernetinio saugumo valdysenos Lietuvoje stiprinimas“** veiklas. Dauguma šių projekto veiklų 2025 m. buvo pabaigtos: stiprinama kibernetinio saugumo valdysena per teisėkūros, metodinės pagalbos, mokymų organizavimo veiklas, taip pat sėkmingai įvykdytos dvi visuomenės kibernetinio saugumo brandai didinti skirtos komunikacijos kampanijos, pritaikytos skirtingoms tikslinėms grupėms: senjorams, regionų gyventojams, moterims bei 15–25 m. jaunimui. Visas kitas veiklas numatoma pabaigti 2026 m. balandžio 30 d.

Daugumai ES valstybių narių[02] į nacionalinę teisę perkėlus 2022 m. gruodžio 14 d. **Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje ES 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**)[03], 2025 m. ES kibernetinio saugumo politika ir toliau siekė užtikrinti skaitmeninės visuomenės saugumą ir ES ekonomikai svarbių sektorių kibernetinį atsparumą. Naujais teisėkūros pasiūlymais ir priimamais kitais teisės aktais siekiama padidinti skirtingų, bet tarpusavyje susijusių ES sektorių atsparumą kibernetinėms ir hibridinėms grėsmėms, pagerinti pasirengimą krizinėms situacijoms, paskatinti informacijos apsikeitimą ir atsakomybės pasidalijimą tarp valstybių narių, ES institucijų. Už Lietuvos kibernetinį saugumą atsakingos institucijos pagal kompetenciją dalyvauja ES teisėkūros etapuose.

Viena iš svarbiausių ES teisėkūros iniciatyvų – EK 2025 m. lapkričio 19 d. pasiūlymas dėl **Skaitmeninio sektoriaus bendrojo rinkinio** (angl. *Digital Omnibus*)[04]. Pasiūlyta sukurti vieną bendrą prieigą (angl. *Single Entry Point*), per kurią subjektai vienu metu galėtų vykdyti savo pareigas teikdami pranešimus apie incidentus pagal kelis teisės aktus: **TIS 2 direktyvą, Bendrąjį duomenų apsaugos reglamentą[05], Skaitmeninės veiklos atsparumo aktą[06], eIDAS reglamentą[07] ir Direktyvą dėl ypatingos svarbos subjektų atsparumo[08]**. Siūloma, kad kiekvienoje ES valstybėje narėje reguliuojami kibernetinio saugumo subjektai galėtų pildyti pranešimą apie kibernetinį incidentą bendroje sistemoje, jį gautų valstybių narių paskirtos kompetentingos institucijos (esant poreikiui, ir keliose valstybėse). Taip siekiama padėti įmonėms, viešojo administravimo subjektams ir fiziniams asmenims laikytis teisės aktų nuostatų mažesnėmis sąnaudomis.

02
Europos kibernetinio saugumo organizacija (angl. *European Cyber Security Organisation* (ECSO) Lietuvą nurodė kaip vieną iš keturių ES šalių, laiku perkėlusių šią direktyvą. „ECSO Baltoji knyga – TIS 2 įgyvendinimas: iššūkiai ir prioritetai“ (angl. *ECSO White Paper – NIS2 Implementation: Challenges & Priorities*).

03
2026 m. sausio 20 d. EK, pristatydama naują kibernetinio saugumo priemonių paketą, pasiūlė tikslines TIS 2 direktyvos pataisas, kuriomis siekiama supaprastinti ES kibernetinio saugumo taisyklių ir rizikos valdymo reikalavimus ES įmonėms.

04
2025 m. lapkričio 19 d. Europos Komisijos pasiūlymas dėl Europos Parlamento ir Tarybos Reglamento, kuriuo siekiant supaprastinti skaitmeninio sektoriaus teisės aktų sistemą iš dalies keičiami reglamentai (ES) 2016/679, (ES) 2018/1724, (ES) 2018/1725, (ES) 2023/2854 ir direktyvos 2002/58/EB, (ES) 2022/2555 ir (ES) 2022/2557 ir panaikinami reglamentai (ES) 2018/1807, (ES) 2019/1150, (ES) 2022/868 ir Direktyva (ES) 2019/1024, (Skaitmeninio sektoriaus bendrasis rinkinys).

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).

06
2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011.

07
2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.

08
Europos Parlamento ir Tarybos direktyva (ES) 2022/2557 2022 m. gruodžio 14 d. dėl ypatingos svarbos subjektų atsparumo, kuria panaikinama Tarybos direktyva 2008/114/EB.

2025 m. birželio 25 d. EK pasiūlė **ES Kosmoso aktą**[09] – naują plataus masto priemonių rinkinį Europos kosmoso sektoriaus taršai mažinti, saugumui ir konkurencingumui Europoje ir jos eksporto rinkose stiprinti. Akto pagrindinis tikslas – spręsti saugumo, atsparumo ir tvarumo problemas, veikti bendrai, o ne fragmentiškai (daugelis ES valstybių narių kuria nacionalinius kosmoso įstatymus arba vadovaujasi jau galiojančiais). Pagal šį aktą visi veiklos kosmose vykdytojai turės atlikti išsamius rizikos vertinimus per visą palydovų gyvavimo ciklą, laikydamiesi kosmoso sektoriaus kibernetinio saugumo taisyklių, ir informuoti apie incidentus. 2025 m. pabaigoje Lietuva kartu su 10 kitų ES valstybių narių pritarė neoficialiame dokumente (angl. *non-paper*) išdėstytai pozicijai, kad nauji kibernetinio saugumo reikalavimai turėtų būti grindžiami jau galiojančiu teisiniu reglamentavimu (pvz., TIS 2 direktyva), siekiant išvengti naujų besidubliuojančių taisyklių ir perteklinės naštos verslui bei valstybės institucijoms.

Atsižvelgdama į tai, kad sveikatos priežiūros sektorius vis dažniau tampa kibernetinių atakų taikiniu, EK 2025 m. sausio mėn. paskelbė **Europos ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinio saugumo veiksmų planą**[10], kuriuo siekiama gerinti ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinį saugumą visoje ES. Bendradarbiaujant valstybių narių sveikatos priežiūros paslaugų teikėjams ir kibernetinio saugumo bendruomenei, planas laipsniškai buvo įgyvendinamas 2025 m. Jo bus toliau laikomasi ir 2026 m.

2025 m. vasario mėn. **EK paskelbė ES veiksmų planą dėl kabelių saugumo**[11]. Ekspertų darbo grupė parengė ES valstybėse narėse esančių ir planuojamų povandeninių duomenų kabelių infrastruktūros žemėlapį, rizikos vertinimą, nurodė pagrindinius rizikos scenarijus ir gaires, kaip atlikti rizikos scenarijų testavimą. Taip pat parengtas Europos interesų prioritetų sąrašas (angl. *Priority List of Cable Projects of European Interest*), kuriuo vadovaujantis projektams, susijusiems su kabelių, nutiestų Baltijos jūros dugne, infrastruktūra, turėtų būti teikiamas ES finansavimo prioritetas.

2024 m. gruodžio 10 d. įsigaliojo **Kibernetinio atsparumo aktas**[12], nustatantis skaitmeninių produktų, tiekiamų ES rinkai, projektavimo, kūrimo ir gamybos kibernetinio saugumo reikalavimus, taip pat šių produktų tiekimo į rinką taisykles bei kitų ekonominės veiklos vykdytojų (importuotojų, platintojų) pareigas. Kibernetinio atsparumo aktas bus pradėtas taikyti 2027 m. pabaigoje. Lietuva, kaip ir kitos ES valstybės narės, turės paskirti notifikuojančiąją instituciją, taip pat vieną ar kelias rinkos priežiūros institucijas. Siekiant įgyvendinti Kibernetinio atsparumo aktą, būtina parengti ir priimti teisės aktų pakeitimus, apibrėžiančius minėtas procedūras, bei sankcijų taikymo mechanizmus. KAM, būdama atsakinga už Kibernetinio atsparumo akto įgyvendinimą Lietuvoje, 2025 m. pradėjo pasiruošimą Kibernetinio atsparumo akto nuostatų įgyvendinimui: parengė Kibernetinio atsparumo akto įgyvendinimo Lietuvoje priemonių planą ir inicijavo diskusijas su kitomis valstybės institucijomis dėl galimo šio teisės akto įgyvendinimo modelio. 2025 m. rudenį KAM

09
2025 m. birželio 25 d. Europos Komisijos pasiūlymas dėl Europos Parlamento ir Tarybos Reglamento dėl Sąjungos kosminės veiklos saugos, atsparumo ir tvarumo.

10
2025 m. sausio 15 d. Europos Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui bei Regionų komitetui – Europos veiksmų planas dėl ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinio saugumo (COM(2025) 10 galutinis).

11
2025 m. vasario 21 d. Europos Komisijos bendras komunikatas Europos Parlamentui ir Tarybai – ES veiksmų planas dėl kabelių saugumo.

12
2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas).

parengė Lietuvos Respublikos Vyriausybės nutarimo „Dėl Reglamento (ES) 2024/2847 įgyvendinimo“ projektą. Nutarimo tikslas – paskirti KAM notifikuojančiąja institucija, kuri priims sprendimus dėl įstaigų skyrimo atlikti produktų su skaitmeniniais elementais, patenkančiais į Kibernetinio atsparumo akto taikymo sritį, atitikties vertinimo procedūras.

2019 m. priimtas **Kibernetinio saugumo aktas**[13] padėjo pamatus pirmosios ES lygmens kibernetinio saugumo sertifikavimo sistemos diegimui, siekiant užtikrinti tinkamą IRT produktų, paslaugų, procesų kibernetinio saugumo lygį ES. Pastaruoju metu ES ir visame pasaulyje vykstantys spartūs technologiniai ir geopolitiniai pokyčiai bei praktiniai suinteresuotųjų šalių lūkesčiai atskleidė, kad tokio reglamentavimo nepakanka šiandienos kibernetinio saugumo rizikoms suvaldyti. 2025 m. EK pasiūlė peržiūrėti Kibernetinio saugumo aktą, siekdama pašalinti kibernetinio saugumo sertifikavimo sistemos įgyvendinimo kliūtis bei sumažinti augančias IRT tiekimo grandinės saugumo rizikas. Taip pat siekiama suteikti ES kibernetinio saugumo agentūrai (toliau – ENISA) didesnius įgaliojimus gerinant bendrą suvokimą apie kibernetinio saugumo grėsmes ir incidentus, kibernetinio saugumo standartus ir sertifikavimą, pagalbą reaguojant į išpirkos reikalaujančias atakas bei kibernetinio saugumo specialistų rengimo srityse. 2025 m. balandžio 11 d. EK pradėjo vykdyti viešas konsultacijas su valstybėmis narėmis dėl Kibernetinio saugumo akto peržiūros[14]. 2025 m. pabaigoje Lietuva kartu su 19 kitų ES valstybių narių prisijungė prie neoficialaus dokumento (angl. *non-paper*) dėl ENISA funkcijų išplėtimo peržiūrint Kibernetinio saugumo aktą, ir kartu su 6 valstybėmis narėmis – prie kito neoficialaus dokumento (angl. *non-paper*) dėl ES kibernetinio saugumo sertifikavimo sistemos pagal Kibernetinio saugumo aktą valdymo, procesų ir taikymo apimties peržiūros, kad sertifikavimas taptų realia priemone stiprinti kibernetinį saugumą ir pasitikėjimą visoje ES.

2025 m. septynios Šiaurės ir Baltijos šalys[15], vadovaudamosi 2025 m. vasario 4 d. įsigaliojusio **Kibernetinio solidarumo akto**[16] nuostatomis, paskelbė, kad inicijuoja **Šiaurės–Baltijos kibernetinio konsorciumo** (angl. *Nordic-Baltic Cyber Consortium*, (NBCC) sudarymą. Kibernetiniams incidentams vis dažniau vienu metu paveikiant kelias valstybes, konsorciume dalyvaujančios šalys siekia sistemingai gauti ir keistis informacija apie kibernetines grėsmes Šiaurės ir Baltijos regione. Tai leis atsakingoms valstybės institucijoms efektyviau nustatyti regionui aktualias kibernetinio saugumo tendencijas, aptikti ir analizuoti silpnąsias pažeidžiamas vietas ir koordinuoti atsakomuosius veiksmus. Be to, konsorciumas kurs pažangias kibernetinio saugumo technologijas, įskaitant DI sprendimus, ir skatins viešojo sektoriaus, verslo ir mokslo institucijų bendradarbiavimą, taip prisidedant prie viso regiono kibernetinio atsparumo stiprinimo. Projekto įgyvendinimas numatomas 2026–2029 metais, įgyvendinimą Lietuvoje koordinuos NKSC.

13
2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas).

14
2026 m. sausio 20 d. EK pristatytas naujas kibernetinio saugumo priemonių paketas apima Kibernetinio saugumo akto peržiūrėjimo pasiūlymą.

15
Danija, Lietuva, Latvija, Estija, Suomija, Norvegija, Islandija ir stebėtoja Švedija.

16
2024 m. gruodžio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2025/38, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Kibernetinio solidarumo aktas).

Įgyvendinant Lietuvos Respublikos Seimo politinių partijų 2022 m. pasirašyto susitarimo „Dėl Lietuvos nacionalinio saugumo ir gynybos artimiausio laikotarpio stiprinimo“ nuostatas dėl Lietuvos kariuomenės kibernetinės gynybos pajėgumų stiprinimo, nuo 2025 m. sausio 1 d. veiklą pradėjo **Lietuvos kariuomenės Kibernetinės gynybos valdyba** (toliau – LK KGV). LK KGV yra atsakinga už kibernetinės erdvės operacijų planavimą ir vykdymą, strateginio ir operacinio lygmens ryšių bei informacinių sistemų diegimą, taip pat užtikrina sąveiką su NATO, krašto apsaugos sistemos ir kitų institucijų bei organizacijų ryšių ir informacinėmis sistemomis. 2025 m. LK KGV organizavo kasmetines tarptautines kibernetinės gynybos pratybas „Gintarinė migla“ (angl. *Amber Mist*), subūrusias apie 300 dalyvių iš Lietuvos valstybės institucijų, akademinės bendruomenės ir privataus sektoriaus, taip pat atstovus iš 18 NATO ir partnerių šalių. LK KGV aktyviai dalyvavo NATO, ES, regiono ir dvišaliuose kibernetinės gynybos karinio bendradarbiavimo renginiuose ir pratybose, LK KGV personalas tobulinosi įvairiuose kvalifikacijos kėlimo kursuose.

Didėjant kibernetinėms grėsmėms kritinėms paslaugoms ir infrastruktūrai, ES vis daugiau dėmesio skiria **tiekimo grandinių ir tarpusavyje susietų sistemų kibernetinio saugumo rizikų** vertinimui ir jų mažinimui. Tinklų ir informacinių sistemų bendradarbiavimo grupės (angl. *NIS Cooperation Group*) Tiekimo grandinės saugumo darbo grupė, į kurią įtrauktas KAM atstovas, bendradarbiaudama su EK ir ENISA, atliko du ES lygio saugumo rizikos vertinimus, t. y. ES teisėsaugos ir saugumo operatorių ES sienos perėjimo punktuose naudojamos aptikimo įrangos rizikos vertinimą ir prisijungusių ir automatizuotų transporto priemonių ir jų tiekimo grandinių rizikos vertinimą. Kiekviename iš šių ES lygio saugumo rizikos vertinimų buvo identifikuota virš 10 labiausiai tikėtinų rizikų, pateikta išsami apžvalga apie nustatytus kibernetinio saugumo pavojus, jų galimas pasekmes ir priemones, būtinas pavojams sumažinti. Tikimasi, kad 2026 m. ES priims **tiekimo grandinės saugumo priemonių rinkinį** (angl. *EU ICT Supply Chain Security Toolbox*), atsižvelgdama į susietųjų ir automatizuotų transporto priemonių (angl. *Connected and Automated Vehicle,* CAV) bei aptikimo įrangos kibernetinio saugumo rizikos vertinimo rezultatus.

2025 m. siekiant konsoliduoti KAM valdomų tarpinstitucinių telekomunikacijų tinklų tvarkymą vienoje įstaigoje, KVTC pradėjo vykdyti **Vyriausybinio plačiajuosčio šifruoto duomenų ir balso perdavimo tinklo** tvarkytojo funkcijas. Pagrindiniuose **Saugiojo valstybinio duomenų perdavimo tinklo** (toliau – Saugusis tinklas) mazguose buvo įdiegta duomenų perdavimo įranga, skirta tinklo saugumui stiprinti ir nepertraukiamam veikimui mobilizacijos ir ekstremaliųjų situacijų atvejais užtikrinti bei priklausomybei nuo trečiųjų šalių paslaugų mažinti. KVTC taip pat pradėjo vykdyti dalies Saugiajame tinkle esančių išorinių valstybės informacinių išteklių auditą, kurio rezultatais remiantis bus toliau tobulinama kibernetinių saugos priemonių architektūra, užtikrinanti Saugiajame tinkle esančių informacinių išteklių pasiekiamumą ir saugumą. 2025 m. KVTC SOC bendradarbiaudamas su kitomis instituci-

jomis nustatė ir užblokavo virš 22 tūkst. kenksmingų IP adresų, kurie įvairiais būdais bandė sutrikdyti Saugiojo tinklo veiklą.

2025 m. KVTC pradėjo vykdyti įstaigos, atsakingos už „**Galileo**“[17] pagrindu sukurtos pasaulinės navigacijos palydovų sistemos paslaugos valstybės institucijoms ir įstaigoms teikimą, funkcijas.

Kibernetinio saugumo stiprinimas kaip atsakas į proveržio technologijų plėtrą

DI tampa reikšminga priemone viešojo sektoriaus veiklos efektyvumui, sprendimų kokybei ir organizaciniam atsparumui didinti. DI leidžia analizuoti didelius duomenų kiekius ir identifikuoti neįprastą sistemos elgseną realiuoju laiku. Tuo pačiu metu DI kelia naujų iššūkių, nes gali būti naudojamas sudėtingesnėms kibernetinėms atakoms, tokioms kaip socialinė inžinerija, kai siekiama išvilioti jautrius duomenis (angl. *Phishing*), ar kenkimo programų kūrimas. Todėl DI poveikis kibernetiniam saugumui dvejopas – DI tampa ir gynybos, ir puolimo įrankiu. Būtina nuosekliai stiprinti organizacijų gebėjimus įgyvendinti kibernetinio saugumo reikalavimus, valdyti su DI susijusias rizikas ir užtikrinti valstybei svarbių sektorių atsparumą kibernetinėms grėsmėms.

Atsižvelgiant į nacionalinius ir ES strateginius dokumentus DI srityje, 2025 m. KAM pradėtas nuoseklus DI taikymo galimybių, rizikų ir valdymo modelių vertinimas. 2025 m. spalio mėn. KAM sudaryta darbo grupė DI diegimo krašto apsaugos sistemoje ir KAM darbotvarkei parengti[18]. Darbo grupei pavesta įvertinti DI diegimo krašto apaugos sistemoje galimybes, nustatyti prioritetines sritis, reikalingus resursus ir kontrolės mechanizmus.

Valstybės kontrolės (toliau – VK) 2025 m. gegužės 9 d. **audito ataskaitoje Nr. VAE-6 „Dirbtinio intelekto valdymas viešajame sektoriuje“** rašoma, kad didžioji dalis viešojo sektoriaus subjektų, kurie taiko DI technologijas savo veikloje, neanalizuoja ir nevertina DI rizikos, nes rizikos analizės metodikos nepateikia rekomendacijų, kaip turi būti valdomos naujos DI keliamos grėsmės. Kad viešojo sektoriaus subjektai tinkamai valdytų DI riziką ir užtikrintų saugumą per visą DI gyvavimo ciklą, VK pateikė KAM rekomendaciją patobulinti kibernetinio saugumo informacinę sistemą taip, kad subjektai atlikdami kibernetinio saugumo rizikų vertinimo procedūras DI įsivertintų kaip vieną iš grėsmių. Atsižvelgiant į rekomendaciją, 2025 m. parengta ir patvirtinta **Kibernetinio saugumo rizikų vertinimo metodika**[19] buvo papildyta **DI rizikos vertinimu**.

17
Galileo – tai ES pasaulinė palydovinė navigacijos sistema, sukurta siekiant teikti labai tikslias padėties nustatymo ir laiko nustatymo paslaugas, nepriklausomai nuo kitų tarptautinių sistemų.

18
Lietuvos Respublikos krašto apsaugos ministro 2025 m. spalio 10 d. įsakymas Nr. V-949 „Dėl darbo grupės dirbtinio intelekto diegimo krašto apsaugos sistemoje ir Krašto apsaugos ministerijoje darbotvarkei parengti sudarymo“.

19
Kibernetinio saugumo rizikų vertinimo metodika paskelbta Kibernetinio saugumo informacinėje sistemoje (toliau – KSIS) ir prieinama tik kibernetinio saugumo subjektams.

Tobulėjant kvantiniams kompiuteriams, didėja grėsmė kriptografijai viešuoju raktu. Kriptografija yra duomenų šifravimo, elektroninio pasirašymo ir elektroninio autentifikavimo sprendimų pagrindas. Siekiant užtikrinti koordinuotą ES valstybių narių pasirengimą kvantinei erai ir laiku pereiti prie kvantiškai atsparios – **postkvantinės kriptografijos** (angl. *Post-Quantum Cryptography*, PQC)[20], 2025 m. birželio 11 d. Tinklų ir informacijos saugumo bendradarbiavimo grupės (angl. *NIS Cooperation Group*) Postkvantinės kriptografijos darbo grupė, kurios narys KAM atstovas, paskelbė **Koordinuoto perėjimo prie postkvantinės kriptografijos gaires**[21] (angl. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*). Gairės nustato etapus ir konkrečius uždavinius, kuriuos turi įgyvendinti visos ES valstybės narės. Gairėse pateikti pasiekimo rodikliai, leidžiantys vertinti pereinamojo laikotarpio pažangą ir užtikrinti nuoseklų postkvantinės kriptografijos įgyvendinimą visoje ES. 2025 m. KAM buvo sudaryta Nacionalinė perėjimo prie postkvantinės kriptografijos koordinavimo darbo grupė[22]. Ją sudarė atstovai iš skirtingų ministerijų, joms pavaldžių įstaigų, NKSC, taip pat ekspertai iš ypatingos svarbos ir kitų itin svarbių sektorių. Darbo grupė nustatė rizikos vertinimu pagrįstus perėjimo prie saugesnės, kvantiniams kompiuteriams atsparios kriptografijos etapus Lietuvoje, parengė nuoseklaus ir koordinuoto perėjimo prie postkvantinės kriptografijos proceso valdymo organizacijose gairių projektus[23]. Siekdama informuoti visuomenę apie kvantinių kompiuterių grėsmes, KAM 2025 m. vykdė įvairias komunikacijos veiklas: buvo publikuojami straipsniai, rekomendacijos, pranešimai žiniasklaidai bei parengtas dažniausiai užduodamų klausimų (DUK) rinkinys KAM svetainės skiltyje „**Postkvantinė kriptografija**“. Pradėta komunikacija per KAM sukurtą ir palaikomą komunikacijos kanalą **LinkedIn platformoje „Postkvantinės kriptografijos koordinavimas Lietuvoje“**. Kanalas naudingas kibernetinio saugumo specialistams, IT įmonių vadovams ir administratoriams, organizacijų bei projektų vadovams, technologijų ekspertams ir visiems, vienaip ar kitaip prisidedantiems prie perėjimo prie postkvantinės kriptografijos arba besirūpinantiems pasirengimu saugumo iššūkiams ateityje.

20

Postkvantinė kriptografija – nauji kriptografiniai metodai, atsparūs kvantinių kompiuterių atakoms.

21

Koordinuoto perėjimo prie postkvantinės kriptografijos gairės (angl. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*).

22

Lietuvos Respublikos krašto apsaugos ministro 2025 m. gegužės 22 d. įsakymas Nr. V-459 „Dėl Nacionalinės perėjimo prie postkvantinės kriptografijos koordinavimo darbo grupės sudarymo“.

23

2026 m. kovo 25 d. buvo patvirtintas Lietuvos Respublikos Vyriausybė nutarimas Nr. 185 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo“, kuriuo nustatoma pareiga kibernetinio saugumo subjektams pradėti planuoti ir įgyvendinti nuoseklių perėjimą prie postkvantinės kriptografijos nutarime nustatytais terminais.

Dalyvavimas formuojant ir įgyvendinant ES kibernetinio saugumo politiką

TIS 2 direktyvos nuostatos įpareigoja valstybes nares užtikrinti veiksmingą **kibernetinių krizių valdymą**, įskaitant strateginį koordinavimą ir operatyvų informacijos apsikeitimą nacionaliniu ir ES lygmenimis. Šiame kontekste svarbų vaidmenį atlieka **ES ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas** (angl. *European Cyber Crisis Liaison Organisation Network* (toliau – **EU-CyClone**), skirtas koordinuotam reagavimui į didelio masto kibernetinio saugumo krizes ES.

KAM atstovai 2025 m. dalyvavo EU CyCLONe susitikimuose, kuriuose buvo aptartas naujasis ES krizių valdymo mechanizmas, numatytas 2025 m. birželio 6 d. ES Tarybos priimtoje rekomendacijoje dėl **ES kibernetinio saugumo krizių valdymo plano** (angl. *EU Blueprint on Cybersecurity Crisis Management*)[24]. Šio plano tikslas – užtikrinti koordinuotą ir savalaikį ES institucijų bei valstybių narių veikimą didelio masto kibernetinių krizių metu. KAM atstovai dalyvavo dvejose CyCLONe organizuotose kasmetinėse kibernetinių krizių valdymo pratybose: „Blue Olex 2025“ ir „SOPEX 2025“. Pratybose gilintas standartinių veiklos procedūrų (angl. *Standard Operating Procedure,* SOP) supratimas ir efektyvus jų taikymas didelio masto kibernetinių incidentų atveju ES. Pratybos simuliavo įvairius kibernetinius incidentus, paveikusius visą ES.

2025 m. ES aktyviai naudojo **kibernetinės diplomatijos** priemones, siekdama stiprinti tarptautinį bendradarbiavimą per kibernetinius dialogus su partneriais. Tokie dialogai leidžia ES aptarti kylančias kibernetines grėsmes ir plėtoti bendradarbiavimą kibernetinio saugumo srityje. 2025 m. ES surengti kibernetiniai dialogai su bendramintėmis partnerėmis – Jungtine Karalyste, Ukraina, Brazilija, Pietų Korėja, Indija ir Persijos įlankos bendradarbiavimo Taryba. ES valstybės narės 2025 m. sausio 27 d. sankcionavo dar 3 Rusijos karinės žvalgybos pareigūnus dėl aktyviai rengiamų kibernetinių išpuolių prieš Estijos institucijas. Šiuo metu į ES sankcijų sąrašą įtraukta 17 fizinių asmenų ir 4 juridiniai asmenys, keliantys grėsmę ES valstybėms (jiems taikomos ribojamosios priemonės). 2025 m. ES pratęsė ES sankcijų mechanizmo taikymą dėl kibernetinių atakų ir nusikalstamos veiklos elektroninėje erdvėje iki 2026 m. gegužės 18 d. Solidarizuodamosi su Jungtine Karalyste, ES valstybės narės 2025 m. gruodžio 9 d. pasmerkė dvi Kinijos kibernetinio saugumo įmones, kurios vykdė kibernetines atakas prieš Jungtinės Karalystės ir kitų valstybių partnerių sistemas. ES, siekdama atgrasyti trečiųjų šalių ir nusikalstamų veikėjų keliamas kibernetines grėsmes bei atakas prieš ES ir jos valstybes nares, tęsė 2019 m. įtvirtintų ribojamųjų priemonių taikymą, t. y. įtraukimą į ES sankcijų taikymo sąrašą.

24

2025 m. birželio 6 d. ES Tarybos rekomendacija dėl ES kibernetinio saugumo krizių valdymo plano.

Per PESCO ES valstybės narės kartu kuria ES kibernetinės gynybos pajėgumus. Lietuva nuo 2018 m. vadovauja **PESCO projektui**. Jo 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.

2025 m. PESCO projekto koordinavimą iš Lietuvos perėmė Belgija, ji vadovavo reagavimo komandų operacinėms veikloms – organizavo pajėgų pratybas, mokymus, reagavimo į paramos prašymus veiksmus ir surengė metinį PESCO projekto Tarybos susitikimą Gente.

2025 m. **Kibernetinės greitojo reagavimo pajėgos** buvo aktyvuotos 2 kartus – dalyvavo ES mokymo misijoje Somalyje, kur vykdė misijos tinklų pažeidžiamumo vertinimą, ir vyko į Moldovą atlikti Moldovos valstybės institucijų tinklų pažeidžiamumo vertinimo ir prisidėti prie Moldovos parlamento rinkimų kibernetinio saugumo užtikrinimo.

PESCO projekte jau dalyvauja 12 ES valstybių narių[25], Kibernetinės greitojo reagavimo pajėgos didina galimybes reaguoti į daugiau kibernetinių incidentų vienu metu tiek ES valstybėse narėse, tiek ES institucijose, misijose ir operacijose bei šalyse partnerėse. Prie PESCO projekto prisijungiant vis daugiau narių ir daugėjant pajėgumų pasitelkimo atvejų, projektas susilaukia vis daugiau dėmesio iš kitų ES valstybių narių, taip pat ir iš ES institucijų. PESCO projektas įtraukiamas į įvairius ateities planavimo scenarijus, susijusius su ES kibernetine gynyba, kibernetinio saugumo užtikrinimu ir reagavimu į galimus incidentus ES šalyse, institucijose bei ES bendrosios saugumo ir gynybos politikos misijos ir operacijose.

2025 m. buvo toliau tęsiamas bendradarbiavimas su **Moldova** kibernetinio saugumo ir kibernetinės gynybos srityse. Moldova susiduria su tokiomis pačiomis kibernetinėmis grėsmėmis iš Rusijos kaip ir Lietuva. Todėl glaudus dvišalis Lietuvos ir Moldovos bendradarbiavimas sudaro prielaidas sistemingam informacijos apsikeitimui, geriųjų praktikų ir patirties dalijimuisi bei abipusei pagalbai. Bendradarbiavimas prisideda prie abiejų valstybių kibernetinio saugumo ekspertų kompetencijų stiprinimo ir kibernetinių atakų atrėmimo. 2025 m. KAM, NKSC ir LK KGV atstovai lankėsi Moldovoje ir susitiko su pagrindinių Moldovos kibernetinio saugumo institucijų atstovais (tiek kariniame, tiek civiliniame sektoriuje). Vizitų metu buvo aptarti Moldovos kibernetinės aplinkos iššūkiai (pavyzdžiui, koordinuotos dezinformacijos kampanijos ir kibernetinės atakos Moldovos rinkimų metu), turimi instituciniai pajėgumai ir galimos praktinio bendradarbiavimo kryptys. Moldova 2025 m. pasinaudojo Kibernetinių greitojo reagavimo pajėgų teikiama parama, kuri padėjo stabilizuoti situaciją ir sustiprinti kibernetinį atsaką.

25
PESCO projekto dalyviai: Estija, Kroatija, Lenkija, Lietuva, Nyderlandai, Rumunija, Belgija, Slovėnija, Danija, Austrija, Latvija ir Italija. Stebėtojo teisėmis PESCO projekte dalyvauja Graikija, Prancūzija, Ispanija ir Suomija.

Dvišalio bendradarbiavimo su ES valstybėmis narėmis stiprinimas ir plėtra

Dvišalis bendradarbiavimas kibernetinio saugumo srityje buvo formuojamas pagal pagrindines XX Vyriausybės numatytas veiklos kryptis ir jas atitinkantį 2025 m. KAM veiklos planą. Strateginėmis partnerėmis išliko Vokietija, Lenkija ir Baltijos šalys. Siekdama įgyvendinti numatytus tikslus KAM kartu su kitomis institucijomis – Užsienio reikalų ministerija (toliau – URM), NKSC, LK KGV rengė kibernetinio saugumo dvišalius susitikimus, konsultacijas bei dialogus. Susitikimų metu aptartos pagrindinės bendradarbiavimo kryptys su artimiausiais regiono kaimynais, rengtos konsultacijos svarbiausiais ES kibernetinio saugumo ir teisėkūros darbotvarkės klausimais, dvišalio bendradarbiavimo gairės.

2025 m. KAM skyrė daug dėmesio regioninio bendradarbiavimo stiprinimui, ypač su **Lenkija** kaip su strategine Lietuvos partnere, turinčia vienodus kibernetinio saugumo interesus. Šio prioriteto įgyvendinimo kontekste buvo parengtas **Lietuvos ir Lenkijos bendradarbiavimo kibernetinio saugumo srityje gairių projektas** (angl. *Lithuania–Poland Roadmap for Cooperation in Cybersecurity Area for 2026–2029*). Jis numato sistemingą koordinaciją tarp abiejų valstybių kibernetinės gynybos struktūrų, civilinių kibernetinių pajėgumų stiprinimą, informacijos mainus, taip pat bendrų pratybų ir mokymų organizavimą. 2026 m. bus siekiama patvirtinti šias bendradarbiavimo gaires ir sukurti ilgalaikio Lietuvos ir Lenkijos dvišalio bendradarbiavimo pagrindą kibernetinio saugumo srityje.

2025 m. sausio mėn. įvyko KAM ir **Latvijos** gynybos ministerijos dvišalės konsultacijos dėl kibernetinio saugumo: apsikeista informacija ir patirtimi dėl TIS 2 direktyvos įgyvendinimo nacionaliniu lygiu, aptarti jos praktinio įgyvendinimo iššūkiai. Konsultacijų metu taip pat buvo įvertintos glaudesnio bendradarbiavimo galimybės, įskaitant reguliarių Baltijos šalių (3B) kibernetinio saugumo direktorių konsultacijų formatą, bendradarbiavimą vykdant kibernetinių grėsmių paieškos operacijas (angl. *Cyber Threat Hunt*[26]), prisidedančias prie regioninio kibernetinio atsparumo stiprinimo ir glaudesnio Lietuvos ir Latvijos ryšio palaikymo.

2025 m. Lietuva siekė plėtoti bendradarbiavimo galimybes ir su Šiaurės Europos valstybėmis. 2025 m. kovo mėn. surengtas pirmasis dvišalis susitikimas su **Suomijos** gynybos ministerijos ir Kibernetinės valdybos atstovais. Buvo pristatyta Lietuvos kibernetinio saugumo ekosistema ir susipažinta su Suomijos pagrindinių institucijų, atsakingų už kibernetinio saugumo užtikrinimą, veiklomis, aptartos platesnės bendradarbiavimo galimybės kibernetinio saugumo ir kibernetinės gynybos srityse.

26 Kibernetinių grėsmių paieškos operacijos (angl. *Cyber Threat Hunt*) – tai kryptinga veikla kenkimo ar įtartinai veiklai organizacijos sistemose aptikti.

Tarptautinio bendradarbiavimo stiprinimas ir iniciatyvos

2025 m. buvo toliau vystomas dvišalis bendradarbiavimas su **JAV** pagal 2024 m. lapkritį patvirtintą **JAV ir Lietuvos 2025–2029 m. bendradarbiavimo kibernetinio saugumo ir kibernetinės gynybos srityje planą**, tęsiamas krašto apsaugos sistemos kibernetinio saugumo specialistų praktinis bendradarbiavimas su JAV Pensilvanijos nacionaline gvardija (angl. *Pennsylvania National Guard,* PANG) ir JAV karinių pajėgų Europoje vadaviete (angl. *U.S. European Command*, USEUCOM. Bendradarbiavimas ypatingai svarbus ugdant praktinius Lietuvos organizacijų kibernetinio saugumo ekspertų įgūdžius. Pavyzdžiui, nuo 2022 m. NKSC ir JAV kibernetinio saugumo vadavietės (angl. *US CYBERCOM*) ekspertai kartu įvykdė 5 kibernetinių grėsmių paieškos operacijas (angl. *Cyber Threat Hunt*) – 2025 m. tokia operacija įvykdyta URM tinkluose. 2025 m. pradėti vykdyti KAM ir JAV karinių pajėgų Europoje vadavietės bendradarbiavimo gairėse numatyti ekspertų mokymai, jie tęsis ir 2026 m. Šie ir kiti JAV ekspertų mokymai ir patirties dalijimasis bei NKSC nuo 2025 m. pradėtos vykdyti aktyvios grėsmių paieškos operacijos stiprina atsparumą kibernetinėms grėsmėms. 2025 m. lapkričio – 2026 m. sausio mėn. JAV laivyno aukštoji mokykla vykdė kibernetinio saugumo mokymus 40 dalyvių: Ukrainos kibernetinio saugumo ekspertams, Lietuvos kritinės infrastruktūros kibernetinių incidentų valdytojams ir Lietuvos kariuomenės kibernetinio saugumo ekspertams.

2025 m. pradėtas bendradarbiavimas su **Kanada**. Ji demonstruoja augantį strateginį interesą Baltijos regione ir turi daug kompetencijų kibernetinių grėsmių paieškos srityje. 2025 m. įvyko praktiniai bei strateginiai susitikimai su Kanados kariuomenės atstovais, o 2025 m. balandį po pirmųjų Lietuvos ir Kanados konsultacijų dėl kibernetinio saugumo dvišaliai ryšiai suintensyvėjo. Pavyzdžiui, Kanados kariuomenės Kibernetinės valdybos ekspertai dalyvavo didžiausiose Lietuvos kariuomenės organizuojamose kibernetinės gynybos pratybose „Gintarinė migla“. Be to, siekiama Kanados kibernetinio saugumo centro atstovų (angl. *Canadian Centre for Cyber Security,* CCCS) įtraukimo į Nacionalinio kibernetinio saugumo centro veiklas, apimančias kibernetinių grėsmių paieškos operacijas, kibernetinių grėsmių analizę bei programinės ir techninės įrangos mokslinius tyrimus.

Lietuva, glaudžiai bendradarbiaudama kibernetinio saugumo srityje su bendramintėmis **Indijos ir Ramiojo vandenynų regiono šalimis**[27], prisideda prie bendro ES, NATO ir Indijos ir Ramiojo vandenynų regiono valstybių kibernetinio saugumo stiprinimo reaguojant į vis didėjančios rizikas kibernetinėje erdvėje, kylančias iš Rusijos, Kinijos, Šiaurės Korėjos ir Irano.

27 Japonija, Australija, Pietų Korėja, Singapūras, Filipinai ir Taivanas.

2025 m. krašto apsaugos sistemos atstovai tęsė intensyvias aukšto lygio ir praktinio pobūdžio konsultacijas su bendramintėmis Indijos ir Ramiojo vandenynų regiono šalimis, taip pat dalyvavo bendrose kibernetinės gynybos pratybose. Vienas didžiausių pasiekimų – 2025 m. pavasarį nuotoliu surengtos pirmosios Lietuvos ir Australijos kibernetinės konsultacijos. Jose dalyvavo abiejų šalių kibernetinių institucijų atstovai bei buvo sutarta 2026 m. pavasarį susitikti Vilniuje.

2025 m. KAM vadovybė vyko dvišalių vizitų į Pietų Korėją bei Singapūrą, kad sustiprintų bendradarbiavimą kibernetinio saugumo srityje – keitėsi informacija apie kibernetinio saugumo grėsmes ir piktavalius bei jų technikas, taktikas ir procedūras. Panašūs dialogai 2026 m. planuojami ir su kitomis regiono partnerėmis.

2025 m. lapkričio mėn. Vilniuje vyko dvyliktosios tarptautinės kibernetinio saugumo pratybos „Gintarinė migla 2025“. Pratybose dalyvavo ir Indijos ir Ramiojo vandenynų regiono valstybių – Japonijos, Pietų Korėjos, Taivano, Singapūro ir Filipinų – atstovai (kaip dalyviai ir stebėtojai). Tai nuoseklus Lietuvos siekis tęsti bendradarbiavimą ir stiprinti partnerystę su Indijos ir Ramiojo vandenyno regionu kibernetinio saugumo srityje.

Lietuvos inicijuotas aukšto lygio NATO, Indijos ir Ramiojo vandenynų regiono ir partnerių šalių **kibernetinio saugumo forumas „Cyber Champions Summit“** 2023 m. pirmą kartą surengtas Vilniuje, pakartotas Australijoje 2024 m. ir 2025 m. suorganizuotas Pietų Korėjoje. Tai svarbiausias NATO bendradarbiavimo su Indijos ir Ramiojo vandenynų regiono šalimis projektas NATO kibernetinės gynybos kontekste.

Lietuva dalyvauja **tarptautinėje iniciatyvoje „Iniciatyva prieš išpirkos reikalaujančias atakas“** (angl. *Counter Ransomware Initiative*, CRI). Tai aukšto lygio daugiausia šalių vienijanti iniciatyva, sujungianti 71 valstybę ir tarptautinę organizaciją, siekiant bendromis pastangomis kovoti su išpirkos reikalaujančiomis kibernetinėmis atakomis. Lietuvos atstovai iš KAM ir NKSC yra vieni iš 6 šios iniciatyvos lyderių ir kartu su Australija yra atsakingi už informacijos dalinimosi gairių rengimą ir patvirtinimą. 2025 m. kasmetiniame iniciatyvoje dalyvaujančių valstybių susitikime Singapūre šios informacijos dalinimosi gairės buvo patvirtintos.

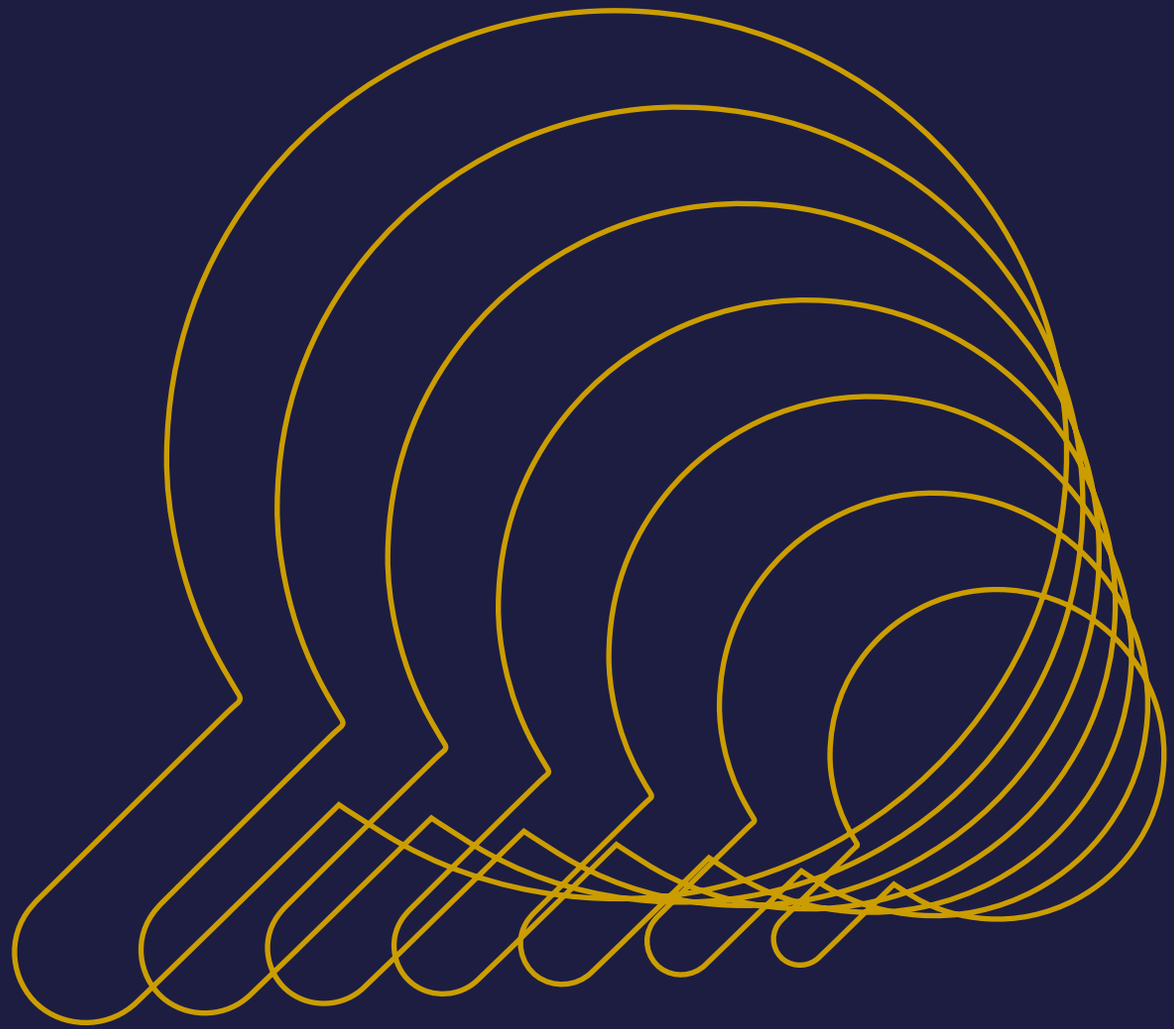
Kibernetinės gynybos kaip NATO atgrasymo ir gynybos dalies stiprinimas

Atsižvelgiant į specifinius kibernetinės erdvės karinio planavimo ir operacijų vykdymo poreikius, atskirose NATO šalyse sąjungininkėse kuriamos kibernetinės pajėgos, tam tikri pokyčiai vykdomi ir NATO štabuose. 2025 m. toliau vystytas **NATO integruotos kibernetinės gynybos centras** (angl. *NATO Integrated Cyber Defence Centre*, NICC), siekiant pagerinti tinklų apsaugą, situacijos suvokimą ir kibernetinės erdvės, kaip vieno iš operacinių domenų, įgalinimą. Šis centras sujungs Aljanso kibernetines struktūras, karinius ir civilinius dėmenis, įtrauks šalių sąjungininkių atstovus.

