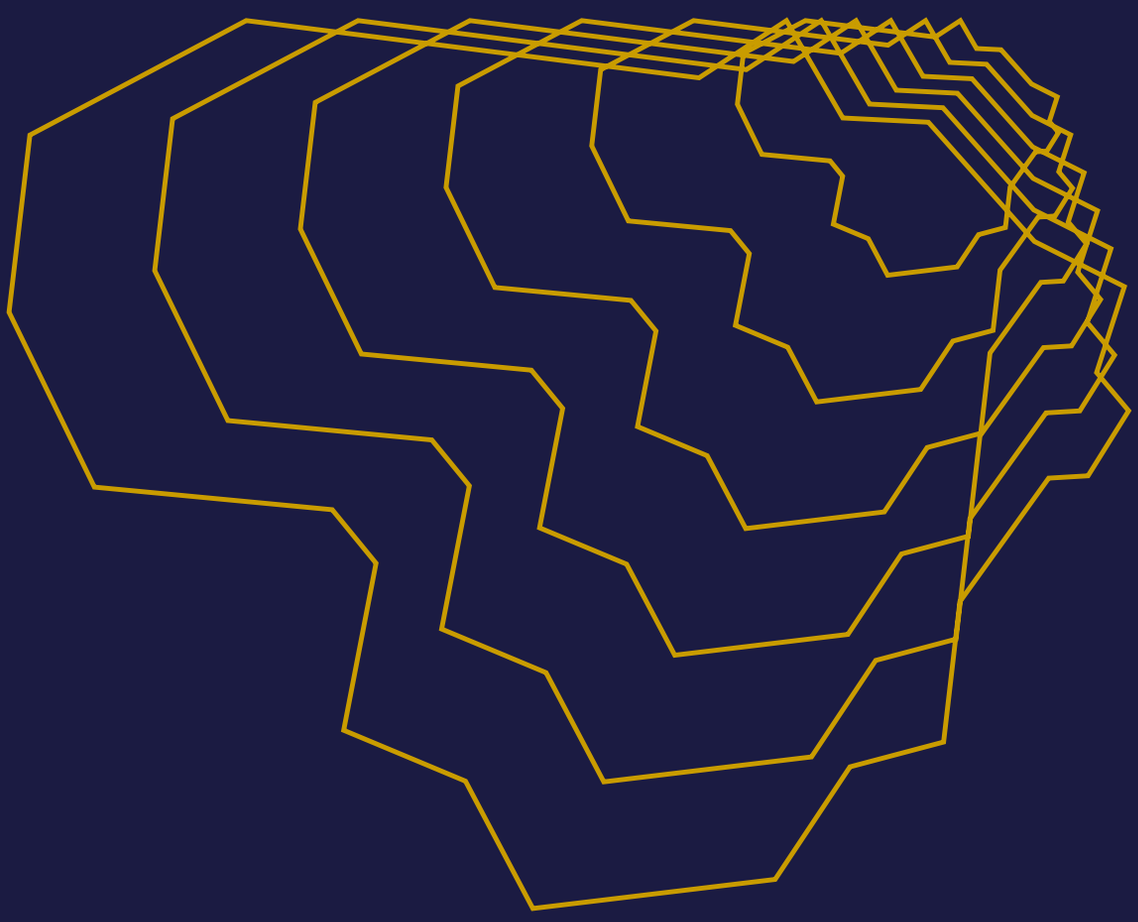
KRAŠTO APSAUGOS
MINISTERIJA

LIETUVOS KIBERNETINIO SAUGUMO BŪKLĖS APŽVALGA: SVARBIAUSIA INFORMACIJA



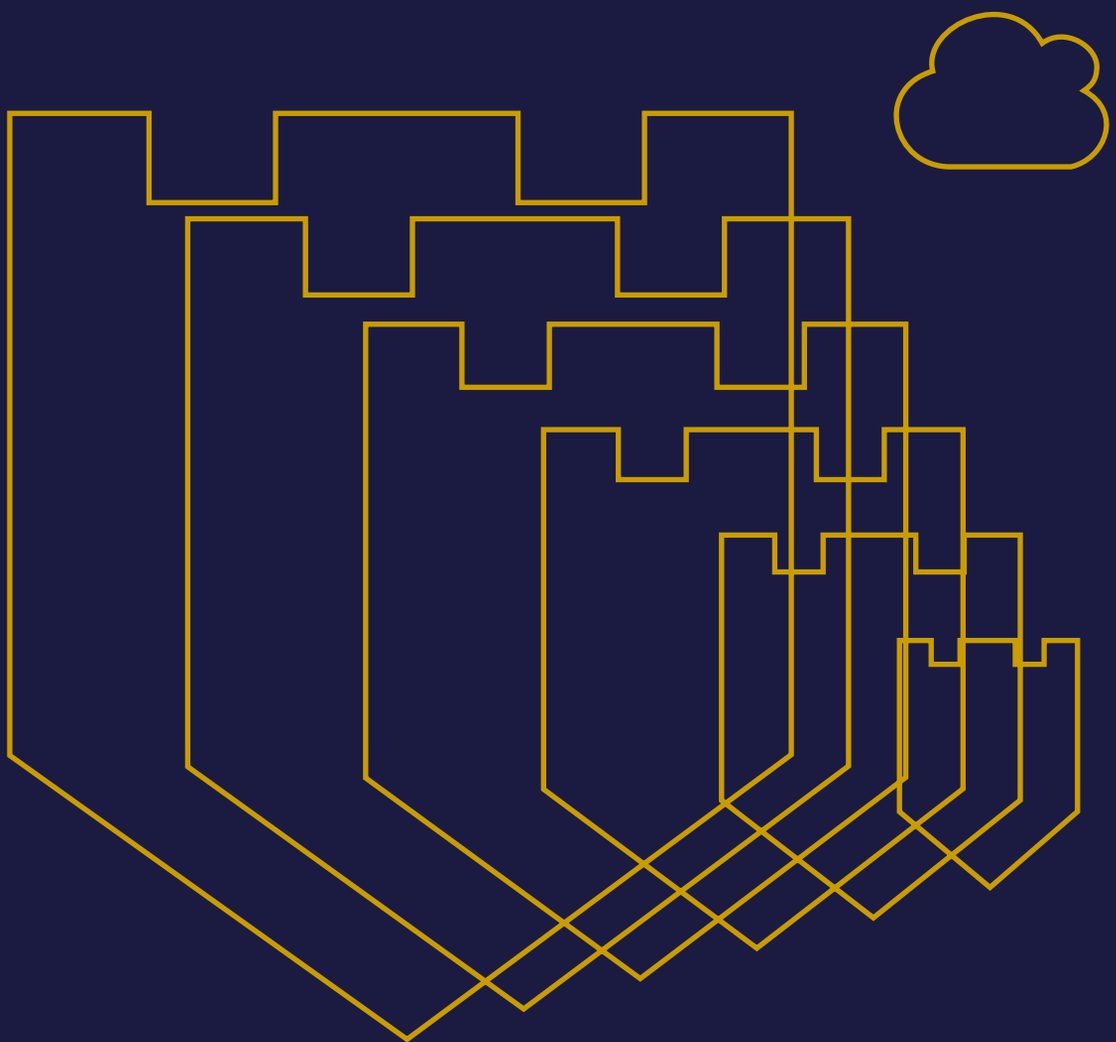
2025

LIETUVOS KIBERNETINIO SAUGUMO BŪKLĖS APŽVALGA: SVARBIAUSIA INFORMACIJA

2025

Vilnius

01



Įžanga

Įžanginis žodis

Robertas Kaunas,
Krašto apsaugos ministras

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.

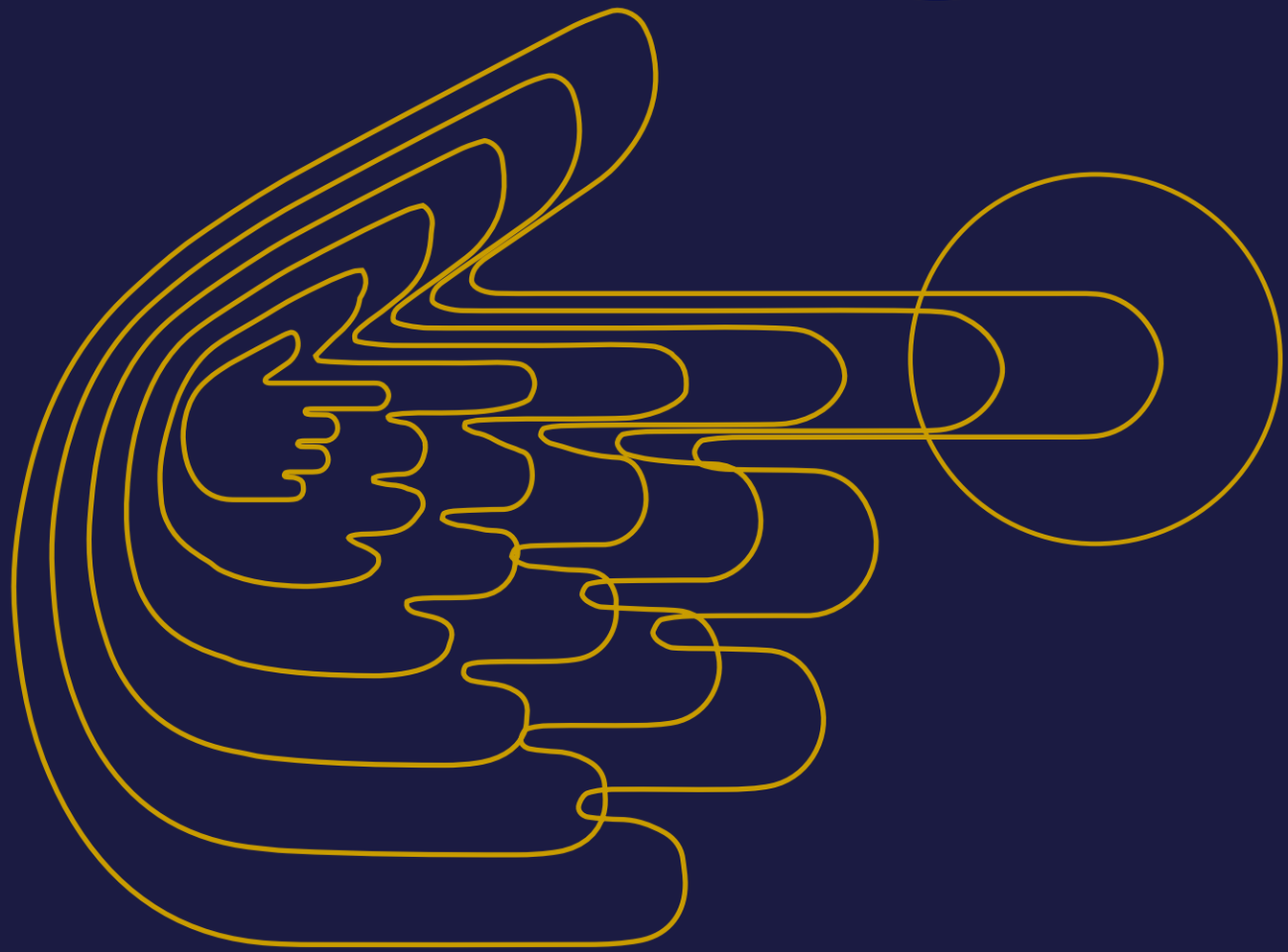
Būtent todėl plečiame atsakomybės lauką. Kibernetinio saugumo subjektų registre 2025 m. – 1 443 organizacijos, privalomų reikalavimų taikymo apimtis išaugo keliskart. Kritines paslaugas teikiančios organizacijos pradeda įgyvendinti konkrečius organizacinius ir techninius standartus – tai svarbus žingsnis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

Esminiai darbai, tendencijos ir statistika



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.

Skaitykite visą ataskaitą

https://kam.lt/wp-content/uploads/2026/05/KS2_2025_ataskaita.pdf

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 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 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 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 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 įtrauktos 1 443 organizacijos, NKSC priežiūros apimtis išaugo beveik 5 kartus. Pradėta kurti nacionalinė saugumo operacijų centrų (angl. *Security Operations Center*, 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 10,1 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 elektroniniu duomenis užšifruojančiais išpirkos reikalaujančio kenkimo programinio kodo virusais (angl. *Ransomware*) ir paskirstytųjų paslaugos trikdymo (angl. *Distributed Denial of Service* (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 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 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“.