Lietuva aktyviai prisideda prie Aljanso kibernetinės gynybos politikos formavimo, kibernetinių pajėgumų stiprinimo, dalyvauja kibernetinės gynybos pratybose ir iniciatyvose. 2025 m. NATO viršūnių susitikime Hagoje, Nyderlandų Karalystėje, buvo priimtas sprendimas, įpareigojantis NATO šalis nares iki 2035-ųjų kasmet skirti 5 proc. bendrojo vidaus produkto (toliau – BVP) gynybai, iš kurių iki 1,5 proc. BVP skirti priemonėms, reikalingoms kritinės infrastruktūros apsaugai, tinklų gynybai, civilių pasirengimui ir atsparumui, inovacijoms bei gynybos pramoninės bazės stiprinimui. Į 1,5 proc. BVP patenka ir kibernetinio saugumo priemonės. Toks sprendimas parodo NATO narių pasiryžimą užtikrinti pakankamą finansavimą gynybai, atsižvelgiant į kintančią geopolitinę situaciją.

04

Lietuvos kibernetinio saugumo būklės apžvalga



NKSC veiklos apžvalga ir kibernetinio saugumo tendencijos

Antanas Aleknavičius,
NKSC prie KAM direktorius

Vadovo žodis

Lietuvos kibernetinio saugumo situacija 2025 m. išliko stabili, matomas bendras kibernetinės brandos ir atsparumo augimas. Tai siejama su kryptinga NKSC veikla, įgyvendinant Kibernetinio saugumo įstatymo nuostatas ir stiprinant kelis kartus išaugusio kibernetinio saugumo subjektų skaičiaus pasirengimą jas įgyvendinti. 2025 m. balandžio mėn. sudarėme kibernetinio saugumo subjektų registrą, į jį įtraukta daugiau kaip 1400 organizacijų. Stiprindami jų atsparumą, automatizavome informavimą apie nutekėjusius prisijungimo duomenis ir pradėjome rengti kibernetinių grėsmių sektorių ataskaitas. Tuo pačiu metu pradėjome kurti naują nacionalinę Kibernetinių incidentų valdymo platformą, į kurią 2026 m. bus pradėti jungti kibernetinio saugumo subjektų Saugumo operacijų centrai, ir duomenų apsikeitimas taps automatizuotas. Žvelgiant į 2026 m., vienas iš svarbesnių darbų bus pirmasis kibernetinio saugumo subjektų brandos vertinimas ir jų Saugumo operacijų centrų duomenų integravimas į NKSC duomenų srautą. Taip pat nuosekliai stiprinsime NKSC, kaip pagrindinio kibernetinio saugumo subjekto, vaidmenį nacionaliniu lygiu.

1 443
organizacijos, įtrauktos į Kibernetinio saugumo subjektų registrą.

25 %
mažiau kibernetinių incidentų nei 2024 m.

70 000
Nacionalinė DNS užkarda užblokavo virš 70 tūkst. žalingų domenų.

52 000
asmenų baigė NKSC siūlomus mokymus 2025 m. Parengtos 5 naujos mokymų programos.

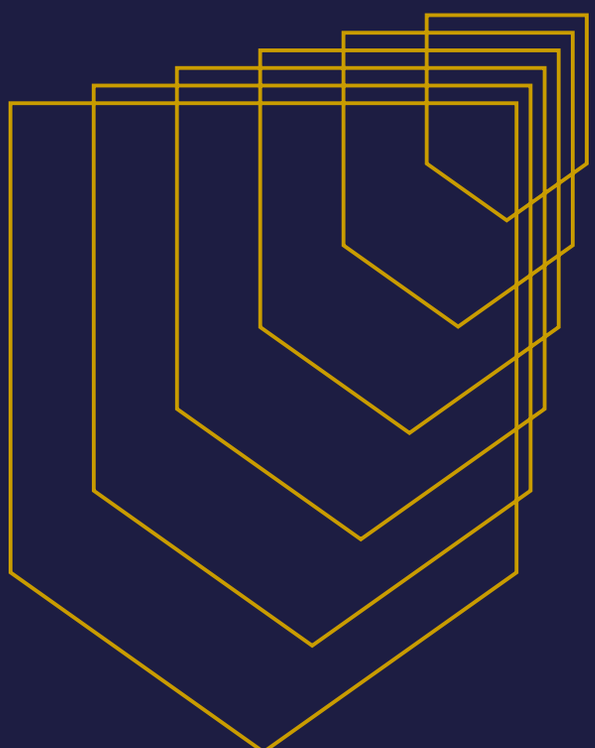
NKSC vaidmuo nacionalinėje kibernetinio saugumo ekosistemoje

NKSC – pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už vieningą kibernetinių incidentų, grėsmių ir pažeidžiamumų valdymą, kibernetinio saugumo subjektų (toliau – KSS) atitikties teisės aktų nustatytiems reikalavimams įgyvendinimo stebėseną ir kontrolę, informacinių išteklių kibernetinį saugumą bei išteklių akreditaciją ir visuomenės kibernetinio saugumo kompetencijų stiprinimą.

2025 m. išmoktos pamokos, aplinkos pokyčiai, darę įtaką NKSC veiklai

2025 m. NKSC veiklos sričių apimčiai reikšmingą įtaką darė kibernetinio saugumo teisinio reglamentavimo pokyčiai, išaugęs KSS skaičius, kintančios kibernetinės grėsmės. Šie pokyčiai lėmė žymiai didesnę veiklos apimtį priežiūros bei metodinės pagalbos srityse, aukštos kvalifikacijos darbuotojų poreikį bei būtinybę stiprinti tarpinstitucinį ir tarptautinį bendradarbiavimą.

Svarbus funkcijų konsolidavimo vienoje organizacijoje pokytis, leidęs sustiprinti kibernetinio saugumo organizavimą, įvyko 2025 m. sausio 1 d., NKSC perėmus Nacionalinės šifrų paskirstymo ir Apsaugos nuo elektromagnetinės spinduliuotės (TEMPEST) tarnybų funkcijas, susijusias su įslaptintos informacijos ryšių ir informacinių sistemų saugos reikalavimų įgyvendinimu, kriptografinių priemonių apsauga ir apsauga nuo elektromagnetinės spinduliuotės.



Kibernetinių incidentų mažėjo, tačiau socialinės inžinerijos grėsmės išlieka reikšmingos

Šiame skyriuje pateikiami apibendrinti 2025 m. NKSC sukaupti statistiniai duomenys ir informacija apie bendrą kibernetinių grėsmių situaciją Lietuvoje. NKSC kibernetinių grėsmių paveikslą analizuojanti informacija ir duomenys pagal KSĮ nurodytus ypatingos svarbos ir kitus itin svarbius sektorius pateikti šios ataskaitos priede „Grėsmių žemėlapis“ (toliau – ataskaitos priedas).

NKSC registruotų kibernetinių incidentų dinamika

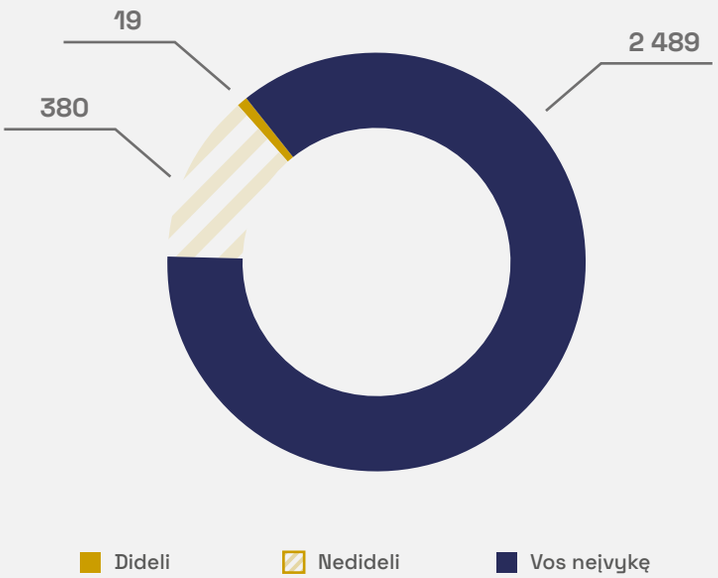
2025 m. NKSC užregistravo 2888 **kibernetinius incidentus**[01], iš kurių 19 buvo priskirti **dideliems**, 380 – **nedideliems** ir 2489 – **vos neįvykusiems incidentams** (**1 pav.**). NKSC tokį pasiskirstymą vertina teigiamai, kadangi didelių incidentų registruota nedaug, nedidelių incidentų kiekis buvo pakankamai reikšmingas, bet šių incidentų padariniai dažniausiai didelės žalos nesukėlė, o didžiąją dalį sudarė vos neįvykę incidentai, kurie buvo laiku užkardyti ir jokios įtakos neturėjo.

Palyginus su 2024 m., kai buvo užregistruoti 3874 kibernetiniai incidentai, 2025 m. fiksuojamas bendro incidentų skaičiaus sumažėjimas 25 proc. NKSC vertinimu, incidentų skaičiaus sumažėjimas negali būti vertinamas vienareikšmiškai, nes įtakos galėjo turėti kelios priežastys. NKSC **blokuojamų domenų valdymo sistemoje „Vasaris“** užblokavo virš 70 tūkst. žalingų domenų ir taip apsaugojo daugybę Lietuvos interneto naudotojų nuo socialinės inžinerijos keliamų grėsmių. NKSC matomas organizacijų sąmoningumo didėjimas ir diegiamos apsaugos priemonės, padedančios laiku aptikti grėsmes ir užkirsti kelią incidentams, yra dar viena teigiama incidentų mažėjimo priežastis. Deja, kitos incidentų skaičiaus mažėjimo priežastys gali būti susijusios su 2024 m. spalio mėn. įsigaliojusiu atnaujintu KSĮ, kurio nuostatos galimai nėra teisingai suprastos ir todėl KSS vangiau praneša apie įvykusius kibernetinius incidentus.

01

2024 m. lapkričio 12 d. įsigaliojus Nacionaliniam kibernetinių incidentų valdymo planui, patvirtintam **Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“**, pasikeitė kibernetinių incidentų klasifikavimo tvarka. Incidentai skirstomi į didelius, nedidelius ir vos neįvykusius incidentus.

2025 m. registruoti kibernetiniai incidentai, vnt.

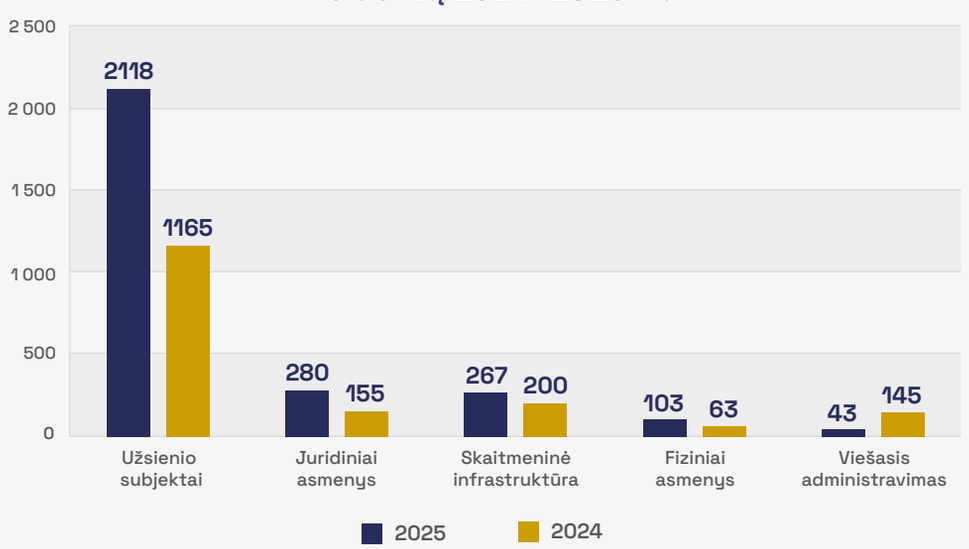


< 1 pav.

2025 m. registruoti kibernetiniai incidentai, vnt. *(šaltinis – NKSC)*

2025 m. dauguma kibernetinių incidentų buvo susiję su **užsienio subjektų**[02] **prieglobos paslaugų infrastruktūra** – užfiksuota 2118 incidentų, ir tai reikšmingai lenkia kitas sritis, kuriose buvo fiksuoti incidentai. Gerokai mažesnis incidentų skaičius fiksuotas Lietuvos juridinių asmenų[03] informacinėse sistemose (280), skaitmeninėje infrastruktūroje (267) ir tarp fizinių asmenų[04] (103) (**2 pav.**).

5 sritys, kuriose fiksuota daugiausiai kibernetinių incidentų 2024–2025 m.



< 2 pav.

5 sritys, kuriose fiksuota daugiausia incidentų 2024–2025 m. *(šaltinis – NKSC)*

02 Užsienio subjektas – užsienio šalies prieglobos arba interneto paslaugos teikėjas, kurio infrastruktūroje būna nesaugios interneto svetainės arba kenkėjiškas programinis kodas.

03 Juridinis asmuo – juridiniai asmenys, ne kibernetinio saugumo subjektai.

04 Fiziniai asmenys – Lietuvos ar užsienio šalių piliečiai.

Tiek 2024 m., tiek 2025 m. užsienio subjektų prieglobos paslaugų infrastruktūroje fiksuojamų incidentų skaičius ir toliau išlieka didelis (2024 m. – 1165). Toks pasiskirstymas rodo, kad reikšminga kenkėjiškos veiklos dalis yra susijusi su užsienyje veikiančia infrastruktūra, kuri naudojama kenkėjiškam turiniui skelbti ir platinti, ir tai apsunkina reagavimą ir tarptautinį bendradarbiavimą.

Lietuvos juridinių asmenų informacinėse sistemose fiksuojamų incidentų skaičius ir toliau auga – nuo 155 atvejų 2024 m. iki 280 atvejų 2025 m. Dažniausiai šie incidentai susiję su socialine inžinerija, pagrindinės jų priežastys – nepakankamas darbuotojų budrumas, saugumo žinių trūkumas ir žmogiškosios klaidos. Tai rodo, kad didžiausia rizika vis dar kyla ne dėl technologijų, o dėl žmonių elgsenos. Svarbu pabrėžti, kad čia kalbama apie Lietuvoje registruotus juridinius asmenis, kurie nepatenka į KSĮ reguliuojamus sektorius. Tendencijos šioje srityje iš esmės atitinka bendrą Lietuvos kibernetinių incidentų statistiką – vyrauja socialinės inžinerijos atvejai.

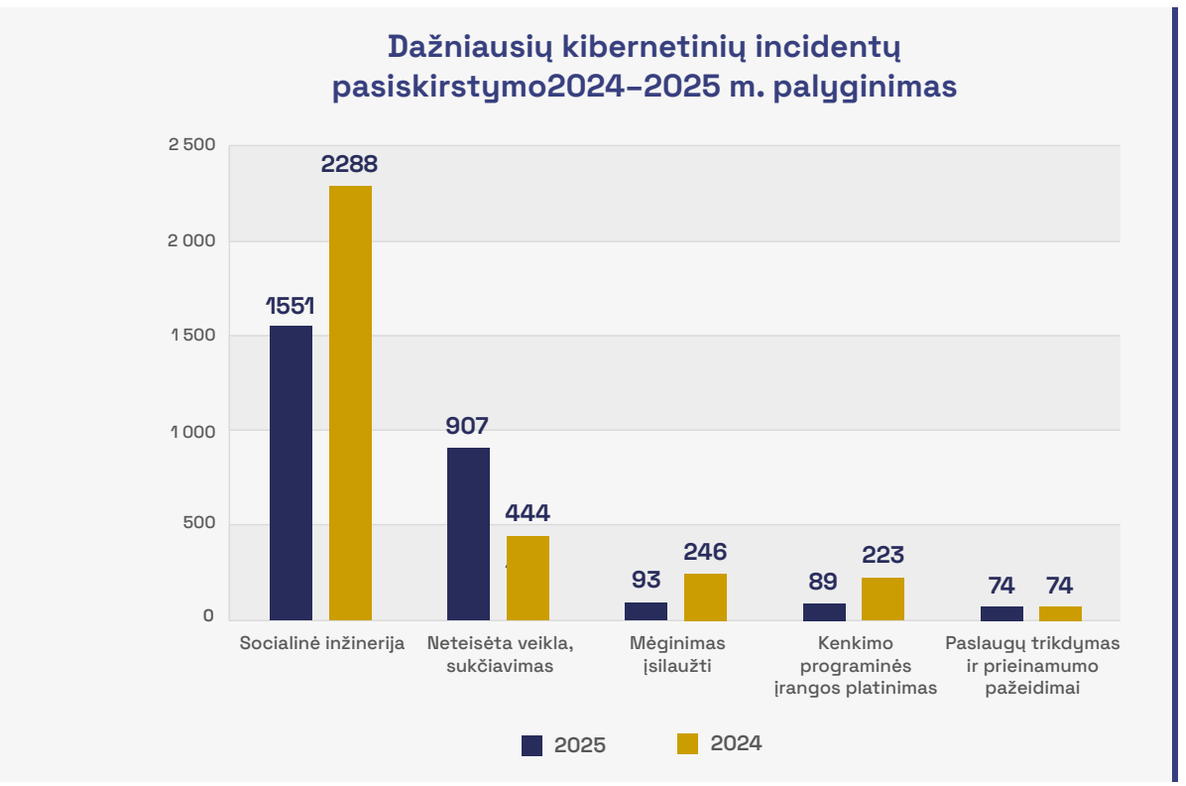
Lietuvos skaitmeninėje infrastruktūroje (pvz., debesijos, prieglobos paslaugų teikėjų, telekomunikacijų įmonių ir kt.) incidentų skaičius taip pat išlieka reikšmingas (267). Šioje srityje fiksuoti incidentai, susiję su paslaugų trikdymu, bandymais įsilaužti ar įvairiais veiklos trikdžiais. Skaitmeninė infrastruktūra tampa ne tik atakų taikiniu, bet ir platforma, per kurią gali būti vykdomos tolesnės kibernetinės atakos. Didelė dalis incidentų patenka į grupę *„Kitos kategorijos“*, t. y. nepriskiriama konkrečioms **Nacionalinio kibernetinių incidentų valdymo plano** grėsmių kategorijoms. Tai rodo, kad incidentų pobūdis būna įvairus ir ne visada lengva incidentus suklasifikuoti. Jų priežastys gali būti labai skirtingos – nuo žmogiškųjų klaidų iki techninių sutrikimų ar net išorinių veiksnių, tokių kaip gamtos reiškiniai.

Fiziniai asmenys, patiriantys incidentus, dažniausiai yra Lietuvos Respublikos piliečiai. Jie nukenčia dėl įvairialypės socialinės inžinerijos, susijusios su investiciniu sukčiavimu, suklastotomis internetinėmis parduotuvėmis ar apgaulės būdu gauta prieiga prie el. bankininkystės.

Pažymėtina, kad šioje dalyje nurodyta bendra visų NKSC registruotų kibernetinių incidentų statistika apima užsienio subjektus, Lietuvos juridinius ir fizinius asmenis bei kibernetinio saugumo subjektus, kurie pranešė apie kibernetinius incidentus. Ataskaitos priede pateikiama papildoma analizė, kurioje vertinami tik ypatingos svarbos ir kituose itin svarbiuose sektoriuose įvykę dideli ir nedideli incidentai, ir dėl šios priežasties ataskaitos priede pateikiami incidentų statistiniai duomenys nelygintini su bendrosios statistikos duomenimis.

Socialinė inžinerija – pagrindinė grėsmė, sparčiai daugėja sukčiavimo atvejų

Tiek 2025 m., tiek 2024 m. NKSC daugiausia registravo **socialinės inžinerijos principais grįstų kibernetinių incidentų**. 2025 m. šio tipo incidentai (1551) sudarė 54 proc. visų registruotų incidentų (2024 m. – 59 proc.). Tačiau 2025 m. beveik trečdaliu (32 proc.) sumažėjo šio tipo incidentų skaičius (2024 m. – 2 288) (**3 pav.**). NKSC šį pokytį sieja tiek su sėkminga kenkėjiškų domenų blokavimo veikla, tiek su didėjančiu interneto naudotojų budrumu, tiek ir su didėjančia organizacijų branda bei sėkmingai diegiamomis apsaugos priemonėmis. Tačiau nepaisant registruotų šio tipo incidentų skaičiaus mažėjimo, socialinės inžinerijos atvejai vis dar kelia didelę grėsmę organizacijoms ir fiziniams asmenims.



< 3 pav.

Dažniausių kibernetinių incidentų pasiskirstymo 2024–2025 m. palyginimas *(šaltinis – NKSC)*

Pastebima, kad nusikaltėliai pasitelkia personalizuotas žinutes, imituoja oficialių institucijų svetaines ir kuria itin realistiškus, į kasdienes situacijas panašius scenarijus. Pavyzdžiui, piktavaliai naudojo „Google“ paieškos variklio reklamos paslaugas (angl. *Google Ads*), kai kenkėjiškos svetainės „Google“ paieškos rezultatuose atsiranda aukštesnėse pozicijose nei oficialių institucijų ar paslaugų teikėjų svetainės. Tokiais atvejais vartotojai, ieškodami konkrečių paslaugų ir neatkreipdami dėmesio į svetainės adresą, patenka į kenkėjiškas svetaines ir gali netekti jautrių duomenų.

NKSC, siekdamas ugdyti darbuotojų gebėjimą atpažinti socialinės inžinerijos laiškus ir tinkamai į juos reaguoti, 2025 m. surengė 4 imitacines socialinės inžinerijos pratybas, per kurias KSS darbuotojams iš viso buvo išsiųsta daugiau kaip 448 tūkst. imitacinių laiškų ir 610 kartų buvo tikrinamas darbuotojų gebėjimas atpažinti socialinės inžinerijos metodais sukurtus el. laiškus.

NKSC ragina organizacijas nuolatos ugdyti savo darbuotojų atsparumą kibernetinėms grėsmėms ir periodiškai organizuoti įvairias pratybas, tarp kurių turėtų būti ir imitacinių socialinės inžinerijos atakų. Ilgametė NKSC pratybų organizavimo patirtis rodo, kad dalis sąmoningų darbuotojų apie gautus įtartinus el. laiškus informuoja ne tik savo organizacijos kibernetinio saugumo specialistą, bet ir kitas valstybės institucijas. NKSC teikia rekomendacijas[05], kaip saugiai organizuoti imitacines socialinės inžinerijos pratybas savo darbuotojams.

2025 m. aktualia grėsme išlieka ir nuosekliai didėja **neteisėta veikla, sukčiavimas**[06] –šių incidentų skaičius 2025 m. padidėjo 104 proc. (2024 m. – 444, 2025 m. – 907). Didėjant sukčiavimo mastams, nusikaltėliai sparčiau išnaudoja skaitmenines paslaugas, socialinės inžinerijos metodus ir vartotojų sąmoningumo spragas, nei saugumo priemonės spėja prisitaikyti.

2025 m., palyginus su 2024 m., žymiai sumažėjo **mėginimų įsilaužti** (angl. *Intrusion Attempts*) (2024 m. – 246, 2025 m. – 93) ir **kenkimo programinės įrangos platinimo** incidentų (2024 m. – 223, 2025 m. – 89).

Paslaugų trikdymo ir prieinamumo pažeidimų grupėje situacija 2025 m. išliko stabili (2024 m. – 74, 2025 m. – 74).

Stiprindami bendradarbiavimą ir siekdami užtikrinti automatizuotą duomenų apsikeitimą apie kibernetinius incidentus **finansų sektoriuje** ir greitesnį reagavimą į grėsmes, **NKSC** su **Lietuvos banku** 2025 m. liepos 28 d. pasirašė **bendradarbiavimo susitarimą**. Susitarimo tikslas – šalims bendradarbiauti ir keistis kibernetinio saugumo informacija, kad būtų užtikrintas glaudus finansų sektoriaus ir kitų ypatingos svarbos sektorių kibernetinio saugumo sistemos ryšys ir Lietuvoje padidėtų bendras kibernetinio saugumo lygis. NKSC indėlis – suteikti Lietuvos bankui prieigą prie Kibernetinio saugumo informacinės sistemos[07] (toliau – KSIS) (grėsmių indikatorių mainų platformos, bandomosios aplinkos (angl. *Sandbox*), saugios duomenų apsikeitimo terpės ir kt.) ir Nacionalinės kibernetinių incidentų valdymo platformos; dalintis informacija apie žinomas kibernetinių išpuolių taktikas, metodus ir procedūras, geriausią kibernetinio saugumo praktiką, naujausias tendencijas, grėsmes ir programinės įrangos vertinimo ataskaitas; reguliariai dalintis informaciniais biuleteniais apie regionines ir nacionalines kibernetines grėsmes finansų sektoriuje; kviesti Lietuvos banko atstovus dalyvauti NKSC organizuojamose pratybose ir mokymuose.

05

NKSC rekomendacijos, kaip suorganizuoti imitacines socialinės inžinerijos pratybas.

06

Neteisėta veikla, sukčiavimas: (angl. Fraud): vagystė, apgavystė, neteisėtas išteklių (angl. *Unauthorized Use of Resources*), nelegalios programinės įrangos ar autorių teisių (angl. *Copyright*) naudojimas, tapatybės klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai.

07

KSIS paskirtis – informacinių technologijų priemonėmis tvarkyti duomenis, susijusius su KSIS nariais, įskaitant duomenis, nurodytus KSĮ 19 straipsnio 1 dalyje.

2025 m. kovo 27 d. **NKSC** kartu su **Generaline prokuratūra, Lietuvos policija, RRT, Lietuvos banku ir Pinigų plovimo prevencijos kompetencijų centru pasirašytas memorandumas dėl bendradarbiavimo siekiant mažinti sukčiavimo skaitmeninėje erdvėje atvejus**. NKSC indėlis – pritaikyti KSIS, kad šalys galėtų keistis su kibernetinio saugumo užtikrinimu susijusiais duomenimis ir informacija, įgalinant šalis atlikti savo funkcijas; dalintis informacija su šalimis apie užblokuotas žalingas svetaines; organizuoti nemokamus mokymus visuomenei apie kibernetinio saugumo užtikrinimo svarbą; skelbti rekomendacijas apie kibernetinių incidentų prevenciją, informuoti apie galimas kibernetines grėsmes ir teikti rekomendacijas apie prevencines priemones šioms grėsmėms valdyti.

Reguliarūs mokymai ir imitacinės socialinės inžinerijos pratybos padeda darbuotojams geriau atpažinti grėsmes, sumažina žmogiškųjų klaidų tikimybę ir didina organizacijos atsparumą kibernetiniams incidentams.

Duomenys dažniausiai nutekinami skaitmeninės infrastruktūros ir viešojo administravimo sektoriuose

NKSC nutekintus duomenis[08] traktuoja kaip viešai prieinamus prisijungimo duomenis ar kitą su autentifikavimu susijusią informaciją, kuri gali būti panaudota neteisėtai prieigai prie informacinių sistemų ar paslaugų. Skirtingai nei VDAI vykdant asmens duomenų apsaugos reguliavimą, NKSC analizuoja nutekintų prisijungimo duomenų mastą, pasiskirstymą, tendencijas ir jų panaudojimą žalingose kibernetinėse veiklose.

2025 metais NKSC aptiko daugiau kaip 106 tūkst. **nutekintų prisijungimo duomenų** viešuosiuose ir uždaruose informacijos šaltiniuose. Tai rodo, kad nutekintų prisijungimo duomenų panaudojimas yra pagrindinis būdas siekiant neteisėtai užvaldyti naudotojų paskyras.

2025 m. buvo automatizuotas informavimo apie nutekėjusius prisijungimo duomenis procesas. Per 2025 metus NKSC apie nustatytus duomenų nutekėjimus informavo 221 organizaciją, išsiųsta beveik 3000 pranešimų (2024 m. – 2000). Automatizavimas leidžia greičiau informuoti organizacijas, trumpinti reagavimo laiką ir mažinti nutekintų duomenų panaudojimo riziką kibernetinėse atakose. Dažniausiai kibernetinės grėsmės yra specifinės atskiriems sektoriams ir aktualios konkrečiai veiklos sričiai. Siekdamas užtikrinti, kad kiekvienas sektorius gautų papildomos informacijos apie jam aktualias kibernetines grėsmes, susipažintų su pasaulinėmis tendencijomis ir gerąją praktiką galėtų pritaikyti išankstiniam pasirengimui bei apsisaugojimui, NKSC 2025 m. pradėjo rengti **sektorių kibernetinių grėsmių ataskaitas**. Pirmiausia parengta **finansų sektoriaus ataskaita**[09]. Pagrindiniai šių ataskaitų naudos gavėjai yra sektoriaus įstaigų saugos įgaliotiniai ar kibernetinio saugumo / IT ekspertai.

08

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

09

2026 m. pradėtos rengti ataskaitos sveikatos sektoriui, taip pat planuojama rengti ataskaitas geriamojo vandens ir nuotekų valymo sektoriams.

Tobulinamas informavimo apie nutekėjusius duomenis procesas užtikrina tikslesnį ir operatyvesnį informacijos perdavimą, didinantį organizacijų pasirengimą reaguoti į galimas grėsmes. Kartu gerėja gaunamų duomenų kokybė ir jų analitinis pritaikomumas, kas sudaro pagrindą efektyvesniam jų panaudojimui rengiant sektoriaus grėsmių ataskaitas. Šie pokyčiai stiprina kibernetinio saugumo stebėseną ir gerina rizikų identifikavimo bei vertinimo procesus.

Organizacijos vis plačiau diegia papildomas apsaugos priemones, siekdamos sumažinti neteisėtos prieigos riziką ir sustiprinti bendrą saugumo lygį. Viena efektyviausių priemonių išlieka **dviejų žingsnių autentifikavimas**. Jis reikšmingai sumažina neteisėtos prieigos tikimybę ir padeda užkirsti kelią galimam duomenų nutekėjimui.

Nutekintų duomenų mastui išliekant dideliam, pagrindinės priežastys nesikeičia – dominuoja **žmogiškasis faktorius** ir **kenkimo programinės įrangos** (angl. *Malware*) **tipas vartotojų duomenims slapta rinkti ir perduoti kibernetiniams piktavaliams**[10]. Nutekinti duomenys sudaro sąlygas tolimesnėms plataus masto kibernetinėms atakoms.

Išsamesnė nutekintų duomenų analizė, įskaitant jų pasiskirstymą ypatingos svarbos ir kituose itin svarbiuose sektoriuose bei galimą panaudojimą kibernetinėse veiklose, pateikiama šios ataskaitos priede.

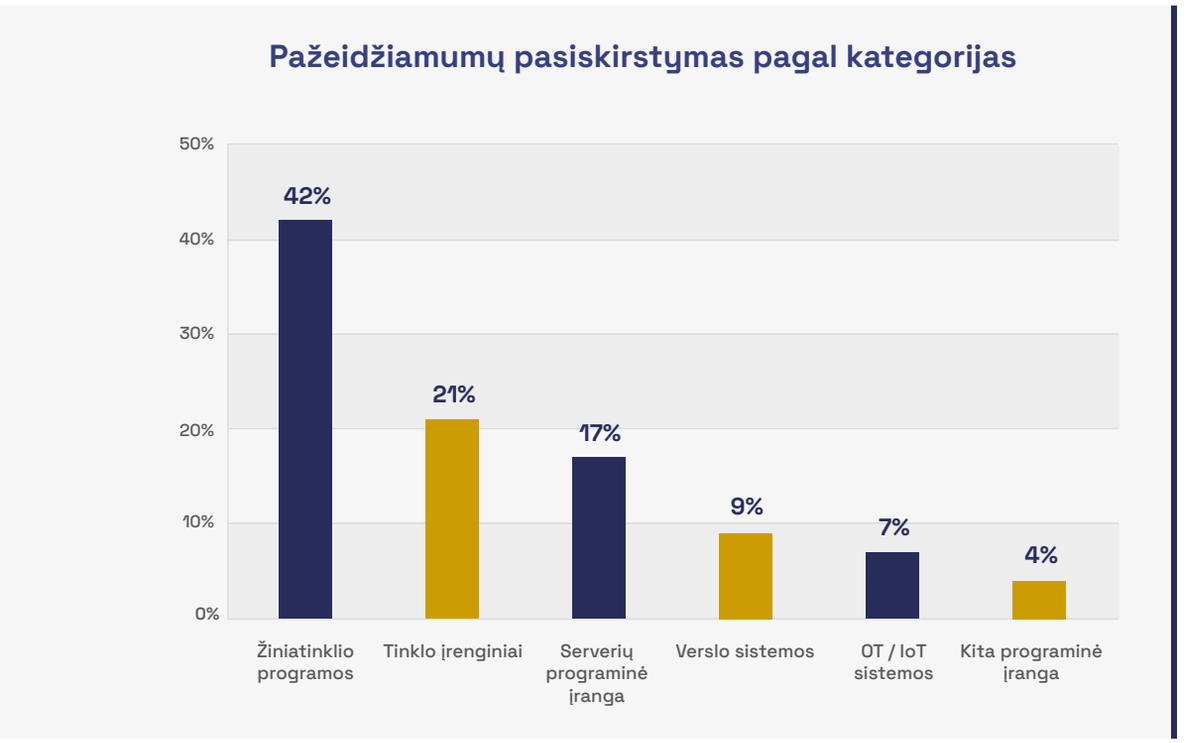
Didžiausią riziką keliantys pažeidžiamumai: nuo žiniatinklio programų iki daiktų interneto sistemų

2025 m. NKSC ir toliau fiksavo reikšmingą tinklų ir informacinės sistemos spragų[11] (toliau – spragos), keliančių riziką valstybinėms institucijoms ir privataus sektoriaus organizacijoms, skaičių. 2025 m. NKSC prioritetą skyrė didesnio kritinio laipsnio ir lengviau išnaudojamiems pažeidžiamumams, ir organizacijos būdavo dažniau informuojamos apie didžiausią grėsmę keliančius atvejus. Dėl šios metodinės atrankos 2025 m. NKSC išsiųstų pranešimų skaičius (2 679) nėra tiesiogiai palyginamas su 2024 m. pranešimų skaičiumi (6 700). Atsižvelgiant į šiuos skaičius negalima daryti išvados apie bendrą pažeidžiamų informacinių sistemų skaičiaus mažėjimą.

Analizuojant 2025 m. valdytus pažeidžiamumus pagal technologijas ir produktų tipus, didžiausią dalį sudarė **žiniatinklio programų ir turinio valdymo sistemų saugumo spragos** (42 proc.) (**4 pav.**). Šioje kategorijoje dominavo turinio valdymo sistema *WordPress* ir su ja susiję įskiepiai, kurie dėl plataus paplitimo ir trečiųjų šalių komponentų gausos išlieka dažnu piktavalių taikiniu. Ataskaitos priede pateikiama detalesnė šios kategorijos analizė.

10
Skirtingai nei kitų tipų kenkimo programinė įranga, šis kenkimo programinės įrangos tipas dažniausiai neveikia destruktyviai – jis skirtas vertingai informacijai nepastebimai rinkti.

11
Tinklų ir informacinės sistemos spraga – tinklų ir informacinės sistemos trūkumas, įskaitant informacinių ir ryšių technologijų produktų arba informacinių ir ryšių technologijų paslaugų trūkumus, dėl kurio gali įvykti kibernetinis incidentas ar kuriuo gali būti pasinaudota kibernetinei grėsmei sukelti.



< 4 pav.

Pažeidžiamumų pasiskirstymas pagal kategorijas
(šaltinis – NKSC)

Didelę riziką kėlė **tinklo įrenginių pažeidžiamumai**, susiję su saugasienėmis (angl. *Firewalls*), virtualiais privačiais tinklais (angl. *Virtual Private Network*, VPN) ir kitais perimetro apsaugos sprendimais (21 proc.). Tokie pažeidžiamumai daro itin didelį poveikį, nes sudaro sąlygas piktavaliams apeiti perimetro apsaugą ir pasiekti organizacijų vidaus išteklius. Dažnais taikiniais išliko plačiai naudojamų gamintojų produktai, tokie kaip *Fortinet* ir *Cisco*, jie neretai tampa masinių skenavimo ir išnaudojimo kampanijų objektais.

Serverių programinės įrangos spragos, apimančios įvairias serverių paslaugas, protokolus, pašto sistemas, failų perdavimo sprendimus ir infrastruktūros valdymo įrankius (17 proc.), taip pat dažnai išnaudojamos ir neretai būna kaip tarpinis etapas, leidžiantis piktavaliams išlaikyti ilgalaikę prieigą prie sistemų arba plėsti užvaldymą organizacijos viduje.

Atskirai išskirtinos **verslo informacinės sistemos**, įskaitant ryšių su klientais valdymo (angl. *Customer Relationship Management*, CRM), įmonės išteklių planavimo (angl. *Enterprise Resource Planning*, ERP), grupinio darbo ir kitas specializuotas platformas, kurių pažeidžiamumai 2025 m. sudarė mažesnę dalį, tačiau pasižymėjo potencialiai dideliu poveikio lygiu dėl šiose sistemose saugomų jautrių duomenų (9 proc.).

Operacinių technologijų (angl. *Operational Technology*, OT) ir **daiktų interneto** (angl. *Internet of Things*, IoT) sistemų pažeidžiamumai išliko aktualūs ir 2025 m., patvirtindami, kad pramoninių įrenginių ir susijusių technologijų saugumui vis dar skiriama per mažai dėmesio (7 proc.). Šių sistemų pažeidžiamumai yra ypač pavojingi dėl jų dažno naudojimo kritinėse paslaugose ir procesuose, taip pat dėl galimų fizinių pasekmių, kurias gali sukelti šių spragų išnaudojimas.

Interneto svetainės ir kitos žiniatinklio programos išlieka vienu dažniausių taikinių. NKSC stebi viso LT domeno interneto svetaines ir apie nustatytus pažeidžiamumus informuoja pažeidžiamų svetainių prieglobos paslaugų teikėjus, kad jie informaciją perduotų savo klientams ir susijusios saugumo spragos būtų užkardytos laiku.

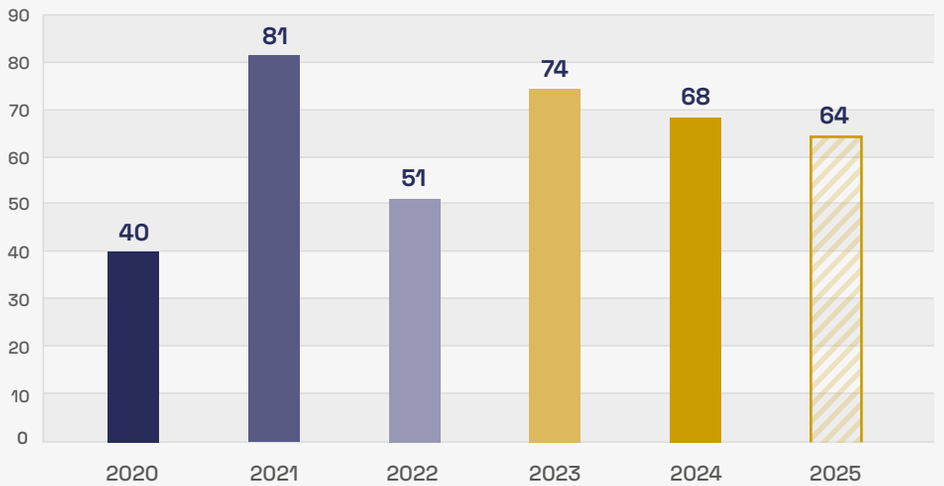
Tinklo įrenginiai, dažnai atliekantys pagrindinę perimetro apsaugos funkciją, kartu išlieka ir vienu pagrindinių piktavalių patekimo į organizacijos infrastruktūrą kelių. NKSC stebi ir skelbia naujausią informaciją apie pažeidžiamumus, atlieka pažeidžiamų sistemų paiešką ir informuoja interneto paslaugų teikėjus, kad ši informacija būtų perduota jų klientams.

Atsakingi pranešėjai nuolat praneša apie nustatytas spragas

Atsakingas saugumo spragų atskleidimas ir toliau išliko svarbia kibernetinio saugumo ekosistemos dalimi, leidžiančia spragas identifikuoti ir pašalinti dar prieš joms tampant realių kibernetinių incidentų priežastimi. Šis mechanizmas stiprina pasitikėjimą tarp saugumo bendruomenės, infrastruktūros valdytojų ir valstybės institucijų bei prisideda prie bendro šalies kibernetinio atsparumo didinimo.

2025 m. taikant **atsakingo (koordinuoto) atskleidimo principą**[12] buvo gauti 64 pranešimai (**5 pav.**) apie spragas (2024 m. – 68). Stabilus pranešimų srautas leidžia NKSC nuosekliai reaguoti į gautą informaciją ir koordinuoti veiksmus su paveiktomis organizacijomis.

12
Atsakingas spragų atskleidimas – kai informacija apie aptiktas spragas pirmiausia pateikiama pačiai organizacijai, kurios informacinėse sistemose ar produktuose jos buvo aptiktos, ir (ar) spragų atskleidimo procesą koordinuojančiai institucijai – NKSC.

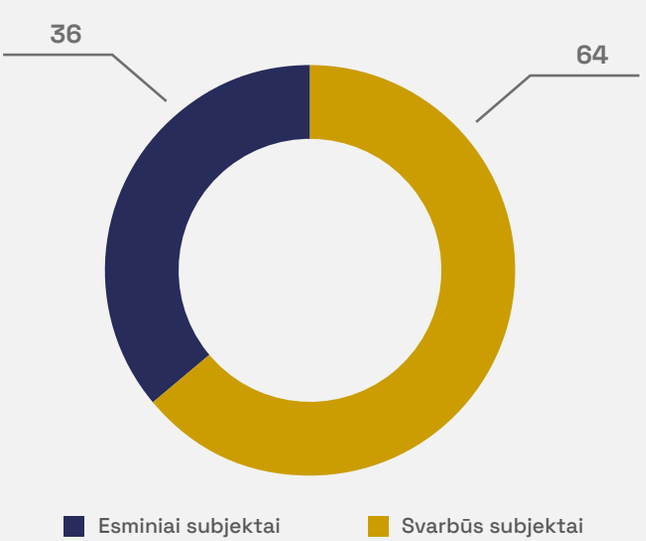


< 5 pav.

Pagal atsakingą spragų atskleidimą gautų pranešimų skaičius *(šaltinis – NKSC)*

Išplėsta KSS aprėptis – dominuoja viešojo administravimo ir sveikatos priežiūros sektoriai

Įgyvendinant KSĮ reikalavimus, 2025 m. balandžio mėnesį buvo pradėta KSS registracija. 2025 m. į Registrą įtraukti 1443 KSS, iš KSĮ prieduose nurodytų **ypatingos svarbos**[13] ir kitų **itin svarbių sektorių**[14]: 526 subjektai (36 proc.) priskirti esminiams KSS ir 917 subjektų (64 proc.) svarbiems (**6 pav.**). KSS skaičius Registre yra nuolat atnaujinamas priklausomai nuo gaunamų duomenų[15].



< 6 pav.

Esminių ir svarbių KSS pasiskirstymas procentais *(šaltinis – NKSC)*

13

Lietuvos Respublikos kibernetinio saugumo įstatymo I priede nurodyti sektoriai.

14

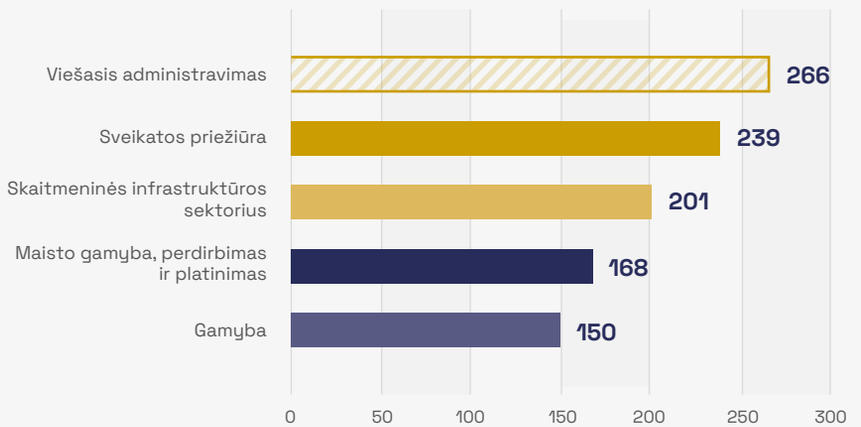
Lietuvos Respublikos kibernetinio saugumo įstatymo II priede nurodyti sektoriai.

15

Į Registrą pradedami įtraukti nauji KSS, atsižvelgiant į Kibernetinio saugumo subjektų identifikavimo pagal specialiuosius kriterijus metodiką, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

Didžiausias KSS skaičius registruotas viešojo administravimo sektoriuje (266 vnt.), antroje vietoje – sveikatos priežiūros sektorius (239 vnt.), trečioje vietoje – skaitmeninės infrastruktūros sektorius (201 vnt.) (**7 pav.**).

5 sektoriai, kuriuose registruota daugiausia KSS, vnt.



< 7 pav.

5 sektoriai, kuriuose registruota daugiausia KSS *(šaltinis – NKSC)*

Įgyvendinant KSĮ reikalavimus, NKSC priežiūros ir stebėsenos apimtis išaugo beveik penkis kartus. Dauguma naujai įtrauktų KSS priklauso privačiam sektoriui (60 proc. registruotų KSS). Efektyviai išaugusių KSS priežiūrai ir stebėsenai NKSC įgyvendino automatizuotus stebėsenos sprendimus, įdiegė KSIS, kurios viena iš paskirčių – tvarkyti duomenis, susijusius su kibernetinio saugumo rizikos valdymo priemonių įgyvendinimo stebėsena.

Siekdamas sudaryti sąlygas KSS tinkamai įgyvendinti teisės aktų reikalavimus, NKSC pradėjo teikti nemokamas paslaugas, kurios yra pasiekiamos KSS prisijungus prie KSIS:

- atsisiųsti kibernetinio saugumo politikos dokumentų šablonus, kibernetinio saugumo rizikos valdymo metodiką,
- bendrauti su kitais jos nariais,
- gauti iš NKSC aktualią informaciją apie kibernetinio saugumo grėsmes,
- dalintis grėsmių indikatoriais (angl. *Indicators of Compromise*, IoC),
- diegti kibernetinio saugumo priemones ir automatizuoti kibernetinių incidentų aptikimą,
- pranešti NKSC apie įvykusius kibernetinius incidentus ir pateikti papildomą informaciją, reikalingą kibernetinių incidentų tyrimui.

KSIS naudotojams taip pat sudaryta galimybė nemokamai naudotis NKSC sukurtais pratybų įrankiais, leidžiančiais pasitikrinti organizacijų kibernetinių incidentų valdymo planus prisijungus prie NKSC **kibernetinio poligono** (angl. *Cyber Range*) bei ugdyti darbuotojų atsparumą socialinės inžinerijos atakoms dalyvaujant NKSC organizuojamose pratybose.

Nepakankamas dėmesys kibernetinio saugumo reikalavimų įgyvendinimui

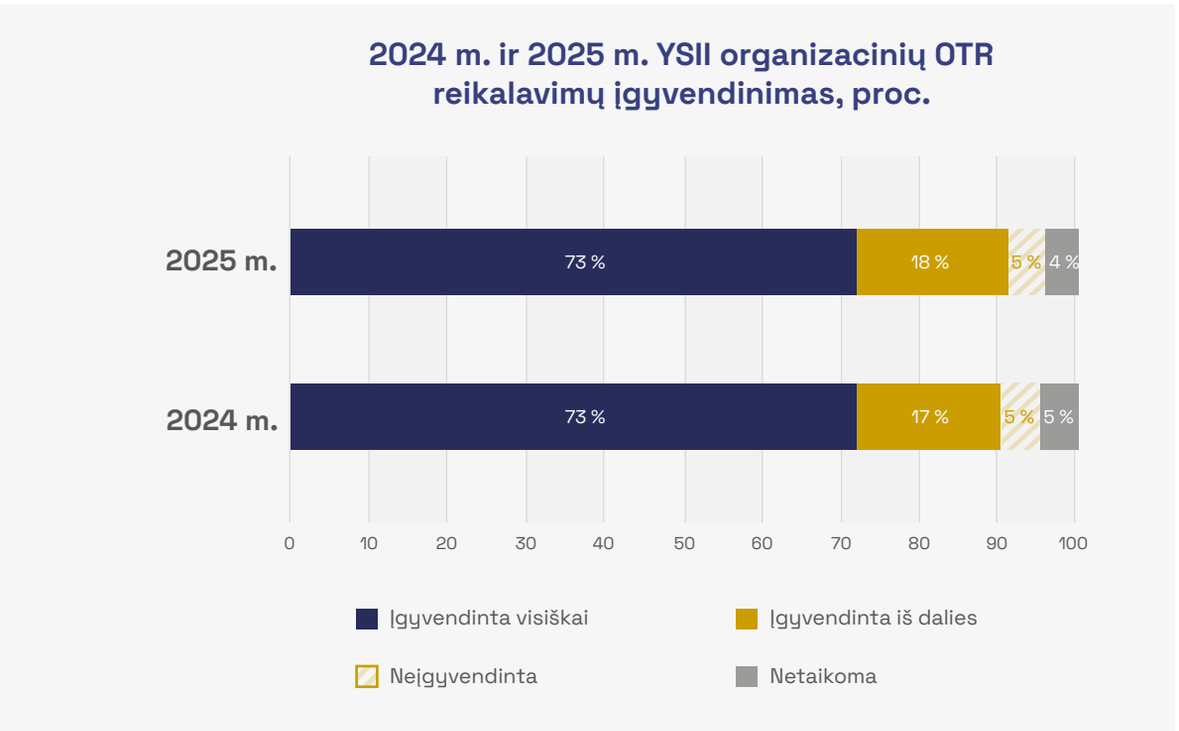
Organizacijų kibernetinis atsparumas priklauso nuo pasirengimo atpažinti grėsmes, užkirsti joms kelią, laiku aptikti incidentus, į juos reaguoti, atkurti veiklą ir nuolat tobulinti saugumo procesus. Pagal 2024 m. atnaujinto KSĮ reikalavimus KSS **organizacinius** kibernetinio saugumo reikalavimus turi įgyvendinti iki 2026 m. balandžio 17 d., **techninius** – iki 2027 m. balandžio 17 d., todėl 2025 m. buvo skirti pasiruošti kibernetinio saugumo reikalavimų įgyvendinimui.

Subjektai, iki KSĮ įsigaliojimo dienos buvę Lietuvos Respublikos Vyriausybės patvirtintame **Ypatingos svarbos informacinės infrastruktūros** (toliau – YSII) **ir jos valdytojų sąraše** ir nuo 2025 m. balandžio 17 d. įtraukti į Registrą, privalėjo toliau užtikrinti savo valdomų TIS atitiktį iki atnaujinto KSĮ įsigaliojimo dienos galiojusiems Lietuvos Respublikos Vyriausybės nustatytiems **Organizaciniams ir techniniams kibernetinio saugumo reikalavimams** (toliau – OTR), kol atsiras pareiga užtikrinti savo valdomų TIS atitiktį KSĮ nustatytoms kibernetinio saugumo rizikos valdymo priemonėms.

NKSC nuolat vykdo kibernetinių saugumo reikalavimų įgyvendinimo stebėseną ir, vertindamas YSII būklę, 2025 m. atliko 15 patikrinimų: 9 daliniai organizacinių OTR patikrinimai, 6 išsamūs YSII valdytojų atitikties vertinimai, kurių metu buvo vykdomi tiek dokumentiniai ir darbo vietų patikrinimai, tiek išorės skenavimai ir įsilaužimo testavimai. Po patikrinimų KSS buvo pateiktos rekomenduojamos valdymo priemonės identifikuotiems trūkumams ir neatitiktims pašalinti. Pastarųjų įgyvendinimo stebėseną atlieka NKSC.

Be minėtų patikrinimų, NKSC vertino OTR taikymą YSII valdančiose organizacijose taikydamas vadinamąjį **savideklaracijos principą**, kai YSII organizacijos pačios deklaruoja savo duomenis apie atitiktį OTR. Kasmet atliekamas tokių duomenų surinkimas atskleidžia deklaruojamą YSII kibernetinio saugumo būklę. Pagal YSII savideklaracijos duomenis, **organizacinius** OTR (pavyzdžiui, patvirtinta kibernetinio saugumo politika, incidentų valdymo procedūros, prieigos teisių valdymas, rizikos vertinimas ir kt.) tiek 2024 m., tiek 2025 m. visiškai buvo įgyvendinę 73 proc. YSII valdytojų (**8 pav.**)[16].

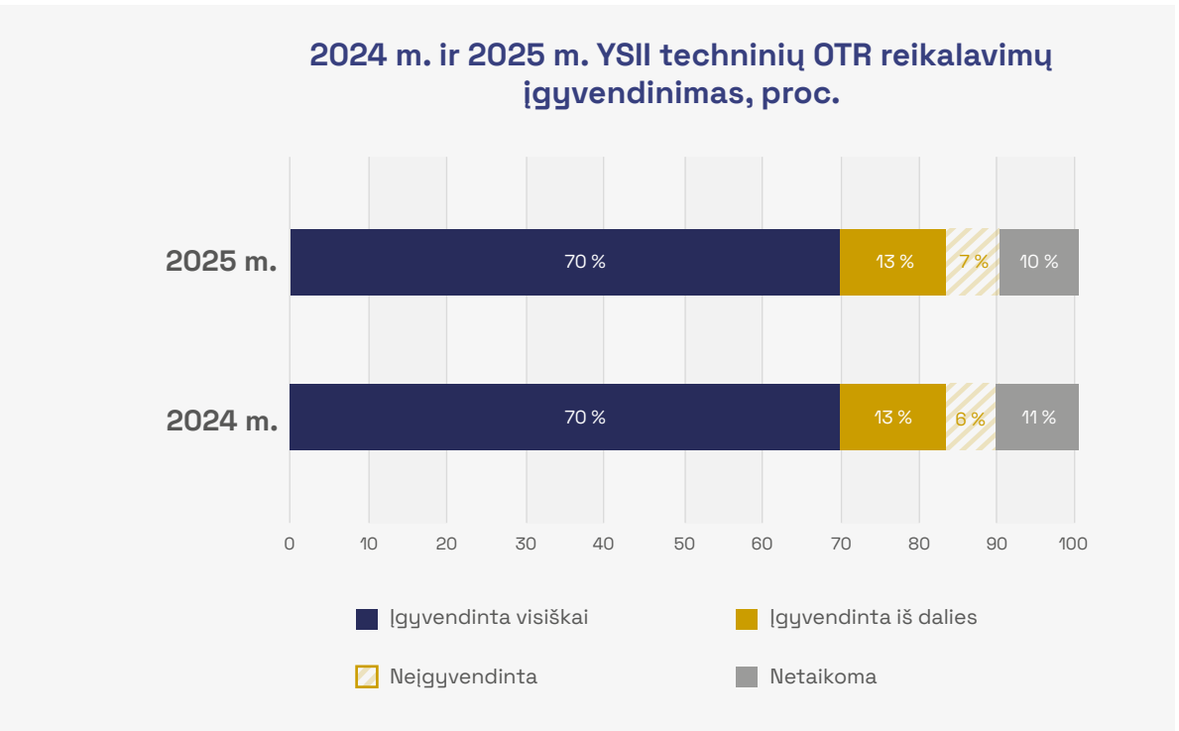
16
„Netaikoma“ – kai YSII valdytojo valdomai infrastruktūrai (technologinėms sistemos) netaikomi informacinių sistemų reikalavimai.



< 8 pav.

2024 m. ir 2025 m. YSII organizacinių OTR reikalavimų įgyvendinimas
(šaltinis – NKSC)

Techninius OTR (pavyzdžiui, atpažinties, tapatumo patvirtinimo, administratorių paskyrų kontrolės, audito įrašų valdymo, mobiliųjų įrenginių valdymo ir kitus reikalavimus), kaip ir 2024 m., įgyvendino 70 proc. YSII valdytojų (**9 pav.**).



< 9 pav.

2024 m. ir 2025 m. YSII techninių OTR reikalavimų įgyvendinimas
(šaltinis – NKSC)

2025 m. YSII savideklaracijos duomenys rodo, kad bendras OTR įgyvendinimas išliko stabilus, o remiantis duomenimis, galima daryti išvadą, kad daliai organizacijų OTR įgyvendinimas vis dar nėra prioritetinė valdymo sritis. Antra vertus, matyti, kad dalis organizacijų nuosekliai išlaiko kibernetinį saugumą kaip prioritetą ir sistemiškai laikosi taikomų OTR.

Saugumo aplinkos pokyčiai ir tendencijos

Vertinant bendrą incidentų skaičiaus mažėjimo tendenciją (-25 proc.), galima daryti atsargiai pozityvią išvadą, kad dalį šio pokyčio galėjo lemti kryptingai stiprinamas nacionalinis ir organizacijų kibernetinis saugumas. Prie teigiamų rezultatų, tikėtina, prisidėjo NKSC taikomos efektyvios grėsmių blokavimo priemonės, auganti organizacijų kibernetinio saugumo branda. Šie veiksniai rodo nuoseklų saugumo ekosistemos stiprėjimą ir sudaro prielaidas tolesniam incidentų rizikos mažėjimui.

NKSC tobulinamas informavimo apie nutekėjusius duomenis procesas ir gerinama duomenų kokybė sudaro palankesnes sąlygas tikslesniam grėsmių vertinimui ir efektyvesniam sektorių informavimui apie aktualias rizikas.

Atitiktis kibernetinio saugumo reikalavimams yra svarbus organizacijų atsparumo pagrindas, tačiau savaime negarantuoja realaus saugumo. Kibernetinio saugumo reikalavimai yra minimalus apsaugos lygis, nes grėsmės kinta greičiau, nei atnaujinami teisės aktai ar standartai. Todėl vien formalus kibernetinio saugumo reikalavimų įgyvendinimas gali sudaryti klaidingą saugumo jausmą. Praktikoje organizacijų atsparumą lemia ne tik atitiktis, bet ir nuolatinis rizikų vertinimas, pažeidžiamumų valdymas, gebėjimas laiku aptikti incidentus ir greitai į juos reaguoti bei darbuotojų budrumo stiprinimas. 2025 m. YSII savideklaracijos duomenys rodo stabilų bendrą OTR įgyvendinimo lygį, o didžioji dalis (apie 70 proc.) organizacijų nuosekliai išlaiko kibernetinį saugumą kaip prioritetinę sritį.

NKSC, siekdamas padėti organizacijoms įsivertinti kibernetinio saugumo rizikas, 2025 m. parengė **Kibernetinio saugumo rizikų vertinimo metodiką**[17], skirtą padėti KSS įvertinti kibernetinio saugumo rizikas. Nors metodika yra rekomendacinio pobūdžio, kibernetinio saugumo rizikų vertinimas yra privalomas pagal **Kibernetinio saugumo reikalavimų aprašą**[18].

2025 m. socialinės inžinerijos principais grįsti kibernetiniai incidentai vis dar išlieka viena didžiausių kibernetinių grėsmių, nes, nepaisant jų skaičiaus mažėjimo, jie vis dar sudaro daugiau nei pusę visų registruotų incidentų. Todėl darbuotojų kritinio mąstymo ugdymas ir jų gebėjimų atpažinti tokio tipo atakas stiprinimas išlieka pagrindine NKSC organizuojamų kibernetinio saugumo pratybų ašimi. Socialinės inžinerijos simuliacijos pratybas rengiantys

17 Kibernetinio saugumo rizikų vertinimo metodika pasiekiama tik KSIS ir prieinama tik KSS.

18 Kibernetinio saugumo reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

KSS atstovai teigia, kad pastebi teigiamą darbuotojų elgsenos pokytį: vis didesnė dalis gavusiųjų įtartiną laišką informuoja kibernetinio saugumo specialistus. 2025 m. patvirtintas **Kibernetinio saugumo mokymų, skirtų kibernetinio saugumo subjekto vadovui, kibernetinio saugumo vadovui ir saugos įgaliotiniui ir kibernetinio saugumo auditoriui, tvarkos aprašas**[19] (toliau – Aprašas). Aprašo tikslas – nustatyti KSS valdymo organų narių, KSS vadovų ir jo įgaliotų asmenų, kibernetinio saugumo subjekto, jeigu jis yra fizinis asmuo, kibernetinio saugumo vadovų ir saugos įgaliotinių bei kibernetinio saugumo auditą atliekančių auditorių kibernetinių saugumo mokymų vykdymo tvarką. Augantis kibernetinio saugumo mokymų dalyvių skaičius atspindi nuosekliai augantį visuomenės ir organizacijų poreikį stiprinti kibernetinio saugumo žinias bei praktinius įgūdžius.

2025 m. gruodžio mėnesį KAM užsakymu atlikta apklausa atskleidė, kad mažiau nei pusė (47 proc.) apklaustų gyventojų teigia žinantys, kaip elgtis kibernetinio saugumo incidento atveju. Palyginti su 2024 m., kai šis rodiklis siekė 51 proc., fiksuojamas nedidelis neigiamas pokytis, rodantis išliekantį poreikį stiprinti visuomenės informuotumą ir pasirengimą.

Siekdamas didinti KSS ir kitų organizacijų kibernetinį atsparumą, stiprinti kibernetinio saugumo reikalavimų veiksmingumą ir suteikti praktines gaires aktualiausiose kibernetinio saugumo srityse, NKSC 2025 m. parengė **10 rekomendacijų**[20].

Nutekėjusių duomenų mastas išlieka didelis, o dominuojančios priežastys kartojasi, todėl žmogiškasis faktorius ir kenkimo programinės įrangos tipas vartotojų duomenims slapta rinkti ir perduoti kibernetiniams piktavaliams tebėra reikšmingi rizikos veiksniai, sudarantys prielaidas tolimesnėms atakoms.

Interneto svetainės, žiniatinklio programos ir tinklo įrenginiai išlieka vienais dažniausių kibernetinių grėsmių taikinių, o nustatomi pažeidžiamumai rodo, kad dalis organizacijų vis dar nepakankamai užtikrina viešai prieinamų sistemų ir perimetro apsaugos priemonių atnaujinimą laiku bei atsparumą kibernetinėms grėsmėms.

19

NKSC direktoriaus 2025 m. birželio 13 d. įsakymas Nr. 1-96 „Dėl Kibernetinio saugumo mokymų, skirtų kibernetinio saugumo subjekto vadovui, kibernetinio saugumo vadovui ir saugos įgaliotiniui ir kibernetinio saugumo auditoriui, tvarkos aprašo tvirtinimo“.

20

NKSC interneto svetainės skiltis „Rekomendacijos“.

DI ir automatizacijos poveikis saugumo aplinkai

Pasaulyje matomas augantis DI panaudojimas pažeidžiamumų aptikimo ir jų išnaudojimo kontekste. DI sprendimai piktavalių vis dažniau buvo taikomi naudojimosi saugumo spragomis (angl. *Exploit*) generavimui ir spragų paieškos automatizavimui. Lietuvoje šios tendencijos daugiausiai pasireiškė atsakingo atskleidimo praktikoje. Keliuose 2025 m. gautuose pranešimuose buvo akivaizdžių DI panaudojimo atvejų, kuomet DI buvo naudojamas spragų paieškos ir išnaudojimo aprašymams rengti. Aprašymų tekstai buvo didelės apimties, bet padriki ir nekonkretūs, keliantys teorines hipotezes ir nenurodantys konkrečių paveiktų sistemų.

Saugus ir atsakingas DI sprendimų taikymas organizacijose turi būti grindžiamas išankstiniu rizikų vertinimu, aiškiai apibrėžtais DI naudojimo tikslais ir atsakomybėmis bei užtikrinant, kad DI nebūtų naudojamas kaip galutinių sprendimų priėmėjas kritinėse srityse. Didelis dėmesys turi būti skiriamas duomenų apsaugai, techninėms ir organizacinėms saugumo priemonėms, įskaitant prieigos kontrolę, tiekimo grandinės rizikų vertinimą ir DI veikimo stebėseną.

Didėjant DI sprendimų taikymo mastui viešajame ir privačiame sektoriuose, aktualėja su šių technologijų naudojimu susijusios kibernetinio saugumo, duomenų apsaugos ir veiklos patikimumo rizikos. DI sprendimai vis dažniau tampa incidentų taikiniu, o jų netinkamas naudojimas gali lemti klaidingus sprendimus, duomenų nutekinimą ar neteisėtą prieigą prie informacinių sistemų. Atsižvelgdamas į tai, NKSC parengė **Rekomendacijas saugiam dirbtinio intelekto (DI) sprendimų naudojimui organizacijoje**. Rekomendacijų tikslas – stiprinti organizacijų gebėjimą saugiai ir atsakingai naudoti DI, užtikrinti rizikų valdymą ir duomenų apsaugą.

KSS, atliekant kibernetinio saugumo rizikos vertinimą vadovaujantis **Kibernetinio saugumo rizikų vertinimo metodika**, rekomenduojama įsivertinti šias DI grėsmes (sudarytas grėsmių katalogas):

- **apgaulingos DI užklausos,**
- **DI sprendimų klaidos,**
- **DI duomenų užkrėtimas (angl. *Data Poisoning*),**
- **DI nekontroliuojamas veikimas,**
- **duomenų nutekėjimas per DI modelius,**
- **piktnaudžiavimas DI,**
- **DI tiekimo grandinės pažeidžiamumai.**

Svarbi kibernetinio saugumo užtikrinimo sąlyga yra darbuotojų mokymai, užtikrinantys saugų ir atsakingą DI sprendimų naudojimą, galimų rizikų supratimą bei kritinį DI pateikiamų rezultatų vertinimą[21]. Darbuotojų kompetencijų stiprinimas prisideda prie organizacijų atsparumo didinimo ir nacionalinio kibernetinio saugumo stiprinimo.

Savo ruožtu 2025 m. DI savo veikloje aktyviau pasitelkė ir NKSC, siekdamas didinti pažeidžiamumų valdymo efektyvumą nacionaliniu lygmeniu. DI sprendimai buvo naudojami naujai aptinkamų pažeidžiamumų monitoringui ir pirminiam vertinimui, pažeidžiamų įrenginių paieškai. Tokie įrankiai leidžia lengviau apdoroti didelius duomenų kiekius, greičiau reaguoti į kintančią grėsmių aplinką ir sumažinti laiką nuo spragos identifikavimo iki paveiktos sistemos valdytojo informavimo.

Rizikos, susijusios su priklausomybe nuo išorinių paslaugų teikėjų ir tiekimo grandinių

Remiantis ENISA parengta **2030 m. grėsmių prognoze**[22], organizacijos pažeidžiamumai per tiekimo grandinę ir trečiąsias šalis, įskaitant ir paslaugų teikėjus trečiosioms šalims (subteikėjus), yra įvardijami kaip aktualiausia kibernetinio saugumo grėsmė iki 2030 m. Trečiųjų šalių paslaugų teikėjai dažnai pasižymi žemesne kibernetinio saugumo branda ir atveria galimybes piktavaliams per jų ar subteikėjų infrastruktūrą įsilaužti net į stipriausią IT infrastruktūrą turinčias organizacijas.

Net ir tada, kai organizacija pakankamai gerai saugo savo IRT infrastruktūrą, tiekimo grandinėje esantys išorės partneriai ir jų IRT infrastruktūroje galimos spragos tampa silpniausia grandimi, į kurią dažniausiai ir taikosi piktavaliai.

Atsižvelgdamas į tai, NKSC 2025 m. parengė **Rekomendacijas trečiųjų šalių valdymui**[23]. Rekomendacijų tikslas – suteikti organizacijoms gaires, padedančias valdyti TIS, kai IRT paslaugas teikia trečiosios šalys. Rekomendacijose akcentuojama būtinybė nuosekliai taikyti atitinkamas saugumo kontrolės priemones ir parengti tiekimo grandinės saugumo valdymo tvarkos aprašą. Jame turi būti aiškiai įvardinti trečiosios šalies valdymo principai, atsakomybės ribos ir trečiųjų šalių gyvavimo ciklas – nuo atrankos iki sutarties nutraukimo.

Labai mažos, mažos ir vidutinės įmonės (toliau – MVĮ) yra neatsiejama tiekimo grandinės dalis – nuo jų saugumo priklauso ir stambiųjų organizacijų bei kritinės infrastruktūros apsauga. Net gerai apsisaugojusios didžiosios organizacijos tampa pažeidžiamos, jei jų tiekėjai ar partneriai – dažnai MVĮ – netaiko būtinų kibernetinio saugumo priemonių.

21
2026 m. NKSC Kibernetinio saugumo mokymų platformoje pristatė naują mokymų kursą „Saugus dirbtinio intelekto naudojimas“, skirtą didėjančioms su dirbtinio intelekto technologijomis susijusioms rizikoms valdyti.

22
2030 m. grėsmių prognozė (angl. *Foresight Threats 2030*).

23
Trečiųjų šalių valdymo rekomendacijos.

Didinant organizacijų kibernetinio saugumo brandą ir stiprinant visos šalies tiekimo grandinės atsparumą, **NKSC nuotolinėje mokymų platformoje** 2025 m. pristatė naujus mokymus vadovams ir darbuotojams:

- Mokymai vadovams orientuoti į strateginius sprendimus – kaip kurti ir palaikyti kibernetinį saugumą organizacijoje, ugdyti jos brandą bei pasirinkti tinkamas priemones pagal verslo plėtros mastelį;
- Mokymai darbuotojams padės suprasti asmeninės atsakomybės svarbą už įmonės kibernetinį saugumą, išmokys taikyti praktinius sprendimus, laikytis kibernetinės higienos ir atsakingai naudoti technologijas, įskaitant DI įrankius.

Papildomos įžvalgos iš kitų ataskaitų

Lietuvos kibernetinis saugumas yra glaudžiai susijęs su regionine geopolitine įtampa ir valstybės vykdoma strategine užsienio politika. Priešiškų valstybių remiamos grupuotės sistemingai pasitelkia hibridinio spaudimo įrankius, prioritetiniu taikiniu pasirinkdamos šalies kritinę infrastruktūrą ir viešojo sektoriaus subjektus. Lietuvoje, kaip ir kitose Vakarų valstybėse, fiksuojami bandymai išnaudoti **priežiūrinės kontrolės ir duomenų rinkimo sistemų** (angl. *Supervisory Control and Data Acquisition*, SCADA) pažeidžiamumus. Socialinio tinklo „Telegram“ kanaluose periodiškai pasirodo pranešimų apie tariamai sėkmingus įsilaužimus į kritinės infrastruktūros sistemas, tačiau ar tokia informacija patikima, dažniausiai patvirtinti neįmanoma. Daugumos tokių viešųjų incidentų tikslas kelti sumaištį plačiojoje visuomenėje. Kita vertus, šie incidentai rodo nuolatinį piktavalių susidomėjimą priežiūrinės kontrolės ir duomenų rinkimo sistemomis. Nors dalis atakų neturi didelio technologinio poveikio, jų sukeltas informacinis triukšmas naudojamas kaip **hibridinio karo elementas**, demonstruojant tariamus pajėgumus prieš NATO ir ES valstybes.

ENISA **Sektorinių grėsmių kraštovaizdžio 2025 m. ataskaitoje**[24] pažymi, kad **viešasis sektorius** ir **skaitmeninė infrastruktūra** išlieka prioritetiniais taikiniais visoje ES. Ekspertų vertinimu, tokios grėsmės kaip **duomenų vagystė, duomenų nutekėjimas** ir **išpirkos reikalavimo programinės įrangos** (angl. *Ransomware*) atakos išliks dažnos artimiausiu laiku. Dėl aktyvaus DI naudojimo šios grėsmės tik didės, taps pavojingesnės ir vis sunkiau identifikuojamos.

24
ENISA sektorinių grėsmių kraštovaizdis 2025 m. (angl. *ENISA Sectoral Threat Landscape 2025*).

NKSC žvilgsnis į 2026 m.

2026 m. kibernetinėje erdvėje išliks aktualios **duomenų nutekinimo, socialinės inžinerijos, išpirkos reikalavimo programinės įrangos (angl. *Ransomware*)** grėsmės, ir jas dar labiau sustiprins **DI** panaudojimas. Kibernetinės atakos taps labiau automatizuotos, tikslingesnės ir sunkiau atpažįstamos, o **žmogiškasis faktorius** ir toliau išliks viena silpniausių saugumo grandžių. Tikėtina, kad ir toliau tiek **įsilaužėliai aktyvistai**[25], tiek **priešiškų valstybių remiami kibernetiniai piktavaliai** veiks turėdami ideologinių motyvų, derindami viešą informacinį poveikį su tikslingais bandymais neteisėtai gauti prieigą prie organizacijų tinklų ir duomenų.

NKSC veiklos prioritetai, kuriems nuolat skiriamas didžiausias dėmesys:

- KSS brandos vertinimas ir kontrolė;
- Kibernetinių incidentų valdymo platformos vystymas, prijungiant KSS SOC ir automatizuojant duomenų apsikeitimą;
- kibernetinių grėsmių paieška;
- kibernetinių incidentų valdymas;
- prevencinių kibernetinio saugumo priemonių plėtra;
- kibernetinio saugumo kompetencijų ugdymas.

NKSC tolesni žingsniai stiprinant kibernetinį saugumą:

- parengti kibernetinės krizės valdymo mobilizacijos metu veiksmų planą ir ištestuoti jį per „Vyčio skliauto“ pratybas;
- stiprinti vidaus organizacinius procesus: sertifikuoti NKSC procesus ir paslaugas bei funkcijas pagal tarptautinius standartus (ISO; SIM3);
- diegti duomenimis grįsto paslaugų teikimo bei funkcijų vykdymo sprendimus (įskaitant DI panaudojimą);
- parengti ir pradėti įgyvendinti „Cyber Lietuva“ (angl. Cyber Campus LT) konceptą;
- sėkmingai užbaigti ES lėšomis įgyvendinamus projektus.

25 Įsilaužėliai aktyvistai (angl. *hacktivist*) – idealoginiais ir politiniais motyvais veikiantys kibernetiniai veikėjai, siekiantys informacinio poveikio ar spaudimo pasitelkdami kibernetines atakas.

Policijos veiklos apžvalga ir nusikalstamų veikų elektroninėje erdvėje tendencijos

Arūnas Paulauskas,
Lietuvos policijos generalinis komisaras

Vadovo žodis

Pastarieji metai dar kartą parodė, kad kibernetinės grėsmės nebėra izoliuotas technologinis reiškinys – jos vis dažniau susipina su dezinformacija, hibridinėmis grėsmėmis ir kasdieniais visuomenės įpročiais elektroninėje erdvėje. 2025 m. ypač išryškėjo poreikis greitai reaguoti, stiprinti tarpinstitucinį pasitikėjimą ir gebėjimą veikti koordinuotai, kai kinta ne tik grėsmių mastas, bet ir jų pobūdis. Šiame kontekste teisėsaugos vaidmuo išlieka esminis užtikrinant atsakomybę ir saugumą elektroninėje erdvėje. Žvelgiant į 2026 metus, prioritetu tampa ilgalaikio atsparumo stiprinimas – investuojant į žmones, partnerystes ir sprendimus, kurie leistų ne tik reaguoti, bet ir užbėgti grėsmėms už akių.

Policijos vaidmuo nacionalinėje kibernetinio saugumo ekosistemoje

Policija yra pagrindinė teisėsaugos institucija, atsakinga už nusikalstamų veikų elektroninėje erdvėje prevenciją, atskleidimą ir tyrimą, taip pat už reagavimą į su kibernetiniais incidentais susijusias nusikalstamas veikas. Policijos veikla prisideda prie bendros Lietuvos kibernetinio saugumo ir atsparumo sistemos užtikrinimo stiprinant teisės

2 838
policijoje registruotos nusikalstamos veikos, įvykdytos elektroninėje erdvėje, tai yra 28 proc. mažiau negu 2024 m.

10.5 %
nusikalstamų veikų, įvykdytų elektroninėje erdvėje, ištyrimo padidėjimas lyginant su 2024 m.

7 %
mažiau nusikalstamų veikų, susijusių su sukčiavimu. Tai pirmas kartas po tokių nusikalstamų veikų daugėjimo per pastaruosius 5 metus.

viršenybę kibernetinėje erdvėje, mažinant kibernetinių grėsmių poveikį visuomenei ir kritinei infrastruktūrai bei užtikrinant atsakomybės neišvengiamumą. Policijos vaidmuo skiriasi nuo kitų nacionalinių institucijų tuo, kad ji veikia kaip teisėsaugos institucija, turinti įgaliojimus vykdyti ikiteisminius tyrimus ir taikyti baudžiamąją atsakomybę už nusikaltimus, įvykdytus elektroninėje erdvėje.

11 000

policijos perduotų pranešimų apie žalingus išteklius (nuorodas, paskyras, finansų įstaigų sąskaitas ir pan.) suinteresuotoms institucijoms.

1 426

įgyvendintos prevencinės priemonės gyventojų sąmoningumui dėl nusikalstamų veikų elektroninėje erdvėje didinti.

42 020

gyventojų pasiekė policijos įgyvendintos sąmoningumo didinimo prevencinės priemonės.

2025 m. išmoktos pamokos, aplinkos pokyčiai, darę įtaką policijos veiklai

Policijai skirtas svarbus vaidmuo užtikrinant atsakomybės neišvengiamumą kibernetinėje erdvėje ir stiprinant visuomenės pasitikėjimą. 2025 m. policijos veiklą reikšmingai paveikė per pirmąjį 2025 m. pusmetį intensyviai augęs nusikalstamų veikų, įvykdytų elektroninėje erdvėje, mastas ir sudėtingumas bei spartus IRT naudojimas nusikalstamoms veikoms vykdyti. Policija privalėjo ne tik operatyviai reaguoti, bet ir stiprinti darbuotojų kompetencijas, tarpžinybinį bendradarbiavimą bei proaktyvų informacijos apsikeitimą su policijos nacionaliniais bei tarptautiniais partneriais. Policijos ir partnerių gebėjimas sutelkti pajėgas bei valdyti nusikalstamumo elektroninėje erdvėje rizikas padėjo reikšmingai sumažinti tokių nusikaltimų skaičių 2025 m. antrąjį pusmetį ir stabilizuoti nuo 2022 m. augusią jų dinamiką.

Nusikalstamos veikos elektroninėje erdvėje vis dažniau susipina su hibridinėmis grėsmėmis, todėl jų prevencija ir tyrimas turi būti integruoti į bendrą nacionalinę saugumo sistemą. 2025 m. patirtis parodė, kad veiksmingas kibernetinis saugumas priklauso nuo ankstyvo grėsmių nustatymo, koordinuoto institucijų veikimo ir operatyvaus teisėsaugos reagavimo. Policijai ir kitoms suinteresuotoms institucijoms svarbu pereiti prie veiklos modelių ir priemonių, susijusių su ilgalaikiu pajėgumų stiprinimu, technologinių sprendimų diegimu, siekiant pereiti nuo reagavimo prie prognozuojamo ir duomenimis grįsto veikimo kibernetinio saugumo srityje.

Nusikalstamumo elektroninėje erdvėje rizikos veiksniai nesikeičia – didžiausia grėsme išlieka socialinė inžinerija

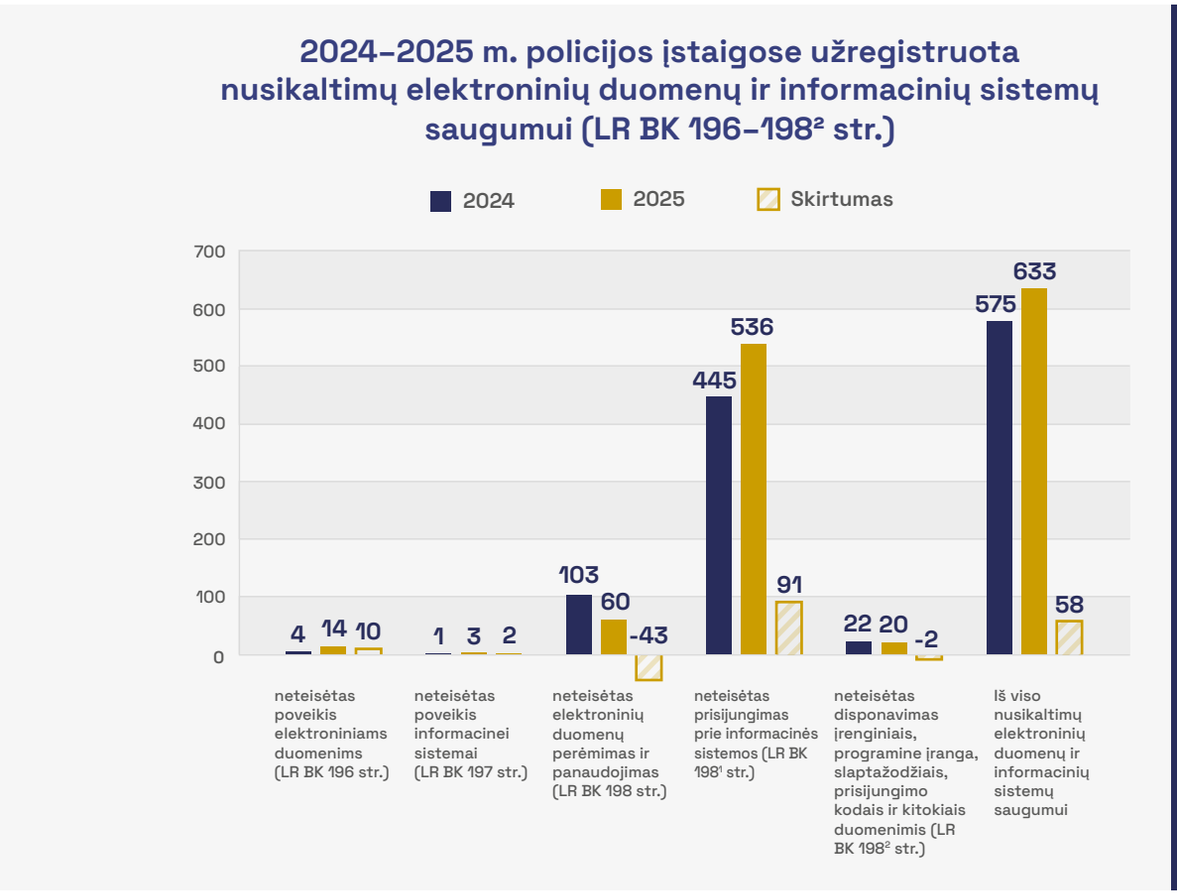
Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui būklės lygis išliko stabilus

Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – IRD prie VRM) duomenimis, 2025 m. policija užregistravo 633 nusikaltimus **elektroninių duomenų ir informacinių sistemų saugumui** (Lietuvos Respublikos baudžiamojo kodekso (toliau – LR BK) 196–198[2] str.), t. y. 58 nusikaltimais, arba 9,2 proc., daugiau nei 2024 m. Bendroje nusikalstamumo struktūroje nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui 2025 m. sudarė 2 proc., arba 1 proc. punktu, daugiau nei 2024 m. Nusikaltimų elektroninėje erdvėje siaurąja prasme kiekybiniai rodikliai 2025 m. (**1 pav.**):

- LR BK 196 str. „Neteisėtas poveikis elektroniniams duomenims“ – 2025 m. užregistruota 14 nusikaltimų (2024 m. – 4), tai yra 71,4 proc. daugiau nei 2024 m.;
- LR BK 197 str. „Neteisėtas poveikis informacinei sistemai“ – 2025 m. užregistruoti 3 nusikaltimai (2024 m. – 1), tai yra 66,7 proc. daugiau nei 2024 m.;
- LR BK 198 str. „Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“ – 2025 m. užregistruota 60 nusikaltimų (2024 m. – 103), tai yra 41,7 proc. mažiau nei 2024 m.;
- LR BK 198[1] str. „Neteisėtas prisijungimas prie informacinės sistemos“ – 2025 m. užregistruoti 536 nusikaltimai (2024 m. – 445), tai yra 17 proc. daugiau nei 2024 m.;
- LR BK 198[2] str. „Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis“ – 2025 m. užregistruota 20 nusikaltimų (2024 m. – 22), tai yra 9,1 proc. mažiau nei 2024 m.

Nusikaltimai elektroninėje erdvėje plačiąja prasme apibrėžiami kaip nusikaltimai, kuriems įvykdyti buvo naudojamos IRT, 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, nusikaltimo tikslas yra kompiuterinė sistema.



< 1 pav.