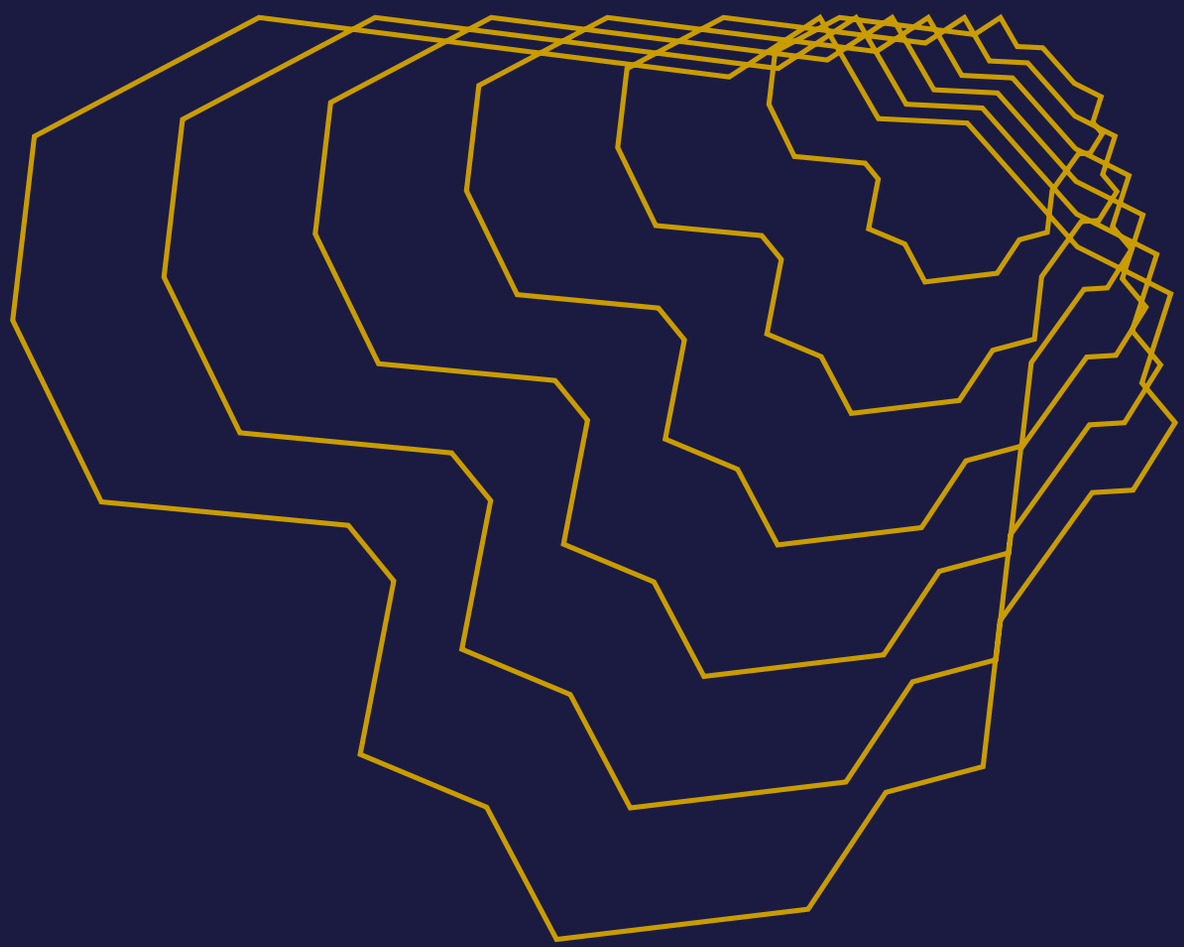
2025 m. DI tapo grėsme ir LK SKD veiklos srityje – jis naudojamas kibernetinėse atakose, socialinės inžinerijos ir sukčiavimo schemose, informacinėse bei psichologinėse operacijose. DI įgalina kur kas didesnį priešiškų kampanijų mastą, greitesnį naratyvų adaptavimą ir aukštesnį personalizacijos bei maskavimo 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.



LIETUVOS KIBERNETINIO SAUGUMO BŪKLĖS APŽVALGA: SVARBIAUSIA INFORMACIJA 2025

Išleido Lietuvos Respublikos krašto apsaugos ministerija,
Totorių g. 25, LT-01121 Vilnius, www.kam.lt
2026-05-20. Užsakymas Nr. GL-413

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