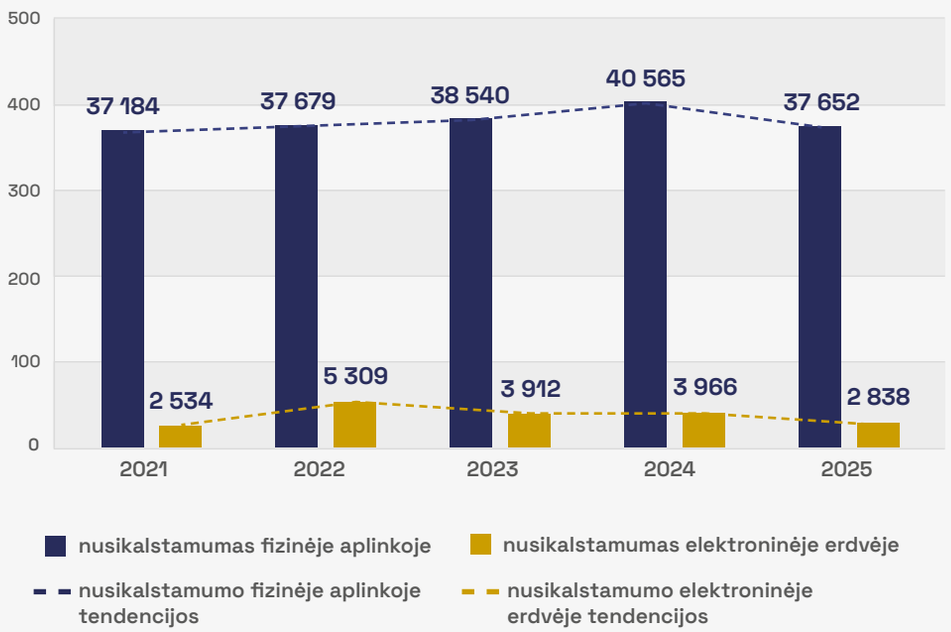
2024–2025 m. policijos įstaigose, atliekančiose ikiteisminius tyrimus, užregistruoti nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui *(šaltinis – IRD prie LR VRM)*

Pavojingiausių nusikalstamų veikų, įvykdytų elektroninėje erdvėje, susijusių su poveikiu informacinėms sistemoms ir (ar) jų duomenims (LR BK 196, 197, 198 str.), būklės lygis stabiliai išlieka žemas. Didžiausią riziką kelia neteisėtas prisijungimas prie informacinių sistemų (LR BK 198¹ str.), tačiau, policijos vertinimu, šių nusikalstamų veikų dinamika taip pat išlieka stabili ir nedideli svyravimai rodo, kad situacija yra valdoma.

Kitų nusikalstamų veikų, padarytų elektroninėje erdvėje, sumažėjo, tačiau sukčiavimas išieka aktualia problema

IRD prie VRM duomenimis, 2025 m. policija užregistravo 40 490 nusikalstamų veikų, iš jų 2 838 nusikalstamos veikos, arba 7 proc., **padarytos elektroninėje erdvėje**. Tokių nusikalstamų veikų, palyginti su 2024 m., sumažėjo 28 proc., arba 1 128 nusikalstamomis veikomis. 2025 m. nusikalstamų veikų, padarytų fizinėje aplinkoje, sumažėjo 7 proc., t. y. 2 913. Bendroje nusikalstamumo struktūroje nusikalstamų veikų, padarytų elektroninėje erdvėje, santykis 2025 m. sumažėjo 2 proc. punktais. 2025 m. sumažėjęs tiek bendrojo nusikalstamumo, tiek nusikalstamumo elektroninėje erdvėje lygis nerodo nusikalstamumo rizikos augimo. Ši situacija išlieka stabili pastaruosius penkerius metus (**2 pav.**).

2021–2025 m. policijos įstaigose užregistruotas nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui skaičius (LR BK 196–198[2] str.)



< 2 pav.

2021–2025 m. policijoje registruotas nusikalstamumas pagal padarymo vietos požymį *(šaltinis – IRD prie LR VRM)*

2025 m. išliko tendencija, kad nusikalstamumą elektroninėje erdvėje ypač lemia:

- sukčiavimas (LR BK 182 str.) – 44 proc. (palyginti su 2024 m., 37 proc. mažiau);
- nusikaltimai elektroninėje erdvėje siaurąja prasme – 21 proc. (palyginti su 2024 m., 9 proc. daugiau);
- neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas (LR BK 215 str.) – 15 proc. (palyginti su 2024 m., 4 proc. mažiau);
- disponavimas pornografiniu turiniu (LR BK 309 str.) – 7 proc. (palyginti su 2024 m., 28 proc. mažiau);
- 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. (palyginti su 2024 m., 10 proc. mažiau);
- kurstymas prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę (LR BK 170 str.) – 1 proc. (palyginti su 2024 m., 16 proc. daugiau);
- dokumento suklastojimas ar disponavimas suklastotu dokumentu (LR BK 300 str.) – 1 proc. (palyginti su 2024 m., 52 proc. mažiau);

- jaunesnio negu šešiolikos metų asmens tvirkinimas (LR BK 153 str.) – 1 proc. (palyginti su 2024 m., 60 proc. mažiau);
- šmeižimas (LR BK 154 str.) – 1 proc. (palyginti su 2024 m., 23 proc. mažiau).

2025 m. **sukčiavimas elektroninėje erdvėje**, siekiant turtinės naudos, sudarė didžiąją dalį – 81 proc. (16 proc. daugiau nei 2024 m.) – nusikalstamų veikų, įvykdytų elektroninėje erdvėje. Elektroniniai nusikaltimai, siekiant kitų tikslų, o ne turtinės naudos, 2025 m. sudarė 19 proc. ir jų buvo registruota nedaug:

- kibernetinis chuliganizmas;
- buitiniai konfliktai;
- duomenų nutekinimas;
- žmonių terorizavimas.

Sukčiavimas elektroninėje erdvėje: dominuoja apgaulingi skambučiai ir svetainių klastojimas internete

2025 m. dominavo tie patys sukčiavimo elektroninėje erdvėje būdai kaip ir 2024 m., tik apgaulingų skambučių ir svetainių klastojimo internete skaičius labai išaugo:

1. **apgaulingi telefoniniai skambučiai** (2025 m. sudarė 19 proc. Lyginant su 2024 m., jų padaugėjo 36 proc.);
2. **svetainių klastojimas internete** (2025 m. sudarė 16 proc. Lyginant su 2024 m., tokių atvejų padaugėjo 95 proc.).

Kitų sukčiavimo elektroninėje erdvėje atvejų, tokių kaip avansinis sukčiavimas, apgaulingos SMS žinutės, investicinis sukčiavimas, prekių ar paslaugų užvaldymas apgaule, grobstymas iš sąskaitų be socialinės inžinerijos požymio, apgaulingi elektroniniai laiškai, buvo registruota mažiau arba jų padaugėjimas yra vertinamas kaip nerizikingas. Policijos tiriami sukčiavimo elektroninėje erdvėje atvejai rodo, kad sukčiai naudojasi sukauptais duomenimis apie savo taikinius ir yra rizika, kad lengvai paveikiamos ir tampančios finansiškai priklausomos sukčiavimo aukos ateityje gali būti išnaudojamos ne vien kaip turtinių nusikaltimų netyčiniai bendrininkai, bet ir kitiems tikslams, pavyzdžiui, hibridinėms atakoms.

Apgaulingi telefoniniai skambučiai. 2025 m. sukčiavimo elektroninėje erdvėje atvejai, išsiskyrę sistemiškomis ypatingai didelės finansinės žalos padarymo pasekmėmis, buvo socialinės inžinerijos metodas, susijęs su apgaulingų telefoninių skambučių schemų taikymu. Spartus šio nusikalstamo reiškinio augimas prasidėjo 2024 m. ir tęsėsi visą 2025 m. pirmąjį pusmetį. Institucijų taikytos prevencinės priemonės padėjo valdyti riziką ir 2025 m. antroje pusėje registruotų atvejų, susijusių su apgaulingais telefoniniais skambučiais, lyginant su 2025 m. pradžios laikotarpiu, sumažėjo apie 1,4 karto. Teigiamą situacijos pokytį lėmė veiksmingos policijos ir kitų institucijų taikytos užkardymo ir prevencijos priemonės, dėl kurių buvo visiškai apribota telefoninių sukčių, naudojusių apgaulingų pranešimų apie nelaimę schemą, veikla.

2025 m. kovo ir gruodžio mėnesiais Lietuvos policija dalyvavo tarptautinėse operacijose, per kurias buvo atskleisti ir užkardyti Ukrainoje veikę skambučių centrai. Tai leido užbaigti dar nuo 2022 m. pradėtus ikiteisminius tyrimus.

Vis dėlto tenka konstatuoti, kad apgaulingų telefoninių skambučių grėsmės rizika išlieka aukšta dėl organizuoto nusikalstamumo įtakos. Jos pagrindinis veiksnys yra nuo 2024 m. sistemingai rusakalbių telefoninių sukčių taikomas ES teritorijoje migruojančių tarptautinių nusikalstamų grupių veiklos modelis. Jei 2024 m. telefoniniai sukčiai orientavosi į žemo informacinio raštingumo visuomenę ir aktyviausiai taikė apsimetėlių internetinės „Google“ platformos specialistais, bankininkais ir policininkais derinį, tai 2025 m. telefoniniai sukčiai aktyviai išnaudojo Lietuvoje pakeistą telefono numerių rašymo tvarką – apsimesdami ryšio operatorių atstovais, jie įtikindavo gyventojus, kad jų telefono numeriui iškilo problema.

Policijos vertinimu, apgaulingų telefoninių skambučių skaičius gali didėti dėl rizikos, susijusios su 2025 m. pradėtomis taikyti naujomis manipuliavimo schemomis: 1) bauginimu, kad nukentėjusieji finansuoja Rusijos kariuomenę; 2) nukentėjusiųjų išprovokavimu atskleisti duomenis ir (ar) perduoti grynuosius pinigus, banko korteles, apsimetant elektros tinklų, banko ir policijos darbuotojais; 3) fiktyvios kompensacijos siūlymu vaistų ir maisto papildų pirkėjams.

Telefoninio sukčiavimo grėsmė išsiskiria vis agresyvesne nusikaltėlių taktika ir skirtingo masto daroma žala. Nukentėjusieji ne tik patiria finansinių nuostolių, bet dažnai netyčia tampa ir nusikaltimų bendrininkais. 2025 m. apgaulingų skambučių organizatoriai pradėjo aktyviai išnaudoti nukentėjusiuosius kaip **sąskaitų mulus ir (ar) grynųjų pinigų kurjerius**. Tokiu būdu išnaudojami nukentėjusieji arba iš savo sąskaitų išgrynina pervestas svetimas lėšas ir jas perduoda atsiųstiems telefoninių sukčių kurjeriams, arba šiems gavėjams perduoda iš kitų apgautų žmonių paimtas siuntas su grynaisiais pinigais ir mokėjimo kortelėmis. 2025 m. ikiteisminių tyrimų duomenys rodo, kad anoniminiai apgaulingų skambučių

organizatoriai grynųjų pinigų kurjerius aktyviai verbuoja darbo skelbimais socialiniame tinkle „Facebook“ ir jų veiksmus koordinuoja virtualiai internetinio bendravimo programėlėje „Telegram“ sukurtose grupėse. 2025 m. taip pat nustatyta, kad apgaulingi skambučiai daugiausia susiję su asmens tapatybės duomenų išviliojimu. Užvaldyti svetimi biometriniai duomenys panaudojami banko sąskaitoms finansinių technologijų bendrovėse atidaryti, kad būtų atliekamos operacijos su nusikalstamu būdu gautomis lėšomis.

Policija nustato atvejus, kai nusikalstamos veikos elektroninėje erdvėje yra organizuojamos naudojant specialią techninę infrastruktūrą, teikiamą kaip paslauga kitiems nusikaltimams vykdyti. 2025 m. policija pradėjo 5 ikiteisminius tyrimus dėl **SIM spiečių įrangos**[01] (angl. *SIM box*), skirtos automatiniams skambučiams užtikrinti, bei skambučių peradresavimo vietos, iš kurios skambinama, maskavimo. Atlikta SIM spiečių įrangos duomenų analizė leido nustatyti, kad SIM kortelės buvo panaudotos sukčiavimui Lietuvoje. Atskleisti SIM spiečių įrangą administravę asmenys veikė arba individualiai, arba buvo oficialiai įsteigę kompiuterijos paslaugų teikimo verslą. Individualiai veikę asmenys naudojosi „Telegram“ grupėse veikiančių organizatorių ir jų administruojamų interneto svetainių paslaugomis.

Svetainių klastojimas internete. 2025 m. nauja išskirtine grėsme tapo svetainių klastojimas internete. Šis reiškinys tapo sistemingas 2024 m. lapkričio mėnesį ir nuosekliai dinamišku tempu augo iki 2025 m. birželio mėnesio. Policija operatyviai reagavo ir aktyviai dalyvavo vykdant apsimestinių svetainių blokavimą. 2025 m. antrąjį pusmetį registruotų atvejų, susijusių su prisijungimu prie klastotų svetainių, sumažėjo apie 2,5 karto, tačiau nuo spalio mėn. vėl išryškėjo lėtas augimas. Tai rodo, kad sukčiavimo organizatoriai laukia tinkamos progos naujai svetainių klastojimo internete bangai sukelti, todėl ši nusikalstama veikla ilgam gali tapti vienu dominuojančių sukčiavimo būdų. Sistemingą svetainių klastojimo internete reiškinį galėjo paskatinti 2023 m. pradėtos tarpinstitucinės prevencinės veiklos, itin apribojusios sukčių galimybes nuorodas į apsimestines svetaines platinti apgaulingomis telefoninėmis žinutėmis ir internetinio bendravimo priemonėmis. Svetainės internete klastojamos, siekiant užvaldyti elektroninės bankininkystės vartotojų ir jų finansinių instrumentų duomenis, kad būtų galima grobti lėšas iš sąskaitų. 2025 m. sukčiai sistemingai klastojo plačiai visuomenėje naudojamų viešųjų ir finansų paslaugų subjektų interneto svetaines: sveikatos (*esveikata*), mokesčių (VMI, EDS), socialinės apsaugos (SODRA), nuosavybės registravimo (Registrų centras, REGITRA), draudimo (Lietuvos draudimas), energetikos paslaugų (*Elektrum*, *Ignitis*, ESO, *Enefit*), telekomunikacijos paslaugų (TELE2), bankininkystės (*Artea*, SEB, *Swedbank*), viešojo susisiekimo (JUDU), parkavimo vietų (UNIPARK). Interneto svetainė *esveikata.lt* buvo sistemingai klastojama, kai į pabaigą artėjo Lietuvos vairuotojams valstybės nustatytas sveikatos pažymėjimų atnaujinimo terminas. VMI, EDS, SODROS svetainių klastojimas sutapo su Lietuvos gyventojams valstybės nustatytu turto deklaravimo terminu. 2025 m. pabaigoje tiksliniais sukčiavimo taikiniais tapo bankų (SEB, Swedbank) klientai.

01
SIM spiečių įranga – tai įrenginys, kuris naudoja didelį kiekį SIM kortelių (dažniausiai mobiliųjų operatorių), kad galėtų nukreipti ar priimti telefono skambučius bei tekstinius pranešimus, veikia prijungtas prie kompiuterinės įrangos, gali būti naudojamas nusikalstamoms veikoms vykdyti.

Apgaulingos SMS žinutės. Dėl 2023 m. pradėtos veiksmingos tarpinstitucinės prevencinės veiklos žymiai sumažėjo nuorodų platinimo apgaulingomis žinutėmis į apsimestines svetaines atvejų, tačiau 2025 m. pabaigoje atsirado rizikos ženklų, kad apgaulingos SMS žinutės vėl tampa sistemingu reiškiniu. 2025 m. sukčiavimo organizatoriai pradėjo siųsti apgaulingus pranešimus apie prievolę sumokėti baudą tokiems viešųjų paslaugų teikėjams, kaip policija (e. policija, e. protokolas, policijoje registruoto įvykio identifikacinis kodas (ROIK), parkavimo įmonė (UNIPARK), viešojo susisiekimo įmonė (JUDU).

Sukčiavimo atvejai, pasižymintys didele finansine žala. 2025 m. 25 proc. daugiau nei 2024 m. buvo registruota sukčiavimų, kurie dėl didelės finansinės žalos ir (ar) organizuoto bendrininkavimo yra kvalifikuojami kaip sunkūs nusikaltimai. Atvejai, kai sukčiavimo būdu buvo užvaldyta daugiau nei 10 tūkst. eurų, 2025 m. sudarė 18 proc., ir tai yra 16 proc. daugiau nei 2024 m. Tai lėmė išaugęs sukčių gebėjimas nustatyti mažiausiai socialinės inžinerijos metodams atsparias visuomenės grupes, taip pat gerai žinoti jų finansinę padėtį ir tikslingai orientuotis į šiuos pagrindinius sukčiavimo taikinius. Finansų rinkos dalyvių duomenimis, iš Lietuvos gyventojų ir juridinių asmenų 2025 m. apgaule buvo kėsintasi išvilioti 58,8 mln. eurų, tačiau finansų įstaigoms pavyko apsaugoti 38 mln. eurų, tai yra virš dviejų kartų daugiau negu 2024 m., kai buvo apsaugota apie 15 mln. eurų. 2025 m. gyventojų patirti nuostoliai siekė 20,5 mln. eurų, tai yra nežymiai daugiau (apie 0,5 mln. eurų) lyginant su 2024 m.[02]

2025 m. nustatyti 3 (2024 m. – 1) įsilaužimo į finansų įmonių vidaus informacines sistemas atvejai. Finansų įstaigos yra įtrauktos į Kibernetinio saugumo subjektų registrą, todėl 2025 m. atakų prieš šiuos subjektus padažnėjimas kelia susirūpinimą. 2 atvejai buvo susiję su įsilaužimu į finansų įmonių vidaus sistemas ir lėšų iš administruojamų klientų sąskaitų pasisavinimu. 3-iasis įvykis buvo susijęs su vieno iš Lietuvos bankų veiklos trikdymu, organizavus DDoS ataką prieš banko interneto svetainę.

Dažniausi nusikalstamų veikų elektroninėje erdvėje būdai. 2025 m. **išpirkos reikalavimo programinės įrangos** (angl. *Ransomware*) kodo virusų atvejų tarp kitų nusikalstamų veikų elektroninėje erdvėje buvo fiksuota vos 1 proc., ir tokių atvejų skaičius išliko panašus kaip ir 2024 m. **DDoS atakos** 2025 m. tarp visų nusikalstamų veikų elektroninėje erdvėje sudarė iki 1 proc. – panašiai kaip ir 2024 m. Policijos teigimu, šios nusikalstamos veikos 2025 m. nebuvo sistemingos ir masinės, todėl tokių nusikalstamų veikų rizika išliko nuosekliai neaukšta.

Išskirtinis 2025 m. pokytis buvo tas, kad staiga pradėjo dominuoti atvejai, **susiję su svetainių klastojimu internete**: šie atvejai tarp visų nusikalstamų veikų elektroninėje erdvėje sudarė 32 proc. ir jų, lyginant su 2024 m., padaugėjo 92 proc. Kiti dominuojantys įsilaužimo į informacines sistemas būdai išliko tokie patys kaip ir 2024 m., ir jų 2025 m. užregistruota mažiau nei 2024 m., arba jų padidėjimas yra vertinamas kaip nerizikingas: apgaulingų žinučių, skambučių, elektroninių laiškų, svetimų banko mokėjimo kortelių panaudojimo atvejai.

02
VšĮ Pinigų plovimo prevencijos kompetencijų centro 2025 m. duomenys.

Dažniausi nusikalstamų veikų elektroninėje erdvėje padariniai. 2025 m. nusikalstamos veikos elektroninėje erdvėje turėjo tokius pat padarinius kaip ir 2024 m., pavyzdžiui: elektroninių duomenų stebėjimas ar pasisavinimas, elektroninių duomenų neteisėtas paskelbimas, paskyrų perėmimas ir kt. Tačiau išliko ilgametė tendencija, kad dažniausi ir labiausiai dominuojantys elektroninių nusikaltimų padariniai yra neteisėtos finansinės operacijos užvaldytose svetimose banko sąskaitose. Tokie atvejai 2025 m. sudarė 63 proc. ir, lyginant su 2024 m., jų padaugėjo 18 proc.

2025 m. pirmą kartą nustatyta požymių, kad užvaldytos svetimų vartotojų mobiliųjų programėlių paskyros buvo naudojamos vertimuisi ūkine, komercine veikla, neturint leidimo ar licencijos, taip pat siekiant nuslėpti pajamas ir išvengti mokesčių. Šios rizikos veiksniai susiję su Lietuvoje apsigyvenusių karo pabėgėlių ar ekonominių migrantų neteisėtais interesais. Pavyzdžiui, imigrantas, užvaldęs svetimą BOLT programėlės vartotojo paskyrą, įgijo profesinei kvalifikacijai ir ūkinės veiklos teisėtumui pagrįsti būtinus svetimus dokumentus ir tokiu būdu neteisėtai vertėsi pavežėjo veikla.

2025 m. pirmą kartą nustatyta nusikalstamos veikos schema, skirta vartotojų SIM kortelėms perimti – nusikalstamai veikęs asmuo nuotoliniu būdu, identifikuodamasis vogta tapatybe, užsakydavo ryšio operatoriaus paslaugą dėl SIM kortelės keitimo į virtualią e-SIM kortelę. Užvaldyti abonentiniai telefono numeriai buvo panaudoti prieigai prie svetimų socialinių tinklų ir el. pašto vartotojų paskyrų. SIM kortelės nutekinimas ypatingai grėsmingas, nes nukentėjusieji gali prarasti visas savo interneto paslaugas ir visą savo sukurtą veiklą bei gyvenimą elektroninėje erdvėje.

Dažniausiai atakuotos informacinės sistemos. 2025 m. dažniausiai nusikalstamos veikos elektroninėje erdvėje buvo nukreiptos į elektroninės bankininkystės vartotojų paskyras. Tokie atvejai 2025 m. sudarė 74 proc. ir, lyginant su 2024 m., jų padaugėjo 15 proc. Kitos nusikalstamos veikos elektroninėje erdvėje buvo nukreiptos į tuos pačius taikinius kaip ir 2024 m., pavyzdžiui: į informacinių sistemų vartotojų paskyras, socialinių tinklų paskyras, elektroninio pašto paskyras ir kt.

Atakuoti ar neteisėti (neteisėtai paskelbti) elektroniniai duomenys. 2025 m. aktyviųjų atakų, nukreiptų į valstybės ir tarnybos paslaptis, elektroninėje erdvėje nebuvo. 2025 m. išliko ilgametė teigiama tendencija, susijusi su sąlyginai maža tokių nusikalstamų veikų rizika jautriai valstybės valdymo, nacionalinio saugumo ir institucijų veiklos informacijai. Atkreiptinas dėmesys, kad tiek 2025 m., tiek per pastaruosius penkerius metus šios nusikalstamos veikos žalingų padarinių įslaptintai informacijai nesukėlė. 2025 m. išliko ilgametė tendencija, kad dažniausiai nusikalstamos veikos elektroninėje erdvėje buvo orientuotos į elektroninius mokėjimo instrumentus ir (ar) jų vartotojų duomenis. Tokie atvejai 2025 m. sudarė 77 proc. ir, lyginant su 2024 m., jų padaugėjo 13 proc.

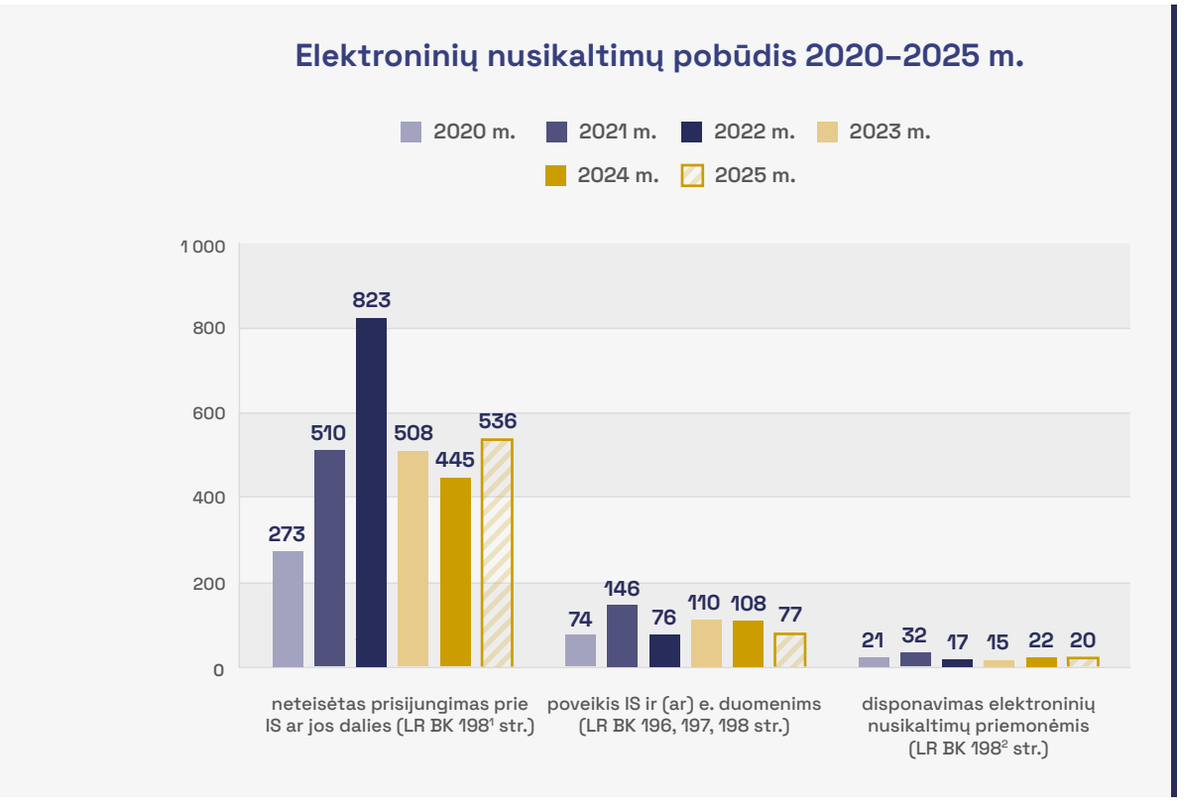
Tačiau 2025 m. nustatyti 5 (2024 m. – 3) **neteisėto duomenų stebėjimo ar nutekinimo iš valstybės informacinių sistemų atvejai** rodo rizikos valstybės informaciniams ištekliams padidėjimą. Keturi 2025 m. atvejai buvo susiję su personalo tarnybiniu piktnaudžiavimu ir nutekintų duomenų panaudojimu nusikalstamiems tikslams.

2025 m. nustatyti 2 atvejai (2024 m. – 8), susiję su nutekintų duomenų realizavimu elektroninėje erdvėje. Iš dovanų kuponais prekiaujančios Lietuvos įmonės informacinės sistemos nutekinti klientams parduotų dovanų kuponų duomenys buvo panaudoti suklastotiems kuponams gaminti, siekiant klastotes realizuoti. Atliekant ikiteisminį tyrimą dėl vienos iš Lietuvos viešojo maitinimo įmonės duomenų užšifravimo buvo nustatyta, kad išpirkos (angl. *Ransomware*) reikalavimo programišių grupuotė „Black Nevas“ savo tamsiajame internete (angl. *Dark Net*) platina iš įmonės duomenų bazės nutekintus klientų duomenis.

Atakuoti subjektai. 2025 m. nusikalstamų veikų elektroninėje erdvėje, nukreiptų prieš Lietuvos valdžios institucijų, ministerijų, nacionalinio, viešojo saugumo, krašto apsaugos, teisėsaugos, ikiteisminio tyrimo institucijų informacines sistemas, nebuvo. 2025 m. atskleistas vienas duomenų nutekinimo iš teismų informacinės sistemos atvejis siejamas su tarnybiniu piktnaudžiavimu dėl savanaudiškų paskatų ir jis neturėjo kenkimo valstybei tikslų. Pastarųjų penkerių metų stebėsena rodo, kad nusikalstamoms veikoms elektroninėje erdvėje prieš valstybės institucijų informacines sistemas nėra būdingi sistemingai ir masiškai organizuojamo kenkimo požymiai, todėl valstybės institucijų informacinių sistemų situacija išlieka neaukštos rizikos. Tačiau išlieka ilgalaikė tendencija, kad nusikalstamos veikos elektroninėje erdvėje dažniausiai yra nukreiptos prieš elektroninės bankininkystės vartotojus (juridinius ir fizinius asmenis). Tokie atvejai 2025 m. sudarė 76 proc. ir jų, lyginant su 2024 m., padaugėjo 16 proc.

Saugumo aplinkos pokyčiai ir tendencijos

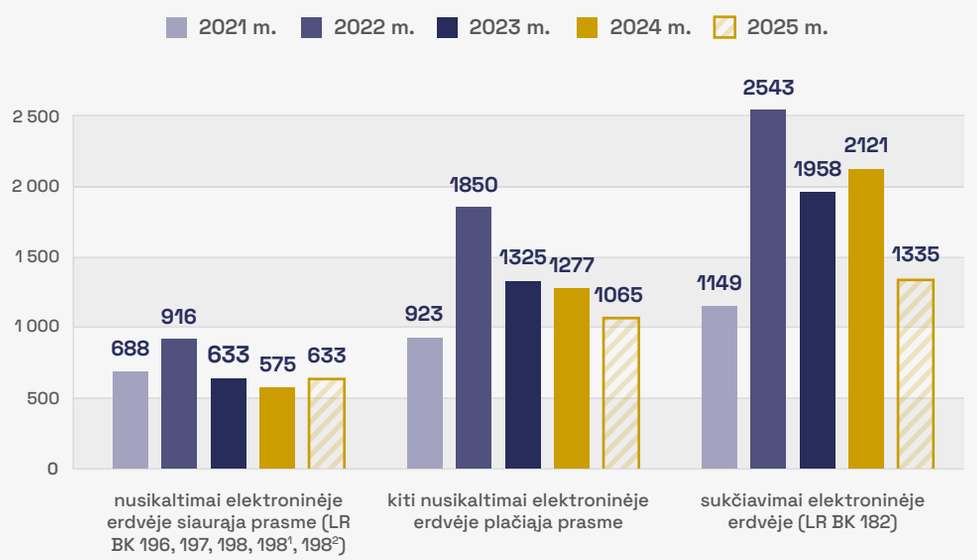
Pastarųjų penkerių metų duomenys rodo, kad policija veiksmingai kontroliuoja **nusikalstamumą elektroninėje erdvėje siaurąja prasme**. Pavojingiausių nusikalstamų veikų, įvykdytų elektroninėje erdvėje, susijusių su poveikiu informacinėms sistemoms ir (ar) jų duomenims (LR BK 196, 197, 198 str.), būklės lygis stabiliai išlieka žemas, o 2025 m. net sumažėjo. Nusikalstamų veikų, susijusių su disponavimu priemonėmis, skirtomis nusikalstamoms veikoms elektroninėje erdvėje vykdyti (LR BK 198[2] str.), skaičius rodo, kad policija nuolat atskleidžia ypatingai sudėtingus nusikaltimus ir atseka jų padarymo įrankius. Didžiausią nusikalstamumo elektroninėje erdvėje riziką kelia neteisėtas prisijungimas prie informacinių sistemų (LR BK 198[1] str.), tačiau šių nusikalstamų veikų dinamika išlieka stabili, ir nedideli svyravimai rodo, kad situacija yra valdoma (**3 pav.**).



< 3 pav.

Policijoje registruotų kibernetinių nusikaltimų, klasifikavus pagal poveikio pobūdį, 2020–2025 m. dinamika Lietuvoje
(šaltinis – IRD prie LR VRM)

Nors 2025 m. esmine tiek bendrojo nusikalstamumo, nusikalstamumo elektroninėje erdvėje problema išliko **sukčiavimas elektroninėje erdvėje**, šio nusikaltimo būklės lygis po spartaus augimo per 2022–2024 m. laikotarpį dinamiškai krito, ir tai rodo, kad situacija stabilizavosi. Stabilią ir nedidėjančią nusikalstamumo elektroninėje erdvėje situaciją patvirtina ir tai, kad 2025 m. kito nusikalstamumo elektroninėje erdvėje, išskyrus sukčiavimą, lygis išliko panašus kaip ir per pastaruosius penkerius metus. Ši tendencija rodo, kad valstybė išlieka atspari kibernetinėms atakoms ir geba valdyti nusikalstamumo elektroninėje erdvėje rizikas bei jų poveikį bendrai nusikalstamumo situacijai šalyje (**4 pav.**).



< 4 pav.

Policijoje registruotų elektroninių nusikaltimų elektroninėje erdvėje 2021–2025 m. dinamika Lietuvoje *(šaltinis – IRD prie LR VRM)*

2025 m. kovo 27 d. reaguodami į labai išaugusį sukčiavimų elektroninėje erdvėje mastą, **Lietuvos policija, Lietuvos Respublikos generalinė prokuratūra, NKSC, RRT, Lietuvos bankas ir VšĮ Pinigų plovimo prevencijos kompetencijų centras** pasirašė **Memorandumą dėl bendradarbiavimo siekiant mažinti sukčiavimo skaitmeninėje erdvėje atvejus**. Šiuo memorandumu buvo įtvirtinti operatyvaus informacijos apsikeitimo tarp šių institucijų, bendrai taikomų prevencinių priemonių ir koordinuotų veiksmų principai, skirti greitam sukčiavimo schemų identifikavimui ir nutraukimui. Memorandume numatyta, kad policija realiuoju laiku vykdo nuolatinę gaunamų pranešimų apie sukčiavimus ar bandymus sukčiauti stebėseną, užtikrina greitą reagavimą ir koordinuotų veiksmų vykdymą pagal kompetenciją, įgyvendina nusikalstamų veikų ir administracinių nusižengimų skaitmeninėje erdvėje atskleidimą ir atlieka jų tyrimą, organizuoja gyventojų švietimo kampanijas ir prevencines priemones. Taip pat numatyta vykdyti nuolatinę įvykių analizę ir teikti pasiūlymus dėl efektyvesnio jų užkardymo, teisinio reguliavimo tobulinimo. Užtikrintas operatyvesnis informacijos apsikeitimas ir bendros iniciatyvos su finansų ir ryšių sektoriumi yra viena efektyviausių priemonių stiprinant nacionalinį atsparumą sukčiavimui elektroninėje erdvėje ir leidžia greičiau identifikuoti nusikalstamas schemas bei užkirsti kelią daromai žalai.

Dar iki Memorandumo pasirašymo 2025 m. sausio 27 d. policijoje sustiprintas darbo **24/7 režimu modelis**, užtikrinantis nuolatinį nenutrūkstamą reagavimą į sukčiavimą elektroninėje erdvėje ir apsikeitimą informacija su partneriais realiuoju laiku. Šis veiklos organizavimo

pokytis leido reikšmingai sutrumpinti reagavimo į pranešimus apie sukčiavimą laiką, operatyviau blokuoti nusikalstamas finansines operacijas ir žalingas nuorodas bei užkirsti kelią tolimesnei žalai gyventojams bei verslui.

2025 m. buvo tęsiama **policijos virtualaus patrulio** veikla, siekiant įspėti interneto vartotojus apie gresiančius pavojus dėl galimų sukčiavimų bei įžymių asmenų paskyrų ir kitų duomenų vagysčių elektroninėje erdvėje. Policijos virtualus patrulis 2025 m. savo „Facebook" paskyroje paskelbė 103 prevencinius pranešimus. Per 2025 m. policijos virtualus patrulis nustatė ir užregistravo 577 galimus teisės pažeidimus (2024 metais – 505 pažeidimus), iš kurių dėl 56 pradėti ikiteisminiai tyrimai, dėl 415 – administracinio nusižengimo bylų teisenos, o dėl 42 asmenims buvo surengti prevenciniai pokalbiai, jie oficialiai įspėti. Policijos virtualus patrulis socialiniame tinkle „Facebook" dėl galimų neapykantos kurstymo atvejų, viešosios tvarkos pažeidimų bei sukčiavimų viešai įspėjo 1 854 vartotojus. Be to, policijos virtualaus patrulio iniciatyva užblokuota 2 451 „Facebook" vartotojų netikra ar užvaldyta paskyra ir kiti puslapiai. Tai rodo reikšmingą policijos prevencinės veiklos suaktyvėjimą.

Atsižvelgdama į nusikaltimus elektroninėje erdvėje tarptautiniame kontekste, Lietuvos policija 2025 m. toliau tęsė aktyvų bendradarbiavimą su kitomis ES šalių teisėsaugos institucijomis: dalyvavo įgyvendinant **Europos kovos su nusikalstamumo grėsmėmis tarpdisciplininės platformos prioritetus** kovojant su sparčiausiai augančiais nusikaltimais elektroninėje erdvėje: kibernetiniais išpuoliais, vaikų seksualiniu išnaudojimu internete ir sukčiavimo internete schemomis.

2025 m. išryškėjo tam tikri esamo **teisinio reguliavimo apribojimai**. Sparčiai besikeičiant technologijoms ir dažnėjant jų naudojimui nusikalstamose veikose (pavyzdžiui, DI, SIM spiečių įranga) atsirado poreikis atnaujinti teisinį reguliavimą, sustiprinti policijos pareigūnų analitines kompetencijas. Identifikuotos situacijos, kai esamas teisinis reguliavimas ar procedūros ne visuomet leidžia pakankamai greitai gauti ir panaudoti ikiteisminiam tyrimui reikalingus duomenis bei ne visais atvejais galima efektyviai vykdyti baudžiamąjį persekiojimą už tam tikrus neteisėtus veiksmus.

Visuomenės elgsenoje 2025 m. vyravo prieštaringos tendencijos – vertinant policijos gautus pranešimus, paaiškėjo, kad dalis gyventojų tapo labiau informuoti ir kritiškesni kibernetinių grėsmių atžvilgiu, tačiau sukčiams taikant personalizuotus sukčiavimo scenarijus, išliko pažeidžiamų grupių, kurios dėl skaitmeninių įgūdžių stokos ar emocinio spaudimo tapo pagrindiniais sukčiavimo taikiniais. Be to, augantis skaitmeninių paslaugų naudojimas, nuotoliniai finansiniai sprendimai ir socialinių tinklų populiarumas didina tiek nusikalstamų veikų elektroninėje erdvėje rizikų mastą, tiek jų suvaldymo sudėtingumą.

DI ir automatizacijos poveikis saugumo aplinkai

Nors tiriant nusikalstamas veikas elektroninėje erdvėje kol kas fiksuojami tik pavieniai akivaizdūs DI panaudojimo atvejai, ryškėja tendencija, kad nusikalstamas veikas vykdantys asmenys vis dažniau pasitelkia DI sprendimus. DI naudojamas automatizuotam apgaulingų pranešimų generavimui, realistiškam kalbos ir vaizdo klastojimui, taip pat nukentėjusiųjų profiliavimui, pasitelkiant viešai prieinamus ar nutekintus duomenis. Taip kuriami vis įtikinamesni ir sunkiau atpažįstami sukčiavimo scenarijai.

DI plėtra sudaro sąlygas nusikalstamas veikas vykdyti didesniu mastu ir greičiu, jas personalizuoti ir vykdyti realiuoju laiku, dažnai be tiesioginio žmogaus įsikišimo. Ypač reikšmingas DI poveikis socialinės inžinerijos srityje, kai manipuliuojama emocijomis ir pasitikėjimu institucijomis, imituojant valstybės institucijų ar finansų įstaigų komunikaciją.

DI leidžia vykdyti vis sudėtingesnius nusikaltimus, jiems vis sunkiau užkirsti kelią vien prevencinėmis priemonėmis, todėl policijai būtina stiprinti analitinius pajėgumus, diegti pažangias duomenų analizės priemones ir trumpinti sprendimų priėmimo laiką.

2025 m. **Sunkaus ir organizuoto nusikalstamumo grėsmių ES vertinime**[03] (toliau – **SOCTA ataskaita**), kurį kas ketverius metus atlieka **Europos Sąjungos teisėsaugos bendradarbiavimo agentūra** (angl. *European Union Agency for Law Enforcement Cooperation* (EUROPOL) (toliau – **Europolas**), pažymėta, kad spartus DI ir kitų naujųjų pažangių technologijų, tokių kaip blokų grandinės ar kvantinė kompiuterija, vystymasis ypač lemia sunkaus ir organizuoto nusikalstamumo augimą. Dėl šių technologijų nusikalstamos operacijos tampa veiksmingesnės, operatyvesnės, lengviau pasiekiamos, išradingesnės ir sunkiau atsekamos. Minėtame dokumente nurodyta, kad su **DI plėtra siejamos šios grėsmės**:

- **daugės kibernetinių atakų prieš ypatingos svarbos infrastruktūrą, vyriausybes, įmones ir visuomenę; atakų organizatoriai pastaruoju metu siekia ne tik pelno, bet veikia ir dėl ideologinių įsitikinimų, turi destabilizacijos tikslų;**
- **elektroninio sukčiavimo mastas padidės, nes DI padės organizuoti socialinę inžineriją ir palengvins prieigą prie duomenų;**
- **seksualinis vaikų išnaudojimas internete padidės dėl vaikų pornografijos turinio (angl. *Child Sexual Abuse Material*, CSAM) kūrimo ir nusikaltėlių internetinio saugumo užtikrinimo DI priemonėmis;**
- **neteisėtos migracijos, kaip hibridinio karo instrumento, organizatoriams DI padės naudotis skaitmenine rinkodara, užtikrins palankesnes verbavimo ir finansinių operacijų galimybes;**
- **DI padės elektroninėje erdvėje neteisėtai prekiauti narkotikais, šaunamaisiais ginklais, atliekomis.**

03 2025 m. Sunkaus ir organizuoto nusikalstamumo grėsmių Europos Sąjungai vertinimas (angl. *EU Serious and Organised Crime Threat Assessment (EU-SOCTA 2025)*.

Kita vertus, atkreiptinas dėmesys, kad DI policijoje vertinamas ne tik kaip grėsmių šaltinis, bet ir kaip priemonė, galinti ateityje sustiprinti prevenciją bei reagavimo efektyvumą. 2025 m. **Lietuvos kriminalinės policijos biuras** skyrė ypatingai didelį dėmesį, kad būtų sukurtas ir įdiegtas **pažangus technologinis įrankis** teisėsaugos institucijų analitinei veiklai tobulinti. Pažangaus analitinio technologinio įrankio diegimas sudaro prielaidas reikšmingai sustiprinti duomenimis grįstą analizę ir sudėtingų, tarpvalstybinių kibernetinių nusikaltimų atskleidimą, prisidedant prie efektyvesnės nacionalinės kibernetinio saugumo ir atsparumo sistemos.

Atsižvelgiant į DI plėtros tendencijas, jis išlieka ilgalaikiu iššūkiu nacionaliniam kibernetiniam saugumui, reikalaujančiu nuolatinio teisėsaugos institucijų darbuotojų kompetencijų stiprinimo, teisinio reguliavimo adaptavimo ir tarpinstitucinio bendradarbiavimo.

Rizikos, susijusios su priklausomybe nuo išorinių paslaugų teikėjų ir tiekimo grandinių

Tiriant nusikalstamas veikas elektroninėje erdvėje, policijos veiklos efektyvumas reikšmingai priklauso nuo įvairių išorinių technologinių ir paslaugų ekosistemos dalyvių. Didelė dalis skaitmeninių pėdsakų, reikalingų nusikalstamoms veikoms ar jų vykdytojams identifikuoti, yra kaupiama ir valdoma elektroninių ryšių paslaugų teikėjų, debesijos infrastruktūros operatorių bei kitų tarpininkų, todėl tyrimų operatyvumas dažnai priklauso nuo šių subjektų techninių galimybių ir tarptautinio bendradarbiavimo procedūrų greičio. Nusikaltėliai dažnai panaudoja paslaugų teikėjus, veikiančius už ES ribų, ir tampa sunkiau operatyviai gauti duomenis (pvz.: Azijos šalių prieglobos paslaugų teikėjai, tarpiniai serveriai JAV ir pan.). Tikėtina, kad dalį su duomenų gavimo trukme susijusių problemų padės spręsti nuo 2026 m. pradedamas taikyti naujas Europos Sąjungos teisinis reguliavimas: 2023 m. balandžio 12 d. **Europos Parlamento ir Tarybos reglamentas (ES) 2023/1543**[04] bei 2023 m. liepos 12 d. **Europos Parlamento ir Tarybos direktyva (ES) 2023/1544**[05]. Šis teisės aktų paketas turėtų sudaryti prielaidas teisėsaugos institucijoms greičiau ir tiesiogiai kreiptis į skaitmeninių paslaugų teikėjus dėl tyrimams reikalingų duomenų išsaugojimo ir jų pateikimo.

Tiriant sukčiavimo, neteisėto prisijungimo prie informacinių sistemų ar kitus su finansiniais srautais susijusius nusikaltimus, tyrimų efektyvumas priklauso nuo finansų įstaigų ir virtualiųjų valiutų platformų bendradarbiavimo. Sukčiams įgijus galimybę per kelias sekundes ar minutes pervesti lėšas, teisėsaugos galimybės operatyviai gauti reikalingus duomenis ar inicijuoti procesinius veiksmus, susijusius su lėšų identifikavimu ar jų judėjimo stabdymu, dažnai priklauso nuo formalių teisinių procedūrų ar tarptautinio bendradarbiavimo procedūrų, kurios gali užtrukti kelias savaites, o kartais – ir mėnesius. Atsižvelgiant į tai, svarbu plėtoti Europos Sąjungos lygmens teisinį reguliavimą, įgalinant teisines ir technines priemones, kurios sudarytų galimybes identifikuoti ir sulaikyti lėšas.

04
2023 m. liepos 12 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/1543 dėl Europos įrodymų pateikimo orderių ir Europos įrodymų saugojimo orderių elektroniniams įrodymams baudžiamajame procese ir laisvės atėmimo bausmių vykdymui pasibaigus baudžiamajam procesui.

05
2023 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva (ES) 2023/1544, kuria nustatomos suderintos paskirtųjų įmonių ir teisinių atstovų skyrimo elektroniniams įrodymams baudžiamajame procese rinkti taisyklės.

Papildomos įžvalgos iš kitų ataskaitų

Tarptautinės grėsmės

ES Taryba, atsižvelgdama į SOCTA ataskaitą, 2025 m. birželio 13 d. patvirtino **ES 2026–2029 m. politinio ciklo prioritetus**[06], tarp kurių nustatyta nusikalstamumo elektroninėje erdvėje kontrolė ir numatytas sustiprintas teisėsaugos reagavimas į didžiausias **pastarojo laikotarpio grėsmes**, t. y.:

- kibernetinės atakos
- vaikų seksualinis išnaudojimas internete
- sukčiavimo elektroninėje erdvėje schemos

Koordinuojant Europolui, 2026–2029 m. ciklui suplanuotas priemones, skirtas pavojingiausiam kibernetiniam nusikalstamumui užkardyti, įgyvendins bendradarbiaujančių ES šalių teisėsaugos institucijos, tarp kurių savo uždavinius vykdys ir Lietuvos policija.

2025 m. Organizuoto nusikalstamumo internete grėsmių vertinimo ataskaitoje[07] (toliau – **IOCTA ataskaita**) Europolas kaip ir kasmet apžvelgė nusikalstamų veikų elektroninėje erdvėje ekosistemą ES ir analizavo šio nusikalstamumo padarinius, vykdytojų ir nukentėjusiųjų savybes. Pateiktose ataskaitos išvadose ypatingai akcentuota **duomenų vagysčių grėsmė**, siejama su šiomis aplinkybėmis:

- **Nutekintus duomenis nusikaltėliai naudoja ir kaip prekę, ir kaip priemonę tokiems kibernetiniams nusikaltimams, kaip kibernetinės atakos, sukčiavimas elektroninėje erdvėje, seksualinis vaikų išnaudojimas internete, turto prievartavimas, daryti.**
- **Duomenų nutekinimo organizatoriai naudojasi didele metodų, specializuotų konkretiems nusikaltimų darymo etapams, įvairove, išnaudodami tiek informacinių sistemų, tiek žmonių pažeidžiamumą. Vienu iš populiariausių metodų išlieka socialinė inžinerija. Neteisėtų duomenų ekosistemas, bendrininkaudami su nusikalstamais tinklais, aktyviai išnaudoja į hibridinį karą įsitraukę subjektai; jie yra auganti grėsmė valstybės duomenų saugumui.**

06
ES Tarybos išvados dėl Europos daugiadisciplininės platformos kovai su nusikalstamomis grėsmėmis (EMPACT) stiprinimo ir ES kovos su nusikalstamumu prioritetų kitam Europos daugiadisciplininės platformos kovai su nusikalstamomis grėsmėmis (EMPACT) ciklui 2026–2029 m. (angl. *Council Conclusions on the Enhancement of EMPACT and on EU Crime Priorities for the Next EMPACT Cycle* 2026–2029).

07
2025 m. Organizuoto nusikalstamumo internete grėsmių vertinimo ataskaita (angl. *Internet Organised Crime Threat Assessment (IOCTA) 2025*).

- **Iššūkiu yra tapęs didžiųjų kalbos modelių (angl. *Large Language Models*, (LLM) ir kitų DI generavimo programų pasitelkimas socialinės inžinerijos technikoms tobulinti, siekiant automatizuoti komunikaciją su aukomis ir kriminalinius procesus. Pasitelkiant DI, taip pat siekiama apeiti informacinių sistemų saugumo priemones, taip didinant atakų mastą ir sudėtingumą. DI technologijomis naudojamasi tiek siekiant nutekinti duomenis, tiek nutekintus duomenis naudoti DI būdais įgalintose atakose, įskaitant išmanųjį vaizdo klastojimą (angl. *Deepfake*)[08], sintetinių medijų (angl. *Synthetic Media arba AI-generated Media*) ir netikros tapatybės kūrimą.**
- **Nutekintų duomenų prekybos augimą, be kitų veiksnių, skatina ir šešėlinė ekonomika. Nusikalstamame pasaulyje vis svarbesnė tapo prekyba prieigomis patekti į jau įsilaužtas ar pažeistas informacines sistemas ir perimtomis vartotojų paskyromis, taip pat paslauginis nusikaltimas (angl. *Crime-as-a-Service*). Vadinamieji pirminės prieigos tarpininkai (angl. *Initial Access Brokers*) aktyviai siūlo ir reklamuoja pavogtus duomenis bei prieigas specializuotose kibernetinių nusikaltėlių platformose.**
- **Nutekintų duomenų pardavėjai (duomenų tarpininkai) naudojasi platformomis, pritaikytomis nusikalstamoms veikloms apsaugoti ir nuo teisėsaugos slapstytis. Pardavimo sandoriuose, nutekintų duomenų transakcijoms, taip pat keistis informacija apie taikiniais tapusias aukas, įskaitant vaikus, plačiai naudojamos ištisinio šifravimo (angl. *End-to-End Encrypted*) programėlės.**

Tarptautinių grėsmių aktualumas Lietuvai

Policijos stebimos kitose šalyse vyraujančios nusikalstamų veikų elektroninėje erdvėje grėsmės, ypač susijusios su sukčiavimu elektroninėje erdvėje, yra aktualios ir Lietuvai: anksčiau minėtų Europolo ataskaitų išvados visiškai atitinka Lietuvos situaciją dėl **augančios sunkaus ir organizuoto nusikalstamumo įtakos sukčiavimui elektroninėje erdvėje**, todėl šio nusikalstamo reiškinio kontrolė Lietuvos policijai išlieka veiklos prioritetu.

Panašumai:

- Apgaulingų skambučių ir SMS žinučių, taip pat interneto svetainių klastojimo schemose, siekiant tiek išvilioti duomenims, tiek užvaldyti pinigines lėšas, taikoma **įvairiapusė socialinė inžinerija**, kurią Europolas vertina kaip **vieną iš pagrindinių grėsmių**. Lietuvoje sukčiavimo organizatorių naudojama socialinė inžinerija sudaro nusikalstamumo elektroninėje erdvėje pagrindą ir savo masiškumu kelia didžiausią riziką visuomenės saugumui elektroninėje erdvėje. Sukčiavimo organizatoriai savo tapatybei paslėpti naudoja Europolo IOCTA ataskaitoje minimas priemones, tokias kaip nusikalstamos **SIM spiečių įrangos** paslaugos, dėl kurių Lietuvoje 2025 m. jau buvo pradėti pirmieji ikiteisminiai tyrimai.

08
Išmanioji vaizdo klastotė – DI technologija sukurti arba pakeisti vaizdo, garso ar nuotraukų įrašai, kurie atrodo labai tikroviškai, tačiau iš tikrųjų yra suklastoti.

- Lietuvoje kasmet nustatomi **prekybos nutekintais duomenimis** ir **jų neteisėtai apyvartai skirtos paslaugų infrastruktūros naudojimo atvejai** – tai pripažinta **tarptautinė grėsmė**. Taip pat Lietuvoje nuo 2025 m. tapo žinomi nutekintų mobiliųjų programėlių vartotojų paskyrų naudojimo šešėlinėje ekonomikoje atvejai. Dar anksčiau tarp mūsų šalies nepilnamečių, kurie dėl amžiaus cenzo neturi teisės vairuoti, sistemingu reiškiniu tapo nutekintų paskyrų paklausa ir jų naudojimas dalijimosi automobiliais paslaugoms.
- Lietuvoje per pastaruosius keletą metų susiformavo **prekybos narkotinėmis ir psichotropinėmis medžiagomis elektroninėje erdvėje tradicija ir infrastruktūra**, todėl mūsų šaliai yra svarbi Europolo įžvalga SOCTA ataskaitoje dėl DI pasitelkimo organizuojant tokią ir panašią nusikalstamą veiklą.

Tačiau policija įžvelgia ir nemažai reikšmingų skirtumų, analizuodama grėsmių, išskirtų Europolo SOCTA ir IOCTA ataskaitose, pasireiškimą Lietuvoje.

Skirtumai:

- Lietuvoje, priešingai nei nurodoma Europolo SOCTA ataskaitoje, per pastaruosius keletą metų ypatingai **sumažėjo** kibernetinių atakų, susijusių su **elektroninius duomenis užšifruojančiais išpirkos reikalavimo programinės įrangos kodo virusais** (angl. *Ransomware*) ir **DDoS**.
- Lietuvoje taip pat nematomi augančios **rizikos valstybės institucijų ir kritinės infrastruktūros subjektų informacinėms sistemoms** ir **hibridinio karo** veiksmų jose požymiai.
- Lietuvoje dar nėra akivaizdūs nusikalstamo naudojimosi **DI technologijomis** požymiai.

Rezonansiniai 2025 m. įvykiai

Iš tarptautinės bendrovės „Amazon“ išviliota daugiau nei 2,5 mln. eurų.

2025 m. Lietuvos kriminalinės policijos biuro pareigūnai kartu su Lietuvos Respublikos generalinės prokuratūros prokurorais atskleidė beprecedentį sukčiavimo atvejį elektroninėje erdvėje ir sulaikė Lietuvos Respublikos pilietį, kuris galimai pasinaudodamas neteisėtomis pinigų grąžinimo schemomis iš tarptautinės bendrovės „Amazon“ išviliojo virš 2,5 mln. eurų. Bendradarbiaujant su viena didžiausių internetinės prekybos bendrovių „Amazon“ ir tarptautine virtualiųjų valiutų bendrove „Binance“ buvo nustatyta, kad Lietuvos Respublikos pilietis žinučių susirašinėjimo platformoje „Telegram“ sukūrė grupę, kurioje kartu su bendrininkais susitardavo atlikti prekių pirkimus iš „Amazon“. Kuomet užsakytos prekės pasiekdavo „klientus“, jie, piktnaudžiaudami įsigytų prekių grąžinimo politikos taisyklėmis, pareikšdavo, kad jos neatkeliavo arba atkeliavo tik tuščia dėžė, tad pinigai būdavo grąžinami pirkėjui. Atliktų kratų ir poėmių metu pas įtariamąjį ir jo galimus bendrininkus paimta beveik 5 mln. eurų vertės virtualios valiutos ir virš 700 tūkst. eurų grynųjų pinigų. Ši išskirtinė sukčiavimo schema yra beprecedentė ir pirmoji Lietuvoje, kai iš tarptautinės skaitmeninės prekybos bendrovės išviliota itin didelė pinigų suma. Tačiau atskleistas atvejis parodė, kad Lietuvos policija deda visas pastangas išsiaiškinti naujas sukčiavimo schemas ir sulaikyti jų organizatorius bei vykdytojus.

Tarptautinė operacija „Eastwood“ – kirtis programišių grupuotei „NoName057(16)“

2025 m. liepos 14–17 d. tarptautinė teisėsaugos bendruomenė vykdė operaciją „Eastwood“, kuria nusitaikyta į prorusišką programišių grupuotę „NoName057(16)“, vykdžiusią kibernetines DDoS tipo atakas. Teisėsaugos institucijos iš Vokietijos, Čekijos, Prancūzijos, Suomijos, Italijos, Lietuvos, Lenkijos, Ispanijos, Švedijos, Šveicarijos, Nyderlandų ir Jungtinių Amerikos Valstijų vienu metu ėmėsi koordinuotų veiksmų prieš grupuotės narius ir jų naudojamą infrastruktūrą. Operaciją koordinavo Europolas, ją rėmė Europos Sąjungos bendradarbiavimo baudžiamosios teisenos srityje agentūra (angl. *European Union Agency for Criminal Justice Cooperation* (Eurojust), ENISA, taip pat Belgija, Kanada, Estija, Danija, Latvija, Rumunija ir Ukraina. Prie operacijos prisijungė ir partneriai iš privataus sektoriaus – „ShadowServer“ bei „abuse.ch“. Operacijos metu sutrikdyta grupuotės naudotos infrastruktūros veikla, kurią sudarė daugiau nei šimtas kompiuterinių sistemų visame pasaulyje, o didžioji dalis grupuotės centrinių serverių buvo atjungta nuo tinklo. „NoName057(16)“ – tai ideologinė programišių grupuotė, atvirai reiškianti paramą Rusijai bei Rusijos ir Ukrainos karo kontekste vykdanti DDoS tipo kibernetines atakas. Tokios

atakos metu interneto svetainė ar paslauga tyčia užtvindoma didžiuliu duomenų srautu, kad taptų nepasiekiama vartotojams. Su „NoName057(16)“ grupuote siejami asmenys iš pradžių taikėsi į Ukrainą, tačiau vėliau dėmesį nukreipė į šalis, remiančias Ukrainą kare su Rusija, – dauguma jų yra NATO narės. 2025 m. viena iš atakų buvo surengta per NATO viršūnių susitikimą Nyderlanduose. Operacija „Eastwood“ parodė aukšto lygio tarptautinės teisėsaugos koordinacijos gebėjimą realiuoju laiku reaguoti į ideologiškai motyvuotas, su geopolitiniu kontekstu susijusias kibernetines grėsmes. Kibernetinės grėsmės nepaiso sienų, todėl atsakas į jas turi būti globalus ir darniai koordinuotas.

Policijos žvilgsnis į 2026 m.

Policijos vertinimu, tikėtina, kad artimiausiu laiku išliks aktualios **sukčiavimų elektroninėje erdvėje, socialinės inžinerijos** ir **ideologiškai motyvuotų kibernetinių atakų** tendencijos, ypač susijusios su geopolitine situacija regione ir hibridinėmis grėsmėmis. **DI panaudojimas** nusikalstamose veikose gali padidinti nusikalstamų veikų mastą ir įtaigumą.

Šiame kontekste reikalingi papildomi sisteminiai sprendimai, susiję su **teisės aktų pritaikymu** sparčiai kintančiai technologinei aplinkai, ypač DI, duomenų prieinamumo ir tarptautinio informacijos apsikeitimo srityse. Policijos veiklos srityje išlieka poreikis nuosekliai stiprinti nusikalstamų veikų elektroninėje erdvėje tyrimo pajėgumus, tobulinti pareigūnų kompetencijas bei investuoti į skaitmenines kriminalistikos, duomenų analizės ir technologines priemones, reikalingas nusikalstamų veikų atskleidimui.

Policijos veiklos efektyvumui didelę įtaką turės ir tolesnis **tarpinstitucinio bendradarbiavimo stiprinimas**, įtraukiant finansų, ryšių, technologijų sektorius ir tarptautinius partnerius. Tarpinstitucinio bendradarbiavimo stiprinimas tampa vienu esminių veiksnių užtikrinant veiksmingą atsaką į kibernetines grėsmes.

VDAI veiklos apžvalga ir asmens duomenų apsaugos tendencijos

Dijana Šinkūnienė,
VDAI direktorė

Vadovo žodis

Asmens duomenų apsauga ir kibernetinis saugumas yra neatsiejami, todėl 2025 metai išsiskyrė poreikiu prisitaikyti prie besikeičiančių kibernetinių grėsmių. Kibernetinio saugumo incidentai, 2025 m. įvykę tiek duomenų valdytojų infrastruktūroje, tiek tiekimo grandinėse, atskleidė žmogiškojo faktoriaus svarbą, prieigos kontrolės ir vidaus procedūrų spragas, dėl kurių net pažangiausių saugumo priemonių gali nepakakti.

VDAI 2025 m. veikla buvo orientuota į prevenciją ir rizikų mažinimą: didinta duomenų valdytojų, duomenų tvarkytojų, duomenų apsaugos pareigūnų kompetencija, stiprintas tarpinstitucinis bendradarbiavimas, taikytos stebėsenos ir kontrolės priemonės. Veiksminga asmens duomenų apsauga reikalauja sisteminio požiūrio, kuris apima tiek organizacijų vidaus procesus, tiek tiekėjų priežiūros užtikrinimą, tiek visuomenės informuotumo didinimą. Tik sisteminis požiūris į duomenų apsaugą užtikrina, kad asmens duomenų naudojimas bus ne tik teisėtas ir saugus, bet ir patikimas, skaidrus bei etiškas.

223

gauti pranešimai apie ADSP. Iš jų 69 įvyko dėl kibernetinių incidentų.

713 644

Dėl kibernetinių incidentų paveiktų duomenų subjektų skaičius.

22 | 9 | 5

Duomenų valdytojams ir tvarkytojams dėl įvykusio ADSP: paskirtos 5 administracinės baudos (bendra suma 27 029 Eur), pateikti 9 nurodymai ir 22 rekomendacijos, kaip išvengti ar geriau valdyti ADSP.

49

skaityti pranešimai nacionaliniuose ir tarptautiniuose renginiuose.

17

parengtų metodinių dokumentų, siekiant skleisti informaciją apie asmens duomenų apsaugą ir skatinti atsakingą elgesį su asmens duomenimis.

VDAI vaidmuo nacionalinėje kibernetinio saugumo ekosistemoje

VDAI, būdama atsakinga už asmens duomenų apsaugą Lietuvoje, nagrinėja pranešimus apie ADSP, vykdo ADSP prevenciją, t. y. užtikrina, kad duomenų valdytojai[01] ir duomenų tvarkytojai[02] taikytų tinkamas technines ir organizacines saugumo priemones, laikytųsi teisės aktų reikalavimų bei nuolat stiprintų atsparumą kibernetinėms grėsmėms.

Šia veikla siekiama, kad organizacijos užtikrintų tinkamą asmens duomenų apsaugos lygį ir Lietuvoje mažėtų kibernetinių incidentų, kurių metu paveikiami asmens duomenys.

2025 m. išmoktos pamokos, aplinkos pokyčiai, darę įtaką VDAI veiklai

2025 m. VDAI nustatė, kad kibernetiniai incidentai paveikia didelį skaičių asmenų ir didelius asmens duomenų kiekius, įskaitant specialiųjų kategorijų asmens duomenis. Todėl būtina nuolat didinti viešojo ir privataus sektorių kibernetinį atsparumą ir stiprinti asmens duomenų apsaugą. 2025 m. pastebėta, kad tokios greitai besikeičiančios rizikos, kaip DI taikymas įvairiuose sektoriuose (viešajame, finansų, medicinos ir kt.) ir netgi intensyvus DI naudojimas, piktavaliams kuriant įsilaužimų strategijas, tampa vis įtikinamesnės ir lengviau įgyvendinamos. Taip pat 2025 m. dažnai pasitaikydavo kibernetinių incidentų, susijusių su debesijos paslaugomis ir tiekimo grandinės partneriais, kai dėl netinkamos prieigos kontrolės, saugumo konfigūracijų spragų ar trečiųjų šalių pažeidžiamumų buvo neteisėtai atskleisti ar prarasti asmens duomenys.

01

Duomenų valdytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones.

02

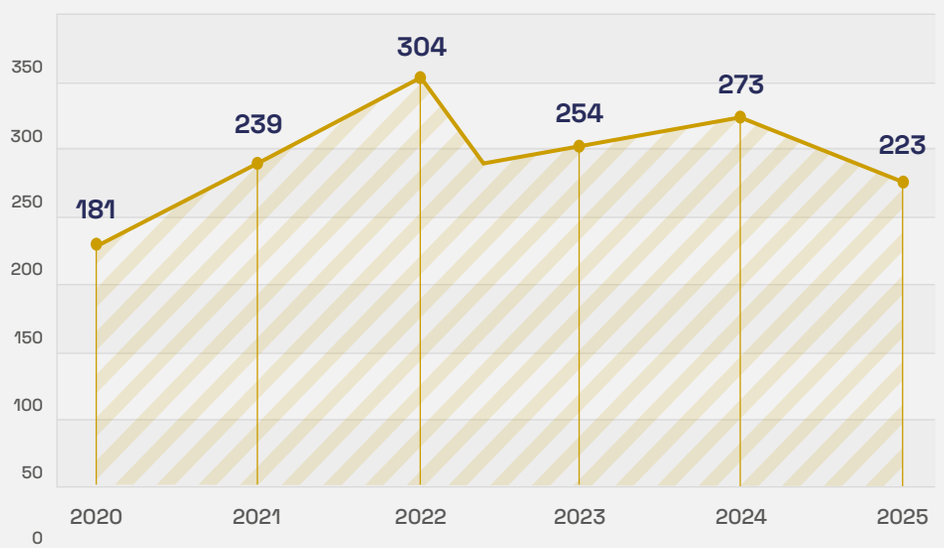
Duomenų tvarkytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis.

Pranešimų apie asmens duomenų saugumo pažeidimus gauta mažiau, tačiau pažeidimų poveikis duomenų subjektams išlieka didelis

VDAI gautų pranešimų apie ADSP dinamika

2025 m. VDAI gavo 223 pranešimus apie ADSP. Palyginti su ankstesnių metų duomenimis, 2025 m. VDAI gavo mažiau pranešimų apie ADSP negu 2024 m. (2024 m. gauti 273 pranešimai). Įvertinus turimus duomenis, daroma išvada, kad viešasis ir privatusis sektoriai tampa sąmoningesni, skiria daugiau dėmesio, kad žmogiškosios klaidos nepasikartotų ir būtų nuolat stiprinamas kibernetinis atsparumas. Svarbu pabrėžti, kad VDAI nuolat teikia konsultacijas, organizuoja konferencijas ir mokymus, rengia metodinę dokumentaciją, siekdama, kad duomenų valdytojai ir duomenų tvarkytojai galėtų lengviau pritaikyti rekomendacijas savo veikloje ir užtikrintų atitinkamų duomenų apsaugos lygį (**1 pav.**).

2020–2025 m. pranešimų apie ADSP dinamika



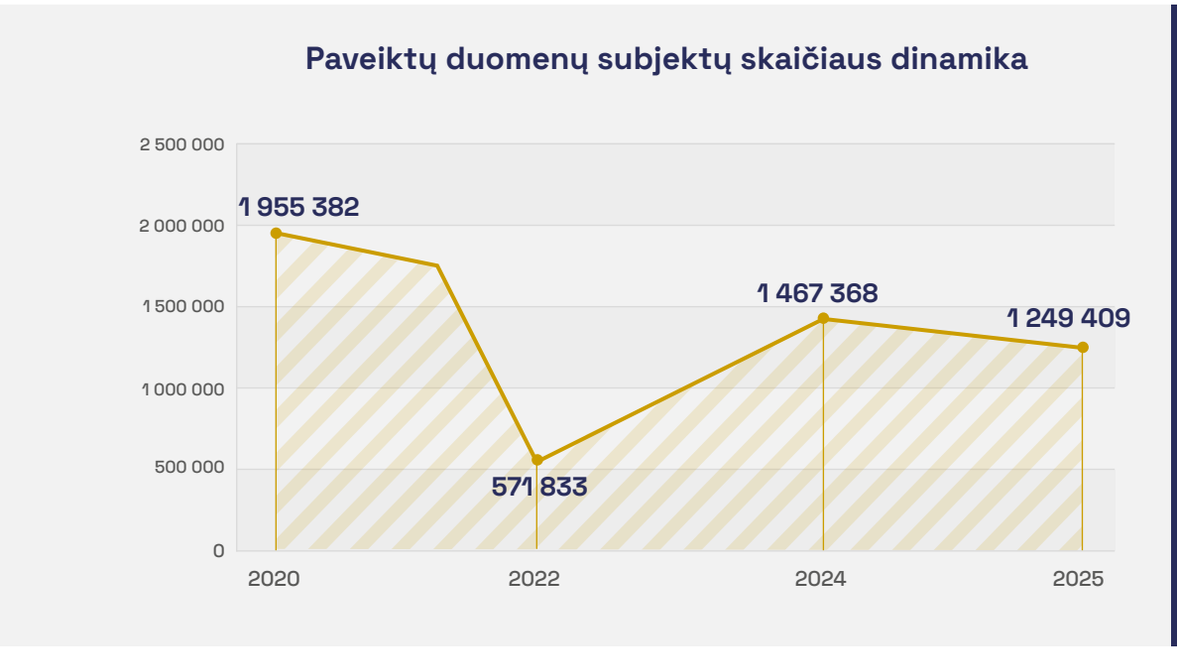
< 1 pav.

2020–2025 m. pranešimų apie ADSP dinamika
(šaltinis – VDAI)

Lietuvoje paveiktų duomenų subjektų skaičius – 1 249 409. Lyginant su praėjusių metų duomenimis, paveiktų duomenų subjektų[03] skaičius sumažėjo beveik 200 tūkst. (2024 m. paveiktų duomenų subjektų skaičius – 1 467 368 (**2 pav.**).

03

Duomenų subjektas – fizinis asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma, pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

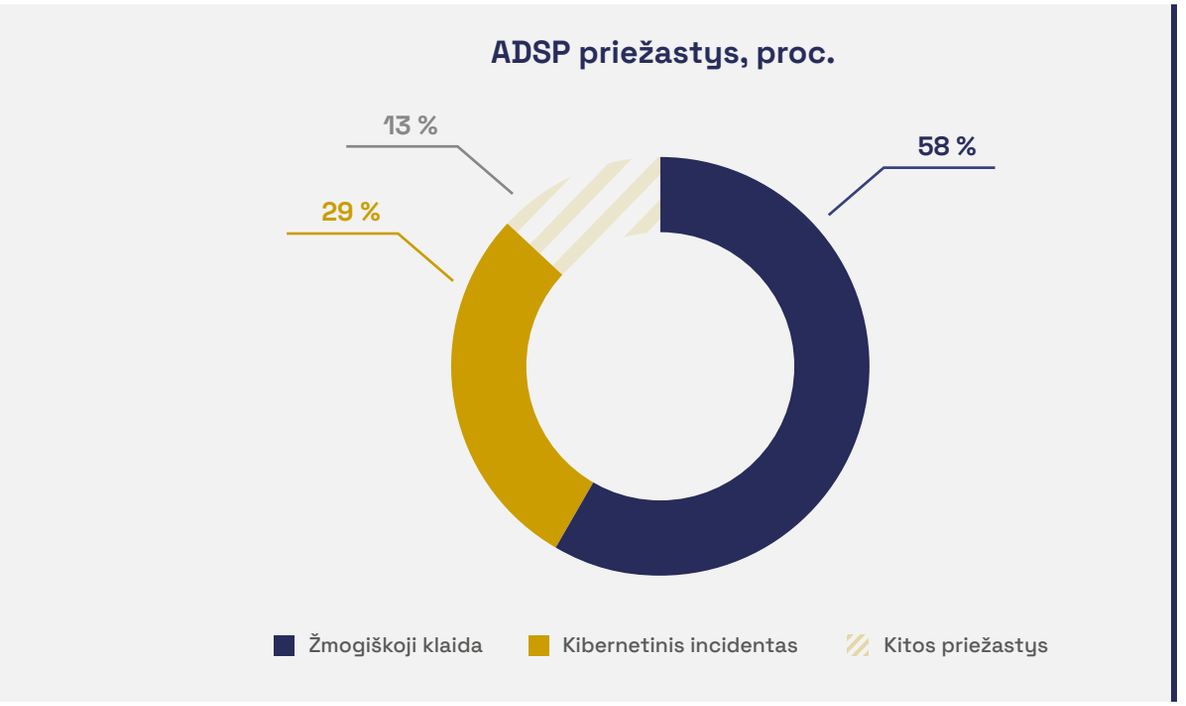


< 2 pav.

Paveiktų duomenų subjektų skaičiaus dinamika
(šaltinis – VDAI)

ADSP, įvykusių dėl kibernetinių incidentų, skaičius sumažėjo

Išanalizavusi 2025 m. gautus pranešimus apie ADSP, VDAI nustatė, kad 29 proc. ADSP įvyko dėl kibernetinių incidentų (2024 m. – 33 proc.). 58 proc. ADSP įvyko dėl žmogiškosios klaidos[04]. Dėl kitų priežasčių[05] 2025 m. įvykę ADSP sudaro 13 proc. (**3 pav.**).



< 3 pav.

ADSP priežastys
(šaltinis – VDAI)

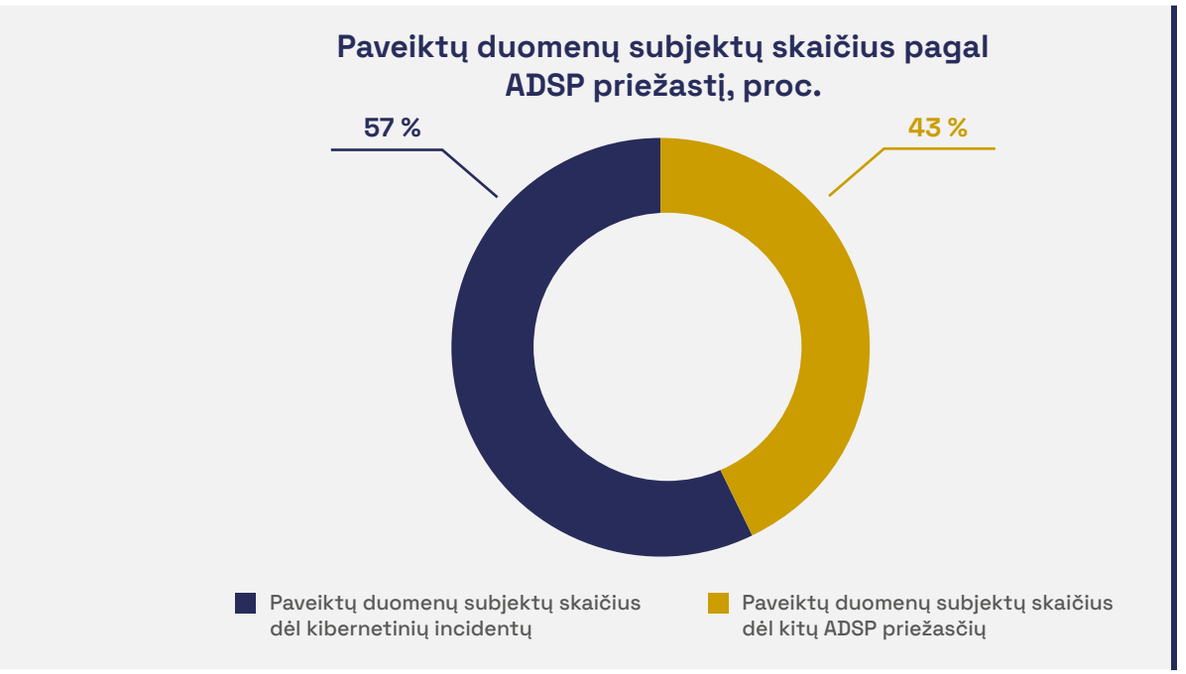
04

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

05

ADSP dėl kitų priežasčių įvyksta dėl įvairių IT sistemų trikdžių, kilusių dėl IT sistemų klaidų, dėl kurių atnaujinti duomenys nebuvo laiku perduoti, todėl duomenų valdytojai negalėjo laiku suteikti paslaugų, taip pat nustatyta, kad buvo netinkamai atlikti programavimo darbai arba neatliktas sistemų testavimas prieš paleidimą sudarė sąlygas situacijoms, kai asmens duomenys buvo prieinami asmenims, neturintiems teisės su jais susipažinti.

VDAI teigimu, 2025 m. **ADSP, įvykusių dėl kibernetinių incidentų**, skaičius galėjo sumažėti dėl naujos redakcijos KSĮ nuostatų taikymo, taip pat praplėsto KSS skaičiaus, aiškiai reglamentuotų techninių ir organizacinių priemonių, taip pat reguliariai vykdomos VDAI švietimo veiklos, t. y. renginių organizavimo ir metodinių dokumentų rengimo. Tačiau, nors dėl kibernetinių incidentų įvyko tik 29 proc. ADSP iš visų 2025 m. gautų pranešimų apie ADSP, tačiau jų metu buvo **paveikti net 57 proc. duomenų subjektų** (iš viso 713 644), t. y. daugiau nei pusė iš visų 2025 m. paveiktų asmenų, duomenys. Dėl kitų priežasčių buvo paveikti 43 proc. duomenų subjektų duomenys (iš viso 535 765, **4 pav.**).



< 4 pav.

Paveiktų duomenų subjektų skaičius pagal ADSP priežastį *(šaltinis – VDAI)*

Neteisėtai gauta prieiga prie IS, socialinė inžinerija ir duomenų viliojimo (angl. *Phishing*) atakos, duomenų užšifravimo ir išpirkos reikalavimo atakos (angl. *Ransomware*) yra vieni dažniausių kibernetinių incidentų, dėl kurių įvyksta ADSP

Vertinant 2025 m. gautus ADSP pranešimus, kurie įvyko **dėl kibernetinio incidento**, nustatyta, kad:

- 45 proc. incidentų įvyko piktavaliams neteisėtai gavus prieigą prie informacinių sistemų;
- 26 proc. – dėl socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) atakų; jų dalis, palyginti su 2024 m. (18 proc.), reikšmingai išaugo;
- 16 proc. – dėl duomenų užšifravimo ir išpirkos reikalavimo (angl. *Ransomware*) atakų, kai prieš užšifravimą duomenys buvo nukopijuojami ir naudojami papildomam spaudimui (grasinant juos paviešinti) tamsiojo interneto forumuose (angl. *Dark Web Forums*);

- 7 proc. – dėl kredencialų brukimo (angl. *Credential Stuffing*) ir brutaliųjų (angl. *Brute Force*) atakų, kai naudojant nutekėjusius ar spėjant slaptažodžius buvo gaunama prieiga prie informacinių sistemų;
- 3 proc. – dėl SQL įterpimo[06] (angl. *SQL Injection*) atakų;
- 3 proc. – dėl sistemų veiklos sutrikdymo atakų.

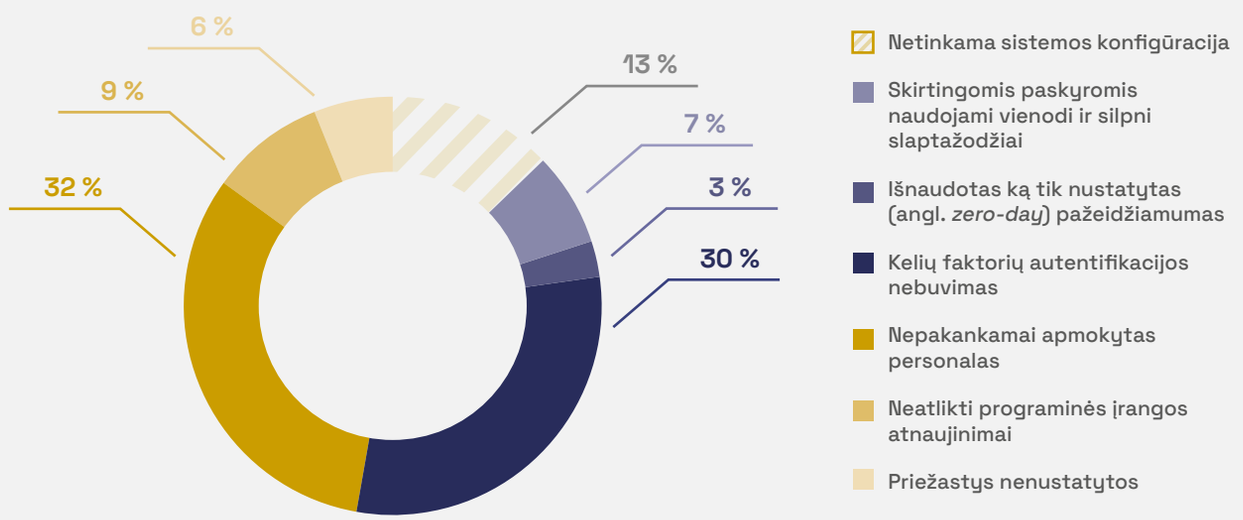
Atkreiptinas dėmesys, kad 2024 m. SQL įterpimo ir sistemų veiklos sutrikdymo incidentų nepasitaikė. 2025 m. piktavaliai pradėjo vis aktyviau užvaldinėti tinklapius ar duomenų bazes, taip pat trikdyti sistemų veiklą – sistemos tapdavo nepasiekiamos ir laikinai nutrūkdavo paslaugų teikimas.

Įvertinusi gautus pranešimus apie ADSP dėl kibernetinių incidentų, VDAI nustatė, kad 2025 m. **pagrindinės kibernetinių incidentų priežastys** panašios į 2024 m. (**5 pav.**).

v 5 pav.

Kibernetinių incidentų priežastys
(šaltinis – VDAI)

Kibernetinių incidentų priežastys, proc.



Papildomai atkreiptinas dėmesys, kad 6 proc. iš visų 2025 m. gautų pranešimų apie ADSP (įvykusių dėl kibernetinių incidentų) nebuvo nustatytos incidento priežastys. Taip atsitinka dėl to, kad žurnaliniai įrašai yra saugomi trumpą laiką, taip pat saugomi tame pačiame serveryje arba nėra taikomos priemonės, apribojančios galimybę žurnalinius įrašus ištrinti, sugadinti ar pakeisti.

06 Užvaldymas, pagrįstas specialaus SQL kodo įterpimu į užklausą

Saugumo aplinkos pokyčiai ir tendencijos

2025 m. patvirtino, kad kibernetinis saugumas ir asmens duomenų apsauga yra tarpusavyje glaudžiai susijusios sritys, kurioms būtinas koordinuotas ir kolektyvinis atsakas. Įsigaliojus naujos redakcijos KSĮ ir jo poįstatyminių teisės aktų nuostatoms, VDAI teigimu, gerėja kibernetinio saugumo rizikos valdymas, taikant technines ir organizacines priemones, užtikrinančias kibernetinį atsparumą ir asmens duomenų apsaugą.

VDAI praktika 2025 m. parodė, kad Lietuvoje ir Europoje įvykę ADSP, dėl kurių nukentėjo Lietuvos gyventojai, atskleidė sistemines silpnąsias vietas: žmogiškąjį faktorių, tiekimo grandinių pažeidžiamumą ir nepakankamą trečiųjų šalių kontrolę. Tai patvirtino poreikį stiprinti darbuotojų kompetencijas, vidaus kontrolę, rizikos ir incidentų valdymo brandą bei poreikį griežčiau vertinti naudojamus DI įrankius. Kadangi ne visiems DI kūrėjams yra taikomi griežti asmens duomenų apsaugos ar kibernetinio saugumo reikalavimai, nustatyti **Bendrajame duomenų apsaugos reglamente**[07] (toliau – BDAR) ar KSĮ ir kituose teisės aktuose, tokių įrankių naudojimas gali pažeisti pateiktų asmens duomenų konfidencialumą.

Atsižvelgdama į tai, kad vis dažniau atsiranda įrankių ar technologijų, keliančių grėsmę asmens duomenų saugumui, VDAI nedelsdama apie tai informuoja visuomenę savo **svetainėje**, taip pat bendradarbiauja su kitomis Lietuvos institucijomis, užtikrinančiomis asmens duomenų apsaugą ir kibernetinį saugumą, ir kitomis Europos duomenų apsaugos institucijomis, įskaitant **Europos duomenų apsaugos valdybą** (angl. *European Data Protection Board*, EDAV), ir užtikrina bendrą Europos pozicijos formavimą ir nuoseklų jos taikymą Lietuvos asmens duomenų apsaugos sistemoje.

Dažniausios ADSP priežastys ir praktikoje nustatomi trūkumai rodo, kad šiuos pažeidimus dažniausiai lemia pasikartojantys organizaciniai ir techniniai asmens duomenų saugumo valdymo trūkumai:

- 2025 m. ADSP ir toliau dažnai įvyksta dėl prieigos kontrolės valdymo organizacijų kompiuterių tinkluose spragų, kai suteikiant prieigą nėra taikomi apribojimai, nesilaikoma „mažiausių teisių privilegijos“ ir „būtina žinoti“ principų, netaikomas dviejų ir daugiau veiksnių autentifikavimas privilegijuotas teises turintiems, nuotoliniu būdu besijungiantiems ar virtualų privatų tinklą naudojantiems vartotojams;
- duomenų valdytojai ir duomenų tvarkytojai neužtikrina reguliaraus informacinių sistemų, tinklų ir programinės įrangos spragų vertinimo, todėl laiku neidentifikuojamos saugumo spragos, ir jomis gali būti pasinaudota kibernetinių atakų metu;

07
2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir str. dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).

- 2025 m. dažna problema išlieka, kai piktavaliai pašalina duomenų atsargines kopijas ir įvykių žurnalinius įrašus, saugomus toje pačioje vietoje. Tada duomenų valdytojai ar duomenų tvarkytojai nebegali lengvai atkurti duomenų prieinamumo bei tinkamai atlikti kibernetinio incidento ir ADSP tyrimo;
- socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) atakos sėkmingos dėl vis dar aktualios problemos – nepakankamo darbuotojų gebėjimo atpažinti kenkėjiškus laiškus ar kitus pranešimus ir papildomų tapatybės autentifikavimo priemonių netaikymo, įgalinančio pasinaudoti išviliotais prisijungimo duomenimis. Atpažinti kenkėjiškus pranešimus vis sunkiau, nes vis dažniau naudojamos DI priemonės, kurios sukuria realistiškus, kalbiškai taisyklingus ir individualizuotus laiškus ar kitus pranešimus;
- vis dar pasitaiko atvejų, kai įvykus kibernetiniam incidentui duomenų valdytojai neįstengia tinkamai atlikti kibernetinio incidento tyrimo ir nustatyti priežasčių, kurių išaiškinimas galėtų ateityje padėti išvengti tokio pobūdžio atakų.

Atsižvelgdama į minėtas ADSP priežastis, VDAI siūlo vadovautis **KSĮ** ir **Kibernetinio saugumo reikalavimų apraše**[08], **ISO standarte 27002:2022**[09] ir VDAI **gairėse**[10] nustatytais reikalavimais ir rekomendacijomis, kad duomenų valdytojai ir duomenų tvarkytojai, siekdami užtikrinti pavojų atitinkantį saugumo lygį, taikytų tinkamas organizacines ir technines priemones.

DI ir automatizacijos poveikis saugumo aplinkai

2024 m. birželio mėn. priimtu **DI aktu**[11] visoje ES sukurta patikimo ir į žmogų orientuoto DI bendroji rinka. Jo tikslas – skatinti inovacijas ir DI diegimą, kartu užtikrinant aukšto lygio sveikatos, saugos ir pagrindinių teisių, įskaitant demokratiją ir teisinę valstybę, apsaugą. DI aktas pradėtas taikyti etapais, visa apimtimi jis bus pradėtas taikyti nuo 2027 m. rugpjūčio 2 d. Šiuo metu jau taikomi draudimai taikyti nepriimtiną riziką keliančią praktiką ir įpareigojimai bendrosios paskirties DI modeliams. Tačiau dauguma nuostatų, visų pirma, reglamentuojančių didelės rizikos DI sistemas, bus pradėtos taikyti nuo 2026 m. rugpjūčio 2 d. arba 2027 m. rugpjūčio 2 d. Šios nuostatos apima išsamius duomenų valdymo, skaidrumo, dokumentavimo, žmogaus vykdomos priežiūros ir patikimumo reikalavimus, siekiant užtikrinti, kad ES rinkai teikiamos DI sistemos būtų saugios, skaidrios ir patikimos. Atkreiptinas dėmesys, kad 2025 m. EK pateikė pasiūlymus dėl **Skaitmeninio sektoriaus bendrojo rinkinio**[12] keitimo ir **Bendrojo skaitmeninės srities dokumentų rinkinio dėl dirbtinio intelekto** (angl. *Digital Omnibus on AI*)[13].

08
2018 m. rugpjūčio 13 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

09
ISO/IEC 27002:2022 standartas „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“.

10
VDAI 2024 m. rugpjūčio 13 d. gairės „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“.

11
2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1689, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas).

12
2025 m. lapkričio 19 m. Europos Komisijos pasiūlymas dėl Europos Parlamento ir Tarybos Reglamento, kuriuo siekiant supaprastinti skaitmeninio sektoriaus teisės aktų sistemą iš dalies keičiami reglamentai (ES) 2016/679, (ES) 2018/1724, (ES) 2018/1725, (ES) 2023/2854 ir direktyvos 2002/58/EB, (ES) 2022/2555 ir (ES) 2022/2557 ir panaikinami reglamentai (ES) 2018/1807, (ES) 2019/1150, (ES) 2022/868 ir Direktyva (ES) 2019/1024, (Skaitmeninio sektoriaus bendrasis rinkinys).

13
2025 m. lapkričio 19 d. Europos Komisijos pasiūlymas dėl Europos Parlamento ir Tarybos Reglamento, kuriuo dėl suderintų dirbtinio intelekto taisyklių įgyvendinimo supaprastinimo iš dalies keičiami Reglamentai (ES) 2024/1689 ir (ES) 2018/1139, (Bendrasis skaitmeninės srities dokumentų rinkinys dėl dirbtinio intelekto).

2025 m. DI sistemos tapo esminėmis, pakeitusiomis kibernetinių grėsmių pobūdį ir mastą. Remiantis **ENISA** duomenimis[14], 2025 m. ir toliau buvo stebimas DI naudojimas vykdant įvairius įsilaužimus, daugiau nei 80 proc. pasaulyje fiksuotų socialinės inžinerijos atakų jau buvo paremtos DI sugeneruotu turiniu. DI naudojamas kuriant apgaulingus el. laiškus, vykdant internetinį sukčiavimą, taip pat kuriant kenkimo programas.

VDAI 2025 m. savo veikloje atkreipė dėmesį į dedamas dideles pastangas, kad žmonės taptų sąmoningesni – organizuojant renginius, rengiant metodinę dokumentaciją, vykdant socialinės inžinerijos simuliacijas didelis dėmesys skiriamas priemonėms, kaip apsisaugoti pačiam ar apsaugoti organizacijos darbuotojus bei visuomenę. **BDAR** ir **Kibernetinio saugumo reikalavimų apraše** yra nustatyti reikalavimai, kuriuos taikant būtų užtikrinamas kibernetinis atsparumas. Tačiau 2025 m. iš visų VDAI gautų pranešimų apie ADSP, kurie įvyko dėl kibernetinio incidento, net 26 proc. įvykdyti panaudojus socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) metodus. Pastebima, kad tokių atakų mastui ir veiksmingumui galėjo turėti įtakos būtent DI, leidžiantis kurti realistišką, personalizuotą ir sunkiau atpažįstamą apgaulingą turinį.

Apibendrinant reikia pabrėžti, kad 2025 m. žymi esminį lūžį, kai DI ir automatizacija tapo neatsiejama tiek kibernetinių grėsmių, tiek duomenų apsaugos dalimi. DI ne tik padidino atakų mastą ir sudėtingumą, bet ir privertė institucijas persvarstyti savo požiūrį į saugumą. Reikia turėti omenyje, kad DI įtaka tik stiprės, ir organizacijos turės nuolat tobulinti savo gynybos priemones, vertinti DI keliamas rizikas ir bendradarbiauti keisdamosi informacija apie naujausias grėsmes. Todėl VDAI ir toliau stiprins priežiūros bei konsultavimo veiklą, teiks metodines rekomendacijas dėl saugaus DI sprendimų taikymo, aktyviau vykdys rizika grįstus patikrinimus bei skatins organizacijas atlikti **poveikio duomenų apsaugai vertinimus** (PDAV), kad užtikrintų, jog inovacijos būtų diegiamos atsakingai ir laikantis asmens duomenų apsaugos reikalavimų.

Rizikos, susijusios su priklausomybe nuo išorinių paslaugų teikėjų ir tiekimo grandinių

Vertindama 2025 m. gautus ADSP pranešimus, VDAI pastebi, kad duomenų valdytojai skiria nepakankamą dėmesį tikrindami, ar jų pasitelkti duomenų tvarkytojai, tvarkydami asmens duomenis, įgyvendina tinkamas technines ir organizacines priemones, kaip to reikalauja BDAR, kad užtikrintų tvarkomų asmens duomenų saugumą.

14
ENISA grėsmių kraštovaizdis 2025 m. (angl. *Enisa Threat Landscape 2025*).

VDAI, vertindama gautus pranešimus apie ADSP, susijusius su duomenų tvarkytojais, nustatė, kad:

- duomenų valdytojai būna nepasirašę sutarčių, įskaitant asmens duomenų tvarkymo;
- nėra susitarimų, kuriuose būtų nurodyti reikalavimai duomenų tvarkytojams;
- duomenų valdytojai nevertino, ar duomenų tvarkytojai taiko sutartyse ar kituose dokumentuose nurodytas technines ir organizacines priemones, užtikrinančias tinkamą asmens duomenų saugumo lygį;
- duomenų tvarkytojai nepakankamai rūpinasi duomenų valdytojų asmens duomenimis [15].

Siekdama užtikrinti asmens duomenų apsaugą, kai asmens duomenis tvarko duomenų tvarkytojai, VDAI rekomenduoja:

- užtikrinti, kad su duomenų tvarkytojais būtų pasirašytos paslaugų teikimo sutartys, asmens duomenų tvarkymo susitarimai ar kiti dokumentai, kuriuose būtų nustatyta prievolė užtikrinti, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų BDAR reikalavimus;
- jeigu yra galimybė, užtikrinti, kad būtų reguliariai atliekami duomenų tvarkytojų auditai, kurių metu duomenų valdytojas galėtų įsitikinti, jog duomenų tvarkytojas laikosi sutartyse ar kituose dokumentuose nustatytų reikalavimų.

VDAI nuolat teikia konsultacijas ir rengia metodinius dokumentus, kad organizacijos stiprintų tiekėjų rizikos vertinimo procesus, reguliariai atliktų saugumo auditus ir užtikrintų aiškias atsakomybes bei incidentų valdymo tvarką sutartiniuose santykiuose.

Papildomos įžvalgos iš kitų ataskaitų

Lietuvoje 2025 m. asmens duomenų apsaugos ir kibernetinio saugumo srityse stebimi procesai iš esmės atitinka nacionalinių, ES ir tarptautinių analizių bei ataskaitų išvadas. Remiantis **ENISA ataskaita**[16] didžiausią dalį asmens duomenų saugumo pažeidimų sudaro incidentai, susiję su žmogiškuoju faktoriumi, socialine inžinerija ir neteisėta prieiga prie informacinių sistemų, o didžiausią pavojų duomenų valdytojams kelia kibernetiniai incidentai, įvykę dėl **išpirkos reikalaujančių programų** ir **tiekimo grandinių pažeidžiamumų išnaudojimo**. Šioje ENISA ataskaitoje nurodomos 2025 m. tendencijos sutampa su VDAI veikloje pastebimomis ADSP priežastimis. Todėl papildomai pažymėtina, kad techninės ir organizacinės saugumo priemonės turi būti papildomos nuosekliu darbuotojų kompetencijų stiprinimu, vidaus procedūrų aiškumu ir operatyviu incidentų valdymu, kad asmens duomenų tvarkymas atitiktų BDAR ir kitų teisės aktų reikalavimus.

15

BDAR 32 straipsnio 1 dalyje yra įtvirtintas reikalavimas, kad tiek duomenų valdytojas, tiek duomenų tvarkytojas turi įgyvendinti tinkamas technines ir organizacines duomenų saugumo priemones, kad būtų užtikrintas pavojų atitinkantis saugumo lygis.

16

ENISA grėsmių kraštovaizdis 2025 m. (angl. *Enisa Threat Landscape 2025*).

Rezonansiniai 2025 m. įvykiai

ADSP susijęs su duomenų tvarkytojo aplaidumu.

2025 m. kovą VDAI gavo iš 4 duomenų valdytojų pranešimus apie tą patį ADSP. Pranešimuose nurodyta, kad buvo paveikta viešosios debesijos platforma, t. y. duomenų tvarkytojo infrastruktūroje įvyko kibernetinis incidentas, kurio metu buvo užšifruoti visų duomenų valdytojų viešosios debesijos platformoje laikomi duomenys, taip pat buvo užšifruota ir dalis paveiktoje platformoje saugomų atsarginių kopijų. Kibernetinis incidentas įvyko piktavaliui neteisėtai gavus prieigą prie nuotolinio darbalaukio protokolo (angl. *Remote Desktop Protocol*), kuris buvo pasiekiamas per išorinį tinklą. Prieš įvykstant kibernetiniam incidentui duomenų tvarkytojas nebuvo įgyvendinęs tinklų segmentavimo ir IP adresų filtravimo, o prieiga prie debesijos informacinių sistemų nebuvo apsaugota papildomais tapatybės autentifikavimo mechanizmais, kaip yra numatyta KSĮ, tarptautiniuose standartuose, įskaitant ISO/IEC 27002:2022, VDAI gairėse ir kibernetinio saugumo gerojoje praktikoje. Atsižvelgdama į tai, VDAI nustatė, kad duomenų tvarkytojas (debesijos paslaugų teikėjas) neįgyvendino pakankamų techninių ir organizacinių saugumo priemonių, kurios būtų užtikrinusios, kad neįvyktų ADSP. Atsižvelgiant į tai, darytina išvada, kad ADSP įvyko dėl nepakankamų duomenų tvarkytojo taikytų organizacinių ir techninių priemonių teikiant viešosios debesijos platformos paslaugas. Papildomai pažymėtina, kad duomenų tvarkytojui (debesijos paslaugų teikėjui) kyla pareiga įgyvendinti tinkamas saugumo priemones, o duomenų valdytojui pareiga nuolatos vertinti rizikas, įskaitant susijusias su tiekimo grandine.

VDAI žvilgsnis į 2026 m.

Remiantis 2025 m. VDAI patirtimi, vertinant gautus ADSP pranešimus, galima pagrįstai prognozuoti, kad 2026 m. DI naudojimo iššūkiai, susiję su asmens duomenų apsauga, išliks aktualūs ir pareikalaus nuoseklaus priežiūros institucijų bei organizacijų dėmesio. Socialinė inžinerija išliks dažniausiu atakų inicijavimo būdu, vis dažniau pasitelkiant DI priemones. Atsižvelgiant į tai, duomenų valdytojams ir duomenų tvarkytojams būtina reguliariai peržiūrėti ir įvertinti taikomas technines ir organizacines priemones, kad jos padėtų apsisaugoti nuo kibernetinių atakų ir asmens duomenų saugumo pažeidimų.

Atsižvelgdama į tai, VDAI įsipareigoja ir toliau aktyviai vykdyti visuomenės švietimą bei stiprinti gyventojų informuotumą apie kibernetinio sukčiavimo atvejus, siekdama padėti jiems laiku atpažinti grėsmes ir veiksmingai nuo jų apsisaugoti. VDAI kiekvienais metais daug dėmesio skiria metodinės informacijos rengimui, ji skelbiama VDAI tinklapyje, taip

pat aktuali informacija skelbiama socialiniame tinkle **„LinkedIn“**. 2025–2027 m. VDAI įgyvendina projektą SolPriPa 3: žinok savo teises ir pareigas. SolPriPa (liet. *sprendžiant privatumo paradoksą*, angl. *Solving Privacy Paradox*) – teisės į asmens duomenų apsaugą, kaip vieno iš svarbiausių vartotojų pasitikėjimo skaitmenine ekonomika veiksnių, aukštų standartų skatinimo projektas. Projekto tikslas – kurti tinklalaides, informacinius grafikus, mokomuosius vaizdo įrašus ir organizuoti kitas veiklas, skirtas plačiosios visuomenės ir verslo atstovų žinioms apie duomenų subjektų teises plėsti ir galimoms teisių gynimo priemonėms pagal BDAR taikyti. Visa aktuali informacija bus skelbiama VDAI tinklapyje.

Atsižvelgiant į tai, kad ADSP, įvykę dėl kibernetinių incidentų, kelia didelį pavojų duomenų subjektams (pažeidus asmens duomenų konfidencialumą, prieinamumą ir vientisumą), 2026 m. ypatingas dėmesys bus skiriamas VDAI ir NKSC bendradarbiavimui stiprinti. Ir toliau keisimės informacija apie nagrinėjamus ADSP, vykdysime bendrus tikrinimus, kai įvyks ADSP, ypatingą dėmesį skirsime bendroms pratyboms, nes jos padeda duomenų valdytojams geriau pasiruošti ADSP ir kibernetiniams incidentams, užtikrinant tinkamą jų valdymą ir priežiūros institucijų informavimą. Bus skatinamas aktyvus viešojo ir privataus sektoriaus įsitraukimas į nacionalinio atsparumo kibernetinėms grėsmėms stiprinimą bei aukšto asmens duomenų apsaugos lygio užtikrinimą, plėtojant informacijos apie kylančias rizikas ir gerąją praktiką dalinimąsi.

RRT veiklos apžvalga ir elektroninių ryšių tinklų vientisumo bei vartotojų apsaugos tendencijos

Jūratė Šovienė,
RRT tarybos pirmininkė

Vadovo žodis

2025 m. dar kartą įsitikinome, kad ryšių ekosistemos atsparumas prasideda nuo informuoto vartotojo, nuoseklaus švietimo ir gebėjimo apsaugoti šalies infrastruktūrą nuo kylančių grėsmių. Visuomenės pranešimų apie incidentus skaičius augo, ir RRT edukacinės iniciatyvos padėjo tūkstančiams žmonių skaitmeniniame pasaulyje jaustis saugiau.

Žvelgdami į 2026 m., sieksime toliau stiprinti ryšių tinklų, skaitmeninės erdvės ir skaitmeninių paslaugų saugumą bei patikimumą, ypatingą dėmesį skirdami geopolitinėms rizikoms ir vartotojų įgalinimui.

RRT vaidmuo nacionalinėje kibernetinio saugumo ekosistemoje

RRT nacionalinėje kibernetinio saugumo ekosistemoje užtikrina patikimą elektroninių ryšių infrastruktūrą kaip pagrindą inovatyviems sprendimams, stiprina pasitikėjimą skaitmeninėmis paslaugomis, įgalina ekosistemą saugoti vartotojų – ypač nepilnamečių ir kitų pažeidžiamų asmenų – interesus bei didina visuomenės skaitmeninį raštingumą.

3 518
gautų pranešimų RRT interneto karštąja linija „Švarus internetas“ apie draudžiamą ir neigiamą poveikį nepilnamečiams darančią informaciją (beveik 62 proc. daugiau nei 2024 m.).

2263
pranešimai, dėl kurių buvo imtasi reikiamų veiksmų (2024 m. – dėl 1488 pranešimų).

22 759
vyresnio amžiaus žmonės dalyvavo skaitmeninio raštingumo mokymuose, kuriuos vykdydama projektą „Nė vienas nėra pamirštas“ RRT surengė kartu su partneriais. Iš viso surengta 100 mokymų.

Augant duomenų srautams, nusikalstamoms veikoms persikeliant į elektroninę erdvę ir išliekant žalingiems radijo ryšio trukdžiams, elektroninių ryšių infrastruktūros kokybės ir nepertraukiamumo užtikrinimas tampa strategine valstybės atsparumo sąlyga, todėl RRT veikla apima tiek reguliavimą ir priežiūrą, tiek ilgalaikę prevenciją.

13 298 316

ryšio operatorių blokuotų apgaulingų skambučių (63 proc. daugiau nei 2024 m.).

5 725 890

ryšio operatorių blokuotų apsimestinių SMS žinučių „beveik 80 proc. daugiau nei 2024 m.).

6 mln.

pašalintų reklamų ar neteisėto turinio, atsižvelgus į RRT sertifikuotų patikimų pranešėjų pateiktus 2000 pranešimus.

2025 m. išmoktos pamokos ir aplinkos pokyčiai

2025 m. netrūko iššūkių – nuo tarpvalstybinių žalingų radijo trukdžių iki augančio telefoninio sukčiavimo masto. Dėl nuolat didėjusio išorės grėsmių poveikio elektroninių ryšių infrastruktūrai ir visuomenės aktyvumo pranešinėjant apie neteisėtą ar žalingą turinį internete RRT veikla buvo dinamiška. 2025 m. įvykiai parodė, kad elektroninių ryšių atsparumas ir saugumas vis labiau priklauso nuo tarpinstitucinio, tarptautinio ir ES lygmens koordinavimo, greito keitimosi informacija bei suderintų teisinių ir technologinių priemonių. Net ir stabiliai veikiant elektroninių ryšių infrastruktūrai, būtina nuolat stiprinti prevenciją, stebėseną ir visuomenės skaitmenines kompetencijas, nes grėsmės tampa sisteminės, ilgalaikės ir vis labiau orientuotos į vartotojų elgseną bei galimus pažeidžiamumus.

Stiprinama skaitmeninės erdvės priežiūra ir padidėjęs visuomenės aktyvumas pranešant apie netinkamą turinį internete

Elektroninių ryšių tinklų atsparumas

2025 m. Lietuvos elektroninių ryšių infrastruktūra išlaikė stabilų atsparumo lygį, o didesnio masto viešųjų ryšių tinklų sutrikimų dinamika iš esmės nekito. Paslaugų teikėjai RRT pateikė 18 pranešimų apie viešųjų ryšių tinklų vientisumo pažeidimus, kai paslaugos buvo sutrikusios ilgiau nei vieną valandą ir paveikė reikšmingą naudotojų dalį (2024 m. buvo 6, 2023 m. – 17 pranešimų). Dauguma viešųjų ryšių tinklų vientisumo pažeidimų kilo dėl viešųjų ryšių tinklo įrangos gedimų arba planinių atnaujinimo darbų, o paslaugų teikimas būdavo atkuriamas maždaug per 2 valandas. 2025 m. nefiksuota nei stichinių reiškinių sukeltų, nei didelį rezonansą sukėlusių viešųjų ryšių tinklų sutrikimų. RRT vykdoma elektroninių ryšių paslaugų teikėjų priežiūra leidžia užtikrinti viešųjų elektroninių ryšių paslaugų kokybę ir išvengti arba sumažinti su viešųjų ryšių tinklų vientisumo pažeidimais susijusias rizikas, pvz., ryšio praradimą krizių atvejais.

Radijo ryšio atsparumo stiprinimas – atsakas į radijo trukdžius iš Rusijos

RRT veikla pasaulinės palydovinės navigacijos sistemos (angl. *Global Navigation Satellite System*) (toliau – GNSS) trukdžių stebėsenos ir analizės srityje yra svarbi visuomenės saugumui ir valstybės atsparumui. Ankstyvas GNSS trukdžių identifikavimas, operatyvus informacijos apsikeitimas bei glaudus bendradarbiavimas su viešojo ir privataus sektoriaus subjektais padeda užtikrinti, kad orlaiviai, laivai, specialiosios tarnybos ir kiti naudotojai galėtų patikimai naudotis GNSS. Tai ypač aktualu pasienio regionuose.

2025 m. fiksuoti GNSS trukdžiai iš Kaliningrado teritorijos veikė orlaivių, laivų valdymo sistemas. GNSS trukdžių intensyvumas per 2025 m. kito. Gruodžio pabaigoje pasiekė visą parą veikiančio trikdymo lygį. Klaidinančių signalų šaltinių skaičius Kaliningrade išaugo nuo 3 iki 35, ir signalų poveikis buvo juntamas iki 450 km nuo šaltinio. GNSS trukdžiai paveikė ir Baltijos jūros, Klaipėdos uosto bei pasienio teritorijas, taip pat – mobiliojo ryšio bazines stotis Panemunės pasienyje.

RRT 2025 m. veiksmingai sprendė žalingųjų radijo trukdžių problemas:

- iškėlė GNSS trukdžių Baltijos regione klausimą ES ir tarptautiniu lygmenimis – Tarptautinė telekomunikacijų sąjunga (angl. *International Telecommunication Union* (ITU) įpareigojo Rusiją nutraukti trukdžius;
- vykdė GNSS trukdžių tyrimus, įdiegė ADS-B (angl. *Automatic Dependent Surveillance-Broadcast*) aviacinių duomenų stebėseną, kuri leidžia realiu laiku nustatyti GNSS trukdžių šaltinius, jų mastą ir poveikį;
- siekdama sumažinti tarpvalstybinių žalingųjų radijo trukdžių neigiamą poveikį radijo ryšio kokybei, nustatė taisykles, kokiais atvejais RRT skirs papildomus radijo dažnius mobiliojo ryšio operatoriams[01].

Efektyvesnė vartotojų apsauga nuo sukčiavimo elektroninėje erdvėje

2025 m. RRT kryptingai stiprino sukčiavimo elektroninėje erdvėje prevenciją. **RRT tarybai priėmus 2025 m. balandžio 8 d. nutarimą Nr. TN-209**[02], elektroninių ryšių tinklų operatoriams (toliau – operatoriai) atsirado daugiau galimybių blokuoti apgaulingus skambučius ir keistis informacija apie tokius numerius bei abonentus, naudojančius tarptautinį tarptinklinį ryšį: nuo 2025 m. spalio 1 d. fiksuotas staigus apgaulingų skambučių blokavimų augimas – per vieną gruodžio savaitę operatoriai sulaikydavo nuo 600 tūkst. iki 1 mln. apgaulingų skambučių. 2025 m. iš viso užblokuota 13 298 316 apgaulingų skambučių (63 proc. daugiau nei 2024 m.) ir 5 725 890 apsimestinių SMS žinučių (beveik 80 proc. daugiau nei 2024 m.) operatorių tinkluose. RRT kartu su operatoriais identifikavo SIM spiečių įrangos naudojimo atvejus Vilniuje ir surinktą informaciją perdavė policijai. Tokia RRT veikla padeda išvengti susidūrimo su sukčiais ne tik vartotojams – lengviau ir policijai ištirti bei užkardyti nusikalstamas veikas.

2025 m. kovo 27 d. **RRT pasirašė tarpinstitucinį memorandumą** su Generaline prokuratūra, Lietuvos policija, NKSC, Lietuvos banku ir Pinigų plovimo prevencijos kompetencijų centru dėl bendradarbiavimo siekiant mažinti sukčiavimą skaitmeninėje erdvėje. Pagal šį memorandumą RRT vykdo operatorių priežiūrą ir elektroninių ryšių tinklų stebėseną, su kitomis kompetentingomis institucijomis dalinasi informacija apie blokuojamus telefoninius skambučius, SMS žinutes, sukčiavimo atvejus, vykdo vartotojų švietimą.

01
Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos 2025 m. rugpjūčio 6 d. nutarimas Nr. TN-420 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos 2025 m. birželio 3 d. nutarimo Nr. TN-339 „Dėl Elektroninių ryšių išteklių skyrimo ir naudojimo taisyklių patvirtinimo“ pakeitimo“.

02
Lietuvos Respublikos ryšių reguliavimo tarnybos tarybos 2025 m. balandžio 8 d. nutarimas Nr. TN-209 „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“.

Elektroninė atpažintis kaip kritinė prieiga prie paslaugų elektroninėje erdvėje

Elektroninė atpažintis ir kvalifikuotas elektroninis parašas yra priemonės, naudojamos patikimam tapatybės patvirtinimui prisijungiant prie elektroninių paslaugų ar atliekant teisiškai reikšmingus veiksmus elektroninėje erdvėje tiek viešajame, tiek privačiame sektoriuje. 2025 m. kvalifikuotu elektroniniu parašu naudojosi 40 proc. 18 metų ir vyresnių Lietuvos gyventojų. Dažniausi elektroninio parašo naudojimo atvejai buvo asmeninių elektroninių dokumentų pasirašymas (65 proc.), transakcijų pasirašymas elektroninės bankininkystės sistemoje (52 proc.), operacijos „Sodroje“ ar kitose valstybinėse informacinėse sistemose (49 proc.) ir darbinių elektroninių dokumentų pasirašymas (46 proc.). Esant tokiam tapatybės patvirtinimo būdų naudojimo paplitimui, elektroninės atpažinties ir elektroninio pasirašymo patikimumas bei saugumas yra tiesiogiai susiję su elektroninių paslaugų prieinamumu ir pasitikėjimu elektronine erdve, nes šių paslaugų sutrikimai ar saugumo spragos gali paveikti daug naudotojų ir paslaugų teikėjų.

2025 m. RRT, vykdydama kvalifikuotos elektroninės atpažinties ir kvalifikuotų patikimumo užtikrinimo paslaugų priežiūrą, priėmė sprendimus, susijusius su šių paslaugų teikimu Lietuvoje. 2025 m. lapkričio 13 d. **RRT suteikė Migracijos departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos leidimą teikti kvalifikuotų elektroninio parašo sertifikatų sudarymo paslaugas**, taip išplėsdama kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų ratą ir sudarydama galimybę rinkai naudotis papildoma alternatyva šioje srityje[03]. 2025 m. lapkričio mėn. RRT taip pat gavo UAB „Paysera“ pranešimą apie ketinimą teikti aukšto saugumo užtikrinimo lygio elektroninės atpažinties priemonę[04].

Rengiantis europinės **skaitmeninės tapatybės dėklės** (angl. *EU Digital Identity Wallet (EUDI Wallet)* diegimui Lietuvoje pagal 2024 m. balandžio 11 d. **Europos Parlamento ir Tarybos reglamentą** (ES) 2024/1183[05], svarbu aiškiai nustatyti ir apibrėžti visų atsakingų organizacijų kontaktus, pagal kompetenciją apibrėžti organizacijų atsakomybės sritis, incidentų eskalavimo tvarką ir veikiančius informacijos apsikeitimo kanalus tarp institucijų bei paslaugų teikėjų. Tai padės užtikrinti, kad plečiantis elektroninių paslaugų sąveikai būtų galima koordinuotai ir operatyviai reaguoti į kylančias rizikas ir incidentus.

03

2026 m. pradžioje Lietuvoje buvo 7 patikimumo užtikrinimo paslaugų teikėjai ir 3 elektroninės atpažinties paslaugų teikėjai.

04

RRT atlikus UAB „Paysera“ pateiktos elektroninės atpažinties priemonės atitikties vertinimą, UAB „Paysera“ 2026 m. sausio 28 d. oficialiai pripažinta kvalifikuotos elektroninės atpažinties paslaugų teikėju, atitinkančiu aukšto saugumo lygio reikalavimus.

05

2024 m. balandžio 11 d. Europos Parlamento ir Tarybos Reglamentas (ES) 2024/1183, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu.

Skaitmeninių paslaugų priežiūra: rizikos ir stiprėjanti ekosistema

RRT vykdo skaitmeninių paslaugų koordinatorės funkcijas pagal **Skaitmeninių paslaugų akto** (toliau – SPA)[06] reikalavimus ir yra atsakinga už šio akto įgyvendinimo vykdymą ir priežiūrą. 2025 m. SPA nuostatų įgyvendinimas Lietuvoje pasireiškė aktyvesniu bei spartesniu institucijų, vartotojų, patikimų pranešėjų reagavimu į neteisėtą bei žalingą turinį interneto platformose ir kompleksinių sprendimų paieška tokioms sisteminėms rizikoms, kaip žala nepilnamečiams, dezinformacija, sukčiavimo kampanijos ir kt., įvertinti bei sumažinti ir didesne Lietuvos bei užsienio tarpininkavimo paslaugų teikėjų priežiūra bei proaktyvia atsakomybe užtikrinant SPA atitiktį.

2025 m. pirmąjį pusmetį Lietuvos institucijos labai didelėms interneto platformoms pateikė 480 pranešimų ir privalomų nurodymų dėl neteisėto turinio pašalinimo. Palyginkime: visoje ES per šį laikotarpį tokių pranešimų buvo apie 2700. Tai rodo, kad Lietuva yra viena aktyviausiai SPA mechanizmus taikančių valstybių. Didžioji dalis pranešimų buvo susiję su socialiniais tinklais, kur neteisėtas turinys – nuo sukčiavimo schemų iki dezinformacijos – plinta sparčiausiai ir daro didžiausią žalą vartotojams.

Gautų interneto platformų vartotojų skundų pagal SPA 53 straipsnį dėl galimų SPA pažeidimų skaičius išaugo nuo 3 (2024 m.) iki 25 (2025 m.). Tai rodo, kad paslaugų vartotojai aktyviau naudojasi SPA suteikiamais teisių gynimo mechanizmais. Vartotojų skundai apėmė tiek Lietuvos, tiek užsienio interneto platformų paslaugų teikėjus, dėl kurių RRT kreipėsi į kitų ES šalių koordinatorius. 2025 m. RRT pateiktuose vartotojų skunduose atsispindi įvairūs minėtų paslaugų teikėjų atitikties SPA trūkumai: nuo tinkamo pranešimų apie neteisėtą turinį mechanizmo nebuvimo iki neaiškiai apibrėžtų naudojimosi sąlygų, lemiančių vartotojų paskyrų blokavimą, ir pan.

2025 m. stiprėjo ir visa SPA ekosistema:

- RRT pateikė oficialius duomenis EK tyrimui dėl galimų vienos labai didelės interneto platformos SPA pažeidimų;
- RRT sertifikavo du naujus patikimus pranešėjus (angl. *Trusted Flagger*)[07], t. y. UAB „Piracy Meter“ ir VšĮ „Debunk EU“, o dar šešiems kandidatams RRT suteikė konsultacijas ir dalis iš jų 2026 m. pateiks paraiškas gauti patikimo pranešėjo statusą[08].

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).

07

Patikimi pranešėjai – nepriklausomos organizacijos ar kompetentingos institucijos, turinčios ekspertinių žinių ir kompetencijos, nustatant neteisėtą turinį, kurių pranešimai platformoms nagrinėjami prioriteto tvarka siekiant užtikrinti veiksmingą turinio priežiūrą. Patikimo pranešėjo statusą pagal SPA suteikia valstybės narės, kurioje pareiškėjas yra įsisteigęs, skaitmeninių paslaugų koordinatorius.

08

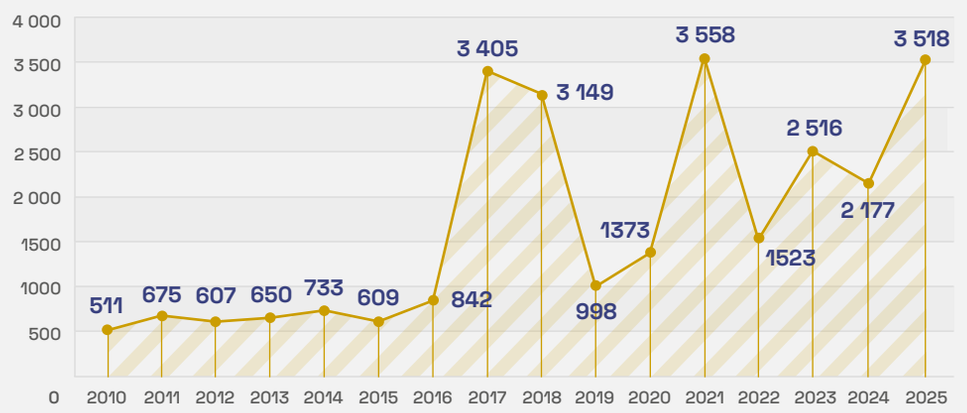
Iš viso Lietuvoje 2025 m. veikė 3 patikimi pranešėjai.

2025 m. Lietuvoje sertifikuoti patikimi pranešėjai pateikė apie 2000 pranešimų, į kuriuos atsižvelgus pašalinta apie 6 mln. neteisėto turinio, susijusio su finansiniu sukčiavimu, intelektinės nuosavybės apsauga ir kenksmingais augalininkystės produktais, nuorodų. Kadangi patikimų pranešėjų pranešimai pagal SPA interneto platformose vertinami prioritetine tvarka ir be nepagrįsto delsimo, didesnis patikimų pranešėjų skaičius praktiškai sustiprina greitesnį neteisėto turinio identifikavimą interneto platformose ir šalinimą bei didina SPA mechanizmų veiksmingumą. Kitaip tariant, patikimų pranešėjų ekosistemos plėtra yra vienas geriausių būdų mažinti neteisėto turinio sklaidą internete.

Nepilnamečių apsauga internete: karštoji linija „Švarus internetas“ ir apsauga nuo žalingo turinio

2025 m. **RRT interneto karštoji linija „Švarus internetas“** išliko svarbiu kanalu nepilnamečiams žalingam ar neteisėtam turiniui internete identifikuoti ir jo pašalinimui inicijuoti. 2025 m. gauta 3518 pranešimų – beveik 62 proc. daugiau nei 2024 m. (**1 pav.**).

RRT karštąja linija gautų pranešimų dinamika 2010–2025 m.

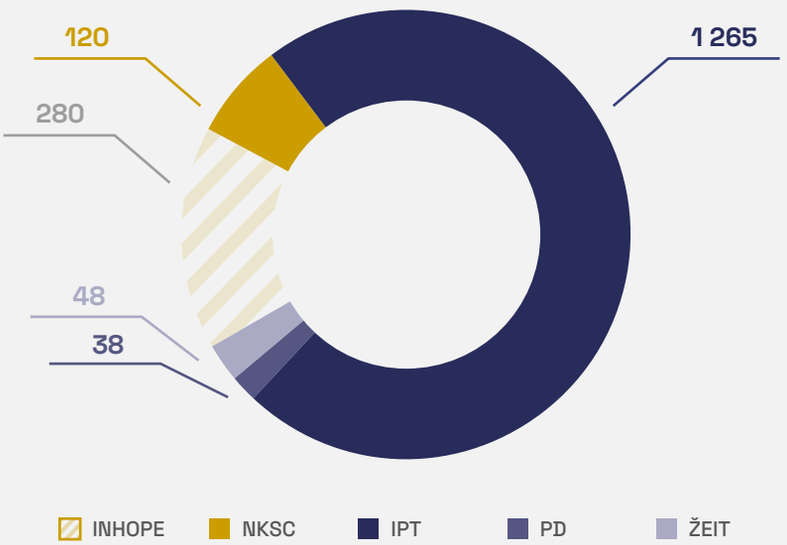


< 1 pav.

RRT karštąja linija gautų pranešimų dinamika 2010–2025 m.
(šaltinis – VDAI)

Pasitvirtinusių pranešimų, t. y. pranešimų apie draudžiamą ir neigiamą poveikį nepilnamečiams darančią informaciją, dėl kurios pašalinimo galima imtis veiksmų, buvo 2263 (2024 m. – 1488). Šis pasitvirtinusių pranešimų augimas rodo, kad visuomenė vis geriau atpažįsta nepilnamečiams neigiamą poveikį darantį turinį ir pasitiki sukurtais reagavimo mechanizmais. RRT atliktų veiksmų su pasitvirtinusiais pranešimais, gautais karštąja linija, diagrama (**2 pav.**).

Veiksmai, atlikti su pranešimais



1265 pranešimai persiųsti prieglobos, interneto paslaugų teikėjams, svetainių valdytojams, interneto platformoms;

280 pranešimų apie vaikų seksualinio išnaudojimo vaizdus persiųsta tarptautinės interneto karštųjų linijų asociacijos INHOPE narėms;

38 pranešimai persiųsti tyrimui Policijos departamentui (iš jų 30 – apie vaikų seksualinio išnaudojimo vaizdus);

48 pranešimai persiųsti Žurnalistų etikos inspektoriaus tarnybai (ŽEIT);

120 pranešimų persiųsta NKSC (įtariant kibernetinį incidentą ar sukčiavimą kibernetinėje erdvėje);

512 pranešimų buvo pasikartojantys, dėl kurių jau buvo imtasi anksčiau aprašytų veiksmų.

< 2 pav.

2025 m. RRT atliktų veiksmų su pranešimais, gautais karštąja linija, apie galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darantį turinį internete, diagrama
(šaltinis – RRT)

2025 m. per RRT interneto karštąją liniją „Švarus internetas“ buvo sustiprintas operatyvesnis reagavimas į sukčiavimą kibernetinėje erdvėje ir įtariamus kibernetinius incidentus: 120 pasitvirtinusių pranešimų perduota NKSC, inicijuojant kenkimo domenų blokavimą sistemoje „Vasaris“. Dėl to sutrumpėjo laikas nuo vartotojo pranešimo iki pritaikytos apsaugos priemonės.

Daugiausia nerimo kelia itin **sparčiai augantis kibernetinių patyčių mastas**. 2025 m. RRT gavo 186 su patyčiomis susijusius pranešimus, iš kurių pasitvirtino net 143 pranešimai (2024 m. pasitvirtinusių pranešimų buvo 47, o 2023 m. – vos 27). Palyginti su 2024 m., pasitvirtinusių pranešimų apie patyčias skaičius padidėjo apie tris kartus, o per trejus metus – daugiau nei penkis kartus. Patyčių kibernetinėje erdvėje daugėja ne tik dėl didėjančio vaikų aktyvumo internete, bet ir dėl to, kad patyčios vis dažniau vyksta uždarose grupėse ar nišinėse platformose, kur turinys nėra viešas ir jį sunkiau nustatyti bei įvertinti.

Vaikų seksualinio išnaudojimo medžiaga yra draudžiama visame pasaulyje, todėl į tokius pranešimus reaguojama nedelsiant. Nustačius tokį turinį Lietuvoje, informacija perduodama policijai ir prieglobos paslaugų teikėjui, kad neteisėtas turinys būtų kuo greičiau pašalintas. 2025 m. pranešimų apie **vaikų seksualinio išnaudojimo vaizdus internete** padaugėjo 18 proc. Kadangi didžioji dalis tokio turinio buvo užsienio serveriuose, pranešimai perduoti kitų šalių interneto karštosioms linijoms, siekiant operatyviai pašalinti turinį ir imtis tolesnių veiksmų.

2025 m. RRT siekė sustiprinti mokyklų ir viešųjų bibliotekų galimybes apsaugoti nepilnamečius nuo žalingo turinio. RRT aprobavo 4 naujas filtravimo priemones. Tačiau **filtravimo priemonių diegimas** išliko nevienodas – dalis įstaigų vis dar neturi technologinių sprendimų, todėl apsauga išlieka fragmentiška. Todėl reikia efektyvesnių IT sprendimų ir tvaresnių diegimo modelių, kartu aiškiau apibrėžiant steigėjų ir įstaigų, kurios turi naudoti filtravimo priemones, atsakomybę bei stiprinant metodinę ir organizacinę pagalbą, kad filtravimo priemonių taikymas būtų užtikrintas nuosekliai visose prieigos vietose.

Edukacinė veikla: skaitmeninių įgūdžių stiprinimas Lietuvoje

2025 m. toliau buvo plėtojamas **RRT inicijuotas ir Lietuvos Respublikos Prezidento globojamas projektas „Nė vienas nėra pamirštas“**, skirtas visuomenės skaitmeniniams įgūdžiams stiprinti ir saugesniam naudojimuisi skaitmeninėmis technologijomis skatinti. Projekto veiklos 2025 m. pasiekė dešimtis tūkstančių gyventojų visoje Lietuvoje: skaitmeninio raštingumo mokymuose dalyvavo daugiau kaip 22,7 tūkst. vyresnio amžiaus žmonių ir 2,4 tūkst. moksleivių, o Saugesnio interneto dienai skirtą renginį „Skaitmeninė banga“ gyvai ir nuotoliu stebėjo daugiau kaip 80 tūkst. įvairaus amžiaus gyventojų. Taip pat buvo sustiprintas skaitmeninių įgūdžių sklaidos tinklas regionuose – bandomuosiuose mokymuose dalyvavo 200 viešųjų bibliotekų, jų darbuotojai tapo skaitmeninio raštingumo ambasadoriais vietos bendruomenėse. Projektas sulaukė tarptautinio įvertinimo – iniciatyva pateko į Europos skaitmeninių įgūdžių apdovanojimų finalą kategorijoje „Įtrauktis į skaitmeninį pasaulį“. Projekto veiklą numatoma tęsti ir 2026 m.

Prie visuomenės skaitmeninių įgūdžių stiprinimo prisidėjo ir RRT ekspertų dalyvavimas Vilniaus miesto savivaldybės kartu su švietimo iniciatyva „EDU Vilnius“ vykdomame projekte „Vilnius yra mokykla“. RRT specialistai Vilniaus mokyklose vedė 18 edukacinių pamokų, kuriose dalyvavo apie 450 mokinių.

Saugumo aplinkos pokyčiai ir tendencijos

2025 m. įvykiai parodė, kad žalingieji radijo trukdžiai yra ilgalaikė ir sisteminė problema. Jos sprendimui būtina technologinė pažanga, atsakingų institucijų ir elektroninių ryšių tinklų operatorių bendradarbiavimas bei vieningas ES atsakas, užtikrinantis saugią ir patikimą radijo ryšių aplinką visame regione, įskaitant diplomatinius, teisinius ir technologinius sprendimus bei koordinuotą reagavimą.

2025 m. RRT inicijuotos reguliacinės ir technologinės priemonės dėl sukčiavimo kibernetinėje erdvėje pasiteisino – apgaulingų skambučių blokavimas tapo efektyvesnis. Tačiau sukčiavimo metodai sparčiai keičiasi, daugėja suklastotų lietuviškų numerių ir socialinės inžinerijos metodų, todėl reikės ne tik nuolat atnaujinti prevencines priemones, bet ir aiškiau reglamentuoti SIM kortelių registravimą ir naudojimą, gerinti duomenų apsikeitimo modelį bei stiprinti techninį ir analitinį bendradarbiavimą su teisėsauga.

SPA įgyvendinimo praktika rodo, kad Lietuva yra tarp aktyviausiai SPA mechanizmus taikančių ES valstybių. Didelis pranešimų skaičius ir patikimų pranešėjų indėlis rodo veikiančią institucijų, platformų ir pranešėjų bendradarbiavimo sistemą, leidžiančią greičiau identifikuoti ir šalinti neteisėtą turinį, tačiau kartu išryškina poreikį toliau stiprinti institucinius ir techninius pajėgumus.

RRT karštosios linijos „Švarus internetas“ veikla rodo didėjantį visuomenės sąmoningumą: padaugėjo pranešimų apie draudžiamą ir neigiamą poveikį nepilnamečiams darančią informaciją. Kita vertus, išryškėjo ir nauji iššūkiai. Draudžiama ir neigiamą poveikį nepilnamečiams daranti informacija vis dažniau plinta uždarose skaitmeninėse erdvėse ir neretai laikoma užsienio serveriuose, todėl tokio turinio nustatymas ir šalinimas vis labiau priklauso nuo operatyvaus institucijų ir tarptautinių partnerių bendradarbiavimo. Be to, išlieka poreikis nuosekliau diegti technines nepilnamečių apsaugos priemones – turinio filtravimo būdai švietimo ir viešosiose įstaigose vis dar taikomi nevienodai.

RRT vykdomos skaitmeninių įgūdžių stiprinimo iniciatyvos rodo, kad visuomenės atsparumas kibernetinėms grėsmėms tiesiogiai priklauso nuo gyventojų skaitmeninio raštingumo. Didėjantis gebėjimas atpažinti sukčiavimo ir kitas kibernetines grėsmes tampa svarbia prevencijos priemone, todėl būtina nuosekliai stiprinti visuomenės skaitmeninius įgūdžius ir plėsti švietimo iniciatyvas įvairioms visuomenės grupėms.

DI ir automatizacijos poveikis saugumo aplinkai

Siekiant užtikrinti saugesnę kibernetinę erdvę, DI modeliai yra galinga priemonė, padedanti interneto platformoms aptikti neteisėtą ir žalingą turinį ar net neleisti vartotojams tokį turinį paskelbti, ypač jei jis susijęs su tokiomis baudžiamosiomis veikomis, kaip vaikų seksualinis išnaudojimas, terorizmas ir kt.

2025 m. Lietuvoje pradėtas sistemingas pasirengimas įgyvendinti 2024 m. ES priimtą **Dirbtinio intelekto aktą**[09] (toliau – DI aktas), nustatantį suderintas DI sistemų kūrimo, tiekimo ir naudojimo taisykles vidaus rinkoje. 2025 m. balandžio 1 d. RRT buvo paskirta nacionaline kompetentinga rinkos priežiūros institucija ir bendruoju kontaktiniu punktu pagal DI aktą. Atsižvelgiant į DI technologijų horizontalaus taikymo pobūdį, t. y. į taikymą įvairiuose sektoriuose bei siekiant sukurti aiškų ir nuoseklų teisinį pagrindą DI akto įgyvendinimui, 2025 m. Ekonomikos ir inovacijų ministerija kartu su RRT pradėjo rengti **įstatymo dėl DI akto įgyvendinimo projektą**[10], kuriame numatoma nustatyti atsakingas institucijas, jų kompetencijas, tarpusavio bendradarbiavimo principus bei priežiūros ir vykdymo užtikrinimo mechanizmus.

09
2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 2024/1689, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas).

10
Lietuvos Respublikos įstatymo „Dėl Europos Sąjungos Dirbtinio intelekto akto įgyvendinimo“ projektas.

DI akto reikalavimai, ypač taikomi didelės rizikos DI sistemoms, apima rizikos valdymą, duomenų kokybę, incidentų registravimą, žmogaus priežiūrą, sistemų patikimumą ir atsparumą. Jų įgyvendinimas prisideda prie saugesnio DI naudojimo, mažina tokių sistemų pažeidžiamumų išnaudojimo riziką ir prisideda prie bendro nacionalinio kibernetinio atsparumo.

Rizikos, susijusios su priklausomybe nuo išorinių paslaugų teikėjų ir tiekimo grandinių

RRT vykdomoje „Švaraus interneto“ veikloje labai svarbus veiksnys, susijęs su priklausomybe nuo trečiųjų šalių, – interneto platformų ir prieglobos paslaugų teikėjų veiksmų greitis. Praktika parodė, kad greitas perėjimas nuo pranešimo prie konkrečių veiksmų – turinio pašalinimo, prieigos apribojimo arba informacijos perdavimo atsakingoms institucijoms – leidžia efektyviausiai sumažinti žalos mastą ir trukmę.

Papildomos įžvalgos iš kitų ataskaitų

2025 m. **Europos skaitmeninių paslaugų valdybos parengta sisteminių rizikų ataskaita**[11] kaip vieną iš rizikos faktorių identifikuoja DI sistemų panaudojimą neteisėtam turiniui kurti, kuris yra platinamas per interneto platformas ir taip stipriai prisideda prie tokių sisteminių rizikų kaip smurtas prieš moteris, vaikų seksualinis išnaudojimas, dezinformacija, sukčiavimas ir kt. Vieno iš **Lietuvos patikimų pranešėjų 2025 m. ataskaitoje**[12] taip pat nurodoma, kad nusikaltėliai vis dažniau naudojasi pažangiomis priemonėmis, tokiomis kaip generatyvinis DI ir algoritminė manipuliacija – šios technologijos leidžia automatizuoti svetainių kūrimą, pritaikyti sukčiavimo turinį skirtingoms kalboms ir regionams bei naudoti išmaniojo vaizdo klastojimo (angl. *Deepfake*) įrašus, įtikinamai apsimetant patikimais asmenimis ir taip gerokai padidinant sukčiavimo schemų sėkmės tikimybę.

RRT žvilgsnis į 2026 m.

2026 m. RRT skirs dėmesio kovai su sukčiavimu elektroninių ryšių tinkluose stiprinti – tobulins apgaulingų skambučių prevencijos priemones ir stiprins bendradarbiavimą su teisėsaugos institucijomis. Taip pat bus stiprinamas SPA įgyvendinimas – dirbama su tarpininkavimo paslaugų teikėjais dėl atitikties SPA reikalavimams, plėtojama patikimų pranešėjų ekosistema ir stiprinamas bendradarbiavimas su EK bei kitų šalių skaitmeninių paslaugų koordinatoriais. Vienas iš prioritetų bus DI rinkos priežiūros modelio sukūrimas ir nuoseklios DI sistemų priežiūros užtikrinimas. Be to, bus stiprinamos ir saugesnės skaitmeninės aplinkos priemonės, užtikrinančios žalingo turinio prevenciją, nepilnamečių apsaugą ir visuomenės skaitmeninio raštingumo didinimą.

11 **Pirmoji Europos skaitmeninių paslaugų valdybos ataskaita**, parengta bendradarbiaujant su Komisija pagal SPA 35 straipsnio 2 dalį, apie labiausiai pastebimas ir pasikartojančias sistemines rizikas bei jų mažinimo priemones.

12 **Patikimo pranešėjo „Debunk.org“ 2025 m. ataskaita.**

Priešiškos informacinės aplinkos vertinimas

Plk. Liutauras Bagočiūnas,
LK SKD direktorius

Vadovo žodis

2025 m. visoje Europoje stebėjome išaugusius hibridinių incidentų, neaplenkusių ir Lietuvos, skaičius. Nuolatiniai oro erdvės pažeidimai, incidentai, keliantys grėsmę civilinei aviacijai, ir kritinės infrastruktūros pažeidimai buvo naudojami priešiškiems naratyvams informacinėje erdvėje skleisti, siekiant didinti nepasitikėjimą Lietuvos gynybos pajėgumais ir NATO vienybe. Besiplečiant informacinei erdvei, priešiškiems veikėjams vis lengviau skleisti klaidinančią informaciją, ir demokratinės valstybės privalo stiprinti visuomenės atsparumą propagandai ir dezinformacijai. Lietuvos kariuomenės Strateginės komunikacijos departamentas prisideda prie sistemingos priešiškos informacinės erdvės stebėsenos ir analizės, visuomenės švietimo ir atsparumo informacinėms grėsmėms didinimo.

LK SKD vaidmuo nacionalinėje kibernetinio saugumo ekosistemoje

LK SKD stebi ir analizuoja laisvai prieinamuose informaciniuose kanaluose skleidžiamą priešišką Rusijos ir Baltarusijos komunikaciją, susijusią su Lietuvos gynybos klausimais bei Lietuvos kariuomenės veikla.

3 707

3 707 identifikuoti informaciniai incidentai, kai buvo skleista priešiška, klaidinanti ar melaginga informacija apie Lietuvą ar jos partnerius (NATO, ES)

70 %

visų identifikuotų informacinių incidentų, nukreiptų prieš Lietuvą ar jos partnerius, dominavo gynybos ir saugumo tematika

LIETUVOS KARIUOMENĖ

kariuomene.lt

LK.kanceliarija@mil.lt

+370 5 278 5032

2025 m. išmoktos pamokos, aplinkos pokyčiai, darę įtaką LK SKD veiklai

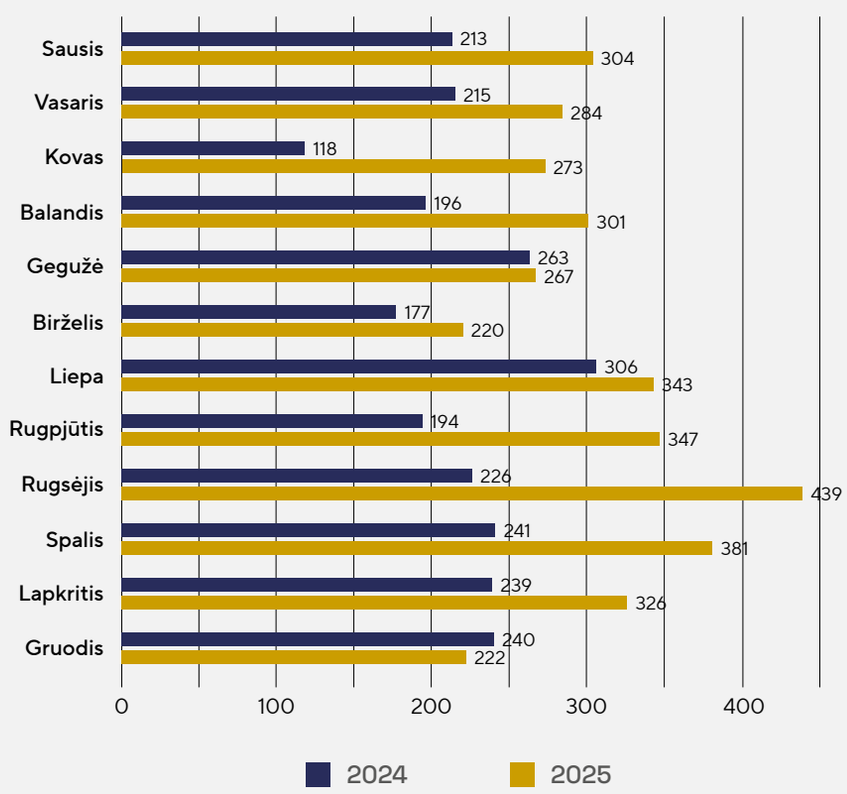
2025 m. tik dar kartą patvirtino, kad visapusiškai informacinės erdvės stebėsenai vykdyti ir priešiškai veiklai užkardyti ypatingai svarbus glaudus tarpinstitucinis bendradarbiavimas. Daugiametė, sistemiška Rusijos ir Baltarusijos informacinės erdvės stebėsena leidžia atpažinti tendencijas, numatyti priešiškų šalių strateginius tikslus ir taikinius. Bendradarbiavimas su žiniasklaida, visuomenės informavimas yra svarbūs veiksniai siekiant apriboti priešiškų valstybių įtaką informacinėje erdvėje.

Stiprinama skaitmeninės erdvės priežiūra ir padidėjęs visuomenės aktyvumas pranešant apie netinkamą turinį internete

LK SKD identifikuotų informacinių incidentų dinamika

2025 m. LK SKD identifikavo 3 707 informacinius incidentus, kai buvo skleista priešiška, klaidinanti ar melaginga informacija apie Lietuvą ar jos partnerius (NATO, ES). Lyginant su 2024 m., aptariamuoju laikotarpiu informacinių incidentų padaugėjo. Tai siejama su aktyvėjančiu priešišku Baltarusijos veikimu informacinėje erdvėje ir nuosekliu Rusijos veikimu prieš NATO ir ES.

Priešiškų informacinių incidentų grafikas 2024 m. ir 2025 m.



< 2 pav.

Priešiškų informacinių incidentų grafikas 2024 m. ir 2025 m. (*šaltinis – LK SKD*)

Gynybos ir saugumo tematika ne vienerius metus išlieka dominuojanti priešiškoje informacinėje aplinkoje. 2025 m. ji sudarė 70 proc. visų identifikuotų informacinių incidentų, nukreiptų prieš Lietuvą ar jos partnerius. Ši tema apžvelgiamaisiais metais išlieka aktuali dėl besitęsiančios Rusijos agresijos prieš Ukrainą, dėl Rusijos ir Baltarusijos pastangų menkinti NATO rytinio flango šalių pajėgumų stiprinimą, dėl reakcijos į pradėtą NATO jūrų stebėjimo misiją „Baltic Sentry“ ir vykdytos informacinės kampanijos bendrų Rusijos ir Baltarusijos pratybų „Zapad-2025“ kontekste.

Saugumo aplinkos pokyčiai ir tendencijos

Aktyviausiais propagandos sklaidos kanalais išliko valstybinės ir režimų kontroliuojamos žiniasklaidos priemonės, taip pat socialiniai tinklai, daugiausiai – „Telegram“. Priešiškas žinutes komunikavo Rusijos ir Baltarusijos pareigūnai, režimui palankūs ekspertai, apžvalgininkai, žurnalistai ir kiti propagandininkai.

Gynybos ir saugumo temoje 2025 m. ypatingai didelis dėmesys skirtas Baltijos jūros regionui ir Kaliningrado sričiai. Šią tendenciją pirmiausiai lėmė 2025 m. sausio viduryje prasidėjusi NATO Baltijos jūros stebėsenos misija „Baltic Sentry“. Rusijos propaganda kaltino NATO vykdant „modernų piratavimą“ ir pažeidžiant tarptautinę jūrų teisę. Šiame kontekste NATO ar atskiros Aljanso šalys taip pat kaltintos planuojant įvykdyti Kaliningrado blokadą ar okupuoti šį regioną.

Priešiškų valstybių taikiniu buvo Lietuvos gynybos politikos sprendimai, ypatingai išnaudota pasienio su Rusija ir Baltarusija gynybos stiprinimo tema. Propaganda siekė menkinti Lietuvos, taip pat kitų NATO rytinio flango valstybių, gebėjimą užtikrinti savo saugumą.

2025 m. stebėtas augantis Baltarusijos režimo vykdomas informacinis spaudimas prieš Lietuvą, siekiant įtikinti tiek vidaus, tiek išorės auditorijas, kad Lietuvos vykdoma užsienio politika yra neracionali, agresyvi Baltarusijos atžvilgiu ir kenksminga Lietuvos piliečiams. Baltarusijos pareigūnai apeliavo į Lietuvos visuomenę, siekdami įtikinti, kad oficiali Lietuvos valstybės pozicija užsienio politikos klausimais neatspindi Lietuvos visuomenės valios.

Dvišalių JAV ir Rusijos santykių atkūrimas lėmė pokyčius Kremliaus ir Minsko komunikacijoje. Aktyviai siekta išnaudoti tarp NATO valstybių kilusias įtampas, didesnis informacinis spaudimas nukreiptas prieš Europos valstybes, jos kaltintos derybų dėl taikos Ukrainoje trikdymu.

2025 m. LK SKD fiksuoti nauji priešiški naratyvai:

- NATO veiksmai ir provokacijos Baltijos jūroje didina konflikto riziką;
- NATO taikdarių dislokavimas Ukrainoje yra provokacija ir kelia grėsmę Rusijai;
- Europa siekia išlaikyti įtampą tarptautinėje politikoje;
- JAV nėra suinteresuotos transatlantiniu bendradarbiavimu su Europos šalimis;
- NATO nėra pajėgi užtikrinti savo oro erdvės gynybos;
- Lietuva dirbtinai kelia krizę pasienyje su Baltarusija;
- Ukraina siekia įtraukti NATO į konfliktą su Rusija;
- Europa nėra pajėgi užtikrinti savo gynybos be JAV;
- Raketos „Orešnik“ Baltarusijoje yra atsakas į NATO keliamas grėsmes;
- NATO ir ES siekia destabilizuoti saugumo situaciją Moldovoje;
- NATO ruošiasi per artimiausius penkerius metus pradėti konfliktą su Sąjungine valstybe;
- Atsijungimas nuo energetinio BRELL žiedo lemia neišvengiamą kainų kilimą ir nepatikimą elektros tiekimą;
- Pratybos „Zapad“ yra grynai gynybinio pobūdžio, o NATO pratybos – puolamojo.

2025 m. informaciniai incidentai neretai buvo glaudžiai susiję su įvykiais fizinėje erdvėje, kuriuos Vakarų šalių pareigūnai vis dažniau įvardino kaip galimas **Rusijos ir Baltarusijos hibridines atakas**. Rusija ir Baltarusija naudojosi šiais įvykiais, kad sustiprintų propagandinius naratyvus. Priešiškos šalys naudojo ir kitus metodus, tokius kaip manipuliavimas Vakarų žiniasklaidos šaltiniais ir jų pateikiama informacija. Kremlius toliau platino savo istorines interpretacijas ir melagienas socialiniuose tinkluose ir tradicinėse medijose.

Rusijos ir Baltarusijos priešiška komunikacija yra vertinama kaip daugiakryptė, kuria lygiagrečiai siekiama paveikti mažiausiai 3 skirtingas auditorijas: Vakarų šalių, Lietuvos ir vidines Rusijos ir Baltarusijos auditorijas. Priešiškų valstybių skleidžiamos žinutės yra konstruojamos ir pritaikomos kiekvienai auditorijai, atsižvelgiant į numatomus poveikio tikslus, kurie, numanoma, strateginiu lygmeniu koreliuoja tarpusavyje.

Informaciniu spaudimu siekta įtikinti Rusijos ir Baltarusijos vidaus auditorijas tariamu NATO agresyvumu, o Vakarų šalių auditorijos baugintos Rusijos kariniais pajėgumais. Priešiškos valstybės siekė diskredituoti Lietuvos gynybos ir užsienio politiką, didinti Lietuvos visuomenės nepasitikėjimą vyriausybe.

LK SKD 2025 m. tęsė aktyvų bendradarbiavimą su kitomis informacinės erdvės stebėseną vykdančiomis institucijomis, dalyvavo Nacionalinio krizių valdymo centro (toliau – NKVC) koordinuojamoje analitikų darbo grupėje. Kartu su kitomis Lietuvos institucijomis LK SKD prisidėjo prie greitos ir efektyvios reakcijos į informacinius incidentus, platesnio informacinio paveikslo sudarymo ir rekomendacijų pateikimo sprendimų priėmėjams ir valstybės institucijų komunikacijos specialistams.

Siekdami informuoti visuomenę apie informacines grėsmes, 2025 m. LK SKD atstovai skaitė pranešimus įvairioms visuomenės grupėms, dalyvavo konferencijose ir diskusijose, bendradarbiavo su žiniasklaida.

LK SKD bendradarbiavo su užsienio partneriais, pirmiausia su **NATO Strateginės komunikacijos kompetencijų centru** (angl. *NATO Strategic Communications Centre of Excellence,* NATO StratCom CoE). NATO šalių susitikimų formatuose Lietuvos kariuomenė dalinosi įžvalgomis, analitiniais produktais ir tyrimais. Šio formato susitikimai leidžia Lietuvos kariuomenės analitikams susipažinti su naujausiomis tendencijomis, informacinės erdvės stebėsenos įrankiais, pasisemti patirties iš partnerių, kurie susiduria su panašiomis grėsmėmis.

DI ir automatizacijos poveikis saugumo aplinkai

2025 m. DI tapo struktūriniu grėsmės daugikliu LK SKD veiklos srityje – jis naudojamas kibernetinėse atakose, socialinės inžinerijos ir sukčiavimo schemose, informacinėse bei psichologinėse operacijose. DI įgalina kur kas didesnį priešiškų kampanijų mastą, greitesnį naratyvų adaptavimą ir aukštesnį personalizacijos bei maskavimo lygį, todėl tradicinės stebėsenos ir reagavimo priemonės tampa nepakankamos.

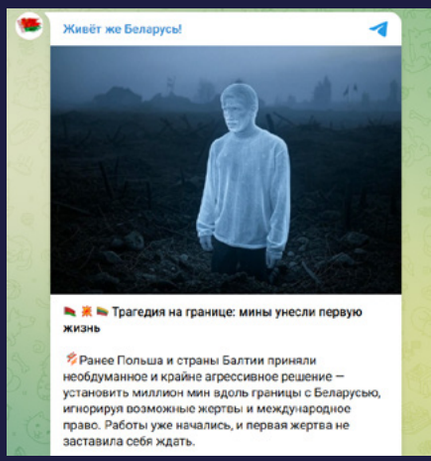
Viešosios komunikacijos, informacinės aplinkos vertinimo, informacinių ir psichologinių operacijų srityse DI yra tiek grėsmė (*išmaniojo vaizdo klastojimas, angl. Deepfake*, koordinuota manipuliacija, automatizuoti naratyvų tinklai), tiek būtinas gynybinis įrankis, leidžiantis automatizuoti stebėjimo procesus, atlikti naratyvų ir auditorijų analizę bei remti sprendimų priėmimą.

Siekiant užtikrinti veiksmingą atsaką, LK SKD būtina sistemingai integruoti DI į informacinės aplinkos stebėseną ir analizę, sukurti aiškias DI naudojimo taisykles ir etikos standartus, stiprinti personalo kompetencijas (ypač medijų ir kognityvinio raštingumo, DI ir duomenų analizės srityse) bei dar labiau sutvirtinti sąveiką su NATO ir nacionaliniais partneriais. Iki 2030 m. DI integracija turi tapti viena iš prioritetinių LK SKD pajėgumų vystymo krypčių, nes be DI paremto situacijos suvokimo ir reagavimo gynyba informacinėje erdvėje taps struktūriškai neadekvati grėsmių mastui ir tempui.

Rezonansiniai 2025 m. įvykiai

Melaginga informacija apie užminuotą pasienį

- 2025 m. kovo 24 d. socialinio tinklo „Telegram“ kanale „Zhivet zhe Belarus“ pasirodė klaidinanti informacija, neva, Norviškių kaime, esančiame Lietuvos ir Baltarusijos pasienyje, išėjęs pasivaikščioti asmuo žuvo nuo detonavusios minos. Pranešime sukurtas emocinis fonas, kad Lietuvos miškai virsta mirties spąstais.
- Tą pačią dieną viename didžiausių Baltarusijos portalų „Belarus Segodnia“ pasirodė straipsnis, diskreditavęs Baltijos šalių ir Lenkijos sprendimą pasitraukti iš Otavos konvencijos teigiant, kad šis sprendimas kelia grėsmę ne tik kariams, bet ir civiliams bei laukiniams gyvūnams. Pakartotas pasakojimas apie pirmąją auką, žuvusią dėl šio Lietuvos sprendimo. Teigta, kad apie šį incidentą neinformavo ne tik Lietuvos, bet ir oficialios Europos institucijos.
- Kovo 25 d. Lietuvos žiniasklaidą pasiekė sufabrikuotas laiškas, kuriame „susirūpinusi pilietė“ prašė pagalbos dėl neva Lietuvos ir Baltarusijos pasienyje žuvusio savo vyro. Laiške rašoma, kad po tariamo nelaimingo atsitikimo buvo kreiptasi į Lietuvos policijos pareigūnus, tačiau žuvusio asmens šeimai buvo pagrasinta tylėti. Kaip ir incidentuose, pasirodžiusiuose Baltarusijos informacinėje erdvėje, taip ir minėtame laiške akcentuojama, kad Lietuvos valdžia neva nėra suinteresuota savo piliečių saugumu.



2 pav.

Šaltinis: Telegram

Vertinimas

- Šie atskiri incidentai yra vieningos informacinės kampanijos dalis, skirta tiek Baltarusijos, tiek Lietuvos auditorijoms paveikti.
- Baltarusijos auditorijai skirtos žinutės atkartojo įtvirtintus naratyvus apie tariamą Lietuvos ir kitų kaimyninių valstybių agresyvumą Rusijos ir Baltarusijos atžvilgiu, taip pat menkino NATO rytinio flango gynybinius įtvirtinimus.
- Sufabrikuotu laišku, tikėtina, buvo bandoma patikrinti Lietuvos žiniasklaidos atsparumą informacinėms atakoms ir paskleisti naratyvą Lietuvos informacinėje erdvėje, taip sukeliant Lietuvos visuomenės nepasitenkinimą. Tikėtina, kad priešiški veikėjai siekė pasinaudoti Lietuvos žiniasklaidos aplaidumu, tikėdamiesi, kad klaidinanti informacija bus išplatinta Lietuvos vidaus auditorijai. Tačiau portalo redakcija, gautame laiške atpažinusi įtarimą keliančius požymius, kreipėsi į atsakingas Lietuvos institucijas dėl situacijos patikslinimo.

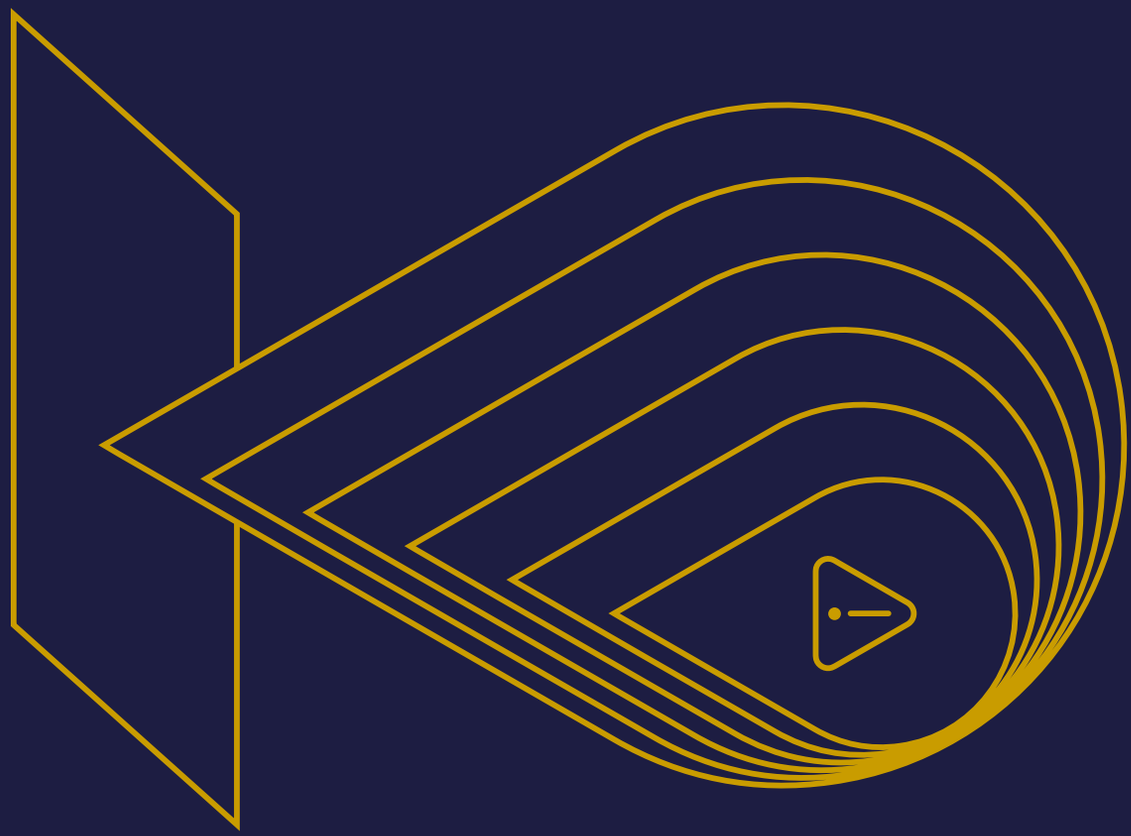
LK SKD žvilgsnis į 2026 m.

Tikėtina, kad artimiausiu metu Rusijos ir Baltarusijos priešiška veikla informacinėje erdvėje išliks aktyvi, bus siekiama paveikti Lietuvai ir jos sąjungininkams svarbias sritis – gynybą, užsienio politiką ir konstitucinius pagrindus. Numatoma, kad 2026 m. ir toliau stebėsime agresyvią retoriką NATO atžvilgiu, Rusija toliau sieks bauginti Vakarų auditorijas karo grėsme, bandys neigiamai paveikti Vakarų paramą Ukrainai ir NATO vienybę. Tikėtina, kad Baltarusijos spaudimas prieš Lietuvą informacinėje, diplomatinėje ir net fizinėje erdvėje išliks labai intensyvus.

Siekiant užkardyti informacines grėsmes būtinas glaudus tarpinstitucinis bendradarbiavimas, užtikrinantis greitą informacinių incidentų atpažinimą ir sklandesnį sprendimų priėmimą. LK SKD siekia prisidėti prie visuomenės atsparumo informacinėms grėsmėms stiprinimo, todėl 2026 m. toliau vykdys šviečiamąsias veiklas, dalinsis įžvalgomis su žiniasklaida ir visuomene.

04

Priedas „Grėsmių žemėlapis“



Turinys

Įvadas

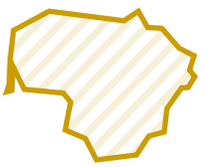
Nacionalinės kibernetinio saugumo būklės ataskaitos 2025 priedas „Grėsmių žemėlapis“ – tai NKSC koordinuotas kibernetinių grėsmių situacijos Lietuvoje vertinimas, parengtas bendradarbiaujant su Valstybės saugumo departamentu ir Antruoju operatyvinių tarnybų departamentu prie Krašto apsaugos ministerijos. Vertinime analizuojami registruotų incidentų, sistemų pažeidžiamumų bei duomenų nutekėjimų duomenys, taip pat nagrinėjamas platesnis kibernetinių grėsmių kontekstas – užsienio veikėjų aktyvumas.

Šiame priede pateikiami duomenys skiriasi nuo Nacionalinės kibernetinio saugumo būklės ataskaitoje 2025 nurodytų statistinių duomenų, nes duomenų imtis siauresnė – analizuojami tik ypatingos svarbos ir kiti itin svarbūs sektoriai[01], taip pat atsižvelgiama į skirtingus duomenų kriterijus.

Dokumentas skirtas sprendimų priėmėjams ir kibernetinio saugumo specialistams, siekiant pateikti koncentruotą grėsmių vertinimą bei išryškinti aktualiausias tendencijas ir galimas rizikas nacionaliniam saugumui.

01
Ypatingos svarbos ir kiti itin svarbūs sektoriai – sektoriai, nurodyti Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymo 1 ir 2 prieduose.

Santrauka



Bendras kibernetinių grėsmių lygio įvertinimas – Geltonas

Vertinimas atliktas išanalizavus kibernetinę veiklą viešojoje erdvėje, t. y. įvertinus kibernetinių incidentų reikšmingumą, pažeidžiamumų mastą ir nutekintų duomenų kiekį.

Spalvų reikšmės

Žalia – žemas grėsmės lygis, kibernetinė erdvė stabili, reikšmingų incidentų, pažeidžiamumų ar duomenų nutekėjimų mastas nedidelis.

Geltona – vidutinis grėsmės lygis, fiksuojamas padidėjęs kibernetinis aktyvumas, nustatomi pavieniai reikšmingesni incidentai, pažeidžiamumai ar duomenų nutekėjimai.

Oranžinė – aukštesnis nei vidutinis grėsmės lygis, fiksuojamas dažnesnis ar didesnio masto poveikis, didėja pažeidžiamumų, incidentų ar nutekėjimų apimtys, galimi koordinuotos veiklos požymiai.

Raudona – aukštas grėsmės lygis, nustatomas reikšmingas poveikis informacinių sistemų saugumui, paslaugų veikimui ar duomenų saugumui.

2025 m. kibernetinių grėsmių situacija Lietuvos kibernetinėje erdvėje išliko įtempta. Pagrindiniai taikiniai buvo skaitmeninės infrastruktūros bei viešojo administravimo sektoriai. Nors bendras incidentų skaičius nebuvo didelis, fiksuoti atvejai rodo nuoseklų piktavalių aktyvumą – paslaugų trikdymą ir informacijos rinkimą.

Per 2025 m. Lietuvos ypatingos svarbos ir kituose itin svarbiuose sektoriuose užfiksuoti 73 kibernetiniai incidentai, iš kurių 13 – dideli (18 proc.). Viešojoje erdvėje identifikuota daugiau kaip 300 pranešimų apie tariamas ar realias kibernetines atakas prieš Lietuvos subjektus, daugiausia viešojo administravimo ir transporto sektoriuose.

Iš 153 vertintų informacinių sistemų 98 nustatytos kaip pažeidžiamos. Taip pat išlieka tiekimo grandinių ir technologinės priklausomybės rizika.

2025 m. aptikta daugiau kaip 106 tūkst. nutekintų duomenų įrašų. Didžiausi kiekiai fiksuoti birželio, rugsėjo ir lapkričio mėnesiais, tačiau pažymėtina, kad aptikimo momentas ne visada sutampa su faktiniu duomenų praradimo laiku.

Apibendrinimas:

73
kibernetiniai incidentai, iš jų 13 – dideli.

>270
viešų pranešimų apie atakas prieš Lietuvos subjektus.

98
pažeidžiamos informacinės sistemos iš 153 vertintų.

>106 tūkst.
aptiktų nutekintų duomenų įrašų.

Spalvų reikšmės pagal temas

Incidentai. Fiksuotas nuoseklus piktavalių aktyvumas – informacijos rinkimas ir paslaugų trikdymas. Nors bendras incidentų skaičius nėra didelis, dalis atvejų buvo itin reikšmingi.

Tinklų ir informacinės sistemos spragos. Aptikti pažeidžiamumai daugiausia susiję su pasenusiais komponentais ir netinkama konfigūracija. Bendras rizikos lygis išlieka žemas.

Duomenų nutekinimas. Didelis nutekintų duomenų įrašų mastas su ribotais nustatyto poveikio požymiais valstybės informacinių sistemų saugumui.

Informacinis fonas. Vidutinis aktyvumo lygis, fiksuoti užsienio grupuočių vieši pareiškimai ir informacinio poveikio požymiai.

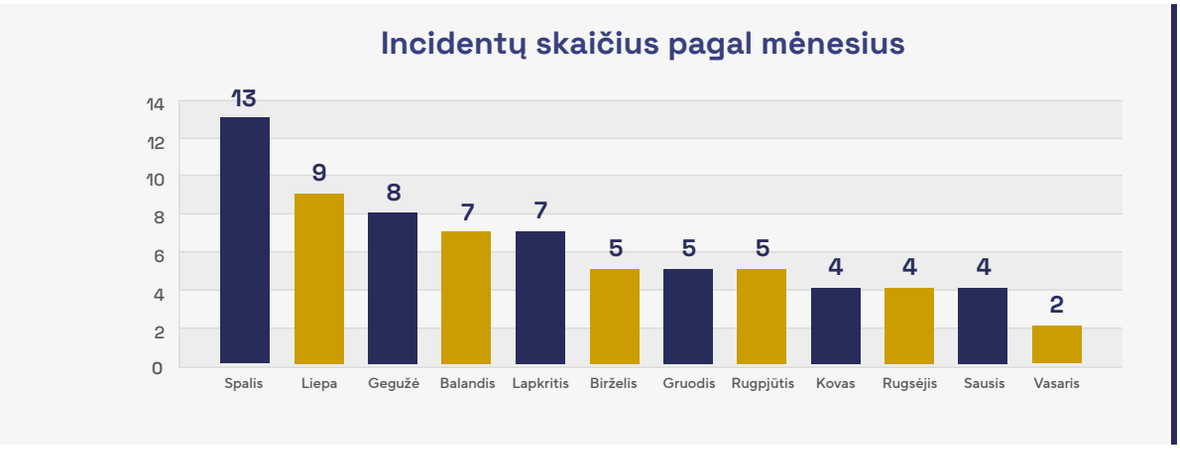
Kibernetinio saugumo situacija ypatingos svarbos ir kituose itin svarbiuose sektoriuose

Šiame skyriuje analizuojama informacija apie ypatingos svarbos ir kituose itin svarbiuose sektoriuose registruotus kibernetinius incidentus, nustatytas tinklų ir informacinių sistemų spragas bei duomenų nutekėjimą. Pateikiami duomenys vertinami siekiant nustatyti pagrindines kibernetinių grėsmių tendencijas, jų pasiskirstymą bei galimą poveikį kritinių paslaugų veikimui.

Incidentai

2025 metais Lietuvos ypatingos svarbos ir kituose itin svarbiuose sektoriuose registruotų kibernetinių incidentų pasiskirstymas buvo netolygus tiek laiko, tiek sektorių pjūviu, tačiau neišryškėjo vienas nuolat dominuojantis laikotarpis ar vienas kritinis sektorius. Fiksuota nuosekli incidentų dinamika su pavieniais aktyvumo šuoliais bei didesnis incidentų skaičius tam tikrose srityse.

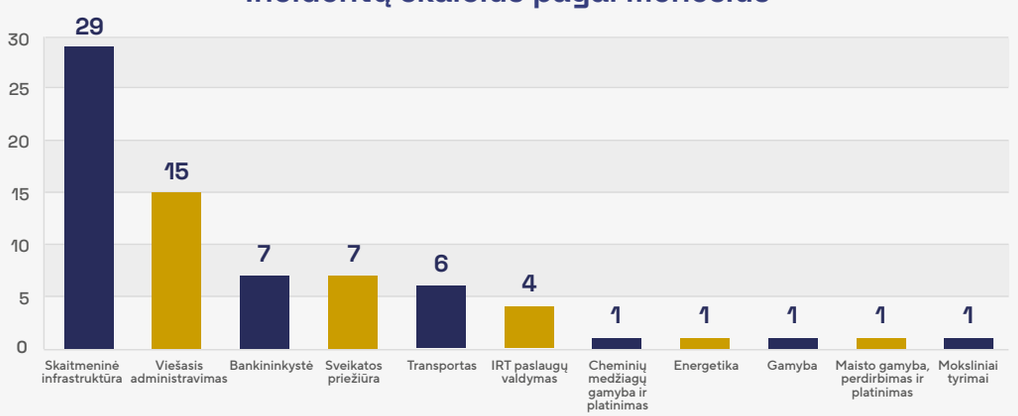
Daugiausia incidentų fiksuota spalį (13), jis aktyviausias mėnuo nagrinėjamu laikotarpiu (**1 pav.**). Piktavalių aktyvumas buvo padidėjęs liepos (9) ir gegužės (8) mėnesiais, fiksuotas epizodinis incidentų padaugėjimas. Balandžio ir lapkričio mėnesiais registruota po 7 incidentus; birželio, rugpjūčio ir gruodžio mėnesiais – po 5. Mažiausiai incidentų nustatyta vasario mėnesį (2); kovo, rugsėjo ir sausio mėnesiais – po 4 incidentus. Tokia dinamika rodo kibernetinių grėsmių nuoseklumą, tačiau ji nėra sezoniškai nuspėjama, aktyvumo padidėjimas labiau susijęs su trumpalaikėmis kampanijomis ar tikslinėmis operacijomis.



< 1 pav.

Incidentų skaičius pagal mėnesius
(šaltinis – NKSC)

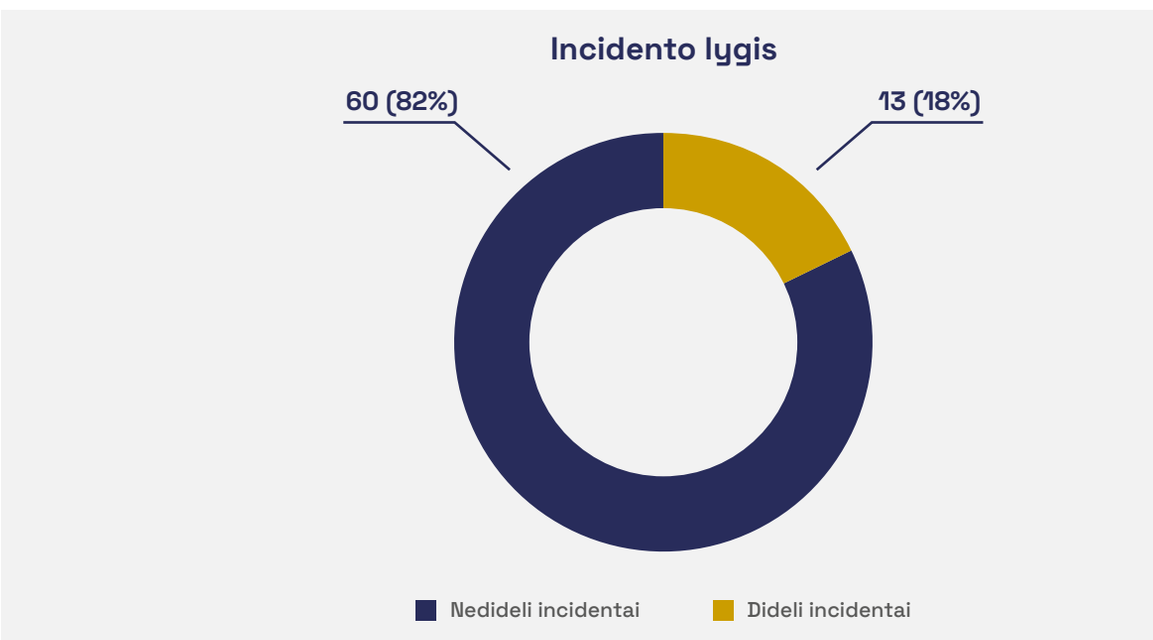
Vertinant incidentų pasiskirstymą sektoriuose (**2 pav.**), matyti ryški koncentracija srityse, susijusiose su didžiausia skaitmenine integracija ir svarbių paslaugų prieinamumu. Didžiausias incidentų skaičius fiksuotas skaitmeninės infrastruktūros sektoriuje (29), jis ženkliai lenkia kitus sektorius ir išlieka pagrindiniu kibernetinių incidentų taikiniu. Tai siejama su plačiai naudojamomis, viešai prieinamomis ir tarpusavyje glaudžiai susietomis informacinėmis sistemomis. Antras pagal incidentų skaičių buvo viešojo administravimo sektorius (15), kuriame incidentai atspindi šio sektoriaus svarbą valstybės veiklos tęstinumui ir visuomenės pasitikėjimui. Bankininkystės (7), sveikatos priežiūros (7) ir transporto (6) sektoriuose fiksuotas vidutinis incidentų skaičius, rodantis nuolatinį, tačiau ne itin intensyvų piktavalių aktyvumą.



< 2 pav.

Incidentų skaičius pagal sektorius
(šaltinis – NKSC)

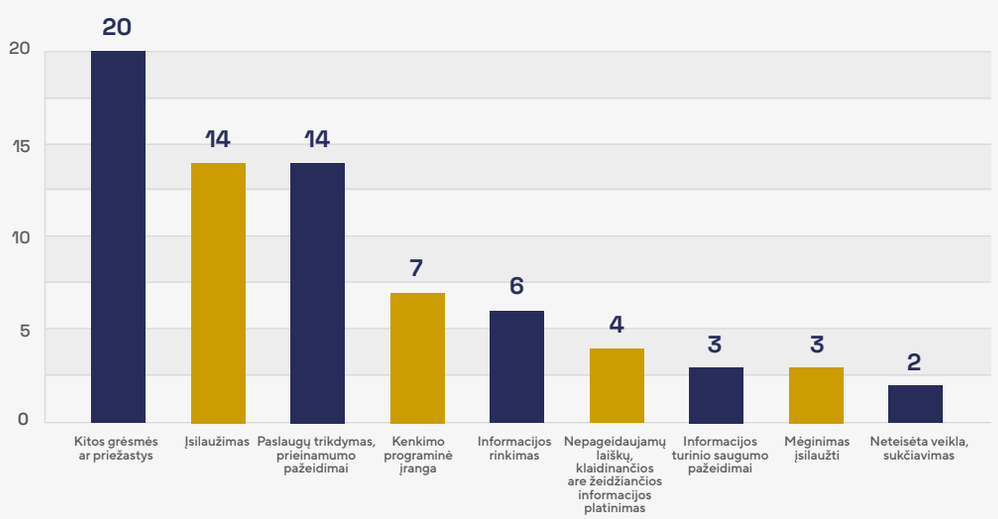
Daugiausia registruotų įvykusių incidentų (**3 pav.**) buvo nedideli – iš viso 60 atvejų (82 % visų incidentų), dažniausiai lokalūs, trumpalaikiai ir neturėję ilgalaikio poveikio informacinių sistemų veikimui ar paslaugų teikimo tęstinumui. Užfiksuota 13 didelių incidentų (18 %).



< 3 pav.

Incidento lygis
(šaltinis – NKSC)

Incidentų pasiskirstymas pagal kategorijas (**4 pav.**) rodo, kad kibernetinių grėsmių pobūdis išlieka įvairus ir fragmentiškas. Daugiausia incidentų priskirta kategorijai „Kitos grėsmės ar priežastys“ (20), apimančiai nestandartinius ar kombinuotus atvejus, kurie neatitiko apibrėžtų kategorijų. Reikšmingą dalį sudarė įsilaužimo (angl. *Intrusion*) atvejai (14) bei paslaugų trikdymo ir DDoS atakos (14) – siekta tiek neteisėtos prieigos, tiek sutrikdyti paslaugų veikimą. Mažiau incidentų buvo susiję su kenkimo programine įranga (angl. *Malware*) (7), informacijos rinkimu (angl. *Information Gathering*) (6) ir kitomis veikomis, įskaitant dezinformacijos sklaidą ar duomenų viliojimą (angl. *Phishing*).



< 4 pav.

Incidentų pasiskirstymas pagal kategorijas
(šaltinis – NKSC)

Apibendrinant galima teigti, kad ypatingos svarbos ir kituose itin svarbiuose sektoriuose kibernetinių grėsmių pasireiškimas išlieka nuoseklus, dinamiškas ir lankstus. Incidentų struktūra rodo ne tik nuolatinį piktavalių aktyvumą, bet ir didėjantį grėsmių kompleksiškumą, kai taikomi įvairūs metodai ir taktikos, siekiant išnaudoti sistemų ir procesų trūkumus.

Vertinant 2025 m. fiksuotus incidentus platesniame nacionalinio saugumo kontekste, pažymėtina, kad kibernetinė erdvė išlieka dinamiška ir nuosekliai besivystanti.

Priešiškų valstybių piktavaliai toliau tęsia veiklą, siekdami savosios valdžios atstovų numatytų strateginių tikslų. Svarbių Lietuvos organizacijų informacinėms sistemoms didžiausią grėsmę kelia priešiškų valstybių kibernetinio šnipinėjimo grupuotės. Turėdamos didelius finansinius išteklius, kompetencijų ir motyvaciją veikti prieš Lietuvos ir kitų NATO valstybių organizacijas, šnipinėjimo grupuotės siekia įgyvendinti sudėtingas, sunkiai atskleidžiamas operacijas, skirtas jautriai informacijai perimti, dezinformacijai skleisti.

Tarptautiniai incidentai pateikiami kaip pavyzdžiai, leidžiantys įvertinti galimą kibernetinių grėsmių poveikį Lietuvos kontekste.

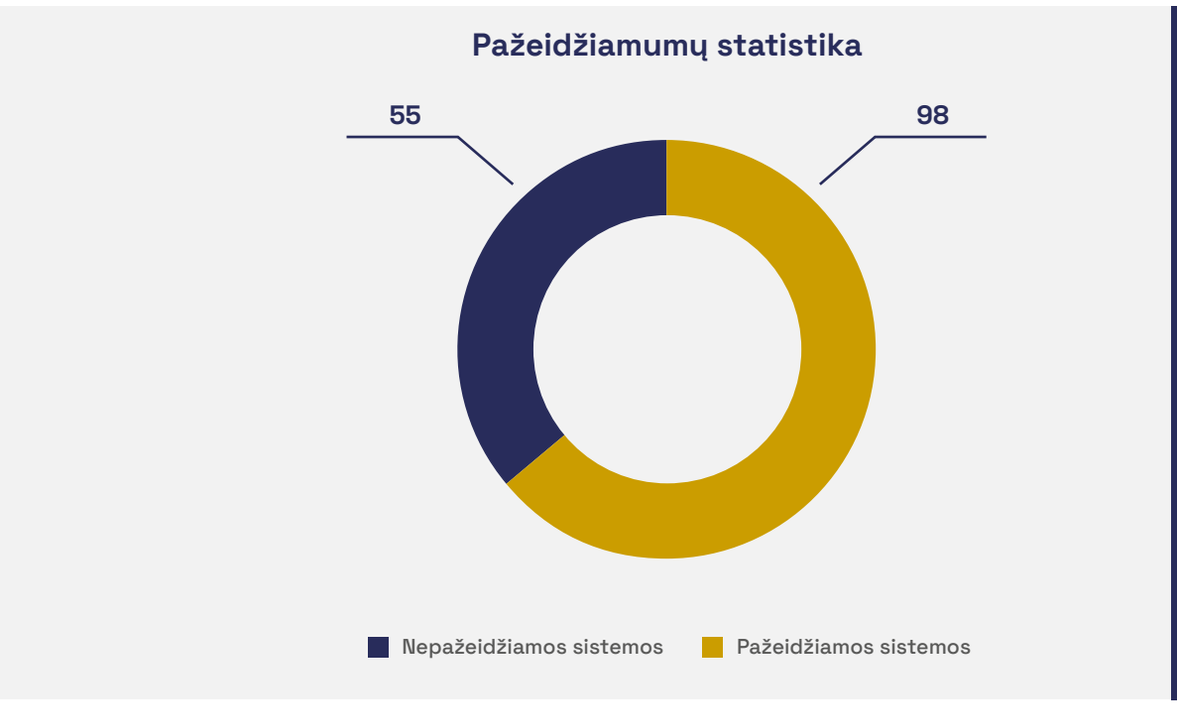
Sausį įvykdyta ataka prieš Slovakijos geodezijos, kartografijos ir kadastrų registrus sutrikdė nuo šių duomenų priklausančių valstybės ir privačių organizacijų veiklą.

Rugsėjį ataka prieš „Collins Aerospace“ MUSE sistemą sukėlė skrydžių trikdžius Londono (Heathrow), Briuselio, Berlyno ir Dublino oro uostuose.

Gruodį Lenkijoje buvo užkardyta koordinuota ataka prieš energetikos infrastruktūrą. Jei ataka būtų buvusi sėkminga, be šildymo būtų likę apie pusė milijono gyventojų.

Tinklų ir informacinės sistemos spragos

2025 m. ypatingos svarbos ir kituose itin svarbiuose sektoriuose išbandytos 153 sistemos (**5 pav.**), iš kurių 98 nustatytos kaip pažeidžiamos, o 55 – kaip nepažeidžiamos. Šie duomenys atspindi tikslinės ir nuoseklios stebėsenos rezultatus, todėl turėtų būti vertinami kaip realiai nustatytų atvejų visuma, o ne bendras visų sektorių pažeidžiamumo (angl. *Vulnerability*) lygis. Pateikiama statistika apima žiniatinklio taikomąsias programas (angl. *Web Applications*). Jose nustatyta daugiausia spragų.

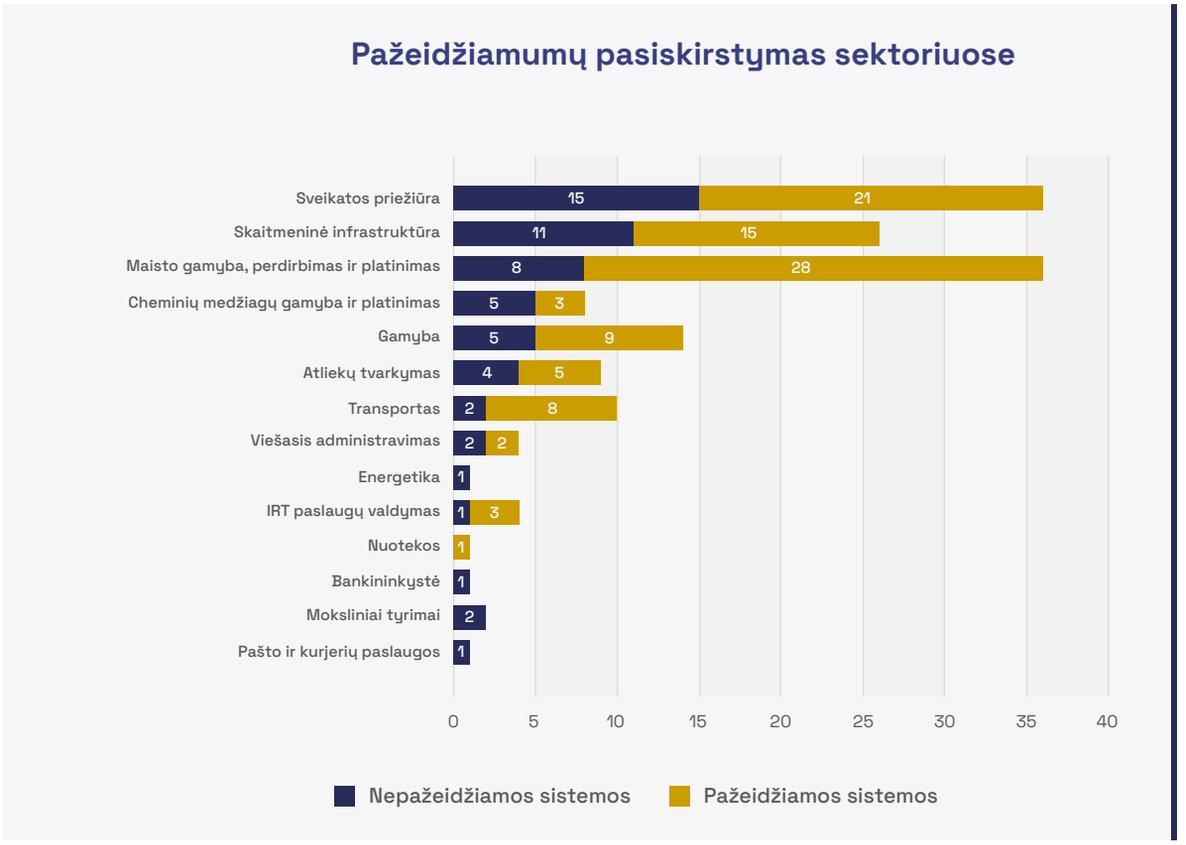


< 5 pav.

Pažeidžiamumų statistika
(šaltinis – NKSC)

Pažeidžiamumų pasiskirstymas sektoriuose (**6 pav.**) rodo skirtingą saugos vertinimų aktyvumą ir sistemų brandos lygį. Daugiausia pažeidžiamų sistemų nustatyta sveikatos priežiūros (21 pažeidžiama, 15 nepažeidžiamų) bei maisto gamybos, perdirbimo ir platinimo sektoriuose (28 pažeidžiamos, 8 nepažeidžiamos). Čia fiksuotas didesnis saugumo spragų paplitimas. Tai gali būti siejama su nevienodu saugumo priemonių taikymu, pasenusių technologijų naudojimu ar nepakankamu atnaujinimų valdymu.

Svarbu pabrėžti, kad ši statistika neatspindi visų galimų internetinių ar sektorių pažeidžiamumų. Duomenys yra vertintų sistemų tikslinės, nuoseklios stebėsenos ir analitinio darbo rezultatas.



< 6 pav.

Pažeidžiamumų pasiskirstymas sektoriuose *(šaltinis – NKSC)*

Lietuvos kibernetinėje erdvėje fiksuojama kryptinga ir tęstinė pažeidžiamumų paieška, būdinga pažangioms ir ilgalaikėms kibernetinėms operacijoms. Priešiškų valstybių remiami piktavaliai reguliariai analizuoja valstybės institucijų ir kritinės infrastruktūros sistemas, siekdami identifikuoti technines spragas.

Pažeidžiamumų išnaudojimas dažnai yra pirmasis etapas sudėtingesnėje atakos grandinėje, kurios tikslas – užsitikrinti ilgalaikę nesankcionuotą prieigą ir rinkti žvalgybinę informaciją.

Ilgalaikėje perspektyvoje tikėtina technologinė pažanga, įskaitant dirbtinio intelekto panaudojimą pažeidžiamumams identifikuoti ir išnaudoti.

Pažeidžiamumų išnaudojimo rizika taip pat vertintina tiekimo grandinių (angl. *Supply Chain*) ir technologinės priklausomybės kontekste.

Beveik neabejotina, kad daugumai vieno sektoriaus organizacijų pasirinkus to paties tiekėjo paslaugas ar produktus, išauga sėkmingo įsilaužimo ir didelio masto kibernetinių atakų tikimybė. Tiekimo grandinių panaudojimas sukuria naujas puolimo kryptis ir padidina puolimo galimybes. Per mažai kibernetiniu saugumu besirūpinančios organizacijos gali įgalinti įsilaužėlius pasiekti ir kitas grandinėje esančias atsparesnes organizacijas.

Pavyzdžiui, 2025 m. spalį „Amazon Web Services“ debesijos paslaugų (angl. *Cloud Services*) nutrūkimas įvyko ne dėl kibernetinės atakos, tačiau pademonstravo, kaip sėkminga kibernetinė ataka prieš vieną tiekėją galėtų paveikti tarptautines tiekimo grandines.

2025 m. kibernetinėje erdvėje fiksuota reikšminga DI technologijų integracija į atakų planavimo ir vykdymo procesus. DI naudojimas leidžia piktavaliams didinti operacijų mastą, greitį ir prisitaikymą, kartu mažinant žmogiškųjų išteklių poreikį. Skirtingai nei ankstesniais metais, DI vis dažniau integruojamas ne tik kaip pagalbinė priemonė, bet ir kaip sudėtinė kenkimo operacijų dalis.

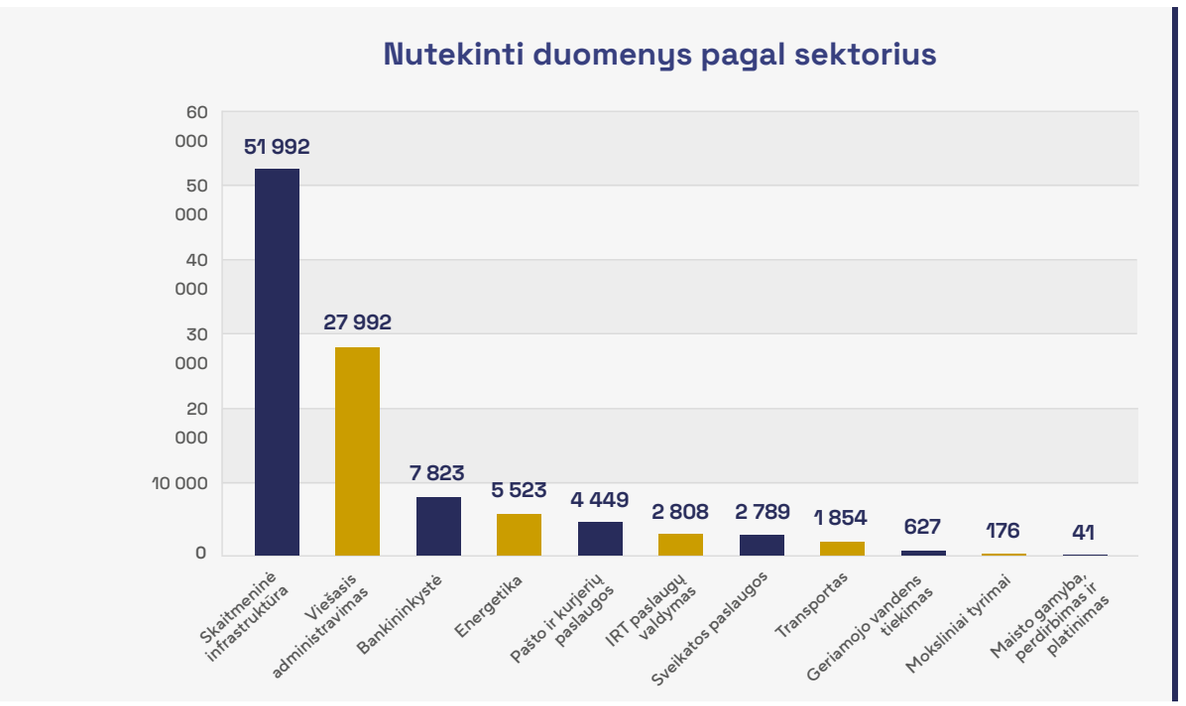
DI reikšmingai transformuoja skirtingus kibernetinių atakų etapus. Žvalgybos fazėje jis leidžia automatizuoti viešų duomenų rinkimą ir analizę, spartinti taikinių profiliavimą bei identifikuoti pažeidžiamumus. Kenkėjiško kodo kūrimo etape DI sudaro sąlygas generuoti nuolat kintantį, sunkiau aptinkamą kodą, pritaikytą konkrečioms sistemoms ar pažeidžiamumams.

Pristatymo etape DI naudojamas kuriant įtikinamas, taikiniui pritaikytas žinutes, didinant socialinės inžinerijos operacijų efektyvumą. Išmaniojo vaizdo klastojimo (angl. *Deepfake*) technologijos leidžia imituoti patikimus asmenis ar institucijas, taip dar labiau didinant apgaulės sėkmės tikimybę.

Tolimesniuose etapuose DI leidžia adaptuoti atakos parametrus realiuoju laiku, imituoti tikrus procesus ir taip išvengti aptikimo. Taip pat jis naudojamas užkrėstų sistemų valdymui, generuojant unikalius veiksmus kiekvieno vykdymo metu bei efektyviau identifikuojant vertingus duomenis, mažinant duomenų nutekinimo (angl. *Data Exfiltration*) kiekį ir aptikimo tikimybę.

Duomenų nutekinimas

2025 metais ypatingos svarbos ir kituose itin svarbiuose sektoriuose užfiksuota daugiau kaip 106 tūkst. nutekintų prisijungimo duomenų. Nutekėjimų pasiskirstymas buvo netolygus tiek laiko, tiek sektorių pjūviu. Didžiausi nutekėjimų kiekiai fiksuoti skaitmeninės infrastruktūros (51 992) ir viešojo administravimo (27 992) sektoriuose (**7 pav.**).



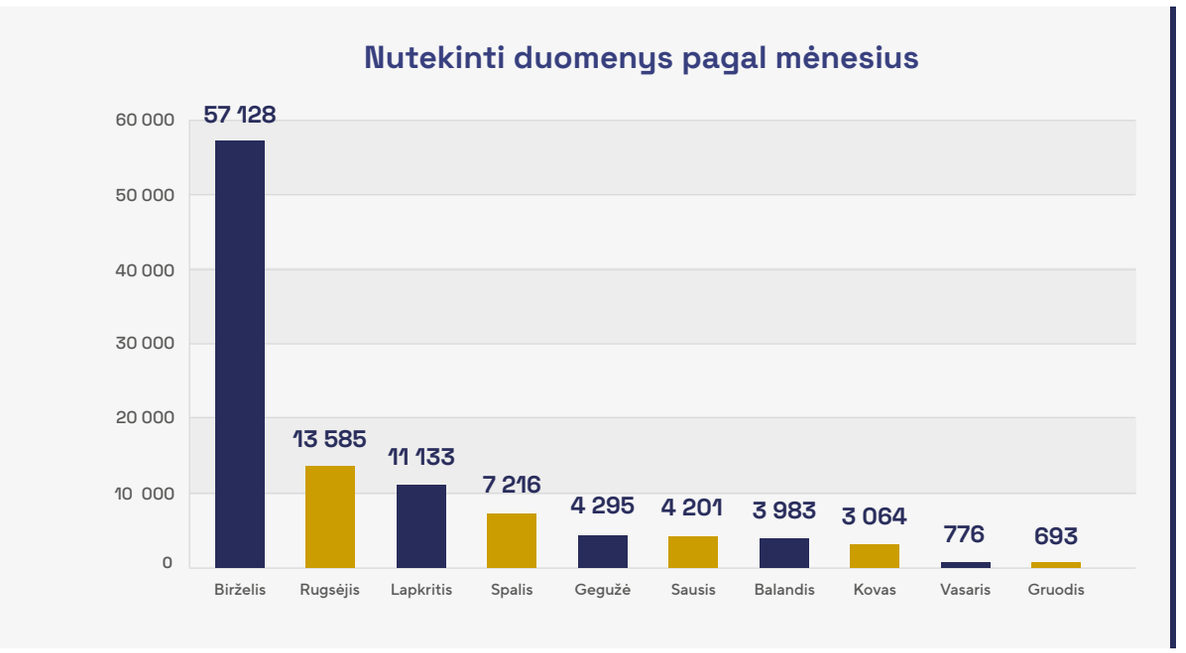
< 7 pav.

Nutekinti duomenys pagal sektorius *(šaltinis – NKSC)*

Nutekėjimų dinamikoje išsiskiria pavieniai aktyvumo šuoliai, ypač birželio (57 128), rugsėjo (13 585) ir lapkričio (11 133) mėnesiais (**8 pav.**).

Pažymėtina, kad naudojama nauja nutekintų duomenų fiksavimo paslauga vis dar yra vystymo stadijoje, todėl galimi duomenų svyravimai, susiję su naudojamų įrankių atnaujinimu ir naujų subjektų įtraukimu.

Taip pat atkreiptinas dėmesys, kad duomenų nutekėjimo atvejai dažniausiai yra fiksuojami ne jų įvykimo momentu, bet vėliau – kai duomenys tampa viešai prieinami, patenka į nutekintų duomenų rinkinius arba yra paviešinami trečiųjų šalių platformose. Dėl šios priežasties faktinis nutekėjimų laikas gali skirtis nuo jų nustatymo datos.



< 8 pav.

Nutekinti duomenys pagal mėnesius *(šaltinis – NKSC)*

Svarbu pabrėžti, kad ši statistika atspindi aptiktus nutekintus duomenis, o ne faktinį nutekėjimo momentą ar incidentų skaičių. Duomenų aptikimas dažnai vyksta retrospektyviai, todėl sektoriai su didesniu nutekintų duomenų kiekiu nebūtinai patyrė daugiau pažeidimų per ataskaitinius metus, tačiau juose identifikuota daugiau jau viešai prieinamų duomenų rinkinių.

Duomenų nutekėjimai šiame kontekste veikia kaip papildomas rizikos daugiklis. Nutekinta informacija gali būti naudojama taikinių profiliavimui, socialinės inžinerijos operacijoms ir tolimesnių kibernetinių veiksmų planavimui. Net ir pavieniai ar senesni duomenų rinkiniai išlieka vertingi, nes gali būti derinami su kitais šaltiniais, stiprinant operacinį tikslumą ir veiksmų efektyvumą.

Atkreiptinas dėmesys, kad kibernetiniai incidentai vis dažniau naudojami kaip informacinio poveikio priemonė. Vieši pranešimai apie atakas ir informacinės kampanijos veikia kartu, siekiant formuoti pažeidžiamumo ar nestabilumo įspūdį. Fiksuojamos koordinuotos komunikacijos tendencijos, kai kibernetiniai veiksmai derinami su naratyvų formavimu socialiniuose tinkluose ir kitose viešosios komunikacijos platformose.

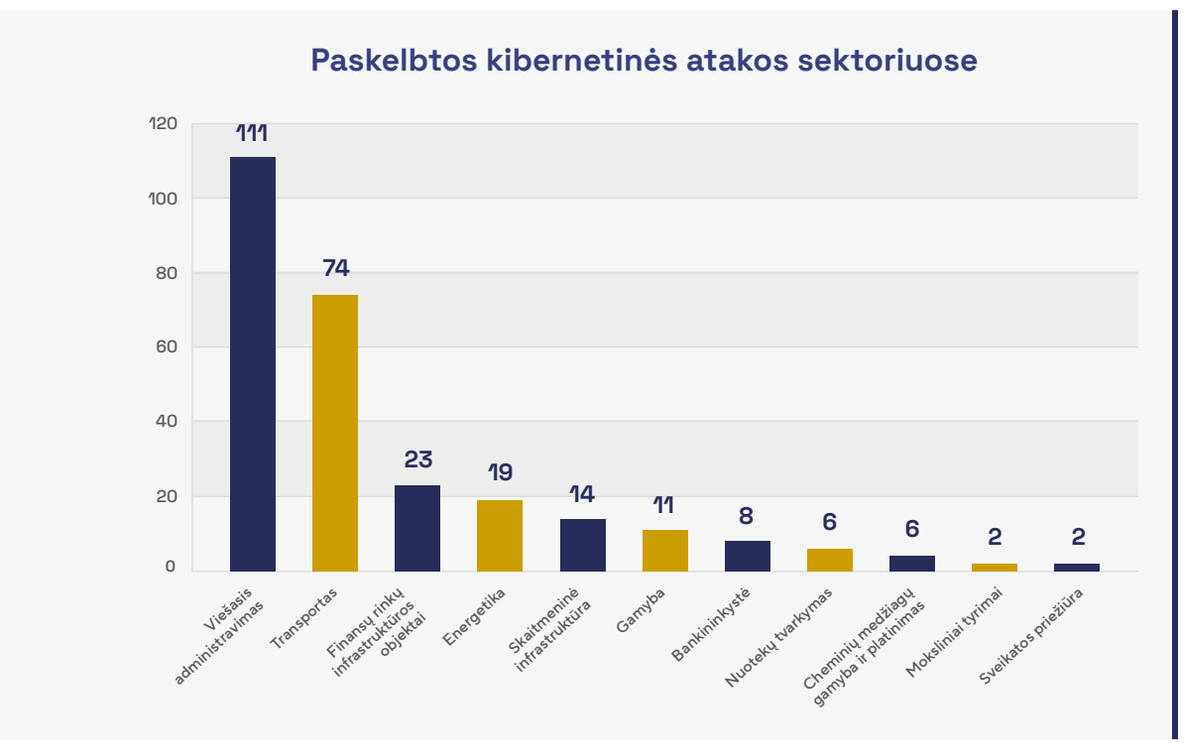
Nutekinti duomenys kelia ne tik finansinę ar reputacinę, bet ir strateginę žalą. Priešiškų valstybių piktavaliai gali naudoti nutekintą informaciją taikinių profiliavimui, socialinės inžinerijos operacijoms ar tolimesnių kibernetinių veiksmų planavimui. Informacija, gauta per duomenų nutekėjimus, gali būti integruojama į platesnes žvalgybines ar informacines kampanijas, sustiprinant jų poveikį.

4. Informacinis fonas

Šiame skyriuje analizuojama vieša informacija apie kibernetinę veiklą prieš Lietuvos subjektus. Ji ne visada atspindi faktiškai įvykusius incidentus, tačiau yra reikšminga vertinant grėsmių kontekstą ir informacinį poveikį.

Viešai paskelbti pranešimai apie kibernetines atakas prieš Lietuvos subjektus

2025 m. viešojoje erdvėje fiksuotas didelis pranešimų apie kibernetines atakas prieš Lietuvos subjektus skaičius. Daugiausia pranešimų buvo siejama su viešojo administravimo sektoriumi (111), turinčiu simbolinę reikšmę ir platų matomumą (**9 pav.**). Taip pat dažnai minėti transporto (74) ir finansų rinkų infrastruktūros (23) sektoriai, o likusi dalis pasiskirstė tarp energetikos, gamybos ir kitų sričių. Pažymėtina, kad tokie pranešimai ne visais atvejais atspindi realų poveikį informacinėms sistemoms ir dažnai naudojami kaip informacinio poveikio ar propagandos priemonė.

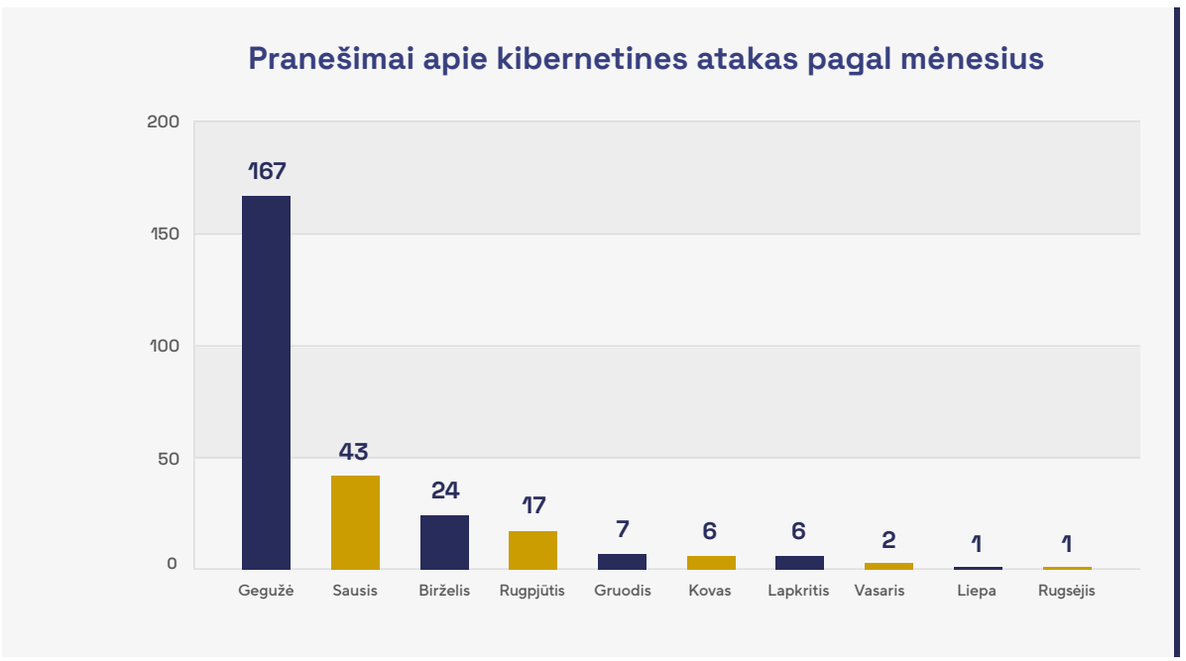


< 9 pav.

Paskelbtos kibernetinės atakos sektoriuose *(šaltinis – NKSC)*

Atakų dinamika ir kategorijos

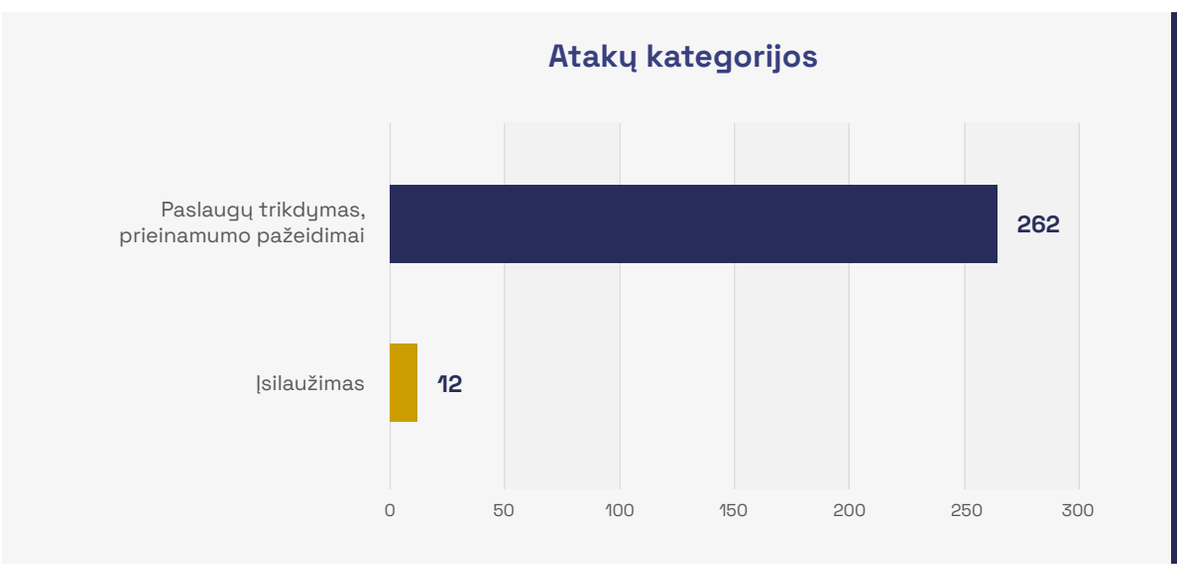
Viešų pranešimų apie atakas pasiskirstymas pagal mėnesius (**10 pav.**) buvo netolygus su ryškiais aktyvumo šuoliais, pikas pasiektas gegužę (167). Šie svyravimai labiau atspindi informacinės veiklos intensyvumą ir piktavalių komunikacinius sprendimus, o ne realų atakų lygį.



< 10 pav.

Pranešimai apie kibernetines atakas pagal mėnesius
(šaltinis – NKSC)

Dominuojanti atakų, apie kurias buvo pranešta, kategorija buvo paslaugų trikdymas (DDoS) (**11 pav.**), jis sudarė absoliučią daugumą atvejų (262). Pranešimų apie įsilaužimus fiksuota ženkliai mažiau (12), kas rodo, kad viešajame naratyve prioritetas teikiamas greitai suprantamiems ir didesnį emocinį poveikį turintiems trikdymo scenarijams.

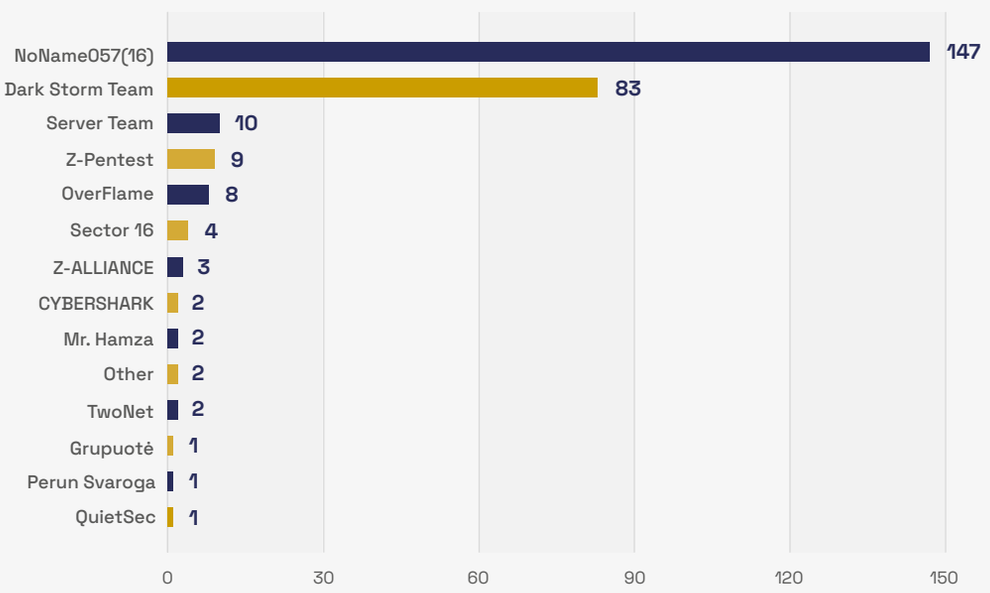


< 11 pav.

Atakų kategorijos
(šaltinis – NKSC)

Viešai atakas prieš Lietuvos subjektus deklaravusios grupuotės

2025 m. informaciniame fone dominavo ribotas skaičius grupuočių, kurios generavo didžiąją dalį pranešimų apie atakas prieš Lietuvos subjektus (**12 pav.**). *NoName057(16)* (147 pranešimai) ir *Dark Storm Team* (83) kartu formavo pagrindinį informacinį naratyvą.



< 12 pav.

Kibernetinių atakų grupuotės
(šaltinis – NKSC)

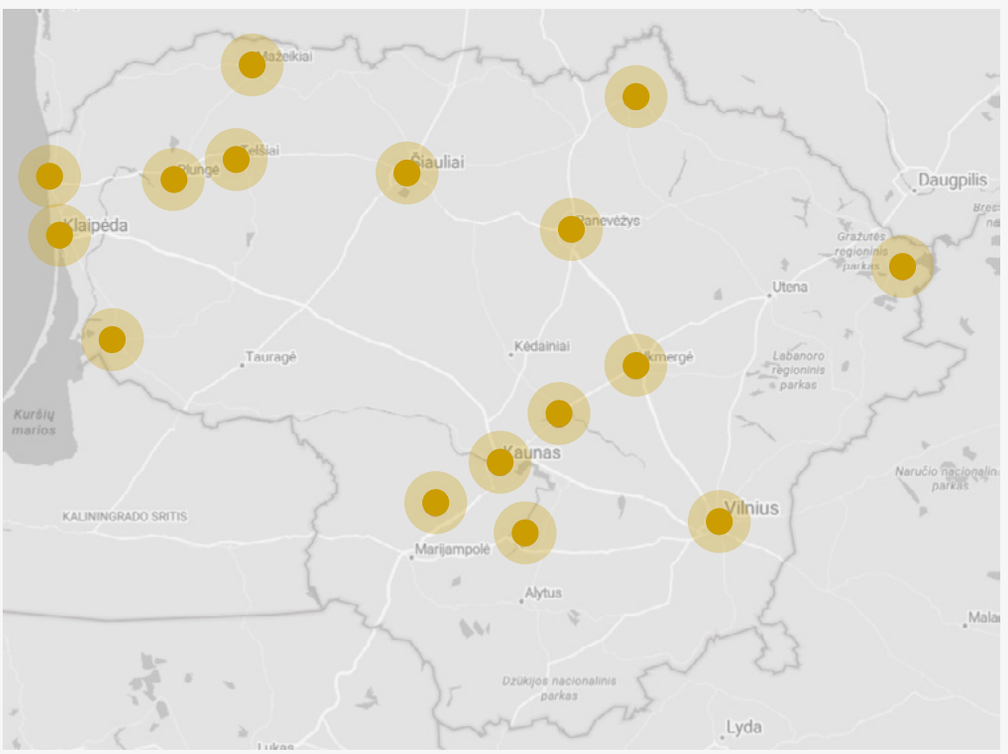
Toks pasiskirstymas rodo, kad viešai deklaruojama kibernetinė veikla yra kryptinga ir kartotinė, o ne spontaniška. Šių grupuočių aktyvumas vertintinas kaip platesnių regioninių informacinių kampanijų dalis, orientuota į geopolitiniu požiūriu jautrias valstybes, įskaitant Baltijos šalis.

Taikinių geografinis pasiskirstymas Lietuvoje

2025 m. viešų pranešimų apie kibernetines atakas analizė rodo aiškią taikinių koncentraciją didžiuosiuose Lietuvos miestuose (**13 pav.**). Didžiausias viešai minimų subjektų skaičius fiksuotas Vilniuje (204), pagrindiniame administraciniame, politiniame ir skaitmeninės infrastruktūros centre.

Toks pasiskirstymas rodo, kad informacinė veikla sąmoningai orientuojama į labiausiai atpažįstamas ir simboliškai reikšmingas vietoves, siekiant sustiprinti poveikį viešajai erdvei ir formuoti platesnio masto pažeidžiamumo įspūdį nacionaliniu lygmeniu.

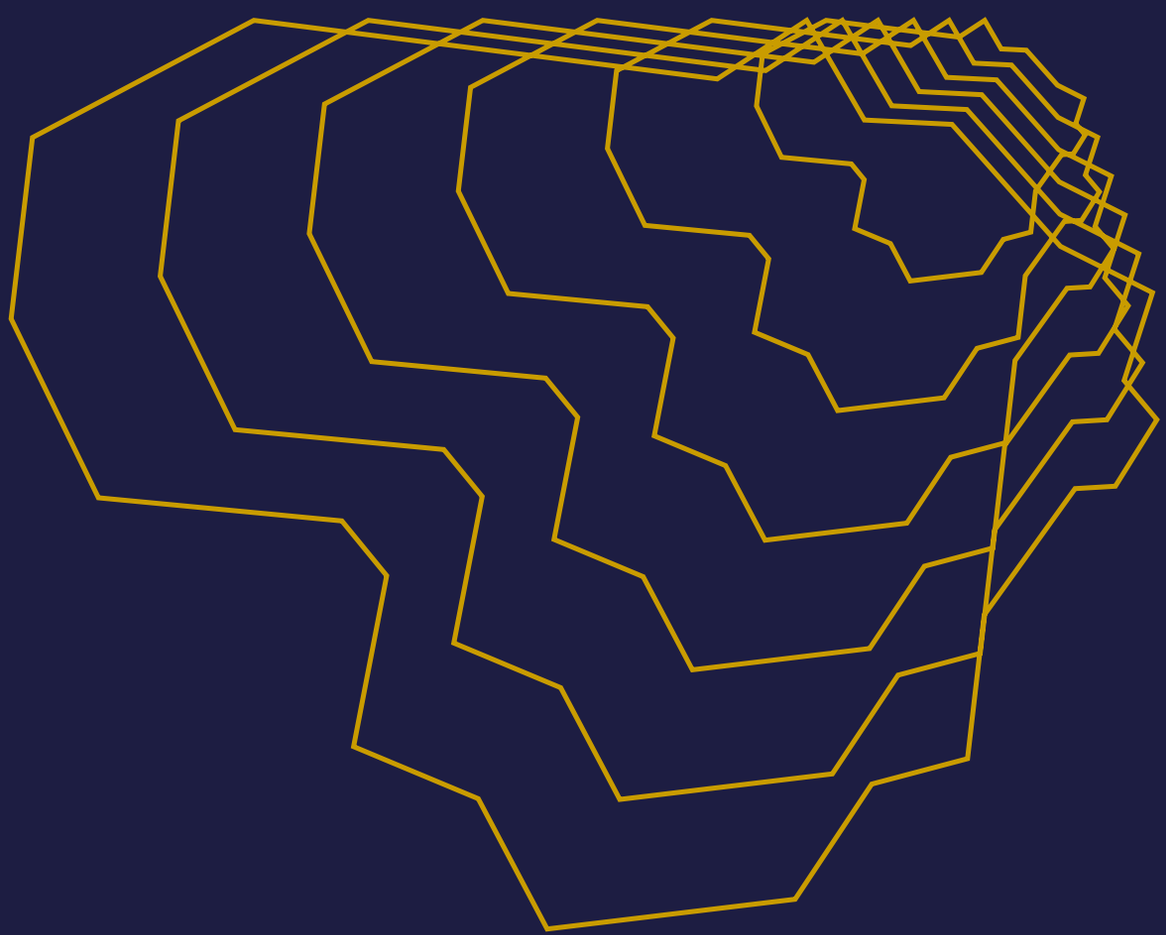
Atakuojamų organizacijų vietos Lietuvoje



< 13 pav.

Atakuojamų organizacijų vietos Lietuvoje
(šaltinis – NKSC)

Viešai deklaruojamos kibernetinės atakos dažnai vyksta kartu su informacinėmis kampanijomis, kurių tikslas kurti nestabilumo ir pažeidžiamumo įspūdį. Ryškios koordinuotos veiklos tendencijos, kai kibernetiniai veiksmai derinami su naratyvų sklaida socialiniuose tinkluose ir kitose viešosios komunikacijos platformose.



NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA

2025

Išleido Lietuvos Respublikos krašto apsaugos ministerija,
Totorių g. 25, LT-01121 Vilnius, www.kam.lt
2026-05-20. Užsakymas Nr. GL-402

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 2783-7017